EU Data Cooperatives

L'ingresso delle cooperative di dati nell'ordinamento europeo

a cura di

Fabio Bravo

Giappichelli

EU Data Cooperatives

L'ingresso delle cooperative di dati
nell'ordinamento europeo


IUSTITIAM COLIMUS

EU Data Cooperatives

L'ingresso delle cooperative di dati nell'ordinamento europeo

a cura di

Fabio Bravo

Giappichelli

ISBN/EAN 979-12-211-1146-0
ISBN/EAN 979-12-211-6085-7 (ebook)

Pubblicazione finanziata con fondi del Progetto di Terza Missione 2023/2024 dell'Università di Bologna in tema di Cooperative di dati. Responsabile Scientifico del Progetto: Prof. Fabio Bravo. Partner di Progetto: Università di Bologna, Dipartimento di Sociologia e Diritto dell'Economia (Dipartimento Proponente Capofila) e Dipartimento di Scienze Giuridiche (Dipartimento Aggregato); Legacoop Romagna; Federcoop Romagna; Fondazione PICO Innovazione Cooperativa; Alma Vicoo; Onit spa. La pubblicazione è tra i risultati dell'attività progettuale. I contributi selezionati in quest'opera sono pervenuti mediante procedura di call for papers, presidiata dal Comitato Scientifico Internazionale, dal Comitato Tecnico e dal Comitato Editoriale di progetto.

Sito Internet di Progetto: https://site.unibo.it/cooperative-di-dati

G. Giappichelli Editore

Via Po, 21 - 10124 Torino
Tel. 011-81.53.111
http://www.giappichelli.it

Questo libro è stato stampato su carta certificata, riciclabile al 100%

Stampa: LegoDigit s.r.l. - Lavis (TN)

DATA COOPERATIVES

UNIVERSITY OF BOLOGNA – THIRD MISSION PROJECT

PROJECT PARTNERS

University of Bologna, Department of Sociology and Business Law (Lead and Proposing Department) and Department of Legal Studies (Aggregated Department), Legacoop Romagna, Federcoop Romagna, PICO Foundation (Digital Innovation Hub), AlmaVicoo (University Center for the Training and Promotion of Cooperative Enterprises), Onit S.p.a.

PROJECT WEBSITE

https://site.unibo.it/cooperative-di-dati

Indice

Capitolo XXXVI

Cooperative di dati e principio di neutralità dei fornitori di servizi di intermediazione dei dati: questioni critiche [707]

Daniele Sborlini

Introduzione

Fabio Bravo

Grazie ad un intervento fortemente innovativo del legislatore europeo, mediante l'emanazione del *Data Governance Act* (Reg. UE 2022/868), le *cooperative di dati* hanno fatto ingresso nell'ordinamento europeo *sub species* di intermediari di dati, personali e non personali. In tale regolamento il regime giuridico delle *Data Cooperatives*, seppur insufficientemente tratteggiato, le colloca nel ruolo di fornitori del servizio di intermediazione di dati, non senza talune incongruenze. Ciò nonostante, la nuova disciplina presenta interessanti novità, che meritano di essere esplorate con attenzione, per tradurre in operatività concreta le potenzialità offerte dai nuovi strumenti delineati dal recente regolamento europeo. Le prospettive che si aprono a fronte di tale intervento normativo sono molteplici, di grande respiro e tutte assai rilevanti.

Per un verso c'è la possibilità concreta, per i *data subject* e i *data holder*, di divenire protagonisti delle decisioni relative ai propri dati, esercitando su di essi una *governance duale*, non solo a titolo individuale, ma anche in forma collettiva: attraverso le dinamiche societarie l'interessato, unitamente ad altri soggetti con cui si aggrega, potrà discutere e decidere le modalità di impiego dei dati conferiti ed individuare le forme di redditività, negoziando in forma collettiva con i *data user*, mediante lo schermo societario offerto dalla cooperativa di dati, condizioni economiche e di utilizzo che *uti singulo* l'individuo non è in grado di ottenere.

È risaputo che il modello non intermediato di trasferimento dei dati personali da parte degli interessati ai fornitori di servizi della società dell'informazione ha portato i primi a trasferire, più o meno consapevolmente, nelle mani dei secondi grandi quantità di dati senza un adeguato ritorno in termini economici o di benefici conseguibili. Gli interessati, ovvero i soggetti a cui i dati si riferiscono, tengono a non comprendere la portata economica dell'uso dei dati che conferiscono. L'aggregazione dei *data subject* e dei *data holder* in forma collettiva, con conferimento dei dati in una struttura organizzata di cui tali soggetti conferenti mantengono il controllo, rivoluziona profondamente le dinamiche sull'utilizzo dei dati, consentendo di moltiplicare e ottimizzare i benefici conseguibili.

Nasce un nuovo modo di fare impresa con i dati, distante dai modelli capitalistici: il mutualismo tipico dell'agire in forma cooperativa diviene elemento virtuoso

connotante la gestione economica dei dati, mediante innovativi modelli di *business* che, improntati ad un *neomutualismo digitale*, possono interpretare meglio l'attuale processo di sviluppo tecnologico, economico e sociale.

Si pongono problemi di varia natura. Si pensi ai temi relativi alla qualificazione giuridica delle "cooperative di dati", allo "statuto" delle cooperative di dati e, ancora, alle altre dinamiche di diritto societario. Si pongono ulteriori questioni relative alla sostenibilità economica dell'impresa esercitata nelle forme della cooperativa di dati e alle tecniche di quantificazione degli *asset* costituiti da dati, sia per la formazione dei bilanci e per l'eventuale valutazione in ordine ai conferimenti dei soci (ove si percorresse la via della "conferibilità" dei dati personali o non personali), sia per la corretta individuazione del valore dei dati nelle dinamiche di mercato in cui si forniscono i servizi di intermediazione di dati. Altro tema di rilievo è dato dalla connessione tra cooperative di dati e *intelligenza artificiale*, in quanto le prime possono contribuire ad alimentare in maniera virtuosa i sistemi di IA, il cui funzionamento si basa di necessità sull'uso di grandi quantità di dati. Per altro verso con le cooperative di dati si vengono a realizzare nuovi paradigmi nella tutela dell'interessato, in quanto il nuovo intermediario può agire in maniera più efficace per assicurare agli interessati, soprattutto ove siano membri della cooperativa, una tutela rafforzata dei propri diritti e dei propri interessi. E così via.

Nell'analizzare l'affascinante mondo delle cooperative di dati s'è voluto percorrere la strada del dialogo tra il mondo accademico e quello imprenditoriale, con l'obiettivo, tra gli altri, di porre le basi per la realizzazione di un modello fattibile, sostenibile ed efficiente di «cooperativa di dati», da collocare entro i principi e la cornice teorica del neomutualismo digitale.

È nato così il Progetto di Terza Missione dell'Università di Bologna sulle Cooperative di dati, che ho avuto l'onore di ideare e coordinare in qualità di responsabile scientifico. Al Progetto hanno preso parte, in qualità di Partner, il Dipartimento di Sociologia e Diritto dell'Economia dell'Università di Bologna, quale dipartimento capofila proponente (referente Prof. Avv. Fabio Bravo) e il Dipartimento di Scienze Giuridiche, quale dipartimento aggregato (referente Prof. Daniela Memmo), nonché Legacoop Romagna (referente Dott. Emiliano Galanti). Federcoop Romagna (referente Dott. Luca Petrone), Fondazione PICO Innovazione Cooperativa (referente Dott. Piero Ingrosso), Alma Vicoo (referente: Dott. Piero Ingrosso) e Onit spa (referente: Dott. Vladimiro Buda). Pressoché costante è stata anche la partecipazione di Legacoop Nazionale (Dott. Giorgio Nanni) e dei propri consulenti (Avv. Pier Luigi Morara).

Sono stati attivati tavoli di confronto tra i Partner per la messa a fuoco dei problemi e delle attività per giungere alle possibili soluzioni, che potessero coniugare la concretezza tipica del mondo imprenditoriale con l'analisi tipica del mondo accademico. Ha preso forma, in tale ambito, anche questa pubblicazione, i cui contributi sono stati selezionati a seguito di sette *calls for papers*, su temi considerati rilevanti per gli obiettivi di progetto e, segnatamente: (1) cooperative di dati e diritto societario; (2) cooperative di dati, *data protection* e *data governance*; (3) coopera-

tive di dati e mercati digitali; (4) cooperative di dati, processi produttivi e mutualismo digitale; (5) cooperative di dati e pubbliche amministrazioni; (6) cooperative di dati e soluzioni tecnologiche (IT); (7) cooperative di dati e *case analysis*.

Si tratta di una serie di *calls for papers* vertenti su ambiti disciplinari diversi, attivate con l'intento di promuovere un approfondimento che consentisse di giungere ad un avanzamento delle conoscenze nel settore, mediante la realizzazione di sinergie tra il mondo accademico e quello imprenditoriale.

Le *calls for papers* sono state precedute dalla pubblicazione di due contributi di avvio delle riflessioni progettuali: il primo a mia firma (F. BRAVO, *Le cooperative di dati*, 2023), il secondo a firma di Luca Petrone (L. PETRONE, *Il mercato digitale europeo e le cooperative i dati*, 2023), apparsi sia sulla rivista scientifica *Contratto e impresa*, sia sul sito di progetto.

L'iniziativa si è giovata del prezioso apporto di un Comitato scientifico internazionale e di un Comitato tecnico di assoluto rilievo. Anche le adesioni alle *calls for papers* hanno avuto una caratura internazionale: i contributi provengono, oltre che dall'Italia, anche dall'Argentina, dall'Irlanda e dalla Nigeria. L'opera rispecchia il carattere internazionale dei riscontri avuti, sicché alcuni scritti sono in lingua italiana, altri in inglese e in spagnolo.

Viene offerto, inoltre, un modello di statuto di cooperativa di dati elaborato nell'ambito delle attività progettuali, con l'intento di favorire sia la discussione sugli strumenti operativi per la costituzione e l'operatività di una cooperativa di dati, sia per favorire il concreto avvio delle cooperative di dati.

Nel volume manca un contributo: quello dell'amica Dianora Poletti, che generosamente mi aveva dato la sua calorosa ed entusiastica adesione nel clima di confronto che avevamo coltivato da tempo. Purtroppo la sua prematura scomparsa ha reso impossibile raccogliere in quest'opera le sue sempre acute e stimolanti riflessioni, solo in parte anticipate nei suoi noti scritti sull'attività di intermediazione di dati nel *Data Governance Act*. L'occasione mi è cara per ricordarla affettuosamente.

Il Progetto sulle Cooperative di dati, svolto nel 2023/2024, di cui in quest'opera si raccolgono i primi risultati, segna solamente l'inizio di un percorso destinato a proseguire negli anni a venire, aperto alla partecipazione di chi vorrà unirsi ai lavori.

Capitolo I

Data Cooperatives

Fabio Bravo

Abstract: Data cooperatives have recently been regulated as data intermediation services providers under the Data Governance Act (EU Reg. 868/2022), in a forward-looking approach by the European legislator. The aim is to introduce new dynamics in the data market in favour of European companies, new business models characterised by digital mutualism and solidarity, and new data protection techniques, with the empowerment of the data subjects thanks to the mediation of intermediaries in which, in the cooperative scheme, the data subject participates as a member. This is a highly innovative but incomplete legal framework, that requires careful analysis, at a legal level, in order to frame and resolve the multiple issues that the matter presents and that we intend to address with this work.

1. The EU's Data governance strategy and the inclusion of 'services of data cooperatives' within the scope of 'data intermediation services' in the Data Governance Act (Regulation (EU) 2022/868).

Following the EU strategy for data, outlined by the European Commission in its

communication of 19 February 2020 on a European strategy for data (COM(2020) 66 final), the European legislator has launched initiatives characterised by increased exploitation of personal and non-personal data, taking the regulatory path already defined in this area marked by a mainly protectionist vision. The first of these initiatives involves European data governance, as laid down in the Data Governance Act (DGA), Regulation (EU) 2022/868,[1] adopted just four years after the implementation of the reforms on protection of personal data ushered in with the General Data Protection Regulation (GDPR).[2]

The path taken by the EU is very clear: once the right to the protection of personal data[3] had been construed as a modern understanding of the right to privacy[4] and affirmed as a fundamental right of the individual[5] enshrined in the main sources of primary law (Article 8 of the Charter of Fundamental Rights of the EU; Article 16 TFEU), striking a delicate balance between market needs and the free movement of data,[6] attention was focussed on initiatives aimed at strengthening the data-based 'market'[7] rendered more dynamic by the development of artificial intelligence solutions.[8] The European legislator has thus provided a new impetus to the sector, giving concrete form to the 2020 strategy by issuing the new data governance rules, which take three main forms:

(i) regulation of the re-use of personal and non-personal data managed by the public administration in order to increase their use for purposes other than those for which they were originally collected, by third parties and for commercial or non-commercial purposes, based on the assumption that data managed by public bodies with public funding must be used for the benefit of citizens, businesses and, in gen-

---

[1] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2023 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act).

[2] Regulation (EU) 2022/868 (DGA) entered into force 20 days after the date of its publication in the OJEU on 3 June 2022, and applied, under Article 38 DGA, from 24 September 2023. The GDPR, on the other hand, came into force in 2016 and applied from 25 May 2018.

[3] S. RODOTÀ, *Tecnologie e diritti*, Bologna, 2021, *passim.*

[4] S. WARREN-L. BRANDEIS, *The right to privacy*, in *Harvard Law Review*, 1890, IV, 5, pp. 193-220.

[5] G. GONZÁLEZ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer, 2014.

[6] F. BRAVO, *Il "diritto" a trattare dati personali nell'svolgimento dell'attività economica*, Milan, 2018; N. ZORZI GALGANO (ed.), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milan, 2019; V. RICCIUTO, *L'equivoco della privacy. Persona vs. personal data*, Naples, 2022.

[7] F. BRAVO, *Il commercio elettronico dei dati personali*, in T. PASQUINO-A. RIZZO-M. TESCARO (ed.), *Questioni attuali in tema di commercio elettronico*, Naples, 2020, pp. 83-130.

[8] G. FINOCCHIARO, *Intelligenza Artificiale e protezione dei dati personali*, in *Giur. it.*, 2019, p. 1670 ff.; G. ALPA (ed.), *Diritto e intelligenza artificiale. Profili generali, soggetti, contratti, responsabilità civile, diritto bancario e finanziario, processo civile*, Pisa, 2020; G. ALPA, *Intelligenza artificiale. Il contesto giuridico*, Modena, 2021; A. MANTELERO, *Beyond Data. Human Rights, Ethical and Social Impact Assessment in AI*, Springer, 2022.

eral, the community, although obviously also fulfilling the requirements in relation to protection of the rights and freedoms of data subjects laid down in the GDPR;

(ii) regulation of intermediation services for personal and non-personal data through the activities of 'data intermediation services providers', who stand between users and third-party companies acquiring and using such data, currently without adequate return for users;

(iii) regulation of data altruism, for solidarity and altruistic purposes, facilitated by 'data altruism organisations' (Article 16 ff. DGA).

Precisely within the framework of data intermediation services,[9] the Data Governance Act expressly includes 'services of data cooperatives', providing a definition of such services (point 15 of Article 2 DGA) but not of the 'data cooperative' specifically, meaning that the term and its particular characteristics must be construed using an interpretative approach, a unique case in the data governance area.

The purpose of this paper is both to provide a critical analysis of the legal framework on the subject of data cooperatives in the light of the new European regulation on data governance – through a reading also aimed at creating an overall framework for this issue (much needed given the sporadic measures recently adopted by the European legislator) – and to identify the problems and opportunities that this framework presents, also suggesting a possible path for further analysis aimed at developing scenarios that appear extremely interesting in terms of data exploitation and market digitalisation. This study forms part of the research being carried out at the University of Bologna under the 'Progetto di Terza Missione' (Third Mission Project) on data cooperatives, of which the author is the scientific coordinator. It is also intended as a work stimulating debate and research activities in this unusual field, to which the entire scientific community, the business world and institutions operating in the sector are invited to make their contribution.[10]

2. Definition of the 'data cooperative'.

It can be inferred from an examination of the above-mentioned point 15 of Article 2 DGA defining 'services of data cooperatives' that 'data intermediation services' can also be carried out by a 'data cooperative', understood as '(...) an *organisational structure* constituted by *data subjects*, *one-person undertakings* or *SMEs* who are *members* of that structure, having as its main objectives to support its members in the exercise of their rights with respect to certain data, including with regard to making informed choices before they consent to data processing, to ex-

[9] F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in *Contratto e Impresa Europa*, 2021, 1, pp. 199-256; D. POLETTI, *Gli intermediari dei dati*, in *European Journal of Privacy Law & Technologies*, 2022, 1, p. 46 ff.

[10] See also F. BRAVO, *Le cooperative di dati*, in *Contratto e impresa*, 2023, 3, pp. 757-799, and the project website, available at https://site.unibo.it/cooperative-di-dati.

change views on data processing purposes and conditions that would best represent the interests of its members in relation to their data, and to negotiate terms and conditions for data processing on behalf of its members before giving permission to the processing of non-personal data or before they consent to the processing of personal data' (point 15 of Article DGA).

This is a rather broad notion, which can be difficult to apply. It refers, for instance, to an 'organisational structure' that has as its 'members' data subjects, one-person undertakings and/or SMEs, without express reference to the corporate form. This suggests that the provision of 'services of data cooperatives' can possibly also be carried out by entities other than corporations, although the 'cooperative society' – in all its various forms – is the entity actually called on to play the role of 'data cooperative', at least under the Italian and European legal systems.[11]

One example would be where the 'organisational structure' is 'constituted' by temporary joint ventures (*Associazioni temporanee di imprese*, ATI) or temporary groupings of enterprises (*Raggruppamenti temporanei di imprese*, RTI), or even by 'networks of enterprises' (*Reti di imprese*), which carry out 'data intermediation services' by means of 'cooperation' for the benefit of their members.

The concept of 'data cooperative' is not strictly defined in the DGA and opens the way for different individual forms. Moreover, the European legislator, deliberately concise on this aspect, chose to place the emphasis on the general element, the provision of the 'service', and not on the individual nature of the services provider. In doing so, however, it defined 'services of data cooperatives' without mentioning the 'cooperative society', making generic reference to an organisational structure constituted by its 'members', who could be the natural persons to whom the data refer ('data subjects', within the meaning of Regulation (EU) 2016/679), one-person undertakings or small and medium-sized enterprises (SMEs), which has as its 'main objectives' to provide support to these 'members' in relation to the use of data during the provision of the service. The definition expressly considers three of these objectives, mentioning them alternatively and not (necessarily) cumulatively, as is clear from the disjunctive 'or' between the last and penultimate items. In particular, the 'organisational structure' is required to act mainly to: (i) support its members in the exercise of their rights under the legal system, by providing information to help in the exercise of their data rights, in particular where personal data are concerned; (ii) facilitate an internal discussion among their 'members', based on exchange of 'views on data processing purposes and conditions'[12], in order to 'best represent the interests of its members in relation to their data',[13] (iii) '(...) *or* to negotiate terms and conditions for data processing on behalf of its mem-

[11] On the 'European cooperative society' see in particular Regulation (EC) No 1435/2003 and Directive 2003/72/EC.

[12] Art. 2(1)(15) DGA.

[13] *Ibid*.

bers (...)',[14] in other words to agree with third parties who will use the data which legal and economic terms and conditions should regulate activities involving the use of the personal and non-personal data of its members, whether natural persons or legal entities. The definition of the service in question specifies that such negotiation must be carried out prior to giving authorisation or consent to data processing by the 'members' of the 'organisational structure' providing the service.

The use of the disjunctive 'or' before the reference to the negotiation of terms and conditions for the use of the data should also be read as not tying the provision of the data cooperative service to this aspect, leaving open the possibility of other operational scenarios where the use of the data would be predominantly for the benefit of the 'members' of the structure, with any negotiation being limited to use of the data to third parties.[15]

Further confirmation of the European legislator's openness to not altogether clear-cut solutions with respect to the possible individual form used for the provision of services of data cooperatives is provided by recital 31 of the DGA, which instead adopting the term 'organisational structure' uses 'group', giving it different meanings, either as a synonym of the organisational structure itself and, therefore, of the 'data cooperative' to which the members belong, or as a synonym of an aggregation of several members interested in management or use of data, due to their shared interests and positions with respect to other members, in the context of internal discussion on data governance in order to achieve solidarity-related objectives.

Expressly mentioning '*data cooperatives*', to which no such explicit reference is made in the subsequent text of the Regulation, recital 31 notably states that 'data cooperatives seek to achieve a number of objectives, in particular to strengthen the position of individuals in making informed choices before consenting to data use, influencing the terms and conditions of data user organisations attached to data use in a manner that gives better choices to the individual members of the *group* or potentially finding solutions to conflicting positions of individual members of a *group* on how data can be used where such data relate to several data subjects within that *group*. In that context it is important to acknowledge that the rights under Regulation (EU) 2016/679 are personal rights of the data subject and that data subjects cannot waive such rights. Data cooperatives could also provide a useful means for one-person undertakings and SMEs which, in terms of knowledge of data sharing, are often comparable to individuals.'

Obviously, the 'organisational structure' par excellence, for the purposes of the provision of the services of data cooperatives, should take the form of a cooperative society, to which reference will be made, unless otherwise specified or otherwise apparent from the context.

The defining features of the data cooperative are as follows:

(i) the individual members retain control over their own data and their use by

[14] *Ibid*.

[15] See sections 4 and 5 of this paper on this aspect.

the cooperative, although internal discussion is envisaged, allowing individual members to manage '*individual* governance' of their own personal data, even in the event that decisions are reached at the level of the 'organisational structure' on a specific use of such data, together with the data of other members. The exercise of individual governance should be fostered by the use of dedicated electronic means aimed at facilitating qualitative and quantitative control over data, such as a control dashboard to identify – through a special platform allowing interaction between the members of the data cooperative – which data to provide, the scope of their circulation, for how long, for what purposes and for what types of processing, and so on;

(ii) '*collective* governance' over the data provided by individual members is exercised by the 'organisational structure' (i.e. the data cooperative) and defined by its individual members through (democratic) discussion between them on how data can be used in cooperative form, notwithstanding, however, decisions taken individually by the individual members. In other words, a '*dual* governance' is created, according to which the strategic and operational choices outlined at the level of the data cooperative (through 'collective governance') do not preclude the exercise of 'individual governance', at least when dealing with personal data belonging to individual members who can be considered data subjects within the meaning of the GDPR. In other words, different levels of individual exercise of governance could be defined, depending on the characteristics of the data (personal and non-personal, in addition to the classifications concerning the various types of personal data) and the individual characteristics of the members (whether they are natural persons or legal entities, or whether they are data subjects, one-person enterprises and SMEs). Here again, dialogue and strategic choices regarding the use of data could make use of telematic tools for interaction, through dedicated platforms, with specific functions aimed at fostering interactions of 'participatory' governance, including, for example, the ParteciPA tool proposed by Legacoop Romagna to its associated cooperative societies [16] – comparable to certain examples of good practice in the public administration [17] – and other similar tools of participatory democracy, such as Decidim,[18] a digital platform for the active participation of citizens that can also be used within enterprises, including cooperatives, to foster internal democracy or, in the case of the data cooperative, to launch forms of dialogue and exchange of opinions on specific issues, such as the use of data and the purposes of and conditions for processing that can best represent the interests of members. Electronic tools of

[16] See the Legacoop Romagna management meeting, open to the public, on the question of 'Digital and energy transition', held in Ravenna on 26 June 2023 and organised jointly with Federcoop Romagna, which featured a demonstration of this participatory tool (ParteciPA) for the benefit of Legacoop Romagna member cooperatives.

[17] In this regard, see, merely by way of example, the Italian Government's ParteciPa platform for public consultation and participation processes (https://partecipa.gov.it/), which is also used by other institutional entities, including at local level.

[18] See https://dedidim.org.

participatory democracy can also be used effectively to discuss and resolve internal conflicts on the best use of data, obtaining effective solutions more speedily;

(iii) the interests of the 'members' are pursued, especially as regards the use of personal and non-personal data aggregated and managed through the data cooperative;

(iv) data-based, cooperative data intermediation services for the benefit of the 'members' are provided to the members and possibly also to other third parties, with a view to use and re-use of personal data in accordance with the European data governance regulatory framework.

3. Digital neo-mutualism and data cooperatives.

Article 10 DGA expressly provides that data intermediation rules also apply to the services provided by data cooperatives, without, however, specifying how these 'data cooperatives' can operate in the digital market under data protection, data governance and sector-specific rules on cooperatives (as well as other applicable rules, including competition law).

It is evidently important to update the rules governing this specific sector, identifying the critical issues to be resolved and the opportunities to be seized, in a context that appears to be highly dynamic.

By including the services of data cooperatives in rules applying to data intermediation services, the DGA aimed to support highly innovative scenarios, based on the mutualistic model applied to the exploitation of data in the digital market. These are topics of great interest from both an academic and a business perspective, leading to new ways of doing business in the digital market.

It should be kept in mind that the processes of 'digital transformation' in the cooperative sector lead to consolidation of 'mutualism' as a growth model not only for the economy, but also for the wider society in which the enterprise operates. For cooperative enterprises, digital transformation is not just a modernisation process based on computerisation and the digitalisation of traditional processes, as if we were dealing with the question of merely overcoming analogue processes and tools; instead, it constitutes an integral and fundamental part of a development strategy for the social and solidarity-based economy. Suffice it to note that with digital transformation cooperative enterprises aim to improve the wellbeing, quality of life and work of the people involved in the mutualistic pact, increasing forms of participation and developing the communities in which they operate, for reasons of solidarity, far removed from traditional capitalist models, capable of producing beneficial effects for the relevant stakeholders.

To understand these aspects, it is useful to refer to the concept of 'neo-mutualism',[19] in its more recent form of 'digital neo-mutualism', as a growth model for

[19] P. VENTURI-F. ZANDONAI, *Neomutualismo. Ridisegnare dal basso competitività e* welfare, Milano, 2022.

the economy, businesses, people and communities, within the framework of objectives and tools that the EU has recently put in place with the DGA. Indeed, through this Regulation, the EU intended to pursue the objective of encouraging the creation of a European digital single market based on the use and re-use of data, strengthening the role of European companies.

The European data management model, as intended by the European legislator, stands in contrast to the business model pursued by 'Big Tech' characterised by surveillance capitalism; the former is geared both to establishing an anthropocentric vision, thus ensuring the protection of individual and social solidarity, and to re-establishing a competitive regime among companies, counteracting the substantial oligopoly of multinationals in the digital market, as well as fostering the emergence of much smaller European companies.

See in this sense the European Commission's communication on a European strategy for data of 23 February 2020 (COM(2020) 66), which states, for instance, that 'the EU has everything to play for in the data economy of the future. Currently, a small number of Big Tech firms hold a large part of the world's data. This could reduce the incentives for data-driven businesses to emerge, grow and innovate in the EU today, but numerous opportunities lie ahead. A large part of the data of the future will come from industrial and professional applications, areas of public interest or internet-of-things applications in everyday life, areas where the EU is strong. Opportunities will also arise from technological change, with new perspectives for European business in areas such as cloud at the edge, from digital solutions for safety critical applications, and also from quantum computing. These trends indicate that the winners of today will not necessarily be the winners of tomorrow. But the sources of competitiveness for the next decades in the data economy are determined now. This is why the EU should act now.

The EU has the potential to be successful in the data-agile economy. It has the technology, the know-how and a highly skilled workforce. However, competitors such as China and the US are already innovating quickly and projecting their concepts of data access and use across the globe. In the US, the organisation of the data space is left to the private sector, with considerable concentration effects. China has a combination of government surveillance with a strong control of Big Tech companies over massive amounts of data without sufficient safeguards for individuals.

In order to release Europe's potential we have to find our European way, balancing the flow and wide use of data, while preserving high *privacy*, security, safety and ethical standards' (section 2).

The communication continues: 'The Commission's vision stems from European values and fundamental rights and the conviction that the *human being* is and should remain *at the centre*. The Commission is convinced that businesses and the public sector in the EU can be empowered through the use of data to make better decisions. It is all the more compelling to seize the *opportunity presented by data for social and economic good*, as data – unlike most economic resources – can be replicated at close to zero cost and its use by one person or organisation does not

prevent the simultaneous use by another person or organisation. That potential should be put to work to address the needs of individuals and thus *create value for the economy and society*. To release this potential, there is a need to *ensure better access to data and its responsible usage*' (section 3).

Based on the European Commission's approach, as set out in its communication on the European strategy for data, it seems that the theoretical framework for *digital mutualism* might well consider the introduction of the legal model of data cooperatives as a development factor for data governance.

It is significant that the document-manifesto entitled '*Le cooperative e le sfide dell'innovazione digitale: il neomutualismo in dieci tesi*' (Cooperatives and the challenges of digital innovation: neo-mutualism in 10 theses), drawn up for Legacoop and the PICO Foundation for cooperative innovation by academics (including economists, computer scientists, sociologists and jurists from universities in Milan, Turin, Pisa, Rome, Naples, Palermo and Catania), points out that, despite the risks of digitalisation and the data-driven society generated by a massive concentration of data in the hands of a few very large companies (in other words, risks arising from the 'exploitation for private and merely profit-related purposes of the immense mass of data' and from a 'distorted and non-transparent use of data for the purpose of controlling and directing the behaviour of persons', as well as of workers), there are also great opportunities for companies, society and individuals to be taken advantage of both in terms of their scope and their value (*ivi*, pp. 1-3).

The manifesto-document on digital mutualism goes on to state that: 'The sense and purpose of digitalisation and digital transformation in the cooperative area is to strengthen, reinforce and affirm mutualism as a model for the growth of the economy, society and people,' pointing out that 'for cooperative enterprises, digital transformation is not merely a question of overcoming the analogue, but is part of the strategy for the development of the social and solidarity-based economy. Cooperative enterprises, through digital transformation, aim to enhance wellbeing, while increasing forms of participation, quality of life and quality of work for those involved in the mutualistic pact, supporting and developing the community in which they operate' (*ivi*, p. 4).

The cooperative model, in processes of digital transformation, is capable of orienting the economy towards a plurality of markets, reducing the risks of monopolisation, while at the same time creating 'practices of economic, environmental and social sustainability' (*ivi*, p. 4) by empowering its members to choose the actions to be taken in using solidarity-based criteria, driving the enterprise towards 'a generative and not just extractive economic model' (*ivi*, p. 4).

Significantly, it is also noted that a cooperative approach to data and information and the digital mutualism model lead 'to the development of open, transparent and participatory modes of governance; to the circularity of services and performances; to the exchange of energy and time; to the development of knowledge paths; to the birth of innovative compensatory models; to the definition of new alliances between consumers, members and enterprises; and to the reduction of social risks generated by automation processes' (*ibid.*).

The approach adopted within the theoretical framework of digital mutualism is not only instrumental for the performance of entrepreneurial activity in cooperative form, '(...) but also for society as a whole. Through (…) [digital mutualism] it is natural to face the multiple challenges and social divides that are ushered in by the new era: from the risk of recovery without employment to increasing individualism, or inequality of opportunities and conditions based on gender, ethnicity and age. *Digital mutualism* facilitates a fair redistribution of the added value produced and the emergence of a sustainable economy based on reuse with community circularity. *Digital mutualism* ensures the redistribution of the benefits of automation and robotization, and of data and production efficiency, without innovation contributing solely to profit. Finally, *digital mutualism* fosters cooperation between cooperatives and, by streamlining work, can give people more time, thus offering them freedom in their lives' (*ibid.*).

The document also points out that 'Faced with the epochal changes that are sweeping society and the economy, neo-mutualism innovates and reaffirms the distinctiveness of the cooperative enterprise model with respect to the capitalist model. It extends and expands the establishment of new forms of self-entrepreneurship, intergenerational activity, member protagonism, reciprocity and cooperation between cooperatives and supply chains, as well as the emergence of innovative cooperative enterprises. Neo-mutualism consolidates the role of cooperatives in supporting democracy and communities' (*ibid.*).

Data cooperatives fit into this approach and theoretical framework, which in turn dovetails with the political and economic strategies announced by the European Commission in 2020 and given a legal basis with the enactment of the DGA. In this specific context, data cooperatives, expressly mentioned by the European legislator for the provision of data intermediation services, can be seen as an instrument well able to respond to 'sustainability' needs at an economic, social, and legal level, through a business model characterised by mutual solidarity and democracy that goes beyond an internal frame of reference and using data in such a way that the *social* function of data processing is inevitably developed.[20]

Access to the dynamics of personal data exploitation certainly brings added value both to cooperative enterprises, which act as data cooperatives, and to the individuals participating in them as members and users of the services they provide, as well as to third parties who interact with data cooperatives while participating in data exploitation processes.

The adoption of this kind of *business* model in the digital market centred on the use of data brings about the additional added value of the competitive entry of even small companies and European citizens into a market dominated by large multina-

[20] On these aspects, see recital 4 of the GDPR, and on legal aspects A. RICCI, *Sulla «funzione sociale» del diritto alla protezione dei dati personali*, in *Contratto e impresa*, 2017, 2, p. 586 ff.; F. BRAVO, *Il principio di solidarietà in materia di protezione dei dati personali nelle decisioni del Garante e della Corte di Cassazione*, in *Contratto e impresa*, 2023, 2, p. 407 e p. 412 ff.

tionals.

The use of data collected by data cooperatives, of course, must always be carried out in compliance with the legal conditions determining the lawfulness of the processing, while respecting the fundamental rights of the individual, to be reconciled with the cooperative system of governance in this specific sector.

4. Data cooperatives and models of operation.

The business models that data cooperatives can use to deliver their services have been the subject of widespread analysis in literature appearing internationally, most of which not in the legal field, published in the years prior to the Data Governance Act. [21]

According to one proposed classification [22] based on criteria analysing data flow patterns impacting data governance, data cooperatives can be classified as follows, recalling that the data in question can be personal or non-personal data and that the classification therefore also requires detailed legal analysis on the feasibility of the different solutions, based on the regulations applicable to the type of data processed.

(i) *Member-to-cooperative*. According to this model, data provided by members are shared within the data cooperative for internal use, while the cooperative collects, stores and processes the data for the purpose of providing the service.

(ii) *Member-to-member* (*intra-cooperative*). Under this second model, data are shared between individual members of the cooperative, which assumes the role of facilitator of the data exchange, i.e. the 'intermediary' between individual 'members'. A member would thus be given access to certain data, deemed useful in themselves, for re-use, or for the purpose of forming a benchmark for the evaluation of a certain activity or service or for assessing the performance of a certain action.

(iii) *Federated*. This third model involves movement and sharing of data between different organisations, for instance, between different data cooperatives

---

[21] See, for example J. TAIT, *The Case for Data Cooperatives*, Whitepaper Series, *Open Data Manchester*, 6th September 2021, in *https://thedataeconomylab.com/2021/09/06/the-case-for-data-cooperatives/*; E. BIETTI-A. ETXBERRIA-M. MANNAN-J. WONG, *Data Cooperatives in Europe: A Legal and Empirical Investigation*, White Paper created as part of *The New School's Platform Cooperativism Consortium and Harvard University's Berkman Klein Center for Internet & Society*, Research Sprint, December 2021, in *https://cyber.harvard.edu/sites/default/files/2022-02/Data_Cooperatives_Europe-group2.pdf*; A. PENTLAND-T. HARDJONO-J. PENN-C. COLCLOUGH-B. DUCHARME-L. MANDEL, *Data Cooperatives: Digital Empowerment of Citizens and Workers*, Whitepaper, in *MIT Connection Science*, 1 February 2019, *https://ide.mit.edu/sites/default/files/publications/Data-Cooperatives-final.pdf*; T. HARDJONO-A. PENTLAND, *Data Cooperatives: Towards a Foundation for Decentralized Personal Data Management*, in *MIT Connection Science*, 15th May 2019, https://arxiv.org/pdf/1905.08819.

[22] See J. TAIT, *op. cit.*, p. 5.

with similar purposes or similar data governance processes.

(iv) *Third-party*. This further model is based on more traditional operating arrangements, whereby the data collated by the cooperative are shared with other organisations that have a structure different from the data cooperative, based on the authorisation or consent given by the individual members who are the data subjects, or on relevant sharing agreements that might take the form of licences, after negotiating the terms and conditions for re-use, by the data cooperative acting in its capacity as intermediary.

(v) *Open data*. In this last model, the data provided to the cooperative are made available to and freely accessible by all.[23]

This classification hints at the complexity of the models that can be used for data cooperatives. The complexity involved in each model derives both from the types of data governance adopted and from the nature and type of data and processing operations carried out, as well as from the instruments used to make such models legally possible (from the statutes and regulations of data cooperatives, to agreements between data cooperatives and third parties; from unilateral acts of authorisation and consent for data processing, to agreements between cooperatives and third parties, taking into account the proper role that the cooperative might eventually play). In some cases the cooperative will be able to act on its own, as an entity autonomously and distinct from its members; in other cases it will have to act in the name and on behalf of its members; in still other cases it might act as a facilitator or mediator for the conclusion of agreements or, more generally, of legal acts (including acts such as consent in relation to protection of personal data) that will be stipulated directly by the member (using the tools made available by the data cooperative, including technological solutions, for example use of specific digital platforms allowing interaction, control and exercise of data rights) or by the member through the cooperative, through suitable forms of delegation (see 7.4 below).

5. An example of a data cooperative: Driver's Seat.

Although the European legislation on data cooperatives is quite recent (considering that the DGA dates from 30 May 2022, was published in the OJ on 3 June 2022 and came into force twenty days later, but, according to its Article 38, 'shall apply from 24 September 2023'), data cooperatives are already provided for under foreign law, in the US and Germany, for instance.

A brief examination of a typical case can serve to better understand how this phenomenon is integrated into the legal system, although the operational aspects may be more complex, based on the various operational models of data governance outlined above.

---

[23] See J. TAIT, *op. cit.*, p. 5.

Among the various data cooperatives present in different sectors (e.g. health, transport, agriculture, the gig economy),[24] Driver's Seat seems noteworthy.[25] This is a US data cooperative operating in the transport sector, offering 'ride-sharing' services (along the lines of the Uber model) and 'delivery' services using riders (similar to Glovo or Deliveroo), but managed as a cooperative and adopting a mutualistic arrangement rather than the traditional capitalist model.

The members of the data cooperative use a specific app to exercise control over the data generated in the provision of the service, deciding whether and when to share it. The collected data are then analysed by the data cooperative they belong to in order to maximise the benefit for the members, with a view to exploiting the data to their advantage, in both monetary and non-monetary terms.

While in capitalist models data analysis relating to the provision of the service (ride-sharing, food-delivering, etc.) is carried out to the advantage of the company itself, in order to streamline the production process and maximise profit, with results that often go against workers' interests,[26] the mutualistic model involves analysis of data collected during the course of the activity essentially serves the interests of the individual workers, as well as the cooperative itself and third parties.

Workers, for instance, will be able to benefit from the analysis of the data generated by the system to streamline service provision to their advantage, identifying the most profitable time slots, the most profitable routes and the most profitable modes of remuneration (for instance, whether remuneration is better calculated on the basis of time spent or distance travelled where transport of persons or goods is concerned), and so on. Workers may also benefit from the data in monetary terms where they are transferred (in aggregate form) to third parties, whether public or private, through the cooperative.

Aggregated traffic data generated by Diver's Seat's multiple 'drivers' or 'riders', with the relevant data analysis, allow, for example, public authorities to develop targeted policies on road, traffic and urban development. On the other hand, analysis of data generated by Diver's Seat could be used by businesses to plan and decide whether to open sales outlets and whether to acquire additional space to be allocated for customer parking in an urban context marked by the growing development of e-commerce and food delivery, which could compromise the validity of analysis for business plans carried out using more traditional techniques.

This case study reveals the extraordinary impact of data cooperatives, which, using solidarity-based and mutualistic approaches, can introduce virtuous economic models that are socially sustainable. This example also clearly illustrates the role of the data cooperative, which is not a mere collector of raw data, to be passed on

---

[24] See also E. BIETTI-A. ETXEBERRIA et al., *op. cit.*, p. 8.

[25] See also https://driversseat.co.

[26] The question of riders is relevant here, with the Italian DPA, for example, ordering injunctions against Foodinho s.r.l. on 10 June 2021, online document No 9675440, and against Deliveroo on 22 July 2021, online document No 9685994.

to third parties for their analysis and use: the data cooperative can generate added value from the collection of data if it undertakes further analysis, the results of which can directly serve its members, who will have an immediate return in terms of what the cooperative can achieve to their benefit, and not necessarily in purely monetary terms. Data analysis makes it possible to make better decisions, to increase well-being, to obtain better living and working conditions, as well as making it possible to provide data analysis services for the benefit of third parties, allowing various forms of monetisation to the benefit of such data 'producers'.

6. The applicable data governance rules.

6.1. The obligation to notify the competent authority for data intermediation services and public registration.

The explicit regulatory mention given to data cooperatives in the context of the European data governance framework (the DGA) aims to seize the new market opportunities offered by these business models, which in the data exploitation sector offer enormous potential because they incentivise, as already mentioned, virtuous and socially sustainable business models, because recent regulatory provisions allow new and valid competitors to enter the data market, and because they give data subjects new instruments of control over data, in addition to the individual instruments offered under the data protection regulations.

In addition to opening up the market and enhancing control tools for data subjects involved in data cooperatives, the European legislator is also concerned with establishing supervisory mechanisms, and has provided the relevant instruments and rules.

It should be borne in mind, in this respect, that in point (c) of Article 10, the DGA includes '*services of data cooperatives*' among the intermediation services subject to a mandatory *notification* procedure, to be addressed to the newly established '*competent authority for data intermediation services*' (Article 11(1) and Article 13 DGA)[27]. It also requires compliance with specific '*conditions for providing data intermediation services*', set out in Article 12 DGA, also regulating the use of a common logo for the provision of the service (Article 11(9) and (10) DGA).

The notification, which must be made to the competent authority for data intermediation services prior to the provision of the service, must include, under Article 11(6) DGA, information relating to: (a) the identity ('the name') of the data intermediation services provider; (b) the legal status, form, ownership structure, rele-

[27] In Italy, Legislative Decree 7 October 2024, No. 144, has designated the "Agenzia per l'Italia Digitale" (AgID) – Agency for Digital Italy – as the competent authority under Regulation (UE) 2022/868 (DGA).

vant subsidiaries and, where the data intermediation services provider is registered in a trade or other similar public national register, registration number; (c) the address of the data intermediation services provider's main establishment in the Union, if any, and, where applicable, of any secondary branch in another Member State or that of the legal representative; (d) a public website where complete and up-to-date information on the data intermediation services provider and the activities can be found; (e) the data intermediation services provider's contact persons and contact details; (f) a description of the data intermediation service the data intermediation services provider intends to provide, and an indication of the categories listed in Article 10 under which such data intermediation service falls, which also includes data cooperative services; g) the estimated date for starting the activity, if different from the date of the notification.

Notification to the competent authority authorises the provider of data intermediation services – in this case, the data cooperative services provider – to provide its intermediation services in all Member States (Article 11(5) DGA). Under DGA rules, the service can only start following this notification, which has the effect of authorising the performance of the activity throughout the European market (Article 11(4) and (5) DGA).

If the data intermediation services provider is established outside the EU and intends to offer its data intermediation services, including data cooperative services, within the European market, it must designate a legal representative in one of the Member States in which it wishes to operate, and remain subject to the jurisdiction of that Member State.

The competent authority for data intermediation services, as provided for under Article 11(10) DGA, must then notify the Commission of each new notification by electronic means without delay. Based on the notifications received from each national authority, the Commission will keep and regularly update a public register of all data intermediation services providers – including data cooperatives – providing their services in the Union.[28]

The notification to the competent national authority for data intermediation services and the subsequent entry in the public register of providers, kept by the European Commission, are intended both to make stakeholders aware of the individual characteristics and activities of providers, also for the purposes of possible controls, and to trigger the supervisory functions of the competent authority under the DGA.

As already noted elsewhere, 'The powers of the supervisory authority are very broad: it has supervisory functions over the data sharing service, monitoring and controlling compliance with the Data Governance Act; it can request from the providers of data-sharing services all the information necessary to verify compliance, especially with regard to the requirements and conditions for the provision of the service and, in the event of a breach – following an investigation using a procedure

[28] On this subject, see also Section 6.3 below.

in which the provider must be given the opportunity to respond with observations within a reasonable time – it can take appropriate and proportionate measures to ensure compliance with the Data Governance Act; furthermore and as deemed appropriate, the authority can also impose dissuasive financial penalties (including periodic penalties with retroactive effect) and require the termination or postponement of the provision of the data sharing service.'[29]

6.2. Conditions for service provision and specific features of data cooperatives.

Rules on the provision of the data cooperative service, as for other data intermediation services, are also outlined in Article 12 DGA, which lays down the 'conditions' for providing the services. These provisions pave the way for extensive control by the competent authority, which is required to carry out supervisory activities in the sector.

The first 'condition' concerns both *exclusivity of purpose* with the respect to the use of the data for which the provider is providing the service, and the *criterion of separation*, at individual level, between the provider and the user, of data subject to intermediation. Specifically, point (a) of Article 12 DGA provides that 'the data intermediation services provider [and thus also the provider of the data cooperative service] shall not use the data for which it provides data intermediation services for purposes other than to put them at the disposal of data users and shall provide data intermediation services through a separate legal person the provider of data intermediation services shall not use the data for which it is providing data intermediation services for any purpose other than to make those data available to the users of the data and shall provide data intermediation services through a separate legal entity.'

The rule, as it is formulated, can easily be circumvented, as in the case of corporate groups or related companies, where one of them acts as intermediary and another as data user.

Although this restriction is comprehensible in the case of non-mutualistic data intermediation companies, it appears possibly excessive for data cooperatives, for which it might have been better to allow, in a clear manner, the possibility of using the data provided by members, in line with the requirements of cooperative activities. Indeed, it makes no sense that data collected from members can only benefit other entities, for the purposes of carrying out the intermediation service, and cannot instead be used by the cooperative itself, to its own advantage and therefore also to the advantage of those who participate in the cooperative in accordance with a mutualistic and solidarity-based approach.

---

[29] F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, cit., p. 247.

This line of reasoning extends in two directions: on the one hand, one could intervene at an interpretative level and apply, in a non-rigid manner, the 'condition' concerning the obligation of individual separation between (the services provider of) the data *cooperative* and the data *user*, derogating its application in view of the mutualistic nature of the cooperative, in order to maintain the typical rules of the cooperative society, which need to be coordinated systemically with the hastily drafted provisions, on this point, contained in the DGA. In other words, the very nature of the cooperative could allow for an interpretation that would take advantage of the function of the 'data cooperative', also because the data themselves are being used for the cooperative and therefore also for the benefit of the members who established it.

On the other hand, appropriate regulatory action could perhaps be taken – either at European or national level, to coordinate domestic and EU regulations – to provide more detailed explanation of data governance rules in the specific case of '*data cooperatives*', allowing data to be used by cooperatives in the mutualistic spirit that sets them aside from and contrasts them with the more typically capitalistic model.

This solution also appears plausible in the light of condition (c), which provides that 'the data collected with respect to any activity of a natural or legal person for the purpose of the provision of the data intermediation service, including the date, time and geolocation data, duration of activity and connections to other natural or legal persons established by the person who uses the data intermediation service' can be used only 'for the development of that data intermediation service' by the services provider. Use of such data may concern, for example, the detection of fraud or cybersecurity which are the responsibility of the providers themselves. Condition (c), however, significantly closes by emphasising that the data collected for the intermediation service 'shall be made available to the data holders upon request'.

Where the data intermediation service is provided in the form of a cooperative, therefore, the cooperative itself should be allowed to use the data to operate taking the mutualistic approach, as well as to make them available to 'data holders', in other words those who, according to the definitions of the DGA and in accordance with applicable Union or national law, have the right to grant access to or to share certain personal data or non-personal data (point (8) of Article 2 DGA). Strictly speaking, this expression does not refer to 'data subjects', in other words the natural persons to whom the personal data relate; however, this could be an error, since in the original wording in the proposal for a regulation the definition also included data subjects, amendments to the definition being made in the final draft in response to critical remarks by the EDPB (European Data Protection Board) and the EDPS (European Data Protection Supervisor). In any case, it should be noted that even were the data to refer to data subjects, they would in any case be covered by the GDPR, which provides for exercise of the right of access and portability under Articles 15 and 20 respectively. Therefore, at a systematic level, no problems would arise were the data to be made available by the data cooperative to their member-data subjects.

A further 'condition' for the provision of data intermediation services, set out in point (d) of Article 12 DGA, requires the provider to facilitate 'the exchange of the data in the format in which it receives [them] from a data subject or a data holder' and to 'convert the data into specific formats only to enhance interoperability within and across sectors or if requested by the data user or where mandated by Union law or to ensure harmonisation with international or European data standards', as well as to 'offer an opt-out possibility regarding those conversions to data subjects or data holders, unless the conversion is mandated by Union law.'

This is a provision that not only evidently aims, at a systematic level, ideally to give continuity to the right to data portability referred to in Article 20 GDPR, mentioned above, but which, in terms of the mutualistic approach typically taken by cooperatives, facilitates the sharing and use of data among members, even if they were originally provided in different formats. Similarly, the condition set forth in point (i) is also worth noting, which imposes the obligation on the services provider to adopt appropriate measures to ensure interoperability with other data intermediation services, 'inter alia, by means of commonly used open standards in the sector in which the data intermediation services provider operates'.

It should in fact be considered that 'One of the problems of applying data portability lies precisely in the compatibility between the data formats used by the data controller required to transmit the data and those used by the data controller receiving the transmitted data, at the request of the data subject, in electronic, structured and machine-readable format. The same problem might obviously also arise when sharing non-personal data, so that the system outlined by the (...) DGA relies precisely on the data *intermediaries* to solve technical interoperability issues also, in a value-added offer that, on the one hand, brings together data 'demand' and 'supply' and, on the other, promotes and amplifies this offer through consultancy activities and technical input.'[30]

Other conditions outlined in Article 12 DGA aim to preserve fair competition practices. This is especially true of point (b), according to which 'the commercial terms, including pricing, for the provision of data intermediation services to a data holder or data user shall not be dependent upon whether the data holder or data user uses other services provided by the same data intermediation services provider or by a related entity, and if so to what degree the data holder or data user uses such other services.'

This is another aspect that should be noted in relation to the functioning of data cooperatives, because it is of value not only externally, towards third party beneficiaries or recipients of the intermediation service offered by the data cooperative, but also internally, since attitudes aimed at excluding or discriminating against members in accessing services are precluded. This provision is also confirmed by

[30] F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, cit., p. 251 f.

point (f), which obliges the provider – in our case the data cooperative – to ensure that the procedure for access to its service is fair, transparent and non-discriminatory for both data subjects and data holders, as well as for data users, including with regard to prices and terms of service.

Still on the level of internal relevance, the condition provided for in point (e) is particularly important, since it states that intermediation services, including those of data cooperatives, 'may include offering additional specific tools and services to data holders or data subjects for the specific purpose of facilitating the exchange of data, such as temporary storage, curation, conversion, anonymisation and pseudonymisation, such tools being used only at the explicit request or approval of the data holder or data subject and third-party tools offered in that context not being used for other purposes.'

It follows from the above that (i) models of data cooperatives in which the intermediation service envisages recipients who are the members themselves and not necessarily third parties [31] comply with European law; (ii) 'dual' data governance (collective and individual) is of importance; and (iii) the possibility exists for activating services beyond just data collection and exchange, which are the aims of mere intermediation.

Article 12 DGA also provides for conditions that aim to meet *security* requirements, specifically including non-personal data, in order to add protection standards similar to those in force for personal data under the GDPR. Such conditions include those governing:

(i) business continuity, meaning the recoverability of the data provided and processed by the supplier, as well as their accessibility, in case of events affecting the data processing and management system (point (h));

(ii) procedures to prevent fraudulent or abusive practices in relation to parties seeking access through its data intermediation services (point (g));

(iii) the adoption of technical, legal and organisational measures in order to prevent the transfer of or access to non-personal data that is unlawful under Union law or the national law of the relevant Member State (point (j));

(iv) the adoption of necessary measures to ensure an appropriate level of security for the storage, processing and transmission of non-personal data, with the further requirement of the highest level of security for the storage and transmission of competitively sensitive information (point (l));

(v) the obligation to inform 'data holders' without delay in the event of a data breach and, in particular, in the event of an unauthorised transfer, access or use of the non-personal data that have been shared by them through the intermediation service (in the present context, through the data cooperative).

The DGA introduces another condition for the provision of the service taken from the GDPR: in point (o) of Article 12, the DGA introduces the obligation to keep records of data intermediation activities, recalling the provisions of Article 30

[31] See, *supra*, para. 4.

GDPR on records of processing activities. This is essentially a measure aimed at allowing the supervisory authority of the sector more incisive control over the intermediation activity carried out by the provider (conducted, *inter alia*, by monitoring compliance with the GDPR, acquiring information using powers including those of inspection, ordering the suspension or cessation of the activity and imposing dissuasive, periodic or retroactive administrative pecuniary sanctions, in addition to the power to initiate legal proceedings).

Particular attention should then be paid to the conditions set out in points (m) and (n) of the same article, because of their data protection implications. From the perspective of the European legislator, providers of data intermediation services – including, in particular, data cooperatives – are obliged to pursue the '*best interests*' of data subjects when providing them with services. Therefore, their interest must be deemed to take precedence over that of the providers, who are obliged to facilitate 'the exercise of their rights, in particular by informing and, where appropriate, advising data subjects in a concise, transparent, intelligible and easily accessible manner about intended data uses by data users and standard terms and conditions attached to such uses before data subjects give consent' (point (m)).

Finally, where the intermediary provides the technological means to obtain the consent of 'data subjects' or the authorisations of 'data holders', it must not only specify the third-country jurisdiction in which the data use is intended to take place, but also provide them with tools to both give and withdraw consent and permissions to process data (letter (n)).

Despite of the complex form they are given, the conditions listed in Article 12 DGA do not appear complete: it would be useful to provide, in particular, dedicated rules on the prevention and management of any conflict of interest that could arise between the provider of the intermediation service (including in cooperative form) and the data subjects and data holders who use the service (as members of the cooperative).[32]

6.3. Common logo for services providers, title of 'data intermediation services provider recognised in the Union'.

The new rules contained in the DGA also regulate the introduction and use of a *common logo*, at European level, for data intermediation services, including those of data cooperatives, which can be used – together with the title of 'data intermediation services provider recognised in the Union' – after the intermediary has applied to and received confirmation from the competent authority for data intermediation services that the service complies with the provisions of the DGA, includ-

[32] Cf. F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, cit., p. 252.

ing, in particular, those contained in Article 12 on conditions for providing data intermediation services.

The adoption of a common logo aims to ensure data intermediation services providers are easy to recognise and identify. To achieve this to the fullest extent possible, the European Commission is given the task of establishing a 'design for the common logo' (Article 11(9) DGA). Data intermediation services providers must then display the common logo clearly on every online and offline publication that relates to their data intermediation activities.[33]

To help verify compliance with the DGA and, at the same time, to facilitate the operation of data intermediaries in the European market, the European Commission, as already mentioned, maintains and updates a public register of all data intermediary services providers, including data cooperatives. This register makes available all of the information subject to notification to the national authorities responsible for data intermediation services, with the exception of data relating to the contact persons and contact details of the data intermediation services provider. Such data are, however, easily to obtain by accessing the websites of the intermediaries, using the web addresses that are compulsorily listed in the register (Article 11(6) and (10) DGA).

Those having dealings with data cooperatives and other data intermediation services providers displaying the European logo can thus verify that the provider is included in the public register and view all essential information relating to its activities.[34]

---

[33] The logos have already been produced by the European Commission and were made public in August 2023. They are freely downloadable in various languages and formats, accompanied by a manual with instructions on how to use them: EUROPEAN COMMISSION, *Logos for data intermediaries and data altruism organisations recognised in the Union*, in *https://digital-strategy.ec.europa.eu/en/library/logos-data-intermediaries-and-data-altruism-organisations-recognised-union* (document last consulted on 11 September 2023).

[34] It will therefore be possible to verify, in the public register 'the name of the data intermediation services provider'; 'the data intermediation services provider's legal status, form, ownership structure, relevant subsidiaries and, where the data intermediation services provider is registered in a trade or other similar public national register, registration number'; 'the address of the data intermediation services provider's main establishment in the Union, if any, and, where applicable, of any secondary branch in another Member State or that of the legal representative'; 'a public website where complete and up-to-date information on the data intermediation services provider and the activities can be found (...)'; 'a description of the data intermediation service the data intermediation services provider intends to provide, and an indication of the categories (...) under which such data intermediation service falls into which that data brokering service falls'; 'the estimated date for starting the activity, if different from the date of the notification' (Article 11(6) DGA, as referred to in Article 11(10)).

7. Critical issues emerging from the application of data protection rules and paths toward their resolution.

7.1. From individual to intermediated control.

The new legislation undoubtedly marks an important step in the European legislator's approach to the processing of data, including personal data, moving from a mainly defensive and protectionist position, which had its most recent expression in the GDPR – and which needs to strike a balance with balance with the opposing needs to protect the free movement of data – to a profound rethinking of such movement and relevant control mechanisms.

Control of the data by the individual, with the already established system of data subject consent and, now also, data holder authorisation – in addition to the supervisory function of the Italian DPA (the *Garante per la protezione dei dati personali*) – is accompanied by a mechanism focussed on: (i) prior notification to the competent data intermediation authority, with establishment of a public register of data intermediaries kept by the European Commission; (ii) provision of a comprehensive set of conditions for the provision of the service; and (iii) monitoring of compliance with these conditions by the same authority. On the other hand, a system has been introduced allowing '*enhanced*' exercise of the data subject's rights through the action of the data intermediary on behalf of the data subject, which is likely to be more effective where the intermediary is a data cooperative.

The role of the data intermediary is particularly delicate: acting according to traditional capitalist models might carry the risk of conducting a business activity with a view to maximising profit through strategies and actions that might compromise the rights and interests of the data subject. A case in point would be Weople, a data intermediary acting on behalf of the data subject and exercising, also on the latter's behalf, the right to portability under Article 20 GDPR in order to obtain and gather for itself the personal data of the data subject, using them together with those obtained from other data subjects in its business with third parties in order to obtain remuneration that is partly passed on to the data subject and partly retained as payment for its own intermediation activity.[35]

Prior to the European Commission's communication on a European data strategy (COM(2020) 66) and the work that later led to the DGA, the Italian DPA had shown some concern and intervened in relation to Weople's activities, due to the strong risks possibly entailed in data concentration by the intermediary, exacerbated by its assumption of the exercise of the data subject's rights, on which matter the DPA raised certain doubts and involved the other European authorities on the EDPB.

A preliminary investigation was launched in 2019 following reports forwarded

[35] F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, cit., p. 216 ff.

by large-scale distribution companies that had received requests from Weople to transfer the data that these companies had collected and accumulated over time through loyalty cards: 'Starting in the first months of 2019, several reports have been received by the DPA from large-scale distribution companies complaining of having received from 'Weople' numerous requests to transfer to the platform personal and consumer data recorded in loyalty cards. In fact, the Italian company, managing the app and offering services of various kinds (commercial offers, statistical and market analysis), acts as an intermediary between companies and users by applying, on behalf of these users, to obtain the personal data held by large enterprises with a view to aggregating them in its own database.'[36]

This hints at the potential of the regulatory system that has emerged in relation to data protection and data governance. The data, collected and aggregated by a business, can easily be transferred to another operator who collates and processes them on behalf of the data subject, exercising a crucial intermediation role to the benefit of data subjects and data holders, negotiating data use with third parties.

Under the new data governance rules, the risks generated by intermediation are counterbalanced by the conditions of Article 12 DGA, in particular the condition requiring the intermediary to act in the 'best interest' of the data subject: apart from stating the principle, the provision ties in with the system of control and monitoring of compliance with the regulation entrusted to the competent authority for data intermediation services, to the extent that it is empowered to intervene by ordering corrective measures or imposing the suspension or cessation of the intermediation activity and imposing sanctions.

The regulatory framework on European data governance also underlined the active role of intermediaries, who should act by promoting and protecting the rights of data subjects (and of data holders who are not data subjects), facilitating their exercise by adopting the necessary means to that end (including technological means) and by providing support, including consultancy and representation, when they have been formally authorised to act in the name and on behalf of data subjects.

It is precisely on this point, as we shall see,[37] that the Italian DPA and the EDPB have raised some concerns.

The risks for data subjects (and data holders), which the data governance framework has sought to remedy, appear to be lower in the case of intermediation through data cooperatives, which can generate undoubted effects of empowerment for data subjects (and data holders) in the exercise of their rights because they are structured according to a mutualistic model.

Indeed, this model is better-suited than others for interpreting the regulatory

---

[36] Italian DPA (GPDP), *Dati in cambio di soldi: il Garante privacy porta la questione in Europa. Sotto la lente dell'Autorità la* app "*Weople*", press release dated 1st August 2019, web document No 9126709.

[37] See sections 7.2, 7.3 and 7.4 below.

principle of solidarity,[38] since the cooperative, by its very structure, envisages business operations in the interest of its members, with a democratic structure aimed at fostering discussion, debate and decision-making by them. This system is particularly congenial when the cooperative takes the form of a data cooperative, and its members, whether data subjects or data holders, can discuss choices involving how to use data, as well as make the relevant decisions and maintain data control. Among data intermediaries, data cooperatives are by vocation those best able, in theory, to act first and foremost in interests of data subjects, in accordance with point (m) of Article 12 DGA, above all if they are members.

Indeed, it has been pointed out in the legal literature with regard to the position of data subjects that 'The difficulty in exercising their right to control in a data market shows the need for recourse to forms of organisation, such as data cooperatives or dedicated intermediaries, which would clearly lead to an increasingly collective type of protection, which is given somewhat understated form by Article 80 GDPR, partly carried over by the Italian legislator in the amended Article 142 of the Personal Data Protection Code, which allows the data subject, in submitting a complaint to the Italian DPA, to appoint a voluntary sector body subject to the provisions of [Italian] Legislative Decree No 117/2017 of 3 July that is active in the field of protection of the rights and freedoms of the data to protect their personal data.'[39]

What is more, it is important to note the evident connections between intermediation and the exercise of the power of attorney already highlighted with reference to the data intermediation provided by Weople and based on the exercise of the right to data portability under Article 20 GDPR.[40]

It is worth noting what the legal literature has to say on this matter, effectively arguing that 'In order to ensure that data subjects remain active subjects in relation the flow of their own data, they must essentially share these data with others, providing powers of delegation to exercise their rights. This in turn requires reconsideration of the mechanism of delegation to exercise rights pertaining to the personal sphere, which is covered by [Italian] Law No 675/1996, Article 13 of which provides for the option for data subjects to appoint natural persons or associations as their representatives or attorneys, a provision that subsequently disappeared from Italian data protection legislation.

What is aimed at here is strengthening 'data subject empowerment', although within data movement and increasingly subject to intermediation, since the data subject can request that the data be made available directly to third parties (excluding 'very large platforms' within the meaning of (...) the Digital Services Act), thus transforming data processing into a matter embedded in a dynamic of movement,

---

[38] G. ALPA, *Solidarietà. Un principio normativo*, Bologna, 2022.

[39] D. POLETTI, *op. cit.*, p. 55.

[40] For these aspects relating to delegation, see also F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, cit., p. 244 ff. and, *ivi*, section 4.5 in its entirety.

moreover not relegated to a single contractual relationship but located within a network of contractual relationships.

This is an extremely delicate area, because the market is dynamic and therefore ill-suited to rigidity or anachronistic measures, although the centrality of individuals and the need to protect their rights with strong rules must be safeguarded.'[41]

Data subjects, in the system laid down by the GDPR, find themselves in a position of intrinsic weakness, faced with operators who tend to exclude them from control over their data, making the right to data self-determination a beautiful but essentially empty concept restricted to formal acquisition of consent, where specifically required. Even the control mechanisms entrusted to the supervisory authority prove ineffective in overseeing the fate of all data subjects, since it can act in a limited number of cases, on request or its own initiative, with actions that do not appear to be systematically capable of restoring to all data subjects the sort of governance that the formal enunciation of the right to personal data protection is intended to ensure.[42]

The Data Governance Act seems to intervene with respect to the intrinsic weakness of the data subject that has just been noted, introducing 'dual' governance models, in other words adding to the (weak and ill-defined) 'individual' governance of the data subject another form of governance, which sometimes appears as a '*collective*' governance exercised in the context of the data cooperative that the data subject contributes to creating and establishing, and at other times in the guise of '*aggregate*' governance, exercised by an intermediary (not necessarily the data cooperative), which collects data from different subjects and *negotiates* their use vis-à-vis third parties (acting at the same time on behalf of the data subjects and, in the event of delegation, also representing them, even for the purpose of exercising the rights that the law extends to them).

The individual *governance* outlined in the data protection rules is marked by formal instruments of self-determination and control, such as the expression of consent to the processing of personal data and the rights of the data subject to access and intervene in the processing, and even to object to the processing and request the erasure of data, under certain circumstances. However, these remedies are totally inadequate: consent has turned out to be a weak and merely formal protection tool, totally insufficient to govern the complexity of the forms of processing that have emerged in the digital market; the system based on the rights of data subjects is also intrinsically weak, since they are often unable to assert such rights and find themselves in an unbalanced or asymmetric position that cannot always be overcome by the intervention of the DPA. The DGA aims at strengthening the position of data subjects, taking advantage of the action carried out by intermediaries who, by handling the data of several data subjects, can act as an instrument offering

---

[41] D. POLETTI, *op. cit.*, p. 55 f.

[42] For an analysis of the discrepancies, see the volume by V. RICCIUTO, *L'equivoco della* privacy. *Persona vs. dato personale*, Naples, 2022.

substantial protection, thanks to data subject empowerment that can be achieved through 'intermediated' control. At the same time, a further system of regulation and control is organised in the field of data intermediation, overseen by national authorities at domestic level and by the European Commission at central level.

7.2. Possibility of negotiation on behalf of interested parties.

EDPB-EDPS Joint Opinion 03/2021 on the proposal for a regulation on European data governance (version 1.1 of 9 June 2021) voiced certain criticisms of the *data cooperative service*, including that the service lacked a clear concept, in particular with reference to its nature.[43] The definition of these data intermediaries and the rules applicable to them, especially with regard to their obligations, was also criticised for lack of clarity, which might result in uncertainty in the provision of these services.[44] These problems were not resolved in the final text of the regulation.

The EDPB and the EDPS considered, in particular, that the power to negotiate processing on behalf of data subjects and the position that the European legislator aimed to grant to data cooperatives would add nothing to the power and rights that data subjects already enjoyed under the GDPR, given the rules on transparency obligations for the intermediary data controller and obtaining the free, specific and informed consent of data subjects under Articles 6 ff. of the GDPR.

The passages subject to critical remarks included those contained in recital 24 of the proposal for a regulation on European data governance, later merged with recital 31 in the final DGA text. Issue was taken with the wording stating that 'Data cooperatives seek to achieve a number of objectives, in particular to strengthen the position of individuals in making informed choices before consenting to data use, influencing the terms and conditions of data user organisations attached to data use in a manner that gives better choices to the individual members of the group or potentially finding solutions to conflicting positions of individual members of a group on how data can be used where such data relates to several data subjects within that group (…).'

In this regard, the above-mentioned EDPB and EDPS joint opinion considered, however, 'the position of individuals in making informed choice, or the solving of potential dispute on how data can be used, are not to be considered as *negotiable* conditions but rather as data controllers' obligations as per Regulation (EU) 2016/679. In this regard, it is also to be pointed out that the reference in Recital (24) of the Proposal [now recital 31 of the DGA] to data that would "pertain" to several data subject, insofar as it relates to personal data, may not be consistent with the definition of personal data as per Regulation (EU) 2016/679, which refers to "any information relating to an identified or identifiable natural person".'[45]

---

[43] EDPB-EDPS, Joint Opinion No 3/2021, cit., section 3.4.2.

[44] EDPB-EDPS, Joint Opinion No 3/2021, cit., section 3.4.2.

[45] EDPB-EDPS, Joint Opinion No 3/2021, cit., section 3.4.2.

Again, the EDPB and EDPS found a contradiction between the wording of recital 24 of the proposal for a regulation, which explicitly stated that 'the rights under Regulation (EU) 2016/679 can only be exercised by each individual and cannot be conferred or delegated to a data cooperative', and the power the data cooperative itself would have to negotiate on terms and conditions to be obtained for the benefit of its individual members, before they give consent to the processing of their personal data.

The EDPB and EDPS considered that 'the "terms and conditions" for the processing of personal data are – as a matter of fact – those enshrined in the GDPR and, therefore, they cannot be amended or superseded by means of a contract or other type of private arrangements.'[46]

The position expressed in the joint opinion appears to be the result of a fundamental misunderstanding, which is reflected in questions of method and cannot be agreed. The terms and conditions referred to in the new European data governance framework – on which data cooperatives can negotiate – are quite different from the conditions for lawfulness of processing under the GDPR, which form the legal basis for processing.

Once the legal constraint preventing processing activities from being carried out, with a view to protecting the rights and freedoms of the data subject, has been removed and the legal prerequisite enabling the data holder to carry out processing activities on personal data has been fulfilled – which is, first and foremost, the consent of the data subject, in other words a unilateral act of authorisation aimed at removing the legal constraint that the European legal system has provided for with a view to referring to the data subjects themselves any decisions involved in balancing the interests of processing stakeholders, in order to ensure data self-determination –, the use of personal data (and not '*personal data*' per se) can be the subject of negotiation and contracting, through an agreement that is reached by means of contractual consent (not authorisation), concerning the economic and contractual terms and conditions established between the parties.[47]

---

[46] EDPB-EDPS Joint Opinion 3/2021, cit., section 3.4.2.

[47] For this reconstruction see F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, in G. FINOCCHIARO (ed.), *La protezione dei dati personali in Italia*, Bologna, 2019, p. 140 ff.; F. BRAVO, *Lo "scambio di dati personali" nella fornitura di servizi digitali ed il consenso dell'interessato tra autorizzazione e contratto*, in *Contratto e impresa*, 2019, 1, p. 34 ff. also with commentary on two important Supreme Court cases: Court of Cassation No 1748 of 29 January 2016, the *Segafredo Zanetti case*, and Court of Cassation No 17278 of 2 July 2018, the *AdSpray* case. In the first of these, the Italian Court of Cassation clarified that even where authorising and contractual consent is given in unitary fashion in the same case dealing with a contractual matter, with a single manifestation of will, the authorising consent can still be freely revoked to protect personal rights, and the contractual bond cannot prevent such revocation. Thus, the Court of Cassation also allows the possibility of joint manifestation of the two components (authorising and contractual) which nevertheless remain ontologically distinct, since one relates to the legal regime of personal

The rules on data governance leave unaltered the system for the protection of data subjects with regard to the conditions for lawfulness of processing, which must still apply in this case, and entrust the data cooperative, in its role as intermediary, with the negotiation activity carried out for the benefit of its 'members', in order to obtain advantages far greater than those that data subjects would achieve alone, since they lack any real negotiating power.

The data cooperative, in fact, can aggregate a significant amount of data derived from its members, be they data subjects or data holders, and – in compliance with the conditions of lawfulness laid down in Articles 6 to 9 GDPR – can achieve more favourable conditions for data subjects, which the latter would not otherwise be able to obtain, something borne out by recent market experience.

However, the regulatory framework is significant because it leads to 'assisted' and 'intermediate' forms of collective management of negotiation, for the purposes of conducing data processing contracts.

7.3. Autonomy of consent of the data subjects who are members of a data cooperative, albeit expressed in the formation the will of the entity: resolutions adopted at cooperative members' meetings and data governance.

Another relevant issue concerns correct identification of the condition for the lawfulness of the processing carried out by or through the data cooperative, given that the data subject, acting as a member of the cooperative itself, contributes to 'forming the will' of the entity, through the mechanisms used for adopting members' resolutions.

The need already highlighted to maintain 'dual' control over processing,[48] which does not invalidate the 'individual' governance of the data subject, also applies to consent, which is relevant under Article 6(1)(a) and, where applicable, Article 9(2)(a) of the GDPR, since the member-data subject's contribution to the formation of the will of cooperative cannot result in the automatic transfer to the cooperative of the data subject's own power of self-determination. This principle has

---

rights and the other the legal regime of contract law. Obviously, if the conditions for lawfulness of the processing are those set out in Article 6(1)(b) of the GDPR, the relevant manifestation of will is of an exclusively contractual nature, insofar as the consent to the processing of the data, which is here not required as a prerequisite for lawfulness, is not a prerequisite C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, Torino, 2021, p. 77; G. RESTA, *I dati personali oggetto del contratto. Riflessioni sul coordinamento tra la Direttiva (Ue) 2019/770 e il Regolamento*, in V. RICCIUTO-C. SOLINAS (ed.), *Forniture di servizi digitali e "pagamento" con la prestazione dei dai personali*, Milan, 2022, p. 74; on this subject see also, with reference to unitary manifestation of consent, albeit with different nuances, V. RICCIUTO, *L'equivoco della* privacy. *Persona vs. dato personale*, cit., p. 110 ff., 119 ff., 140 ff.

[48] See section 2 above.

already been expressed in Supreme Court of Cassation ruling No 17911 of 1 June 2022,[49] in a case involving unlawful processing carried out by a cooperative with respect to a member-worker. The latter's lack of consent to processing was contested and the will of the cooperative, formed in the context of a resolution taken at a members' meeting resolution on the functioning of the cooperative, was deemed not to have remedied this lack (the case concerned the publication on the notice board of data relating to disciplinary criticisms and the cooperative's evaluations of the activities performed by the member-worker, through the use of 'smiley faces' placed next to their photos, as part of an internal 'competition'). The court of cassation, in the ruling, in fact clarified that it was irrelevant that 'processing would in any case have been justified, in this case, by the consent expressed within the associative relationship freely established between the members and the cooperative (and between the members themselves). The circumstance that the relationship is associative (or even organisational) in nature, in such a way that the members themselves contribute to the management and formation of the will of the entity in the forms laid down at the members' meeting, does *not in any way imply that any processing of data becomes per se consented to by the individuals in accordance with the forms laid down at the members' meeting.*'[50]

This principle also applies to processing activities carried out by data cooperatives, both as controllers of the data provided by members and as intermediaries within the meaning of the DGA.

It should however be noted that the Court of Cassation did not wish to exclude *a priori* that the will of the data subject, as expressed in the formation of the members' resolution, might constitute a condition for the lawfulness of the processing carried out by the cooperative: the participation in the formation of the entity's will cannot automatically be understood as an expression of will, in the sense that the entity's will does not replace the will of the individual who contributes to its formation. Instead, the specific case must be investigated to determine the presence or otherwise of the prerequisites for the proper formation of the data subject's consent to the processing of personal data, which must, *inter alia*, be sufficiently informed, specific and free.

In the specific sphere of operation of the data cooperative, therefore, it is important to avoid considering issues concerning the data subject's consent to processing of personal data as something absorbed into the entity's decisions. The two levels of governance, individual and collective, must remain distinct.

Any investigation of a specific case will also have to address the issue of freedom of consent in the event that the data subject is a member-worker of the cooperative, since any subordinating employer-employee status – or in any case the un-

[49] On which see S. THOBANI, *Consenso al trattamento e delibere assembleari*, in *Giur. it.*, 2022, 12, p. 2599 ff.

[50] Italian Court of Cassation, division I, ruling No 17911/2022, cit.

equal contractual position involved in the relationship – could jeopardise freedom of consent to process personal data.[51]

Also in relation to the above Supreme Court ruling No 17911, in the appeal, the Italian DPA had the opportunity to clarify in this regard that 'even if the consent of each worker were actually provided for (and documented) (...), this manifestation of will could not constitute a legal basis for legitimising the processing of personal data (other than the special categories of data referred to in Article 9 of Regulation (EU) 2016/679), in light of the asymmetry between the respective parties to the employment relationship and the consequent need, possibly, to ascertain, on each occasion and in concrete terms, the effective freedom of the consent expressed.'[52]

It follows that, even in the case of data cooperatives, investigations into freedom of consent to process personal data must be carried out in greater detail where the data concern member-workers and their work.[53]

---

[51] With regard to the subordinating employer-employee status within the relationship between a cooperative and a member-worker, see, *inter alia*, ruling No 29973 of 14 October 2022 of the Court of Cassation, division IV. The investigation must cover the proper conduct of the employment relationship. The Court of Cassation, in the aforementioned ruling, which also referred to existing case-law on cooperative societies, reiterated that 'The fact that the employment relationship accompanies the associative relationship, which in turn is characterised by participation in business risk, does not exclude the possibility that, within the organisation of the enterprise, a commutative contract of employment can be found together with the contract of participation in the community (para. 4 of ruling No 13967 of 26 July 2004 of the Court of Cassation, united divisions). This possibility is made quite clear in Article 1(3) of Law No 142/2001, which allows the members to establish, with their membership or subsequent to the establishment of the associative relationship, a further employment relationship, even taking the employer-employee form.' Moreover, the Court of Cassation added, in the above ruling, that the distinction between a self-employed relationship and an employer-employee one cannot always be detected in the light of ambiguous criteria such as the exercise of management and disciplinary power by the employer: if the exercise of such power is a sure indication of subordination, its absence does not in itself denote the autonomous nature of the relationship (ruling No 3674 of 27 March 2000, Court of Cassation, labour division). In particular, the normal signs indicative of subordination, such as the fact that of the employee to is subject to the employer's directions, organisational and disciplinary power, have no bearing when the service under the contract is extremely basic, repetitive and predetermined in its manner of performance (ruling No 24561 of 31 October 2013 of the Court of Cassation, division II). At this juncture, subsidiary distinguishing criteria must be used, such as the continuity and duration of the relationship, the manner in which remuneration is paid, regulation of working hours, the presence of an even minimal enterprise-type organisation (including which party is required to provide the instruments necessary for work), as well as the existence of an effective power of self-organisation on the part of workers, something that might also be inferred were they to have other employment relationships (ruling No 9251 of 19 April 2010 of Court of Cassation, labour division, also referred to by the Court of Appeal of Milan as grounds for its decisions No 1536 of 21 January 2009 and No 8569 of 5 May 2004).

[52] Italian DPA (GPDP), Decision No 500 of 13 December 2018, online document No 9068983.

[53] For example, cases similar to the Driver's Seat case analysed above in section 4.

7.4. Possibility of delegating exercise of rights under the GDPR.

In the transition from the text of the proposal for a regulation to the final text of the DGA – and with reference, respectively, to recital 24 (of the proposal) and recital 31 (of the DGA) on data cooperatives – the European legislator decided to remove both the reference to the fact that 'the data subject's rights under Regulation (EU) 2016/679 *can only be exercised by each individual'* and the reference to the fact that these rights '*cannot be conferred or delegated to a data cooperative*'.[54]

In the final version of the text of the DGA, therefore, the original preclusions have disappeared, although the principle of the inalienability of the data subject's rights, including the right to withdraw consent to the processing of personal data, which cannot be abdicated by the data subject even if the exercise of rights is delegated to the data cooperative, is reiterated.

This suggests that data rights can never be transferred and, equally, any operations aimed at making the contribution of members, who provide data to cooperatives, into a contribution *in rem* cannot be countenanced. Personal data are of an entirely different nature and all that can be transferred is the right to use the data, which can always be revoked by the data subject, but not the data themselves, over which the data subjects continue to retain control.

Legal scholars, in commenting on the regulatory developments outlined in the GDA and their implications in the field of data cooperatives, have remarked that 'Although interpretation the European law based on the categories of domestic law should always be conducted with great caution, it would seem reasonable to assume that while the prohibition on a waiver, as a typical act of renunciation, implies that it is impossible to grant rights to the enterprise (i.e., a legal act with ef-

---

[54] Recital 24 of the proposal for a regulation on European data governance expressly provided that 'Data cooperatives seek to strengthen the position of individuals in making informed choices before consenting to data use, influencing the terms and conditions of data user organisations attached to data use or potentially solving disputes between members of a group on how data can be used when such data pertain to several data subjects within that group. In this context it is important to acknowledge that the rights under Regulation (EU) 2016/679 *can only be exercised by each individual and cannot be conferred or delegated to a data cooperative*. Data cooperatives could also provide a useful means for one-person companies, micro, small and medium-sized enterprises that in terms of knowledge of data sharing, are often comparable to individuals.'

The subsequent rewording, contained in recital 31 of the final text of the DGA, instead reads as follows: 'Data cooperatives seek to achieve a number of objectives, in particular to strengthen the position of individuals in making informed choices before consenting to data use, influencing the terms and conditions of data user organisations attached to data use in a manner that gives better choices to the individual members of the group or potentially finding solutions to conflicting positions of individual members of a group on how data can be used where such data relates to several data subjects within that group. In that context it is important to acknowledge that the rights under Regulation (EU) 2016/679 *are personal rights of the data subject and that data subjects cannot waive such rights*. Data cooperatives could also provide a useful means for one-person undertakings and SMEs which, in terms of knowledge of data sharing, are often comparable to individuals.'

fects *in rem*), this does not preclude the conclusion of a delegatory contract (with powers of representation), as an act involving a mere duty. There would thus seem more room for manoeuvre, at least for the external protection of data subjects' rights by a data cooperative acting as a representative of its members.'[55]

In the point 131 of their Joint Opinion No 3/2021, the EDPB and EDPS indeed show that they agree with the principle that data subjects' rights cannot be delegated (which is stated in recital 24 of the proposal for a regulation on European data governance) and point out that this principle contradicts the rules allowing delegation to the data cooperative of the power to negotiate terms and conditions of greater benefit to data subjects.

The final decision of the European legislator, however, was to resolve the contradiction by protecting the data cooperatives' power of negotiation, at the same time eliminating any reference to the prohibition on delegation. Delegation, therefore, is to be considered fully admissible in matters of personal data protection, not only due to the European legislator's change of mind during the passage from proposal to the final text of the regulation, but also for reasons of a systematic nature.

The fact that consent to the processing of personal data is not a strictly personal act, but may also be given by a representative, is also borne out by the GDPR: this is made clear in Article 8 on the child's consent, where it is established that, in cases where minors give consent personally, the right can be exercised on their behalf by the holder of parental responsibility.

Moreover, no rule expressly contradicts this.

It should also be recalled that in Italy, Article 13(4) of Law No 675/1996, later incorporated with amendments into the Personal Data Protection Code (Legislative Decree No 196/2023), literally states that 'In exercising the rights referred to in paragraph 1, the *person concerned may grant*, in writing, *power of attorney or proxy to natural persons or associations.*'

The Italian legislator, in implementing Directive 95/46/EC on the protection of personal data, therefore expressly provided for the possibility of delegation of the exercise of the data subject's rights.

When applying of this provision, the Italian DPA was able to clarify, in a case involving a sports association in relation to the publication of lists, that 'it is not conceivable, nor provided for by law (...) that the association can exercise the personal rights available to each data subject, unless it can demonstrate the existence of a specific *delegation by* the individual member.'[56]

Also in more recent times, after the coming into force of the GDPR, exercise of

---

[55] Thus G. RESTA, *Pubblico, privato e collettivo nel sistema europeo di governo dei dati*, in *Riv. trim. dir. pubbl.*, 2022, 4, pp. 971-995, and *ivi* section 5.

[56] Italian DPA (GPDP), Decision of 30 November 1999, online document No 1164456. See also F. BRAVO, *Associazioni sportive dilettantistiche (ASD) e protezione dei dati personali negli orientamenti del Garante*, in *Diritto dello Sport*, 2021, 2, pp. 11-29, *ibid*., p. 24 f.

the data subject's rights by delegation has repeatedly been shown to be lawful. Thus, for example, the Italian DPA has explained that 'the rules on the protection of personal data provide, in the area of health, that information on the state of health must be communicated to data subjects and can only be communicated to third parties for sufficient legal reasons or on the instructions of the data subjects themselves, and on condition that they grant written *powers* (Article 9 GDPR and Article 83 of the Personal Data Protection Code, in conjunction with Article 22(11) of Legislative Decree No 101//2018 of 10 August; see also general measure of 9 November 2005, available at www.gpdt.it, online document No 1191411, deemed compatible with the GDPR and the provisions of Decree No 101/2018; see Article 22(4) of the said Legislative Decree No 101//2018).'[57]

A power of attorney was also deemed admissible for the purposes of lodging a complaint with the Italian DPA in lieu of the data subject. Indeed, in measure No 209 of 12 May 2022, Online document No 9790093, the DPA ruled on the '(...) complaint submitted to the DPA under Article 77 GDPR on 10 May 2020 in which XX, acting on *powers* granted by his brother XX, resident abroad at the time when the complaint was lodged, requested that Google LLC be ordered to remove from the search results available in association with the name of his brother two URLs reporting news dating back to 2017 relating to a criminal proceeding concerning the complainant in relation to an event that occurred in the Canadian city of XX.'

Article 80(1) of the GDPR expressly provides that the data subject shall have 'the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law.'

As seen above, however, the rule has been loosely interpreted by the Italian DPA, which allowed the complaint to be lodged by the brother of the data subject.[58]

Another and particularly significant case concerned the activity carried out by Hoda, the provider of the Weople service acting as an intermediary to acquire the personal data of data subjects by exercising the right to portability under Article 20 GDPR on behalf of its customers. The Italian DPA, alarmed at the possible risks for data subjects, opened an investigation and referred the matter to the EDPB, but without stopping processing, thus admitting that the intermediary could be granted powers to exercise this right.

---

[57] Italian DPA (GPDP) Decision No 174 of 29 April 2021, online document No 9676143.

[58] Italian DPA (GPDP) Decision No 209 of 12 May 2022, online document No 9790093, cited above.

It should be recalled that in the Decision of the Italian DPA issued on 1st August 2019, online document No 9126709, already referred to above,[59] the DPA stated that 'Starting in the first months of 2019, several reports have been received by the DPA from large-scale distribution companies complaining of having received from 'Weople' numerous requests to transfer to the platform personal and consumer data recorded in loyalty cards. In fact, the Italian company, managing the app and offering services of various kinds (commercial offers, statistical and market analysis), acts as an intermediary between companies and users by applying, on behalf of these users, to obtain the personal data held by large enterprises with a view to aggregating them in its own database.' Significantly, the same document went on to state, on the matter dealt with in summary form in these pages, that 'The Authority's attention was focused, in particular, on correct application by the company of the so-called right to 'data portability' introduced by the new European regulation, further complicated by the fact that this right was being exercised by delegation of powers and with the consequent risk of possible duplication of the databases that were subject to portability.'

The Weople case was also examined in a fact-finding *investigation on Big Data*, carried out jointly by the Italian DPA, the Italian competition authority (AGCM) and the Italian communications authority (AGCOM) (see Italian DPA (GPDP), online document No 9262297 of 10 February 2020), where the business model underlying the provision of the service, based on the exercise of the right to data portability by means of delegation of powers to the intermediary, had been positively assessed, because 'Such initiatives could act as a consumer empowerment tool potentially capable of partially overcoming the above-mentioned restrictions under the current regulation of the right to data portability, by contributing to raising users' awareness of the economic value of their personal data arising from payment for the use of such data by third parties.'

All of this confirms the possibility that the data subjects can delegate power to exercise their rights under the data protection rules, albeit subject to the limitations evident from the regime of protection guaranteed by data subjects themselves and the limitations now laid down in Article 12 of the DGA.

Thus, *inter alia*, delegation of powers can never entail the loss of the rights of the data subjects, who always retain the right to exercise them themselves and to revoke the powers granted. It follows that powers must be delegated in a specific and not generic manner, and in relation to specific processing purposes and identified processing operations. Delegation of powers must also always be such as to guarantee the rights and freedoms of data subjects, as well as to achieve the data subjects' best interests (see also point (m) of Article 12 DGA). Other limits, of a general nature, concern the necessary observance of the principle of fairness and the general clause on good faith. A further limitation obviously also derives from

[59] See section 7.1.

the prohibition of abuse of rights by the attorney, according to the general principles of our legal system.

Both the data protection authority and the authority responsible for data intermediation services, as relevant, will be able to exercise control over these limitations.

8. Future developments: further perspectives and needs for analysis, between competition law, contractual dynamics and digitisation of markets.

Although the regulation of data cooperatives is only hinted at in the Data Governance Act, it has already been possible to identify and analyse its characteristic features and major legal issues. This analysis deserves to be continued, given the importance of the topic and its profound implications for the digital market.

The framework outlined in the new regulation undoubtedly opens up interesting scenarios, on a theoretical level and vis-à-vis its application, as well as for the development of the market and the exploitation of data, with a view to increasing protection for the data subject in the spirit of digital neo-mutualism (as examined above).

The study of the legal implications of data cooperatives appears to be at an early stage, with multiple aspects to be explored and addressed in future research.

One of these concerns the extent and limits of the *individual form* that 'data cooperatives' can take to operate under the DGA, in other words, the extent to which *cooperative forms of intermediation services* are also possible outside the adoption of the legal form of the *cooperative society*.

This also points the way to another related issue, that of compliance with *competition* law.

Whether one adopts, by default, the cooperative society form, or indeed another form for the establishment of the 'organisational structure' for the provision of 'data cooperative services', competition compliance issues may arise.

It should be noted on this point that the European Commission, in its communication on the promotion of cooperative societies in of 23 February 2004 (COM(2004) 18 final) aimed to address the 'confusion and concern regarding the application of competition rules to cooperatives' (see point 3.2.7) that had arisen during the consultation process on cooperatives. It was clarified that 'Co-operatives that carry out economic activities are considered as "undertakings" in the sense of Articles 81, 82 and 86 to 88 of the European Community Treaty (EC). They are therefore subject in full to European competition and state aid rules, and also to the various exemptions, thresholds and *de minimis* rules. There are no grounds for special treatment of co-operatives in the general competition rules; however certain aspects of their legal form and structure should be taken into account on a case-by-case basis, as previous decisions and rulings have demonstrated.

Most cases have involved co-operatives of legal entities (rather than those of

physical persons). Such a co-operative is both an association of undertakings, and (where it has an economic activity) an undertaking in its own right. Both the co-operative and its members are therefore subject to competition rules. Furthermore, competition rules apply not only to the agreements between undertakings (e.g.: the creation of a co-operative and its founding statutes), but also to the decisions made by the co-operative's internal bodies. Therefore, whereas organisation as a co-operative may not necessarily conflict with Article 81 EC, its subsequent behaviour or rules might be considered restrictive of competition. The Commission invites stakeholders' organisations and business support services to ensure a wide dissemination of the competition rules which may be of relevance to the cooperatives in Europe.'

Other questions concern the manners in which cooperative societies will have to deal with the principle of neutrality set out in point (a) of Article 12 DGA, in the light of recital 31 and the definition of the 'services of data cooperatives' provided for in point 15 of Article 2 DGA. Depending on the specific nature of the data co-operatives, additional ways are envisaged of intervening on behalf of the data subject.

Further research will also be required into the compatibility of the different business models of data cooperatives (see section 4 above) with the regulatory framework laid down in the DGA, in the light of the developments in domestic law under the supervision of the competent authority for data intermediation services.

Furthermore, it will be necessary to see how the regulation of data cooperatives interacts with that of cooperative societies proper, examining how data governance and the performance of data intermediation services can be exercised in cooperative form under the current legal regime for cooperatives. In this regard, it will be necessary to examine the issues of the relationship between the formation of the entity's will and the consent of the member, the issue of whether the member-workers' consent is given freely and the issue of determining the conditions for the use of the latter's personal data, also in relations with third parties. What is more, other delicate questions, such as those concerning the 'contribution' of data by the members to the cooperative, both in cases involving the personal data of members who are natural persons (data subjects) and in cases where the members of the cooperative are not a 'data subjects' in the technical sense, but rather 'data holders' within the meaning of the DGA. A case in point would be where one such member is a one-person undertaking or an SME and intends to contribute the data of third-party data subjects, collected and processed in the context of its own business activity, to the cooperative and then transfer them to the data cooperative of which it is a member. Complex scenarios now open up: the connection between company law and the nature of the contribution overlap with the GDPR's data protection regulations and, more recently, with the rules on data governance and data cooperatives laid down in the DGA, which emphasise data intermediation and an approach focussing on reuse.

Further fields of investigation might also concern the interrelationships between different legal areas, not only between GDPR (Regulation (EU) No 2016/679) and

the DGA (Regulation (EU) No 2022/868), to which reference has already been made, but also between these and other European digital market legislation, including the DMA,[60] the DSA,[61] the Data Act[62] and the Artificial Intelligence (AI) Act,[63] as well as, more generally, provisions on data cooperatives in relation to the digital market.

Comparative law analyses aimed at highlighting solutions obtained based on legal experiences in other countries will be especially relevant.

The question of the types of contract used in relation to the negotiation carried out by the cooperatives on the use of data by third parties will be crucial.

What is more, analysis of legal principles and in particular of how the regulatory principle of solidarity is applied in practice with respect to the phenomenon of data cooperatives – within the theoretical framework of 'digital mutualism'[64] – would offer a valuable contribution to studies in the field.[65]

These, together with others only now appearing on the horizon, are undoubtedly important aspects that deserve to be explored in depth – also from an interdisciplinary perspective – in subsequent research on the extensive and uneven topic of data cooperatives, which provides legal scholars with an extraordinary laboratory in the face of market digitisation.

[60] *Digital Markets Act*, Reg. (EU) No. 1925/2022.

[61] *Digital Services Act*, Reg. (EU) No. 2065/2022.

[62] *Data Act*, Reg. (EU) No. 2854/2023.

[63] *Artificial Intelligence Act* (AI Act), Reg. (EU) No. 1689/2024.

[64] See section 3 above.

[65] On the legal principle of solidarity see, once again, G. Alpa, *Solidarietà. Un principio normativo*, cit., *passim.* On the specific issue of data protection, see also F. Bravo, *Il principio di solidarietà in materia di protezione dei dati personali nelle decisioni del Garante e della Corte di Cassazione*, cit., p. 405 ff.

Capitolo II

Il mercato digitale europeo e le cooperative di dati

Luca Petrone

Abstract: This paper analyzes the need to pursue choices geared toward sustaining European data spaces, including personal data, in order to support the competitiveness of European companies before the proprietary logics that characterize non-European markets, in particular by addressing the issue of data cooperatives. This corporate model, which has found for the first time express recognition as an intermediary service in Regulation (EU) 2022/868, could represent an alternative tool to the markedly capitalistic one, which prevails today, through which to give back centrality to citizens, and contribute to making society and the digital economy more supportive and democratic.

1. La regolazione del mercato unico digitale nell'Unione europea.

Ogni giorno il mondo produce sempre più dati digitali e se nel 2018 il loro volume totale ammontava a circa 33 *zettabyte*, tale valore sembrerebbe destinato a quintuplicarsi già entro il 2025 [1], anche grazie alla diffusione delle nuove tecnologie digitali, tra cui i dispositivi mobili, la tecnologia *social*, il *cloud computing* e la comunicazione *machine to machine*.

Proprio questo enorme flusso di informazioni ha trasformato, sta trasformando e trasformerà, in maniera sempre più radicale il modo di produrre, consumare e vivere di miliardi di persone in tutto il pianeta, oltre ad influire in maniera sempre più incisiva sulle politiche di sviluppo e sulla competitività delle imprese.

In particolare queste ultime saranno interessate – *rectius* sono interessate – da un cambiamento epocale che inciderà sulla capacità di "fare impresa" degli opera-

[1] International Data Corporation, *DataAge* 2025 – *The Digitization of the world*, 2018, consultabile al sito *www.idc.com*.

tori economici che vedranno nell'uso dei dati il principale motore di sviluppo dei beni e servizi che essi intenderanno proporre sul mercato.

In ragione di ciò sembrerebbe nelle intenzioni del legislatore eurounitario percorrere scelte orientate a sostenere gli spazi europei dei dati, anche personali, e incoraggiarne il mercato, al fine di sostenere la competitività delle imprese europee di fronte alle logiche proprietarie che caratterizzano i mercati extraeuropei [2] e le imprese tecnologiche in essi stabiliti, c.d. *Big Tech*, presso i quali sono allocate le informazioni digitali della maggioranza di cittadini e delle aziende europee che sembrerebbero esporre l'Unione al rischio di un «colonialismo digitale» [3].

Tale subalternità, oltre alla necessità di far fronte allo sviluppo impetuoso e inarrestabile della c.d. *data economy*, avrebbero spinto l'Unione europea ad affrontare una duplice sfida consistente, da una parte, nel divenire un polo di attrazione per i dati, essendo questi, sempre più materia prima [4] imprescindibile per lo sviluppo dell'economia, e, dall'altra, quella di evitare che il trattamento dei dati si presti ad abusi.

Il contemperamento di tali esigenze, tuttavia, appare tutt'altro che agevole e scontato e necessita, a parere di chi scrive, di una disciplina razionale, in grado di dettare regole volte a garantire le libertà individuali di fronte all'immenso potere della tecnica, senza che ciò rappresenti una sterilizzazione delle possibilità che quest'ultima offre.

In tal senso, aderendo al brocardo elaborato da autorevole dottrina [5] *ubi societas technologica, ibi ius*, varrebbe la pena porsi l'interrogativo se non sia opportuno ed efficace adottare un organico e generale *corpus juris digitalis* [6], dal momento che il flusso ormai continuo di interventi regolamentari [7] sembrerebbe porre il tema della necessità di coordinamento e armonizzazione interna delle diverse discipline che,

---

[2] G. ALPA, *La Proprietà dei dati personali*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, 2019, p. 11 ss.; F. BRAVO, *Intermediazione di dati personali e servizi di* data sharing *dal GDPR al* Data Governance Act, in *Contratto e impresa Europa*, 2021, 1, p. 199 ss.

[3] L. LIONELLO, *La creazione del mercato europeo dei dati: sfide e prospettive*, in *Diritto del Commercio Internazionale*, 2021, 3, p. 675.

[4] Si tratta del modello economico basato sul cd. *capitalismo della sorveglianza*, ossia l'ordine economico che sfrutta l'esperienza umana come materia prima per pratiche commerciali segrete di estrazione, previsione e vendita, in una logica economica parassitaria volta a sovvertire la sovranità popolare. Per un approfondimento sul tema si rimanda a S. ZUBOFF, *Il capitalismo della sorveglianza, il futuro dell'umanità nell'era dei nuovi poteri*, Roma, 2019.

[5] T.E. FROSINI, *Il costituzionalismo nella società tecnologica*, in *Diritto dell'informazione e dell'informatica*, 2020, 3, p. 1; nonché, in precedenza, F. BRAVO, *Ubi societas ibi ius e fonti del diritto nell'età della globalizzazione*, in *Contratto e impresa*, 2016, 6, pp. 1344-1390.

[6] G. CERRINA FERONI, *Luci e ombre della* Data Strategy *europea*, in *www.agendadigitale.eu*, 12 maggio 2022.

[7] In particolare, oltre al *General Data Protection Regulation* (Regolamento UE 2016/679) e al *Data Governance Act* (Regolamento UE 2022/868), si pensi al *Digital Markets Act* (Regolamento UE 2022/1925) e al *Digital Service Act* (Regolamento UE 2022/2065).

ad oggi, sembrerebbe possibile solo a seguito di attività interpretativa.

Nelle intenzioni della Commissione europea il mercato unico di dati deve rappresentare uno spazio «(...) aperto ai dati provenienti da tutto il mondo (...) nel quale sia i dati personali sia quelli non personali, compresi i dati commerciali sensibili, siano sicuri e le imprese abbiano facilmente accesso a una quantità pressoché infinita di dati industriali di elevata qualità, che stimolino la crescita e creino valore, riducendo nel contempo al minimo l'impronta di carbonio e ambientale» [8].

Sempre a parere della Commissione, per raggiungere questi obiettivi, il mercato unico dei dati dovrà essere costruito sulla libera circolazione dei dati all'interno dell'UE e a livello intersettoriale, con la creazione di «(...) spazi comuni europei in settori economici strategici e ambiti di interesse pubblico» [9], l'introduzione di norme e di maccanismi che facilitino e garantiscano l'accesso ai dati ed il loro utilizzo e l'applicazione di standard europei nel mercato unico in particolare sotto il profilo della protezione dei dati personali, della tutela dei consumatori e della concorrenza [10]; in tal senso sono già state identificate nove macro – aree dove la raccolta e la messa a disposizione dei dati dovrebbe avere un impatto sistemico sull'intera organizzazione economica dell'Unione e sulle condizioni di vita dei cittadini europei. In particolari i settori interessati saranno quelli della sanità, della mobilità, dell'industria manifatturiera, dei servizi finanziari, dell'energia, dell'agricoltura o relativi ad altri ambiti strategici quali il *Green Deal* [11], gli spazi europei di dati per la pubblica amministrazione e per le competenze [12].

---

[8] *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni*. *Una Strategia europea per i dati*, Bruxelles, COM (2020) 66 final, p. 5.

[9] *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni*. *Una Strategia europea per i dati*, Bruxelles, COM (2020) 66 final, p. 24.

[10] Il progetto di mercato unico dei dati, presentato nel febbraio 2020, si innesta in un quadro normativo già in parte sviluppato dalle istituzioni europee negli anni precidenti: Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, in G.U.C.E. L 201 del 31 luglio 2002, p. 37; Regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (RGDP), G.U.U.E. L 119 del 4 maggio 2016, p. 1; Regolamento (UE) n. 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea, G.U.U.E. L 303 del 28 novembre 2018, p. 59; Direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio del 20 giugno 2019 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico, G.U.U.E. L 172 del 26 giugno 2019, p. 56.

[11] Consistente nella creazione di uno spazio per utilizzare l'enorme potenziale dei dati a sostegno delle azioni prioritarie del *Green Deal* in materia di cambiamenti climatici, economia circolare, inquinamento zero, biodiversità, deforestazione e garanzia della conformità.

[12] Uno spazio per ridurre i disallineamenti di competenze tra il sistema di istruzione e formazione, da un lato, e le esigenze del mercato del lavoro, dall'altro.

Proprio la creazione di questi grandi *pool* di informazioni digitali potrebbe richiedere non solo l'attività di intermediazione dei servizi di condivisone dei dati, ma anche iniziative legislative e politiche in grado di favorire il loro uso e la domanda di servizi arricchiti di dati.

In questo contesto brevemente descritto, consapevole dell'impossibilità, in questa sede, di poterne offrire una rappresentazione esaustiva, è stato pubblicato il Regolamento (UE) 2022/868, più noto come *Data Governance Act* (*DGA*), che sembrerebbe porsi, almeno nelle intenzioni, in rapporto di discontinuità rispetto al panorama legislativo europeo in materia di protezione dati.

Vale la pena, fin da ora, ricordare che, sul piano dei principi, la disciplina in materia di protezione dei dati personali si colloca indiscutibilmente ai vertici del sistema giuridico europeo e nazionale, in coerenza con il rilievo pubblico che ha da sempre enfatizzato il legame delle garanzie riconosciute all'interessato con il costituzionalismo *post* bellico, sorto sulle macerie delle esperienze autoritarie novecentesche [13], a cui si aggiungono le preoccupazioni connesse all'esigenza di tutela delle persone fisiche di fronte ai rischi derivanti dal trattamento dei dati personali, in un contesto tecnologico in continua espansione. Accanto a tali esigenze di protezione, compiutamente disciplinate nel Reg. UE 679/2016 (GDPR), il legislatore europeo ha più recentemente introdotto nuove norme volte ad incoraggiare la circolazione dei dati, personali e non personali, nella prospettiva di un migliore sviluppo del mercato europeo: ci si sta riferendo al Reg. UE 868/2022, contenente norme sulla *Governance* europea dei dati (*Data Governance Act*), ove le esigenze di protezione dei dati vengono ad essere conciliate con quelle del diritto al libero accesso e riuso dei dati medesimi.

In questa prospettiva non sembra un caso la definizione autonoma che il *Data Governance Act* fornisce di «dato», in rapporto di discontinuità con il panorama legislativo europeo che, da sempre, aveva costruito la relativa definizione in negativo [14] e

---

[13] In tal senso anche la scelta compiuta dalla Carta dei diritti fondamentali UE di prevedere in aggiunta al diritto al rispetto alla vita privata una specifica disposizione sul diritto alla protezione dei dati personali. In particolare, l'art. 8 dispone espressamente che «Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente».

[14] A tal proposito per «*dati*» si intendeva quelli diversi dai dati personali definiti dall'art. 4, punto 1, del Regolamento (UE) 2016/679. Infatti, nel diritto unionale mancava, sino all'entrata in vigore del Regolamento UE 2022/868, una definizione normativa di «dato». L'unica definizione che poteva ritrovarsi nel panorama legislativo era quella di «*dati personali*», definita sin dalla Direttiva 1995/46/CE (art. 2, comma 1, lett. *a*) e poi dall'art. 4, n. 1, Regolamento (UE) 2016/679 come «qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un

in chiave oppositiva rispetto a quella di «dati personali» [15]. In particolare l'art. 2, par. 1, prevede espressamente che per dati deve intendersi «(...) qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi raccolta di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva».

E sembrerebbe essere proprio la definizione riportata a segnare un distacco netto dalla pregressa impostazione, per almeno i seguenti ordini di motivi: *(a)* in primo luogo in quanto la disciplina prende in considerazione cumulativamente dati personali e non personali, nel tentativo di incrementarne l'accesso, l'uso e il riuso, salvo poi a rimarcare, per questi ultimi, la necessità di rispettare comunque la disciplina in materia di dati personali di cui al GDPR, a cui si fa espressamente rinvio, e *(b)* dall'altro in quanto sembrerebbe espandersi la dimensione sintattica dei dati [16]. Infatti, mentre la nozione di dato personale si concentra sulla riconducibilità dello stesso ad uno specifico individuo, individuato o individuabile [17], la formula accolta dal *Data Governance Act* accentuerebbe l'idea della codifica di stati del mondo tramite rappresentanza digitale.

Inoltre, tenendo bene a mente l'attuale disciplina in materia di protezione dei dati personali, la necessità di stimolare la creazione di spazi digitali all'interno dei quali poter far circolare liberamente le informazioni, come suggerito dal legislatore unionale, non potrà non riconsiderare istituti che si sono dimostrati inefficaci al cospetto delle prassi organizzative e di mercato affermatesi nel contesto dell'economia digitale, tra i quali quello del consenso informato che, soprattutto nell'ambito dei rapporti digitali sembrerebbe ormai essersi tradotto in un simulacro formale atto a mascherare una realtà fortemente asimmetrica e in cui l'idea dell'autodeterminazione dell'interessato si è rivelata poco più che un'etichetta priva di riscontri operazionali [18]. Nonostante ciò, nel *Data Governance Act* il richiamo alla necessità del consenso al trattamento dei dati personali previsto nel GDPR rimane costante, seppur si riveli spesso strumento di protezione inadeguato. In questo senso vale la pena osservare che il Regolamento (UE) 2016/679 (GDPR), normativa molto ambiziosa, si basa su un modello di consenso al trattamento dei dati personali che, in

---

identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale». Conseguentemente, per «dato», potevano essere intesi tutti quegli elementi non direttamente riconducibili alla definizione sopra riportata.

[15] G. RESTA, *La regolazione digitale nell'Unione europea – pubblico, privato, collettivo nel sistema europeo di governo dei dati*, in *Riv. trim. dir. pubbl.*, 2022, 4, p. 971.

[16] G. RESTA, *op. cit.*, p. 971.

[17] L'art. 4, par. 1, n. 1, definisce dato personale «qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale».

[18] S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, Bologna, 1973, p. 47 ss.; ID., *Protezione dei dati e circolazione delle informazioni*, ora in *Tecnologia e diritti*, p. 79 ss.

ultima analisi, sembrerebbe rappresentare «(...) un vaso di cristallo fragile e dal contenuto eterodeterminato» [19]. In molti casi, infatti, i contenuti delle *policy* che disciplinano il trattamento dei dati sono spesso talmente complessi e di non facile comprensione da creare disinteresse alla loro consultazione da parte della maggioranza degli interessati. E l'aspetto che dovrebbe destare più allarme, anche tra i cultori del diritto, è la natura razionale della scelta degli utenti che sembrerebbero essere orientati nelle scelte dalla percezione di un generale senso di impotenza, oltre che da superficialità e scarsa conoscenza delle dinamiche economiche alle quali accettano passivamente di aderire.

Il GDPR, in altri termini, rappresenterebbe una normativa avanzatissima, che però sconterebbe una applicazione difficoltosa, resa tale da un meccanismo che opera al di là della possibilità di una gestione effettiva e realistica da parte degli *users*.

Di qui probabilmente la necessità di un ripensamento della tecnica legislativa, che dovrebbe ridurre le asimmetrie in modo sostanziale, eventualmente anche ripensando alcuni istituti o, quantomeno, cercando un equo bilanciamento degli stessi con l'attuale sistema economico, fermo restando che non è possibile ignorare come le politiche sulla digitalizzazione siano in grado di incidere sui meccanismi della democrazia [20].

In tal senso deve rimanere focale per l'Unione europea trovare, attraverso il diritto, un sano equilibrio sociale tra sviluppo dell'economia e politiche a garanzia e protezione della dignità umana, anche a fronte di poteri privati fortissimi; questo anche a tutela degli stessi ordinamenti democratici. Non è, infatti, possibile avere democrazia e sorveglianza di massa, ma solo una delle due. Ed è per questa ragione che non rappresenta un'opzione quella di abbandonare il presidio democratico soprattutto innanzi a fenomeni di condizionamento politico ed elettorale, o di spionaggio contro giornalisti, attivisti, politici. Deve essere forte, a riguardo, la consapevolezza da parte del legislatore eurounitario e nazionale che la compressione del diritto alla riservatezza potrebbe essere in grado di ridurre grandemente, fino anche a farli scomparire, i margini della democrazia.

Altra tematica che non può essere ignorata è quella che riguarda la capacità di generare ricchezza attraverso i dati che, unitamente agli indiscussi vantaggi sul piano dello sviluppo economico e sociale, potrebbe condurre ad una progressiva erosione delle garanzie di tutela degli interessati, generando quello che è stato definito il c.d. «sottoproletariato dei dati», caratterizzato dalla propensione dei soggetti meno abbienti a cedere anche informazioni ad elevato tasso di sensibilità [21] per ricavarne pic-

---

[19] B. CAROTTI, *La politica europea sul digitale: ancora molto rumore*, in *Riv. trim. dir. pubbl.*, 2022, 4, p. 997.

[20] Il c.d. *capitalismo della sorveglianza* imporrebbe il proprio dominio sulla società, espropriando diritto umani fondamentali nel tentativo di sovvertire la sovranità popolare.

[21] Cfr. S. ZUBOFF, *op. cit*., p. 98, secondo la quale «(…) gli utenti sono diventati dei fornitori inconsapevoli di materie prime per un ciclo più grande di generazione dei profitti».

coli introiti, con il rischio di svilimento dei diritti fondamentali della persona [22].

Dunque, alla luce delle esigenze proprie del c.d. mercato digitale, un cambio di rotta appare quanto mai necessario con l'obiettivo di non disperdere le opportunità create dalle tecnologie basata sull'analisi e sull'utilizzo dei dati, prime tra tutte quelle dell'intelligenza artificiale, e promuovere una maggiore circolazione e condivisione dei dati, fermo restando la necessità di tutelare la dignità dei cittadini europei, garantendo agli stessi, per quanto possibile, il controllo dei dati che li riguardano e ponendo agli operatori economici strumenti adeguati per lo sviluppo d'impresa e, al contempo, limiti che, se oltrepassati, potrebbero minare le fondamenta delle democrazie europee.

Questa rappresenta la sfida del futuro su cui si celebrerà la grandezza o si certificherà il fallimento dell'Unione nel campo dell'economia digitale, non essendo più possibile ignorare l'incredibile capacità di sviluppo che i dati, anche personali, possono generare [23] ed occorrendo, altresì, prendere atto della rilevanza, anche patrimoniale [24], degli stessi.

In tale complesso contesto storico, politico ed economico, il *Data Governance Act* sembrerebbe voler raccogliere questa opportunità operando su tre fronti principali: quello del riutilizzo dei dati in mano pubblica, quello della destinazione dei dati per finalità altruistiche e quello dei servizi di intermediazione per lo scambio dei dati, tra i quali vi rientrano le c.d. cooperative di dati. Ed è proprio su quest'ultimo istituto che ci si propone di fornire un approfondimento nelle prossime pagine del presente elaborato.

2. La dimensione collettiva dei dati: i servizi di intermediazione.

All'art. 2, par. 1, n. 11, il Reg. (UE) 2022/868 fornisce la definizione di *servizio di intermediazione dei dati*, prevedendo espressamente che debba intendersi come

---

[22] A. SORO, *L'universo dei dati e la libertà della persona*, Relazione 2018, p. 7, dove viene indicato che «Il diritto alla protezione dei dati personali viene sempre più invocato di fronte alle innumerevoli "servitù volontarie" cui rischiamo di consegnare noi stessi, in cambio di utilità e servizi che paghiamo al prezzo di porzioni piccole o grandi della nostra libertà. Emerge così un nuovo sottoproletariato del digitale, un "Quinto Stato" formato da quanti siano disposti a cedere, con i propri dati, la libertà, in cambio dei servizi offerti in rete solo apparentemente 'a prezzo zero'».

[23] È frequente l'accostamento dei dati personali al nuovo petrolio, per indicare le nuove opportunità commerciali che possono derivare dal relativo trattamento. Cfr. *Personal Data: The "New Oil" of the 21st Century*", Panel discussion at world Economic Forum on Europe and Central Asia 2011 (June 9, 2011).

[24] v. F. BRAVO, *Intermediazione di dati personali e servizi di* data sharing *dal GDPR al* Data Governance Act, cit., p. 212, secondo il quale «(…) il loro indiscutibile valore economico non deve però portare a ritenere che i medesimi siano anche "beni giuridici" in senso tecnico, quale merce che forma oggetto di commercializzazione, rimanendo pur sempre attributi della personalità (…)». In tal senso anche G. RESTA, *Autonomia Privata e diritti della personalità*, in *Biblioteca di diritto privato*, Napoli, 2005.

un «(...) servizio che mira a instaurare, attraverso strumenti tecnici, giuridici o di altro tipo, rapporti commerciali ai fini della condivisione dei dati tra un numero indeterminato di interessati e di titolari dei dati, da un lato, e gli utenti dei dati, dall'altro, anche al fine dell'esercizio dei diritti degli interessati in relazione ai dati personali (...)».

A tal proposito appare interessante segnalare come, dalla definizione di servizio di intermediazione fornita dalla disciplina eurounitaria sembrerebbero volutamente esclusi dal perimento della nozione sopra riportata i modelli del capitalismo informazionale che contraddistinguono l'epoca contemporanea, basati sulla raccolta dei dati degli utenti in cambio della fornitura di servizi formalmente gratuiti, per poi conseguire *extra* profitti tramite la licenza a terzi dei dati aggregati, analizzati e organizzati in formato leggibile dalle macchine.

A conferma di ciò si veda la lett. *a*) del n. 11, attraverso la quale viene previsto espressamente che non rientrano tra i servizi di intermediazione quelli che «ottengono dati dai titolari dei dati e li aggregano, arricchiscono o trasformano al fine di aggiungervi un valore sostanziale e concedono licenze per l'utilizzo dei dati risultanti agli utenti dei dati, senza instaurare un rapporto commerciale tra i titolari dei dati e gli utenti dei dati».

Quella sopra citata è certamente una delle scelte attraverso le quali il legislatore eurounitario ha inteso rimarcare l'intenzione di voler promuovere un modello di condivisione di dati diverso rispetto a quello attualmente dominante nel mercato digitale, proposto da quelle società che sposano un modello di *business* basato sullo sfruttamento industriale dei dati: l'intenzione del legislatore europeo, nel *Data Governance Act*, è proprio quella di stimolare, invece, una maggiore condivisione degli stessi da parte dei cittadini europei aumentando la loro fiducia nella neutralità [25] e nell'affidabilità dei servizi di intermediazione [26].

---

[25] Il *considerando* n. 33 del Reg. (UE) n. 868/2022 indica che «Un elemento essenziale attraverso il quale aumentare la fiducia e il controllo dei titolari dei dati, interessati e utenti dei dati nei servizi di intermediazione dei dati è la neutralità dei fornitori di servizi di intermediazione dei dati riguardo ai dati scambiati tra titolari dei dati o interessati e utenti dei dati. È pertanto necessario che i fornitori di servizi di intermediazione dei dati agiscano solo in qualità di intermediari nelle transazioni e non utilizzino per nessun altro fine i dati scambiati».

[26] Il *considerando* n. 5 del Reg. (UE) n. 868/2022 prevede espressamente che «L'azione a livello dell'Unione è necessaria per aumentare la fiducia nella condivisione dei dati istituendo adeguati meccanismi che garantiscano il controllo da parte degli interessati e dei titolari dei dati sui dati che li riguardano e al fine di affrontare altri ostacoli al buon funzionamento di un'economia competitiva basata sui dati. Tale azione non dovrebbe pregiudicare gli obblighi e gli impegni negli accordi commerciali internazionali conclusi dall'Unione. Un quadro di *governance* a livello dell'Unione dovrebbe avere l'obiettivo di creare fiducia tra gli individui e le imprese per quanto riguarda l'accesso ai dati, la loro condivisione e il loro controllo, utilizzo e riutilizzo, in particolare stabilendo adeguati meccanismi per gli interessati affinché conoscano ed esercitino fattivamente i propri diritti nonché per quanto riguarda il riutilizzo di alcune tipologie di dati detenuti dagli enti pubblici, la fornitura di servizi da parte dei fornitori di servizi di intermediazione dei dati agli interessati, ai titolari e agli utenti dei dati, nonché la raccolta e il trattamento dei dati messi a disposizione a fini altruistici da persone fisiche e giuridi-

Sul tema si sofferma poi il Capo III del *Data Governance Act* che stabilisce i requisiti per i servizi di intermediazione dei dati.

In particolare, l'art. 10, comma 1, del DGA contempla tre tipologie di servizi di intermediazione tra loro molto diversi e, in particolare: *(a)* servizi di intermediazione tra i titolari dei dati e i potenziali utenti dei dati [27], compresa la messa a disposizione di mezzi tecnici o di altro tipo per consentire tali servizi, *(b)* servizi

---

che. In particolare, una maggiore trasparenza per quanto riguarda la finalità dell'utilizzo dei dati e le condizioni in cui i dati sono conservati dalle imprese può contribuire ad aumentare la fiducia». Inoltre anche il *considerando* n. 22 dispone che «Alcuni paesi terzi adottano leggi, regolamenti e altri atti giuridici che mirano a trasferire direttamente i dati non personali o a fornire un accesso diretto agli stessi da parte delle autorità pubbliche nell'Unione, sotto il controllo di persone fisiche e giuridiche poste sotto la giurisdizione degli Stati membri. Le decisioni e le sentenze di autorità giurisdizionali o le decisioni di autorità amministrative di paesi terzi che dispongono un tale trasferimento di dati non personali o l'accesso agli stessi dovrebbero avere carattere esecutivo quando sono basate su un accordo internazionale in vigore tra il paese terzo richiedente e l'Unione o un suo Stato membro, ad esempio un trattato di mutua assistenza giudiziaria. Possono in alcuni casi presentarsi situazioni in cui l'obbligo di trasferire i dati non personali, o di fornirvi accesso, derivante dalla normativa di un paese terzo, sia in conflitto con un obbligo L 152/8 IT Gazzetta ufficiale dell'Unione europea 3 giugno 2022 concorrente di proteggere tali dati a norma del diritto dell'Unione o nazionale, in particolare per quanto riguarda la protezione dei diritti fondamentali della persona o degli interessi fondamentali di uno Stato membro connessi alla sicurezza nazionale o alla difesa, nonché la protezione dei dati commerciali sensibili e dei diritti di proprietà intellettuale, compresi anche gli obblighi contrattuali in materia di riservatezza conformemente a tale normativa. In assenza di accordi internazionali atti a disciplinare simili questioni, il trasferimento o l'accesso a dati non personali dovrebbero essere consentiti solo previa verifica, in particolare, che il sistema giuridico del paese terzo imponga che siano indicati i motivi e la proporzionalità della decisione o della sentenza, che la decisione o la sentenza abbia carattere specifico e che l'obiezione motivata del destinatario sia sottoposta a riesame da parte di un'autorità giurisdizionale competente nel paese terzo, cui sia conferito il potere di tenere debitamente conto dei pertinenti interessi giuridici del fornitore di tali dati. Inoltre, gli enti pubblici, le persone fisiche o giuridiche cui è stato concesso il diritto di riutilizzo dei dati, i fornitori di servizi di intermediazione dei dati e le organizzazioni per l'altruismo dei dati riconosciute dovrebbero garantire, al momento della firma di accordi contrattuali con altre parti private, che i dati non personali detenuti nell'Unione siano accessibili da parte di paesi terzi o ad essi trasferiti solo in conformità del diritto dell'Unione o del diritto nazionale dello Stato membro interessato».

[27] La terminologia utilizzata dal legislatore comunitario pone l'attenzione sul cambio di paradigma nelle strategie dell'UE; come affermato da autorevole dottrina al di là della scelta di trattare in maniera unitaria la categoria di «*dati*», siano essi personali o non personali, sono stati introdotti concetti nuovi per categorie giuridiche soggettive, quali quello di «*titolare dei dati*» anche là dove ci si riferisce a dati personali. In particolare è stato affermato che «*(...)* Fino ad ora l'UE aveva sempre rifiutato di introdurre il concetto di titolarità direttamente riferita ai dati: non era considerato titolare dei dati né il soggetto a cui si riferisce il dato personale, indicato come interessato al trattamento di dati personali, né il soggetto che predispone il trattamento dei dati personali per finalità legittime dal medesimo stabilite, indicato come titolare del trattamento dei dati. Mai fino ad ora s'è voluto riferire il concetto di titolarità direttamente al dato (e non al trattamento) e ciò denota un cambio di paradigma che rischia di essere un preludio all'introduzione, per via normativa, di una reificazione dei dati personali, quali entità giuridicamente rilevanti *ex se* più che quali attributi della persona». Cfr. F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, cit., p. 203.

di intermediazione tra interessati che intendono mettere a disposizione i propri dati personali o persone fisiche che intendono mettere a disposizione dati non personali e potenziali utenti dei dati, permettendo in particolare l'esercizio dei diritti degli interessati di cui al Regolamento (UE) 2016/679; *(c)* servizi di cooperative di dati.

Tali fornitori di servizi dovrebbero operare garantendo il pieno rispetto della disciplina dettata dal Regolamento UE 2016/679 [28] gestendo per conto dei titolari dei dati tutti i diritti degli interessati che lo stesso accorda loro.

A tal proposito perplessità sorgono in merito al potenziale rischio di abusi derivante dalla messa a disposizione di ingenti quantitativi di dati, anche personali, a favore dei soggetti che intenderanno fornire servizi di intermediazione; in tal senso il *considerando* n. 30 del *DGA* prevede espressamente che il modello commerciale di tali fornitori debba garantire che «(...) non vi siano incentivi disallineati che incoraggino i singoli individui a utilizzare tali servizi per mettere a disposizione più dati che li riguardano di quanto non sia nel loro stesso interesse». Inoltre, l'art. 12, par. 1, lett. *a*), del DGA prescrive che il fornitore del servizio di intermediazione «(...) non utilizza i dati per i quali fornisce servizi di intermediazione dei dati per scopi diversi dalla messa a disposizione di tali dati agli utenti dei dati e fornisce servizi di intermediazione attraverso una persona giuridica distinta» e, alla relativa lett. *m*), stabilisce uno specifico obbligo di natura fiduciaria per l'ipotesi in cui il servizio di intermediazione abbia ad oggetto dati personali, nell'intento di rafforzare ulteriormente la trasparenza e l'affidabilità del servizio, stabilendo che «il fornitore di servizi di intermediazione dei dati che offre servizi agli interessati agisce nell'interesse superiore di questi ultimi nel facilitare l'esercizio dei loro diritti, in particolare informandoli e, se opportuno, fornendo loro consulenza in maniera concisa, trasparente, intelligibile e facilmente accessibile sugli utilizzi previsti dei dati da parte degli utenti dei dati e sui termini e le condizioni standard cui sono subordinati tali utilizzi, prima che gli interessati diano il loro consenso».

Dunque dalle norme sopra citate si evince come gli intermediari dei dati, nell'ottica del legislatore eurounitario, dovranno avere un ruolo essenziale nell'economia dei dati, operando sia come strumenti di aggregazione e scambio di quantità considerevoli di dati, rappresentando un'opportunità per il mercato da governare adeguatamente, sia come strumenti per agevolare l'esercizio dei diritti che l'ordinamento riconosce alle persone fisiche a cui i dati si riferiscono.

---

[28] Il *considerando* n. 35 dispone che «Il presente regolamento dovrebbe lasciare impregiudicati l'obbligo incombente ai fornitori di servizi di intermediazione dei dati di rispettare il regolamento (UE) 2016/679 e la responsabilità delle autorità di controllo di garantire il rispetto di tale regolamento. Qualora i fornitori di servizi di intermediazione dei dati trattino dati personali, il presente regolamento non dovrebbe pregiudicare la protezione degli stessi. Qualora siano titolari del trattamento o responsabili del trattamento dei dati quali definiti nel regolamento (UE) 2016/679, i fornitori di servizi di intermediazione dei dati sono vincolati dalle norme di tale regolamento».

3. (*segue*) Le cooperative di dati.

I servizi forniti da cooperative di dati vengono definiti dall'art. 2, par. 1, n. 15), come servizi di intermediazione «offerti da una struttura organizzativa costituita da interessati, imprese individuali o da PMI, che sono membri di tale struttura, avente come obiettivi principali quelli di aiutare i propri membri nell'esercizio dei loro diritti in relazione a determinati dati, anche per quanto riguarda il compiere scelte informate prima di acconsentire al trattamento dei dati, di procedere a uno scambio di opinioni sulle finalità e sulle condizioni del trattamento dei dati che rappresenterebbero al meglio gli interessi dei propri membri in relazione ai loro dati, o di negoziare i termini e le condizioni per il trattamento dei dati per conto dei membri prima di concedere l'autorizzazione al trattamento dei dati non personali o prima che essi diano il loro consenso al trattamento dei dati personali».

Il modello societario cooperativo positivizzato da tempo e utilizzato nei più svariati ambiti del mondo dell'impresa ha per la prima volta, con il *Data Governance Act*, trovato espresso riconoscimento nell'economia digitale e sembrerebbe guadagnare sempre più attenzione offrendo ai cittadini un modo per esercitare potere negoziale per l'uso dei dati, rafforzandone, inoltre, la relativa posizione [29].

Punto di partenza sarebbe il riconoscimento della situazione attuale in cui i dati personali vengono sfruttati senza che venga restituito un valore sufficiente all'individuo e la conseguente necessità di organizzare enti collettivi, con poteri analoghi a quelli di un'associazione con funzioni di rappresentanza sindacale, in grado di rappresentare i diritti delle persone.

Le cooperative di dati, in tal senso, potrebbero diventare l'elemento fondamentale per raggiungere un modello di controllo dei dati che superi quello capitalistico per andare verso un sistema collettivo basato su diritti e responsabilità, con standard legali sostenuti da una nuova classe di rappresentanti che agiscano come fiduciari per i loro soci.

Il modello cooperativo infatti si sposerebbe perfettamente con la necessità di garantire un controllo diffuso dei dati da parte dei relativi titolari. In quest'ottica i soci trasferirebbero in cooperativa i dati, personali e non, che li riguardano avendo certezza di mantenerne il controllo, tenuto conto delle caratteristiche tipiche di questa particolare forma di impresa collettiva.

La cooperativa, come modello societario, infatti, risponde a principi diversi rispetto alle altre società di capitali. E questa diversità viene legittimata a livello costituzionale dall'art. 45, attraverso il quale viene espressamente disposto che «la Repubblica riconosce la funzione sociale della cooperazione a carattere di mutualità e senza fini di speculazione privata. La legge ne promuove e favorisce l'incremento con i mezzi più idonei e ne assicura, con gli opportuni controlli, il carattere e le finalità».

---

[29] Cfr. D. POLETTI, *Gli intermediari di dati*, in *European Journal of Privacy Law & Technologies*, 2022, 1, pp. 45-56, consultabile al sito *https://universitypress.unisob.na.it/ojs/index.php/ejplt/article/view/1623/1092*.

Il favore costituzionale per la cooperazione è dovuto essenzialmente a due ragioni, ossia la tutela delle posizioni economicamente deboli e l'articolazione e diffusione del potere economico che tale modello societario consente, traducendo sul terreno economico i principi di democraticità, uguaglianza e solidarietà che sono alla base del nostro ordinamento giuridico [30]. Modello, questo, antitetico rispetto a quello adottato da quegli operatori economici che fanno del trattamento del dato il relativo *core business* con logiche spiccatamente capitalistiche.

Prevalente in questa fattispecie è, invece, lo scopo mutualistico [31] che trascende gli interessi dei singoli individui che compongono l'ente, rispondendo ad esigenze di più ampia portata, che spesso hanno rilevanza pubblica; scopo mutualistico che nel nostro sistema normativo manca di una definizione propria. Non si tratta, tuttavia, di una lacuna, ma di una specifica scelta dettata dalla difficoltà di giungere ad una definizione in grado di rappresentare il fenomeno cooperativo in tutti suoi aspetti, con il rischio che una definizione eccessivamente rigida avrebbe potuto rappresentare un limite allo sviluppo del movimento. Non solo la finalità mutualistica sarebbe confacente all'obiettivo di creare un mercato digitale europeo che sia distante dal modello adottato oltreoceano, bensì anche altri principi tipici del modello cooperativo, come il principio della parità di trattamento tra soci e della «porta aperta» [32] che trovano espresso riconoscimento legislativo rispettivamente agli artt. 2516 e 2528 c.c.; principi, quelli appena citati che garantirebbero l'idoneità dell'organismo cooperativo a soddisfare astrattamente il medesimo bisogno in un

---

[30] v. Corte cost., sent. n. 408/1989, secondo la quale «(…) alla protezione costituzionale della cooperazione si attribuisce una finalità che va oltre la generica tutela di categorie produttive deboli, in quanto si estende al riconoscimento e alla promozione di una forma di produzione alternativa a quella capitalistica, la giustificazione della protezione stessa è comunemente rinvenuta nella più stretta inerenza che la "funzione sociale" presenta nell'organizzazione cooperativistica rispetto a quella che la detta funzione riveste nelle altre forme di organizzazione produttiva. Funzione sociale che qui viene individuata nella congiunta realizzazione del decentramento democratico del potere di organizzazione e gestione della produzione e della maggiore diffusione e più equa distribuzione del risultato utile della produzione stessa (…)».

[31] Malgrado l'incertezza gli interpreti concordano nel ritenere che lo scopo mutualistico trovi la sua essenza: (a) nello scopo di fornire beni, servizi e occasioni di lavoro a condizioni più vantaggiose di quelle che i soci otterrebbero rivolgendosi al mercato (*mutualità interna*); (b) nello scopo di contribuire al perseguimento di fini di interesse generale per la promozione e lo sviluppo della cooperazione (*mutualità esterna*).

[32] Da sempre uno degli elementi fondamentali del c.d. associazionismo cooperativistico. Tra gli altri v. G. BONFANTE, *Manuale di diritto cooperativo*, Bologna, 2017, p. 25 ss. secondo il quale il riconoscimento legislativo di cui all'art. 2528 c.c., «(…) costituisce, nel nostro ordinamento, il primo caso di disciplina normativa avente valenza generale di tale principio»; ID., *Delle imprese cooperative*, in *Commentario del codice civile Scialoja-Branca*, Bologna-Roma 1999, p. 376 ss.; sul principio della «porta aperta» anche G. DI CECCO, *Il capitale e le altre forme di finanziamento*, in *Le cooperative prima e dopo la riforma*, cit., p. 467 ss.; R. GENCO, *Note sui principi di* corporate governance *e sulla riforma del diritto societario nella prospettiva delle società cooperative*, in *Giur. comm.*, 2000, 2, p. 274.

numero indeterminato di soggetti, assicurando loro un trattamento equo e paritario ed evidenziandone la naturale inclinazione a porsi a servizio di quanti appartengono alla categoria prevista nell'atto costitutivo.

Altro principio che non può non essere menzionato è quello del c.d. voto capitario [33]. In cooperativa, a differenza delle società prettamente capitalistiche, a nessun socio può essere attribuito più di un voto, qualunque sia l'ammontare della quota di capitale sociale detenuta. E questo a garanzia della democraticità della struttura societaria. Tale aspetto garantirebbe un controllo condiviso sui dati che i soci hanno acconsentito a trasferire in cooperativa. Le decisioni sugli stessi non potranno che essere assunte con il voto favorevole della maggioranza dei componenti della compagine sociale, oltre che dal relativo consiglio di amministrazione che, in ogni caso, non potrà che essere composto, almeno per la maggioranza, da soci della cooperativa.

Ovviamente la creazione di una struttura collettiva e di coordinamento volta a socializzare il valore dei dati ed i singoli membri di essa, genererebbe non soltanto un possibile guadagno in termini monetari, seppur limitato [34], trattandosi di modello societario che risponde alla logica di limitare il lucro soggettivo dei singoli soci, ma anche – e soprattutto – sul piano del controllo sulle modalità di trattamento e sull'utilizzo secondario dei dati. Andrebbe contemperato con l'esigenza di garantire al singolo il controllo sui dati personali che lo riguardano, conformemente alla disciplina in materia di protezione dei dati personali.

I pochi esempi emersi nella prassi [35] hanno, in ogni caso, mostrato come le cooperative di dati possano rappresentare, soprattutto a livello locale, un sistema interessante di gestione dei dati con carattere imprenditoriale alternativo rispetto agli schemi caratteristici del capitalismo estrattivo e non è un caso che è al modello delle cooperative di dati che si guarda con crescente interesse, anche nell'ambito dei dibattiti sulle c.d. *smart cities* [36].

Una cooperativa di dati potrebbe tradursi operativamente in una cooperativa di servizi consistenti, a titolo meramente esemplificativo, nella gestione condivisa dei dati, anche attraverso la conservazione degli stessi, con misure tecniche e organiz-

---

[33] V. art. 2538, co. 2, c.c. dispone espressamente che «Ciascun socio cooperatore ha un voto, qualunque sia il valore della quota o il numero delle azioni possedute (…)».

[34] In tal senso si rimanda a quanto disposto dall'art. 2514 c.c. In particolare al comma 1, lett. *a)*, viene espressamente riconosciuto «(…) il divieto di distribuire i dividendi in misura superiore all'interesse massimo dei buoni postali fruttiferi, aumentato di due punti e mezzo rispetto al capitale effettivamente versato».

[35] Si riscontrano a livello europeo alcuni isolati esempi, quali, le cooperative dei dati create da conducenti di taxi (*Driver's seat*), da pazienti (*salus.coop*), o da pescatori (*PescaData*).

[36] Le *smart cities*, in italiano "*città intelligenti*", rappresenterebbero modelli urbani nei quali le risorse, anche informative, dovrebbero venire gestite in modo "intelligente", avendo come scopo quello di migliorare la qualità di vita dei suoi cittadini attraverso l'autosufficienza energetica e la sostenibilità economica.

zative adeguate, nell'aggregazione e nell'interazione degli stessi, nella prospettiva di creare valore per eventuali iniziative commerciali, ma anche solo per la stessa comunità che quegli stessi dati condivide, nell'assistenza e nel supporto all'esercizio dei diritti dei titolari dei dati, nonché soci della cooperativa, siano essi persone fisiche o persone giuridiche.

A tale riguardo, particolare attenzione è stata posta sull'esercizio dei diritti dell'interessato *ex* art. 15 e ss. del Regolamento (UE) 2016/679; in particolare il testo finale del DGA segnerebbe un progresso significativo rispetto all'originaria proposta della Commissione; infatti, il Considerando 24 della proposta, specificamente concernente le cooperative, affermava che «è importante riconoscere che i diritti a norma del regolamento (UE) 2016/679 possono essere esercitati soltanto a titolo individuale e non possono essere conferiti o delegati a una cooperativa di dati». Ebbene, una siffatta formulazione avrebbe certamente escluso in radice la possibilità di considerare possibile un esercizio mediato, avvalendosi delle società di intermediazione di servizi, dei diritti che la legislazione eurounitaria in materia di trattamento dati riconosce agli interessati.

Nel testo definitivo del Regolamento (UE) n. 868/2022, il riferimento al «conferimento» e alla «delega» è scomparso e nel corrispondente *considerando* 31 si legge ora, invece, che «i diritti a norma del Regolamento (UE) 2016/679 sono diritti personali dell'interessato e che quest'ultimo non può rinunziarvi».

Secondo autorevole dottrina, «(...) sebbene gli esercizi di esegesi delle norme di matrice europea sulla base delle categorie del diritto interno debbano sempre essere condotti con grande prudenza, sembrerebbe ragionevole ritenere che mentre il divieto della rinunzia, quale tipico atto abdicativo, implichi l'impossibilità del conferimento in società (atto con efficacia reale), esso non preclude invece la stipula di un contratto di mandato (con rappresentanza), in quanto atto con mera efficacia obbligatoria» [37].

Sembrerebbero quindi aprirsi spazi operativi per la tutela esterna dei diritti degli interessati da parte di una cooperativa di dati che operi come rappresentante dei suoi soci.

Fermo restando le considerazioni poc'anzi espresse, altre potenziali criticità potrebbero emergere; in particolare, per ciò che attiene allo sfruttamento dei dati, personali e non, condivisi dai soci mediante attività negoziale con terzi.

La logica stessa di un modello societario come quello cooperativo, seppur con scopo mutualistico, suggerirebbe in ogni caso l'opportunità di riconoscere un conferimento dei dati con correlativi poteri dispositivi in capo alla società. Infatti la cooperativa sarebbe pur sempre un'impresa commerciale, ossia una struttura che opera sul mercato nel tentativo di essere competitiva con le imprese capitalistiche in senso stretto.

Ebbene, le attuali formule legislative, come anticipato nel corso del presente ela-

---

[37] G. RESTA, *La regolazione digitale nell'Unione europea – pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit., p. 971.

borato, escluderebbero tale possibilità, tenuto conto che tra gli obblighi imposti ai servizi di intermediazione ci sarebbe quello della c.d. neutralità (art. 12, comma 1, lett. *a*), così da escludere qualsiasi attività di *data analytics* prodromica ad un'efficace attività negoziale con terzi; il *Data Governance Act* sembra espressamente limitare il ruolo delle cooperative — e a maggior ragione degli altri intermediari dei dati — a un'attività di consulenza precedente alla manifestazione del consenso, o al massimo a quella di trasmissione a terzi della manifestazione di volontà dell'interessato; dunque lo stesso consenso, strumentale all'esercizio di diritti personalissimi come quelli in materia di trattamento dati, figurerebbe come atto personale non delegabile a terzi [38].

Dunque l'impostazione che sembrerebbe essere stata data al DGA, sarebbe, a parere di chi scrive, limitativa per una cooperativa di dati, la quale, per conseguire efficacemente i propri scopi sociali e per contendere il primato del modello imprenditoriale lucrativo, necessiterebbe di un più ampio margine di azione. È per questa ragione che la natura personale del consenso, «(...) che pure costituisce un baluardo dell'autodeterminazione nell'ambito dei rapporti di mercato, trasposto alla sfera dei rapporti fiduciari e ai sistemi di imprenditoria sociale, meriterebbe forse di essere superato (...) sì da riconoscere la possibilità di rappresentanza nell'espressione del consenso al trattamento dei dati, con il solo limite della soggezione della procura ai requisiti fissati dall'art. 7 GDPR, e in particolare a quello della specificità» [39].

Dopotutto, lo stesso Regolamento (UE) 2016/679, non sembrerebbe escludere in radice la possibilità che il consenso possa essere espresso mediante l'istituto della rappresentanza; l'art. 8 del GDPR, infatti, prevede espressamente che gli esercenti la potestà genitoriale possano validamente esprimere un consenso per il minore d'età.

Se è senz'altro vero che la tipicità della fattispecie citata potrebbe far propendere per l'esclusione di possibili interpretazioni estensive della norma, il mero silenzio in merito alla possibilità di fare utilizzo all'istituto della c.d. rappresentanza volontaria non potrebbe essere *a fortiori* inteso come un divieto assoluto. Siffatta interpretazione, infatti, mal si concilierebbe con lo sforzo che il legislatore eurounitario sta compiendo per la creazione di un mercato unico digitale europeo e la legittimazione di soggetti di diritto in grado di dare pieno riconoscimento alla dignità dei titolari dei dati.

---

[38] A tal proposito, ad esempio, il *considerando* 31 prevede che tra gli obiettivi della cooperativa ci sia quello di «rafforzare la posizione dei singoli individui, affinché compiano scelte informate prima di acconsentire all'utilizzo dei dati, influenzando i termini e le condizioni stabiliti dalle organizzazioni di utenti dei dati, cui è subordinato l'utilizzo dei dati, in modo da offrire scelte migliori ai singoli membri del gruppo»; all'art. 12, comma 1, lett. *m*), nel delineare il contenuto fiduciario dei doveri gravanti sugli intermediari di dati personali (tra i quali rientrano le cooperative), contempla specifici compiti di consulenza, in modo tale da fornire agli interessati adeguate informazioni sulle proposte negoziali dei terzi «prima che gli interessati diano il loro consenso».

[39] G. RESTA, *La regolazione digitale nell'Unione europea – pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit., p. 971.

Il percorso avviato, che rappresenta indiscutibilmente un lodevole tentativo di creare un modello di sviluppo e di gestione dei dati dei cittadini europei orientato alla tutela della dignità e della libertà degli stessi, meriterebbe di essere maggiormente valorizzato, anche aprendo con più decisione all'autonomia contrattuale.

In questa prospettiva occorrerebbe operare una rilettura del sistema normativo delineato dal GDPR che mantenga viva l'esigenza protezione della persona, ma che, al contempo, sia compatibile con le esigenze di ulteriore sviluppo delineate dal *Data Governance Act*, evitando letture anacronistiche, rappresentative di una visione superata e non più rispondente appieno alle moderne esigenze di protezione di cui necessitano i cittadini europei. Beninteso, non si auspica un affievolimento delle tutele, ma una maggiore flessibilità nella gestione dei dati che ci riguardano e che decidiamo di condividere. Occorre compiere un passo più deciso in questa direzione, evitando che il bilanciamento tra le esigenze di protezione dei dati personali e quelle di libera circolazione (entrambi presenti nella disciplina del GDPR) finiscano per porsi in una palese contraddizione di fondo, di ostacolo alla creazione di un mercato unico dei dati e, con esso, allo sviluppo del progresso tecnologico e sociale che ci si aspetta nel contesto della *data-driven society*.

La storia, evidentemente, non finisce mai.

È ciclica ed ogni epoca è segnata da nuove minacce che obbligano le istituzioni ed i cittadini tutti a riflettere e ridiscutere in merito a questioni e a diritti che – a volte con eccessiva sicurezza – vengono, dagli stessi, ritenuti acquisiti; ed ogni generazione deve imporre le proprie volontà e la propria immaginazione per poter superare le contraddizioni sociali, economiche e politiche del proprio tempo.

Come consentire uno sviluppo armonioso dell'economia, senza cedere alla bramosia del capitalismo della sorveglianza, tutelare i soggetti più fragili, redistribuire la ricchezza. Sono queste le sfide che la società europea e le prossime generazioni saranno chiamate ad affrontare. Gli strumenti sui quali poter discutere ad avviare tavoli di confronti ci sono. L'augurio è quello di non perdere l'occasione di portare maggiore democraticità e solidarietà in una società, come quella contemporanea, che, caratterizzata da un irragionevole liberismo economico, sembrerebbe averle, almeno in larga parte, smarrite.

Capitolo III

Le cooperative di dati: la disciplina della fattispecie tra statuto sociale e regolamenti interni

Gianluca Riolfo

Abstract: Data Governance Act, Regulation (EU) 2022/868, seeks to increase trust in data sharing, strengthen mechanisms to increase data availability and overcome technical obstacles to the reuse of data. To reach these objectives an important role is played by so called "data intermediaries": they will function as neutral third parties that connect individuals and companies with data users. One of these intermediaries are "data cooperatives". The Regulation does not define and regulate them. These brief reflections attempt to offer a first reconstructive proposal for the drafting of a data cooperative statute.

1. Introduzione.

Il Regolamento (UE) 2022/868 (c.d. *Governace Data Act*), al fine di «istituire un regime orizzontale per il riutilizzo di talune categorie di dati protetti detenuti da enti pubblici e per la fornitura di servizi di intermediazione dei dati e di servizi basati sull'altruismo dei dati» [1], prevede che – tra gli intermediari di dati – possano esservi anche le «cooperative di dati».

[1] Secondo il dettato del *considerando* n. 3. Tali finalità sono poi ulteriormente specificate nel *considerando* n. 5, a mente del quale «L'azione a livello dell'Unione è necessaria per aumentare la fiducia nella condivisione dei dati istituendo adeguati meccanismi che garantiscano il controllo da parte degli interessati e dei titolari dei dati sui dati che li riguardano e al fine di affrontare altri ostacoli al buon funzionamento di un'economia competitiva basata sui dati», con «l'obiettivo di creare fiducia tra gli individui e le imprese per quanto riguarda l'accesso ai dati, la loro condivisione e il loro controllo, utilizzo e riutilizzo, in particolare stabilendo adeguati meccanismi per gli interessati affinché conoscano ed esercitino fattivamente i propri diritti nonché per quanto riguarda il riutilizzo di alcune

In cosa si sostanzino tali cooperative non è spiegato dal legislatore europeo. Non troviamo infatti una definizione di "cooperativa di dati" ma solamente quella di «servizi di cooperative di dati» [2], da intendersi come «servizi di intermediazione dei dati offerti da una struttura organizzativa costituita da interessati, imprese individuali o da PMI, che sono membri di tale struttura, avente come obiettivi principali quelli di aiutare i propri membri nell'esercizio dei loro diritti in relazione a determinati dati, anche per quanto riguarda il compiere scelte informate prima di acconsentire al trattamento dei dati, di procedere a uno scambio di opinioni sulle finalità e sulle condizioni del trattamento dei dati che rappresenterebbero al meglio gli interessi dei propri membri in relazione ai loro dati, o di negoziare i termini e le condizioni per il trattamento dei dati per conto dei membri prima di concedere l'autorizzazione al trattamento dei dati non personali o prima che essi diano il loro consenso al trattamento dei dati personali» [3].

All'interprete spetta il compito di ricostruire una fattispecie che la disciplina normativa pare solamente abbozzare [4]: il compito è indubbiamente non agevole ma, nello stesso tempo, affascinante. Il punto di partenza non può che essere dato dalla disciplina interna (codicistica) delle società cooperative non ravvisandosi – nelle intenzioni del legislatore europeo – la volontà di dare vita ad un tipo o modello "nuovo" di società (o ente).

Non possono, peraltro, nascondersi le peculiarità che connotano una cooperativa "di dati" e l'attività di intermediazione degli stessi, se non altro per il fatto di operare con "dati" (personali o meno) di una serie di soggetti. Tali dati [5] sono di difficile inquadramento giuridico e sono oggetto di disciplina da parte di vari provvedimenti normativi, sia europei che interni [6].

Tra le tante questioni da affrontare in tema, come strutturare la cooperativa attraverso la disciplina statutaria e regolamentare (interna) occupa una posizione preminente. Lo spazio di autoregolamentazione è indubbiamente ampio ma vanno sem-

---

tipologie di dati detenuti dagli enti pubblici, la fornitura di servizi da parte dei fornitori di servizi di intermediazione dei dati agli interessati, ai titolari e agli utenti dei dati, nonché la raccolta e il trattamento dei dati messi a disposizione a fini altruistici da persone fisiche e giuridiche».

[2] Su tali aspetti si veda ampiamente F. BRAVO, *Le cooperative di dati*, in *Contr. impr*., 3, 2023, p. 759 ss.

[3] Art. 2, n. 15, Reg. (UE) 2022/868.

[4] Oltre agli obiettivi che le cooperative di dati dovrebbero perseguire alcuni tratti caratterizzanti le stesso sono ricavabili dalle regole poste per tutti i servizi di intermediazione di dati dall'art. 12 del sopra richiamato regolamento.

[5] Definiti dall'art. 2, n. 1, Reg. (UE) 2022/868 come «qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi raccolta di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva».

[6] Si pensi, solo per fare qualche richiamo, al Regolamento (UE) 2016/679 (noto come *GDPR*), al Regolamento (UE) 2022/1925 ("relativo a mercati equi e contendibili nel settore digitale"), al Regolamento (UE) 2022/2065 ("relativo al mercato unico dei servizi digitali"), e così via.

pre tenute in considerazione le regole generali in tema di cooperative e quelle, per così dire speciali, in materia di intermediazione dei dati.

In particolare, uno dei primi aspetti su cui soffermarsi è quello della "costruzione" del rapporto sociale. È innegabile che i "dati" (secondo i dettami del *GDPR*) sono oggetto di «diritti personali dell'interessato e che quest'ultimo non può rinunciarvi». Vi è quindi una dicotomia tra una «*governance* individuale» sui propri dati da parte del singolo ed una «"*governance*" collettiva» dell'insieme dei dati dei soci da parte della cooperativa [7]. Essa può essere ricomposta ed armonizzata utilizzando per la disciplina della "*governance* collettiva", lo statuto sociale (funzionale a delineare il "rapporto sociale") e per la definizione della "*governance* individuale" lo strumento regolamentare interno (funzionale a disciplinare il "rapporto mutualistico").

Le brevi riflessioni che seguono sono focalizzate su tali aspetti.

2. Lo statuto e la regolamentazione del rapporto sociale.

Nella ricostruzione del "rapporto sociale" va anzitutto definito come il socio possa diventare tale o, per meglio dire, quale conferimento lo stesso può essere chiamato ad effettuare.

L'ipotesi che si intende presentare è che il conferimento sia fatto in denaro. Una somma, definita nello Statuto (o successivamente deliberata dall'assemblea), versata la quale (o, comunque, assunto l'impegno a versarla) il socio acquista la qualità di "socio" e diviene titolare dei diritti e degli obblighi ad essa legati.

Con il conferimento del denaro si attiva il "rapporto sociale" e si realizza quella "*governance*" collettiva che significa, nella sostanza, poter contribuire con il proprio voto a fissare gli obiettivi della gestione e le modalità concrete di realizzazione dell'oggetto sociale [8].

---

[7] In tal senso F. BRAVO, *op. cit*., p. 762, che rileva come ad una «permanenza in capo ai singoli membri del controllo sui propri dati e sulla loro utilizzazione da parte della cooperativa, seppur in una logica di confronto interno, lasciando ai singoli membri la "*governance*" individuale sui propri dati personali, anche nel caso in cui si giungesse, a livello di "struttura organizzativa", a decisioni su un determinato utilizzo dei dati medesimi, unitamente a quelli di altri soggetti membri», si affianchi «una "*governance*" collettiva sui dati conferiti dai singoli membri, esercitata dalla "struttura organizzativa" (… cooperativa di dati) e definita dai singoli membri che la compongono attraverso un confronto (democratico) tra i membri medesimi, avente ad oggetto le modalità di utilizzo dei dati in forma cooperativa, facendo comunque salve le decisioni adottate individualmente dai singoli membri. In altre parole, si viene a realizzare una "*governance*" duale, in base alla quale le scelte strategiche ed operative delineate a livello di cooperativa di dati (tramite la "*governance* collettiva") non precludono l'esercizio della "*governance* individuale", quantomeno qualora si tratti di dati personali facenti capo a singoli membri qualificabili come interessati al trattamento ai sensi del Reg. UE 679/2016».

[8] In sostanza lo svolgimento di quelle attività di intermediazione nei dati a beneficio dei propri soci che, descritte e fissate nello statuto, costituiscono il fine ultimo dell'agire societario e l'interesse sociale che gli amministratori devono perseguire.

I propri "dati" non devono essere conferiti dal socio ma solamente resi disponibili alla cooperativa per l'esercizio dell'impresa. Come si dirà subito appresso, la messa a disposizione dei dati costituisce oggetto di quel rapporto mutualistico che deve trovare definizione e descrizione in un apposito regolamento interno.

Ciò non esclude che si possa immaginare un conferimento in senso tecnico-giuridico del dato. Ciò a patto di considerare il dato stesso quale bene o utilità idonea a ciò. È noto come ad una società possa essere conferita qualunque utilità suscettibile di valutazione economica (denaro, beni mobili o immobili, beni immateriali, prestazioni d'opera o servizi, crediti, aziende e così via). Ed è altresì pacifico che tale conferimento di beni, (escluso quindi il denaro e la propria attività personale) possa essere anche nella forma del godimento a beneficio della società [9].

Diversa è però la disciplina dei conferimenti in natura (comprensivo di crediti e aziende) o di prestazioni nelle società di persone rispetto a quelli delle società di capitali. Nelle prime il valore del conferimento è lasciato alla determinazione effettuata dai soci nello statuto mentre nelle seconde – laddove ammesso [10] – il valore del conferimento deve necessariamente essere fissato da una perizia di stima fatta da un soggetto terzo ed indipendente [11].

L'opinione prevalente ritiene che i dati relativi ad un soggetto costituiscano attributi della sua personalità (similmente al nome o all'immagine, tanto per esemplificare), pur se una «visione patrimonialistica e obiettivizzata dei dati personali» pare emergere sin dal GDPR [12].

Tenendo per buona la prima posizione, non vi è dubbio che il soggetto possa attribuire ad altri il diritto di utilizzare i propri dati ma conservando sempre il potere di riappropriarsi, in ogni momento, del diritto di utilizzo [13].

---

[9] Il riferimento ai conferimenti in godimento è espresso per le società di persone (*ex* art. 2254 c.c.) ma si ritiene ammissibile anche per le società di capitali.

[10] Ad esempio nella società per azioni non è ammesso il conferimento di prestazioni d'opera o di servizio (art. 2342, u.c., c.c.) ma è consentito emettere una particolare categoria di azioni (c.d. con prestazioni accessorie) a cui è legato un obbligo di *facere*, ulteriore rispetto all'impegno a versare la quota di capitale sottoscritta (art. 2345 c.c.). Nelle società a responsabilità limitata è ammesso il conferimento di prestazioni d'opera o servizio ma esso deve essere garantito attraverso il rilascio, da parte del socio conferente a beneficio della società, di una polizza assicurativa o di una fideiussione pari al valore ad esse assegnato all'atto del conferimento (art. 2464, comma 6, c.c.).

[11] Le ragioni di tale regolamentazione sono note: nelle società di persone la consistenza effettiva del capitale sociale rileva in maniera relativa, essendoci la garanzia illimitata e solidale dei soci per le obbligazioni sociali. Nelle società di capitali invece, l'unica garanzia per i creditori sociali è data dal capitale sociale la cui consistenza deve essere fissata e determinata nell'atto costitutivo e deve permanere (salvo operazioni di riduzione del capitale) per tutta l'esistenza della società.

[12] Si vedano, ad es., le diverse posizioni in F. BRAVO, *Intermediazione di dati personali e servizi di* data sharing *dal GDPR al* Data Governance Act, in *Contr. impr. Europa*, 1, 2021, p. 226 ss. nonché p. 236 ss. (ed *ivi* ulteriori riferimenti alle principali posizioni dottrinali in tema).

[13] Significativamente F. BRAVO, *Intermediazione*, cit., p. 240, rileva come l'interessato «cui i dati appartengono (*data holder*)» può «concedere a terzi l'accesso a tali dati o la fruizione in condivisione,

Tutto ciò porta a ritenere che, se di conferimento in senso tecnico-giuridico si vuol parlare, esso dovrà essere della facoltà di utilizzo del dato, quindi un conferimento in godimento alla cooperativa [14]. Ma con almeno un paio di questioni problematiche: la prima (forse superabile), è costituita dalla possibile difficoltà di "valorizzare" quei dati al fine dell'iscrizione a capitale del "conferimento". La seconda, a mio avviso di più ardua soluzione, è legata al fatto che l'uscita del socio dalla società – nel caso di conferimento in godimento – non legittima lo stesso a riottenere la disponibilità del bene (il cui godimento permane in capo alla società fino al termine della stessa). Il socio uscente (o i suoi eredi) avrebbero diritto solo al valore della loro quota. Ma ciò pare scontrarsi con il fatto che l'utilizzo dei dati consesso da un soggetto ad un altro deve sempre poter essere revocato [15].

Ritengo, in definitiva, che ammettere la percorribilità di un "conferimento" di "dati" nella cooperativa possa comportare in corto circuito tra diritto societario e diritto privato di difficile soluzione.

3. Il regolamento e la disciplina del rapporto mutualistico.

Appare allora più agevole regolare la messa a disposizione dei dati alla cooperativa attraverso il rapporto mutualistico: il socio diviene tale sottoscrivendo una quota di capitale sociale (in denaro) e, contestualmente, stipulando un apposito contratto con la cooperativa al fine di consentire alla stessa di utilizzare (per i fini sociali e a beneficio dei soci stessi) i dati apportati dal socio [16].

---

finanche l'utilizzo per finalità commerciali, ma sempre "sotto il proprio controllo". La dimensione del "controllo", menzionata espressamente nella definizione di titolare dei dati, perdura anche di fronte alla concessione dell'accesso o della condivisione in favore dell'utente dei dati, per l'utilizzo commerciale o non commerciale che questi ne faccia e ciò, con riguardo ai dati personali, è funzionale alla loro natura di attributo della persona, non disponibile e non rinunciabile ed è ricollegabile al concetto di autodeterminazione informativa ben esplorato in dottrina». Per altro, ID, *Le cooperative di dati*, cit., p. 788, rimarca che «l'utilizzo del dato personale (e non il "dato personale" in sé) può essere oggetto di negoziazione e di contrattualizzazione, attraverso un accordo che si raggiunge mediante un consenso di natura contrattuale (non autorizzatorio), vertente sulle condizioni economiche e contrattuali (*terms and conditions*) stabilite tra le parti».

[14] Sempre secondo F. BRAVO, *Le cooperative di dati*, cit., p. 792, «i diritti sui dati non possono essere mai oggetto di trasferimento e, al contempo, sono da escludere operazioni volte a configurare l'apporto dei soci, che forniscono dati alle cooperative, come una sorta di conferimento "reale". I dati personali hanno tutt'altra natura e, al più, ciò che può essere conferito riguarderà il diritto all'utilizzo dei dati, sempre revocabile ad opera dell'interessato, ma non i dati in sé, su cui i *data subject* continuano a mantenere inalterato il controllo».

[15] Senza contare che, laddove lo si volesse ammettere, la restituzione del diritto di utilizzo dei dati (il conferimento in godimento effettuato) comporterebbe probabilmente la necessità di riduzione del capitale sociale venendo meno uno dei conferimenti.

[16] Ancora F. BRAVO, *Le cooperative di dati*, cit., p. 793: «mentre il divieto della rinunzia, quale tipico atto abdicativo», implicherebbe «l'impossibilità del conferimento in società (atto con efficacia

Il modello potrebbe essere quello delle cooperative di lavoro, dove i diritti e i doveri del socio in quanto lavoratore sono disciplinati da un accordo *ad hoc*, caratterizzante – appunto – il suddetto rapporto mutualistico. La duplicità di rapporti (sociale e mutualistico) è pacificamente ammessa anche in giurisprudenza. Così, secondo Cass. civ., 28 marzo 2007, n. 7646, «il socio di una cooperativa, beneficiario del servizio mutualistico reso da quest'ultima, è parte di due distinti (anche se collegati) rapporti (che non vanno, peraltro, sovrapposti, attesa la diversità della natura giuridica e la non assoluta omogeneità della relativa disciplina), l'uno di carattere associativo, che discende direttamente dall'adesione al contratto sociale e dalle conseguente acquisizione della qualità di socio, l'altro (per lo più di natura sinallagmatica), che deriva dal contratto bilaterale di scambio, per effetto del quale egli si appropria del bene o del servizio resogli dall'ente».

La regolamentazione generale del rapporto mutualistico può trovare spazio in un apposito regolamento interno [17], predisposto dall'organo amministrativo ed approvato (magari con maggioranze rafforzate, quali quelle dell'assemblea straordinaria) da parte dell'assemblea dei soci [18]. Esso dovrebbe contenere le regole generali per la disciplina del rapporto mutualistico, da declinarsi poi nei singoli accordi da stipulare tra socio e cooperativa. Nella sostanza, il regolamento viene ad assumere il ruolo di "condizioni generali di contratto" dello scambio mutualistico.

Nelle cooperative di dati il regolamento dovrà quindi specificare la tipologia di dati che il soggetto si rende disponibile ad apportare, la tipologia di contratto (in ipotesi, mandato con rappresentanza) che abilita la cooperativa a trattare/utilizzare i dati per conto del socio, le modalità di espressione del consenso informato, la durata del rapporto mutualistico [19], le modalità dell'eventuale rinnovo o della revoca del mandato alla società, e così via.

Atto costitutivo/statuto e regolamento sono evidentemente legati a doppio filo, così come il rapporto sociale e quello mutualistico traggono linfa uno nell'altro. Le vicende dell'uno possono incidere sull'altro (si pensi, ad es., ai requisiti richiesti dallo statuto per l'ammissione a socio – avere determinate tipologie di dati da apportare per l'utilizzo da parte della cooperativa secondo il proprio oggetto sociale –, le cause di recesso o esclusione, le conseguenze su entrambi i rapporti della morte del socio, e così via) [20].

---

reale), esso non preclude invece la stipula di un contratto di mandato (con rappresentanza), in quanto atto con mera efficacia obbligatoria».

[17] La previsione generale è contenuta nell'art. 2521, u.c., c.c.

[18] Un regolamento per disciplinare il rapporto mutualistico è obbligatorio per legge solamente nelle cooperative di lavoro. Ciò non toglie che l'obbligatorietà del regolamento possa derivare, per altre tipologie di cooperative, da un espresso richiamo ad esso nell'atto costitutivo/statuto.

[19] Durata che potrebbe non corrispondere con quella della società cooperativa.

[20] In definitiva, ai regolamenti può essere utilmente demandata la fissazione delle modalità e delle discipline da osservare nella esecuzione dei conferimenti da parte dei soci e dei criteri di ripartizione dei ristorni, in proporzione alla quantità e qualità degli scambi mutualistici. Ne consegue che i rego-

In definitiva, per consentire una piena esplicazione dei diritti individuali del titolare dei dati nell'ambito di una *governance* societaria collettiva della massa dei dati stessi apportati, scindere la fonte di regolamentazione del rapporto sociale (atto costitutivo/statuto) dal rapporto mutualistico (regolamento) potrebbe rappresentare la soluzione migliore.

4. Riflessioni di sintesi.

Le presenti brevi riflessioni costituiscono solamente un punto di partenza per una riflessione che dovrà essere "esplosa" in molteplici direzioni. Non solo verso gli aspetti più strettamente societari e di *governance* della cooperativa di dati (tanto per citarne qualcuno, i requisiti degli amministratori, l'eventuale presenza di amministratori indipendenti, l'adeguatezza degli assetti con particolare riferimento alla prevenzione dei rischi tecnologici) ma anche con riguardo ai profili più strettamente civilistici e contrattuali (la tipologia di accordo che innerva il rapporto mutualistico e le particolari condizioni e clausole di esso in conformità non solo al *Data Governance Act* ma, anche, al *GDPR* e al quadro normativo interno ed europeo in tema di dati e loro gestione).

Un lavoro che si preannuncia molto impegnativo per gli interpreti ma che, se ben condotto, può portare all'emersione di un modello di *business* nuovo e più democratico. Gli spazi per l'autonomia privata sono molto ampi e vanno ben sfruttati.

Ciò che deve guidare l'operatore ed il giurista nella costruzione del modello è l'ineliminabile e fondamentale condizione della mutualità: la gestione e l'utilizzo dei dati da parte della cooperativa è improntata sul servizio che questa rende ai propri soci. Il superiore interesse del titolare dei dati a trarre vantaggi economici dall'uso dei dati stessi è la *mission* imposta alla cooperativa.

D'altra parte il *Governance Data Act* appare funzionale alla creazione di un mercato dei dati in cui l'interesse dei titolari debbono prevalere sulle logiche di mercato e sui modelli di *business* in cui il dato viene sfruttato economicamente da imprese nel loro esclusivo interesse.

Richiamando alcuni passaggi dei Considerando del Regolamento, «ai fini della progettazione, della creazione e del mantenimento delle condizioni di parità nell'economia dei dati, è necessaria una solida *governance* in cui i portatori di interessi di uno spazio comune europeo di dati devono partecipare ed essere rappresentati» [21].

L'obiettivo è «aumentare la fiducia nella condivisione dei dati istituendo adeguati meccanismi che garantiscano il controllo da parte degli interessati e dei titolari dei dati sui dati che li riguardano (…). Un quadro di *governance* a livello del-

lamenti dovranno disciplinare l'attività svolta dalla cooperativa prevedendo modalità, termini e condizioni per lo svolgimento dei rapporti di scambio mutualistico fra società e soci, comprese eventuali sanzioni applicabili per gli inadempimenti.

[21] *Considerando* n. 2.

l'Unione dovrebbe avere l'obiettivo di creare fiducia tra gli individui e le imprese per quanto riguarda l'accesso ai dati, la loro condivisione e il loro controllo, utilizzo e riutilizzo, in particolare stabilendo adeguati meccanismi per gli interessati affinché conoscano ed esercitino fattivamente i propri diritti nonché per quanto riguarda il riutilizzo di alcune tipologie di dati detenuti dagli enti pubblici, la fornitura di servizi da parte dei fornitori di servizi di intermediazione dei dati agli interessati, ai titolari e agli utenti dei dati, nonché la raccolta e il trattamento dei dati messi a disposizione a fini altruistici da persone fisiche e giuridiche. In particolare, una maggiore trasparenza per quanto riguarda la finalità dell'utilizzo dei dati e le condizioni in cui i dati sono conservati dalle imprese può contribuire ad aumentare la fiducia» [22].

La cooperativa di dati può essere uno di questi "meccanismi". All'interprete il compito di renderlo operativo e funzionale.

[22] *Considerando* n. 5.

Capitolo IV

Le cooperative di dati: un approccio moderno ai dati per la *gig economy*

Adriana Topo-Massimiliano Rosa[*]

Abstract: The purpose of this paper is to explore how the discipline related to data cooperatives, introduced by the Data Governance Act (Reg. EU 2022/868), can contribute to the development of a new paradigm for data use in the gig economy. The approach traditionally pursued by Labor Law has been to limit the collection and use of work-related data. This approach stems from the recognition that an accumulation of information available to business organizations produces a plurality of negative consequences for the weaker party to the labor relationship: the ability to gather and process data allows the employer to exercise more pervasive and precise control over the worker and to become aware of subjective conditions that can be used to enact discriminatory practices. Instead, the DGA can stimulate a modern approach to both personal and non-personal data collected in the workplace. The challenge lies in not viewing data as mere information likely to harm workers, but as assets that can be enhanced in the interest of workers. Taking into account inputs offered by the DGA, the paper aims to reflect on the opportunities and challenges of data cooperatives, with a specific focus on the gig economy. The first section outlines the main national and european provisions relevant to the processing of platform workers' data. The objective is to demonstrate how the aim of these regulations is to limit the circulation of data and, at the same time, to promote transparency. In the second section, a brief overview of data cooperatives is undertaken, raising some interpretative issues for gig economy data cooperatives. It is then examined how data cooperatives can contribute to the development of platform cooperativism, a broader movement aimed at building a democratic economic model based on the sharing of ownership and profits generated through digital platforms, as an alternative to platform capitalism.

[*] Adriana Topo è autrice dei parr. 1 e 4, Massimiliano Rosa è autore dei parr. 2 e 3.

nuovo paradigma per la valorizzazione dei dati nella *gig economy*: cornice teorica e applicazioni pratiche.

1. L'approccio tradizionale del diritto del lavoro tra limitazione alla circolazione dei dati dei lavoratori e trasparenza.

Il potenziamento tecnologico della capacità delle imprese di raccogliere ed elaborare sempre più ingenti quantità di dati permette lo sviluppo di modalità di controllo dei lavoratori che, se non adeguatamente governate, sono in grado di incidere profondamente sulla qualità e dignità del lavoro. Infatti, le moderne organizzazioni digitalizzate sono in grado di acquisire e analizzare flussi informativi che consentono al datore di lavoro di ricostruire con estrema precisione tutte le attività svolte, o non svolte, dal prestatore durante e, financo, al di fuori dell'orario di lavoro.

Inoltre, il datore di lavoro può avere interesse a raccogliere quante più informazioni possibili sulla personalità, la vita privata e le condizioni soggettive di candidati all'assunzione e lavoratori. Per acquisire una conoscenza completa sulle persone con cui ha intenzione di intraprendere una relazione lavorativa o con cui collabora, il datore di lavoro spesso ricerca informazioni ulteriori rispetto a quelle strettamente funzionali a valutare la capacità e l'attitudine professionale dei prestatori, con il rischio che tali conoscenze siano poste a fondamento di comportamenti discriminatori nell'accesso e nella gestione del rapporto di lavoro. Infatti, la conoscenza di informazioni "sensibili", costituenti dati personali – come ad esempio condizioni di salute, opinioni politiche, religiose e sindacali e, persino, gusti e preferenze soggettive – rischia di esporre i lavoratori a trattamenti sfavorevoli, fondati su pregiudizi o su informazioni prive di significato ai fini della valutazione dell'attitudine professionale.

Un elemento di analisi significativo da tenere in considerazione per comprendere i rischi correlati al trattamento dei dati personali è che i lavoratori potrebbero non essere consapevoli della stessa acquisizione e conservazione dei dati da parte del datore. A titolo di esempio, i lavoratori potrebbero non essere a conoscenza di tutti i dati costantemente memorizzati all'interno degli strumenti di lavoro. Ugualmente, il datore di lavoro potrebbe impiegare strumenti per controllare in modo occulto l'esecuzione del lavoro e gli altri comportamenti che un lavoratore tiene durante il lavoro.

Lo scenario delineato rende evidente come la soggezione dei lavoratori, e dunque la loro vulnerabilità, siano elementi intrinseci alla relazione di lavoro e tale debolezza risulta notevolmente accresciuta in ragione dell'utilizzo di strumenti di lavoro e di metodi organizzativi che rendono difficile mantenere un effettivo controllo sui dati.

Non vi è dubbio che il trattamento dei dati dei lavoratori presenti peculiarità e criticità settoriali che devono essere tenute in considerazione. La relazione lavora-

tiva si caratterizza quale rapporto di durata che richiede un continuo e costante trattamento di dati personali dei lavoratori per molteplici finalità. Il rapporto di lavoro è, cioè, un rapporto ad alta "intensità informativa" [1]. L'acquisizione dei dati inizia già nella fase di selezione del personale e può continuare financo a seguito della cessazione della relazione lavorativa, ad esempio qualora risulti necessaria la conservazione di alcuni dati per adempiere a obblighi di legge. Di frequente, datore di lavoro-titolare del trattamento e candidato/lavoratore-interessato hanno interessi contrapposti in relazione al trattamento e alla conservazione dei dati. Il datore di lavoro ha interesse a disporre delle informazioni necessarie ad organizzare efficacemente la propria attività produttiva e forza lavoro, a controllare il corretto adempimento della prestazione e a sanzionare l'inadempimento dei dipendenti. Invece, i lavoratori hanno interesse a mantenere privati determinati aspetti della propria vita e personalità, a svolgere la prestazione senza essere sottoposti a un monitoraggio continuativo e pervasivo e a comprendere le modalità con cui il datore di lavoro utilizza i loro dati.

Tuttavia, un equo contemperamento tra i diversi interessi che connotano il rapporto lavorativo difficilmente si può ottenere in assenza di un intervento eteronomo. L'inderogabilità delle norme giuslavoristiche si basa, infatti, sul presupposto che i dati oggetto di trattamento da parte del datore appartengono a coloro che si candidano all'assunzione o a lavoratori in forza, cioè a soggetti che si trovano in una posizione di relativa debolezza nel mercato del lavoro. Il consenso alla cessione dei dati da parte di soggetti istituzionalmente meritevoli di protezione potrebbe non riflettere l'autentica volontà dei lavoratori, che, con tale cessione, si potrebbero porre in una condizione di più accentuata debolezza nei confronti del datore. L'accesso generalizzato ai dati personali dei lavoratori può, infatti, accrescere considerevolmente i poteri datoriali, come efficacemente espresso nel preambolo del Commentario al *Code of practice on the protection of workers' personal data* adottato nel 1997 dall'Organizzazione Internazionale del Lavoro (OIL): «*the less, therefore, that the persons concerned know about who is processing which data for which purposes, the less they are able to assess their individual situation and to express and defend their interests: in short, they have difficulty in determining their own personal development. The quest for principles to govern the processing of personal data expresses, therefore, the need to protect human dignity*». Per tali ragioni, l'approccio tradizionale del Diritto del Lavoro si è basato sulla adozione di norme inderogabili finalizzate ad evitare che i prestatori, in condizione di subalternità rispetto all'imprenditore, perdano il controllo sui propri dati personali.

Le tutele apprestate dalla disciplina giuslavoristica si sono mosse lungo due principali direttrici: l'imposizione di limiti al trattamento dei dati del lavoratore e la trasparenza.

---

[1] A. TOPO, *Circolazione di informazioni, dati personali, profilazione e reputazione del lavoratore*, in C. PISANI-G. PROIA-A. TOPO (a cura di), *Privacy e lavoro. La circolazione dei dati personali e i controlli nel rapporto di lavoro*, Milano, 2022, p. 389 ss.

Del resto, tali garanzie risultano funzionali a rafforzare la protezione del lavoratore in ulteriori ambiti, come quello della salute e sicurezza sul lavoro. Infatti, un eccessivo monitoraggio e la mancanza di trasparenza circa l'utilizzo dei propri dati può incidere sul benessere psicologico del lavoratore e indurlo a incrementare i ritmi della prestazione, aumentando così il rischio di infortuni. Fenomeni di stress lavoro-correlato sono, del resto, percentualmente più consistenti in quelle situazioni in cui, ad esempio, il lavoratore è costretto a restare connesso agli strumenti di lavoro aziendali, senza beneficiare di quel diritto alla "disconnessione" del quale molto è stato scritto durante la pandemia da Covid-19[2].

Per quanto concerne la prima direttrice di intervento (limitazioni al trattamento dei dati dei lavoratori), possono essere considerate disposizioni emblematiche l'art. 8, l. n. 300/1970 (c.d. Statuto dei lavoratori)[3] e l'art. 10, d.lgs. n. 276/2003 (c.d. decreto Biagi)[4], entrambe richiamate dall'art. 113, d.lgs. n. 196/2003[5].

Entrambe le disposizioni vietano lo svolgimento di indagini e trattamenti di dati personali di candidati e lavoratori inerenti a profili tipicamente connessi a fenomeni di discriminazione o comunque non attinenti alla valutazione dell'attitudine professionale del lavoratore: l'art. 8 St. Lav. con riferimento al datore di lavoro, mentre l'art. 10 del decreto Biagi con riguardo alle agenzie per il lavoro (art. 4, d.lgs. n. 276/2003) nonché agli altri soggetti pubblici e privati autorizzati o accreditati ad operare nel mercato del lavoro (artt. 6 e 7, d.lgs. n. 276/2003 e art. 12, d.lgs. n. 150/2015).

---

[2] Per tutti, si rinvia a V. MAIO, *Il lavoro da remoto tra diritti di connessione e disconnessione*, in M. MARTONE (a cura di), *Il lavoro da remoto. Per una riforma dello smart working oltre l'emergenza*, Piacenza, 2020, p. 85 ss.

[3] Ai sensi dell'art. 8 St. Lav. «è fatto divieto al datore di lavoro, ai fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore».

[4] A norma dell'art. 10 del decreto Biagi, rubricato «divieto di indagini sulle opinioni e trattamenti discriminatori», «è fatto divieto alle agenzie per il lavoro e agli altri soggetti pubblici e privati autorizzati o accreditati di effettuare qualsivoglia indagine o comunque trattamento di dati ovvero di preselezione di lavoratori, anche con il loro consenso, in base alle convinzioni personali, alla affiliazione sindacale o politica, al credo religioso, al sesso, all'orientamento sessuale, allo stato matrimoniale o di famiglia o di gravidanza, alla età, all'handicap, alla razza, all'origine etnica, al colore, alla ascendenza, all'origine nazionale, al gruppo linguistico, allo stato di salute nonché ad eventuali controversie con i precedenti datori di lavoro, a meno che non si tratti di caratteristiche che incidono sulle modalità di svolgimento della attività lavorativa o che costituiscono un requisito essenziale e determinante ai fini dello svolgimento dell'attività lavorativa. È altresì fatto divieto di trattare dati personali dei lavoratori che non siano strettamente attinenti alle loro attitudini professionali e al loro inserimento lavorativo». Tali limiti, però, non possono in ogni caso impedire «di fornire specifici servizi o azioni mirate per assistere le categorie di lavoratori svantaggiati nella ricerca di una occupazione».

[5] Ai sensi del quale «resta fermo quanto disposto dall'articolo 8 della legge 20 maggio 1970, n. 300, nonché dall'articolo 10 del decreto legislativo 10 settembre 2003, n. 276». Per un commento della disposizione v. A. TOPO-M. ROSA, *Commento al d.lgs. n. 196/2003*, in *Codice commentato del lavoro*, Milano, in corso di pubblicazione.

Per quanto riguarda la trasparenza in merito all'utilizzo dei dati dei lavoratori, risulta particolarmente significativo il comma terzo dell'art. 4 della l. n. 300/1970, così come novellato dall'art. 23, d.lgs. n. 151/2015. Ai sensi di quest'ultima disposizione, le informazioni raccolte tramite strumenti tecnologici e di lavoro idonei a consentire il c.d. controllo a distanza dell'attività dei lavoratori «sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità … di effettuazione dei controlli» [6]. In questo modo, il legislatore condiziona la possibilità di utilizzare le informazioni raccolte tramite le apparecchiature tecnologiche, specie per quanto riguarda il loro impiego per l'adozione di sanzioni disciplinari, alla comunicazione preventiva e trasparente delle modalità con cui i dati dei lavoratori sono trattati.

2. (*segue*) Le sfide poste dall'utilizzo dei dati dei lavoratori nel contesto della *gig economy*: gli interventi europei e nazionali di rafforzamento dell'approccio tradizionale del diritto del lavoro.

Di recente si sta assistendo ad un aggiornamento del *corpus* normativo rilevante in materia di trattamento dei dati dei lavoratori al fine di fronteggiare le nuove sfide poste dalla gestione algoritmica del lavoro, specie nel contesto del lavoro tramite piattaforme digitali.

Il riferimento è alla direttiva UE 2024/2831 relativa al miglioramento delle condizioni di lavoro nel lavoro mediante piattaforme digitali, nonché all'art. 1-*bis*, d.lgs. n. 152/1997, recante «ulteriori obblighi informativi nel caso di utilizzo di sistemi decisionali o di monitoraggio automatizzati», introdotto dall'art. 4, d.lgs. n. 104/2022 (c.d. decreto trasparenza) e già modificato dal d.l. n. 48/2023 (c.d. decreto lavoro), convertito nella l. n. 85/2023.

La necessità di un *upgrade* normativo è stata avvertita in ragione delle numerose criticità sorte con riferimento al trattamento dei dati dei lavoratori utilizzati per alimentare algoritmi in grado di assumere decisioni automatizzate, o comunque deputati a fornire indicazioni rilevanti per la gestione del rapporto di lavoro. Il c.d. *algorithmic management of work* sfrutta, infatti, l'analisi dei dati attraverso l'applicazione di algoritmi per supportare o sostituire il decisore umano nell'esercizio delle tipiche funzioni manageriali [7].

---

[6] Nello specifico, la previsione si riferisce alle informazioni raccolte da: i) impianti audiovisivi e altri strumenti tecnologici dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori; ii) strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e strumenti di registrazione degli accessi e delle presenze.

[7] Uno studio congiunto condotto dall'Organizzazione Internazionale del Lavoro (OIL) e dall'European Commission's Joint Research Centre (JRC) relativo all'impatto della gestione algoritmica sull'organizzazione e sulla qualità del lavoro descrive il fenomeno come l'utilizzo di algoritmi «*which are digitally encoded and implemented by computers, and which process data*» nell'ambito del *manage-*

L'ambito in cui la gestione algoritmica si manifesta con maggiore evidenza, anche se non esclusivamente, è il lavoro tramite piattaforme digitali[8]. Infatti, le informazioni acquisite sul lavoratore – che possono essere le valutazioni fornite da clienti e/o esercenti, la revoca della disponibilità a fornire il servizio in uno *slot* temporale precedentemente selezionato, il numero di ordini accettati e rifiutati, la

---

ment, inteso come «*a set of tasks which are necessary for the administration of an organisation ... normally implemented by a specialised position which is at the top of the organisational hierarchy: the manager(s) ... summarised in five functions: planning (i.e. deciding in advance), staffing, commanding, coordinating and controlling ... With algorithmic management, all these functions can be supported or at least partly implemented with computer algorithms, if the associated managerial problems can be numerically encoded in a more or less unambiguous way*» (S. BAIOCCO-E. FERNANDEZ MACÍAS-U. RANI-A. PESOLE, *The Algorithmic Management of work and its implications in different contexts*, in *Background paper Series*, 21 giugno 2022, pp. 5-6).

S. BAIOCCO-E. FERNÁNDEZ MACÍAS definiscono il fenomeno come «*the use of computer programmed procedures, which can be AI or non-AI powered, to coordinate labour input in an organisation. It involves, for example, the definition and assignment of work shifts, the development and delivery of job-related instructions, the assessment of workers' performance and the assignment of rewards or penalties*» (*Algorithmic management: A basic compass*, European Commission, JRC Science for Policy Brief on Labour, Education and Employment, 2022, p. 1).

[8] Il fenomeno della gestione algoritmica, caratteristico delle piattaforme digitali, è diffuso anche in settori produttivi tradizionali, come nel settore della logistica, dove spesso addetti al *picking* e/o carrellisti ricevono indicazioni su prodotti da prelevare e tempistiche non dai propri superiori, bensì tramite applicazioni incorporate in *wearables* o strumenti di lavoro (cfr. A. DELFANTI, *Machinic Dispossession and Augmented Despotism: Digital Work in an Amazon Warehouse*, in *New Media & Society*, 2019, vol. 23, p. 39; A. WOOD, *Algorithmic Management: Consequences for Work Organisation and Working Conditions*, European Commission, *JRC Working Papers Series on Labour, Education and Technology*, 2021).

In giurisprudenza, con riferimento al settore logistico nazionale, cfr. Trib. di Padova, Sez. Lav., sent. 3 marzo 2023, n. 126, commentata da G. SANFILIPPO, *La verifica della genuinità dell'appalto nelle organizzazioni d'impresa (ultra)digitalizzate*, in *LavoroDirittiEuropa*, 22 giugno 2023 e da L. NANNIPIERI, *Eterodirezione "algoritmica" negli appalti della logistica. Verso un quadro giurisprudenziale in mutamento*, in *Rivista Italiana di Informatica e Diritto*, 2023, 1, p. 205. La pronuncia ha ravvisato forme di gestione algoritmica del lavoro in una controversia avente ad oggetto l'accertamento della genuinità o meno di contratti di appalto con cui un'impresa committente aveva demandato specifiche lavorazioni a terzi, fornendo «il programma informatico che dice al lavoratore cosa deve essere spostato, dove si trova e dove deve essere portato» (p. 5). La sentenza ha ritenuto che, dietro lo schema del contratto di appalto, in realtà, si celasse una prestazione di mera fornitura di manodopera da parte dell'impresa appaltatrice in quanto il sistema che consentiva di dirigere e controllare l'attività dei lavoratori faceva capo all'impresa committente. Tale elemento è stato ritenuto dirimente ai fini dell'imputazione in capo alla committente, quale datore di lavoro effettivo, del rapporto di lavoro formalmente intercorrente tra dipendente e impresa appaltatrice.

Tuttavia, mentre le piattaforme digitali sono ontologicamente strutturate su sistemi di gestione algoritmica, nei settori standard tali sistemi sono incorporati all'interno di un'organizzazione di lavoro preesistente, circostanza che può rendere più difficile identificarne l'utilizzo, specie qualora siano impiegati come supporto per decisioni comunicate ai lavoratori dal personale dell'impresa (v. S. BAIOCCO-E. FERNANDEZ MACÍAS-U. RANI-A. PESOLE, *The Algorithmic Management of work and its implications in different contexts*, cit., p. 17).

tempestività nel completare il servizio – sono elaborate dagli algoritmi delle piattaforme per attribuire un punteggio ai lavoratori. Il *ranking* può impattare sulle condizioni di lavoro e sul reddito dei *platform workers*, potendo incidere sull'allocazione delle offerte di lavoro; sull'ordine di prenotazione degli *slot* temporali di svolgimento della prestazione e, quindi, sulla probabilità di lavorare nei turni che presentano una maggiore richiesta di servizi; sulla stessa possibilità di accedere al proprio *account*, il quale può essere sospeso o, financo, disattivato automaticamente dalla piattaforma se il lavoratore scende al di sotto di un punteggio minimo [9]. Tale assetto gestionale prescinde pressoché integralmente dall'intervento di personale della piattaforma, essendo i processi automatizzati [10].

L'utilizzo dei dati per gestire la prestazione lavorativa non rappresenta certo una novità propria del lavoro tramite piattaforma. Tuttavia, quest'ultimo presenta significativi elementi di discontinuità rispetto alle modalità tradizionali di organizzazione del lavoro. Spesso, i *platform workers* non sono informati o adeguatamente informati sui dati raccolti e sul modo in cui questi incidono sulle logiche con cui il sistema automatizzato assume decisioni non vagliate dal personale della piattaforma [11]. Per descrivere questo fenomeno, in dottrina, si è evocata l'immagine suggestiva di un "datore di lavoro-algoritmo" che esercita in maniera impersonale e oscura i poteri datoriali nella struttura organizzativa digitalizzata e dematerializzata della piattaforma, in cui i prestatori, per la natura dell'attività, sono privi di una sede fisica e di un datore di lavoro immediatamente identificabile [12].

---

[9] Per una ricostruzione del funzionamento dell'algoritmo utilizzato da alcune piattaforme digitali cfr. A. ROSENBLAT-L. STARK, *Algorithmic Labor and information asymmetries. A case study of Uber's Drivers*, in *International Journal of Communication*, Vol. 10, 2016; A. INGRAO, *La protezione dei dati personali dei lavoratori nel diritto vivente al tempo degli algoritmi*, in A. BELLAVISTA-R. SANTUCCI (a cura di), *Tecnologie digitali, poteri datoriali e diritti dei lavoratori*, Torino, 2022, p. 127 ss.

[10] Un'analisi condotta dall'Ufficio Internazionale sul Lavoro sui *normative gaps* presenti nella legislazione internazionale con riguardo al lavoro tramite piattaforme evidenzia che: «*it is an algorithm that offers and grants services or tasks to workers, defines their time slots, calculates the rankings on which their activities and income depend, and decides whether they will continue to provide services for the platform or remain deselected from it*» (GB.347/POL/1, par. 18).

[11] Emblematica in tal senso è l'ordinanza di ingiunzione 10 giugno 2021, n. 234 del Garante per la protezione dei dati personali che ha rilevato la commissione di diverse infrazioni da parte di una nota piattaforma di *food delivery*, specie sotto il profilo della trasparenza dei trattamenti. Il Garante ha riscontrato che non erano state comunicate ai *riders* le effettive modalità di trattamento dei dati relativi alla propria posizione geografica – consistenti nella visualizzazione su mappa del percorso effettuato e nella raccolta sistematica del dato ogni quindici secondi – ma soltanto generiche informazioni sul ricorso alla geolocalizzazione. Inoltre, il provvedimento ha ravvisato omissioni informative circa la «effettuazione di trattamenti automatizzati compresa l'attività di profilazione ... preordinati all'assegnazione di un punteggio al rider al dichiarato fine di determinare la priorità nella prenotazione degli slot» e sulle «informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato».

[12] A. ALOISI-V. DE STEFANO, *Your Boss Is an Algorithm: Artificial Intelligence, Platform Work and Labour*, Hart Publishing, UK, 2022.

Come anticipato, per far fronte a tali sfide, nel contesto europeo è stata adottata la direttiva 2024/2831 sul lavoro tramite piattaforme digitali [13], mentre nell'ordinamento nazionale il c.d. decreto trasparenza ha introdotto specifici obblighi informativi in caso di utilizzo nell'impresa di sistemi «integralmente» automatizzati. Tali interventi regolatori, per quanto innovativi, sembrano collocarsi nel segno della continuità con l'approccio tradizionale del Diritto del Lavoro, fondato, da un lato, sulla limitazione all'accesso e all'utilizzo dei dati dei lavoratori, dall'altro, sulla trasparenza circa l'utilizzo di tali dati.

Partendo dalla direttiva europea, questa presenta tra i propri scopi quello di «migliorare la protezione delle persone che svolgono un lavoro mediante piattaforme digitali per quanto riguarda il trattamento dei loro dati personali, aumentando la trasparenza, l'equità, la supervisione umana, la sicurezza e la responsabilità delle pertinenti procedure di gestione algoritmica nel lavoro mediante piattaforme digitali» (*considerando* n. 16) [14].

Il legislatore europeo ritiene che le sfide poste dal lavoro mediante piattaforme digitali richiedano misure ulteriori rispetto a quelle contenute nel Reg. (UE) 2016/679, che pur contiene specifiche garanzie anche per quanto riguarda i processi decisionali automatizzati relativi alle persone fisiche (artt. 13, par. 2, lett. f), 14, par. 2, lett. g), 15, par. 1, lett. h) e 22). In effetti, il GDPR è stato individuato da parte della dottrina come possibile rimedio alla opacità delle decisioni algoritmiche [15] e alcune decisioni ne hanno fatto applicazione per accrescere la trasparenza e ridurre l'asimmetria informativa che caratterizza il lavoro tramite piattaforme digitali [16]. D'altro

---

[13] Per un primo commento sulla direttiva v. G. SMORTO-A. DONINI, *L'approvazione della Direttiva sul lavoro mediante piattaforme digitali: prima lettura*, in *Labour & Law Issues*, 2024, vol. 10, n. 1, p. 24 ss.

[14] Nello specifico, la direttiva presenta un duplice obiettivo: «migliorare le condizioni di lavoro e la protezione dei dati personali nel lavoro mediante piattaforme digitali» (art. 1, par. 1). Entrambi gli obiettivi «sono perseguiti contemporaneamente e, sebbene si rafforzino reciprocamente e siano indissolubilmente legati, l'uno non è secondario rispetto all'altro» (*considerando* n. 16).

[15] In ordine al dibattito giuslavoristico interno sull'effettività dell'art. 22 GDPR come garanzia per la trasparenza algoritmica, si rinvia a G. PELUSO, *Obbligo informativo e sistemi integralmente automatizzati*, in *Labour & Law Issues*, 2023, vol. 9, n. 2, p. 111, nota 34: «sull'inesistenza nel GDPR di un diritto ad avere una spiegazione in relazione al processo decisionale automatizzato, v: G. Gaudio, *Algorithmic management, poteri datoriali e oneri della prova: alla ricerca della verità materiale che si cela dietro l'algoritmo*, *LLI*, 2020, 2, 29 ss.; G. Fioriglio*, Intelligenza artificiale, privacy e rapporto di lavoro: una prospettiva informatico-giuridica*, *LDE*, 2022, 3, 10. Sottolinea, invece, come "In relazione al funzionamento degli algoritmi, i principi di prevenzione e della trasparenza impongono, a favore dell'interessato, gli obblighi di informazione preventiva e di spiegazione delle operazioni che si avvalgono dell'A.I (c.d. *right of explaination*: artt. 13 e 15 GDPR)": P. Tullini, *Dati*, in M. Novella-P. Tullini (a cura di), *Lavoro Digitale*, Giappichelli, 2022, 121».

[16] Nel già citato provvedimento del 10 giugno 2021, n. 234, il Garante per la protezione dei dati personali ha ritenuto violati: i) l'art. 13, par. 2, lett. f), GDPR «considerato che la predetta informativa non fa riferimento alla effettuazione di trattamenti automatizzati compresa l'attività di profilazione …

canto, come rilevato nella relazione introduttiva alla proposta di direttiva [17], «sebbene tali diritti siano particolarmente pertinenti per le persone che lavorano mediante piattaforme digitali soggette a gestione algoritmica, recenti procedimenti giudiziari hanno messo in evidenza le limitazioni e le difficoltà che i lavoratori – e in particolare le persone che svolgono un lavoro mediante piattaforme digitali – devono affrontare quando intendono far valere i loro diritti in materia di protezione dei dati nel contesto della gestione algoritmica [18]. Ciò riguarda in particolare la difficoltà di tracciare la linea di demarcazione tra decisioni algoritmiche che incidono o meno sui lavoratori in modo sufficientemente "significativo"» [19].

Per tali ragioni, l'art. 7 della direttiva prevede specifiche limitazioni al trattamento dei dati personali dei *platform workers* mediante sistemi decisionali o di monitoraggio automatizzati [20], funzionali a contrastare la soggezione dei lavoratori

---

preordinati all'assegnazione di un punteggio al rider al dichiarato fine di determinare la priorità nella prenotazione degli slot (fasce orarie determinate dalla società all'interno delle quali sono inviati gli ordini di consegna); sono state pertanto altresì omesse "informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato"»; ii) l'art. 22, par. 3, GDPR in quanto «non risulta … che la società abbia provveduto ad attuare misure appropriate "per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano (…), di esprimere la propria opinione e di contestare la decisione" … non vi è evidenza alcuna della adozione di misure relative all'esercizio dei diritti attraverso l'attivazione di canali dedicati (chat accessibile attraverso l'applicazione, sportelli dedicati, email) … Né risulta che gli interessati fossero in alcun modo consapevoli della possibilità di esercitare tali diritti nei confronti delle decisioni adottate mediante l'utilizzo della piattaforma».

L'art. 22 GDPR è stato applicato anche dall'Amsterdam District Court, C/13/689705/HA RK 20-258, 11 marzo 2021, per richiedere a una piattaforma di trasporto via taxi di spiegare la logica sottostante a una decisione completamente automatizzata riguardante un lavoratore (cfr. R. GELLERT-M. VAN BEKKUM-F. ZUIDERVEEN BORGESIUS, *The Ola & Uber judgments: for the first time a court recognises a GDPR right to an explanation for algorithmic decision-making*, in *EU Law Analysis*, 28 aprile 2021).

[17] COM/2021/762.

[18] Cfr. C. HIEßL, *Case Law on Algorithmic Management at the Workplace: Cross-European Comparative Analysis and Tentative Conclusions*, European Commission, European Centre of Expertise in the field of labour law, employment and labour market policies (ECE), 7 aprile 2023.

[19] Come noto, l'art. 22 del GDPR riguarda le decisioni basate unicamente sul trattamento automatizzato, compresa la profilazione, che producano effetti giuridici che riguardano l'interessato o che incidano in modo analogo significativamente sulla sua persona.

[20] I sistemi di monitoraggio automatizzati sono quelli «utilizzati per effettuare, o che sostengono, il monitoraggio, la supervisione o la valutazione, tramite strumenti elettronici, dell'esecuzione del lavoro delle persone che svolgono un lavoro mediante piattaforme digitali o delle attività svolte nell'ambiente di lavoro, anche raccogliendo dati personali» (art. 2, par. 1, lett. h). Invece, i sistemi decisionali automatizzati sono definiti come quei «sistemi utilizzati per prendere o sostenere, tramite strumenti elettronici, decisioni che incidono significativamente sulle persone che svolgono un lavoro mediante piattaforme digitali, comprese le condizioni di lavoro dei lavoratori delle piattaforme digitali, in particolare decisioni che influenzano la loro assunzione, il loro accesso agli incarichi di lavoro e la relativa organizzazione, i loro guadagni, compresa la fissazione del prezzo dei singoli incarichi, la loro sicurezza e salute, il loro orario di lavo-

verso la piattaforma, prevenire abusi e consentire l'esercizio dei diritti fondamentali, specie in materia sindacale [21].

L'art. 9 è, poi, integralmente dedicato alla trasparenza dei sistemi decisionali o di monitoraggio automatizzati, richiedendo agli Stati membri di imporre alle piattaforme di lavoro digitali specifici obblighi informativi in favore dei lavoratori, dei loro rappresentanti e, su richiesta, delle autorità nazionali competenti [22]. Per non vanificare l'effettività della disposizione, tali informazioni devono essere fornite «in forma trasparente, intelligibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro».

Anche l'ordinamento interno, in anticipo rispetto all'introduzione delle regole euro-comunitarie, si è fatto promotore di previsioni finalizzate a «disvelare i dati che regolano il funzionamento dei sistemi organizzativo-manageriali» [23], nel tentativo «di intaccare l'opacità che caratterizza l'esercizio dei poteri datoriali a mezzo degli algoritmi» [24]. Peraltro, gli obblighi informativi introdotti dal d.lgs. n. 104/2022 – che ha inserito l'art. 1-*bis* all'interno del d.lgs. n. 152/1997 – hanno il pregio di perseguire la trasparenza dei «sistemi decisionali o di monitoraggio integralmente auto-

---

ro, il loro accesso alla formazione, la loro promozione o suo equivalente, e la loro situazione contrattuale, compresa la limitazione, la sospensione o la chiusura del loro account» (art. 2, par. 1, lett. *i*).

[21] Ai sensi dell'art. 7, par. 1, «le piattaforme di lavoro digitali, mediante sistemi di monitoraggio automatizzati o di sistemi decisionali automatizzati: a) non trattano dati personali relativi allo stato emotivo o psicologico della persona che svolge un lavoro mediante piattaforme digitali; b) non trattano dati personali relativi a conversazioni private, compresi gli scambi con altre persone che svolgono un lavoro mediante piattaforme digitali e i rappresentanti delle persone che svolgono un lavoro mediante piattaforme digitali; c) non raccolgono dati personali di una persona che svolge un lavoro mediante piattaforme digitali quando questa non sta svolgendo un lavoro mediante le stesse o non si sta proponendo di svolgerlo; d) non trattano dati personali per prevedere l'esercizio di diritti fondamentali, compresi la libertà di associazione, il diritto di negoziazione e di azioni collettive o il diritto all'informazione e alla consultazione stabiliti nella Carta; e) non trattano dati personali per desumere l'origine razziale o etnica, lo status di migrante, le opinioni politiche, le convinzioni religiose o filosofiche, la disabilità, lo stato di salute, comprese le malattie croniche o la sieropositività, lo stato emotivo o psicologico, l'adesione a un sindacato, la vita sessuale o l'orientamento sessuale di una persona; f) non trattano i dati biometrici, quali definiti all'articolo 4, punto 14), del regolamento (UE) 2016/679, di una persona che svolge un lavoro mediante piattaforme digitali per stabilirne l'identità confrontandoli con i dati biometrici di persone fisiche conservati in una banca dati».

[22] Per quanto concerne i sistemi di monitoraggio automatizzati, le informazioni riguardano, tra l'altro, «le categorie di dati e azioni monitorate, supervisionate o valutate da tali sistemi, compresa la valutazione da parte del destinatario del servizio», nonché «i destinatari o le categorie di destinatari dei dati personali trattati da tali sistemi e l'eventuale trasmissione o trasferimento di tali dati personali, anche all'interno di un gruppo di imprese» (art. 9, par. 1, lett. *a*). Invece, le informazioni relative ai sistemi decisionali automatizzati comprendono anche «le categorie di dati e i principali parametri di cui tali sistemi tengono conto e l'importanza relativa di tali principali parametri nel processo decisionale automatizzato, compreso il modo in cui i dati personali o il comportamento della persona che svolge un lavoro mediante piattaforme digitali incidono sulle decisioni» (art. 9, par. 1, lett. *b*).

[23] G. PELUSO, *Obbligo informativo e sistemi integralmente automatizzati*, cit., p. 111.

[24] *Ibidem*, p. 107.

matizzati»[25] anche per i lavoratori dei settori tradizionali, avendo, a differenza della direttiva europea, un ambito di applicazione generalizzato[26].

3. Le cooperative di dati: inquadramento giuridico e questioni interpretative.

Il Regolamento (UE) 2022/868 (d'ora in avanti *Data Governance Act* o DGA) propone un nuovo approccio rispetto ai dati, personali e non personali, prodotti e raccolti (anche) nel contesto lavorativo. Il DGA, infatti, invita a non considerare i dati esclusivamente come rischio, cioè come informazioni utilizzabili a danno dei lavoratori, ma anche come *assets* che possono essere oggetto di valorizzazione[27].

---

[25] In merito all'interpretazione della locuzione «integralmente automatizzati» si rinvia ai contributi di E. DAGNINO, *Modifiche agli obblighi informativi nel caso di utilizzo di sistemi decisionali o di monitoraggio automatizzati (art. 26, comma 2, d.l. n. 48/2023)*, in E. DAGNINO-C. GAROFALO-G. PICCO-P. RAUSEI (a cura di), *Commentario al d.l. 4 maggio 2023, n. 48 cd. "decreto lavoro"*, Bergamo, 2023, p. 56 ss., e di A. TOPO, *Nuove tecnologie e discriminazioni*, relazione presentata all'XXI Congresso Nazionale dell'Associazione Italiana di Diritto del Lavoro e della Sicurezza Sociale (AIDLASS), Messina, 23-25 maggio 2024, versione del 21 maggio 2024, pp. 38 ss.

[26] L'ambito di applicazione soggettivo degli obblighi informativi comprende non solo il datore di lavoro, ma anche, nei limiti della compatibilità, il committente nell'ambito dei rapporti di lavoro di cui all'art. 409, n. 3, c.p.c. (collaborazioni coordinate e continuative), dei rapporti di cui all'art. 2, comma 1, d.lgs. n. 81/2015 (collaborazioni etero-organizzate dal committente) e dei contratti di prestazione occasionale di cui all'art. 54-*bis*, d.l. n. 50/2017. L'ambito di applicazione oggettivo riguarda l'utilizzo di «sistemi decisionali o di monitoraggio integralmente automatizzati deputati a fornire indicazioni rilevanti ai fini della assunzione o del conferimento dell'incarico, della gestione o della cessazione del rapporto di lavoro, dell'assegnazione di compiti o mansioni nonché indicazioni incidenti sulla sorveglianza, la valutazione, le prestazioni e l'adempimento delle obbligazioni contrattuali dei lavoratori».

[27] A. TOPO, *Circolazione di informazioni, dati personali, profilazione e reputazione del lavoratore*, cit., pp. 389 ss., auspica lo spostamento del baricentro regolativo verso la valorizzazione delle potenzialità intrinseche dei dati dei lavoratori.

Secondo A. TROJSI, *Sull'impatto giuslavoristico del Data Governance Act. Riflessioni sistemiche a prima lettura del Regolamento (UE) 2022/868*, in *Federalismi.it*, 2023, 4, p. 283, «si è di fronte ad un'ulteriore maturazione della cultura (anche giuridica, e dunque del diritto) dei dati, improntata ad una visione dinamica di questi. È possibile registrare, cioè, il passaggio dal pregresso atteggiamento "difensivo" di tutela dei dati da utilizzi esterni ritenuti (e vissuti come) un attacco alla propria *privacy*, all'apertura verso le potenzialità dei dati. Il dato viene considerato in positivo come risorsa, nella sua qualità di generatore di valore, e non più solo come bene staticamente da preservare e custodire. Partendo dalla presa d'atto della realtà, ossia della inevitabilità del progresso digitale, e dal riconoscimento del carattere dinamico (appunto, del dinamismo) dei dati, l'intento ordinamentale è di cogliere propositivamente le sfide della digitalizzazione dei mercati. Ovviamente regolandola per evitare le più pericolose derive e distorsioni del diritto della concorrenza se lasciata a sé stessa (quale il *dumping* dei dati), in specie quelle lesive di diritti fondamentali o discriminatorie, ma – pur, dunque, nell'ambito di questo rilevante obiettivo – in un'ottica promozionale, non meramente impeditiva e re-

All'interno del DGA, la disciplina sulle cooperative di dati può contribuire allo sviluppo di una visione, complementare al regime protettivo, in grado di offrire opportunità ai lavoratori della *gig economy*. Infatti, i primi commentatori hanno individuato proprio le *data cooperatives* operanti in tale contesto come *case study* «per comprendere meglio l'atteggiarsi del fenomeno, ai fini dell'inquadramento giuridico, ben sapendo che le modalità operative possono articolarsi con maggiore complessità, in relazione ai diversi modelli operativi di *data governance*» [28].

Al fine di cogliere potenzialità e criticità per i *gig workers*, si ritiene opportuno procedere a un sintetico inquadramento dell'istituto.

Le cooperative di dati rappresentano una delle modalità con cui può essere fornito il servizio di intermediazione dei dati [29], ossia «un servizio che mira a instaurare, attraverso strumenti tecnici, giuridici o di altro tipo, rapporti commerciali ai fini della condivisione dei dati tra un numero indeterminato di interessati [30] e di titolari dei dati [31], da un lato, e gli utenti dei dati [32], dall'altro, anche al fine dell'esercizio

---

strittiva o proibizionistica, volta ad incentivare i flussi di dati e, per tale via, a sviluppare il mercato interno digitale».

[28] F. BRAVO, *Le cooperative di dati*, in *Contratto e impresa*, 2023, 3, pp. 757-799. L'Autore segnala come caso esemplificativo *Driver's Seat*, «una *data coopeative* americana operante nel settore dei trasporti, con servizi di "*ride-sharing*" (analoghi al modello *Uber*) e di "*delivering*" tramite *riders* (analoghi al modello Glovo o Deliveroo), gestiti tuttavia in forma di cooperativa, secondo le logiche mutualistiche, e non secondo il modello capitalistico tradizionale».

J. TAIT, *The Case for Data Cooperatives*, in *Whitepaper Series*, *Open Data Manchester*, 6 settembre 2021, descrive l'attività della *data cooperative* nei seguenti termini: «*Driver's Seat Cooperative in the United States is one such cooperative – it empowers gig-worker drivers to make better decisions about where and when they work by sharing their own collected data to challenge the work allocation algorithms operated by the likes of Uber and Lyft. Giving workers access to the data that is used to manage and control their work practices, especially when many are considered free agents by both these companies and the government, has the potential to counter exploitative employment practices. Value is further returned by anonymised data being sold to city governments to support transport policy. This data has the bonus of being ethically supplied by Driver's Seat members*».

[29] Oltre alle cooperative di dati, l'art. 10 del DGA individua altre due tipologie di servizi di intermediazione dei dati: i) servizi di intermediazione tra i titolari dei dati e i potenziali utenti dei dati; ii) servizi di intermediazione tra interessati che intendono mettere a disposizione i propri dati personali o persone fisiche che intendono mettere a disposizione dati non personali e potenziali utenti dei dati.

[30] La nozione di interessato è la medesima dell'art. 4, par. 1, n. 1, GDPR (art. 2, par. 1, n. 7, DGA).

[31] Il titolare dei dati è «una persona giuridica, compresi gli enti pubblici e le organizzazioni internazionali, o una persona fisica che non è l'interessato rispetto agli specifici dati in questione e che, conformemente al diritto dell'Unione o nazionale applicabile, ha il diritto di concedere l'accesso a determinati dati personali o dati non personali o di condividerli» (art. 2, par. 1, n. 8). Si tratta, quindi, di una figura diversa rispetto al titolare del trattamento di cui all'art. 4, par. 1, n. 7, GDPR, ossia «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali».

[32] L'utente dei dati è «una persona fisica o giuridica che ha accesso legittimo a determinati dati personali o non personali e che ha diritto, anche a norma del regolamento (UE) 2016/679 in caso di dati personali, a utilizzare tali dati a fini commerciali o non commerciali» (art. 2, par. 1, n. 9).

dei diritti degli interessati in relazione ai dati personali» (art. 2, par. 1, n. 11)[33]. Tali servizi non possono limitarsi alla messa a disposizione di strumenti tecnici ai fini della condivisione di dati con altri, essendo essenziale che il servizio miri ad instaurare un rapporto commerciale tra i predetti soggetti[34].

Il DGA non definisce direttamente le cooperative di dati, preferendo, invece, focalizzare l'attenzione sui servizi forniti dalle stesse. Ai sensi dell'art. 2, par. 1, n. 15, per «servizi di cooperative di dati» si intendono «servizi di intermediazione dei dati offerti da una struttura organizzativa costituita da interessati, imprese individuali o da PMI, che sono membri di tale struttura, avente come obiettivi principali quelli di aiutare i propri membri nell'esercizio dei loro diritti in relazione a determinati dati, anche per quanto riguarda il compiere scelte informate prima di acconsentire al trattamento dei dati, di procedere a uno scambio di opinioni sulle finalità e sulle condizioni del trattamento dei dati che rappresenterebbero al meglio gli interessi dei propri membri in relazione ai loro dati, o di negoziare i termini e le condizioni per il trattamento dei dati per conto dei membri prima di concedere l'autorizzazione al trattamento dei dati non personali o prima che essi diano il loro consenso al trattamento dei dati personali».

Il *considerando* n. 31, poi, contribuisce all'inquadramento dell'istituto, precisando che le cooperative di dati mirano «in particolare a rafforzare la posizione dei singoli individui, affinché compiano scelte informate prima di acconsentire all'utilizzo dei dati, influenzando i termini e le condizioni, stabiliti dalle organizzazioni di utenti dei dati, cui è subordinato l'utilizzo dei dati, in modo da offrire scelte migliori ai singoli membri del gruppo, o trovando possibili soluzioni alle posizioni contrastanti dei singoli membri di un gruppo in merito alle modalità di utilizzo dei dati laddove tali dati riguardino più interessati all'interno di tale gruppo. In tale contesto è importante riconoscere che i diritti a norma del Reg. (UE) 2016/679 so-

---

[33] Sono, tuttavia, esclusi almeno i seguenti servizi: «a) servizi che ottengono dati dai titolari dei dati e li aggregano, arricchiscono o trasformano al fine di aggiungervi un valore sostanziale e concedono licenze per l'utilizzo dei dati risultanti agli utenti dei dati, senza instaurare un rapporto commerciale tra i titolari dei dati e gli utenti dei dati; b) servizi il cui obiettivo principale è l'intermediazione di contenuti protetti da diritto d'autore; c) servizi utilizzati esclusivamente da un titolare dei dati per consentire l'utilizzo dei dati detenuti da tale titolare dei dati, oppure utilizzati da varie persone giuridiche all'interno di un gruppo chiuso, anche nel quadro di rapporti con i fornitori o i clienti o di collaborazioni contrattualmente stabilite, in particolare quelli aventi come obiettivo principale quello di garantire la funzionalità di oggetti o dispositivi connessi all'internet delle cose; d) servizi di condivisione dei dati offerti da enti pubblici che non mirano a instaurare rapporti commerciali» (art. 2, par. 1, n. 11).

[34] Il DGA annovera come esempi di servizi di intermediazione dei dati «i mercati dei dati su cui le imprese possono mettere dati a disposizione di terzi, gli orchestratori di ecosistemi di condivisione dei dati aperti a tutte le parti interessate, ad esempio nel contesto degli spazi comuni europei di dati, nonché i pool di dati creati congiuntamente da più persone fisiche o giuridiche con l'intento di concedere licenze per il loro uso a tutte le parti interessate in modo che tutti i partecipanti che contribuiscono al pool siano ricompensati per il loro contributo» (*considerando* n. 28).

no diritti personali dell'interessato e che quest'ultimo non può rinunciarvi. Le cooperative di dati potrebbero altresì rappresentare uno strumento utile per imprese individuali e PMI che, in termini di conoscenze in materia di condivisione dei dati, sono spesso equiparabili ai singoli individui».

In attesa del consolidamento applicativo della disciplina, pare ricavarsi che le cooperative di dati siano organizzazioni – la cui forma giuridica non viene espressamente predeterminata [35] – partecipate da interessati, imprese individuali o PMI, che presentano come obiettivi fondamentali, da un lato, il rafforzamento della posizione individuale dei singoli membri, riuniti in un soggetto collettivo, dall'altro, lo sviluppo di un metodo democratico di confronto tra i membri della cooperativa sulle modalità di massimizzazione dell'interesse comune con riguardo al patrimonio dei dati.

La nozione di cooperative di dati solleva, però, questioni interpretative rilevanti in merito al perimetro degli obblighi a cui sarebbero soggette le cooperative costituite da lavoratori della *gig economy*.

Una prima questione è se le cooperative della *gig economy*, per poter operare, debbano in ogni caso rispettare l'obbligo di notifica preventiva previsto dall'art. 11 [36] e soddisfare le condizioni per la fornitura di servizi di intermediazione dei dati stabilite dall'art. 12. Si tratta di una questione di non poco conto in quanto l'art. 14 istituisce un rigoroso sistema di monitoraggio della conformità, affidato alle autorità competenti per i servizi di intermediazione dei dati.

A tale primo quesito pare potersi fornire risposta negativa. Si ritiene che la coo-

---

[35] In merito all'estensione e ai limiti della forma soggettiva che può essere assunta dalle cooperative di dati si rinvia a F. BRAVO, *Le cooperative di dati*, cit., pp. 757-799.

[36] Ai sensi dell'art. 11, la notifica all'autorità competente per i servizi di intermediazione dei dati autorizza a fornire servizi di intermediazione dei dati in tutti gli Stati membri. La notifica deve contenere le seguenti informazioni: «a) il nome del fornitore di servizi di intermediazione dei dati; b) lo status giuridico, la forma giuridica, l'assetto proprietario, le pertinenti società controllate e, qualora il fornitore di servizi di intermediazione dei dati sia registrato nel registro delle imprese o in un altro registro pubblico nazionale analogo, il numero di registrazione del fornitore di servizi di intermediazione dei dati; c) l'indirizzo dell'eventuale stabilimento principale del fornitore di servizi di intermediazione dei dati nell'Unione e, se opportuno, di eventuali sedi secondarie in un altro Stato membro o l'indirizzo del rappresentante legale; d) un sito web pubblico in cui sono reperibili informazioni complete e aggiornate sul fornitore di servizi di intermediazione dei dati e sulle sue attività, comprese almeno le informazioni di cui alle lettere a), b), c) e f); e) le persone di contatto e i recapiti del fornitore di servizi di intermediazione dei dati; f) una descrizione del servizio di intermediazione dei dati che il fornitore di servizi di intermediazione dei dati intende fornire e un'indicazione delle categorie elencate all'articolo 10 in cui rientra tale servizio di intermediazione dei dati; g) la data prevista di inizio dell'attività, se diversa dalla data della notifica» (par. 6).

A sua volta, l'autorità competente notifica senza ritardo, per via elettronica, ogni nuova notifica alla Commissione, la quale tiene e aggiorna regolarmente un registro pubblico di tutti i fornitori di servizi di intermediazione dei dati che forniscono i loro servizi nell'Unione.

Deve essere altresì notificata ogni eventuale modifica delle informazioni fornite e la cessazione dell'attività, in modo che l'autorità competente possa informare la Commissione, la quale aggiorna di conseguenza il registro pubblico.

perativa sia tenuta a procedere alla notifica e a soddisfare le condizioni stabilite dal DGA solamente qualora intenda svolgere in favore dei propri membri appositi servizi di cooperative di dati, così come definiti dal regolamento [37].

A questo punto, però, sorgono ulteriori questioni su come debbano essere interpretati alcuni requisiti previsti dall'art. 12 con riguardo alle cooperative di dati della *gig economy*, intese nel modo appena chiarito. In particolare, si ritengono problematiche le condizioni imposte dall'art. 12, par. 1, lett. a) e c), le quali, *prima facie*, sembrerebbero impedire alle *data cooperatives* di utilizzare i dati oggetto di condivisione per offrire ai lavoratori-membri servizi ulteriori rispetto a quello di intermediazione dei dati [38]. È vero che il DGA fa salva la possibilità di offrire «servizi supplementari specifici ai titolari dei dati o agli interessati», ma viene altresì precisato, in senso restrittivo, che i servizi aggiuntivi devono avere «lo scopo specifico di facilitare lo scambio dei dati, come la conservazione temporanea, la cura, la conversione, l'anonimizzazione e la pseudonimizzazione» (art. 12, par. 1, lett. e).

Un'interpretazione rigorosa dei predetti criteri pare condurre a conseguenze del tutto irragionevoli. A titolo di esempio, una *data cooperative* che concluda accordi commerciali con enti pubblici per la condivisione dei dati prodotti dai *riders* al fine di migliorare le *policy* su viabilità e sviluppo urbano non potrebbe utilizzare i medesimi dati per sviluppare servizi in favore dei ciclofattorini, come l'individuazione di fasce orarie, percorsi e modalità di remunerazione più redditizi.

Appaiono, quindi, condivisibili le argomentazioni dottrinali che, in via inter-

---

[37] G. Guerini, presidente di CECOP Europa (confederazione europea delle cooperative lavoro industriali e di servizio), commentando la proposta del DGA, rileva in senso critico che «il riferimento alle "data cooperatives" sembra darne una declinazione prevalentemente orientata come "agenzia specializzata" sulla gestione cooperativa dei dati. Mentre andrebbe riconosciuta non solo la possibilità di creare cooperative per la gestione dei dati, ma anche la possibilità di permettere alle cooperative già esistenti di agire come gestori dei dati dei propri membri e associati. Aggiungendo al contenuto caratteristico dello scambio mutualistico di ogni cooperativa (di consumo, di utenza, bancaria, di servizio ecc.) di introdurre la "mutualità dei dati" che i soci conferiscono alla cooperativa, ma mantenendo appunto una "sovranità" su quegli stessi dati. Sarebbe per altro un primo nucleo per istituire quella forma di riconoscimento del diritto alla proprietà dei dati in un modo digitalizzato, che sempre più vive nella "info-sfera" (Floridi)». Cfr. G. GUERINI, *Mutualizzare i dati, per una via cooperativa alla sovranità digitale per imprese e persone*, 15 marzo 2021, reperibile al link: https://www.techeconomy2030.it/2021/03/15/mutualizzare-i-dati-per-una-via-cooperativa-alla-sovranita-digitale-per-imprese-e-persone/.

[38] Ai sensi della lett. a), «il fornitore di servizi di intermediazione dei dati non utilizza i dati per i quali fornisce servizi di intermediazione dei dati per scopi diversi dalla messa a disposizione di tali dati agli utenti dei dati». Invece, a norma della lett. c) «i dati raccolti su qualsiasi attività di una persona fisica o giuridica ai fini della fornitura del servizio di intermediazione dei dati, compresi la data, l'ora e i dati di geolocalizzazione, la durata dell'attività e i collegamenti con altre persone fisiche o giuridiche stabiliti dalla persona che utilizza il servizio di intermediazione dei dati, sono utilizzati solo per lo sviluppo di tale servizio di intermediazione dei dati, il che può comportare l'uso di dati per l'individuazione di frodi o a fini di cibersicurezza e sono messi a disposizione dei titolari dei dati su richiesta».

pretativa, ritengono applicabili le restrizioni all'utilizzo dei dati alle sole società di intermediazione non mutualistiche [39]. Peraltro, i servizi di valorizzazione dei dati (diversi da quelli di intermediazione dei dati in senso proprio) predisposti in favore dei membri sembrano costituire nient'altro che trattamenti dei dati personali dei lavoratori-membri svolti dalla cooperativa-datore di lavoro, rientranti nell'egida regolativa del GDPR, il quale viene espressamente fatto salvo dal *considerando* n. 4.

Un altro profilo meritevole di chiarimento riguarda la necessità o meno per le cooperative di *gig workers* di costituire una persona giuridica distinta per svolgere i servizi di intermediazione dei dati. Tale necessità sembrerebbe ricavarsi dall'art. 12, par. 1, lett. a), a mente del quale «il fornitore di servizi di intermediazione dei dati (…) fornisce servizi di intermediazione dei dati attraverso una persona giuridica distinta». Risulta, infatti, «necessaria una separazione strutturale tra il servizio di intermediazione dei dati e qualsiasi altro servizio fornito, in modo tale da evitare conflitti di interessi. Ciò significa che il servizio di intermediazione dei dati dovrebbe essere fornito mediante una persona giuridica distinta dalle altre attività di tale fornitore di servizi di intermediazione dei dati» (*considerando* n. 33).

La *ratio* della separazione tra enti sembra essere quella di evitare conflitti di interessi che potrebbero compromettere la neutralità dell'intermediario dei dati. Tale rischio, tuttavia, non pare ravvisabile in capo alle cooperative che svolgono attività di organizzazione della prestazione dei propri membri-lavoratori. Infatti, come è stato rilevato, «l'utilizzo del modello cooperativo per la condivisione dei dati offre la possibilità di superare il "conflitto di interessi" tra la proprietà dei dati da parte di un gestore che fornisce servizi e l'utente che genera i dati. Questo poiché la proprietà cooperativa da parte degli utenti-soci crea una "co-ownership" (comproprietà) democratica e mutualistica dei dati» [40]. In considerazione di ciò, le cooperative della *gig economy* potrebbero non essere tenute a costituire una persona giuridica separata per svolgere servizi di intermediazione dei dati.

Risulterebbe, tuttavia, utile una conferma, in sede europea o nazionale, dell'interpretazione proposta, anche in considerazione del fatto che gli oneri connessi alla "duplicazione" delle persone giuridiche potrebbero disincentivare la fornitura dei servizi di intermediazione da parte delle cooperative di *gig workers*, così precludendo alle stesse significative opportunità di valorizzazione, anche economica, dei dati.

---

[39] F. BRAVO, *Le cooperative di dati*, cit., pp. 757-799. Secondo l'Autore, «non ha senso che i dati raccolti dai soci possano andare solamente a beneficio di altri soggetti, nella logica dello svolgimento del servizio di intermediazione, e non possano invece essere utilizzati dalla cooperativa medesima, a proprio vantaggio e, dunque, a vantaggio anche dei soggetti che, nelle forme della cooperativa, partecipano ad essa nelle logiche mutualistiche e solidaristiche».

[40] G. GUERINI, *Mutualizzare i dati, per una via cooperativa alla sovranità digitale per imprese e persone*, cit.

4. (*segue*) Le cooperative di dati come nuovo paradigma per la valorizzazione dei dati nella *gig economy*: cornice teorica e applicazioni pratiche.

Le cooperative di dati sembrano poter rafforzare il *platform cooperativism*, alternativa al *platform capitalism* teorizzata nel 2014 dallo studioso e attivista statunitense Trebor Scholz [41]. Tale movimento mira a costruire un modello economico democratico basato sulla condivisione della proprietà delle piattaforme digitali e dei profitti ingenerati tramite le stesse. Nel contesto della *gig economy*, ciò si traduce nello sviluppo di piattaforme che promuovono la partecipazione, il confronto attivo e condizioni di lavoro eque per i soci-lavoratori. Il corporativismo di piattaforma persegue una strategia diversa rispetto alla promozione di interventi normativi diretti a migliorare le condizioni dei lavoratori delle piattaforme capitaliste, mirando, invece, alla creazione di modelli di impresa "neomutualistici" antitetici rispetto a quelli adottati dagli attori economici che dominano il mercato delle piattaforme [42], assumendo caratteristiche simili a quelle formazioni sindacali che trovavano il proprio *humus* nel cooperativismo.

---

[41] T. SCHOLZ, *Il cooperativismo di piattaforma. La sfida al sistema della sharing economy delle multinazionali*, tradotto a cura di Alleanza Cooperative Italiane, reperibile al seguente link: https://www.alleanzacooperative.it/uffici-studi/wp-content/uploads/2016/07/Il-Cooperativismo-di-piattaforma-v1.pdf.

Lo studioso ha elaborato dieci princìpi funzionali a riportare il senso di equità del lavoro nelle piattaforme lavorative: 1) condivisione della proprietà; 2) salario dignitoso e sicurezza del reddito; 3) trasparenza e portabilità dei dati; 4) apprezzamento e riconoscimento dei lavoratori; 5) lavoro co-determinato e coinvolgimento dei lavoratori sin dal momento della progettazione della piattaforma di lavoro; 6) inquadramento legale protettivo; 7) sussidi e protezioni portatili dei lavoratori; 8) protezione contro comportamenti arbitrari come l'esclusione dalla piattaforma; 9) rifiuto di eccessivo controllo sul posto di lavoro; 10) diritto alla disconnessione digitale.

Si segnalano altresì i contributi di T. CHRISTIAENS, *Platform cooperativism and freedom as non-domination in the gig economy*, in *European Journal of Political Theory*, 2024 e di D.J. BUNDERS-M. ARETS-K. FRENKEN-T. DE MOON, *The feasibility of platform cooperatives in the gig economy*, in *Journal of Co-operative Organization and Management*, 2022, Vol. 1, Issue 1.

[42] S. CAROLI, *Gig economy, rider, piattaforme, cooperazione e prime norme: le nuove regole sono già antiche*, in *Bollettino ADAPT*, 17 luglio 2018, n. 27, ipotizza che le tutele nella *gig economy* potrebbero derivare non dal conflitto, ma dalla cooperazione attraverso lo sviluppo di piattaforme possedute, gestite, e controllate dai *platform worker* stessi come reazione alle promesse non mantenute della *sharing economy* e ai tentativi delle piattaforme di comportarsi come un datore di lavoro fordista.

F. MARTINELLI, *Platform cooperativism: la cooperativa conta più della piattaforma*, 12 gennaio 2024, reperibile al link https://www.vita.it/platform-cooperativism-la-cooperativa-conta-piu-della-piattaforma/#_ftnref11, evidenzia alcune possibili criticità del cooperativismo di piattaforma, tra cui la necessità di competere con le grandi piattaforme (che potrebbero sostenere un minore costo del lavoro), la necessità di assicurare, tramite una appropriata struttura organizzativa, che la cooperativa sia effettivamente governata dai lavoratori e la necessità di spirito imprenditoriale da parte dei lavoratori. A tal proposito, viene riportato che uno dei motivi del fallimento di *Food4Me*, la prima cooperativa di *rider* fondata in Italia nel 2019 con il supporto di CISL Verona e Confcooperative, è stata la difficoltà

Lo sviluppo delle *platform cooperatives* potrebbe incidere profondamente sulle modalità di utilizzazione dei dati dei lavoratori, consentendo ai *platform workers* di partecipare alle decisioni sull'utilizzo dei dati da parte dell'algoritmo della piattaforma [43]. In questo modo, i lavoratori avrebbero una conoscenza approfondita sulle modalità di funzionamento dell'algoritmo e su come elabora i loro dati. La trasparenza algoritmica che il legislatore nazionale ed europeo sta cercando difficoltosamente di far emergere sarebbe, quindi, una caratteristica connaturata all'assetto proprietario e decisionale della piattaforma cooperativa.

Inoltre, non solo verrebbe elisa l'asimmetria informativa che connota le piattaforme non cooperative, ma i soci-lavoratori avrebbero anche la possibilità di "negoziare l'algoritmo". Tale prerogativa è assente nelle piattaforme tradizionali in cui le modalità di funzionamento dell'algoritmo che organizza la prestazione sono decise unilateralmente dai proprietari della piattaforma. Per tale ragione, in dottrina è stata auspicata l'introduzione in capo alle piattaforme di un obbligo di "negoziazione collettiva dell'algoritmo" con le parti sociali [44]. In questo modo, il sindacato potrebbe codeter-

---

dei *riders*, che venivano da altre esperienze con le multinazionali, ad accettare la responsabilità di gestire un'impresa (https://www.veronasera.it/economia/food4me-prima-cooperative-riders-verona-2-novembre-2019.html).

D.J. BUNDERS-M. ARETS-K. FRENKEN-T. DE MOON, *The feasibility of platform cooperatives in the gig economy*, cit., rilevano che le piattaforme cooperative della *gig economy* devono affrontare «*the challenges of raising capital, organising collective decision-making among heterogeneous workers, and finding support*». Secondo gli Autori, «*at present, platform co-ops may be particularly feasible for taxi drivers and for professionals, while the platform co-op model looks much more challenging in other sectoral contexts*». In merito a benefici e sfide del *platform cooperativism* cfr. European Agency for Safety and Health at Work (EU-OSHA), *Digital Plaform work: the Benefits of Platform Cooperativism*, 24 ottobre 2024.

[43] Il rapporto mondiale dell'Organizzazione Internazionale del Lavoro (OIL), *Prospettive occupazionali e sociali nel mondo lavoro. Il ruolo delle piattaforme digitali nella trasformazione del mondo del lavoro*, Ufficio Internazionale del lavoro, Ginevra, 2021, p. 95, riporta che «accanto alle piattaforme di lavoro digitali, si sta sviluppando un'altra tipologia di piattaforma, la "piattaforma cooperativa", che è finanziata ed è di proprietà della collettività. Le piattaforme cooperative, intese come piattaforme di proprietà collettiva, hanno guadagnato popolarità nell'ultimo decennio. Esse sono progettate e possedute dai loro membri, che di solito utilizzano una piccola quota dei loro guadagni per il mantenimento e lo sviluppo della piattaforma. Le piattaforme cooperative sono più trasparenti e responsabili nei confronti dei loro membri rispetto alle piattaforme di lavoro digitali. A differenza di queste ultime, in cui molte attività sono gestite tramite gli algoritmi, nelle piattaforme cooperative il lavoro è codeterminato e le decisioni sono assunte sulla base di processi democratici partecipativi. Esistono attualmente diverse piattaforme cooperative che operano in diversi settori, dai servizi di taxi (Green Taxi Cooperative e ATX co-op Taxi negli Stati Uniti e Eva in Canada) e di consegna (Coopcycle) alle pulizie a domicilio (Up&Go a New York) e all'e-commerce (Fairmondo in Germania). La loro filosofia è quella di creare una vera e propria economia di "condivisione", basata su pratiche di lavoro eque. Per esempio, Eva è una cooperativa che permette ai soci (autisti, riders e lavoratori) di far parte della cooperativa. Gli autisti guadagnano circa il 15 per cento in più rispetto ad altre piattaforme di taxi presenti nella regione».

[44] V. DE STEFANO, *"Negotiating the algorithm": Automation, artificial intelligence and labour*

minare le modalità con cui vengono trattati i dati dei lavoratori delle piattaforme, ricercando soluzioni dirette a minimizzare le informazioni raccolte, garantirne la cancellazione dopo un periodo temporale limitato e assicurarsi che non possano essere utilizzate impropriamente [45]. Nelle piattaforme cooperative, invece, gli stessi lavoratori avrebbero la possibilità di «decidere cosa deve/non deve, può/non può, fare l'algoritmo che governa la piattaforma» [46], anche avvalendosi del sostegno sindacale.

---

protection, Organizzazione Internazionale del Lavoro (OIL), in *Employment Policy Department, Working Paper* n. 246, 2018, 23, secondo il quale «*collective bargaining can play a primary role both at the sectoral and at the workplace level. Collective agreements could address the use of digital technology, data collection and algorithms that direct and discipline the workforce, ensuring transparency, social sustainability and compliance with these practices with regulation. Collective negotiation would also prove pivotal in implementing the "human-incommand" approach at the workplace … All this would also be consistent with collective bargaining's fundamental function as an enabling right and as a rationalisation mechanism for the exercise of employers' managerial prerogatives, allowing moving away from a purely unilateral dimension of work governance. "Negotiating the algorithm" could, therefore, become a crucial objective of social dialogue and action for employers' and workers' organization*».

S. BAIOCCO-E. FERNANDEZ MACÍAS-U. RANI-A. PESOLE, *The Algorithmic Management of work and its implications in different contexts*, cit., p. 26, ritengono che «*codetermination in the definition of the use of algorithms at work can help rebalancing the negotiating power between workers and employers by preventing abuse of contractual disparities and shield workers from unfair employment terms imposed by a party with a significantly stronger bargaining position*».

Nel contesto nazionale, v., tra gli altri, A. PIZZOFERRATO, *Tecnologie digitali, poteri datoriali e diritti dei lavoratori*, in A. BELLAVISTA-R. SANTUCCI, cit., p. 240, il quale afferma che «al fine di tutelare appieno i diritti e gli interessi dei lavoratori, non sembra sufficiente cercare di mitigare *ex post* gli effetti negativi derivanti dall'impiego di algoritmi e forme di intelligenza artificiale, essendo al contrario indispensabile negoziare *ex ante* l'algoritmo stesso. In altre parole, si rende indispensabile definire in maniera condivisa le finalità, la logica e i parametri di funzionamento dei sistemi». Tuttavia, per una efficiente negoziazione collettiva dell'algoritmo, occorre che il sindacato accresca le proprie competenze tecnologiche e/o faccia ricorso a «figure dotate delle competenze indispensabili per negoziare l'algoritmo».

[45] La negoziazione dell'algoritmo potrebbe riguardare anche aspetti ulteriori rispetto all'impiego dei dati dei lavoratori. Ad esempio, le parti sociali potrebbero controllare che gli algoritmi che assegnano il lavoro non mettano eccessivamente sotto pressione i *platform workers*, accrescendo i rischi per la loro salute e sicurezza, richiedendo che sia garantito un "margine di tolleranza" crescente per il completamento delle attività all'aumentare dell'orario di lavoro. Infatti, l'algoritmo dovrebbe tenere conto che, con il trascorrere del tempo, diminuiscono le energie psico-fisiche e la concentrazione e, di conseguenza, dovrebbe aumentare il tempo stimato per portare a termine le attività. Il sindacato, ancora, potrebbe pretendere che l'algoritmo sia adattato per far fronte alle necessità di lavoratori con esigenze particolari, quali lavoratori idonei con limitazioni al lavoro o affetti da disabilità, con un approccio preventivo che tenga in considerazione tali esigenze fin dal momento della progettazione (*accountability by design*). Infatti, modificare successivamente l'algoritmo potrebbe essere tecnologicamente difficile o eccessivamente oneroso.

[46] S. CAROLI, *Gig economy, rider, piattaforme, cooperazione e prime norme: le nuove regole sono già antiche*, cit., p. 2. Nello stesso senso, D.J. BUNDERS-M. ARETS-K. FRENKEN-T. DE MOON, *The feasibility of platform cooperatives in the gig economy*, cit., rilevano come «*members of a platform co-op can democratically determine … provisions concerning the algorithm, privacy, and access*».

Le piattaforme cooperative, assumendo il ruolo di cooperative di dati, potrebbero sfruttare le potenzialità insite nella disciplina del DGA. Tali soggetti, infatti, potrebbero procedere sia alla valorizzazione interna dei dati, impiegandoli per offrire servizi ai soci-lavoratori [47], sia alla valorizzazione esterna, promuovendone la condivisione e la diffusione in un contesto organizzativo in cui le decisioni sono partecipate.

Si ritiene, però, che lo sviluppo delle *data cooperatives* nel contesto lavoristico non dipenderà soltanto dalla capacità di sindacati, movimenti corporativisti e singoli lavoratori di cogliere le opportunità offerte dal DGA, ma anche dalla predisposizione di un quadro favorevole al neocorporativismo digitale da parte delle istituzioni, nazionali ed europee.

Secondo lo studio *Digital Platform Work: the Benefits of Platform Cooperativism*, cit., p. 5, «*many platform coops take pride in the transparent and accountable use of algorithmic tools and in ethical data policies, unlike their corporate counterparts. At the same time, in contrast with corporate businesses in the digital economy, platform coops are less likely to be able to afford to pay for expensive software technologies or to hire engineers and computer scientists to develop these technologies internally and to run them*».

[47] Come detto nel paragrafo precedente, pur ritenendo opportuna una chiarificazione espressa da parte delle istituzioni, si aderisce all'interpretazione per cui nel caso di fornitura del servizio di intermediazione di dati in forma cooperativa «risulta ammissibile l'utilizzo dei dati da parte della cooperativa medesima, nell'ottica della sua operatività secondo logiche mutualistiche» (F. BRAVO, *Le cooperative di dati*, cit., pp. 757-799).

Capitolo V

La tutela dell'interessato nell'economia dei dati: il ruolo delle cooperative di dati

Annarita Ricci-Alessandra Spangaro[*]

Abstract: The paper analyzes the data subject's rights in a context that has widely changed since the Regulation (EU) 2016/679, that it was focused on the personal data protection. Now the European Data Strategy aims to make the EU a leader in a data-driven society. It will create a single market for data where data can flow within the EU and across sectors, for the benefit of all. This objective requires the strengthening of the data subject's rights, providing tools and skills to maximize control of personal data. Within this framework, the purpose of this paper is to analyze the measures, recognized by the Data Governance Act and by the Data Act, that are needed to guarantee this very relevant goal.

1. Lo scenario europeo e il mutamento dell'assetto valoriale.

Lo scenario normativo europeo in ambito digitale è venuto rapidamente ad evolversi in un lasso relativamente breve di tempo, come d'altronde si conviene alla natura del tema trattato. Se, in origine, la materia in esame finiva sostanzialmente per esaurirsi nella tutela dei dati personali, all'epoca trattati in una logica essenzialmente proprietaria e dunque protezionistica [1], oggi lo spettro di azione del Legi-

---

[*] Premesso che lo scritto è il risultato di una riflessione condivisa tra le due autrici, i parr. 1, 5 e 6 sono da attribuirsi ad Alessandra Spangaro, i parr. 2, 3 e 4 sono da attribuirsi ad Annarita Ricci.

[1] F. BRAVO, *Cooperative di dati*, in *Contratto e impresa*, 2023, 3, p. 757 ss., *project version* reperibile in *https://site.unibo.it/cooperative-di-dati/it/attivita-di-ricerca/pubblicazioni*.

slatore comunitario è molto più ampio, molto più stringente per gli Stati membri – come reso evidente dall'adozione dello strumento regolamentare, non esposto a possibili modifiche da parte degli Stati membri, al contrario di quanto avviene con le direttive – e denota un significativo mutamento di prospettiva, espressamente dichiarato nel discorso sullo Stato dell'Unione già nel 2020, dalla Presidente della Commissione Europea, Ursula Von der Leyen, rilevando che «è in gioco la sovranità digitale dell'Europa, sia su piccola che su larga scala», conseguentemente «l'Europa è determinata a utilizzare questa transizione [digitale] per costruire il mondo in cui vogliamo vivere, anche al di là dei nostri confini».

Già con il Regolamento (UE) n. 679 del 2016 (di seguito, anche più semplicemente «GDPR»), d'altronde, si inaugurò una sorta di "logica espansiva" della sovranità europea sui dati, grazie alla previsione secondo la quale il regolamento medesimo può trovare applicazione anche ai trattamenti che non siano effettuati nell'Unione, purché svolti «nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione» (art. 3); l'ampiezza del concetto di "stabilimento" – che, ai sensi del cons. 22 richiede semplicemente «l'effettivo e reale svolgimento di attività nel quadro di un'organizzazione stabile», a prescindere dal tipo di forma giuridica assunta (succursale o filiale dotata di personalità giuridica) – ha poi definitivamente allargato i confini applicativi della normativa [2], nell'ottica espansiva su richiamata.

Il fine ultimo della strategia europea è dunque non solo predisporre una disciplina comune [3] a tutti gli Stati membri, ma, in una prospettiva più ampia e sicuramente più impegnativa, altresì quello di offrire un paradigma normativo utile anche per Stati non europei; l'UE viene quindi a proporsi quale regolatore antesignano di temi che, nelle restanti parti del mondo (si tratta, infatti, di questioni inevitabilmente ed intrinsecamente *globali*), non hanno ancora trovato una idonea disciplina o perché manca totalmente una regolazione oppure perché la regolazione attuata si presenta incompatibile con i valori fondamentali cui il Legislatore europeo ritiene

[2] Il mutamento di prospettiva rispetto al passato emerge con nitore, ove si pensi che la normativa precedente era espressa in forma di direttiva – la c.d. "direttiva madre" in materia di tutela dei dati personali (Direttiva 95/46/CE) – e, conseguentemente, l'ambito territoriale di riferimento era all'epoca parametrato non tanto in ragione dei confini (o di "oltre i confini") della UE, quanto in relazione ai confini di interni di ciascuno Stato membro, in considerazione delle singole leggi nazionali di recepimento; così il relativo art. 4 CE – rubricato coerentemente "Diritto nazionale applicabile" – era teso solo a dirimere possibili contrasti tra le diverse leggi nazionali di recepimento.

[3] Pienamente ed effettivamente comune, di qui – come accennato nel testo – la scelta di utilizzare lo strumento regolamentare invece che la direttiva, posto che l'esperienza data dalla Direttiva 95/46/CE aveva dimostrato che, con l'adozione di ciascuna legge di recepimento nazionale, non si era riusciti a raggiungere l'obiettivo dell'uniformità intraeuropea. Così, significativamente, il cons. 9 del GDPR: «sebbene i suoi obiettivi e principi rimangano tuttora validi, la direttiva 95/46/CE non ha impedito la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica».

di non poter rinunciare [4] (sui quali si tornerà a breve). Nel contempo, detta strategia mira a sfuggire al rischio del c.d. "colonialismo digitale" [5], vale a dire al rischio di una insanabile subalternità dovuta allo stato di fatto che oggi vede la grandissima parte dei dati dei cittadini europei nelle mani dei c.d. "*Big5*" statunitensi.

Il valore fondamentale cui l'Unione ha più volte richiamato la propria azione, espressamente dichiarandolo irrinunciabile, è quello della tutela della persona; la disciplina in materia dunque è e resta antropocentrica, ma il Legislatore europeo è andato abbandonando la logica che inizialmente contraddistingueva la sua azione – che, vedendo nel dato personale una sorta di promanazione della persona, lo relegava all'ambito della incommerciabilità e incedibilità – poiché, nel corso del tempo, essa aveva palesato sempre più la propria finitezza, in special modo al cospetto di utilità, quali i dati, che sono facilmente riproducibili e non consumabili [6]. Il nuovo approccio europeo vuole allora promuovere una inedita possibilità di accesso, "utilizzo responsabile" [7] e condivisione – invece che di mera segregazione – dei dati; «l'UE dovrebbe creare un contesto politico attraente, cosicché entro il 2030 la quota dell'UE dell'economia dei dati (dati conservati, elaborati e utilizzati proficuamente in Europa) corrisponda almeno al suo peso economico, non per imposizione ma per scelta. L'obiettivo è creare uno spazio unico europeo di dati – un autentico mercato unico di dati, aperto ai dati provenienti da tutto il mondo – nel quale sia i dati personali sia quelli non personali, compresi i dati commerciali sensibili, siano sicuri e le imprese abbiano facilmente accesso a una quantità pressoché infinita di dati industriali di elevata qualità, che stimolino la crescita e creino valore» [8]. Se, quindi, di *mercato unico* deve trattarsi, si rendono allora necessari dei pilastri comuni, offerti oggi dal *Data Governance Act* (di seguito, anche più semplicemente «DGA»), pur tenendo sempre ferma la visione antropocentrica, alla quale si è fatto cenno, che vede nel GDPR una delle sue esplicazioni di maggior rilievo. Tali pilastri si innestano nelle tre direttrici poste dal DGA: i servizi di intermediazione, il riutilizzo e l'altruismo dei dati, dati che possono essere, in ciascun frangente, sia personali che non personali [9].

---

[4] G. FINOCCHIARO, *Data and Digital Sovereignty*, in *ERDAL*, *European. Review of Digital Administration & Law*, 2022, 3, p. 9 ss., la quale evidenzia come l'Europa non voglia (e non possa) competere con gli Stati Uniti e la Cina in termini di produzione tecnologica, quanto quale *rulemaker*.

[5] In questi termini si esprime L. PETRONE, *Il mercato digitale europeo e le cooperative di dati*, in *Contratto e impresa*, 2023, 3, p. 800 ss.

[6] «I dati, a differenza della maggior parte delle risorse economiche, possono essere copiati pressoché a costo zero»: così la Comunicazione della Commissione europea del 26 febbraio 2020, reperibile in *https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52020DC0066*.

[7] *Ibidem*.

[8] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, denominata Una strategia europea per i dati", del 19 febbraio 2020, reperibile in *https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52020DC0066*.

[9] Al riguardo per tutti esaustivamente: D. POLETTI, *Il controllo dell'interessato e la strategia eu-*

Nell'economia del presente lavoro sarà possibile soffermarsi solo sul primo dei tre pilastri, vale a dire sui servizi di intermediazione, che vogliono affiancare e coadiuvare l'interessato nell'esercizio dei proprio diritti; ma non può non farsi almeno un cenno all'ultimo profilo indicato, che appare assolutamente rimarchevole: il Legislatore europeo nel DGA ha dato un substrato comune ai dati che abbiano natura personale e non personale, posto che spesso questi ultimi sono portatori di informazioni tanto interessanti (anche in un'ottica di mercato), quanto quelle rivelate dai primi. Ciò appare in modo nitido ove si pensi al c.d. "internet delle cose" (IoT) [10], concetto che va a compendiare qualsiasi tipo di oggetto che registra, salva e comunica informazioni circa l'utilizzo che di esso viene fatto. Tale comunicazione tra oggetti, dalla funzione varia ed eterogenea, moltiplica le possibilità di "interlavoro" tra i medesimi e così offre nuove utilità [11]; se ne fa già uso massivo nella domotica [12], ma rientrano in tale ambito, per esempio, anche gli oggetti *quantified self*, progettati per rilevare e registrare alcune abitudini di vita (es. le ore di sonno) ed applicazioni riferibili al concetto di *smart cities*, per il trasporto intelligente, la regolamentazione del traffico [13], tutti dati – alcuni dal carattere personale, altri invece non personali – la condivisione volontaria (e non remunerata) dei quali va certamente in direzione del soddisfacimento di interessi generali, alla base del c.d. "altruismo dei dati".

Nel nuovo scenario su tratteggiato, pur per brevi cenni, si è allora indotti a riflettere sulla posizione dell'interessato, i diritti del quale rimangono inalterati nella loro formulazione come posta dal GDPR – posto che il DGA fa sempre salve le relative previsioni – ma la cui posizione sostanziale merita oggi una nuova attenzione.

---

ropea sui dati, in *Osservatorio sulle fonti*, 2, 2023, p. 371 e F. BRAVO, *Intermediazione di dati personali e servizi di* data sharing *dal GDPR al* Data Governance Act, in *Contratto e impresa/Europa*, 2021, 1, p. 199 ss.

[10] I cui profili di condivisione dei dati sono regolati nel *Data Act*, cfr. § 3.

[11] Ma anche "nuovi modelli di business", così G. D'ACQUISTO-M. NALDI, *Big Data e Privacy by design*, Torino, 2017, p. 20 ss.

[12] Si pensi, per esempio, all'impianto di riscaldamento che si accende automaticamente se percepisce una temperatura esterna inferiore a tot gradi, oppure ad una sveglia connessa ad un sito di previsioni meteo, che suona in anticipo rispetto all'orario usuale, quando si prevede pioggia e i trasporti sono quindi più lenti. Oggi, poi, tra gli oggetti interconnessi più rilevanti sono ovviamente da annoverare le automobili (al riguardo: E. AL MUREDEN, *Diritto dell'*automotive*. Dalla fabbrica alla strada tra regole, mercato, tecnologie e società*, Bologna, 2024 e E. AL MUREDEN-G. CALABRESI, *Driverless cars. Intelligenza artificiale e futuro della mobilità*, Bologna, 2021; M.C. GAETA, *La protezione dei dati personali nell'Internet of Things: l'esempio dei veicoli autonomi*, in *Dir. inf.*, 2018, p. 147), ma si stanno aprendo nuovi ambiti di applicazioni, ad esempio, nella c.d. "tecnologia indossabile": non solo *smart watch*, ma anche scarpe con sensori per rilevare i passi, il tipo di appoggio del piede ecc.

[13] Cfr. S. FARO-N. LETTIERI, Big data *e internet delle cose: opportunità, rischi e nuove esigenze di tutela per gli utenti della Rete*, in C. PERLINGIERI-L. RUGGIERI (a cura di), *Internet e diritto civile*, Napoli, 2015, p. 279 ss., spec. p. 287.

2. I diritti dell'interessato nella prospettiva protezionistica del Reg. UE n. 679 del 2016 (GDPR).

La formula «diritti dell'interessato» designa un complesso di prerogative che la legge attribuisce all'interessato rispetto al trattamento di dati personali che lo riguardano e che possono essere schematicamente ricondotti a tre concetti: l'accesso, l'intervento, l'opposizione. I diritti dell'interessato possono essere esercitati indipendentemente dalla prova di avere subìto un pregiudizio dal trattamento dei dati o di essere esposti anche solo al pericolo di un danno. Ai fini del loro esercizio, non sono previste specifiche formalità: l'interessato può agire direttamente nei confronti del titolare del trattamento. Se l'istanza non viene accolta, l'interessato può rivolgersi all'Autorità di controllo (nel nostro Paese, il Garante per la protezione dei dati personali) o all'Autorità giurisdizionale.

Particolarmente dettagliata è la disciplina dei diritti dell'interessato, contenuta nel capo III del GDPR, rubricato «Diritti dell'interessato» (artt. 15-23) e, a livello nazionale, nel capo III, rubricato «Disposizioni in materia di diritti dell'interessato» (artt. 2-*undecies*-2-*terdecies*) del Codice in materia di protezione dei dati personali [14].

All'interessato è riconosciuto il diritto di ottenere (dal titolare del trattamento) la conferma o meno dell'esistenza di un trattamento di dati personali a lui riferiti e, nel caso, di ottenere l'accesso ai dati personali ed in particolare, alle seguenti informazioni: le finalità del trattamento; le categorie di dati personali oggetto del trattamento; i destinatari o le categorie di destinatari a cui i dati personali sono stati (o saranno) comunicati; il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; l'origine dei dati personali, quando questi non sono stati raccolti presso l'interessato; l'esistenza del diritto di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento, nonché del diritto di opporsi al loro trattamento; il diritto di proporre reclamo a un'autorità di controllo; l'esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di questo trattamento per l'interessato.

Attraverso l'esercizio del diritto di accesso, l'interessato viene a conoscenza di quali (suoi) dati personali sono oggetto di trattamento, verifica la qualità dei dati personali trattati e la liceità del trattamento, esercita consapevolmente gli altri diritti riconosciutigli dalla legge. Si spiega così che l'esercizio del diritto di accesso sia garantito a prescindere dall'esistenza di una lesione, potenziale o effettiva, lamentata dall'interessato, essendo una prerogativa il cui riconoscimento ha una valenza

[14] Il legislatore italiano, all'atto di adeguamento della disciplina nazionale al Reg. (UE) 679/2016, ha scelto di rinviare alle norme europee che enunciano i diritti (articoli da 15 a 22 del Regolamento), regolamentando a livello interno le limitazioni all'esercizio dei diritti e l'ipotesi dei diritti riguardanti le persone decedute, dando così su quest'ultimo profilo continuità a quanto già previsto dall'art. 9, co. 3, del Codice (ora abrogato) e prima ancora dall'art. 13, co. 3, della l. n. 675 del 1996. Su questo profilo, v. *amplius sub* par. 5.

strumentale rispetto ai diritti di rettifica, integrazione, cancellazione e opposizione.

Chiedendo di correggere o completare le informazioni raccolte, l'interessato tutela l'interesse a che la rappresentazione della sua persona sia vera, completa ed aggiornata. A riguardo, è importante ribadire che queste considerazioni prescindono dal contenuto dell'informazione: non è necessario, invero, che l'informazione presenti un connotato denigratorio, assumendo rilievo che la stessa, per il solo fatto di essere qualitativamente non corretta, è idonea a ledere l'identità della persona, nella complessità delle sue componenti.

Complementare al diritto di rettifica e di integrazione è il diritto dell'interessato di ottenere dal titolare del trattamento la cancellazione dei dati personali: una pretesa configurabile solo in presenza di determinate circostanze, oggetto di una tassativa elencazione [15].

Di pari porta limitata è il diritto dell'interessato alla limitazione del trattamento, consistente nel potere di imprimere sui dati un vincolo di indisponibilità e di inutilizzabilità. A seguito dell'esercizio del diritto di limitazione, i dati non sono cancellati, ma il loro trattamento ad opera del titolare si riduce alla sola operazione di conservazione. La relatività della pretesa, in questo caso, risulta ancor più evidente considerando che la limitazione del trattamento non opera automaticamente, essendo subordinata alla richiesta dell'interessato. Non è richiesto che l'interessato, nel proporre l'istanza di limitazione del trattamento, ne motivi le ragioni, ad esempio, l'inesattezza dei dati o la strumentalità degli stessi a fini probatori: spetterà, pertanto, al titolare dimostrare l'infondatezza della richiesta dell'interessato, provando l'insussistenza delle ipotesi tassativamente indicate dal Reg. (UE) n. 679 del 2016 [16].

L'interessato ha poi il diritto alla portabilità dei dati, ovvero il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati

---

[15] Secondo l'art. 17, par. 1 del Regolamento, il diritto di chiedere la cancellazione dei dati può essere esercitato al ricorrere di uno dei seguenti motivi: «*a)* i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; *b)* l'interessato revoca il consenso su cui si basa il trattamento e non sussiste altro fondamento giuridico per proseguire con il trattamento dei dati personali; *c)* l'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento effettuato per finalità di marketing diretto; *d)* i dati personali sono stati trattati illecitamente; *e)* i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento; *f)* i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione diretti a minori».

[16] L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento al ricorrere di una delle ipotesi indicate dall'art. 18, par. 1 del Regolamento e precipuamente quando: «*a)* l'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali; *b)* il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo; *c)* benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria; *d)* l'interessato si è opposto al trattamento (...), in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato».

personali che lo riguardano o di trasmettere tali dati a un altro titolare del trattamento. Un diritto che, come si avrà modo di rilevare nel prosieguo, è stato valorizzato dai più recenti interventi del Legislatore europeo.

Il Regolamento riconosce, infine, il diritto dell'interessato di opporsi al trattamento dei dati personali. In particolare, secondo quanto sancito dall'art. 21 par. 1, l'interessato ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, par. 1, lettere e) o f) [17], compresa la profilazione sulla base di tali disposizioni.

L'opposizione al trattamento dei dati personali costituisce una dichiarazione di volontà che produce l'effetto di interrompere in via definitiva il trattamento, salvo che il titolare dimostri l'esistenza di motivi legittimi che, prevalendo sugli interessi, sui diritti e sulle libertà dell'interessato, giustifichino la prosecuzione del trattamento. Allorché il trattamento sia effettuato per ragioni di marketing, il diritto di opposizione può essere esercitato dall'interessato in qualsiasi momento e senza la necessità di motivarne le ragioni.

Dall'impianto della disciplina sui diritti dell'interessato, qui sommariamente richiamato [18], si ricava che l'individuo ha in relazione alla circolazione di informazioni riferite alla sua persona la pretesa di esigere che il trattamento dei dati avvenga rispettando la sua dignità, evitando ingiustificate ingerenze nella sua sfera privata e garantendo il costante controllo sulle informazioni che devono rappresentarlo in modo veritiero [19]. Si potrebbe, a voler semplificare, affermare che i diritti dell'interessato consentono alla persona di invocare una più generale pretesa all'esatta rivelazione della propria identità. Non è casuale, sotto questo profilo, che la disciplina sui diritti dell'interessato sia collocata dopo le norme sui principi generali, dettanti regole cui tutti i titolari di trattamento devono conformarsi nella raccolta e nelle successive operazioni effettuate sui dati. La collocazione è invero coerente all'impianto di tutela: attraverso il riconoscimento dei diritti dell'interessato si dà attuazione ai principi di base che ispirano la disciplina in materia di trattamento dei dati personali, così da conformare le attività ai diritti e alle libertà fondamentali della persona [20].

---

[17] Così testualmente la norma: «Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore».

[18] Sia consentito per un approfondimento sul tema il rinvio a A. RICCI *I diritti dell'interessato*, in G. FINOCCHIARO (diretto da), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, 2019, p. 368 ss.

[19] S. RODOTÀ, *Tra diritti fondamentali ed elasticità della normativa: il nuovo Codice sulla Privacy*, in *Eur. dir. priv*., 2001, p. 2 ss. e più di recente, v. G. FINOCCHIARO, *Identità personale su Internet: il diritto alla contestualizzazione dell'informazione*, in *Dir. inform. e informatica*, 2012, 3, p. 383 ss.

[20] La tesi è confermata dall'*European Data Protection Supervisor* nelle «*Guidelines on the Rights of Individuals with regard to the Processing of Personal Data*» (consultabili in *https://www.secure.*

I principi generali sono dettati dall'art. 5 del Regolamento e sono sintetizzabili nei principi di liceità, correttezza e trasparenza del trattamento, di finalità del trattamento, di esattezza dei dati trattati, di pertinenza e non eccedenza dei dati rispetto alle finalità della raccolta, nonché nei principi relativi alla completezza, all'aggiornamento e alla contestualizzazione dei dati trattati. Per quel che rileva in questa sede e rinviando per i necessari approfondimenti alla letteratura consolidatasi in argomento [21], i principi di liceità e di correttezza impongono che il trattamento sia conforme alla legge e che siano adottate modalità di trattamento dei dati rispettose dei diritti e delle libertà dell'interessato [22]. Il principio di finalità impone che il trattamento e i dati che ne sono oggetto siano strumentali a scopi individuati ed espliciti. Secondo i principi di adeguatezza, pertinenza e non eccedenza devono essere trattati i soli dati necessari al perseguimento delle finalità dichiarate. La "necessità" va riferita ai dati oggetto di trattamento e ai requisiti ad essi intrinseci; essa non coincide con la "necessità" del trattamento in sé considerato, da intendersi come uno dei presupposti per la sua liceità. La "necessità" rappresenta, in altri termini, un criterio selettivo delle tipologie di dati personali da incorporare negli strumenti e nelle concrete modalità di attuazione delle diverse fasi del trattamento, dalla raccolta alla conservazione. Il principio di esattezza impone al titolare di verificare, all'atto della raccolta e nelle successive fasi del trattamento, che i dati personali siano corretti e aggiornati e conseguentemente, di adottare «tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati». Risulta evidente che l'esattezza, che deve essere garantita a priori, a prescindere cioè dall'intervento dell'interessato, si pone a tutela della sua identità personale, considerato che informazioni inesatte o parziali possono dare della persona una falsa rappresentazione.

L'obbligo di trattare, in modo lecito e corretto, esclusivamente i dati personali necessari, proporzionati, pertinenti e non eccedenti rispetto agli scopi per i quali i dati stessi sono stati raccolti segna i confini di liceità del trattamento. Accertato che

---

edps.europa.eu), in cui si legge: «*data subjects are safeguarded by a general right, which is that the EU institutions must process their personal data fairly and lawfully, and only for legitimate purposes (Articles 4 to 6 of the Regulation) (...). This general right is complemented by a number of specific rights of the data subject, including the right to be informed stipulated in Section 4 of the Regulation*».

[21] V., tra i volumi monografici, oltre al già citato, G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, *passim*, V. CUFFARO-R. D'ORAZIO-V. RICCIUTO, *I dati personali nel diritto europeo*, Torino, 2019, *passim*.

[22] Secondo E. NAVARRETTA, sub *art. 11*, in C.M. BIANCA-D. BUSNELLI (a cura di), *La protezione dei dati personali: commentario al D.lgs. 30 giugno 2003, n. 196, Codice della privacy*, Padova, 2007, p. 251, la differenza tra liceità e correttezza consiste nel fatto che la liceità definisce a priori le condizioni di legittimità della condotta (nel caso di specie, il trattamento di dati personali), mentre la correttezza si declina in un sindacato a posteriori sulla condotta posta in essere. Più precisamente, anche la regola della correttezza è imposta a priori, ma le specifiche regole che la concretizzano sono affidate alla discrezionalità dell'agente (nel caso di specie, il titolare del trattamento) e solo a posteriori sono valutabili in termini di conformità o difformità al diritto.

i dati non sono più necessari al raggiungimento delle finalità perseguite, ovvero che queste sono irraggiungibili, la ragione che giustifica il trattamento viene meno, i dati devono essere cancellati, distrutti o trasformati in forma anonima e il diritto alla protezione dei dati personali "riacquista la sua assolutezza".

I principi generali individuano inoltre la durata massima del trattamento. Raggiunto lo scopo originario per il quale i dati personali sono stati raccolti, questi devono essere cancellati o trasformati in forma anonima. È quanto sancito dall'art. 5, par. 1, lett. e), secondo cui i dati personali, oggetto di trattamento, devono essere conservati in una forma che consenta l'identificazione dell'interessato per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati. Onde assicurare che i dati personali non siano conservati più a lungo del necessario, è necessario che il titolare del trattamento sottoponga i dati ad un esame periodico, così da verificarne la persistente necessità di trattamento. Se i dati personali, raggiunta la finalità per la quale sono stati raccolti, continuano ad essere conservati, il confine di legittimità è oltrepassato e l'interessato può pretenderne la cancellazione.

I principi generali sin qui ricordati rappresentano regole strumentali a garantire che il trattamento dei dati personali avvenga nel rispetto del diritto della persona di avere e mantenere il controllo sulle informazioni che la riguardano, trattandosi di componenti della sua identità, unica e irripetibile. Si potrebbe altrimenti dire che nella prospettiva del Regolamento europeo n. 679 del 2016, il trattamento dei dati, ancorché coessenziale al funzionamento della vita economico e sociale dei Paesi membri, è al servizio della persona: il trattamento dei dati personali è il presupposto della disciplina, la tutela della persona e la protezione della sua identità il suo scopo. Dal che consegue che la relazione giuridica, ivi descritta, è essenzialmente binaria, intercorrendo tra l'interessato che vanta dei diritti e il titolare del trattamento che, in quanto soggetto che assume la decisione di trattare i dati, è sottoposto ad una complessa serie di obblighi e responsabilità.

Una descrizione, quella sin qui tracciata, che per quanto aderente al dettato normativo corrisponde nella società attuale, in cui i dati rappresentano una risorsa essenziale del mercato, ad una fotografia oramai ingiallita.

3. L'interessato e le sue diverse "vesti" nel quadro attuale.

La fotografia è ingiallita velocemente perché velocemente è mutato il bisogno sociale, di pari passo con l'inarrestabile progresso tecnologico, e così l'assetto valoriale di riferimento. I dati, al di là se di natura personale, si sono oggettivizzativi, divenendo beni in senso giuridico, cose che possono formare oggetto di diritti, individuali e collettivi, e che possono creare nuovi beni. I dati possono invero mescolarsi fra loro, creando nuovi dati e nuovi contenuti informativi[23]. Lo sfruttamento

[23] Anche la giurisprudenza ha preso consapevolezza della possibile duplice natura dei dati: da un lato, componente della personalità su cui il soggetto cui i dati si riferiscono vanta un diritto all'auto-

di queste potenzialità richiede l'intervento dell'uomo, o comunque della macchina utilizzata dall'uomo, capace di valutare e scegliere i dati, collegarli tra loro, elaborarli, e originarne dei nuovi. Ne consegue che al bisogno di garantire, sin dalla progettazione del sistema di raccolta, la qualità e la sicurezza dei dati, si affianca quello di incentivarne lo sfruttamento.

La prospettiva del Legislatore europeo nell'approcciarsi al tema dell'utilizzo dei dati è così inevitabilmente mutata. Se fino a qualche decennio fa, l'attenzione è stata rivolta soprattutto, se non esclusivamente, a garantire la protezione dei dati personali, quali componenti di un diritto fondamentale della persona, a partire dall'ultimo decennio si è delineato un nuovo approccio volto a favorire la valorizzazione e la condivisione dei dati.

«I dati ridefiniranno il nostro modo di produrre, consumare e vivere, generando benefici percepibili in ogni singolo aspetto della nostra vita: da un consumo energetico più consapevole alla tracciabilità dei prodotti, dei materiali e degli alimenti, da una vita più sana a una migliore assistenza sanitaria. (…) I dati sono la linfa vitale dello sviluppo economico: sono la base di molti nuovi prodotti e servizi e generano guadagni in termini di produttività ed efficienza delle risorse in tutti i settori economici, rendendo possibili prodotti e servizi più personalizzati, un miglioramento del processo di elaborazione delle politiche e un potenziamento dei servizi pubblici. Sono inoltre una risorsa essenziale per le start-up e le piccole e medie imprese (…) per quanto concerne lo sviluppo di prodotti e servizi. La disponibilità di dati è essenziale per l'allenamento dei sistemi di intelligenza artificiale, con prodotti e servizi in rapida evoluzione, dal riconoscimento morfologico e *insight generation* a tecniche

---

determinazione e dall'altro, utilità patrimoniale, suscettibile di sfruttamento economico da parte di un soggetto terzo che la utilizza. Fra le più recenti, v. Cons. Stato, 29 marzo 2021, n. 2631 (pubblicata fra l'altro in *Foro it*., 2021, III, coll. 325) che ha confermato la pronuncia del T.A.R. Lazio 10 gennaio 2020, n. 260 (pubblicata fra l'altro in *Giur. it*., 2021, p. 320 ss., con nota di C. SOLINAS, *Circolazione dei dati personali, onerosità e pratiche commerciali scorrette*), particolarmente esplicita sul punto: «Le tesi di parte ricorrente presuppongono che l'unica tutela del dato personale sia quella rinvenibile nella sua accezione di diritto fondamentale dell'individuo, e per tale motivo Facebook era tenuta esclusivamente al corretto trattamento dei dati dell'utente ai fini dell'iscrizione e dell'utilizzo del *social network*. Tuttavia, tale approccio sconta una visione parziale delle potenzialità insite nello sfruttamento dei dati personali, che possono altresì costituire un *asset* disponibile in senso negoziale, suscettibile di sfruttamento economico e, quindi, idoneo ad assurgere alla funzione di "controprestazione" in senso tecnico di un contratto. A fronte della tutela del dato personale quale espressione di un diritto della personalità dell'individuo, e come tale soggetto a specifiche e non rinunciabili forme di protezione (…), sussiste pure un diverso campo di protezione del dato stesso, inteso quale possibile oggetto di una compravendita, posta in essere sia tra gli operatori del mercato che tra questi e i soggetti interessati. Il fenomeno della "patrimonializzazione" del dato personale, tipico delle nuove economie dei mercati digitali, impone agli operatori di rispettare, nelle relative transazioni commerciali, quegli obblighi di chiarezza, completezza e non ingannevolezza delle informazioni previsti dalla legislazione a protezione del consumatore, che deve essere reso edotto dello scambio di prestazioni che è sotteso alla adesione ad un contratto per la fruizione di un servizio, quale è quello di utilizzo di un *social network*».

di previsione più sofisticate e, di conseguenza, decisioni migliori. (…) Rendere disponibile un maggior numero di dati e migliorarne le modalità di utilizzo è inoltre fondamentale per far fronte alle sfide sociali, climatiche e ambientali, contribuendo allo sviluppo di società più sane, più prospere e più sostenibili». Con queste parole la Commissione europea, nella già richiamata comunicazione del 19 febbraio 2020, denominata «Una strategia europea dei dati», ha rivelato l'intento di creare un mercato e regolare uno spazio comune europeo dei dati. Muovendo dalla consapevolezza che i dati rappresentano una risorsa essenziale per la crescita economica, la competitività, l'innovazione, la creazione di posti di lavoro e il progresso sociale in generale, secondo la Commissione europea è necessario «creare uno spazio unico europeo di dati, nel quale sia i dati personali sia quelli non personali, compresi i dati commerciali sensibili, siano sicuri e le imprese abbiano facilmente accesso a una quantità pressoché infinita di dati industriali di elevata qualità, che stimolino la crescita e creino valore (…). Dovrebbe trattarsi di uno spazio nel quale il diritto dell'UE possa essere applicato con efficacia e nel quale tutti i prodotti e i servizi basati sui dati siano conformi alle pertinenti normative del mercato unico dell'Unione europea. Quest'ultima dovrebbe a tal fine combinare una legislazione e una *governance* idonee allo scopo per garantire la disponibilità dei dati, investendo in norme, strumenti e infrastrutture, come pure in competenze per la gestione dei dati».

Norme europee comuni e meccanismi di applicazione efficaci che, secondo la Commissione europea, dovrebbero essere in grado di «garantire che i dati possano circolare all'interno dell'UE e a livello intersettoriale; le norme e i valori europei, in particolare la protezione dei dati personali, la legislazione in materia di tutela dei consumatori e il diritto della concorrenza, siano pienamente rispettati; le norme in materia di accesso ai dati e loro utilizzo siano eque, pratiche e chiare, e siano istituiti meccanismi chiari e affidabili di governance dei dati e, infine, che l'approccio ai flussi di dati internazionali sia aperto ma assertivo, basato sui valori europei».

Orbene, il compito di concretizzare e realizzare gli obiettivi delineati nella citata Comunicazione della Commissione europea è stato assegnato proprio al *Data Governance Act* e al *Data Act*: atti che dai commentatori sono qualificati come i due pilastri del sistema europeo di governo dei dati.

Il *Data Governance Act* è uno strumento intersettoriale che mira a garantire la disponibilità dei dati, disciplinando il riutilizzo dei dati pubblici, prevedendo un regime di notifica per i fornitori di servizi di condivisione dei dati ed incoraggiando il trattamento su base volontaria dei dati per finalità di pubblico interesse. L'obiettivo principale del *Data Act* è, invece, quello di regolare la circolazione dei dati generati dall'uso dei prodotti connessi e dei servizi correlati, attraverso la previsione di un complesso ordine di obblighi, destinato ad incidere sui rapporti tra imprese, sui rapporti tra imprese e consumatori e sui rapporti tra imprese ed enti pubblici e finalizzato ad agevolare l'accesso e l'utilizzo ai dati da parte dei diversi attori, soprattutto quelli più deboli, dell'economia digitale. I due atti si completano così a vicenda, rappresentando il *Data Act* lo strumento di attuazione, nel mercato dei servizi digitali, dei principi generali sanciti dal *Data Governance Act*.

Vasto è, in entrambi i casi, l'ambito di applicazione. Alla creazione e al conseguente sviluppo del mercato unico dei dati sono invero chiamati i soggetti pubblici, le imprese e i singoli. Tra questi soggetti il rapporto giuridico non si configura più solo come una relazione intercorrente tra *data controller* e *data subject*, in virtù della quale il primo tratta, sulla base di uno specifico presupposto di legittimità, i dati riferiti al secondo e deve perciò adempiere ad una serie di adempimenti finalizzati a garantire la qualità e la sicurezza dei dati medesimi, potendo coinvolgere più soggetti che rivestono ruoli diversi, in funzione di specifiche prerogative e competenze e che, in ragione di ciò, assumono autonome responsabilità.

Muta così anche la figura dell'interessato. Da soggetto, titolare della pretesa al controllo sui propri dati personali, pretesa vantabile nei confronti di chi questi dati li ha raccolti e li tratta per una specifica finalità, l'interessato diventa anche produttore di dati laddove, utilizzando beni e servizi, fornisce dati che, uniti ad altri dati, creano nuovi dati. Nel mercato dei dati l'interessato è produttore ma anche consumatore, cui sono riconosciuti i diritti connessi, mentre le imprese che operano al suo interno sono sottoposti ad una serie di obblighi finalizzati a garantire la trasparenza e l'accessibilità ai dati e ad evitare concentrazioni di potere economico che potrebbero avere effetti distorsivi della concorrenza, ostacolando l'equa distruzione del valore derivante dall'uso dei dati. In questo modo, per usare le parole di Poletti, «la normativa sulla protezione dei dati personali si intreccia con la disciplina consumeristica e con la disciplina sulle pratiche commerciali sleali, dando luogo ad una prospettiva di tutela multilivello» [24].

Ma c'è di più, atteso che risulta rafforzato il potere all'autodeterminazione informativa, essenza stessa del diritto al controllo sui propri dati personali. Il riferimento è alla possibilità, sancita dall'art. 2, n. 16 del *Data Governance Act* di donare i dati personali per finalità di interesse collettivo [25]. Potendo decidere di condividere i propri dati personali per un obiettivo di interesse generale, l'interessato da un lato diventa protagonista del mercato dei dati, dall'altro acquisisce una rinnovata consapevolezza del valore dei propri dati, assumendo un ruolo di cittadinanza attiva tramite il conferimento dei propri dati alla "funzione sociale".

---

[24] D. POLETTI, *Il controllo dell'interessato e la strategia europea sui dati*, cit., p. 371.

[25] Particolarmente suggestiva è la scelta lessicale del *Data Governance Act*. La norma citata evoca invero l'«altruismo» dei dati, definendolo come «la condivisione volontaria di dati sulla base del consenso accordato dagli interessati al trattamento dei dati personali che li riguardano, o sulle autorizzazioni di altri titolari dei dati volte a consentire l'uso dei loro dati non personali, senza la richiesta o la ricezione di un compenso che vada oltre la compensazione dei costi sostenuti per mettere a disposizione i propri dati, per obiettivi di interesse generale, stabiliti nel diritto nazionale, ove applicabile, quali l'assistenza sanitaria, la lotta ai cambiamenti climatici, il miglioramento della mobilità, l'agevolazione dell'elaborazione, della produzione e della divulgazione di statistiche ufficiali, il miglioramento della fornitura dei servizi pubblici, l'elaborazione delle politiche pubbliche o la ricerca scientifica nell'interesse generale».

4. (*segue*) L'effettività del diritto al controllo dei (propri) dati personali e i nuovi strumenti di garanzia.

In un contesto così descritto, si avverte ancora più forte il bisogno di garantire l'effettività della tutela dei diritti dell'interessato. Se come insegna Falzea, la ricerca della tutela effettiva «non incide sull'*an* della, ma solo sulle modalità di applicazione della protezione. Ciò significa che il rimedio non si sostituisce al diritto o all'obbligo sostanziale, ma intende fornire uno strumento di tutela adeguata, in presenza di violazioni di interessi e diritti, specie in presenza di forme complesse e fondamentali e di nuovi beni da tutelare» [26], il nuovo impianto regolatorio europeo sembra andare nella giusta direzione.

Da un lato, invero, il *Data Act* sancisce l'obbligo di rendere accessibili all'utente i dati del prodotto e dei servizi correlati. In particolare, l'art. 3 del *Data Act*, sulla falsariga del principio della *privacy by design* affermato dal GDPR, prevede che i prodotti connessi e i servizi correlati siano progettati, fabbricati e immessi sul mercato in modo tale che i dati di tali prodotti e servizi, compresi i metadati necessari a interpretare e utilizzare tali dati, siano, per impostazione predefinita, accessibili all'utente in modo facile, sicuro, gratuito, in un formato completo, strutturato, di uso comune e leggibile da dispositivo automatico e, ove pertinente e tecnicamente possibile, in modo diretto. L'utente cui la norma si riferisce è l'utilizzatore finale che, senza la previsione in capo al fornitore di uno specifico obbligo di condivisione, vedrebbe preclusa la possibilità di accedere ai dati generati dal dispositivo. Ulteriore è l'obbligo posto in capo al venditore, locatore o noleggiante del prodotto (che può, dice la norma, essere anche il fabbricante), di rendere edotto l'utente, prima della conclusione del contratto, del tipo, del formato e del volume stimato di dati che il prodotto può generare; se il prodotto è in grado di generare dati in modo continuo e in tempo reale; se il prodotto connesso è in grado di archiviare dati sul dispositivo o su un *server* remoto, compresa, se del caso, la durata prevista della conservazione; del modo in cui l'utente può accedere a tali dati, reperirli o, se del caso, cancellarli, compresi i mezzi tecnici per farlo, nonché le condizioni d'uso e la qualità del servizio. A ciò si aggiunge l'obbligo imposto al titolare dei dati di mettere a disposizione i dati, su richiesta dell'utente o di altra parte che agisca per suo conto, a soggetti terzi.

Dall'altro lato, il *Data Governance Act* offre un concreto apporto alla garanzia di effettività dei diritti in capo all'interessato, prevedendo tra i compiti attribuiti alla nuova figura degli intermediari dei dati, quello di supportare l'interessato nell'esercizio del diritto al controllo sui propri dati personali [27]. Come si legge nel con-

---

[26] A. FALZEA, *Gli interessi legittimi e le situazioni giuridiche soggettive*, in *Riv. dir. civ.*, 2000, p. 683. Imprescindibile è anche lo scritto di G. VETTORI, *L'attuazione del principio di effettività. Chi e come*, in *Riv. trim. dir. proc. civ.*, 2018, p. 939 ss.

[27] Secondo quanto previsto dall'art. 2, n. 11 del *Data Governance Act*, il "servizio di intermediazione dei dati" «mira a instaurare, attraverso strumenti tecnici, giuridici o di altro tipo, rapporti com-

siderando 30 del *Data Governance Act*, l'intento è quello di «rafforzare la capacità di agire degli interessati e, in particolare, il controllo dei singoli individui in merito ai dati che li riguardano, assistendoli nell'esercizio dei loro diritti. Tali fornitori assisterebbero i singoli individui nell'esercizio dei loro diritti a norma del Regolamento (UE) 2016/679, in particolare gestendone la concessione e la revoca del consenso al trattamento dei dati, il diritto all'accesso ai propri dati, il diritto alla rettifica dei dati personali inesatti, il diritto alla cancellazione (…), il diritto alla limitazione del trattamento e il diritto alla portabilità dei dati (…). In tale contesto, è importante che il modello commerciale di tali fornitori garantisca che non vi siano incentivi disallineati che incoraggino i singoli individui a utilizzare tali servizi per mettere a disposizione più dati che li riguardano di quanto non sia nel loro stesso interesse. Ciò potrebbe comprendere l'offerta di consulenza ai singoli individui quanto ai possibili utilizzi dei loro dati e il controllo della dovuta diligenza degli utenti dei dati prima che sia consentito loro di contattare gli interessati, al fine di evitare pratiche fraudolenti».

Ancora più eloquenti sono il successivo *considerando* n. 31 e l'art. 2, n. 15 del *Data Governance Act* che, nel prevedere la possibilità che i fornitori di servizi di intermediazione possano assumere la veste di cooperative di dati, stabilisce tra i loro obiettivi principali quelli di «aiutare i propri membri nell'esercizio dei loro diritti in relazione ai dati, anche per quanto riguarda il compiere scelte informate prima di acconsentire al trattamento dei dati, di procedere a uno scambio di opinioni sulle finalità e sulle condizioni del trattamento dei dati che rappresenterebbero al meglio gli interessi dei propri membri in relazione ai loro dati, o di negoziare i termini e le condizioni per il trattamento dei dati per conto dei membri prima di concedere l'autorizzazione al trattamento dei dati non personali o prima che essi diano il loro consenso al trattamento dei dati personali».

Nell'impianto del *Data Governance Act*, le cooperative dei dati mirano, più in generale, a sopperire alla asimmetria informativa e conseguentemente alla disparità negoziale, laddove si prevede che esse possono rappresentare utili strumenti anche per le imprese individuali e le piccole medio imprese che, «in termini di conoscenze in materia di condivisione dei dati, sono spesso equiparabili ai singoli individui»[28].

Da quanto sin qui ricostruito emerge la prospettiva di un rapporto gestorio, la cui particolarità è nell'oggetto: un diritto complesso in capo alla persona che, come tiene a ribadire il *Data Governance Act*, è un diritto fondamentale della persona, come tale irrinunciabile, ma al tempo stesso è un diritto che, nel contesto di riferimento, assume il connotato di interesse collettivo, la cui attuazione è necessaria per

---

merciali ai fini della condivisione dei dati tra un numero indeterminato di interessati e di titolari dei dati, da un lato, e gli utenti dei dati, dall'altro, anche al fine dell'esercizio dei diritti degli interessati in relazione ai dati personali (…)». In dottrina v. F. BRAVO, *Intermediazione di dati personali e servizi di* data sharing *dal GDPR al* Data Governance Act, cit., p. 199 ss. e D. POLETTI, *Gli intermediari dei dati*, in *European Journal of Privacy Law & Technologies*, 1, 2022, p. 45 ss.

[28] In questi termini il già più volte richiamato *considerando* n. 31 del *Data Governance Act*.

aumentare la fiducia nella condivisione dei dati personali e così allo sviluppo e al funzionamento del mercato unico europeo dei dati.

5. Le cooperative dei dati quali garanti dell'effettività del diritto al controllo dei (propri) dati personali. L'ipotesi emblematica del *mandato post mortem exequendum*.

La previsione secondo la quale, nell'ambito dei fornitori di servizi di intermediazione dei dati, vi possa essere una "categoria specifica" che rafforzi il «controllo dei singoli individui in merito ai dati che li riguardano» (*considerando* n. 30) e, ulteriormente, la possibilità di costituire cooperative di dati per «rafforzare la posizione dei singoli individui, affinché compiano scelte informate prima di acconsentire all'utilizzo dei dati, influenzando i termini e le condizioni, stabiliti dalle organizzazioni di utenti dei dati, cui è subordinato l'utilizzo dei dati, in modo da offrire scelte migliori ai singoli membri del gruppo» (*considerando* n. 31) evidenziano come, nell'impianto del DGA, si faccia un significativo affidamento sul ruolo di tale nuova figura, il cui ambito di azione appare di ampia portata. Ciò emerge, in primo luogo, da una lettura sinottica dell'attuale *considerando* n. 31 con la corrispondente previsione già contenuta nel *considerando* n. 24 della Proposta di Regolamento sulla *Governance* europea dei dati.

Nella versione provvisoria del testo era espressamente statuito che la cooperativa di dati, pur essendo chiamata al ruolo su delineato, non avrebbe potuto esercitare per conto dell'interessato i diritti a quest'ultimo riservato dal GDPR; più precisamente, il *considerando* n. 24 disponeva che nel contesto delle cooperative di dati «è importante riconoscere che i diritti norma del regolamento (UE) 2016/679 possono essere esercitati soltanto a titolo individuale e non possono essere conferiti o delegati in una cooperativa di dati». Ebbene questa limitazione è venuta meno nella versione definitiva della previsione, oggi contenuta come detto nel già richiamato *considerando* n. 31, nell'ambito del quale semplicemente si precisa che nel contesto delle cooperative di dati «è importante riconoscere che i diritti a norma del regolamento (UE) 2016/679 sono diritti personali dell'interessato e che quest'ultimo non può rinunciarvi». L'irrinunciabilità, quindi, evidentemente non comporta anche la non delegabilità dei diritti dell'interessato, finendo perciò per ammettere un rapporto fiduciario tra l'interessato e una cooperativa che gestisca i dati del primo.

Invero, l'istituto della fiducia era già in parte conosciuto all'ambito del trattamento dei dati personali grazie da una norma contenuta non nel GDPR, ma nel Codice *privacy* (come modificato dal d.lgs. n. 101 del 2018). Come noto, il Regolamento «non si applica ai dati personali delle persone decedute», ma «gli Stati membri possono prevedere norme riguardanti il trattamento dei dati personali delle persone decedute» (*considerando* n. 27 del GDPR); il legislatore italiano ha sfruttato la possibilità concessa dal GDPR inserendo nel Codice *privacy* l'art. 2-*terdecies*, che fa – come detto – un espresso riferimento al rapporto fiduciario laddove ammette

che «I diritti di cui agli articoli da 15 a 22 del Regolamento riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione».

Il rapporto fiduciario si declina qui nella specifica ipotesi del c.d. mandato *post mortem ad exequendum*, che si caratterizza per essere un contratto concluso *inter vivos*, in cui, tuttavia, le attività affidate al mandatario saranno attuate in un periodo successivo al decesso del mandante. Alla configurabilità dell'istituto non osta la previsione di cui all'art. 1722, n. 4, c.c., secondo la quale il mandato si estingue per morte del mandante o del mandatario, posto che si ritiene comunemente che essa sia derogabile [29]; come intuibile, ad ogni modo, per non confliggere con alcuni inderogabili principi successori [30], il mandatario può obbligarsi, ora per allora, alla esecuzione di meri atti materiali, tali da non incidere in alcun modo sui diritti degli eredi del mandante e, dunque, sulla partizione delle relative quote successorie. Proprio per evitare *in nuce* qualsiasi possibilità di conflitto con le regole successorie, si pretende, in via generale, che il mandatario sia chiamato ad eseguire esclusivamente atti a contenuto non patrimoniale [31], con la conseguenza per la quale la validità del mandato *post mortem* potrà essere determinata solo alla luce del tipo di attività che, in concreto, il mandatario sarà chiamato ad eseguire dopo la morte del mandante [32] e dovrà essere esclusa qualora, da tale analisi in concreto, emerga che *quel* patto tra mandante e mandatario debba ritenersi *mortis causa*.

Nell'ambito dei servizi della società dell'informazione, le esigenze che spesso sono alla base di un mandato *post mortem ad exequendum* sono state fino ad oggi assolte, in via generale, dalla funzione denominata "contatto erede", ove l'interessato conferisce al titolare (un *provider* di posta elettronica, un *social network* ecc.) l'incarico – da eseguire esclusivamente alla notizia del decesso dello stesso ovvero dopo un prolungato periodo di inattività dell'*account* dell'interessato medesimo –

---

[29] L. COVIELLO jr., *Il mandato* post mortem, in *Riv. dir. civ.*, 1930, 1; G. SICCHIERO, *Contratti* post mortem*, patti successori ed art. 28 L.N.*, in *Vita not.*, 2018, p. 557.

[30] L'ammissibilità di una simile fattispecie è stata invero a lungo messa in discussione dagli interpreti, in considerazione del potenziale conflitto con norme successorie non derogabili, quali, in particolare, il divieto di patti successori di cui all'art. 458 c.c. e la tutela dei legittimari, cfr. esaustivamente G. SICCHIERO, *Contratti* post mortem*, patti successori ed art. 28 L.N.*, cit., p. 557; S. DEPLANO, *La successione a causa di morte nel patrimonio digitale*, in C. PERLINGIERI-L. RUGGERI (a cura di), *Internet e diritto civile*, Napoli, 2015, p. 427 ss.; A. D'ARMINIO MONFORTE, *La successione nel patrimonio digitale*, Pisa, 2020, p. 27.

[31] L'ipotesi tipica richiamata in argomento è quella relativa al c.d. *ius eligendi sepulcrum*, sul quale cfr. G. BONILINI, *Una valida ipotesi di mandato* post mortem, in *Contr*., 2000, p. 1101; ID., *Il diritto al sepolcro*, in G. BONILINI (diretto da), *Tratt. dir. succ. e donazioni*, I, *La successione ereditaria*, Milano, 2009, p. 819; A. ANSALDO, *In tema di mandato* post mortem, in *Nuova giur. civ. comm.*, 2007, p. 496; G. MUSOLINO, *Il diritto di sepolcro: un diritto al plurale*, in *Riv. not.*, 2001, p. 471 ss.; ID., *Il diritto di sepolcro*, in *Riv. dir. civ*., 2009, p. 63 ss.

[32] G. CAPOZZI, *Successioni e donazioni*, I, Milano, 2015, p. 63.

di contattare la persona indicata da quest'ultimo per darle accesso ai propri contenuti. Tuttavia, nella prassi accade sovente che il *provider*, al contrario, non solo non conceda la possibilità della nomina di un contatto erede, ma ponga espressamente un veto alla trasmissibilità a terzi dei contenuti digitali dell'interessato, predisponendo apposite clausole di intrasmissibilità che vengono sottoscritte dall'utente/interessato (non sempre consapevolmente) al momento dell'apertura dell'*account*. Invero, la validità di tali clausole – idonee ad impedire l'accesso da parte dei congiunti del *de cuius* ai contenuti digitali del proprio congiunto premorto – è stata autorevolmente revocata in dubbio [33] e infatti, nelle non frequenti occasioni in cui la giurisprudenza ha avuto modo di pronunciarsi, ne ha esplicitamente decretato l'illegittimità, affermando che «L'accettazione delle condizioni generali di contratto da parte del defunto al momento dell'acquisto del dispositivo (nella specie, un telefono cellulare) non è idoneo a precludere l'accesso a dati personali in esso contenuti, non soddisfacendo la mera adesione alle condizioni generali di contratto i requisiti sostanziali e formali espressi dall'art. 2-*terdecies* del d.lgs. n. 101/2018, e dal Regolamento europeo sulla protezione dei dati personali 2016/679 UE. Ciò, anche in considerazione delle pratiche negoziali dei fornitori di servizi – nelle quali si radicano le condizioni generali di contratto con gli utenti – non valorizzanti l'autonomia delle scelte dei destinatari», ingiungendo conseguentemente alla società convenuta di prestare assistenza al ricorrente nelle operazioni di recupero dei dati dell'*account* del defunto [34], posto che detto accesso «può essere impedito soltanto in presenza di un espresso divieto, in forma scritta, proveniente dal medesimo interessato [35], e non può essere subordinato a ulteriori requisiti anche se, genericamente, richiamati nel regolamento contrattuale sotto posto all'approvazione del singolo utente, al fine dello sfruttamento del relativo servizio informatico» [36].

Il fatto che i grandi *provider* abbiano più volte cercato di impedire l'esercizio dei diritti enunciato nell'art. 2-*terdecies* palesa la posizione di debolezza dell'interessato, del suo mandatario o dei suoi familiari, i quali, per rimuovere questa opposizione, hanno dovuto attivare un procedimento giudiziario, assumendosi i relativi rischi e i relativi costi.

Questa situazione oggi può andarsi ad inserire nelle maglie e nell'ottica del DGA, con un radicale mutamento di prospettiva. La previsione dell'art. 2, n. 11 del DGA – ove vanno a confluire le riflessioni contenute nei considerando su citati – potrebbe

---

[33] S. DELLE MONACHE, *Successione mortis causa e patrimonio digitale*, in *Nuova giur. civ. comm.*, 2020, p. 460; C. CAMARDI, *L'eredità digitale tra reale e virtuale*, in *Dir. inf.*, 2018, p. 8; G. RESTA, *Dignità, persone, mercati*, Torino, 2014, p. 382.

[34] Trib. Roma, 10 febbraio 2022, in *Rivistapactum.it*.

[35] (…) ai sensi dell'art. 2 *terdecies*, co. 2, del Codice in materia di protezione dei dati personali. Cfr. G. RESTA, *Commento sub art. 2 terdecies*, in S. D'ORAZIO-G. FINOCCHIARO-O. POLLICINO-G. RESTA (a cura di), *Codice della privacy e data protection*, Milano, 2021.

[36] Trib. Milano, 10 febbraio 2021, in *Giur. it*., 2022, p. 1363 e sia consentito il rinvio alla relativa nota di A. SPANGARO, *La successione digitale: la permanenza* post mortem *di aspetti della personalità.*

infatti offrire una efficace soluzione alle problematiche che fino ad oggi si sono manifestate. Nell'ambito del «*servizio di intermediazione dei dati*», teso alla condivisione dei dati, che può operare «anche al fine dell'esercizio dei diritti degli interessati in relazione ai dati personali» (salve le quattro esclusioni successivamente precisate dalla medesima norma) si configura quindi la possibilità di un rapporto fiduciario tra l'interessato ed una cooperativa di dati in base al quale quest'ultima gestisca i diritti che il GDPR riserva al primo, nell'esclusivo interesse del primo ed, eventualmente, anche per il periodo successivo al decesso del medesimo, avendo come obiettivo principale – ai sensi dell'art. 2, n. 15 del DGA – «aiutare i propri membri nell'esercizio dei loro diritti in relazione a determinati dati, anche per quanto riguarda il compiere scelte informate (…) sulle condizioni del trattamento dei dati (…), o di negoziare i termini e le condizioni per il trattamento dei dati per conto dei membri» [37].

Si tratta, al momento, solo di una delle varie possibilità applicative della norma, che poi non potrà sfuggire ad una valutazione in concreto alla luce dei risultati che emergeranno dall'esperienza; ciò che tuttavia già oggi si può rilevare e che la tradizionale posizione di debolezza dell'interessato, dovuto alla sua singolarità a fronte dei grandi *provider*, potrà certamente andare a ridimensionarsi notevolmente proprio grazie alla struttura cooperativa a cui oggi l'interessato medesimo può accedere, così attenuando la sua posizione di monade. Potranno quindi venirsi a fondare cooperative di dati con il precipuo scopo fiduciario di gestire i dati degli interessati (eventualmente anche per il momento successivo al decesso degli stessi) che ne siano membri, conferendo loro quella forza tipica del gruppo che fino ad oggi era loro preclusa.

6. Osservazioni conclusive.

Con quanto riferito nei paragrafi precedenti si è cercato di evidenziare l'evoluzione della posizione dell'interessato nell'odierna economia dei dati; la strategia europea in materia e, in particolare, le analizzate norme del DGA offrono infatti la possibilità al medesimo di affrancarsi – almeno parzialmente – dalla posizione di debolezza legata al presentarsi come una singola molecola in un universo governato da pochi e mastodontici *Big*.

Una siffatta evoluzione, per come è stata enunciata e, al momento, regolata – pur essendo ancora priva di significativi riscontri pratici, essendo entrata in vigore in tempi molto recenti – appare la coerente estrinsecazione della già più volte richiamata strategia digitale europea e dell'ottica antropocentrica che la caratterizza, da ultimo solennemente declamata anche nella *Dichiarazione europea sui diritti e i principi digitali per il decennio digitale*, pronunciata congiuntamente dal Parlamen-

[37] Si noti che l'ipotesi del mandato *post mortem* non esaurisce certamente le possibilità di delega offerte oggi dal DGA, ma ne costituisce solo una possibile sicuramente interessante applicazione concreta, lo precisano esaustivamente: F. BRAVO, *Cooperative di dati*, cit., *project version*, p. 31 ss. e D. POLETTI, *Il controllo dell'interessato e la strategia europea sui dati*, cit., p. 373.

to, dal Consiglio e dalla Commissione [38], del gennaio 2023, ove, considerando, nel Preambolo, che «l'Unione europea è un'«unione di valori», sancita dall'articolo 2 del trattato sull'Unione europea, e si fonda sul rispetto della dignità umana» e, correlativamente, che «la trasformazione digitale interessa ogni aspetto della vita delle persone», presentando anche sfide significative «per le nostre società democratiche e le nostre economie, così come per gli individui (…)», si conclude che «è giunto il momento che l'UE specifichi come si dovrebbero applicare nell'ambiente digitale i suoi valori e diritti fondamentali applicabili *offline*». Ciò significa che l'UE ha assunto l'impegno di garantire che «i diritti riconosciuti nel mondo analogico siano rispettati anche nel mondo digitale», senza che possano esservi trattamenti divergenti solo in ragione del *medium* attraverso il quale tali diritti vengono esercitati.

In questo contesto, la *Dichiarazione* si prefigge, dunque, il fine di promuovere l'azione responsabile di tutti gli attori, pubblici e privati, della rete, ponendo la tecnologia a beneficio delle persone «in tutta sicurezza e nel pieno rispetto dei loro diritti fondamentali», esortando gli stessi operatori del mercato – che traggono significativi vantaggi dalla trasformazione digitale – ad assumersi le conseguenti responsabilità sociali, contribuendo – tra l'altro – ai costi delle infrastrutture, in modo tale da garantire l'accesso con una «connettività di elevata qualità» e a prezzi accessibili a «ogni persona, ovunque nell'UE» (cap. II). Nel capitolo dedicato all'*ambiente digitale equo* (cap. III), viene inoltre enunciato il principio secondo il quale «ogni persona dovrebbe essere in grado di scegliere realmente e liberamente quali servizi online utilizzare, sulla base di informazioni obiettive, trasparenti, facilmente accessibili e affidabili»; ebbene tale principio sembra trovare una significativa concreta attuazione proprio nel *Data Governance Act*, alla luce della funzione tipica del «*servizio di intermediazione dei dati*» offerto dalle cooperative di dati (dell'art. 2, nn. 11 e 15 del DGA) di cui si è già fatto cenno nel paragrafo precedente. E significativo appare anche il fatto che il cap. V dedichi una breve, ma specifica riflessione alla c.d. "*eredità digitale*", statuendo che «ogni persona dovrebbe essere in grado di determinare la propria eredità digitale e decidere cosa succede, dopo la sua morte, ai propri account personali e alle informazioni che la riguardano».

Se dunque questi sono i principi ai quali si ispira l'azione dell'UE, più e più volte enunciati, certamente oggi il *Data Governance Act* sembra offrire un più che utile e concreto strumento attuativo degli stessi e, più specificamente, dei diritti dell'interessato che – pur già chiaramente esplicitati in anni passati, in particolare nel Regolamento (UE) n. 679 del 2016 – avevano trovato più di un ostacolo sul loro percorso; con ciò non si vuole ovviamente affermare la risoluzione di ogni criticità, ma non può negarsi di essere di fronte ad uno strumento inedito e dalle ricche potenzialità.

[38] La Dichiarazione è consultabile sul sito istituzionale dell'Unione europea al *link*: *https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32023C0123(01*).

Capitolo VI

Mutualizzazione dei dati tra terzo settore, *Data Protection Law* e *Digital Service Act*

Giuliana Amore

Abstract: Data cooperatives have recently been introduced and regulated within the Data Governance Act (DGA, EU Reg. 868/2022), as providers of data intermediation services «intended to establish commercial relationships for the purposes of sharing of data between an indeterminate number of data subjects and data controllers, on the one hand, and data users, on the other, through technical, legal or other means (…)» (art. 2, no. 11, DGA). This is a discipline that is as innovative as it is incomplete. The work aims, on a legal level, at a systematic framework of the case in light of the multiple regulatory areas concerned and involved. In particular, we intend to refer to the Third Sector (Third Sector Code), the protection of personal data (General Data Protection Regulation or GDPR) and the new rules for online intermediaries (DSA). The data cooperative, in fact, presents itself as threefold: it is an entity that pursues solidarity purposes, it processes personal data and, finally, it is an intermediary for data services.

1. Premessa.

Le cooperative di dati sono state recentemente introdotte e disciplinate all'interno del *Data Governance Act* (DGA, Reg. UE n. 868/2022), quali fornitori di servizi di intermediazione di dati [1] «volt(*i*) a instaurare rapporti commerciali ai fini della

[1] Trattasi della gestione dei dati in forma cooperativa: una soluzione per tutelare dati di singoli e imprese, per condividere e distribuire equamente il valore aggiunto prodotto dall'uso dei dati, che oggi sono in mano a *corporation* e multinazionali fruttando loro enormi profitti. Si parla, al riguardo, di "neomutualismo digitale" (cfr. P. VENTURI-F. ZANDONAI, *Neomutualismo. Ridisegnare dal basso competitivi-*

condivisione dei dati tra un numero indeterminato di interessati e titolari dei dati, da un lato, e gli utenti dei dati, dall'altro, attraverso mezzi tecnici, legali o di altro tipo (…)» (art. 2, n. 11, DGA). Si tratta di una disciplina tanto innovativa quanto lacunosa, che richiede quindi, sul piano giuridico, un inquadramento sistematico della fattispecie alla luce dei molteplici ambiti normativi interessati e coinvolti [2].

Ci si intende in particolare riferire al Terzo settore (Codice del Terzo settore), alla protezione dei dati personali (*General Data Protection Regulation* o GDPR) e alle nuove regole per gli intermediari *on line* (DSA).

Procedendo con ordine, il *Digital Governance Act* (DGA) specificamente sottolinea come «la Commissione veda un forte potenziale nell'uso dei dati resi disponibili volontariamente dagli interessati o da altri titolari di dati senza chiedere una ricompensa (finanziaria), per scopi di interesse generale». Il *considerando* n. 15, poi, definisce i «servizi delle cooperative di dati (…) *come* servizi di intermediazione dei dati offerti da una struttura organizzativa costituita da interessati, imprese individuali o PMI membri di tale struttura, aventi come obiettivo principale quello di supportare i propri membri nell'esercizio dei loro diritti rispetto a determinati dati, anche per quanto riguarda l'effettuazione di scelte informate prima di acconsentire al trattamento dei dati, per scambiare opinioni sugli scopi e sulle condizioni

---

tà e welfare, Milano, 2022): le cooperative di dati aggregano dati dei soci (singoli o imprese) e li elaborano per creare valore, non solo monetario. Esse si basano su una logica non predatoria, ma di cooperazione. In ambito giuridico cfr. F. BRAVO, *Le cooperative di dati*, in *Contr. e impr.*, 2023, 1, pp. 757-799, e L. PETRONE, *Il mercato digitale europeo e le cooperative di dati*, in *Contr. e impr.*, 2023, 3, pp. 800-817 (entrambi anche in https://site.unibo.it/cooperative-di-dati); J. TAIT, *The Case for Data Cooperatives*, in https://thedataeconomylab.com/2021/09/06/the-casefor-data-cooperatives/; E. BIETTI-A. EXTBERRIA-M. MANNAN-J. WONG, *Data Cooperatives in Europe: A Legal and Empirical Investigation*, December 2021, in https://cyber.harvard.edu/sites/default/files/2022-02/Data_Cooperatives_Europe-group2.pdf; A. PENTLAND-T. HARDJONO-J. PENN-C. COLCLOUGH-B. DUCHARME-L. MANDEL, *Data Cooperatives: Digital Empowerment of Citizens and Workers*, in *MIT Connerction Science*, 1 February 2019, https://ide.mit.edu/sites/default/files/publications/Data-Cooperatives-final.pdf; T. HARDJONO-A. PENTLAND, *Data Cooperatives: Towards a Foundation for Decentralized Personal Data Management*, in *MIT Connection Science*, 15th May 2019, https://arxiv.org/pdf/1905.08819; sulle cooperative, in generale, cfr. *ex multis*, F. CASALE, *Scambio e mutualità nella società cooperativa*, in *Quaderni di Giurisprudenza Commerciale*, Milano, 2005; L.F. PAOLUCCI, *Le società cooperative*, Padova, 2014; F. VELLA-R. GENCO-P.L. MORARA, *Diritto delle società cooperative*, Bologna, 2018.

[2] Ciò si evince, in particolare, dal *considerando* n. 31 del Reg. UE n. 868/2022 (*Data Governance Act*, DGA) viene sottolineato che «le cooperative di dati mirano a raggiungere una serie di obiettivi, in particolare a rafforzare la posizione dei singoli individui, affinché compiano scelte informate prima di acconsentire all'utilizzo dei dati, influenzando i termini e le condizioni, stabiliti dalle organizzazioni di utenti dei dati, cui è subordinato l'utilizzo dei dati, in modo da offrire scelte migliori ai singoli membri del gruppo, o trovando possibili soluzioni alle posizioni contrastanti dei singoli membri di un gruppo in merito alle modalità di utilizzo dei dati là dove tali dati riguardino più interessati all'interno di tale gruppo. In tale contesto è importante riconoscere che i diritti a norma del reg. (UE) 2016/679 sono diritti personali dell'interessato e che quest'ultimo non può rinunciarvi. Le cooperative di dati potrebbero altresì rappresentare uno strumento utile per imprese individuali e PMI che, in termini di conoscenze in materia di condivisione dei dati, sono spesso equiparabili ai singoli individui».

del trattamento dei dati che rappresenterebbero al meglio gli interessi dei suoi membri in relazione ai loro dati e per negoziare termini e condizioni per i dati trattamento per conto dei propri iscritti prima di dare il consenso al trattamento dei dati non personali o prima che questi acconsentano al trattamento dei dati personali».

Orbene, se è vero che il concetto di "cooperativa di dati" non sia rigidamente determinato nel DGA e apra, quindi, la strada a forme soggettive diverse facendo generico riferimento a una organizzazione strutturata costituita dai "membri" che la compongono, da individuarsi nelle persone fisiche cui i dati si riferiscono («interessati», ai sensi del Reg. UE 679/2016), nelle imprese individuali o nelle piccole e medie imprese (PMI), è altrettanto vero come gli «obiettivi principali» solidaristici, variamente declinati, di supporto ai propri "membri" in relazione all'uso dei dati che verrà effettuato nella fornitura del servizio [3], facciano apparire la "società cooperativa" quale soggetto fisiologicamente più adatto per ricoprire il ruolo di "cooperativa di dati", nel nostro ordinamento e in quello europeo [4]. E, proprio alla luce di siffatti obiettivi solidaristici, il pensiero sembra correre, nel nostro ordinamento, altrettanto naturalmente, al d.lgs. n. 117/2017, contenente il c.d. Codice del Terzo settore (CTs), che, com'è noto, ha operato una vera e propria opera di «istituzionalizzazione» [5], ancora oggi in corso di attuazione e finalizzata a riorganizzare per l'appunto il settore degli enti senza scopo di lucro [6], favorendone la gestione e mi-

[3] Tra tali obiettivi, la definizione ne considera espressamente tre, menzionandoli in via alternativa e non (necessariamente) cumulativa, come ben si evince dalla disgiunzione «o» tra l'ultimo e il penultimo di essi. Segnatamente, si richiede che la predetta «struttura organizzativa» agisca al fine principale di: (i) aiutare i loro "membri" nel far valere le facoltà che l'ordinamento giuridico gli riconosce, favorendo l'acquisizione delle informazioni per l'esercizio dei diritti sui propri dati, in particolare qualora si tratti di dati personali; (ii) favorire un confronto interno tra i propri "membri", basato sullo «scambio di opinioni sulle finalità e sulle condizioni del trattamento dei dati»12, per rappresentare «al meglio gli interessi dei propri membri in relazione ai loro dati»; (iii) «(…) o negoziare i termini e le condizioni per il trattamento dei dati per conto dei membri (...)», ossia concordare con soggetti terzi, che utilizzeranno i dati, quali siano le condizioni giuridiche ed economiche volte a regolare i rapporti aventi ad oggetto l'uso di dati, personali e non personali, dei propri membri, persone fisiche o giuridiche.

[4] In tal senso, F. BRAVO, *Le cooperative di dati*, cit.

[5] Così, M. RISPOLI FARINA, *Il codice del Terzo settore tra novità e contraddizioni*, in D. DI SABATO-O. NOCERINO (a cura di), *Il Terzo settore profili critici della riforma*, Napoli, 2019, p. 3; già, G. PONZANELLI, *Quali regole giuridiche per il terzo settore?*, in *Riv. dir. civ.*, 3, 1996, p. 314, osserva come la crescita del *non profit* «conferm(i) il ruolo assolutamente trascurabile delle regole giuridiche sulla nascita e nella diffusione di nuovi fenomeni sociali». Sulla relazione fra le norme giuridiche ed il dinamismo naturale degli enti del Terzo settore, cfr. L. GORI-F. ZANDONAI, *I confini del Terzo settore: una mappa costantemente da riscrivere*, in *Impr. soc.*, 2018, pp. 11 ss.

[6] In tal senso, F. BOSETTI, *Il registro unico nazionale del terzo settore*, in M. GORGONI, *Il codice del terzo settore, Comm. al d. lgs. 3 luglio 2017 n. 117*, Pisa, 2021, p. 361, secondo il quale «il d. lgs. n. 117/2017, istituendo il Registro unico nazionale del Terzo settore, ha inteso dar corpo ai numerosi auspici che da tempo si formulavano, ispirati ad un'esigenza di riordino e di semplificazione di un sistema pubblicitario frammentario» oltreché disorganico: auspici che rappresentavano, in realtà, solo una parte della più ampia necessità di una riforma dell'intera disciplina del Terzo settore. Com'è noto,

gliorandone la trasparenza: un settore normativamente definito mediante un intreccio o combinazione di tre criteri e, precisamente, il perseguimento di finalità civiche, solidaristiche e di utilità sociale, lo svolgimento di attività riconosciute dal legislatore di interesse generale e, infine, una *governance* in grado di impedire la prevalenza di interessi prettamente privati su quelli di più ampio respiro. Ai sensi dell'art. 4 CTs, sono enti del terzo settore anche le "cooperative sociali" purché costituite per il perseguimento di finalità (oltreché civiche e di utilità sociale, anche, per l'appunto) solidaristiche mediante lo svolgimento – in via esclusiva o principale – di una o più attività di interesse generale «in forma di erogazione gratuita di […] beni o servizi, o di mutualità»: da qui, la possibile configurabilità delle cooperative di dati menzionate nel DGA come "cooperative sociali" di cui al Codice del Terzo settore.

In quanto "titolare del trattamento" di dati personali, poi, la cooperativa di dati sarà tenuta ad ottemperare agli obblighi *privacy* scaturenti dal Reg. UE n. 679/2016 (c.d. *GDPR*, *General Data Protection Regulation*) [7] svolgendo anche una sola delle operazioni che concretano un trattamento di dati personali [8], decidendo la finalità e le modalità del trattamento stesso. Ed invero, ai sensi dell'art. 4 GDPR, tali organizzazioni saranno "titolari di trattamento" ogniqualvolta effettuino qualunque operazione applicata a dati personali come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, o anche solo la comunicazione, diffusione, messa a disposizione o interconnessione di dati con qualunque mezzo, incluso quello digitale: sicché appare doveroso verificare presupposti, limiti e condizioni di operatività delle norme del GDPR per le cooperative di dati, coordinando, da un lato, i due Regolamenti UE (il *Data Governance Act* o DGA, volto alla creazione e/o al rafforzamen-

---

ai sensi dell'art. 4 CTS, sono enti del terzo settore le organizzazioni di volontariato, le associazioni di promozione sociale, gli enti filantropici, le imprese sociali, incluse le cooperative sociali, le reti associative, le società di mutuo soccorso, le associazioni, riconosciute o non riconosciute, le fondazioni e gli altri enti di carattere privato diversi dalle società costituiti per il perseguimento, senza scopo di lucro, di finalità civiche, solidaristiche e di utilità sociale mediante lo svolgimento, in via esclusiva o principale, di una o più attività di interesse generale in forma di azione volontaria o di erogazione gratuita di denaro, beni o servizi, o di mutualità o di produzione o scambio di beni o servizi, ed iscritti nel registro unico nazionale del Terzo settore. L. GORI, *Terzo settore e costituzione*, Torino, 2022, p. 1, sottolinea la difficoltà di coniare una definizione di «Terzo settore». Nella letteratura internazionale ha avuto successo la qualificazione del Terzo settore come "*a loose and baggy monster*", ad indicare l'estrema complessità di definire i confini di un complesso di enti, attività e relazioni che si colloca in una zona intermedia fra Stato e mercato. L'espressione è di J. KENDALL-M. KNAPP, *A Loose and Baggy Monster. Boundaries, Definition and Typologies*, Londra, 1995, p. 66 ss. Cfr. anche A. ETZIONI, *The Third Sector and Domestic Missions*, in *Public Administration Review*, 1973, p. 314 ss., che parla al riguardo di «una terza alternativa, in effetti un terzo settore, è cresciuta tra il settore statale e quello del mercato», tra pubblico e privato.

[7] Sulla protezione dei dati personali, cfr. *ex multis*, di recente, R. D'ORAZIO-G. FINOCCHIARO-D. POLLICINO-G. RESTA (a cura di), *Codice della* privacy *e* data protection, Milano, 2021.

[8] Sia i dati personali sia quelli non personali rientrano nell'ambito di applicazione del DGA ma, nel caso di dati personali, si applica il GDPR.

to di un mercato digitale unico europeo, incentrato sulla valorizzazione dei dati, personali e non personali e il *General Data Protection Regulation* o GDPR avente lo scopo di proteggere le persone fisiche dai rischi derivanti dal trattamento dei dati personali e connessi allo sviluppo del mercato e della tecnologia); e tenendo conto, dall'altro, del fatto che il *Data Governance Act* «non deve essere letto nel senso che crea una nuova base giuridica per il trattamento dei dati personali per alcuna delle attività regolamentate, né che modifica gli obblighi di informazione previsti dal Regolamento (UE) 2016/679» (*considerando* n. 4 DGA). Ciò, per non incorrere nelle pesanti sanzioni di cui al Reg. UE n. 679/2016 in caso di *data breach*, là dove la cooperativa di dati tratti per l'appunto dati personali.

Da ultimo, le riflessioni sulle cooperative di dati, in quanto fornitori di servizi di intermediazione di dati, non possono concludersi senza volgere lo sguardo al *Digital Service Act* (DSA) che, com'è noto, prevede obblighi di prevenzione e mitigazione in capo ai c.d. *Internet Service Providers* o ISPs, ossia prestatori di servizi intermediari *on line* o piattaforme *on line*, in parte a prescindere dalle loro dimensioni ed in parte esclusivamente a carico di piattaforme digitali di grandi dimensioni. Gli obblighi concernono, essenzialmente, misure volte a contrastare servizi o contenuti illegali *online* e a garantire la trasparenza e la tracciabilità degli utenti commerciali nei mercati *online*, contribuendo ad identificare venditori di merci illegali, strumenti di prevenzione e gestione del rischio di abusi dei sistemi per le piattaforme di grandi dimensioni e appositi codici di condotta che aiutino le piattaforme e gli altri attori a conformarsi alle nuove norme.

2. Le cooperative di dati come E.T.S.?

Ai sensi dell'art. 2, par. 1, n. 15, DGA, recante la definizione di «servizi di cooperativa di dati», i "servizi di intermediazione dei dati" possono essere svolti anche da una "cooperativa di dati", intesa come «(...) una struttura organizzativa costituita da interessati, imprese individuali o da PMI, che sono membri di tale struttura, avente come obiettivi principali quelli di aiutare i propri membri nell'esercizio dei loro diritti in relazione a determinati dati, anche per quanto riguarda il compiere scelte informate prima di acconsentire al trattamento dei dati, di procedere a uno scambio di opinioni sulle finalità e sulle condizioni del trattamento dei dati che rappresenterebbero al meglio gli interessi dei propri membri in relazione ai loro dati, o di negoziare i termini e le condizioni per il trattamento dei dati per conto dei membri prima di concedere l'autorizzazione al trattamento dei dati non personali o prima che essi diano il loro consenso al trattamento dei dati personali».

Al riguardo, è stato correttamente osservato [9] come l'ampia formula legislativa lasci fondatamente desumere che la fornitura di "servizi di cooperative di dati"

[9] Cfr. F. BRAVO, *Le cooperative di dati*, cit.

possa essere svolta, eventualmente, anche in forme diverse da quella societaria, benché la "società cooperativa" sia il soggetto fisiologicamente chiamato a ricoprire il ruolo di "cooperativa di dati", la «struttura organizzativa» per eccellenza finalizzata alla fornitura dei servizi di cooperative di dati: da qui, l'esigenza di individuare – con maggiore precisione – la declinazione più corretta tra quelle che il modello societario cooperativo offre e può assumere.

Al riguardo, non sembra peregrino muovere dalla recente riforma del Terzo Settore, che ha coinvolto anche le cooperative sociali: la novità più rilevante è rappresentata dall'ampliamento dei settori in cui esse possono operare. Più precisamente, proprio con l'approvazione del d.lgs. n. 112/2017, il tradizionale disposto dell'art. 1, lett. *a*) della l. n. 381/1991 è stato integrato fino a ricomprendere interventi e servizi sociali ai sensi dell'art. 1, co. 1 e 2, l. n. 328/2000 [10] e, in particolare, «tutte *quelle* attività relative alla predisposizione ed erogazione di servizi, gratuiti ed a pagamento, o di prestazioni economiche destinate a rimuovere e superare le situazioni di bisogno e di difficoltà che la persona umana incontra nel corso della sua vita, escluse soltanto quelle assicurate dal sistema previdenziale e da quello sanitario, nonché quelle assicurate in sede di amministrazione della giustizia».

Trattasi di una formula che, fatta eccezione per l'esclusione di specifiche attività ("assicurate dal sistema previdenziale, sanitario e in sede di amministrazione della giustizia"), potremmo qualificare "atipica" in quanto atta a definire un'attività come "sociale" anche in difetto di una puntuale menzione normativa, purché presenti i requisiti all'uopo previsti – in misura elastica, aperta e con le caratteristiche di una "clausola generale" – da siffatta norma e identificati nell'erogazione di servizi destinati genericamente a rimuovere e/o superare situazioni di bisogno e di difficoltà della persona umana. La portata elastica ed aperta dell'art. 1, l. n. 328/2000 non appare sminuita dalla presenza di singole fattispecie di "servizi sociali", menzionati qua e là dal legislatore, e sembra mantenere una sostanziale e preminente atipicità, nella misura in cui una qualunque attività può reputarsi "sociale" ove essa corrisponda alla "clausola generale di intervento sociale", spettando all'interprete il compito di valutare in concreto, caso per caso, tale corrispondenza in ragione della peculiare funzione svolta, nella specie, dalla cooperativa (di dati) e alla luce di un'interpretazione evolutiva dello stesso concetto di "attività sociale": ciò, com'è noto, al fine di adeguare la norma e il concetto di "attività e intervento sociale" all'evolversi della realtà attraverso un'interpretazione-applicazione più aderente alle esigenze sociali.

Orbene, come sottolineato nello stesso DGA, nel *considerando* n. 2, nell'ultimo decennio le tecnologie digitali hanno trasformato l'economia e la società, interessando tutti i settori di attività e la vita quotidiana. I dati sono al centro di questa trasformazione: per rendere l'economia basata sui dati inclusiva per tutti i cittadini dell'Unione, senza divari digitali, essa dovrebbe essere costruita in modo tale da

[10] Questa norma, a sua volta, fa rinvio all'art. 128, co. 2, d.lgs. n. 112/1998.

consentire alle imprese, in particolare alle micro, piccole e medie imprese (PMI), alle *start-up* di prosperare, garantendo la neutralità dell'accesso ai dati, la portabilità e l'interoperabilità dei dati ed evitando effetti di *lock-in*. La Commissione ha così proposto di istituire spazi europei comuni specifici per dominio per la condivisione e la messa in comune dei dati, ove i servizi di intermediazione dei dati – tra cui quelli esercitati dalle cooperative di dati – svolgeranno, per l'appunto, un ruolo chiave nell'economia dei dati, in particolare sostenendo e promuovendo pratiche di condivisione volontaria dei dati tra imprese o agevolando la condivisione dei dati nel contesto degli obblighi stabiliti dal diritto dell'Unione o nazionale. Tali intermediari aiuterebbero le persone (*data subjects*) a esercitare i propri diritti ai sensi del Reg. (UE) 2016/679, in particolare, a dare e revocare il proprio consenso al trattamento dei dati, il diritto di accesso ai propri dati, il diritto alla rettifica di dati personali inesatti, il diritto alla cancellazione o all'oblio, il diritto di limitazione di trattamento e diritto alla portabilità dei dati, che consente agli interessati di trasferire i propri dati personali da un titolare del trattamento all'altro. Più precisamente, le cooperative di dati – secondo il dettato normativo europeo – mirano a raggiungere una serie di obiettivi, come quello di rafforzare la posizione degli individui nel fare scelte informate prima di acconsentire all'uso dei dati, influenzando i termini e le condizioni delle organizzazioni degli utenti dei dati legate all'uso dei dati in modo da offrire scelte migliori ai singoli membri del gruppo o eventualmente trovare soluzioni alle posizioni contrastanti dei singoli membri di un gruppo su come i dati possono essere utilizzati là dove tali dati si riferiscono a diversi interessati all'interno di quel gruppo: obiettivi sostanzialmente e innegabilmente "sociali", perseguiti attraverso la predisposizione ed erogazione di servizi o di prestazioni economiche destinate a rimuovere e superare le situazioni di bisogno e di difficoltà che la persona umana (nella specie, *data subject*) incontra nel corso della sua vita. Ciò, conformemente alla definizione di "attività sociale" contenuta nell'art. 1, co. 1 e 2, l. n. 328/2000.

Ancora una volta, da un punto di vista storico-evolutivo, una tipologia di cooperativa si presenta, dunque, atta a risolvere problemi "collettivi" diversi, progressivamente emersi nel tessuto sociale. Si pensi, in passato, alle cooperative nate per ridurre la marginalità di alcune aree territoriali, o sopperire alla carenza di servizi sociali o ancora alla scarsa qualità e diversificazione dei servizi offerti dal pubblico, a superare il problema della fornitura di energia nei territori limitrofi e a prezzi non monopolistici [11] e ora, per l'appunto, a realizzare la condivisione dei dati tra un numero indeterminato di interessati e titolari dei dati, da un lato, e gli utenti dei dati, dall'altro, attraverso mezzi tecnici, legali o di altro tipo: una problematica collettiva diversa e peculiare, ma comunque nata dalla necessità di rigenerare il nuovo

[11] In tale contesto, si collocano altresì le c.d. cooperative di comunità, aventi come obiettivo primario quello di rispondere ai bisogni (anche eterogenei) della comunità: sull'argomento, cfr. in particolare, S. DEPEDRI-S. TURRI, *Dalla funzione sociale alla cooperativa di comunità: un caso studio per discutere sul flebile confine*, in *Riv. impr. sociale*, 2015, 5, p. 65 ss.

tessuto socio-economico e di offrire una pluralità di servizi alla comunità. Dinanzi a questa naturale evoluzione, la forma cooperativa "sociale" – per così dire funzionalmente "modernizzata" – potrebbe compiere i primi passi e giungere a definire e regolamentare la nuova formula di "attività sociale" imperniata sulla condivisione dei dati (personali e non). Le cooperative di dati si propongono, infatti, di migliorare il benessere, la qualità della vita e del lavoro delle persone coinvolte nel patto mutualistico, accrescere le forme di partecipazione e sviluppare le comunità in cui operano, con logiche solidaristiche, ben distanti dai tradizionali modelli capitalistici, in grado di produrre effetti benefici per gli *stakeholders* di riferimento [12].

In altri termini, nell'ottica sin qui delineata e in ossequio alla *ratio legis* del DGA, la cooperativa sociale appare, da un lato, lo strumento più adatto per realizzare gli obiettivi del legislatore europeo e sembra offrire, dall'altro, una più penetrante tutela per gli interessati (*data subjects*), per le imprese individuali e per le PMI, configurandosi come ente senza fine di lucro che opera per soddisfare bisogni collettivi e perseguire scopi sociali: "rimuovere" e/o "superare" situazioni di difficoltà, in cui "evolutivamente" la persona umana si è venuta a trovare.

A favore di siffatta ricostruzione, sembra sistematicamente militare tutto il DGA, innegabilmente e chiaramente ispirato – tra "cooperative" ed "organizzazioni per l'altruismo dei dati" (artt. 16 ss. DGA) – ad una logica non predatoria, bensì di cooperazione [13], solidarietà e altruismo per un'equa condivisione e distribuzione del valore aggiunto prodotto dall'uso dei dati, oggi in mano per lo più a *corporation* e multinazionali destinatarie di enormi profitti: un modello societario, per la prima volta espressamente riconosciuto quale servizio e strumento di intermediazione nel Reg. (UE) 2022/868, alternativo a quello marcatamente capitalistico, oggi imperante, attraverso il quale restituire centralità ai cittadini e contribuire a rendere la società e l'economia digitale più solidali e democratiche. In altri termini, la cooperativa sociale appare la «struttura organizzativa» migliore per lo svolgimento di servizi di intermediazione dei dati, in quanto caratterizzata da quella stessa visione antropocentrica che porta ad assicurare la tutela della persona e la solidarietà sociale, cui risulta orientato il modello di gestione dei dati, voluto dal legislatore europeo e che prende le distanze dallo schema di *business* perseguito dalle c.d. *Big Tech*, contraddistinto, all'opposto, dal c.d. capitalismo della sorveglianza [14].

---

[12] Così, ancora, F. BRAVO, *Le cooperative di dati*, cit.

[13] Si parla, al riguardo, di un nuovo tipo di mutualismo atto a contrastare lo strapotere delle multinazionali.

[14] S. ZUBOFF, *Il capitalismo della sorveglianza, il futuro dell'umanità nell'era dei nuovi poteri*, Roma, 2019, là dove con l'espressione "capitalismo della sorveglianza" si intende l'ordine economico che sfrutta l'esperienza umana come materia prima per pratiche commerciali segrete di estrazione, previsione e vendita, in una logica economica parassitaria volta a sovvertire la sovranità popolare. Sul punto, cfr. altresì, L. PETRONE, *Il mercato digitale europeo e le cooperative di dati*, cit.; G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati (La regolazione digitale nell'Unione europea)*, in *Riv. trim. dir. pubbl.*, 2022, 4, p. 971; D. POLETTI, *Gli intermediari di dati*, in *European Journal of Pri-*

3. Cooperative di dati e *Data Protection Law*.

Il *considerando* n. 35 dispone specificamente che «il presente regolamento (DGA) dovrebbe lasciare impregiudicato l'obbligo incombente sui fornitori di servizi di intermediazione dei dati di rispettare il Regolamento UE 2016/679 (GDPR)». Più precisamente, qualora una cooperativa di dati, fornendo servizi di intermediazione, tratti dati personali, il DGA non dovrebbe pregiudicare la protezione dei dati personali: essa, in quanto titolare o responsabile del trattamento dei dati come definiti nel Reg. (UE) 2016/679, sarà vincolata dalle norme di tale regolamento. I *considerando* nn. 4 e 7, poi, prescrivono rispettivamente che «il presente Regolamento (DGA) non deve essere letto nel senso che crea una nuova base giuridica per il trattamento dei dati personali per alcuna delle attività regolamentate, né che modifica gli obblighi di informazione previsti dal Regolamento (UE) 2016/679» (*considerando* n. 4) e che «per quanto riguarda i dati personali, il trattamento dei dati personali dovrebbe fondarsi su una o più delle basi giuridiche del trattamento previste dagli articoli 6 e 9 del Regolamento (UE) 2016/679»: da qui, la necessaria conformità dell'operato delle cooperative di dati al GDPR [15], ovviamente con specifico riferimento al trattamento dei dati personali.

E se l'art. 6 GDPR delinea, in generale, le basi giuridiche del trattamento, l'art. 9 integra e specifica tali basi nel caso in cui il trattamento abbia ad oggetto categorie "particolari" di dati personali, prevedendo specifiche prescrizioni, come quelle dettate – al terzo comma – per organismi di tipo associativo, fondazioni, o altro ente senza scopo di lucro (inclusa, nella specie, la cooperativa di dati) che tratti dati c.d. "particolari", o "sensibili" [16] secondo la vecchia etichetta: si pensi ai dati che rivelano le opinioni politiche, le convinzioni religiose o filosofiche,

---

vacy Law & Technologies, 2022, 1, pp. 45-56, consultabile al sito https://universitypress.unisob.na.it/ojs/index.php/ejplt/article/view/1623/1092; F. BRAVO, *Il commercio elettronico dei dati personali*, in T. PASQUINO-A. RIZZO-M. TESCARO (a cura di), *Questioni attuali in tema di commercio elettronico*, Napoli, 2020, p. 83 ss.

[15] In particolare, lo stesso DGA sottolinea come, in genere, l'altruismo dei dati si basi sul consenso degli interessati ai sensi dell'art. 6, par. 1, lett. *a*), e dell'art. 9, par. 2, lett. *a*), del Reg. (UE) 2016/679. Ai sensi del Reg. (UE) 2016/679, le finalità di ricerca scientifica potrebbero essere supportate dal consenso ad alcuni ambiti di ricerca scientifica ove conformi a *standard* etici riconosciuti per la ricerca scientifica oppure solo ad alcuni ambiti di ricerca o parti di progetti di ricerca. L'art. 5, par. 1, lett. *b*), del Reg. (UE) 2016/679 specifica che l'ulteriore trattamento a fini di ricerca scientifica o storica o a fini statistici dovrebbe, conformemente all'art. 89, par. 1, del Reg. (UE) 2016/679, non possono ritenersi incompatibili con le finalità iniziali. Per i dati non personali, le limitazioni all'utilizzo dovrebbero essere reperite nel consenso concesso dal titolare dei dati.

[16] Il GDPR contiene, all'art. 9, una definizione di «categorie particolari di dati personali», che comprendono: i dati che rivelano «l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale»; i dati biometrici e genetici atti ad identificare in modo univoco una persona fisica; dati sanitari (e cioè i dati relativi alla salute) o quelli relativi alla vita sessuale o all'orientamento sessuale della persona.

l'appartenenza sindacale, o in generale quelli relativi alla salute [17].

Più precisamente, l'art. 9 GDPR presenta una «struttura bifasica» [18], ponendo, da un lato, il divieto generale di trattare categorie "particolari" e individuando al tempo stesso, dall'altro, una serie di eccezioni a tale divieto: una delle deroghe al divieto generale di trattamento dei dati "particolari" è costituita proprio dall'ipotesi in cui il trattamento sia finalizzato al perseguimento di scopi determinati e legittimi, individuati nell'atto costitutivo, nello statuto o nel contratto collettivo della fondazione, dell'associazione o di altro organismo *non profit*, nella specie, della cooperativa di dati. Alla luce dell'astratta meritevolezza delle finalità perseguite e delle funzioni svolte da tali strutture organizzative, il legislatore ha quindi operato *ex ante* una valutazione di legittimità del trattamento dei dati "particolari" là dove associazioni, fondazioni e in generale enti del terzo settore, cui le cooperative di dati – come rilevato – potrebbero ricondursi, perseguano, (anche) mediante il trattamento stesso, le loro finalità istituzionali, civiche, solidaristiche e di utilità sociale. In altri termini, trattasi di uno di quei casi in cui al consenso dell'interessato si sostituiscono, quali basi giuridiche per il trattamento delle categorie particolari di dati, esigenze diverse ritenute prevalenti rispetto alla posizione dell'interessato e, nella specie, rappresentate dallo svolgimento di attività da parte di enti senza finalità lucrativa per il perseguimento di scopi politici, filosofici, religiosi, culturali, umanistici e sociali.

La cooperativa di dati potrà quindi trattare i dati per così dire "sensibili", anche senza il consenso dell'interessato, a condizione però che, dal punto di vista soggettivo, il trattamento riguardi unicamente i membri, gli *ex* membri o le persone con regolari contatti con la cooperativa e i dati personali non vengano comunicati all'esterno: in sostanza, l'ente potrà trattare i dati "particolari" senza il consenso dell'interessato allorché il trattamento abbia carattere meramente interno.

Dal punto di vista oggettivo, poi, perché tale trattamento sia lecito, dovrà perseguire scopi determinati e legittimi indicati nello statuto o nell'atto costitutivo [19]:

---

[17] Pensiamo, ad esempio, alle associazioni che operano per un fine di assistenza sociale o socio-sanitaria, che trattano dati relativi alla salute. In generale, gli ETS possono facilmente disporre di dati "particolari" (sensibili): quelli dei beneficiari dell'attività sociale, quando operano proprio nei settori che il legislatore considera più delicati, come ad esempio l'ambito sanitario e della salute (ad es. chi lavora con malati, soggetti portatori di *handicap* o tossicodipendenti, ma anche con anziani portatori di patologie), l'ambito religioso o caratterizzato ideologicamente in senso politico, ma anche filosofico (ad es. un'associazione espressamente e "istituzionalmente" pacifista o antiproibizionista), l'ambito dell'appartenenza etnica (es. associazioni che lavorano con i nomadi o migranti).

[18] Così, R. TUCCILLO, *Art. 9 GDPR*, in A. BARBA-S. PAGLIANTINI (a cura di), *Delle persone*, vol. II, in E. GABRIELLI (diretto da), *Commentario codice civile*, Milano, 2019, p. 153. Cfr., anche, F. BRAVO (a cura di), *Dati personali. protezione, libera circolazione e* governance, Pisa, 2023; G. ALPA, *La normativa sui dati personali. Modelli di lettura e problemi esegetici*, in V. CUFFARO-V. RICCIUTO-V. ZENO ZENCOVICH (a cura di), *Trattamento dei dati e tutela della persona*, Milano, 1998, p. 3 ss.

[19] La finalità perseguibile sarà, in tal caso, la condivisione dei dati e il rafforzamento della posizione degli individui nel fare scelte informate prima di acconsentire all'uso dei dati, influenzando i

ciò, in ossequio al principio c.d. di finalità, sancito dall'art. 5, lett. *b*) del Regolamento UE come uno dei fondamenti del trattamento e alla cui stregua la raccolta dei dati e il loro successivo utilizzo devono avere precise e determinate finalità, che vanno comunicate all'interessato e rispettate. Per la cooperativa dei dati, come in generale per gli ETS, le finalità del trattamento dei dati tendenzialmente coincidono o sono comprese negli scopi istituzionali indicati nello statuto [20].

V'è di più. In quanto titolari di trattamento, le cooperative di dati dovranno predisporre, per tutte le categorie di interessati – e quindi per i soggetti di cui vengono trattati i dati (membri, dipendenti, relativi familiari, donatori, fornitori, beneficiari, volontari, ecc.) – le relative informative, redatte secondo le indicazioni del Regolamento. Lo scopo è quello di informare, appunto, gli interessati sul tipo di dati oggetto di trattamento, sulle modalità e sui tempi di conservazione o sui destinatari, ecc. [21]. In particolare, l'art. 12 GDPR – rubricato come «trasparenza e modalità» –

termini e le condizioni delle organizzazioni degli utenti dei dati legate all'uso dei dati in modo da offrire scelte migliori ai singoli membri del gruppo o eventualmente trovare soluzioni alle posizioni contrastanti dei singoli membri di un gruppo su come i dati possono essere utilizzati laddove tali dati si riferiscono a diversi interessati all'interno di quel gruppo: *considerando* n. 31, DGA.

[20] Ad esempio, quando l'ente raccoglie i dati comuni dei suoi membri per inserirli nel libro soci, per inviare a casa la corrispondenza o il giornale sociale e, comunque, per averne la reperibilità, o raccoglie i dati dei beneficiari dell'attività per garantire il servizio, non potrà senza l'autorizzazione e/o l'informazione specifica ai soci/beneficiari usare tali dati per scopi diversi da quelli istituzionali: così, non potrà comunicare il nome e l'indirizzo o altre informazioni a terzi per *marketing*, iniziative commerciali o comunque per scopi che non riguardano l'ente.

[21] Il GDPR (art. 12, par. 1) prevede che l'informativa sia concisa, trasparente, comprensibile, facilmente accessibile e di linguaggio semplice e chiaro e sia fornita «per iscritto o con altri mezzi» e anche «se del caso, con mezzi elettronici» e anche oralmente, «se richiesto dall'interessato». L'informativa deve contenere: l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante; i dati di contatto del responsabile della protezione dei dati (*Data Protection Officer* o DPO), ove nominato; le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento; qualora il trattamento si basi sull'art. 6, par. 1, lett. *f*) (esistenza di un «legittimo interesse del titolare del trattamento o di terzi» che non leda i diritti e le libertà fondamentali dell'interessato), i legittimi interessi perseguiti dal titolare del trattamento o da terzi; gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali; ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'art. 46 o 47, o all'art. 49, secondo comma, il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili. Inoltre, la stessa informativa deve contenere: il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati; qualora il trattamento sia basato sul consenso prestato dall'interessato (ai sensi dell'6, par. 1, lett. *a*) e art. 9, par. 2, lett. *a*) del GDPR), l'esistenza del diritto di revocare il consenso in qualsiasi momento, senza però pregiudicare la liceità del trattamento effettuato sulla base del consenso prestato prima della revoca; il diritto di proporre reclamo al Garante della Protezione dei Dati Personali; se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un re-

detta le regole generali operanti per l'obbligo di informazione agli interessati alla luce del principio di trasparenza espressamente sancito e relativo tanto alla fase prodromica del trattamento, quanto a quella successiva in cui i dati vengano effettivamente trattati. Le cooperative di dati, in forza dell'art. 12 GDPR, saranno così tenute a fornire informazioni concise, trasparenti, intellegibili e facilmente accessibili, in forma scritta o con mezzi elettronici, purché adeguati alle circostanze e alle modalità di interazione – tra ente titolare del trattamento e interessato – o alle modalità di raccolta delle informazioni medesime.

Con specifico riferimento ai mezzi elettronici, nel caso di utilizzo da parte dell'ente di un sito *internet*, il Gruppo di lavoro Articolo 29 [22] ha raccomandato l'uso di informazioni stratificate che consentano di consultare le sezioni specifiche dell'informativa sulla *privacy*, contestualmente ed in aggiunta ad un unico documento completo in formato digitale al quale gli interessati possano accedere altrettanto facilmente, qualora intendano consultare le informazioni di cui sono destinatari nella loro interezza. Uno degli strumenti di maggiore novità in tema di informazione e di trasparenza è rappresentato proprio dalla possibilità per i titolari di trattamento, e quindi anche per le cooperative di dati, di fornire le informazioni *ex* artt. 13 e 14 GDPR in combinazione con icone standardizzate, presentate elettronicamente e in grado di aumentare la trasparenza, offrendo un quadro facilmente accessibile, intellegibile e chiaro del trattamento previsto.

Per quanto riguarda, poi, i soggetti (ad es. volontari, segretari, personale amministrativo, persone che si occupino del *data entry* nell'anagrafica dei volontari e così via) che, internamente all'ente, hanno accesso ai dati personali, l'ente (titolare del trattamento) dovrà *ex* art. 29 GDPR istruirli *ad hoc* sulle modalità del trattamento [23]. Il GDPR, diversamente dalla disciplina contenuta nel Codice *Privacy*, non prevede espressamente la figura dell'"incaricato", ma neppure la esclude, là dove fa riferimento, proprio nell'art. 29, a «persone autorizzate al trattamento sotto l'autorità diretta del titolare o del responsabile»: chiunque, all'interno o all'esterno dell'organizzazione, svolga questa attività dovrà essere sempre adeguatamente informato e istruito su come trattare i dati. Trattasi di un adempimento di carattere gene-

---

quisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati; l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'art. 22, par. 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

[22] Com'è noto, il Gruppo di lavoro "Articolo 29" (Art. 29 *WP*), poi sostituito dallo *European Data Protection Board* (EDPB), era il gruppo di lavoro europeo indipendente che, fino al 25 maggio del 2018 (entrata in vigore del GDPR) aveva lo scopo di occuparsi di questioni interpretative relative alla protezione della vita privata e dei dati personali.

[23] Art. 29 GDPR: «il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri».

rale, relativo alla formazione dei soggetti per così dire "incaricati" (secondo la vecchia terminologia) ed anche questo chiaramente ispirato ad un altro dei principi fondamentali sanciti dall'art. 5 Reg. UE n. 679/2016 e, in particolare, quelli di «integrità e riservatezza» (lett. f) che per l'appunto impone (nella specie, alla cooperativa di dati) di trattare i dati in modo da garantire anche indirettamente, e cioè attraverso soggetti diversi dall'ente, la medesima sicurezza dei dati e impedire violazioni nel trattamento degli stessi. La sicurezza dei dati non può infatti prescindere da un'accurata istruzione dei soggetti che materialmente trattano i dati personali [24].

Tutti i soggetti per così dire "esterni" all'ente, ossia che trattino o possano trattare dati personali per conto dell'ente stesso (come consulenti, professionisti, altre organizzazioni, soggetti che si occupano della gestione e manutenzione di *software* ecc.), dovranno non soltanto essere istruiti dall'ente, in quanto titolare del trattamento, ma altresì stipulare con quest'ultimo un vero e proprio contratto *ex* art. 28 del Regolamento, che disciplina le modalità con cui devono essere trattati i dati [25]: un contratto scritto, per lo più in forma digitale, dal contenuto predeterminato dalla norma stessa e per effetto del quale il soggetto "esterno" (consulente, professionista, altra organizzazione, soggetto che si occupa della gestione e manutenzione di *software* ecc.) agirà per conto della cooperativa di dati titolare del trattamento [26].

---

[24] Sull'argomento, cfr. M. MASSIMI, *Art. 29 GDPR*, in A. BARBA-S. PAGLIANTINI (a cura di), *op. cit.*, p. 574.

[25] Art. 28 GDPR, par. 3: «I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento (…)». E. MAIO, *Art. 28 GDPR*, in A. BARBA-S. PAGLIANTINI (a cura di), *Delle persone*, cit., p. 566 s. sottolinea come la norma sia strutturata sul modello tedesco (§ 11 *BDSG*), probabilmente per la puntualità della normativa tedesca rispetto alle altre, garanzia di una maggiore efficienza nella protezione dei dati personali dell'interessato e di una limitata discrezionalità dei soggetti coinvolti nel trattamento dei dati.

[26] Si pensi, a titolo esemplificativo, ad un birrificio con molti dipendenti. Firma un contratto con una società addetta all'elaborazione delle buste paga per pagare gli stipendi. Il birrificio indica a tale società quando deve essere pagato lo stipendio, quando un dipendente lascia l'azienda o ottiene un aumento di stipendio, e fornisce tutti gli altri dati per le buste paga e i pagamenti. La società fornisce il sistema informatico e conserva i dati dei dipendenti. Il birrificio è il titolare del trattamento e la società addetta all'elaborazione delle buste paga è il responsabile del trattamento. Nonostante, infatti, i cambiamenti introdotti dal nuovo Reg. UE 2016/679 (GDPR, Regolamento Generale sulla protezione dei dati), le basi normative introdotte dal Codice della *Privacy* (d.lgs. n. 196/2003) rimangono invariate. La terminologia del nuovo Regolamento, da questo punto di vista, si allinea alla normativa nazionale. Le figure coinvolte nel trattamento dei dati sono sempre le stesse: si parla di titolare, responsabile (sostanzialmente corrispondente all'incaricato del trattamento), sia a livello comunitario che a livello nazionale. Il Regolamento definisce, infatti, caratteristiche soggettive e responsabilità del titolare e del responsabile del trattamento negli stessi termini di cui alla direttiva 95/46/CE (e, quindi, al Codice italiano). La disciplina europea ha tuttavia introdotto alcune novità significative, volte a rafforzare la tutela del diritto alla *privacy* e, di conseguenza, i diritti degli interessati.

Proprio in questi termini, sembra legittimo risolvere l'*impasse* interpretativo scaturente dal combinato disposto degli artt. 28 e 29 GDPR alla cui stregua, rispettivamente, «qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento» con i quali ha l'obbligo di stipulare «un contratto (…) *sulla* durata del trattamento, natura e finalità, tipo di dati trattati e categorie di interessati (…)» (art. 28) e «il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non istruito in tal senso dal titolare del trattamento» (art. 29). In sostanza, se è vero che il contratto *ex* art. 29 GDPR va stipulato (non con chiunque, ma) soltanto con chi effettui il trattamento per conto dell'ente titolare del trattamento, è altrettanto vero che chiunque abbia accesso ai dati personali, a prescindere dal contratto *ex* art. 29 GDPR, dovrà comunque essere adeguatamente edotto ed istruito dal titolare del trattamento per poter trattare i dati.

Tutto ciò, sempre e ancora una volta, nel rispetto dei principi generali del Regolamento sanciti dall'art. 5 GDPR. In particolare, in forza del c.d. principio di "limitazione delle finalità", le cooperative di dati, o in generale, le «persone (*da loro*) autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile» (*ex* art. 4, n. 10, GDPR) dovranno raccogliere, trattare ed utilizzare i dati compatibilmente ed esclusivamente per finalità determinate, esplicite e legittime: finalità che, di norma e come già sottolineato, coincideranno con quelle dell'ente stesso indicate nello statuto o nell'atto costitutivo. In tale contesto, il profilo di maggiore criticità attiene alla compatibilità o meno del trattamento effettuato (nella specie) da una cooperativa di dati con le c.d. finalità ulteriori, soprattutto perché il DGA, all'art. 12, vieta al «fornitore di servizi di intermediazione dati *di utilizzare* i dati per i quali fornisce servizi di intermediazione dati per scopi *diversi* da quelli di metterli a disposizione degli utenti dei dati» e, al *considerando* n. 32, sottolinea che i «fornitori di servizi di intermediazione dati svolgano solo il ruolo di intermediari nelle transazioni e non utilizzino i dati scambiati per nessun altro scopo».

Alla luce del combinato disposto delle norme dei due Regolamenti, appare legittimo interpretare restrittivamente siffatto divieto e ritenere ammissibili scopi *diversi* ma *compatibili* con quello di condivisione di dati, fondando la valutazione di compatibilità [27] del trattamento per fini ulteriori proprio sul rapporto di strumentali-

[27] Per stabilire la compatibilità della nuova finalità occorre tenere conto, tra l'altro, di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto; del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento; della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'art. 9, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'art. 10; delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati; dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione: in tal senso, cfr. D. ACHILLE, *Art. 5*, in A. BARBA-S. PAGLIANTINI (a cura di), *Delle persone*, cit., p. 109. È possibile rinvenire alcune importanti linee guida in merito al compimento della valutazione di compatibilità delle finalità nell'*Opinion* n. 3/2013 dell'Art. 29 *Data Protection*

tà delle eventuali finalità ulteriori rispetto a quelle iniziali. L'art. 5, lett. *b*), GDPR ritiene espressamente compatibile con le finalità iniziali «un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici» [28].

Working Party – sebbene si tratti di un'*opinion* scritta sotto la vigenza della Direttiva 95/46/CE, è comunque utile ripercorrere i termini del "*compatibility assessment*", coniugandolo con le attuali previsioni del *GDPR*. In particolare, in tale parere, viene affermato che il (determinante) test di compatibilità debba preferibilmente fondarsi su una valutazione sostanziale (piuttosto che formale, per natura eccessivamente rigida, benché, a prima vista, maggiormente obiettiva e neutrale), la quale, capace di andare oltre agli aspetti meramente formalistici, si basa sulla valutazione dei seguenti (utili e noti) criteri, divenendo, così, un metodo flessibile, pragmatico e maggiormente efficace: il rapporto tra la finalità per la quale i dati sono stati raccolti e la finalità ulteriore di trattamento, sicché l'attenzione deve concentrarsi sul rapporto sostanziale tra le due finalità (originaria ed ulteriore) di trattamento, onde così comprendere se sussiste una situazione in cui l'ulteriore trattamento fosse già (più o meno) implicito nella finalità iniziale ovvero assunto come una fase logica successiva del trattamento in base a tale finalità; in secondo luogo, il contesto in cui i dati sono stati raccolti, e la (ragionevole) aspettativa del soggetto interessato in merito al loro ulteriore utilizzo e al fine di valutare la ragionevole aspettativa del soggetto interessato, è necessario tenere in considerazione la natura del rapporto tra l'interessato e il relativo titolare del trattamento, lo *status* di quest'ultimo nonché la base giuridica su cui si è fondata la finalità di trattamento originaria, onde così comprendere il grado di sorpresa dell'interessato e l'eventuale squilibrio, ai danni dello stesso, nel relativo rapporto; la natura dei dati e l'impatto dell'ulteriore trattamento sul soggetto interessato. Tale terzo fattore esprime un comune approccio, giacché la normativa in parola è stata progettata ed è volta a proteggere le persone fisiche contro l'impatto di un uso improprio ovvero eccessivo dei dati personali: in merito, viene, dunque, ricordato che più sensibili sono le informazioni personali coinvolte, più ristretto è, di conseguenza, l'ambito di un utilizzo compatibile. Infine, rilevano le garanzie applicate dal titolare del trattamento al fine di determinare un trattamento corretto e prevenire un qualsiasi indebito impatto sul soggetto interessato: in merito, il WP 29 ha precisato che la sussistenza di adeguate misure aggiuntive possono essere idonee, in linea di principio, a compensare l'ulteriore finalità di trattamento ovvero il fatto che essa non sia stata chiaramente specificata all'inizio, così come *ex lege* richiesto.

[28] Tale tipo di trattamento, comunque, deve essere realizzato in base ad apposite garanzie, come previste dall'art. 89 GDPR, al fine di tutelare i diritti degli interessati. Le garanzie, ovviamente, sono date dalle misure di sicurezza (tra le quali si può includere la pseudonimizzazione) e il rispetto della minimizzazione dei dati. Il novellato Codice *Privacy* (art. 110-*bis*), poi, stabilisce che l'Autorità di controllo può autorizzare il trattamento ulteriore dei dati per fini di ricerca scientifica o per finalità statistiche da parte di soggetti che svolgano principalmente tali attività, qualora l'informazione agli interessati risultasse impossibile o implicasse uno sforzo sproporzionato, però a condizione che vengano adottate misure appropriate per tutelare i diritti, le libertà e i legittimi interessi degli interessati, ivi incluse forme preventive di minimizzazione e di anonimizzazione dei dati. Peraltro, il *WP* 29 ha sottolineato che, in via potenziale, possono sussistere tre differenti scenari: la compatibilità è *prima facie* ovvia e, quindi, un ulteriore trattamento può essere ritenuto compatibile, in quanto i dati sono trattati per raggiungere, in un modo consueto, le finalità specificate al momento della raccolta; oppure la compatibilità non è ovvia e, dunque, necessita di una ulteriore analisi per verificare la sussistenza di una connessione tra lo scopo specificato ed il modo in cui i dati vengono successivamente elaborati. In altri termini, gli scopi sarebbero correlati, ma non completamente corrispondenti. Infine, l'incompatibilità è ovvia e i dati vengono elaborati in un modo o per scopi aggiuntivi che una persona ragionevole riterrebbe inaspettati, inappropriati o altrimenti discutibili: il trattamento non soddisfa, senz'altro, le aspettative dell'interes-

Nonostante l'ente titolare del trattamento sia dunque chiamato a prevedere *ex ante* e in modo specifico le finalità cui attenersi nello svolgimento delle operazioni di trattamento, non è escluso lo svolgimento di trattamenti ulteriori per scopi diversi: ciò può avvenire nella misura in cui le finalità ulteriori siano "compatibili" rispetto alle finalità per le quali i dati sono stati inizialmente raccolti [29].

Al riguardo, la formulazione dell'art. 5, lett. *b*), GDPR risulta "ambigua", dal momento che non è sufficientemente chiaro quali siano le finalità del trattamento "compatibili" rispetto a quella originaria. L'unica certezza chiaramente detta dal legislatore europeo è, per l'appunto, che «un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è (…) considerato incompatibile con le finalità iniziali» [30].

Altrettanto dubbia è la natura meramente esemplificativa o tassativa del riferimento alle suddette finalità ulteriori specificamente menzionate dal legislatore europeo come "compatibili". La soluzione di tale quesito non sembra poter prescindere da una lettura dell'art. 5, lett. *b*), GDPR in combinato disposto con il successivo art. 6, par. 4 e con il *considerando* n. 50 [31]: sicché l'ente (nella specie, la cooperati-

---

sato. L'allegato 4, poi, contiene ulteriori esempi pratici – da casi semplici e diretti a casi più complessi – che illustrano come può essere effettuata una valutazione di compatibilità sostanziale. I vari esempi includono, tra gli altri, l'elaborazione di dati nell'ambito del *marketing*, le telecamere a circuito chiuso, il trasferimento dei risultati della visita medica pre-assunzione, l'uso di algoritmi per prevedere la gravidanza delle clienti dalle abitudini di acquisto, l'uso di posizioni di telefoni cellulari per informare sulle misure di moderazione del traffico, sull'uso dei registri dei nominativi dei passeggeri, sul trattamento dei dati di misurazione intelligente a fini fiscali o per rilevare un uso fraudolento o sull'applicazione della direttiva sulla conservazione dei dati.

[29] Nel pieno rispetto del ben noto principio di *accountability*, l'ente titolare del trattamento sarà poi chiamato a comprovare di aver agito conformemente al principio di finalità, sulla base di un'attenta valutazione in merito alla compatibilità degli scopi ulteriori del trattamento, così come richiesto ai sensi del combinato disposto degli artt. 5, lett. *b*), e 6, par. 4, GDPR. Più precisamente, il GDPR prevede espressamente che sia possibile ampliare le finalità iniziali del trattamento e che la valutazione in merito alla loro "non incompatibilità", ai sensi e per gli effetti dell'art. 6, par. 4, sia rimessa al titolare e a lui soltanto, rientrando nella sua *accountability* l'esser in grado di dimostrare che il trattamento sia in ogni caso avvenuto nel pieno rispetto della normativa applicabile in materia di protezione dei dati personali.

[30] Norma, questa, che va letta in combinato disposto con l'attuale formulazione dell'art. 110-*bis* del d.lgs. n. 196/2003, come da ultimo emendato dal d.lgs. 10 agosto 2018, n. 101, alla cui stregua l'Autorità Garante per la protezione dei dati personali può autorizzare il trattamento ulteriore dei dati per fini di ricerca scientifica o per finalità statistiche da parte di soggetti che svolgano principalmente tali attività, allorché informare gli interessati risultasse impossibile o implicasse uno sforzo sproporzionato e a condizione che vengano adottate misure appropriate per tutelare i diritti, le libertà e i legittimi interessi degli interessati, ivi incluse forme preventive di minimizzazione e di anonimizzazione dei dati.

[31] *Considerando* n. 50, GDPR: «Il trattamento dei dati personali per finalità diverse da quelle per le quali i dati personali sono stati inizialmente raccolti dovrebbe essere consentito solo se compatibile con le finalità per le quali i dati personali sono stati inizialmente raccolti. In tal caso non è richiesta alcuna base giuridica separata oltre a quella che ha consentito la raccolta dei dati personali (…) L'ul-

va di dati) potrà trattare i dati personali per *finalità* ulteriori, non limitate a quelle di archiviazione nel pubblico interesse, o di ricerca scientifica o storica o a fini statistici, ma ritenute in generale *compatibili* con quelle originarie, alla luce del contesto in cui i dati personali sono stati raccolti e, in particolare, delle ragionevoli aspettative dell'interessato, della natura dei dati personali, delle conseguenze dell'ulteriore trattamento previsto per gli interessati e, infine, dell'esistenza di garanzie adeguate sia nel trattamento originario sia nell'ulteriore trattamento previsto [32].

Così, con precipuo riferimento ad una cooperativa di dati, non sembra possa considerarsi "compatibile" l'uso dei dati personali per l'interconnessione degli interessati e dei titolari dei dati con gli utenti dei dati, lo scambio di dati, l'archiviazione temporanea, la *curation*, la conversione, l'anonimizzazione e la pseudonimizzazione, dal momento che l'art. 12, lett. *e*), DSA specificamente prevede che «tali strumenti veng[a]no utilizzati solo su richiesta esplicita o approvazione del titolare o dell'interessato»; al contrario, potrebbe ritenersi "compatibile" l'utilizzo di dati, ad esempio, per l'individuazione di frodi o di sicurezza informatica, o ancora l'adattamento dei dati scambiati per migliorarne l'utilizzabilità da parte degli utenti stessi o l'interoperabilità, anche attraverso conversione dei dati in formati specifici [33].

Peraltro, se tale interpretazione sistematica – volta a ritenere ammissibili scopi sì diversi, ma "compatibili" – appare fondata per la condivisione dei dati personali, *a fortiori* essa appare condivisibile in riferimento ai dati non personali, che, per natura, non necessitano della medesima protezione e delle stesse cautele riservate dalla legge ai dati personali, trattandosi genericamente di «rappresentazioni e raccolte

---

teriore trattamento a fini di archiviazione nel pubblico interesse, o di ricerca scientifica o storica o a fini statistici dovrebbe essere considerato un trattamento lecito e compatibile. La base giuridica fornita dal diritto dell'Unione o degli Stati membri per il trattamento dei dati personali può anche costituire una base giuridica per l'ulteriore trattamento. Per accertare se la finalità di un ulteriore trattamento sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento dovrebbe, dopo aver soddisfatto tutti i requisiti di liceità del trattamento originario, tener conto tra l'altro di ogni nesso tra tali finalità e le finalità dell'ulteriore trattamento previsto, del contesto in cui i dati personali sono stati raccolti, in particolare le ragionevoli aspettative dell'interessato in base alla sua relazione con il titolare del trattamento con riguardo al loro ulteriore utilizzo; della natura dei dati personali; delle conseguenza dell'ulteriore trattamento previsto per gli interessati; e dell'esistenza di garanzie adeguate sia nel trattamento originario sia nell'ulteriore trattamento previsto (…)».

[32] L'ETS potrà inoltre trattare i dati per finalità ulteriori anche *incompatibili* rispetto a quelle originarie, purché l'interessato abbia prestato il proprio consenso ovvero il trattamento si basi su un atto legislativo dell'Unione o degli Stati membri, che costituisca una misura necessaria e proporzionata per la salvaguardia, in particolare, degli importanti obiettivi di interesse pubblico generale di cui all'art. 23, par. 1, GDPR.

[33] Nell'ipotesi di incompatibilità del trattamento ulteriore con le finalità originarie per le quali il trattamento è stato autorizzato, l'ente dovrà agire in virtù di un'autonoma base giuridica ai sensi dell'art. 6 GDPR. Sull'argomento, cfr. F. RESTA, *Art. 5*, in G.M. RICCIO-G. SCORZA-E. BELLISARIO (a cura di), *GDPR e normativa privacy*, Vicenza, 2018, p. 51 ss. e, in particolare, p. 58.

digitali di atti, fatti o informazioni, (…) anche sotto forma di registrazione sonora, visiva o audiovisiva» (art. 2*,* DGA).

Alla luce, poi, del principio di "minimizzazione e proporzionalità", anch'esso sancito dall'art. 5 GDPR, le cooperative di dati non potranno acquisire informazioni e dati ultronei rispetto a quelli necessari per il raggiungimento dello scopo del trattamento: essi devono cioè assicurarsi che i dati raccolti siano adeguati, pertinenti e non eccedenti rispetto a quanto necessario per il perseguimento delle finalità per cui sono raccolti. Ci si intende riferire, in particolare, all'ipotesi assai frequente nella prassi di un ente che sottoponga agli utenti o a coloro che entrano in contatto con l'ente stesso moduli nei quali conferire un numero o tipologie di dati eccessivi rispetto alle finalità (es. nelle richieste di iscrizione alla *newsletter*, o nella domanda di partecipazione ad un evento o a un seminario sono da considerarsi certamente ultronei la residenza, la data di nascita e il codice fiscale, o due recapiti telefonici, ecc.). In tali casi, occorrerà di volta in volta valutare quali siano i dati strettamente indispensabili per fornire il servizio richiesto e sarà certamente possibile, nello stesso modulo (o *format* di iscrizione ad un corso), proporre all'interessato di conferire i dati ulteriori e di fornire il consenso al trattamento per i diversi servizi cui voglia accedere [34].

Considerazioni pressoché analoghe valgono per il principio della c.d. "limitazione della conservazione", alla cui stregua le cooperative di dati, in quanto titolari di trattamento, dovranno conservare i dati per un periodo di tempo non superiore a quello necessario per il raggiungimento delle finalità per cui sono stati raccolti, a meno che la conservazione non avvenga, ancora una volta, per fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici. In siffatto contesto, appare opportuno interrogarsi sulla possibilità per una cooperativa di dati di conservare, e conseguentemente trattare, i dati personali dei propri membri anche dopo che essi abbiano lasciato l'ente. Il GDPR, all'art. 9 par. 2 lett. *d*), come già rilevato, consente l'utilizzo dei dati (anche sensibili) degli *ex* soci senza specifico consenso, se tale utilizzo è svolto nell'ambito dell'attività dell'ente e con adeguate garanzie (di protezione dei dati), con divieto però di comunicazione all'esterno (per tale comunicazione ci vuole il consenso specifico dell'*ex* socio) [35]: sicché il

[34] Ad esempio, chi partecipa ad un corso organizzato dalla cooperativa di dati acconsentirà facilmente a che il suo indirizzo *mail* sia inserito nella *newsletter* che lo avverta di nuovi eventi formativi.

[35] Peraltro, in applicazione del principio di proporzionalità e minimizzazione dei dati, i dati "trattenuti" dall'associazione dopo l'uscita del socio dovranno però essere strettamente inerenti alle specifiche attività "residue" (es. invio della *newsletter*, convocazione per gli anniversari, ecc.), e quindi potranno, per esempio, ridursi al nominativo e all'indirizzo *mail*. Quanto, poi, alla protezione dei dati in senso stretto, essa è assicurata all'interessato (c.d. *data subject*) attraverso l'esercizio dei diritti indicati dagli artt. da 15 a 22 del GDPR: là dove "soggetti interessati" sono anche gli stessi associati/volontari, e non solo i soggetti esterni all'ETS. In base a tali articoli l'interessato può infatti chiedere al Titolare, cioè all'ente *non profit* di avere conferma che l'ente utilizzi i suoi dati e di sapere quali siano questi dati; di conoscere l'origine dei dati (cioè come e da chi l'ETS li ha acquisiti), le finalità del trattamento, i soggetti a cui i dati vengono comunicati e il periodo di conservazione dei dati; di

trattamento dei dati degli *ex* soci, ammesso dal Regolamento, ha carattere meramente interno. In particolare, l'Autorità Garante della *Privacy* [36] ha non solo precisato che, prima di iniziare o proseguire il trattamento, i sistemi informativi e i programmi informatici utilizzati dagli enti devono essere configurati in guisa da ridurre al minimo l'utilizzazione di dati personali identificativi e da escluderne il trattamento ogniqualvolta le finalità perseguite nei singoli casi possano essere realizzate mediante dati anonimi o opportune modalità che permettano di identificare l'interessato solo in caso di necessità; ma ha altresì circoscritto l'ambito di applicazione della disposizione sia dal punto di vista soggettivo, sia oggettivo.

Sotto il primo profilo, il provvedimento chiarisce che il trattamento potrà essere operato da associazioni, organizzazioni assistenziali e di volontariato, fondazioni, comitati, consorzi e organismi senza scopo di lucro: in sostanza, gli enti del terzo settore, incluse le cooperative di dati alla luce delle riflessioni sin qui svolte. Sotto il secondo profilo, il trattamento dovrà perseguire senza scopo di lucro, finalità civiche, solidaristiche e di utilità sociale indicate nel codice del terzo settore, all'art. 5, tra le quali appare possibile annoverare la condivisione dei dati per la costruzione ed il rafforzamento di un'economia digitale basata sui dati e inclusiva per tutti i cittadini dell'Unione.

Ma il principio di limitazione della conservazione dei dati e l'interrogativo posto, ossia la possibilità o meno per le cooperative di dati di conservare, e conseguentemente trattare, i dati personali dei propri soci anche dopo che essi abbiano – per qualunque ragione o evento – lasciato l'ente, a ben vedere, involge (anche) per tali titolari di trattamento la più ampia e *vexata quaestio* della gestione del patri-

---

rettificare (correggere o integrare) i dati inesatti o incompleti (es. cambio di indirizzo o dello stato civile, aggiornamento del curriculum, ecc.); di cancellare i dati (cd. diritto "all'oblio") quando il trattamento non è più necessario per il raggiungimento delle finalità per cui sono stati raccolti, o in caso di revoca del consenso, o in caso di trattamento illecito o negli altri casi previsti dall'art. 17 GDPR; ottenere una "limitazione del trattamento" nei casi previsti dall'art. 18 GDPR; di poter trasferire i dati ad un altro titolare (diritto "alla portabilità dei dati"); di opporsi al trattamento dei suoi dati, anche se svolto correttamente dall'associazione, se sussistono "motivi particolari" (cioè particolari e valide ragioni: ad esempio se ha presentato domanda di recesso dall'associazione, o se il trattamento, anche se lecito, risulta lesivo della sua dignità o riservatezza); di opporsi al trattamento dei dati svolto per il "*marketing* diretto" (invio di materiale pubblicitario o vendita diretta o compimento di ricerche di mercato o di comunicazione commerciale); di non essere sottoposto ad una decisione basata su un "trattamento automatizzato" di dati (inclusa la cd. profilazione).

[36] Autorizzazione generale n. 3/2016, modificata dal provvedimento n. 146 del 5 giugno 2019, emessa dopo l'entrata in vigore del GDPR ed operante anche con riferimento alle norme in esso contenute: testualmente, «la presente autorizzazione ha efficacia dal 1° gennaio 2017 fino al 24 maggio 2018, tenuto conto che a decorrere dal 25 maggio 2018 sarà applicabile il Regolamento (UE) 2016/679 (relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE) entrato in vigore il 24 maggio 2016, salve le modifiche che il Garante ritenga di dover apportare in conseguenza di eventuali novità normative rilevanti in materia e ferme restando le determinazioni eventualmente adottate dall'Autorità in applicazione del citato Regolamento».

monio digitale per il tempo in cui una persona, nella specie il membro dell'ente, avrà cessato di vivere: questione complessa stante soprattutto l'inadeguatezza degli istituti tradizionali che, seppur adattati alle peculiari caratteristiche del mondo digitale, restano ancorati ad un sistema pensato e sviluppatosi per una realtà ed un contesto socio-economico profondamente diversi e che necessita, quindi, di essere rimeditato alla luce dell'incessante evoluzione digitale, che caratterizza e condiziona ormai la nostra epoca in ogni aspetto, anche quello oltre la morte fisica dell'individuo. Limitandoci in questa sede agli aspetti più strettamente inerenti alla relazione tra cooperative di dati e *data protection*, va osservato come la rilevanza giuridica della questione del trattamento postumo dei dati da parte della cooperativa di dati [37] sia principalmente riconducibile alla circostanza che i dati rappresentano una porzione consistente della ricchezza nelle moderne economie [38]. Muovendo cioè dalla considerazione che i dati personali di un "interessato" (*data subject*) sopravvivano oltre la sua vita, per un periodo anche illimitato di tempo, grazie (o a causa) delle attuali tecnologie dell'informazione e della comunicazione, risulta innegabile l'esigenza di un riconoscimento di diritti e poteri di controllo su tali informazioni [39]

---

[37] Cfr., sull'argomento, I. MASPES, *Successione digitale, trasmissione dell'*account *e condizioni generali di contratto predisposte dagli* internet services providers, in *Contratti*, 2020, 5, p. 583 ss.; G. RESTA, *La "morte" digitale*, in *Dir. inf*., 2014, p. 907 ss., che sottolinea come la maggior parte dei dati personali digitali sia nella disponibilità dei *providers* e la loro (in)trasmissibilità è normalmente regolata nelle condizioni del contratto di servizio. Si tratta di clausole di contratti *standard* unilateralmente predisposte, spesso di origine americana e tendenzialmente volte ad escludere la trasferibilità dell'*account* e dei suoi contenuti. Più recentemente, ID., *La successione nei rapporti digitali e la tutela post-mortale dei dati personali*, in *Contr. e impr*., 2019, p. 86 ss. V., anche, ZENO ZENCOVICH, *La "datasfera". Regole giuridiche per il mondo digitale parallelo*, in AA.VV., *I "profili" del diritto. Regole, rischi e opportunità nell'era digitale* (a cura di L. Scaffardi), Torino, 2018, p. 99; C. CAMARDI, *L'eredità digitale. Tra reale e virtuale*, in *Dir. inf*., 2018, p. 65 ss.; A. VESTO, *Successione digitale e circolazione dei beni* online. *Note in tema di eredità digitale*, Napoli, 2020; A. MAGNANI, *Il patrimonio digitale e la sua devoluzione ereditaria*, in *Vita not*., 2019, p. 1208 ss.; M. TESCARO, *La tutela postmortale della personalità morale e specialmente dell'identità personale*, in *juscivile*, 2014, 10, p. 316 ss.

[38] Con riferimento all'ordinamento giuridico italiano, si segnala un primo rilevante intervento legislativo effettuato con il d.lgs. 10 agosto 2018, n. 101, recante «Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)». Tale legge contiene una previsione specifica circa il trattamento dei dati personali riguardanti le persone decedute. All'art. 2-*terdecies* è infatti previsto che "i diritti di cui agli articoli da 15 a 22 del Regolamento riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione". È fatta salva la volontà dell'interessato, purché risulti in modo non equivoco, di vietare l'esercizio di tali diritti. Cfr., sul tema, P. PATTI-F. BARTOLINI, *Digital Inheritance and post mortem data protection: the Italian Reform*, in *European Review of Private Law*, 2019, p. 1181 ss.

[39] Ci si intende in particolare riferire a documenti digitali *offline*, dati immessi e conservati nei *social media*, messaggi di posta elettronica e via *chat*, profili *on line* personali e professionali, *accounts*,

anche nella fase *post mortem* dell'interessato, quale "prosecuzione" del diritto alla protezione dei dati personali [40]: il quesito allora che si pone attiene non tanto all'*an*, quanto al "chi" e in base a quali norme e principi spetterebbe la protezione dei dati nella fase c.d. "post mortale" [41]. Più precisamente, se è vero che con il principio di limitazione della conservazione, sancito dall'art. 5 lett. *e*), il GDPR consente sia una conservazione prolungata nel tempo dei dati qualora questi, se idonei ad identificare il soggetto interessato, siano trattati per fini di archiviazione nel pubblico interesse, statistici, di ricerca scientifica o storica, sia una protrazione del trattamento dei dati raccolti – là dove sia realizzata e garantita l'impossibilità per chiunque di procedere all'identificazione dell'interessato [42] –, è altrettanto vero che tale principio si scontra innegabilmente con il diritto all'oblio o alla cancellazione dei propri dati che l'interessato può esercitare *ex* art. 17 GDPR [43]. In altri termini, posto che la cooperativa di dati possa continuare a trattare i dati dell'*ex* membro defunto, appare doveroso chiedersi se e a chi vada riconosciuta eventualmente la legittimazione ad opporsi a tale perdurante conservazione da parte dell'ente medesimo o, in generale, ad agire per la protezione dei dati personali.

Ed invero, l'art. 2-*terdecies* (rubricato «Diritti riguardanti le persone decedute»), Codice *Privacy*, come novellato dal d.lgs. n. 101/2018 (emanato per l'adeguamento della normativa nazionale alle disposizioni del Reg. UE n. 679/2016), attribuisce in generale i diritti e i poteri di controllo sui contenuti digitali dell'interessato deceduto, a «chi abbia un interesse proprio, o agisca a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione», salvo diversa disposizione legislativa o divieto scritto, specifico, non equivoco, libero e informato dell'interessato, presentato o comunicato al titolare del trattamento [44]. In conformità, dunque, alla posizione espressa al riguardo dal Gruppo di

---

files conservati attraverso servizi di *cloud computing*: si parla al riguardo della c.d. eredità digitale. Sul punto, cfr. G. RESTA, *La successione nei rapporti digitali e la tutela post-mortale dei dati personali*, in A. MANTELERO-D. POLETTI (a cura di), *Regolare la tecnologia: il Reg. UE 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, Pisa, 2018, p. 400 s.

[40] Ancora G. RESTA, *op. ult. cit*., p. 398, dopo aver sottolineato quanto particolarmente dibattuta nel quadro dell'economia digitale sia la questione circa la "morte digitale" ed il regime dei dati personali digitali nella fase successiva alla morte dell'interessato, parla al riguardo di «*zombie* digitali» i cui dati conservati e trattati da intermediari professionali e quindi sottratti alla disponibilità di eredi e congiunti, sono peraltro oggetto di una riserva contrattuale che ne stabilisce l'intrasmissibilità *mortis causa*.

[41] Così, sempre, G. RESTA, *op. ult. cit.*, p. 402. In altri termini, si tratta di individuare e trovare un valido appiglio per la protezione postuma degli interessi dell'interessato-defunto.

[42] In tal senso, M. DELL'UTRI, *Principi generali e condizioni di liceità del trattamento dei dati personali*, in V. CUFFARO-R. D'ORAZIO-V. RICCIUTO, *I dati personali nel diritto europeo*, Torino, 2019, p. 214.

[43] Sull'argomento, cfr. *ex multis* M.A. LIVI, *Art. 17 Reg. UE n. 679/2016*, in A. BARBA-S. PAGLIANTINI (a cura di), cit., p. 292 ss. e la ricca bibliografia ivi indicata.

[44] Ai sensi dei co. 4 e 5, dell'art. 2 *terdecies* così introdotto, l'interessato ha in ogni momento il diritto di revocare o modificare il divieto e, in ogni caso, il divieto non può produrre effetti pregiudizie-

lavoro WP29 nell'Opinione n. 4/2007[45] e in termini sostanzialmente analoghi ma più circoscritti rispetto all'art. 13, Codice *Privacy*[46], l'art. 2-*terdecies* cit. contiene una disciplina non esattamente rispondente ai principi successori *mortis causa* e senz'altro giustificata dall'obiettivo di tutelare coloro ai quali possa derivare pregiudizio dalla "sopravvivenza" di tali dati[47]. Più precisamente, il legislatore italiano sembra aver adottato non tanto un modello "successorio", seppur "anomalo"[48], stante la mancanza sia di un vero e proprio acquisto *mortis causa* sia di "successori" o eredi meramente familiari, quanto piuttosto un meccanismo di «estensione»[49] in capo a terzi della tutela dei diritti dell'interessato, giustificato non soltanto da «ragioni familiari meritevoli di protezione»[50] e in forza dunque di un legame o interesse familiare[51], ma altresì da un «interesse proprio», autonomo e non derivato, oppure da quello «dell'interessato» deceduto, sulla base di un rapporto fiduciario (mandato). In altri termini, non sembra trattarsi di una vicenda acquisitiva "successoria", neppure "anomala", bensì di una legittimazione "straordinaria"[52] ad agire

---

voli per l'esercizio da parte dei terzi dei diritti patrimoniali che derivano dalla morte dell'interessato nonché del diritto di difendere in giudizio i propri interessi.

[45] In tale opinione, il Gruppo di lavoro WP29 ammette il trattamento di dati relativi a defunti allorché la legge nazionale lo consenta, oppure perché onore e immagine siano tutelati anche dopo la morte della persona.

[46] L'art. 13, co. 3, riconosceva in capo a «chiunque (avesse) interesse» il potere di esercitare i diritti *de quibus* (cancellazione, rettifica e relativa notificazione) sui dati personali concernenti persone decedute.

[47] Sul punto, v. R. RESTUCCIA, *sub art. 13*, in E. GIANNANTONIO-M.G. LOSANO-V. ZENO ZENCOVICH, *La tutela dei dati personali commentario alla L. 675/96*, Padova, 1997, p. 138.

[48] In tal senso, A. ZACCARIA, *op. cit.*, pp. 23 ss., 72, 79 s., 94 e 261 ss.; A. ZOPPINI, *Le «nuove proprietà» nella trasmissione ereditaria della ricchezza (note a margine della teoria dei beni)*, in *Riv. dir. civ.*, 2000, I, pp. 204 e 244; A. PALAZZO-A. SASSI, *Trattato della successione e dei negozi successori*, 1, *Categorie e specie della successione*, Milano, 2012, p. 83 ss.

[49] Utilizza tale espressione G. RESTA, *La successione nei rapporti digitali e la tutela postmortale dei dati personali*, cit., p. 411.

[50] La norma, sebbene in termini più generici, ricalca fortemente gli artt. 7 e 8 c.c., per la tutela del diritto al nome e alla cui stregua i rimedi (inibitori e risarcitori) possono essere esperiti «anche da chi, pur non portando il nome contestato o indebitamente usato, abbia alla tutela del nome un interesse fondato su ragioni familiari degne di essere protette» (art. 8 c.c.) e a prescindere dal fatto che sia erede oppure no.

[51] Nel Parere n. 4/2007 sul concetto di dati personali, Articolo 29 Gruppo di lavoro WP29, viene riconosciuto ai legislatori nazionali il potere di estendere le disposizioni delle leggi nazionali sulla protezione dei dati ad alcuni aspetti riguardanti il trattamento dei dati dei defunti, qualora un interesse legittimo lo giustifichi. In altri termini, è compito degli Stati membri stabilire se ed in quale misura il regolamento debba essere applicato alle persone decedute.

[52] Ciò in termini sostanzialmente analoghi alla legittimazione ad agire per l'adempimento dell'onere nella donazione o nel testamento: sul punto, cfr. A. PROTO PISANI, *Dell'esercizio dell'azione*, in *Comm. cod. proc. civ*. (diretto da E. ALLORIO), Torino, 1973, p. 1065 ss.; M. COSTANZA, *Problemi dell'onere testamentario*, in *Riv. dir. civ*., 1978, II, p. 313 ss.; G. CAPOZZI, *Successioni e donazioni*, I,

ed esercitare i diritti dell'interessato deceduto, per la protezione *post mortem* dei suoi dati personali: legittimazione indipendente dalla titolarità di situazioni giuridiche soggettive [53] ed avente fonte ora in un interesse personale o familiare, ora in un mandato *post mortem* c.d. *exequendum* [54]. Nell'ampia categoria dei legittimati ad esercitare i diritti dell'interessato defunto (nella specie, il membro della cooperativa di dati) saranno perciò compresi non soltanto i congiunti dell'interessato, ma altresì il "mandatario" – quale soggetto incaricato dall'interessato di tutelare la propria identità digitale dopo la morte – e qualunque soggetto che abbia un interesse (patrimoniale o solo morale) alla protezione (in senso ampio) dei dati personali riferiti alla persona deceduta [55]: sicché, a ben vedere, alla luce del combinato disposto degli artt. 5 GDPR e 2-*terdecies* Codice *Privacy*, la cooperativa di dati non solo potrà – in qualità di titolare del trattamento – continuare a conservare e a trattare i dati personali del membro deceduto (*ex* art. 5 *GDPR*), ma nulla sembrerebbe escludere che possa altresì ed eventualmente esercitare i diritti dell'interessato defunto in quanto soggetto avente *lato sensu* un interesse alla protezione dei dati personali di un proprio membro deceduto (*ex* art. 2-*terdecies*, Codice *Privacy*).

Milano, 2002, p. 494 s. Contro il riconoscimento dell'esercizio di determinati diritti in capo a soggetti viventi a ciò meramente legittimati, si obietta che tale ricostruzione è stata elaborata per assicurare la persistenza di diritti, privi a un certo punto di un titolare, nell'interesse di soggetti che, successivamente, li potranno acquistare, laddove, nel caso in esame non vi sarebbero soggetti che in futuro possano divenire titolari dei diritti della personalità del defunto. Ma la tesi della "legittimazione" appare senz'altro meno artificiosa e criticabile della successione c.d. "anomala", che implicherebbe regole notevolmente differenti da quelle dettate nel libro II del codice civile con riguardo alle successioni legittime.

[53] Trattasi di un'autonoma legittimazione all'esercizio dei diritti da parte di soggetti portatori di interessi qualificati, diversi da quello al quale si riferiscono i dati. In altri termini, la norma riconosce e prevede una scissione tra legittimazione (all'esercizio dei diritti e dei poteri di controllo) e titolarità dei diritti: sul punto, cfr. E. BARGELLI, *sub art. 13* (Diritti dell'interessato), in C.M. BIANCA-F.D. BUSNELLI (a cura di), *Tutela della* privacy *(legge 31 dicembre 1996, n. 675)*, in *Nuove leggi civ. comm.*, 1999, p. 416.

[54] Sull'argomento, cfr. N. DI STASO, *Il mandato* post mortem exequendum, in *Fam. pers. succ.*, 2011, p. 685; A. PALAZZO, *Le successioni*, Milano, 2000, p. 53 s. In giurisprudenza, cfr. per tutte Cass., 9 maggio 1969, n. 1584, in *Foro it.*, vol. 92, n. 12, c. 3193 ss., che ha sancito l'ammissibilità nel nostro ordinamento di un mandato *post mortem exequendum*, in quanto non in contrasto con il divieto posto alla volontà del defunto di operare *post mortem*, relativamente ai beni dell'eredità al di fuori del testamento. Con specifico riferimento al *GDPR*, si tratta di una nuova applicazione di tale mandato, propria dell'epoca contemporanea: dinnanzi all'imponente massa di dati generati dalla diffusione delle tecnologie informatiche, destinata a sopravvivere al *de cuius*, occorre gestire l'accesso a *blog*, piattaforme, *account* di posta elettronica e *social network* dell'utente dopo il suo decesso.

[55] La "sopravvivenza" e l'«esercizio post mortale» o prosecuzione dei diritti dell'interessato sono pertanto unicamente sorretti dalla *ratio* della protezione dei dati personali, in via diretta e immediata («interesse proprio» o familiare) ovvero indiretta e mediata, dando esecuzione alla volontà dell'interessato deceduto («in qualità di suo mandatario»): così, G. RESTA, *La successione nei rapporti digitali e la tutela post-mortale dei dati personali*, cit., p. 415.

4. Il Registro dei trattamenti e la nomina del DPO: obbligo o facoltà per le cooperative di dati?

L'art. 30 GDPR, poi, prevede per alcuni titolari di trattamento l'obbligo di un Registro delle attività di trattamento: una sorta di "censimento dei trattamenti", predisposto (anche) in formato elettronico, costantemente aggiornato e all'occorrenza esibito per controlli da parte dell'autorità competente, contenente varie informazioni sui trattamenti svolti, tra cui le generalità del titolare, le finalità del trattamento, le categorie di soggetti interessati (*data subjects*) e dei dati personali trattati, i destinatari della comunicazione dei dati, l'eventuale paese straniero o organizzazione internazionale a cui i dati vengono trasferiti, il momento della cancellazione dei dati e, se possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative adottate.

In un siffatto contesto, appare legittimo chiedersi se le cooperative di dati siano o meno tenute, in qualità di titolari del trattamento, alla redazione, tenuta e conservazione di tali Registri. Orbene, l'art. 30 GDPR stabilisce che siffatto obbligo non sussiste per gli enti «con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10».

A tale stregua, saranno tenute alla redazione del Registro le cooperative di dati titolari di trattamento con 250 o più dipendenti [56]; quanto a quelle con meno di 250 dipendenti, l'art. 30 GDPR contiene un'elencazione delle ipotesi di esenzione dall'obbligo, non del tutto chiara. In particolare, appare fondato ritenere che siano obbligati *ex* art. 30 GDPR gli enti titolari con meno di 250 dipendenti ma i cui trattamenti siano rischiosi per i diritti e le libertà degli interessati: ipotesi, questa, a sua volta assai estesa, perché il *considerando* n. 75 GDPR stabilisce che vi è rischio, ad esempio, quando il trattamento possa comportare discriminazioni o riguardi dati sanitari o "particolari", o ancora se implichi una valutazione della persona o si riferisca a minori o, infine, coinvolga un numero elevato di interessati. Altrettanto dicasi per gli enti con meno di 250 dipendenti e titolari di trattamenti continuativi o non occasionali, anche se non rischiosi, o aventi ad oggetto dati "particolari" (*ex* sensibili) o giudiziari. Questa interpretazione, avvalorata dal *Working Party Article 29* (oggi *European Data Protection Board*, EDPB), comporta in sostanza l'obbligo del Registro per la maggior parte degli enti che trattino dati personali per la loro attività, con meno di 250 dipendenti ma i cui trattamenti siano rischiosi per i diritti e le libertà degli interessati, continuativi o non

[56] Situazione, peraltro, difficile che si verifichi con riferimento agli enti *non profit* e considerato anche il riferimento specifico ai "dipendenti", si può tendenzialmente escludere che ai dipendenti siano equiparabili i volontari e, quindi, che siano tenuti alla redazione del Registro una ODV o un ETS per il solo fatto di aver 250 volontari o più.

occasionali e, anche se occasionali, riguardino dati "particolari" (*ex* sensibili) o giudiziari [57].

Nell'incertezza della norma e muovendo dalla considerazione che comunemente i trattamenti e le attività delle cooperative di dati possano coinvolgere (anche) diritti fondamentali o dati "sensibili", sembra comunque opportuno optare per la predisposizione e la tenuta del Registro, non solo perché l'omissione di siffatto obbligo, là dove si ritenesse sussistente, determinerebbe l'applicazione di una sanzione pecuniaria notevolmente gravosa, ma anche perché il Registro, a ben vedere, può costituire un ottimo strumento di *accountability* o "responsabilizzazione" [58] e di coo-

[57] In particolare, il *Working Party Article 29* ha precisato la natura alternativa delle deroghe, ritenendo che sia sufficiente anche una sola delle condizioni previste dall'art. 30 GDPR per determinare l'obbligo di tenuta del registro. Il Garante, poi, ha precisato che si considerano soggetti obbligati le organizzazioni con almeno 250 dipendenti quelle che, anche in presenza di un numero minore di dipendenti, effettuino trattamenti non occasionali o che possano presentare un rischio, anche non elevato, peri diritti e le libertà dell'interessato o trattamenti delle categorie particolari di dati di cui all'art. 9 GDPR. Associazioni, fondazioni, comitati e, in generale, enti senza scopo di lucro dovranno predisporre e aggiornare il registro ove trattino categorie particolari di dati e/o dati relativi a condanne penali o a reati.

[58] L'innovazione più significativa introdotta dal GDPR è senz'altro rappresentata dal riconoscimento normativo del principio di *accountability*: espressione notoriamente mutuata dai sistemi di *common law* e, come più volte sottolineato in dottrina, difficilmente traducibile se non con uno sforzo ermeneutico complesso e con locuzioni prolisse, oltreché poco efficaci, a tal punto che si preferisce continuare ad utilizzare il termine inglese. Ed invero, la parola *accountability* non esaurisce la propria funzione e il proprio contenuto nella mera "responsabilità", ma include altresì un obbligo di "rendicontazione" o "dimostrazione" «che il trattamento è effettuato conformemente al (...) Regolamento» (art. 24). Più precisamente, l'*accountability* si compone di due voci: "adozione" di misure appropriate ed efficaci per l'adempimento degli obblighi scaturenti dal Regolamento e "dimostrazione" della conformità del trattamento alle norme del GDPR. Obbligo di conformarsi e obbligo di provare la conformità del trattamento rappresentano cioè le due facce della stessa medaglia (*accountability*) in mano al *data controller*, cui è per l'appunto affidato un ruolo "proattivo" nella "valutazione" e nella conseguente "gestione" del rischio connesso al trattamento. Nelle linee guida *Governing the protection of privacy and transborder flows of personal data*, stabilite dalla OECD (*Organization for Economic Cooperation and Development*), il termine *accountability* era già presente nel 1980. In particolare, al § 14 si legge che «*a data controller should be accountable for complying with measures which give effect to the principles stated above. OECD Member countries considered it necessary to develop Guidelines which would help to harmonise national privacy legislation*».

Sul punto, cfr. G.M. RICCIO-G. SCORZA-E. BELISARIO (a cura di), *op. cit*., p. 239; G. FINOCCHIARO, *Il quadro d'insieme sul Regolamento Europeo sulla protezione dei dati personali*, cit., p. 14, nt. 38. Sulla genesi di tale principio, cfr. il Parere del Gruppo di lavoro art. 29 (noto come *WP*29), intitolato *Opinion 3/2010 on the principle of* accountability e, in dottrina, v. in particolare, G.M. RICCIO-G. SCORZA-E. BELISARIO (a cura di), *op. cit*., p. 239 s.; cfr. G. FINOCCHIARO, *Art. 24*, in E. GABRIELLI (diretto da), *Commentario del codice civile. Delle persone*, cit., p. 515 s.; ID., *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, in G. FINOCCHIARO (diretto da), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Torino 2017, p. 12 ss.; G. M. RICCIO-G. SCORZA-E. BELISARIO (a cura di), *op. cit*., pp. 61 e 236 ss. Sulla scia dei *fora* internazionali di *data protection*, si sottolinea la portata globale e assai ampia dell'obbligo di responsabilità, c.d. *overar-*

perazione con l'Autorità di controllo. Più precisamente, il Registro delle attività di trattamento rappresenta un mezzo utile a dimostrare il rispetto e la *compliance* dei dettami del *GDPR*, un documento idoneo ad attestare l'avvenuta implementazione di specifici modelli organizzativi, che assicurino l'adeguatezza dei trattamenti dei dati personali, la loro conformità al Regolamento e l'efficacia delle misure adottate. In altri termini, la tenuta del Registro consente una ricognizione delle attività svolte e si colloca in un sistema di governo trasparente, cui risulta ispirato peraltro anche il *DGA*, frutto di un nuovo approccio culturale e organizzativo fondato nel GDPR sul principio per l'appunto di "responsabilizzazione": per tali ragioni, il Garante ne raccomanda la redazione a tutti i titolari in quanto esso, fornendo piena contezza del tipo di trattamenti svolti, contribuisce non soltanto ad attuare in modo semplice ed accessibile il principio di *accountability*, ma anche perché agevola, al contempo, l'attività di controllo del Garante stesso.

Anche la figura del DPO (*Data Protection Officer*) o RDP (Responsabile della Protezione dei Dati) risulta ispirata al principio di *accountability*, in quanto misura funzionale di autocontrollo degli enti (pubblici e) privati. Trattasi, secondo il *considerando* n. 97 del GDPR, di una persona avente «conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati», che esercita un'attività di consulenza e di assistenza nei confronti del titolare del trattamento (e del responsabile), con riferimento a tutti gli obblighi che il GDPR impone. La nomina del DPO consente, cioè, di realizzare un alto livello di *compliance* al Regolamento ed evitare in tal guisa sanzioni scaturenti dalla violazione delle sue prescrizioni.

Ciò posto, appare legittimo interrogarsi sull'obbligatorietà, o mera opportunità, per una cooperativa di dati di nominare un DPO. Al riguardo, l'art. 37 GDPR stabilisce che siano obbligati a nominarlo, a parte gli enti pubblici, per quel che rileva ai nostri fini, quelli privati che hanno come attività principale [59] lo svolgimento di «trat-

---

ching concept of accountability. Nel parere n. 3 del 2010 del Gruppo di lavoro art. 29 l'*accountability* viene tradotta come responsabilità, affidabilità, assicurazione, obbligo di rendicontare.

[59] L'art. 37, par. 1, lett. *b*) e *c*), GDPR contiene un riferimento alle «attività principali del titolare del trattamento o del responsabile del trattamento». Nel *considerando* n. 97, si afferma che le attività principali di un titolare del trattamento «riguardano le sue attività primarie ed esulano dal trattamento dei dati personali come attività accessoria». Secondo il Gruppo di Lavoro Articolo 29, con "attività principali" si possono intendere le operazioni essenziali che sono necessarie al raggiungimento degli obiettivi perseguiti dal titolare del trattamento o dal responsabile del trattamento. Tuttavia, l'espressione "attività principali" non va interpretata nel senso di escludere quei casi in cui il trattamento di dati costituisce una componente inscindibile dalle attività svolte dal titolare del trattamento o dal responsabile del trattamento. Per esempio, l'attività principale di un ente per l'assistenza socio-sanitaria consiste nella prestazione di assistenza sanitaria, ma non sarebbe possibile prestare tale assistenza nel rispetto della sicurezza e in modo efficace senza trattare dati relativi alla salute, come le informazioni contenute nella cartella sanitaria di un paziente. Ne deriva che il trattamento di tali informazioni deve essere annoverato fra le attività principali di qualunque struttura di questo tipo, tenuta pertanto a nominare un RPD. Si pensi anche ad un'associazione di promozione sociale sportiva che sostiene i valori dello sport, opera per il benessere e la promozione della salute dei cittadini ed è altresì impegnata ad assicurare la corretta organizzazione e gestione delle attività sportive, il rispetto del "*fair play*", la decisa op-

tamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala»; o, ancora, gli enti privati, la cui attività principale consista «nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'art. 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10»: in generale, tutte ipotesi in cui il trattamento dei dati comporti rischi particolarmente alti e tali da imporre la nomina di un DPO.

Procedendo con ordine, le cooperative di dati saranno obbligate a nominare il DPO là dove il trattamento richieda un monitoraggio regolare e sistematico [60] degli interessati che ricorre, ai sensi del *considerando* n. 24, GDPR, allorché «le persone fisiche siano tracciate su *internet*», come nel caso del *tracking on line* (anche) per scopi comportamentali [61]: monitoraggio da intendersi quale osservazione o controllo, normalmente ma non esclusivamente, di comportamenti e da svolgersi in modo «regolare» e «sistematico», ossia, rispettivamente, continuativo o periodico e «metodico o predeterminato» [62]. Ci si intende, ad esempio, riferire al monitoraggio di

posizione ad ogni forma di illecito sportivo. L'attività principale dell'associazione è innegabilmente legata in modo inscindibile al trattamento di dati personali: ne consegue che l'associazione dovrà nominare un RPD. D'altro canto, tutti gli enti svolgono determinate attività quali la predisposizione di strutture *standard* di supporto informatico. Si tratta di esempi di funzioni di supporto necessarie ai fini dell'attività principale o dell'oggetto principale del singolo organismo, ma pur essendo necessarie o essenziali sono considerate solitamente accessorie e non vengono annoverate fra le attività principali.

[60] Il concetto di monitoraggio regolare e sistematico degli interessati non trova definizione all'interno del GDPR; tuttavia, il *considerando* 24 menziona il «monitoraggio del comportamento di detti interessati» ricomprendendovi senza dubbio tutte le forme di tracciamento e profilazione su Internet anche per finalità di pubblicità comportamentale. Testualmente, «per stabilire se un'attività di trattamento sia assimilabile al controllo del comportamento dell'interessato, è opportuno verificare se le persone fisiche sono tracciate su *internet*, compreso l'eventuale ricorso successivo a tecniche di trattamento dei dati personali che consistono nella profilazione della persona fisica, in particolare per adottare decisioni che la riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali».

[61] In tal senso, *Article 29 Data Protection Working Party* (oggi *European Data Protection Board*), *Linee guida sui responsabili della protezione dei dati*, adottate il 13 dicembre 2016 ed emendate il 5 aprile 2017, 16/IT, WP 243 rev.01.

[62] Così, *Article 29 Data Protection Working Party*, *Linee guida*, cit., 11. Più precisamente, l'aggettivo "regolare" ha almeno uno dei seguenti significati a giudizio del Gruppo di lavoro: che avviene in modo continuo ovvero a intervalli definiti per un arco di tempo definito; ricorrente o ripetuto a intervalli costanti; che avviene in modo costante o a intervalli periodici. L'aggettivo "sistematico" ha almeno uno dei seguenti significati a giudizio del Gruppo di lavoro: che avviene per sistema; predeterminato, organizzato o metodico; che ha luogo nell'ambito di un progetto complessivo di raccolta di dati; svolto nell'ambito di una strategia. Altre esemplificazioni di attività indicate dal Gruppo sono il reindirizzamento di messaggi di posta elettronica; attività di *marketing* basate sull'analisi dei dati raccolti; profilazione e *scoring* per finalità di valutazione del rischio (per esempio, a fini di valutazione del rischio creditizio, definizione dei premi assicurativi, prevenzione delle frodi, accertamento di forme di riciclaggio); tracciamento dell'ubicazione; programmi di fidelizzazione; pubblicità comportamentale; dispositivi connessi quali contatori intelligenti, automobili intelligenti, dispositivi per la domotica, ecc.

dati relativi allo stato di benessere psicofisico e alla salute attraverso dispositivi indossabili, alla localizzazione mediante *apps* su dispositivi mobili, all'utilizzo di telecamere a circuito chiuso.

Inoltre, perché una cooperativa dati sia obbligata a nominare il DPO sembra altresì necessario che il monitoraggio venga svolto su «larga scala» e, cioè, relativamente ad «una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale», con un'incidenza «su un vasto numero di interessati» potenzialmente e altamente rischiosa. Nel Regolamento non si dà alcuna definizione di trattamento su "larga scala", ma è il *considerando* n. 91 a fornire indicazioni in proposito [63] e se è pressoché impossibile individuare con esattezza la quantità di dati oggetto di trattamento o il numero di interessati in modo da coprire tutte le eventualità, è tuttavia pensabile la specificazione di alcuni *standard* utili a definire puntualmente e/o quantitativamente il concetto di "larga scala", con riguardo ad alcune tipologie di trattamento maggiormente comuni. Ed ancora una volta, è intervenuto il Gruppo di lavoro Articolo 29 che ha contribuito a delineare questi *standard*, sia raccomandando di tener conto di criteri quantitativi e qualitativi quali il numero degli interessati, l'estensione temporale (durata e persistenza) e geografica del trattamento, il volume, il numero e/o le diverse tipologie di dati oggetto di trattamento [64]; sia elencando a titolo esemplificativo alcune ipotesi di trattamento su "larga scala" come quello avente ad oggetto i dati relativi a pazienti e svolto da un ente o istituto di cura; o riguardanti gli spostamenti di utenti di un servizio (per esempio, il loro tracciamento attraverso titoli di viaggio); o ancora quello di dati di geolocalizzazione raccolti in tempo reale per finalità statistiche, ovvero personali da parte di un motore di ricerca per finalità di pubblicità comportamentale; oppure il trattamento di dati (metadati, contenuti, ubicazione) da parte di fornitori di servizi telefonici o telematici [65].

Alla luce delle considerazioni sin qui svolte, appare quindi legittimo ritenere sussistente l'obbligo di nomina del DPO per quelle cooperative di dati che, nello svolgimento della loro attività principale di condivisione di dati (nella specie) personali, svolgano un monitoraggio sistematico su larga scala dei beneficiari/desti-

---

[63] Il *considerando* in questione vi ricomprende, in particolare, «trattamenti su larga scala, che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato».

[64] *Article 29 Data Protection Working Party* ha indicato, a titolo esemplificativo, come soggetti che svolgono trattamenti su vasta scala, gli ospedali, le aziende di trasporto, le compagnie assicurative e gli istituti di credito, i fornitori di servizi di telecomunicazione.

[65] D'altro canto, lo stesso *considerando* prevede in modo specifico che «il trattamento di dati personali non dovrebbe essere considerato un trattamento su larga scala qualora riguardi dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato». Il *considerando* offre alcune esemplificazioni ai due estremi della scala (trattamento svolto dal singolo medico / trattamento di dati relativi a un'intera nazione o a livello europeo): fra tali estremi si colloca tuttavia un'ampia zona grigia.

natari della loro attività o compiano un trattamento non occasionale di dati "particolari" (*ex* sensibili) "*o*" [66] di dati giudiziari interconnessi con altri dati personali raccolti per finalità diverse.

5. *Data breach*, *policies* e misure adeguate.

Ai sensi dell'art. 12, lett. *j*) e *k*), *Digital Governance Act*, «il fornitore di servizi di intermediazione dati deve mettere in atto misure tecniche, giuridiche e organizzative adeguate al fine di impedire il trasferimento o l'accesso a *dati non personali* illegali ai sensi del diritto dell'Unione o del diritto nazionale dello Stato membro interessato; il fornitore di servizi di intermediazione dati informa senza ritardo i titolari dei dati in caso di trasferimento, accesso o utilizzo non autorizzati dei *dati non personali* che ha condiviso».

Tali disposizioni fanno esplicito riferimento ai dati non personali; per quelli personali, le cooperative di dati saranno dunque soggette, ancora una volta, alle norme del *GDPR* e, in forza del noto principio di *accountability*, esse, in qualità di titolari di trattamento, dovranno garantire un'adeguata sicurezza e protezione dei dati personali, adottando *policies* e procedure idonee al caso concreto, tra le quali vi è sicuramente quella per la gestione di un'eventuale "*data breach*" [67]. Si tratta di una procedura volta a stabilire *a priori* come affrontare la malaugurata ipotesi di una violazione della sicurezza dei dati [68]: si pensi al caso in cui i dati trattati dalla cooperativa, per errore umano o a seguito di un attacco informatico, vengano accidentalmente persi o comunicati a soggetti non autorizzati.

L'ente dovrà quindi dimostrare di aver adottato e costantemente aggiornato tutte le misure tecniche e organizzative atte a garantire il raggiungimento di un livello di sicurezza adeguato ai rischi: il problema, allora, non attiene all'*an*, bensì al *quomodo* della dimostrazione. Al riguardo, non v'è dubbio che qualunque trattamento in-

---

[66] Il testo italiano reca già la congiunzione "o", diversamente dal Regolamento. Sebbene infatti l'art. 37, par. 1, lett. *c*), del Regolamento menzioni il trattamento di categorie particolari di dati ai sensi dell'art. 9 e di dati personali relativi a condanne penali e a reati di cui all'art. 10, nonostante cioè l'utilizzo della congiunzione "e" nel testo, non è apparsa sistematicamente fondata l'applicazione simultanea dei due criteri: il testo, pertanto, è stato più correttamente interpretato e tradotto come se recasse la congiunzione "o".

[67] Per *data breach* o violazione dei dati personali (artt. 4 e 33 GDPR) si intende una violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzato o l'accesso ai dati personali. Si tratta quindi della perdita, del danneggiamento o della fuoriuscita di dati o dell'accesso illecito anche indipendente dalla volontà dell'ente (anche la perdita di una chiavetta USB, il furto del PC, la cancellazione di un archivio dati, l'accesso al computer di estranei, ecc.).

[68] La procedura ha il vantaggio di facilitare le valutazioni che, in questo caso, si rendono necessarie per poter poi adempiere agli obblighi previsti dal Regolamento (annotazione della violazione nell'apposito registro, eventuale notifica al Garante e comunicazione agli interessati).

formatico di dati non possa ormai prescindere dall'adozione di "misure minime", da quelle fisiche e banali – quali la corretta conservazione dei documenti cartacei contenenti i dati – a quelle tecniche ed informatiche come *password* di accesso, sistemi antivirus e di *backup*, ecc. In generale, il GDPR riconosce e attribuisce al titolare del trattamento il potere di scegliere modalità e strumenti di attuazione delle prescrizioni europee a fronte dell'obbligo di dimostrarne l'adeguatezza rispetto al caso concreto. *Pro* e contro, dunque: da un lato, discrezionalità e diritto di scelta e, dall'altro, incertezza della "bontà" dell'operato e delle valutazioni effettuate fino all'eventuale esame da parte dell'autorità giudiziaria o amministrativa. L'*accountability* segna quindi il passaggio da una tutela *ex post* dei dati, propria della disciplina previgente e operante in funzione rimediale sulle violazioni e sui relativi danni, ad una protezione *ex ante* o preventiva tipica del GDPR e basata «sull'esame prudenziale di tutte le attività di trattamento»[69] sin dalla fase iniziale. Il parametro fondamentale che deve presiedere all'adempimento degli obblighi scaturenti dal Regolamento sembrerebbe, dunque, la diligenza del *bonus pater familias* (per così dire) "informatico", formula che riassume la misura dello sforzo o impegno "adeguato" richiesto, in questo caso, all'ente in quanto titolare del trattamento per rispettare il Regolamento[70]. La cooperativa, in quanto «titolare del trattamento», dovrà «mette(re) in atto misure tecniche e organizzative adeguate[71] per garantire, ed

---

[69] Così, L. GRECO, *I ruoli: titolare e responsabile*, in G. FINOCCHIARO (diretto da), *Il nuovo Regolamento europeo sulla* privacy *e sulla protezione dei dati personali*, cit., p. 254.

[70] M. RATTI, *op. cit.*, p. 620, suggerisce che la diligenza richiesta al titolare e al responsabile del trattamento sia "qualificata", stante l'inciso di cui all'art. 82 GDPR, secondo il quale l'evento dannoso non deve essere «in alcun modo» imputabile al danneggiante per liberarsi da responsabilità: di conseguenza, la presenza anche della colpa lieve sarebbe idonea a determinare la sussistenza del nesso materiale tra condotta del titolare danneggiante ed evento dannoso. In generale, sulla nozione e sulle graduazioni della colpa, cfr. in particolare, C. TURCO, *Diritto civile*, I, Torino 2014, p. 363 s. La diligenza, quindi, unitamente alla perizia e alla competenza, sembra rappresentare la regola e, al contempo, il criterio di valutazione del comportamento dell'ente e di imputazione della responsabilità, non in base alle capacità possedute dal medesimo, ma secondo un modello oggettivo e astratto, corrispondente a quello ordinario, oltreché in virtù delle caratteristiche e delle esigenze del trattamento in concreto effettuato: pertanto, sembra sufficiente per escludere l'imputabilità e la responsabilità tendenzialmente "colposa" o "soggettiva" la violazione del Regolamento dipendente da un'impossibilità analogamente soggettiva e cioè caratterizzata dall'assenza di colpa o negligenza, pur se collegata a circostanze attinenti alla sfera di controllo e organizzazione del titolare del trattamento (comunque incolpevole).Per converso, un comportamento debitorio immune da colpa o negligenza non impedirebbe un'imputabilità e una responsabilità per colpa senza colpa o oggettiva, che verrà meno solo nel caso in cui la violazione del Regolamento dovuta ad un'impossibilità parimenti oggettiva di adempiere: non solo indipendentemente da colpa o negligenza, ma causata da eventi estranei alla sfera di controllo e di organizzazione (nella specie) del titolare del trattamento e non rientranti nel rischio tipico inerente all'attività svolta dal titolare del trattamento, imprevedibile ed eccezionali (c.d. caso fortuito: si pensi ad es. ad un totale e prolungato *black out* elettrico), ovvero ineludibili ed insuperabili (c.d. forza maggiore).

[71] Il Regolamento richiama molte volte il concetto di "adeguatezza", necessariamente relativo e

essere in grado di dimostrare, che il trattamento è effettuato conformemente al (...) Regolamento» (art. 24 GDPR). Il Regolamento affida quindi alla discrezionalità del titolare del trattamento, nella specie l'ente, la decisione sulle misure da adottare: discrezionalità libera ma non illimitata, anzi necessariamente parametrata alle condizioni indicate nello stesso art. 24 GDPR, quali la natura, l'àmbito di applicazione, il contesto e le finalità del trattamento, nonché il rischio di lesione dei diritti e delle libertà delle persone fisiche [72]. In altri termini, non vengono astrattamente specificati rigidi comportamenti, ma viene piuttosto assegnato al titolare il compito di scegliere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali: il tutto nel rispetto delle disposizioni normative e alla luce dei criteri indicati nel GDPR. Il Regolamento, infatti, non prevede un elenco esaustivo né tassativo di "misure adeguate", ma si limita ad indicarne alcune. Ciò significa che l'ente titolare del trattamento potrà mettere in atto non solo le misure adeguate "tipiche", già preconfigurate dal legislatore europeo, ma anche nuove o "atipiche" che non rientrino tra quelle normativamente previste, purché nel rispetto dei requisiti fissati dal Regolamento: il che rappresenta la massima espressione ed estrinsecazione del principio di *accountability* e dell'autonomia riconosciuta al titolare del trattamento.

Prima, però, di procedere ad una sia pur breve illustrazione delle misure tecniche e organizzative suggerite dal Regolamento, appare opportuno soffermarsi sul diverso atteggiarsi dell'*accountability* e dell'onere probatorio gravante sull'ente in quanto titolare del trattamento, a seconda che questo abbia adottato misure tipiche o, al contrario, innominate. Per le prime sembra legittimo ritenere sussistente una presunzione relativa [73] di conformità al Regolamento, nel senso che il titolare del trattamento dovrà semplicemente provarne l'adozione, non anche il rispetto degli obblighi imposti dal GDPR, valutato *ex ante* dal legislatore europeo; laddove, trattandosi di misure per così dire atipiche o innominate, in quanto non previste nel Regolamento, l'ente titolare del trattamento dovrà dimostrarne non solo l'adozione (l'*an*), ma altresì la conformità ai principi e l'adeguatezza (*quomodo*): il che sembra suggerito dallo stesso art. 24 GDPR che menziona alcune misure quali «i codici di condotta di cui all'art. 40» e i «meccanism(i) di certificazione di cui all'art. 42»,

---

relazionale, da intendersi come capacità di soddisfare una qualità o un risultato posto come obiettivo. "Adeguatezza" equivale ad "accettabilità" in termini sia tecnici (pertinenza delle misure), sia qualitativi (efficacia della protezione): sul punto, v. G.M. RICCIO-G. SCORZA-E. BELISARIO (a cura di), *GDPR e normativa* Privacy *commentario*, cit., p. 297.

[72] La valutazione di adeguatezza delle misure va condotta *ex ante* e in concreto in una prospettiva prognostica e soggetta ad aggiornamenti. I parametri essenziali di tale valutazione forniti dal GDPR sono: natura, àmbito applicativo, contesto e finalità del trattamento, rischi possibili.

[73] *Contra*, G.M. RICCIO-G. SCORZA-E. BELISARIO (a cura di), *GDPR e normativa* Privacy *commentario*, cit., p. 63, che riconoscono nelle misure indicate dal Regolamento elementi utili a dimostrare l'adempimento degli obblighi del titolare e, quindi, l'*accountability*, ma non rappresentano presupposti per una vera e propria presunzione legale, neppure relativa, di conformità al GDPR della condotta del titolare.

definendole «element(i)» atti a «dimostrare il rispetto degli obblighi del titolare del trattamento», ivi inclusa l'adeguatezza delle misure tecniche e organizzative di sicurezza adottate [74].

Tra le «misure tecniche e organizzative adeguate (...) volte ad attuare in modo efficace i principi di protezione dei dati», menzionate dal Regolamento, si colloca anzitutto la "pseudonimizzazione" [75] (art. 25) definita all'art. 4 come insieme di operazioni idonee ad evitare che i dati personali «possano (...) essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile». Trattasi, in sostanza, di uno strumento in grado di rendere più difficile l'identificazione dell'interessato e la diretta riconducibilità a quest'ultimo delle informazioni personali: al termine del trattamento, i dati non potranno più essere ricollegati o riassociati ad una persona determinata se non mediante dati e informazioni ulteriori, oggetto di separata archiviazione e protezione [76]. In termini pratici, la "pseudonimizzazione" maschera l'identità di un soggetto mediante sia la sostituzione di un dato personale, solitamente univoco, con un altro dato per l'appunto "pseudonimo" – anch'esso univoco, ma non immediatamente intellegibile né direttamente identificativo (un codice, un numero di protocollo) [77] – sia la separazione di tali informazioni aggiuntive; *in secundis*, essa consente, in circostanze predefinite, di riassociare il dato alla persona, ossia di risalire all'identità dell'interessato, utilizzando (a ritroso) le informazioni aggiuntive.

Altro strumento normativamente "adeguato" alla protezione dei dati personali è previsto dal medesimo art. 25 ed è individuato con l'espressione *privacy by default*: trattasi di un rimedio volto a proteggere l'interessato dal rischio di perdere consapevolezza o controllo circa l'utilizzo delle proprie informazioni personali [78]. Adot-

---

[74] In senso conforme, G. FINOCCHIARO, *Art. 24*, in E. GABRIELLI (diretto da), *Commentario del codice civile. Delle persone*, cit., p. 518. Sull'argomento, v. G.M. RICCIO-G. SCORZA-E. BELISARIO (a cura di), *op. cit*., p. 62. Le misure atipiche dovranno in concreto superare una duplice valutazione, relativa alla loro adozione e conformità, e quindi all'adeguatezza, rispetto alle caratteristiche concrete dei dati e del trattamento, nonché al suo impatto e ai rischi che possa determinare per i diritti e le libertà degli interessati.

[75] Il processo di pseudonimizzazione sembra consistere nella formazione di due insiemi parziali di informazioni: il primo raggruppa dati e contiene lo pseudonimo e i dati che permettono l'identificazione; il secondo, complementare al primo, raccoglie pseudonimi e dati personali, senza tuttavia consentire l'identificazione degli interessati. Il processo di pseudonimizzazione consente di riassociare i dati: sul punto, cfr. M. MONTANARI, *Art. 25*, in E. GABRIELLI (diretto da), *Commentario del codice civile. Delle persone*, cit., p. 535 ss.

[76] Ad esempio, mediante l'utilizzo di criptografia a chiavi simmetriche o asimmetriche.

[77] Al riguardo, cfr. G.M. RICCIO-G. SCORZA-E. BELISARIO (a cura di), *GDPR e normativa Privacy commentario*, cit., p. 251 s.: codici "inintellegibili" in luogo della reale identità degli individui.

[78] In realtà, ai sensi dell'art. 25, la protezione dei dati deve essere garantita fin dalla progettazione

tando tale misura, l'ente titolare garantirà, «per impostazione predefinita» (art. 25) e in ossequio al c.d. principio di "minimizzazione" [79], che siano trattati soltanto i dati personali necessari per ciascuna finalità specifica del trattamento: ciò attraverso l'utilizzo di impostazioni in automatico, scelte, predisposte e preselezionate da parte del titolare del trattamento o di chi costruisce il sistema informatico, in guisa da «garantire scelte di *default* orientate verso soluzioni di massima protezione dei dati» [80].

Come già rilevato [81], anche il registro delle attività di trattamento prescritto dall'art. 30 rappresenta una misura normativamente tipica volta a dimostrare la rispondenza del trattamento posto in essere dal titolare ai dettami del Regolamento. Più precisamente, per provare la piena conformità del trattamento al Regolamento, l'ente titolare (del trattamento) che tenga l'apposito registro riuscirà a rendicontare e comprovare l'adeguatezza, la conformità al Regolamento e l'efficacia delle misure adottate. La rendicontazione *ex* art. art. 30 *GDPR* non può considerarsi, quindi, un mero adempimento formale, bensì un mezzo tecnico efficace e pertinente per la corretta gestione dei dati personali.

L'art. 35, poi, disciplina la "preventiva valutazione di impatto sulla protezione dei dati personali" (c.d. DPIA o *Data Privacy Impact Assessment*) che, insieme agli altri mezzi o strumenti sin qui elencati, e in particolare al registro delle attività di trattamento, costituisce un congegno significativo e concreto per garantire e fornire la prova, da parte del titolare, della conformità del trattamento al GDPR. Essa è finalizzata anzitutto a stimare, in relazione alla probabilità e gravità, i rischi per i diritti e le libertà delle persone fisiche a seguito del trattamento di dati; in secondo luogo, lo strumento di DPIA mira alla definizione delle misure idonee ad escludere o ridurre siffatti rischi. Analogamente al registro delle attività di trattamento, esso – richiesto soltanto per quei trattamenti che presentano un rischio elevato per i diritti e le libertà delle persone fisiche – non rappresenta la tappa obbligatoria di un *iter* burocratico, bensì un sistema di gestione del suddetto rischio, utile per "minimizzarlo" o addirittura eliminarlo.

(c.d. *privacy by design*) e per impostazione predefinita (c.d. *privacy by default*): il titolare è chiamato ad implementare misure in grado di proteggere efficacemente i dati personali al momento della progettazione di processi e modelli di trattamento, e a garantire il rispetto del principio di necessità, nel corso dell'esecuzione del trattamento.

[79] Com'è noto, l'art. 5, par. 1, lett. *c*), impone che i dati siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per i quali sono trattati. Il principio di minimizzazione si compone dunque di due "voci": necessità e pertinenza. La prima consiste nella limitazione del trattamento ai soli dati indispensabili per la realizzazione della finalità o scopo del trattamento; la seconda attiene alla funzionalità del dato rispetto allo scopo perseguito, in base ad un nesso eziologico che deve permanere durante tutto il trattamento. Sul principio di minimizzazione, v. tra gli altri G.M. RICCIO-G. SCORZA-E. BELISARIO (a cura di), *op. ult. cit*., p. 57 s.; D. ACHILLE, *Art. 5*, in E. GABRIELLI (diretto da), *Commentario del codice civile. Delle persone*, cit., p. 110 s.

[80] Così, L. GRECO, *I ruoli: titolare e responsabile*, in G. FINOCCHIARO (diretto da), *op. cit.*, p. 256.

[81] V., *supra*, par. 4.

Il Regolamento, inoltre, riconosce efficacia probatoria – circa la conformità del trattamento di dati effettuato dal titolare – ai codici di condotta [82], rispondenti ai requisiti di cui agli artt. 40 e 41. In particolare, la sottoscrizione di un codice costituisce, per espressa disposizione legislativa, elemento atto a dimostrare il rispetto degli obblighi che gravano sul titolare del trattamento e la sussistenza di misure tecniche e organizzative adeguate a *garantirne* la sicurezza. Com'è intuibile, trattasi di codici di comportamento elaborati con il supporto delle associazioni rappresentative e degli organismi esponenziali delle rispettive categorie, allo scopo di integrare i principi generali della disciplina e di adattarli allo specifico ambito o tipologia di trattamento. La funzione dei codici è infatti attuativa e allo stesso tempo complementare; la loro conformità al GDPR è subordinata alla previsione di meccanismi procedurali mediante i quali l'organismo di controllo vigila sul rispetto dei codici medesimi da parte dei soggetti obbligati. Le disposizioni sui codici di condotta sono strettamente correlate a quelle sulla certificazione e sugli organismi privati a ciò abilitati, di cui agli artt. 42 e 43 GDPR. Sulla scia del *risk based approach*, le certificazioni previste dall'art. 42 costituiscono uno strumento a disposizione del titolare del trattamento, nella specie la cooperativa di dati, per valutare l'adeguatezza degli *standards* adottati. Ai sensi dell'art. 42, «gli Stati membri (...) incoraggiano l'istituzione di meccanismi di certificazione (...) allo scopo di dimostrare conformità al Regolamento dei trattamenti effettuati dai titolari di trattamento». Trattasi di una certificazione, rilasciata direttamente dal Garante – o da organismi di certificazione preventivamente accreditati – a seguito di una procedura volontaria di valutazione di conformità. Orbene, come già sottolineato e analogamente ai codici di condotta, la presenza di una certificazione determina di per sé una presunzione di conformità e adeguatezza degli *standards* adottati dal titolare del trattamento con i parametri del Regolamento.

6. Cooperative di dati e *Digital Service Act.*

Come già rilevato [83], la disciplina delle cooperative di dati – in quanto fornitori di servizi di intermediazione di dati [84] – va ricostruita anche alla luce del Regolamento UE 2022/2065, il *Digital Service Act* o DSA che, com'è noto, ha introdotto obblighi di prevenzione e mitigazione in capo ai prestatori di servizi intermediari

---

[82] Per un approfondimento sul tema, v. in particolare, A.R. POPOLI, *Codici di condotta e certificazioni*, in G. FINOCCHIARO (diretto da), *op. cit*., p. 367 ss.

[83] V., *supra*, par. 1.

[84] Sull'argomento, cfr. F. BRAVO, *Intermediazione di dati personali e servizi di* data sharing *dal* GDPR *al* Data Governance Act, in *Contratto e impresa Europa*, 2021, 1, p. 199 ss.; LIONELLO, *La creazione del mercato europeo dei dati: sfide e prospettive*, in *Diritto del Commercio Internazionale*, 2021, 3, p. 675; T. SCHOLTZ, *Platform Cooperativism. Challenging the Corporate Sharing Economy*, New York, 2016.

on line o piattaforme *on line*, in parte a prescindere dalle loro dimensioni ed in parte esclusivamente a carico di piattaforme digitali di grandi dimensioni. Il DSA è destinato, infatti, ad applicarsi a tutti i servizi intermediari che trasmettono o memorizzano informazioni: non solo mercati *online* e *app store*, ma altresì piattaforme c.d. dell'economia collaborativa [85], tra le quali – per l'appunto – sembra corretto collocare i servizi di cooperative di dati. Queste ultime, nel ruolo di fornitori dei servizi di condivisione, anche quando operano nel mercato dei dati personali, mettono in relazione il «titolare dei dati» (c.d. *data holder*) con l'utilizzatore dei dati (c.d. *data user*), offrendo servizi a valore aggiunto, con cui scalfire il ruolo dominante assunto dalle multinazionali d'oltreoceano. Tramite le cooperative di intermediazione dati, i "titolari dei dati" colgono le opportunità dell'intermediazione concedendone l'accesso e l'utilizzo nei confronti di altri soggetti, gli "utenti dei dati" [86].

In particolare, ai sensi dell'art. 10 DGA, tra i servizi di intermediazione dati vengono menzionati quelli definiti dall'art. 2, n. 15, DGA, come quei «servizi di intermediazione dei dati offerti da una struttura organizzativa costituita da interessati, imprese individuali o PMI membri di tale struttura, aventi come obiettivo principale quello di supportare i propri membri nell'esercizio dei loro diritti rispetto a determinati dati, anche per quanto riguarda l'effettuazione di scelte informate prima di acconsentire al trattamento dei dati, per scambiare opinioni sugli scopi e sulle condizioni del trattamento dei dati che rappresenterebbero al meglio gli interessi dei suoi membri in relazione ai loro dati e per negoziare termini e condizioni per i dati trattamento per conto dei propri iscritti prima di dare il consenso al trattamento dei dati non personali o prima che questi acconsentano al trattamento dei dati personali».

Sotto il profilo soggettivo, il *Digital Services Act* non si limita, dunque, ad ope-

---

[85] Con l'espressione "economia collaborativa" si intende un insieme ampio e variegato di pratiche, accomunate essenzialmente dall'utilizzo del "modello piattaforma" e delle tecnologie digitali per mettere in contatto le persone, abilitare scambi e collaborazione. Le risorse scambiate possono essere di vario tipo: beni, risorse materiali e immateriali, competenze, conoscenze e, per l'appunto, dati, messi a disposizione di potenziali interessati per massimizzarne il valore e l'utilità sociale. Il c.d. *platform cooperativism* nasce per offrire un'alternativa (cooperativa) al fenomeno del *platform capitalism* e mira a mantenere la tecnologia come cuore pulsante del modello piattaforma, ma trasforma la *governance* affidandola ad un'organizzazione di tipo cooperativo. Sull'argomento, cfr. in particolare, R. BOTSMAN-R. ROGERS, *What's Mine is Yours: The Rise of Collaborative Consumption*, New York, 2010; E. COMO-F. BATTISTONI, *Economia collaborative e innovazione nelle imprese cooperative: opportunità emergenti e sfide per il futuro*, in *Impr. soc.*, 2015, p. 98 ss.

[86] Il "titolare dei dati" (*data holder*), secondo la terminologia del DGA, è «la persona giuridica o l'interessato che, conformemente al diritto dell'Unione o nazionale applicabile, ha il diritto di concedere l'accesso a determinati dati personali o non personali sotto il proprio controllo o di condividerli». La condivisione dei dati consente infatti all'interessato, neonominato "titolare dei dati", di concederne l'accesso o l'utilizzo all' "utente dei dati" (*data user*), ossia alla «persona fisica o giuridica che ha accesso legittimo a determinati dati personali o non personali ed è autorizzata a utilizzare tali dati a fini commerciali o non commerciali» (art. 2, DSA). In base al GDPR, l'utente dei dati personali altri non è che il titolare del trattamento.

rare per le sole grandi piattaforme, ma si estende a tutte le categorie di imprese, incluse le microimprese e le piccole imprese, che peraltro, alla luce del DGA, possono essere membri di una cooperativa di dati; sotto il profilo oggettivo, il DSA opererà per tutti i prestatori di servizi intermediari di dati, operanti *lato sensu* nell'Unione Europea, indipendentemente dal loro luogo di stabilimento o di residenza e sulla base di un "collegamento sostanziale" con l'Unione stessa: "collegamento sostanziale" sussistente non soltanto là dove le cooperative o comunque i prestatori di servizi di intermediazione di dati siano stabiliti in uno Stato membro dell'Unione ma, in mancanza di tale stabilimento, in virtù dell'esistenza di un numero considerevole di utenti in uno o più Stati membri o dell'"orientamento" delle attività verso uno o più Stati membri. L'"orientamento" delle attività verso uno o più Stati membri può essere determinato sulla base di tutte le circostanze pertinenti, quali l'uso di una lingua o di una moneta generalmente usata nello Stato membro in questione, la possibilità di ordinare prodotti o servizi oppure l'utilizzo di un dominio di primo livello nazionale [87].

La stretta connessione tra DGA e DSA risulta confermata dallo stesso DGA (*Digital Governance Act*), all'art. 12, rubricato come «Condizioni per la fornitura di servizi di intermediazione dati» e contenente una serie di obblighi per la prestazione dei servizi di intermediazione dati, che richiamano e ricalcano chiaramente quelli dettate dal DSA ed i principi in esso contenuti quali la trasparenza, la pubblicità e l'accesso ai dati, nonché il divieto di contenuti illeciti.

Trattasi di obblighi, com'è noto, aventi ad oggetto misure per contrastare i contenuti illegali *online* e l'obbligo per le piattaforme (nella specie) di intermediazione di dati di reagire rapidamente, nel rispetto dei diritti fondamentali, come la libertà di espressione e la protezione dei dati; il potenziamento della tracciabilità e dei controlli sugli operatori commerciali nei mercati *online* per garantire la sicurezza dei prodotti e dei servizi, e impegno a effettuare controlli casuali dell'eventuale ricomparsa di contenuti illegali; più trasparenza e responsabilità delle piattaforme, ad esempio mediante la messa a disposizione di informazioni chiare sulla moderazione dei contenuti o sull'uso di algoritmi per la raccomandazione di contenuti (i c.d. sistemi di raccomandazione [88]); la possibilità per gli utenti di contestare le decisioni

[87] L'"orientamento" delle attività verso uno Stato membro potrebbe anche desumersi dalla disponibilità di un'applicazione nell'apposito sito *online* nazionale, dalla fornitura di pubblicità a livello nazionale o nella lingua usata nello Stato membro in questione o dalla gestione dei rapporti con i membri della struttura organizzativa, ad esempio la fornitura di assistenza nella lingua generalmente parlata in tale Stato membro.

[88] I "sistemi di raccomandazione" sono definiti come «sistemi interamente o parzialmente automatizzati che una piattaforma *online* utilizza per suggerire informazioni specifiche, tramite la propria interfaccia *online*, ai destinatari del servizio o per mettere in ordine di priorità dette informazioni anche quale risultato di una ricerca avviata dal destinatario del servizio o determinando in altro modo l'ordine relativo o l'importanza delle informazioni visualizzate». In base agli artt. 27 e 38 DSA, tutti i fornitori di piattaforme *online* (anche) di dati dovranno specificare nelle condizioni generali i principali parametri utilizzati nei propri sistemi di raccomandazione, al pari delle opzioni a disposizione dei

di moderazione dei contenuti; il divieto di pratiche ingannevoli e di alcuni tipi di pubblicità mirata, come quella rivolta ai minori.

In base al DSA, le piattaforme e gli intermediari di dati *on line* saranno soggetti a quelli proporzionati alla natura dei servizi da loro offerti, nonché alla loro dimensione e al loro impatto. Le piattaforme (ed i motori) *online* di dimensioni molto grandi [89] dovranno rispettare requisiti «supplementari» e più rigorosi, dai quali sono invece esentate le microimprese di piccole e medie dimensioni (PMI), intendendo per tali – secondo la definizione contenuta nella Raccomandazione 2003/361/CE della Commissione – quelle costituite con meno di 250 persone, il cui fatturato annuo non superi i cinquanta milioni di euro, oppure il cui totale di bilancio annuo non oltrepassi i quarantatré milioni di euro: ciò, «a meno che, in ragione del loro raggio d'azione e del loro impatto, esse non soddisfino i criteri per qualificarsi come piattaforme *online* di dimensioni molto grandi ai sensi del regolamento» medesimo. In altri termini, il Regolamento sui servizi digitali definisce una serie di obblighi per così dire "base" per tutti i fornitori di servizi digitali (inclusi, nella specie, quelli di intermediazione di dati) e, altresì, obblighi peculiari riservati a quelli di grandi dimensioni. In particolare, il Capo III definisce in cinque sezioni diverse gli obblighi di diligenza per un ambiente *online* trasparente e sicuro. Vengono, anzitutto, stabiliti gli obblighi applicabili indistintamente a tutti i prestatori di servizi intermediari (anche) di dati, a prescindere dalle loro dimensioni: l'obbligo di istituire un punto di contatto unico per agevolare la comunicazione diretta con le autorità degli Stati membri, la Commissione e il comitato; l'obbligo di designare un rappresentante legale nell'Unione Europea per i prestatori che non sono stabiliti in uno Stato membro, ma offrono i propri servizi nell'Unione stessa; l'obbligo di indicare nelle proprie condizioni generali eventuali restrizioni all'uso dei propri servizi e di agire in maniera responsabile nell'applicare e nel far rispettare tali restrizioni; obblighi di comunicazione trasparente per quanto riguarda la rimozione delle informazioni che siano considerate illegali o contrarie alle condizioni generali dei prestatori e la disabilitazione dell'accesso a tali informazioni.

Seguono gli obblighi applicabili a tutte le piattaforme *online*, ad eccezione di

---

destinatari per modificare o influenzare tali parametri e quelli di dimensioni molto grandi dovranno altresì «assicura(re) almeno un'opzione per ciascuno dei loro sistemi di raccomandazione, non basata sulla profilazione come definita nell'articolo 4, punto 4), del regolamento (UE) 2016/679»: chiarire all'utente la logica alla base di tale attività di raccomandazione è senz'altro il primo passo per garantirgli un maggiore controllo.

[89] Ai sensi dell'art. 33 DSA, sono piattaforme *online* e motori di ricerca *online* di dimensioni molto grandi quelli che hanno un numero medio mensile di destinatari attivi del servizio nell'Unione pari o superiore a 45 milioni e che sono designati come piattaforme *online* di dimensioni molto grandi o motori di ricerca *online* di dimensioni molto grandi a norma del par. 4, ossia sulla base di una decisione adottata dalla Commissione, previa consultazione dello Stato di stabilimento e alla luce dei dati comunicati dal fornitore della piattaforma *online* o del motore di ricerca *online* a norma dell'art. 24, par. 2, o delle informazioni richieste a norma dell'art. 24, par. 3, e di qualsiasi altra informazione a sua disposizione.

quelle qualificabili come microimprese o piccole imprese ai sensi dell'allegato della Raccomandazione 2003/361/CE. Trattasi dell'obbligo per le piattaforme *online* (anche) di intermediazione di dati di istituire un sistema interno di gestione dei reclami relativi alle decisioni adottate in relazione a presunti contenuti o informazioni illegali incompatibili con le loro condizioni generali; di rivolgersi a organismi certificati di risoluzione extragiudiziale delle controversie con gli utenti dei loro servizi; di adottare misure in caso di abusi.

Vi sono, infine, obblighi supplementari (oltre a quelli sin qui elencati) a carico delle piattaforme *online* di dimensioni molto grandi (come definite dall'art. 33 DSA) per la gestione dei rischi sistemici – quali la diffusione di contenuti illegali, gli effetti negativi sui diritti fondamentali, sui processi elettorali e sulla violenza di genere o sulla salute mentale – derivanti dal funzionamento e dall'uso dei loro servizi o connessi a tale uso e funzionamento, adottando misure ragionevoli ed efficaci per l'attenuazione di tali rischi. Questi includono la prevenzione di rischi sistemici, la sottoposizione ad *audit* indipendenti, la possibilità per gli utenti di scegliere di non ricevere raccomandazioni basate sulla profilazione ed anche l'accesso ai propri dati e algoritmi da parte delle autorità e dei ricercatori autorizzati.

Capitolo VII

Le cooperative di dati nel mercato digitale. I principi a salvaguardia dei dati nel modello mutualistico

Elisabetta Posmon

Abstract: By placing data cooperatives within the model of European social market economy, this contribution highlights the benefits of applying the mutual model to the data market. The aim is to underline the capability of Data Cooperatives to operate in accordance with the dictates of solidarity, democracy and sustainability, in order to emphasize the invaluable advantages that the citizens and the enterprises of the Europea Union can derive in entrusting their data to this organizational form.

1. I servizi di cooperative di dati tra promozione del mercato digitale, *privacy* e tutela delle informazioni personali.

L'art. 10 del Regolamento (UE) n. 868/2022 sulla *European Data Governance* (d'ora innanzi DGA) estende la disciplina della fornitura di servizi di intermediazione dei dati, ai servizi di cooperative di dati.

Il *Data Governance Act* costituisce un pilastro fondamentale della strategia per i dati, annunciata dalla Commissione europea nella Comunicazione del 19 febbraio 2020 [COM(2020) 66 final], seguita dall'adozione del *Data Act* con il Regolamento (UE) n. 2854/2023 sull'accesso equo ai dati e sul loro utilizzo, che sarà operativo dal 12 settembre 2025.

Attraverso la strategia per i dati l'Unione europea intende mettere a frutto il potenziale economico dei dati personali e non personali, a beneficio dell'intera comunità e fare dell'Europa una *leader* nell'economia mondiale dei dati.

A questo scopo, nel considerando n. 3 del DGA il legislatore europeo si richiama alla necessità di «(…) migliorare le condizioni per la condivisione dei dati nel mercato interno, creando un quadro armonizzato per gli scambi di dati e stabilendo alcuni requisiti di base per la *governance* dei dati».

La legge sulla governance europea dei dati regola i procedimenti e le strutture organizzative per migliorare la condivisione dei dati nel mercato interno, creando un quadro di norme e pratiche comuni agli Stati membri per gli scambi di dati, avente come fine di accrescere la fiducia tra gli individui e le imprese per quanto riguarda la loro condivisione e il riutilizzo.

L'art. 1 del DGA individua l'ambito oggettivo di applicazione del regolamento nel riutilizzo dei dati raccolti dagli enti pubblici, nella fornitura di servizi di intermediazione di dati, nell'altruismo dei dati e nell'istituzione di un comitato europeo per l'innovazione in materia di dati e altruismo dei dati.

Nel caso delle cooperative di dati, i servizi di intermediazione di dati sono offerti da strutture organizzative a carattere mutualistico, costituite da interessati, imprese individuali e PMI.

All'interno del regolamento, delle cooperative di dati è fatta espressa menzione nel considerando n. 31, dove sono enunciati alcuni tra gli obiettivi principali affidati a questa forma organizzativa, accanto a quelli richiamati sotto la definizione di servizi di cooperative di dati presente all'art. 2, par. 1, n. 15 del regolamento (Reg. UE 868/2022)[1].

Proprio con riferimento alle *data cooperatives*, nel *considerando* 31 del DGA il legislatore europeo sottolinea l'importanza di riconoscere che i diritti a norma del regolamento generale sulla protezione dei dati (Reg. UE n. 679/2016) sono diritti personali dell'interessato e che quest'ultimo non può rinunciarvi, mantenendo fede alla visione strategica di incoraggiare lo sviluppo di una società e di una economia dei dati antropocentriche.

Non sfugge d'altra parte la costante tensione tra il perseguimento di interessi economici e la volontà di accrescere la competitività dei mercati, da un lato, e la tutela della persona, dall'altro, espressione dell'indirizzo personalista a cui la politica dell'Unione non vuole rinunciare, anche a fronte del valore economico attribuito alle informazioni personali.

L'Unione europea «pone la persona al centro della sua azione» recita il preambolo della Carta di Nizza, dove il diritto alla protezione dei dati viene sancito quale fondamentale diritto di libertà.

---

[1] All'interno del regolamento, un ulteriore centrale richiamo alle *data cooperatives* è presente all'art. 10 del DGA, che estende ai servizi di cooperative di dati l'applicazione della procedura di notifica e i requisiti prescritti dal capo III per l'esercizio dei servizi di intermediazione dei dati. Anche nel caso delle cooperative di dati quindi l'avvio dell'attività viene notificato all'autorità competente in materia di intermediazione di dati designata dallo Stato membro, la quale esercita funzioni di monitoraggio e controllo sul loro operato intervenendo con correttivi, ordini di sospensione o di cessazione dell'attività di intermediazione, qualora la stessa sia esercitata in modo non conforme ai requisiti prescritti dall'art. 12 del regolamento, nonché irrogando possibili sanzioni.

L'affermazione è di centrale importanza, se si considera che la protezione delle informazioni personali è sottoposta a continue sfide nella rete, e fuori, dal momento che ogni individuo concede di continuo informazioni [2].

Nel mondo dei consumi e nella logica capitalistica seguita dalle *Big Tech*, la sorveglianza sui comportamenti individuali invade gran parte della vita di ciascuno e si presenta come un connotato delle relazioni di mercato [3].

Chi raccoglie sistematicamente informazioni ha interesse ad influenzare i comportamenti di consumo affinché vengano il più possibile ripetuti [4].L'obiettivo della sorveglianza è la «classificazione»: la società della sorveglianza si connota quindi progressivamente come società della classificazione [5].

Sono queste le significative parole del Professor Stefano Rodotà, il quale in un celebre scritto sulla riservatezza avvertiva: «Viviamo in un mondo nel quale cresce il valore aggiunto delle informazioni personali, con un cambiamento di paradigma, dove il riferimento al valore in sé della persona e alla sua dignità diviene secondario rispetto alla trasformazione dell'informazione in merce» [6].

È allora significativo che la politica di innovazione antropocentrica che l'Unione europea sta promuovendo dimostri che la funzione assunta dal diritto alla protezione dei dati è di fungere da strumento a salvaguardia delle garanzie democratiche di governo dell'identità individuale e dell'umanità, al cospetto delle tensioni imposte dal potere della tecnica [7].

---

[2] Così S. RODOTÀ, *Riservatezza*. *Con un saggio di Antonio Soro e un ricorso di Franco Gallo*, Roma, 2021, p. 100-101, opera che ripropone la voce enciclopedica *Riservatezza* di Stefano Rodotà pubblicata in *Enciclopedia italiana Treccani* nel 2000. Secondo la significativa sottolineatura dell'autore: «La privacy allora s'impone come diritto fondamentale; si specifica come diritto all'autodeterminazione informativa e, più precisamente, come diritto a determinare le modalità di costruzione della sfera privata nella loro totalità; si presenta infine come precondizione della cittadinanza dell'età elettronica».

[3] In ciò si riflette il mutato senso sociale della privacy, non più ancorata soltanto al criterio dell'esclusione dell'altro, ma trasformata e rafforzata dal diritto di mantenere il controllo sui propri dati ovunque essi si trovino, e di opporsi alle interferenze esterne: così S. RODOTÀ, *Il mondo nella rete. Quali diritti, quali vincoli*, Torino, 2014, p. 27 ss.

[4] Così S. RODOTÀ, *Riservatezza*, cit. 96 ss.

[5] S. RODOTÀ, *Privacy, libertà, dignità. Discorso conclusivo della Conferenza internazionale sulla protezione dei dati* tenuto in occasione della *26th International Conference on Privacy and Personal Data Protection*, Poland, Wroclaw 14, 15, 16 September 2004, pubblicata nel sito ufficiale del Garante Privacy.

[6] S. RODOTÀ, *Riservatezza*, cit., p. 100, in cui l'autore mette in evidenza come le tecnologie della comunicazione e dell'informazione manifestino «una sorta di "naturale" tendenza a entrare in conflitto con il diritto di costruire liberamente la propria sfera privata, inteso come autodeterminazione informativa, come potere di controllare la circolazione delle proprie informazioni». Tutto questo, afferma Rodotà «viene presentato come un prezzo obbligato per godere delle crescenti opportunità offerte dalla società dell'informazione» (p. 94).

[7] A. SORO, *Un diritto di libertà*, in RODOTÀ, *Riservatezza*, cit., p. 7 ss.

Per quanto gli strumenti tecnologici siano straordinari mezzi di conoscenza e progresso, si richiama perciò alla necessità che la disponibilità di una tecnologia non possa legittimare ogni qualsivoglia suo utilizzo.

Spetta al diritto governare la tecnica nella sua evoluzione, vagliandola attraverso valori diversi da quelli offerti dalla tecnologia stessa, quali il rispetto della dignità della persona e la salvaguardia dei valori fondamentali di libertà e autonomia dell'individuo [8].

2. Il modello mutualistico delle cooperative di dati nell'economia sociale di mercato europea.

Diversamente dai modelli capitalistici, in cui l'intermediazione dei dati viene svolta ad esclusivo vantaggio dell'impresa al fine di massimizzare il profitto [9], con gli evidenti rischi che questo comporta per i diritti degli interessati, le cooperative di dati operano al servizio dei *data subjects* e dei *data holders* che ne sono membri, quali interessati, imprese individuali e PMI.

D'altra parte, agire nell'interesse dei propri membri fa parte dell'intrinseca natura del modello mutualistico.

Nella Costituzione italiana la mutualità e l'assenza di speculazione privata rappresentano gli elementi chiave della «funzione sociale», riconosciuta come l'essenza più intima della organizzazione cooperativa, e che la contraddistingue rispetto alle altre forme di organizzazione produttiva (art. 45 Cost.).

Nel farne memoria, la Corte Costituzionale in una recente pronuncia (Corte Cost. n. 93/2022) ha ricordato che «La rilevanza costituzionale della cooperazione trova (…) la sua ragion d'essere nella più stretta inerenza che la funzione sociale presenta nell'organizzazione cooperativistica rispetto a quella che la detta funzione riveste nelle altre forme di organizzazione produttiva» [10].

Detta funzione sociale presente nel fenomeno cooperativo, si manifesta nella sua connaturale tensione verso il raggiungimento di finalità costituzionali, quali la realizzazione sul piano economico del principio di democraticità della gestione (art. 1 Cost.), la difesa e lo sviluppo della personalità dei soci secondo il principi di solidarietà economica e sociale (art. 2 Cost.), la rimozione degli ostacoli che si frap-

---

[8] Il legame tra libertà, dignità e privacy «impone di guardare a quest'ultima come ad un fondamentale fattore di contrasto alle potenti logiche che premono per la trasformazione delle nostre organizzazioni sociali in società, della sorveglianza, della classificazione, della selezione discriminatoria»: così S. RODOTÀ, *Privacy, libertà, dignità*, cit.

[9] Per una analisi dei modelli *business* che applicano schemi di monetizzazione dei dati personali S. MARTINELLI-C.R. CHAUVENET, *Legal teck, Contract re-design & Big data per professionisti e imprese*, 2022, Milano, p. 202 ss.

[10] Così Corte Cost. 12 aprile 2022, n. 93.

pongono alla realizzazione del principio di uguaglianza e la possibilità di accesso ad una più corretta distribuzione della ricchezza e delle risorse (art. 3, comma 2, Cost.), nonché, la valorizzazione del lavoro come espressione della persona e come attività di rilievo sociale (art. 4 Cost.) [11].

La funzione sociale che è propria dello scopo mutualistico rende naturale l'inquadramento delle cooperative di dati nel modello europeo dell'economia sociale di mercato.

Di recente, il modello dell'economia sociale di mercato è stato definito dalla migliore dottrina come modello *sui generis* in quanto certamente basato sul mercato e sulle sue libertà, ma non per questo insensibile alle esigenze sociali poiché vengono da esso riconosciuti «l'interna connessione, la coessenzialità, di diritti fondamentali e diritti sociali, i limiti dell'autonomia privata e i compiti sociali delle istituzioni europee» [12].

I principali tratti distintivi del moderno concetto di economia sociale, ispirato ai valori dell'associazionismo democratico e della mutualità cooperativa hanno preso forma in Europa nel corso del XIX secolo, quando le iniziative solidaristiche hanno iniziato a contrapporsi all'economia capitalistica pura [13].

Queste origini storiche sono descritte nei documenti ufficiali dell'Unione, da cui emergere che la cooperazione è venuta presentandosi come rimedio al capitalismo selvaggio, sensibile alle esigenze sociali, in unione con i programmi degli economisti autori dei correttivi all'economia di mercato [14].

In origine, il modello dell'economia sociale di mercato si delinea quindi come la proposta di una riconciliazione tra etica ed economia, attraverso la moralizzazione del comportamento degli operatori economici [15].

---

[11] G. TATARANTO, *Mutualità e gestione di servizi nelle cooperative: i principi nella riforma del diritto societario*, in *Notariato*, 2, 2022, p. 121 ss.

[12] Sono le parole di G. ALPA, *Solidarietà. Un principio normativo*, Bologna, 2022, p. 221 ss.

[13] *Ibidem*.

[14] Per l'evoluzione storica del concetto di economia sociale G. ALPA, *Solidarietà. Un principio normativo*, cit., pp. 222-225 richiama la relazione dal titolo «*L'economia sociale nell'Unione europea*» elaborata dal Ciriec (*International Centre of Research and Information on the Public, Social and Cooperative Economy*) su richiesta del Comitato economico e sociale europeo, in particolare il contenuto dei capitoli 1 e 2.

[15] G. ALPA, *Solidarietà. Un principio normativo*, cit., pp. 223-225, il quale ricorda l'influenza sulle teorie dell'economia sociale di due grandi economisti della seconda metà del XIX secolo, John Stuart Mill e Lèon Walras, i quali hanno contribuito a dare identità a quello che attualmente si riflette in un primo comparto dell'economia sociale di mercato, incentrato sulle imprese sociali e sugli enti che non sono votati alla ricerca di lucro. Accanto ad essa, si presenta una economia sociale di mercato intesa in accezione più ampia, che affonda le proprie radici «nei fondamenti del socialismo attraverso i partiti e i sindacati della fine dell'Ottocento», universalmente impiegata per descrivere le scelte politiche dell'Unione, e che «si pone al centro di due schieramenti esistenti, l'uno informato all'economia di mercato libero, prevalente nell'America del nord, e l'altro dell'economia di Stato (…) concentrata sul mercato diretto dello Stato come in Russia e in Cina, informate al "capitalismo di Stato"».

Nelle politiche dell'Unione, si affermano tutt'oggi quali obiettivi strategici della nuova economia sociale la prevalenza dell'individuo e dell'obiettivo sociale sul capitale, l'applicazione dei principi di solidarietà e responsabilità, insieme ai nuovi obiettivi di sviluppo sostenibile [16].

Le istituzioni europee stanno assegnando all'economia sociale un rilievo significativo, basti pensare al suo inserimento tra i quattordici ecosistemi del piano industriale con cui l'Europa si appresta alla transizione verso la neutralità climatica e la *leadership* digitale, elaborato dalla Commissione il 10 marzo 2020 nella Comunicazione dal titolo «Una nuova strategia industriale per l'Europa» [COM(2020) 102 final] [17].

E ancora, si pensi alla proposta di raccomandazione del Consiglio sullo sviluppo delle condizioni quadro dell'economia sociale [COM(2023) 316 final] presentata dalla Commissione il 13 giugno 2023, avente l'obiettivo di incoraggiare gli Stati membri affinché elaborino e attuino strategie di economia sociale.

Da questo bacino di iniziative affiorano anche le cooperative di dati, che secondo le parole riprese dai primi commenti della disciplina, possono quindi contribuire a «rigenerare il principale giacimento storico, quello dell'economia sociale oggi sempre più chiamata in causa come modalità concreta e fattibile per rilanciare il modello economico sociale europeo» [18].

Tanto più, se si considera che le stesse potranno assumere molto facilmente la forma giuridica delle società cooperative [19], attuale pilastro dell'economia sociale di mercato dell'Unione europea, nonché elemento chiave della innovazione sociale, al contempo dotate di un forte potere nel mercato globale in cui competono a pieno titolo con le società a scopo di lucro.

---

[16] F. VENTURI-P. ZANDONAI, *Neomutualismo. Ridisegnare dal basso competitività e welfare,* Milano, 2022, p. 42, i quali osservano che nella definizione di economia sociale proposta nei documenti europei si può cogliere la ricerca di «un equilibrio tra elementi di missione (prevalenza del fattore umano sul capitale) e di peculiarità organizzativa (*governance* inclusiva) con riferimento alle forme giuridiche che li incarnano (associazioni, fondazioni, mutue, cooperative)». Questo equilibrio tra sostanza degli obiettivi e forma organizzativa, affermano gli autori «porta inevitabilmente a tracciare un perimetro mobile dell'economia sociale considerando in particolare la diversità di sistemi giuridici e policy che caratterizzano gli Stati nazionali che costituiscono l'Unione».

[17] Cfr. P. VENTURI-F. ZANDONAI, *Neomutualismo*, cit., p. 41.

[18] In questi termini F. BRAVO, *Le cooperative di dati*, in https://site.unibo.it/cooperative-di-dati/it (a cui si rinvia per i riferimenti citati nel presente scritto) e in *Contratto e impresa*, 2023, 3, p. 757 ss.

[19] F. BRAVO, *Le cooperative di dati*, cit., p. 4 ss. il quale ritiene che la società cooperativa, nelle sue diverse declinazioni, possa costituire il soggetto fisiologicamente chiamato a ricoprire il ruolo di cooperativa di dati ai sensi del DGA, quantomeno nel nostro ordinamento e in quello europeo (sulla Società Cooperativa Europea si vedano, in particolare, il Reg. CE n. 1435/2003 e la Dir. 2003/72/CE).

3. Cooperative di dati, personalismo e principio di solidarietà.

Nel mercato dei dati in via di sviluppo, il potenziale «sociale» delle cooperative di dati emerge ancor più chiaramente dando lettura alla definizione presente al par. 1, n. 15 dell'art. 2 del DGA in cui, come principale obiettivo dei servizi di cooperative di dati, viene enunciato quello di «aiutare i propri membri nell'esercizio dei loro diritti» in relazione ai dati gestiti dalla cooperativa.

Il verbo «aiutare» inserito nella definizione dei servizi di cooperative di dati esprime un tratto distintivo della mutualità, che consiste nel contenuto altruistico dello scopo che anima i partecipanti alla cooperativa.

Se si pensa soprattutto agli interessati, è evidente che in una sola parola il legislatore europeo esprime l'intima connessione tra il principio pluralista e il principio personalista.

Non solo gli interessati (o le persone fisiche, in generale) sono ritenuti bisognosi di aiuto.

Il considerando n. 31 del DGA presenta le cooperative di dati come uno strumento utile anche per imprese individuali e PMI, equiparando queste ultime in termini di conoscenze in materia di condivisione dei dati, ai singoli individui.

Dal nostro ordinamento costituzionale e dai principi fondamentali dell'Unione europea, l'individuo è inserito in un intreccio di rapporti sociali, che fanno da premessa al maturare delle condizioni per il pieno sviluppo della sua personalità.

In ciò si riassume il rilievo costituzionale delle formazioni sociali, collocate in posizione servente rispetto all'individuo e il compito della Repubblica di fare da garante alle libertà dell'individuo all'interno del gruppo [20].

E se, come è vero, la persona è inseparabile dalla comunità, altrettanto può dirsi della comunità dalla solidarietà [21].

Il principio di solidarietà si incarna così nel personalismo, dando espressione al valore della cura dell'altro come parte del concetto stesso di persona [22]

È perciò in virtù della matrice di fratellanza e coesione sociale che è propria della solidarietà, che l'individuo, naturalmente spinto dall'egoistico appagamento dei propri bisogni, può tornare ad essere membro effettivo e responsabile di una comunità.

Il parallelismo è tanto evidente, quanto necessario, dato che le cooperative di dati in quanto soggetti dell'economia sociale privilegiano le persone, nonché obiettivi sociali e ambientali, rispetto al profitto.

---

[20] F. GALGANO, *La forza del numero e la legge della ragione. Storia del principio di maggioranza*, Bologna, 2007, p. 157 ss.

[21] A. LEPORE, *Principio di solidarietà e autonomia negoziale nel sistema giuridico italiano*, in *Annali della Facoltà Giuridica dell'Università di Camerino – Studi online*, 9, 2022, p. 4.

[22] *Ibidem*.

Per definizione sono chiamate ad operare nell'interesse dei propri membri, con effetti positivi di potenziamento delle posizioni di *data subjects* (e di *data holders*) nell'esercizio dei loro diritti [23].

Oltre a costituire uno spazio interno sicuro in cui dialogare favorendo uno scambio di opinioni e una partecipazione attiva alle decisioni prese con riguardo all'utilizzo dei dati collezionati e gestiti tramite la cooperativa, sul piano esterno, le *data cooperatives* curano l'interesse dei propri membri nei rapporti con gli utenti dei dati.

Il DGA non manca d'altra parte di darne conferma.

Da ciò l'importanza di richiamare alcuni passaggi del regolamento (Reg. UE n. 868/2022) particolarmente significativi in tal senso.

Si consideri dapprima il *considerando* n. 31 del DGA, nella parte in cui fa espresso richiamo alla *mission* delle cooperative di dati di rafforzare la posizione dei propri membri, affinché compiano scelte informate prima di acconsentire all'utilizzo dei dati, personali e non personali, anche esercitando la propria influenza sui termini e le condizioni di utilizzo stabiliti dalle organizzazioni di utenti dei dati, in modo da offrire scelte più consapevoli e vantaggiose [24].

Segue, poi, al par. 1, n. 15, art. 2 DGA, un secondo richiamo al ruolo delle cooperative di dati nelle attività negoziali con gli utenti dei dati al fine di concordare i termini e le condizioni per il trattamento per conto dei membri, prima di concedere l'autorizzazione al trattamento dei dati non personali, o prima che essi diano il loro consenso al trattamento dei dati personali, con gli evidenti vantaggi che questo comporta anche a fronte dei rischi a cui sono esposti soggetti contrattualmente deboli come consumatori e PMI.

Va non di meno considerato che nel caso di fornitura di servizi di intermediazione dei dati in forma cooperativa, una valorizzazione dei dati può avvenire anche mediante l'utilizzo dei dati raccolti a favore della stessa cooperativa, e dunque a beneficio dei membri che la costituiscono, con la possibilità di attivare servizi ulteriori rispetto a quelli di sola raccolta e scambio dei dati, oggetto di mera intermediazione [25].Sempre in chiave collaborativa, si consideri, infine, quanto enunciato all'art. 12, par. 1, lett. *m*) del DGA dove il legislatore europeo si sofferma sul compito delle *data cooperatives* di assistere e supportare i propri membri allo scopo «di

---

[23] Così F. BRAVO, *Le cooperative di dati*, cit., p. 24.

[24] Questo passaggio fa trasparire il percorso verso una tutela sempre più di matrice collettiva, secondo F. BRAVO, *Le cooperative di dati*, cit., p. 24.

[25] Così F. BRAVO, *Le cooperative di dati*, cit., p. 17 ss., secondo il quale «risulta ammissibile l'utilizzo dei dati da parte della cooperativa medesima, nell'ottica della sua operatività secondo logiche mutualistiche, nonché la loro messa a disposizione dei "titolari dei dati", ossia di quei soggetti che, secondo la "nomenclatura" del *Data Governance Act*, hanno diritto di concedere l'accesso a determinati dati personali o non personali o di condividerli, conformemente al diritto dell'Unione o di uno Stato membro (art. 2, par. 1, n. 8, DGA)».

facilitare l'esercizio dei loro diritti, in particolare informandoli e, se opportuno, fornendo loro consulenza in maniera concisa, trasparente, intellegibile e facilmente accessibile sugli utilizzi dei dati da parte degli utenti dei dati e sui termini e le condizioni standard cui sono subordinati tali utilizzi, prima che gli interessati diano il loro consenso».

4. (*segue*) L'applicazione del principio democratico e del principio di sostenibilità.

Della definizione del fenomeno cooperativo fa parte anche il concreto attuarsi di fattori strutturali di democraticità, quali il rispetto della porta aperta e l'effettiva partecipazione alla vita delle *data cooperatives*, le quali garantiscono a ciascun membro il peso necessario per esercitare la propria influenza.

Le cooperative di dati sono dotate di una organizzazione interna a carattere democratico che si esprime in primo luogo nella operatività del principio della porta aperta, per merito del quale viene assicurata una adesione libera e volontaria a chiunque intenda usufruire dei servizi da queste offerti, accettando gli effetti connessi alla propria adesione.

I principi di uguaglianza e democraticità che governano questo schema organizzativo garantiscono l'applicazione del metodo democratico anche nel processo decisionale e di controllo, attribuendo a ciascun membro il diritto di concorrere fattivamente alla formazione della volontà collettiva relativa all'impiego dei dati, e conservandone al contempo il controllo.

Nelle cooperative di dati il principio di democraticità si traduce, quindi, nell'esercizio di una *governance* collettiva (art. 12, par. 1, n. 15, DGA) in grado di assicurare un confronto democratico interno che sfocia nella partecipazione di ciascun membro alle scelte strategiche ed operative sui dati affidati alla gestione della cooperativa, resa possibile anche dall'utilizzo di strumenti telematici di interazione, quali possono essere apposite piattaforme volte a favorire gli scambi a distanza di una governance partecipata. Al contempo, sui dati conferiti, ai membri della cooperativa è riconosciuto l'esercizio di una *governance* individuale, nel senso che viene data loro la possibilità di conservare il controllo sui propri dati e sul relativo utilizzo, con l'ausilio anche in questo caso di strumenti elettronici *ad hoc* [26].

I due piani di *governance*, individuale e collettiva, concorrono ma occorrono entrambi, in quanto è necessario assicurare al soggetto interessato, che partecipa alla formazione della volontà collettiva, di mantenere il controllo individuale sul trattamento dei dati personali ai sensi del Reg. (UE) n. 679/2016 [27].

---

[26] *Ibidem.*

[27] Nuovamente BRAVO, *Le cooperative di dati*, cit., pp. 6, 20-29, il quale mette in luce l'importanza di mantenere una *governance duale* sui dati, collettiva e individuale, come affermato dalla

Sempre in chiave democratica, le cooperative di dati intervengono qualora vi siano da sciogliere eventuali posizioni contrastanti dei membri di un gruppo in merito alle modalità di utilizzo dei dati, ove tali dati riguardino più interessati all'interno della stessa cooperativa.

Il passaggio mette ancora una volta in luce il potenziale delle cooperative di dati, le quali operano ispirando la propria azione ai principi di democraticità, solidarietà e uguaglianza, attraverso i quali si esplica la funzione sociale che è propria di questa forma organizzativa.

A tali principi si aggiunge il più recente corollario del principio di solidarietà, ossia il principio di sostenibilità [28] .

In una relazione dinamica tra sistema ecologico e sistema antropico, la sostenibilità è diventata punto cardine per le scelte economiche e sociali a livello globale [29].

La risposta alla sfida di uno sviluppo autenticamente sostenibile coinvolge anche le cooperative di dati, le quali seguono missioni rappresentative degli interessi dei propri membri, sempre con l'attenzione rivolta alla cura di interessi esterni, e quindi in armonia con la tutela degli interessi diffusi della comunità.

Per queste ragioni, il modello mutualistico applicato al mercato delle informazioni personali (e non personali) attraverso le cooperative di dati, potrà fare da motore allo sviluppo di una economia dei dati che è insieme più giusta e sostenibile, in quanto basata sul pilastro comunitario e quindi in grado di influire sulle logiche del duopolio Stato e mercato [30].

Un rinforzo significativo delle organizzazioni cooperative in termini di sostenibilità è attribuibile, oggigiorno, anche all'assorbimento del digitale [31].

Occorre, infatti, far mente del fatto che uno sviluppo digitale consapevole e sostenibile è parte integrante dell'attuale strategia di trasformazione ed espansione dell'economia sociale e solidale in chiave tecnologica [32], indirizzo dal quale prende

---

Cassazione (Cass. n. 17911 del 1° giugno 2022, su cui S. THOBANI, *Consenso al trattamento e delibere assembleari*, in *Giur. it.*, 2022, XII, p. 2599 ss.) intervenuta in un caso di trattamento illecito posto in essere da una cooperativa nei confronti del socio lavoratore, in una fattispecie in cui veniva contestato il difetto del consenso al trattamento di costui, senza che potesse supplire, in tal senso, la volontà collettiva formatasi in seno all'adozione della delibera assembleare.

[28] Così G. ALPA, *Solidarietà un principio normativo*, cit., p. 275.

[29] E. GIOVANNINI, *Principio di sostenibilità*, Torino in *Aspenia online*.

[30] P. VENTURI-F. ZANDONAI, *Neomutualismo. Ridisegnare dal basso competitività e welfare*, cit., p. 92 ss. Concentrarsi troppo sull'efficacia percepita dei mercati e dello Stato, e perciò trascurare il ruolo sociale della comunità, genera uno squilibrio a cui si può porre rimedio solo attraverso il potenziamento delle organizzazioni del terzo pilastro, ovvero grazie al potenziamento delle comunità. Sono queste le parole del premio Nobel per l'economia R. RAJAN, *Il terzo pilastro. La comunità dimenticata da stato e mercati*, Milano, 2019, p. 415 ss.

[31] P. VENTURI-F. ZANDONAI, *Neomutualismo*, cit., p. 4 ss.

[32] F. BRAVO, *Le cooperative di dati*, cit., p. 7.

forma la più moderna delle declinazioni assunte dal mutualismo: il neomutualismo digitale [33].

L'interesse per la comunità e l'attenzione per l'innovazione tecnologica che ispirano l'azione della forma cooperativa, danno la misura di quanto le cooperative di dati possano operare per uno sviluppo sostenibile delle proprie comunità, interne ed esterne, attraverso politiche capaci di conciliare al meglio l'iniziativa economica privata con la tutela dei diritti umani e dell'ambiente [34].

Divengono con ciò ancora più evidenti i benefici dei servizi di intermediazione di dati offerti dalle *data cooperatives*, in primo luogo per coloro che vi partecipano quali membri, non di meno, per i fruitori dei servizi erogati dalla cooperativa e per i soggetti terzi che con essa interagiscono, favorendo in una prospettiva generale la crescita delle persone, delle comunità, delle imprese e dell'economia.

5. Un breve accenno all'inquadramento teorico della fattispecie di scambio oneroso o gratuito di dati personali. Il doppio consenso.

La riflessione svolta ha permesso di raggiungere una ragionevole convinzione sulla sussistenza di un insieme di condizioni in grado di assicurare, nel caso di servizi di intermediazione dei dati offerti da cooperative di dati, un processo di valorizzazione dei dati personali e non personali per i cittadini dell'Unione e per gli operatori economici, più protetto e garantito.

Al termine del presente lavoro si coglie l'occasione per svolgere almeno un accenno alla riflessione teorica che sul piano ricostruttivo rende compatibile un accordo di scambio a titolo oneroso o gratuito di dati personali, con lo *status* costituzionale europeo della protezione dei dati.

Per quanto le cooperative di dati operino in una direzione senz'altro rassicurante, innegabilmente rimane notevole l'impatto del DGA, e più in generale della strategia europea per i dati sull'assetto normativo in materia di protezione dei dati personali.

D'altro canto, a fare da premessa allo sviluppo del mercato dei dati non può che essere la negoziabilità delle informazioni personali.

Come già in apertura sottolineato, l'Unione europea proclama il proprio indirizzo personalista anche a fronte della rilevanza economica dei dati.

Il diritto alla protezione dei dati personali è garantito dall'art. 8, par. 1, della Carta

---

[33] P. VENTURI-F. ZANDONAI, *Neomutualismo*, cit., p. 13 ss., dove si osserva che l'avvento del neomutualismo segna un ritorno del mutualismo sotto sembianze diverse dal passato, descritto ora come «meccanismo sociale» prima ancora che come «forma organizzativa» e generato da una nuova domanda di legame sociale che si manifesta grazie ad iniziative sorte dal basso.

[34] Per questi aspetti, con riferimento alla sostenibilità in rapporto all'iniziativa economica G. ALPA, *Solidarietà un principio normativo*, cit., p. 277.

dei diritti fondamentali dell'Unione europea [35] e dall'art. 16, par. 1, del Trattato sul funzionamento dell'Unione europea. La stessa Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, precisamente all'art. 8, par. 1 riconosce e sancisce la tutela e il rispetto di tale diritto.

La dogmatica tradizionale dei diritti fondamentali muove dalla tesi della irrinunciabilità ed indisponibilità di tali posizioni giuridiche, in quanto connaturate alla persona, tant'è che fin da subito è stata avvalorata la tesi che riconduce la disciplina del trattamento dei dati, al sistema dei diritti della personalità [36].

Il discorso si salda, allora, con l'opinione di chi ritiene non accettabile l'idea riconosciuta da alcuni che la persona eserciti un diritto di proprietà sui propri dati e ne possa disporre liberamente [37].

Si comprende al contempo la critica alla impostazione che attribuisce natura traslativa di un diritto, al consenso dell'interessato reso in forza della disciplina in materia di protezione dei dati [38].

Tale consenso, non vale a trasferire un diritto dall'interessato al titolare del trattamento, essendo piuttosto strumentale a rimuovere un limite all'esercizio di poteri e facoltà che l'ordinamento prevede già autonomamente in capo al titolare stesso (connotato comune a tutte le condizioni di liceità) [39]. La legittimazione a trattare dati personali del titolare del trattamento non deriva infatti dal soggetto privato a cui i dati si riferiscono. Si tratta, piuttosto, di un potere che il titolare del trattamento riceve in via autonoma dall'ordinamento giuridico, il cui contenuto consiste nella possibilità di determinare le finalità del trattamento, le modalità, i mezzi, nonché l'ambito di circolazione dei dati, entro il perimetro delineato dalla normativa europea e nazionale.

Tale potere sorge in capo al titolare del trattamento in via autonoma [40].

È piuttosto per il suo esercizio che si richiede un fondamento legittimo, che opera come condizione di liceità del trattamento e tale fondamento si ravvisa nel con-

---

[35] V. ZENO ZENCOVICH, *Ragioni ed obiettivi del codice*, in F. CARDARELLI-S. SICA-V. ZENO ZENCOVICH (a cura di), *Il codice dei dati personali. Temi e problemi*, Milano, 2004, p. 4 in cui l'autore afferma che si tratta di «un risultato cui non è certamente estraneo l'operoso intervento del Garante italiano ed in particolare del suo presidente prof. Rodotà componente della commissione che ha redatto la Carta».

[36] La dottrina italiana è rimasta nel complesso insensibile alle lusinghe del modello proprietario ed ha piuttosto fin da subito avvalorato la riconduzione della disciplina del trattamento dei dati al sistema dei diritti della personalità, questa la sottolineatura di G. RESTA, *Il diritto alla protezione dei dati personali*, in F. CARDARELLI-S. SICA-V. ZENO ZENCOVICH (a cura di), *Il codice dei dati personali. Temi e problemi*, cit., pp. 21-23, 51.

[37] G. ALPA, *L'identità digitale e la tutela della persona. Spunti di riflessione*, in *Contratto e impresa*, 2017, III, p. 727 ss.

[38] F. BRAVO, *Lo "scambio di dati personali" nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto*, in *Contratto e impresa*, 2019, 1, p. 34 ss.

[39] F. BRAVO, *Lo "scambio di dati personali"*, cit., p. 34 ss.

[40] *Ibidem.*

senso dell'interessato al trattamento dei dati personali [41].

Al consenso al trattamento dei dati viene perciò riconosciuta natura di autorizzazione integrativa, il cui effetto consiste nel rimuovere un limite all'esercizio di un diritto o di un potere già acquisito dal titolare del trattamento [42].

Nel caso di un accordo avente ad oggetto lo scambio a titolo oneroso o gratuito dei dati personali, il consenso dell'interessato si sdoppia.

È quanto affermato in dottrina e in giurisprudenza con riferimento ai contratti di fornitura di servizi digitali in cambio di dati personali dell'interessato, in luogo del pagamento di un corrispettivo in denaro [43].

Ed è quanto, per ciò che qui interessa, conserva la propria validità anche con riferimento alla fattispecie giuridica dello scambio di dati personali dell'interessato promossa dal legislatore europeo e resa possibile dal quadro armonizzato di norme introdotte dal *Data Governance Act*, attuabile anche attraverso l'intermediazione delle cooperative di dati.

Anche in questo caso, come già in quello preso in esame dall'accennata dottrina e dalla giurisprudenza, all'accordo, a titolo oneroso o gratuito, avente ad oggetto atti di esercizio dei diritti sui dati personali dell'interessato, si aggiunge l'atto di autorizzazione integrativa previsto in funzione del trattamento, senza che il primo consenso possa mai sostituirsi al secondo.

I due consensi dall'interessato di diversa natura convivono e interagiscono, essendo tra loro funzionalmente collegati [44].

In sintesi, serve un primo consenso, reso ai fini del trattamento dei dati personali che rimuove il limite previsto dall'ordinamento al potere del titolare di svolgere le attività di trattamento sui dati dell'interessato, e che si esprime attraverso un atto unilaterale di autorizzazione integrativa.

A questo si aggiunge un secondo consenso, questa volta di natura contrattuale, con il quale l'interessato concede l'esercizio di diritti sui propri dati, anche in una

---

[41] *Ibidem.*

[42] Contrapponendola alla autorizzazione costitutiva, giacché riferibile ad una situazione di potere precostituito del titolare del trattamento, l'autore (F. BRAVO, *Lo "scambio di dati personali"*, cit., p. 34 ss.) rinvia alla definizione di autorizzazione integrativa proposta da A. AURICCHIO, voce *Autorizzazione* (*dir. priv.*), in *Enc. dir.*, Milano, IV, 1959, p. 506 ss. Per il riconoscimento della natura autorizzatoria del consenso al trattamento dei dati personali, anche Cass., sez. I, 29 gennaio 2016, n. 1748 in *Danno e Resp.*, 2017, 1, p 47 ss., con nota di E. BARNI, resa in materia di utilizzazione dell'immagine (rientrante nel genere delle informazioni personali ai sensi dell'art. 8 CEDU sulla tutela della vita privata).

[43] F. BRAVO, *Lo "scambio di dati personali"*, cit. con riferimento a Cass., sez. I, 2 luglio 2018, n. 17278 in *Nuova giur. civ.*, 2018, 12, p. 1775 con nota di F. ZANOVELLO. In tal senso già Cass. n. 1748/2016, cit., che riconosce autonomia al consenso alla utilizzazione della propria immagine, rispetto al consenso contrattuale con cui viene pattuito l'esercizio di tale diritto dietro il pagamento di un compenso.

[44] Così BRAVO, *Lo "scambio di dati personali"*, cit. Cfr. anche Cass. n. 1748/2016 cit.; Cass. n. 17278/2018, cit.

logica di natura patrimoniale, nell'ambito del quale non si spoglia mai dei diritti fondamentali sui propri dati.

Sul consenso contrattuale ricadono gli effetti della revoca del consenso al trattamento, essendo a quest'ultimo ontologicamente collegato [45].

Sarà quindi il doppio consenso ad accompagnare l'esercizio sui dati personali di diritti in senso patrimoniale (o gratuito), nel rispetto della natura fondamentale del diritto alla protezione dei dati personali, la cui sussistenza – come una costante – andrà vagliata con riferimento alla massa di eterogenee interazioni negoziali che il sistema di condivisione dei dati personali inaugurato dal DGA porterà alla luce.

[45] *Ibidem*.

Capitolo VIII

Leveraging Data Cooperatives in Empowering Ethical AI Development and Data Protection

Bukola Adesokan

Abstract: The proliferation of Artificial Intelligence (AI) technologies has catalysed significant advancements across various sectors, driven by the remarkable learning capabilities of AI systems. However, the reliance on extensive datasets, often from human interactions without explicit consent, has raised profound ethical and legal concerns regarding data protection and ownership. In response, this paper explores the potential of data cooperatives as a mechanism to address these challenges and foster ethical AI development. Data cooperatives, collaborative organisations governed by transparency and collective ownership principles, empower individuals to control their data usage in AI training. Through consent management and transparent governance structures, data cooperatives enable individuals to assert their rights over their personal data while promoting privacy protection and legal compliance. The paper also examines real-world examples of data cooperatives, such as MiData and Driver's Seat, to illustrate their practical implications and benefits. Additionally, the paper examines how a data cooperative, Karya, is already using its platform to provide datasets from its members to AI companies while compensating them for their contributions. This paper sheds light on the transformative potential of data cooperatives by addressing potential challenges and considerations associated with using them and offering recommendations for future research and collaboration. It contributes to the ongoing discourse on ethical data practices and governance in the digital age, paving the way for responsible AI development and safeguarding individuals' data rights.

1. Introduction.

In recent years, the proliferation of Artificial Intelligence (AI) technology has

ushered in a transformative era across various sectors. With their remarkable learning capabilities, these advanced systems have become indispensable tools for deciphering complex datasets, thereby driving crucial decision-making processes. Central to this AI revolution is training these systems with extensive and diverse datasets,[1] often open-sourced or sourced from human interactions and actions. This data serves as the lifeblood of AI learning algorithms, enabling them to generate nuanced and contextually relevant outputs.[2] However, the reliance on human data has also raised significant ethical and legal concerns, particularly regarding the unauthorised and unethical use of individuals' data.[3]

This growing discourse on data ownership and privacy rights underscores the urgent need for mechanisms to protect individuals' data rights and ensure ethical data practices in AI development. Moreover, the daunting challenge of obtaining consent from the vast array of data subjects further complicates the ethical landscape of AI development.[4] In response to these pressing concerns, this paper seeks to explore the multifaceted challenges inherent in data gathering for AI development and elucidate the ethical imperatives surrounding data acquisition.

Specifically, this paper aims to investigate how data cooperatives can emerge as a promising mechanism to address these challenges, fostering a framework wherein data is sourced, utilised, and governed in a manner that upholds transparency, fairness, and accountability principles. By examining the role of data cooperatives in facilitating collective data ownership and control, this paper endeavours to provide insights into how these cooperative structures can navigate the intricate terrain of data ownership in AI development, offering a pathway towards equitable and responsible data utilisation.

Furthermore, this paper will delve into potential issues arising from the use of data cooperatives and explore strategies to mitigate these challenges. This paper seeks to contribute to the ongoing discourse on ethical data practices and governance in the digital age by critically analysing data cooperatives' theoretical underpinnings and practical implications in AI development. Through a comprehensive examination of these issues, this paper aims to shed light on the transformative potential of data cooperatives in promoting ethical AI development and safeguarding individuals' data rights.

---

[1] Tooploox, *5 Main Challenges with Datasets and AI Ethics*, https://tooploox.com/datasets-and-ai-ethics, accessed on 3 June 2024.

[2] Usercentrics, Artificial Intelligence (AI), Personal Data And Consent, 2023, https://usercentrics.com/knowledge-hub/artificial-intelligence-ai-act-and-consent/, 5 June.

[3] F. HEIKE-V.F. EDUARD-T. AUREILA, *Transparency You Can Trust: Transparency Requirements for Artificial Intelligence Between Legal Norms and Contextual Concerns*, 2019, (*Big Data & Society)*, volume 6, issue 1.

[4] Tooploox, *5 Main Challenges with Datasets and AI Ethics*, https://tooploox.com/datasets-and-ai-ethics, accessed on 3 June 2024.

2. Scope and Approach of Data Cooperatives.

A data cooperative is a collaborative organisation formed by individuals or entities to pool and manage data resources for mutual benefit.[5] Unlike traditional data-sharing arrangements, data cooperatives are founded on principles of democratic governance, transparency, and collective ownership of data.[6] Members of a data cooperative typically contribute data assets to a shared pool, which is then governed collectively according to agreed-upon rules and principles.[7]

The Data Governance Act[8] (DGA) defines the services of a data cooperative as data intermediation services offered by an organisational structure constituted by data subjects, one-person undertakings, or Small and Medium Enterprises who are members of that structure, having as its main objectives to support its members in the exercise of their rights concerning certain data, including making informed choices before they consent to data processing, to exchange views on data processing purposes and conditions that would best represent the interests of its members concerning their data, and to negotiate terms and conditions for data processing on behalf of its members before permitting the processing of non-personal data or before they consent to the processing of personal data.[9]

Data cooperatives are typically formed through a structured process that involves several key steps. Initially, individuals or organisations interested in forming a data cooperative identify common interests and objectives related to data sharing and collaboration. Membership recruitment follows, where potential members are invited to join the cooperative and contribute their data assets.[10] Governance structures are established to facilitate decision-making and ensure accountability, with members having a voice in the cooperative's operations and policies. Data-sharing agreements are developed to govern how data will be accessed, used, and shared among members.[11]

Members of a data cooperative hold certain powers and responsibilities within

---

[5] B. EMRE, *Data cooperative: A new intermediary on the horizon*, (Centre for IT & IP Law) 2021, https://www.law.kuleuven.be/citip/blog/data-cooperative-a-new-intermediary-on-the-horizon/, 2 June 2024.

[6] M. SAMEER-D. MILLINDE-M. LIYING, *The Key To Designing Sustainable Data Cooperatives*, (World Economic Forum) 2022, https://www.weforum.org/agenda/2022/02/the-key-to-designing-sustainable-data-cooperatives/, 2 June 2024.

[7] J. ZHU-O. MARJANOVIC, *A Taxonomy of Data Cooperatives*, (*PACIS 2022 Proceedings* 257), https://aisel.aisnet.org/pacis2022/257/, 5 May 2024.

[8] Regulation (EU) 2022/868 of the European Parliament and of the Council.

[9] Article 2.15 of the Data Governance Act.

[10] H. ERNST, *Personal Data Cooperatives. A New Data Governance Framework for Data Donations and Precision Health*, in J. KRUTZINNA-L. FLORIDI (eds), *The Ethics of Medical Data Donation*. Philosophical Studies Series, 2019, vol 137. Springer, Cham.

[11] *Ibid*.

the organisation. They participate in decision-making processes, elect representatives to serve on governing bodies, and contribute to formulating data-sharing policies. Additionally, members have rights regarding data access, usage, and privacy protection, which are enshrined in the cooperative's bylaws and agreements.[12] An example of a data cooperative is an app-based ride-hailing platform named Driver's Seat Cooperative,[13] which receives datasets from different drivers and empowers driving gig workers to increase their earnings, counter algorithmic management by gig companies with worker-developed technology, provide transparent data for policymaking in workforce and transportation sectors, and establish a cooperatively-owned business to support its mission. The data derived from this cooperative is sold to cities to inform their transportation strategies, and local decision-makers are drawn to it because the data is been collected ethically Increasing membership will generate more detailed insights for them, along with helping them move towards sustainability.[14]

Another example of the use of data cooperatives is MiData[15], which operates as a data cooperative by providing a platform for individuals to contribute their personal data for medical research and clinical studies while maintaining control over their data and participating in the governance of the cooperative. Also, the Data Commons Cooperative is used to pull data together for research purposes to promote networking and growth, as well as power new products, services, and resources.[16]

Data cooperatives offer several benefits for individuals, organisations, and society as a whole.[17] Data cooperatives empower individuals to exercise control over their data usage by providing mechanisms for consent management, data access control, and transparency. This enhances privacy protection, promotes data sovereignty, and ensures fair compensation for data contributions. For organisations, data cooperatives foster collaboration, innovation, and knowledge sharing, enabling them to leverage collective intelligence and data resources for competitive advantage.[18] For society, data cooperatives drive positive social and economic out-

---

[12] H. THOMAS-P. ALEX, *Data Cooperatives: Towards a Foundation for Decentralised Personal Data Management*, 2019, https://www.researchgate.net/publication/333309091_Data_Cooperatives_Towards_a_Foundation_for_Decentralized_Personal_Data_Management, 5 May 2024.

[13] https://www.driversseat.co/.

[14] T. JULIAN (Open Data Manchester), *A Case for Data Cooperatives. The White Paper Series*, 2021, https://thedataeconomylab.com/2021/09/06/the-case-for-data-cooperatives/, 5 May 2024.

[15] https://www.midata.coop/en/home/.

[16] Data Commons Cooperative, https://datacommons.coop/, 10 May 2024.

[17] F. ALEXANDER, *Data Cooperative*, in *Internet Policy Review*, 2024, volume 13, issue 2, https://policyreview.info/glossary/data-cooperative, 3 June 2024.

[18] B. MICHAEL-C. IGOR-C. ISABEL, *Data cooperatives as catalysts for collaboration, data sharing, and the (trans)formation of the digital commons*, https://www.researchgate.net/publication373052009/

comes by promoting responsible data stewardship, supporting data-driven decision-making, and fostering inclusive growth and development.[19]

The Data Governance Act also recognises the role of data cooperatives in empowering individuals to make informed choices about data usage.[20] These cooperatives influence terms and conditions for data user organisations, offering better choices to individual members and resolving conflicts within the group.

Data cooperatives are crucial in empowering individuals to make informed decisions about data usage and assert their data protection, privacy, ownership, and control rights. By providing a platform for collective action and advocacy, data cooperatives amplify the voices of individuals and communities in shaping data governance policies and practices. Moreover, data cooperatives enable individuals to participate in the data economy on their terms by facilitating fair and transparent data transactions, promoting data literacy and awareness, and advocating for ethical data practices and standards.

3. Data Usage Issues in AI System Training.

AI systems development involves a multifaceted process of AI training, which is crucial for nurturing AI's cognitive abilities. This process entails teaching an AI system to perceive, interpret, and learn from vast datasets (data mining), enabling it to make informed decisions or inferences based on the provided information,[21] just like children learn to distinguish between dogs and cats by starting with basic pictures and progressing to nuanced traits, AI evolves from simple data inputs to precise understanding through iterative training processes.[22]

AI systems, in their quest for intelligence, are trained from a variety of datasets, both opened-sourced[23] and data from the actions of humans to enhance their performance and capabilities. The global AI training dataset market size was valued at $2.39 billion in 2023 and is projected to grow from $2.92 billion in 2024 to $17.04 billion by 2032.[24] This estimated growth indicates that tech and AI-developing

_Data_Cooperatives_as_Catalysts_for_Collaboration_Data_Sharing_and_the_TransFormation_of_the_Digital_Commons 3 June 2024.

[19] *Ibid*.

[20] Recital 31 of the Data Governance Act.

[21] K.J. JACOBY, *Tech Explainer: What is AI Training*, https://www.performance-intensive-computing.com/objectives/tech-explainer-what-is-ai-training, 3 April 2024.

[22] M. CHEN, *What is AI Model Training and Why is it so Important*, https://www.oracle.com/artificial-intelligence/ai-model-training/, accessed 7 April 2024.

[23] Open source data encompasses large datasets accessible to anyone with an internet connection, sourced externally and ranging from public government data to economic trend analyses from financial institutions.

[24] Fortune Business Insights, *Al Training Dataset Market Size, Share & Industry Analysis, By*

companies are investing heavily in acquiring and developing datasets for their AI training. The demand for data providers who curate and sell datasets is also very important.

These datasets often comprise personal data harvested from individuals, most times without any legal bases for processing the data, such as consent, contract, legitimate interest, legal obligation, or public interest,[25] raising significant concerns regarding data protection, privacy, and control.

Legal obligation may be one of the lawful bases relied on for using individuals' data. For instance, auditing AI systems for compliance with legislation, such as data protection laws, may necessitate the processing of personal data to test system performance across different demographics.[26] This falls under the category of legal obligation, specifically covering auditing and testing activities.

Consent is an appropriate lawful basis in cases where the AI developers have a direct relationship with the individuals whose data are to be used in training the AI system. However, consent must be freely given, specific, informed, and unambiguous, and it must have a clear affirmative act on the part of the individuals. For AI system developers, obtaining consent from every individual whose data is essential for system development poses a formidable challenge, some have argued that all data used are purely scrapped off the internet, i.e. open-sourced and do not require consent.[27] The sheer scale and diversity of datasets required for effective AI training make securing explicit consent from each data subject impractical. Moreover, the dynamic nature of data collection and use in AI development further complicates the consent process, necessitating alternative approaches to ensure data privacy and compliance with regulatory frameworks.

While there may not be overt instances of individuals discovering their data being used in the training of AI systems without consent, the prevalence of data sharing among big tech firms underscores the pervasive lack of transparency and accountability in data usage.[28]

Type (Text, Audio, Image, Video, and Others), By Deployment Mode (On-Premises and Cloud), By End-Users (IT and Telecommunications, Retail and Consumer Goods, Healthcare, Automotive, BFSI, and Others), and Regional Forecast, 2024-2032, https://www.fortunebusinessinsights.com/ai-training-dataset-market-109241, on 28 May 2024.

[25] Article 6 of the General Data Protection Regulation (GDPR).

[26] Information Commissioner's Office (UK), *How do we ensure Lawfulness in AI*, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/how-do-we-ensure-lawfulness-in-ai/#inferences), 13 May 2024.

[27] M. HEIKKLÄ, *Open AI's Hunger for Data is Coming Back to Bite it*, 2023 (MIT Technology Review), https://www.technologyreview.com/2023/04/19/1071789/openais-hunger-for-data-is-coming-back-to-bite-it/?truid=, 12 May 2024.

[28] G. SARKAR, *Google, Meta, Amazon, Others May Face Penalty For Data Sharing Without Customer Consent*, 2023 (Inc42), https://inc42.com/buzz/google-mata-amazon-others-may-face-penalty-for-data-sharing-without-customer-consent/, 5 May 2024.

The absence of consent in the use of individuals' data further exacerbates privacy concerns and undermines individuals' rights over their personal data. This lack of legal justification for data usage perpetuates a culture of opacity and non-accountability, posing significant challenges to ensuring ethical data practices and compliance with data protection laws like the General Data Protection Regulation (GDPR).

To address these challenges, data cooperatives emerge as promising solutions. They provide structured frameworks for ethical data collection, sharing, and utilisation. By facilitating informed consent and promoting transparency in data practices, data cooperatives empower individuals to exercise control over their personal data and ensure compliance with privacy regulations.

4. How Data Cooperatives Can Empower Individuals Data Usage By AI Developers and Enhancing Privacy And Legal Compliance For AI Developers.

One of the primary issues facing AI developers is the acquisition of high-quality training data to optimise the performance and capabilities of AI systems. The nature of data collection and utilisation in AI development further complicates the ethical landscape, necessitating robust mechanisms to ensure transparency, accountability, and compliance with regulatory frameworks.[29] The GDPR, for instance, mandates stringent requirements for the lawful processing of personal data, including obtaining explicit consent from data subjects[30] and adhering to data minimisation, purpose limitation, and accountability principles.

Data cooperatives have emerged as pivotal players in the contemporary data landscape. In AI system development training, data cooperatives can be used to empower individuals to control their data usage by AI developers while enhancing privacy and legal compliance. Operating within a secure IT platform like financial bank accounts, data cooperatives afford individual data account holders complete control over their data usage.[31] Each record is encrypted, and only the account holder possesses the decryption key, ensuring that neither the IT platform administrator nor the cooperative's management can access the data. Moreover, account holders can become cooperative members, participating in demo-

---

[29] T. YAQOOB, *Ethical Considerations in AI Development and Deployment*, 2023 (CoinTelegraph), https://cointelegraph.com/explained/ethical-considerations-in-ai-development-and-deployment, 10 May 2024.

[30] Art. 7 of the GDPR.

[31] E. HAFEN-D. KOSSMANN-A. BRAND, *Health data cooperatives. Citizen empowerment*, in *Methods of Information in Medicine*, 2014, volume 53, Issue 2: pp. 82-86, https://doi.org/10.3414/ME 13-02-0051, 5 May 2024.

cratic governance by electing the board and voting on investment decisions.[32]

In the context of AI system development and training, the utilisation of data cooperatives presents a multifaceted approach to address the complex challenges surrounding data usage, privacy, and legal compliance. Within this cooperative model, individuals entrust their data rights to the cooperative entity, which acts as a custodian overseeing data management and negotiating favourable privacy policies and terms of use on behalf of its members.[33]

Data cooperatives can serve as intermediaries between AI developers and individual data owners, facilitating transparent communication and consent management. When AI developers seek access to data for training or testing purposes, data cooperatives translate developers' requirements to members and provide mechanisms for informed decision-making. Members can opt in or opt out of data-sharing initiatives based on their preferences, with transparency measures such as data usage policies and audit trails ensuring accountability.

In practice, AI developers may approach data cooperatives to request access to the data of cooperative members for the purpose of training or testing their AI systems. The cooperative then serves as an intermediary, facilitating communication between the developers and its members. The cooperative translates the developers' requirements to the members, ensuring clarity and transparency regarding the intended usage of their data. Members are empowered to make informed decisions regarding data sharing, with the option to opt-in or opt-out based on their preferences. Transparency measures, including data usage policies and audit trails, ensure that members are fully aware of how their data will be utilised, holding the cooperative accountable for adherence to ethical standards.

Additionally, data cooperatives adopt principles of data ethics and responsible data stewardship to guide their operations and decision-making processes. By promoting ethical data practices, data cooperatives foster trust and collaboration between individuals, AI developers, and other stakeholders, ultimately contributing to the responsible advancement of AI technologies.

5. An Innovative Approach to Implementing Data Cooperatives in AI Development Process.

Successful implementation of data cooperatives in the AI development process requires a systematic and comprehensive approach. An innovative approach involves emphasising collaboration, transparency, and adherence to legal and ethical stand-

---

[32] *Ibid*.

[33] D. JAMIE, *Data Protection Beyond Data Rights: Governing Data Production Through Collective Intermediaries*, in *Internet Policy Review*, 2023, vol. 12, issue 3, https://policyreview.info/articles/analysis/data-protection-beyond-data-rights, 11 May 2024.

ards. This approach encompasses several key steps, from establishing legal frameworks to govern data cooperatives' operations to engaging in consultations with AI developers and cooperative community members. Responsible data practices could be promoted through these steps to foster trust and cooperation among stakeholders and ultimately advance the ethical development of AI technologies.

Importantly, where the data cooperative operates in any member state of the European Union, the cooperative may be required to register as a data altruism organisation if the state has technical and organisational measures in place for this purpose.[34] The DGA defines data altruism[35] as the voluntary sharing of data on the basis of the consent of data subjects to process personal data pertaining to them or permissions of data holders to allow the use of their non-personal data without seeking or receiving a reward that goes beyond compensation related to the costs that they incur where they make their data available for objectives of general interest as provided for in national law.

The following are the steps that can be adopted to properly implement data cooperative in obtaining data for ethical AI development.

(i) *Establishing Legal Frameworks*

The first step in the approach involves data cooperatives establishing robust legal frameworks tailored to align with the DGA,[36] that would govern the cooperatives' operations. This includes the formulation of rules, policies, and procedures to ensure compliance with relevant laws and regulations governing data usage. By putting in place comprehensive legal frameworks, data cooperatives create a solid foundation for ethical data practices and facilitate transparency and accountability in their operations.

(ii) *Initial Discussions with AI Developers*

When policies, procedures, and frameworks guiding the cooperatives are already in place, AI developers can initiate discussions to communicate their needs for the AI development projects with the data cooperatives. These consultations allow AI developers to outline the purpose, scope, and requirements for data usage while also addressing any concerns or questions raised by the data cooperatives. AI developers and data cooperatives can establish mutual understanding and trust by engaging in open and transparent dialogue, laying the groundwork for successful collaboration.

(iii) *Member Engagement and Consent*

Following discussions with AI developers, members of the data cooperative convene to discuss and be provided avenues for opting in or opting out of data-

[34] Art. 16 DGA.

[35] Art. 2.16 DGA.

[36] Chapter IV of the DGA.

sharing initiatives. This process ensures that members have full autonomy and control over the use of their data, allowing them to make informed decisions based on their preferences and values. By empowering members to exercise their data rights, data cooperatives promote transparency and accountability in data-sharing practices while also fostering trust and cooperation within the cooperative community.

(iv) *Drafting Agreements*

Once the consent of the members is obtained, data cooperatives proceed to draft agreements to govern the data-sharing initiatives with the AI developers. Data cooperatives may implement agreements on behalf of their members, binding all interested parties once a consensus is reached. These agreements outline the terms of data usage, including the purpose, duration of data use, and compensation arrangements. By formalising these agreements, data cooperatives ensure that AI developers obtain data in a manner that is compliant with legal and ethical standards while also providing individuals with insight into how their data is used. Importantly, data is licensed to AI developers rather than sold, preserving the integrity of individuals' data rights while enabling fair compensation for its usage. This approach also provides a mechanism for AI developers to ethically and legally obtain data for training or testing their AI systems.

AI developers provide clarity and transparency regarding data usage, rights, and responsibilities, ensuring legal compliance and accountability in data-sharing practices by formalising these agreements.

This innovative approach to implementing data cooperatives in AI development benefits all stakeholders. By exploring the multifaceted challenges and opportunities inherent in implementing data cooperatives in the AI development process through collaborative efforts and a commitment to ethical data stewardship, we can harness the transformative potential of AI technologies while safeguarding individuals' rights promoting the common good and fostering responsible AI development and a sustainable data ecosystem for the future. In this regard, we can consider the following use case.

(i) *Karya's Approach to Implementing Data Cooperatives*

Karya[37] is a pioneering data cooperative designed to address data needs for ethical AI development while providing dignified digital work opportunities to economically disadvantaged communities in India.[38] By leveraging ethical practices, Karya ensures that data collection and usage are transparent, fair, and beneficial to its contributors, creating a sustainable and ethical data ecosystem.

---

[37] About Karya, https://karya.in/, accessed on 15 May 2024.

[38] H. LISA-J. SUHANI-K. ANAHITA, *Bringing Work Home: Flexible Arrangements as Gateway Jobs for Women in West Bengal*, https://steg.cepr.org/publications/bringing-work-home-flexible-arrangements-gateway-jobs-women-west-bengal, 4 June 2024.

Karya's model involves deploying digital work platforms that allow rural workers to participate in data collection and annotation tasks.[39] The platform offers tasks like data labelling and translation, ensuring fair compensation through direct payments to workers and significantly improving their economic conditions.[40] This platform ensures that contributors are compensated fairly, often significantly above the local minimum wage.

Karya's user-friendly design and impactful social mission earned it the IF Design Award for Social Impact in 2023.[41] The award highlighted Karya's innovative approach to providing dignified digital work opportunities for rural communities in India. Karya provides datasets for AI-developing companies by collecting data from its workers (members), who consent to and understand the scope of their data usage. This involves structured tasks such as data annotation and content generation, which are essential for training AI models. As of recently, Karya reports that its platform has been used to complete over 40 million tasks and has empowered over 32,000 workers (members).[42]

Karya significantly contributes to the development of AI models, especially in under-represented languages and regions by providing high-quality, diverse datasets. This approach enhances the accuracy and applicability of AI systems, ensuring that AI development benefits a broader demographic.[43] Karya's success demonstrates the potential of data cooperatives to balance the needs of AI developers with the rights and benefits of data contributors.

(ii) *Impact of Implementation of Data Cooperatives*

Implementing data cooperatives to access data for AI development has the potential for significant outcomes, although it may also lead to challenges and limitations. By examining current use cases such as Karya,[44] we can glean insights into the effectiveness and impact of data cooperatives in practice.

From the use case of Karya, it is clear that data cooperatives can bring several positive impacts. One notable impact of data cooperatives is their potential role in promoting ethical AI development by prioritising transparency, fairness, and accountability in data usage. Data cooperatives can set standards for ethical data practices that can influence broader industry norms by establishing legal frameworks and governance structures that uphold these principles. This includes ensuring that data is collected, processed, and utilised in a manner that respects individ-

[39] *Ibid*.

[40] IBID.

[41] IF Design Awards, 'Social Impact Prize 2023', https://ifdesign.com/en/winner-ranking/project/karya/610827, 1 June 2024.

[42] Karya at LSE 100x Summit Day 2023, https://www.youtube.com/watch?v=mQdgjx60BGc, 28 May 2024.

[43] *Ibid*.

[44] About Karya, https://karya.in/, accessed on 15 May 2024.

uals' privacy rights, mitigates algorithmic bias, and promotes equitable access to AI technologies.[45]

Furthermore, data cooperatives can contribute to the democratisation of AI by empowering diverse stakeholders, including data owners, AI developers, and end-users, to participate in decision-making processes and shape the development and deployment of AI systems. This inclusive approach to AI development fosters greater trust, legitimacy, and acceptance of AI technologies within society, leading to more responsible and socially beneficial applications of AI.[46]

Another potential impact is that data cooperatives could play a crucial role in addressing ethical challenges associated with data governance and ownership. By providing mechanisms for individuals to control their data usage and receive fair compensation for its usage, data cooperatives help mitigate risks such as data exploitation, surveillance, and discrimination. This, in turn, promotes data sovereignty and empowers individuals to assert their rights in the digital age.[47]

Through an analysis of these potential impacts and empirical evidence from existing use cases, we can gain a comprehensive understanding of the transformative potential of data cooperatives in advancing ethical AI development. Harnessing the collective power of data cooperatives, stakeholders can collaborate to build a more inclusive, transparent, and accountable AI ecosystem that benefits society as a whole.

6. Challenges and Considerations.

While the use of data cooperatives in AI development systems holds significant potential for advancing the development of ethical AI, it is imperative to acknowledge that challenges may also arise from its implementation. As data cooperatives emerge as promising mechanisms for ethical data sourcing and utilisation, it is essential to critically examine the hurdles and considerations that accompany their integration into AI development processes, from technical and operational complexities to ethical and regulatory dilemmas, understanding and addressing these challenges are crucial for ensuring the effectiveness, transparency, and fairness of data cooperatives in the AI ecosystem.

The following are the challenges necessary for consideration.

---

[45] D. JAMIE, *Data Protection Beyond Data Rights: Governing Data Production Through Collective Intermediaries*, in *Internet Policy Review*, 2023, vol. 12, issue 3, https://policyreview.info/articles/analysis/data-protection-beyond-data-rights, 11 May 2024.

[46] M. KATHRINE, *Radical proposal: Data Cooperatives Could Give Us More Power Over Our Data*, https://hai.stanford.edu/news/radical-proposal-data-cooperatives-could-give-us-more-power-over-our-data, 5 May 2024.

[47] S. MARK, *Cooperatives Should Embrace the Opportunities of AI*, https://platform.coop/blog/cooperatives-should-embrace-the-opportunities-of-ai/, 13 May 2024.

(i) *Difficulty in Withdrawal of Consent*

One of the primary challenges associated with implementing data cooperatives for controlling data usage in AI training is the difficulty of members withdrawing their consent once their data has been used in training the AI system. In any data processing activity, including AI training, consent from individuals is crucial for ensuring the lawful and ethical handling of their data. However, for consent to be valid, individuals must also have the ability to withdraw their consent[48] as easily as they provided it initially.[49] This poses a significant challenge in the context of AI development, where data may be continuously utilised to train and improve AI models over time.

The question arises: How can individuals request the removal or withdrawal of their data once it has been incorporated into the AI system? Unlike traditional data processing activities where data can be easily deleted or anonymised,[50] the complex nature of AI systems raises concerns about the feasibility of withdrawing consent retroactively.[51] Furthermore, the concept of licensing data adds another layer of complexity. In scenarios where data is licensed to AI developers for a specified period, what happens when the licence expires? Can the data be retrieved, and if so, how? Additionally, does the licence's expiration necessitate the erasure of the AI's memory, considering that the trained model may still retain insights derived from the licensed data?

These critical issues underscore the need for robust mechanisms and protocols to facilitate the withdrawal of consent and the management of data usage rights within data cooperatives. Addressing these challenges requires careful consideration of legal, technical, and ethical frameworks to ensure transparency, accountability, and respect for individuals' data rights throughout the AI development lifecycle.

(ii) *Potential Barriers to Interoperability and Regulatory Compliance*

Indeed, navigating jurisdictional regulatory requirements poses a significant challenge for implementing data cooperatives in AI development.[52] Different countries have distinct data protection laws and regulations, so ensuring compliance across multiple jurisdictions can be complex and demanding. Global corporations

---

[48] Article 7.3.1 of the GDPR.

[49] Information Commissioner's Office (UK), *How do we ensure Lawfulness in AI*, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/how-do-we-ensure-lawfulness-in-ai/#inferences, 13 May 2024.

[50] Ada Lovelace Institute, UK AI Council, *Exploring Legal Mechanism for Data Stewardship*, 2021, https://www.adalovelaceinstitute.org/wp-content/uploads/2021/03/Legal-mechanisms-for-data-stewardship_report_Ada_AI-Council-2.pdf, 5 June 2024.

[51] Usercentrics, Artificial Intelligence (AI), Personal Data And Consent, 2023, https://usercentrics.com/knowledge-hub/artificial-intelligence-ai-act-and-consent/, 5 June 2024.

[52] M. AHMED-B. SPOONER-J. ISHERWOOD, *A Systematic Review of the Barriers to the Implementation of Artificial Intelligence in Healthcare*, Cureus. 2023, (PubMed Central) Vol. 10, Issue 3.

engaging in AI development must contend with varying legal frameworks governing data usage, privacy, and security.

Interoperability presents yet another challenge. Data cooperatives may need to integrate with existing data systems and platforms used by AI developers, government agencies, and other stakeholders. Ensuring seamless data exchange and compatibility between different systems and formats is essential for maximising the utility and value of data cooperatives in AI development. Additionally, regulatory compliance extends beyond data protection laws to encompass other legal and ethical considerations. Data cooperatives must adhere to industry standards, best practices, and ethical guidelines governing data collection, usage, and sharing. This includes obtaining proper consent from data subjects, implementing robust security measures to protect sensitive information, and respecting individuals' rights to privacy and data ownership.

(iii) *Maintenance, Storage, and Preservation of Member Data*[53]

As data cooperatives endeavour to collect, manage, and maintain diverse datasets, they encounter significant challenges related to maintaining, storing, and preserving member data to ensure that the collected data remains accessible, relevant, and of high quality over time. This necessitates robust systems and processes for data storage, management, and curation.

One of the primary concerns is scalability, particularly as data cooperatives expand in membership and scope. The growing influx of data from an increasing number of members poses challenges in terms of infrastructure and processes. Scalability becomes crucial to ensure that the cooperative's systems can handle the growing volumes of data efficiently while maintaining effectiveness. Scaling up data management systems and platforms requires substantial investments in technology and personnel to accommodate the expanding datasets.

Moreover, maintaining the quality and relevance of the data is paramount. Data collected by cooperatives must be accurate, reliable, and up-to-date to ensure its utility for various applications, including AI development. However, ensuring data quality can be challenging, especially when dealing with diverse sources and formats of data. Data cleansing, normalisation, and validation processes are essential to address inconsistencies and errors in the collected datasets.

Additionally, data preservation is crucial to retain the integrity and usability of historical data. Cooperatives must implement strategies for long-term data preservation to ensure that valuable insights derived from past data remain accessible for future analysis and research. This involves adopting data archiving and backup mechanisms to safeguard against data loss or corruption.

---

[53] H. THOMAS-P. ALEX, *Data Cooperatives: Towards a Foundation for Decentralised Personal Data Management*, 2019, https://www.researchgate.net/publication/333309091_Data_Cooperatives_Towards_a_Foundation_for_Decentralized_Personal_Data_Management, 5 May 2024.

(iv) *Scope of Data Usage*

Data protection issues present significant challenges in the implementation of data cooperatives for controlling data usage in AI training. One key issue revolves around the lack of clear guidelines or yardsticks to determine how AI developers will utilise the data collected by cooperatives. Unlike traditional data usage scenarios where the scope of use may be more defined, AI applications introduce complexities that may extend beyond initial consent agreements. Individuals may consent to specific uses of their data, but AI algorithms can potentially utilise the data for multiple purposes, some of which may not have been anticipated or explicitly consented to by the individual.

While data cooperatives provide individuals with a sense of transparency and control over their data by offering visibility into where their data is being used, concerns arise regarding whether the data usage scope aligns with the consent threshold established by individuals. Consent mechanisms within data cooperatives may struggle to account for the multifaceted nature of AI use cases, where data can be repurposed or combined with other datasets to derive new insights. This complexity can make it challenging for individuals to fully understand the implications of consenting to data usage within the context of AI development.

Furthermore, the lack of clarity surrounding consent in AI-driven data processing raises questions about accountability and responsibility. While individuals may consent to data usage based on certain assumptions or expectations, developers may not always understand the underlying reasons for AI-driven processing decisions. This disconnect can create ambiguity around the ethical and legal implications of data usage within data cooperatives, highlighting the need for robust governance mechanisms and transparency in AI development processes.

(v) *Fair Compensation and Equity*

Determining fair monetary compensation for data usage within data cooperatives presents a complex challenge, particularly in ensuring equity across diverse demographics and societal contexts. Several factors contribute to this challenge, including variations in economic conditions, cultural norms, and historical inequalities among different populations.

One key consideration is the equitable distribution of compensation among data contributors, regardless of their geographical location or socioeconomic status. While data cooperatives aim to empower individuals by providing economic opportunities through data sharing, disparities in compensation rates based on geographic or demographic factors can exacerbate existing inequalities. For example, paying individuals from economically disadvantaged regions or marginalised communities lower compensation rates than their counterparts in wealthier regions would perpetuate economic disparities and contribute to social injustice.

Additionally, addressing gender and other forms of intersectional inequalities is crucial in determining fair compensation within data cooperatives. Women and other marginalised groups may face systemic barriers to accessing economic op-

portunities, including discrimination in employment and unequal pay. Failing to account for these disparities in compensation structures within data cooperatives can further marginalise vulnerable populations and reinforce existing power imbalances.

Furthermore, data cooperatives must navigate complex societal contexts, including over-representative misogynistic attitudes, which may impact the fair treatment of women and other marginalised individuals. In such contexts, there is a risk of perpetuating gender-based discrimination and exploitation through data exploitation practices.

7. The Way Forward: Future Directions and Recommendations.

As we look ahead to the future of more data cooperatives being used to enhance individual control over data usage in AI training like Karya, several key research directions and practical recommendations emerge. These recommendations encompass various aspects, ranging from regulatory oversight to technical infrastructure and communication strategies. By implementing these recommendations, we can foster data cooperatives' responsible and effective operation while promoting transparency, compliance, and trust among members and stakeholders.

(i) *Development of Proper Storage Systems*

Proper storage systems must be developed to ensure the secure and efficient management of data within data cooperatives, and technical personnel dedicated to overseeing storage and maintenance activities must be established. These personnel would be responsible for implementing robust data storage infrastructure, ensuring data security and integrity, and addressing any technical issues that may arise. Investing in the right technology and expertise can enable data cooperatives to enhance their data management capabilities and mitigate data breaches or loss risks.

(ii) *Operating a Record Book for Activities and Operations*

Another important recommendation is the establishment of a comprehensive record-keeping system to document the activities and operations of data cooperatives. This record book would serve as a transparent and accountable repository of information detailing key decisions, transactions, and interactions within the cooperative. Data cooperatives can facilitate internal governance, compliance monitoring, and external audits by maintaining accurate records, thereby enhancing transparency and accountability to members and regulators.

(iii) *Establishment of Policies Aligned with Regulatory Requirements*

Data cooperatives should develop and implement policies tailored to fit the provisions of the DGA and the GDPR. These policies should outline clear guidelines and procedures for data collection, usage, sharing, and retention, ensuring compli-

ance with legal and ethical standards. Data cooperatives can minimise legal risks, protect member rights, and build stakeholder trust by aligning with regulatory requirements.

(iv) *Avenue for Communication with Members and Cooperative Leaders*

Effective communication channels should be established to facilitate dialogue and engagement between cooperative members and leaders. This avenue for communication can take various forms, including regular meetings, newsletters, online forums, and feedback mechanisms. Fostering open and transparent communication can enable data cooperatives to solicit input from members, address concerns, and build consensus on key issues affecting the cooperative's operations and direction.

8. Conclusion.

In conclusion, the utilisation of data cooperatives presents a promising avenue for enhancing individual control over data usage in AI development processes. This paper has explored the potential benefits, challenges, and considerations associated with implementing data cooperatives, drawing insights from existing use cases and research findings.

Data cooperatives offer a collaborative framework for individuals to pool and manage their data resources, empowering them to exercise greater agency over how their data is used. Data cooperatives can promote responsible data usage while safeguarding individual rights and interests by establishing transparent governance structures, implementing ethical data practices, and fostering community engagement.

However, implementing data cooperatives is not without its challenges. Concerns related to consent withdrawal, regulatory compliance, data protection, and equitable compensation require careful consideration and proactive measures to address. Additionally, the scalability and interoperability of data cooperatives pose technical and logistical challenges that must be navigated to ensure their effectiveness and sustainability.

Moving forward, it is imperative to pursue future research directions and practical recommendations aimed at advancing the development and adoption of data cooperatives. This includes enhancing data governance frameworks, strengthening legal and regulatory frameworks, promoting ethical data practices, facilitating interdisciplinary collaboration, and empowering community engagement.

Furthermore, collaboration between stakeholders, including policymakers, researchers, industry players, and civil society organisations, is essential for driving progress in this space. By working together, we can harness the transformative potential of data cooperatives to foster innovation, promote economic empowerment, and advance the ethical development of AI systems.

In summary, data cooperatives represent a promising model for democratising data access and usage, empowering individuals, and promoting responsible AI development. Through concerted efforts and collaboration, we can realise their full potential and shape a more equitable, transparent, and inclusive future for AI.

Capitolo IX

Cooperative di dati per creare un'Intelligenza Artificiale Sociale

Vanni Rinaldi

Abstract: New information technologies are changing the traditional way of seeing things and in some ways also the world as we know it. Artificial Intelligence (AI) could lead humans to overcome their cognitive and biological limits. Thus wrote the philosopher Sebastiano Maffettone in the preface of the book from Coops to Co-Apps, which set the objective of critically analyzing the relationship between us as users and the digital platforms to create "a new virtuous and equal relationship" in the cyberspace. This question is also at the basis of this paper, which aims to analyze the risks but also the remedies, facing the tumultuous development of AI technologies. To make them not only more reliable but also more fair, preserve them from the exclusive purpose of profit and reduce the harm for the users/citizens. To achieve this objective, it is proposed to diversify the concept of Artificial Intelligence, expanding it to a new category defined as "Social Artificial Intelligence". The creation (feeding) of these Social AI will have to take place through a new cooperative entity (or service): the "data cooperatives", which are finally available to European citizens, thanks to the Data Governance Act. The second chapter compares the current AI model based on the expropriation of user data by digital capitalist companies with social artificial intelligence. Social AI is a technology for the use and analysis of digital data that responds primarily to the needs of citizens/users, whose ownership is democratic, enhancing the human factor. We could define it as a sort of digital public good, as opposed to the dominant use of AI managed by capitalist companies whose ultimate goal is profit and "control". The rest of the chapter presents the numerous risks of the AI, as it is developed today, before moving on to depict the remedies. In the third chapter is analyzed the possibility of sharing digital data in a cooperative form to build real "trust networks" capable of competing with the "expropriatory" logic of private platforms. Is also analyzed the case of "data cooperatives" and the "digital mutualism", understood as an alternative to the risks of the capitalistic model. These are also elements of a renewal of cooperative principles accepting the changes introduced by digital technologies, and using them for a "cooperative rebirth" in the construction of public digital goods and between them the Social Artificial Intelligence. Finally, an analysis is dedicated in the fourth chapter on how to build an Alliance between the forces of the "Social Economy" to be able to create Social AI in Italy. Some sectors are analyzed in which to concretely experiment with this possibility and also what are the economic and technological resources available to create a favorable and safe envi-

ronment for the use of Artificial Intelligence guided no longer only by individual profit but also by common well-being.

Sommario: 1. Premessa. – 2. L'Intelligenza Artificiale e l'Intelligenza Artificiale Sociale. – 2.1. Cos'è l'Intelligenza Artificiale. – 2.2. I rischi dell'Intelligenza Artificiale. – 2.3. I rimedi. – 3. Condividere i dati per costruire beni comuni digitali. – 3.1. Un "New Deal" dei dati. – 3.2. Il contesto giuridico europeo sull'utilizzo e la condivisione dei dati. – 3.3. Il ruolo delle cooperative di dati e il mutualismo digitale. – 4. Le cooperative di dati e l'Intelligenza Artificiale Sociale. – 4.1. L'Intelligenza Artificiale Sociale. – 4.2. Un'Alleanza per l'IA Sociale.

1. Premessa.

«Le nuove tecnologie informatiche stanno cambiando il modo tradizionale di vedere le cose e in qualche maniera anche il mondo così come lo conosciamo. La Intelligenza Artificiale (IA) potrebbe condure l'essere umano a superare i suoi limiti cognitivi e biologici. Con il rischio futuribile ma non troppo di creare un universo in cui l'intelligenza sia separata dalla consapevolezza e dalla umanità stessa. Un rischio distopico quest'ultimo che impone una riflessione pubblica. Non si tratta di una novità. Proprio su un presupposto di questo tipo, le ICTs (*Information and Communication Technologies*) sono state studiate non solo dal punto di vista della scienza e delle sue applicazioni ma anche dal punto di vista del loro impatto morale, sociale e ontologico» [1]. Così ha scritto il Filosofo Sebastiano Maffettone nella prefazione del libro dalle Coop alle Co-App, nel quale veniva posto l'obiettivo di analizzare criticamente il rapporto tra noi utenti e le piattaforme digitali per creare «un nuovo rapporto virtuoso e paritetico» e quindi più giusto, tra queste entità nel nuovo mondo digitale. Un tentativo di "mutualizzare il digitale" attraverso la condivisione dei dati digitali in forma cooperativa che il progetto «*Cooperative Commons*» [2], guidato dal Prof. Maffettone e realizzato da Legacoop e dall'Università Luiss nel 2013, aveva posto alla base di un modello alternativo, appunto cooperativo e democratico, del futuro digitale. Questo ragionamento è alla base anche di questo *paper*, che vuole analizzare i rischi ma anche i rimedi, di fronte al tumultuoso sviluppo delle tecnologie dell'IA, per renderle non solamente più affidabili ma anche più giuste, sottraendole almeno in parte all'esclusiva finalità del profitto e ai danni che ciò comporterebbe per noi utenti/cittadini. Per far questo viene proposto di diversificare il concetto di Intelligenza Artificiale, ampliandolo ad una nuova categoria definita come «*Intelligenza Artificiale Sociale*». La creazione (alimentazio-

[1] S. MAFFETTONE, *Prefazione*, in V. RINALDI, *Dalle Coop alle Co-App. Per una condivisione etica dei Big Data*, Soveria Mannelli (CZ), 2019, pp. 7-11.

[2] *Il Manifesto "Cooperative Commons"*, in V. RINALDI, *Dalle Coop alle Co-App. Per una condivisione etica dei Big Data*, cit., pp. 89-91.

ne) di queste IA Sociali dovrà avvenire attraverso un nuovo soggetto (o servizio) cooperativo: le «*cooperative di dati*», che sono finalmente a disposizione dei cittadini europei, e quindi anche italiani, grazie al *Data Governance Act*[3]. Nel secondo capitolo viene confrontato l'attuale modello di IA basato sull'espropriazione dei dati degli utenti e sul loro utilizzo da parte delle imprese capitalistiche digitali (il modello molto efficacemente analizzato e descritto dalla Prof.ssa Shoshana Zuboff nel suo libro sul «Capitalismo di sorveglianza»)[4], con l'IA Sociale. L'IA Sociale è una tecnologia di utilizzo e analisi dei dati digitali che risponde prioritariamente ai bisogni dei cittadini/utenti, la cui proprietà è democratica, valorizzando il fattore umano. Quindi potremmo definirla come una sorta di bene pubblico digitale, in contrapposizione all'utilizzo dominante di IA gestite da società capitalistiche il cui fine ultimo è il profitto e il "controllo"[5]. Nel prosieguo del capitolo vengono presentati i numerosi rischi a cui l'IA, così come oggi viene sviluppata, sottopone noi tutti per passare poi a raffigurare i rimedi possibili sia da un punto di vista "passivo" (comprendendo in questa categoria gli elementi più di natura giuridica) sia da un punto di vista più "contrattualistico", per consentire agli utenti di riequilibrare il rapporto attivando appunto delle IA Sociali per realizzare obiettivi rispondenti a degli interessi generali. Per consentire questo obiettivo di "*empowerment*" del cittadino/consumatore, nel terzo capitolo viene analizzata la possibilità di condividere i dati digitali in forma cooperativa per costruire delle vere e proprie "reti fiduciare" capaci di competere con le logiche "espropriative" delle piattaforme private. Vengono enumerati anche i dispositivi giuridici che a livello europeo consentono una simile strategia di condivisione dei dati, e infine viene analizzato il caso delle "cooperative dei dati" e i presupposti giuridico-politici del "mutualismo digitale", inteso come alternativa ai rischi del modello "espropriativo capitalistico", ma anche come elemento rinnovamento dei principi cooperativi in direzione dell'accoglimento dei cambiamenti introdotti dalle tecnologie digitali, e il loro utilizzo ai fini di una "rinascita cooperativa"[6] per la costruzione di beni digitali pubblici, tra cui appunto le IA Sociali. Infine viene dedicato un approfondimento nel quarto capitolo su come costruire un'Alleanza tra le forze dell'"Economia Sociale" per poter realizzare in concreto IA Sociali in Italia, e si analizzano alcuni settori in cui sperimentare concretamente tale possibilità e anche quali sono i mezzi economici e tecnologici a disposizione di questo progetto.

---

[3] Regolamento europeo inserito nella strategia digitale della UE che regolamenta l'utilizzo dei dati digitali (Reg. UE n. 868/2022, relativo alla *governance* europea dei dati).

[4] S. ZUBOFF, *Il capitalismo della sorveglianza: il futuro dell'umanità nell'era dei nuovi poteri*, Roma, 2023.

[5] *Ibidem.*

[6] J. RIFKIN, *La società a costo marginale zero*, Milano, 2014, pp. 296-305.

2. L'Intelligenza Artificiale e l'Intelligenza Artificiale Sociale.

2.1. Cos'è l'Intelligenza Artificiale.

Come ha recentemente sottolineato il Filosofo Maurizio Ferraris «nel momento in cui le nostre attenzioni sono polarizzate dall'Intelligenza Artificiale, diamo per scontato di sapere cosa è l'intelligenza naturale, il che è tutt'altro che ovvio» [7]. È però un dato di fatto che da quando i primi prototipi di Intelligenza Artificiale sono stati rilasciati nel *web*, molto si è teorizzato su cos'è e a cosa serve l'Intelligenza Artificiale. Al netto comunque, della inevitabile polarizzazione tra tecno catastrofisti e tecno entusiasti, si può affermare che L'IA è sicuramente una tecnologia prodotta dall'uomo, come le altre, per soddisfare i suoi bisogni.

La definizione di sistemi di IA contenuta ad esempio nell'*Executive Order* di Biden è molto ampia e non si limita all'IA generativa o ai sistemi che sfruttano le reti neurali. Si tratta di «un sistema basato su macchine che può, per un dato insieme di obiettivi definiti dall'uomo, fare previsioni, raccomandazioni o decisioni che influenzano ambienti reali o virtuali» [8].

Così pure come la definizione dell'originaria Proposta di Regolamento UE sull'IA, del 21 aprile 2021, che all'art. 3, n. 1), forniva la seguente definizione: «"sistema di intelligenza artificiale" (sistema di IA): un *software* sviluppato con una o più delle tecniche e degli approcci elencati nell'allegato I, che può, per una determinata serie di obiettivi definiti dall'uomo, generare *output* quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono» [9].

Nel 1991 agli albori della ricerca applicata sulla Intelligenza Artificiale l'ingegnere americano James Albus definì l'intelligenza come «la capacità di un sistema di agire in modo appropriato in un ambiente incerto, dove le azioni appropriate sono quelle che aumentano le probabilità di successo» [10]. Quindi, forse, come sostiene il Prof. Cristianini, «abbiamo cercato l'intelligenza nei posti sbagliati: non arriverà nella forma di un robot senziente, quanto piuttosto in quella di un'infrastruttura in grado di apprendere, o magari di una macchina sociale che prende deci-

---

[7] M. FERRARIS, *Aspenia 2024*, tratto dal *Corriere della Sera*, Milano, 21 marzo 2024.

[8] Cfr. THE WHITE HOUSE, *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, 30 October 2023, https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.

[9] COMMISSIONE EUROPEA, *Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'unione*, Bruxelles, 21 aprile 2021, COM(2021) 206 final, https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0006.02/DOC_1&format=PDF.

[10] N. CRISTIANINI, *La scorciatoia: come le macchine sono diventate intelligenti senza pensare in modo umano*, Bologna, 2023, p. 15.

sioni cruciali per noi e su di noi, con criteri che non riusciamo a capire. Il suo comportamento sarà plasmato da relazioni statistiche scoperte in dati prodotti da attività umane e progettato al fine di perseguire qualche scopo [11]. La nuova scienza delle macchine intelligenti parla la lingua della probabilità e dell'ottimizzazione matematica, non più quella della logica e del ragionamento formale» [12]. L'IA è in definitiva un ulteriore strumento tecnico umano, e quindi come tale non ha certo finalità autonome.

Le forme di IA che abbiamo visto all'opera finora sono infatti un'esplosiva ed energivora concentrazione di Hardware (*computer* e *chip*), algoritmi (e alla fin fine secondo Cristianini, un algoritmo è solo una ricetta) [13] ed enormi quantità di dati digitali (i famosi *Big Data*). Oggi, ad esempio, le raccomandazioni di Amazon si basano su centinaia di milioni di clienti, quelle di YouTube su due miliardi di utenti, e il primo modello di linguaggio – GPT-3 – aveva circa 175 miliardi di parametri, che devono essere appresi analizzando circa 45 terabyte di testo ottenuti da fonti diverse [14]. Questa potentissima miscela tecnologica riesce a simulare statisticamente un agente intelligente ovvero un qualsiasi sistema in grado di agire nel suo ambiente, usando informazioni sensoriali per prendere decisioni. Anche se non sa perché lo fa, anche se accosta su base probabilistica parole ad altre parole senza altro intento che quello di trovare appunto una relazione statisticamente probabile di successo. Questo perché la tecnologia è competenza (usata) senza comprensione. Non ho alcun bisogno, dice il Prof. Ferraris, di conoscere le leggi della fisica per andare in bicicletta così come non ho alcun bisogno di conoscere le leggi dell'informatica per usare un telefonino [15].

Figuriamoci quindi se ne ha bisogno una macchina. E allora ci ammonisce Cristianini, «grandi quantità di dati e modelli non-teorici del mondo possono generare comportamenti utili, anche se non ci possono insegnare niente del fenomeno stesso che riproducono. Potrebbe non esistere alcun modo di interpretare le decisioni delle nostre macchine, il che sarebbe invece desiderabile per controllare che non prendano una brutta piega» [16]. Il punto è che l'IA sa fare il suo compito in una maniera più efficace dell'essere umano. Quindi, se come è probabile, questo strumento diventerà generalista, si potrà usare più o meno per fare qualsiasi cosa: per scrivere un articolo, una tesi universitaria, analizzare un referto medico, disegnare un edificio, guidare un'automobile, supportare un giudice ad emettere una sentenza con validità giuridica, etc.

---

[11] N. CRISTIANI, *op. cit*., p. 210.

[12] N. CRISTIANI, *op. cit*., p. 30.

[13] N. CRISTIANI, *op. cit*., p. 27.

[14] N. CRISTIANI, *op. cit*., p. 56.

[15] M. FERRARIS-G. SARACCO, *Tecnosofia, tecnologia e umanesimo per una scienza nuova*, Roma-Bari, 2023, p. 112.

[16] N. CRISTIANI, *op. cit*., p. 74.

Allora ci si deve necessariamente, e rapidamente, porre il problema di quali rischi questa nuova tecnologia comporta e di come contenerli per raggiungere gli obiettivi desiderati.

Esattamente come è sempre stato fatto per tutte le tecnologie che hanno un impatto significativo sulle persone e sulla società. Ma dobbiamo anche interrogarci su come fare a rendere questa nuova tecnologia, e tutti gli enormi vantaggi che ne possono derivare per la società, affidabile e utilizzabile per scopi sociali. Come ha ricordato Papa Francesco «L'intelligenza artificiale deve essere intesa come una galassia di realtà diverse e non possiamo presumere a priori che il suo sviluppo apporti un contributo benefico al futuro dell'umanità e alla pace tra i popoli [17]. Tale risultato positivo sarà possibile solo se ci dimostreremo capaci di agire in modo responsabile e di rispettare valori umani fondamentali come "l'inclusione, la trasparenza, la sicurezza, l'equità, la riservatezza e l'affidabilità"» [18].

Ecco dunque che sorge la necessità di immaginare un nuovo tipo di IA: un'Intelligenza Artificiale sì, ma Sociale.

Uno strumento tecnologico che nel proprio "DNA Digitale" cioè, sia nella forma proprietaria dei mezzi tecnici, che nella sua governance, così come negli algoritmi che la animano, abbia i principi dell'"umanità". E che, sempre secondo le parole di Papa Francesco, «porterà più eguaglianza… favorendo l'ascolto dei molteplici bisogni delle persone e dei popoli» [19].

L'IA sociale, come vedremo nel quarto capitolo, dovrebbe essere dunque una sorta di bene pubblico digitale, caratterizzato da un punto di vista identitario come un soggetto collettivo a partecipazione volontaria, con governance democratica, mutualistico e solidaristico. Perché «non è responsabilità di pochi, ma dell'intera famiglia umana» [20].

2.2. I rischi dell'Intelligenza Artificiale.

Molti sono i potenziali rischi dell'Intelligenza Artificiale che bisognerà prendere in considerazione con serietà e rapidità. Come ha scritto Cristianini: «la tecnologia può indebolire certi valori sociali, come privacy, uguaglianza, autonomia o libertà di espressione, per esempio consentendo sorveglianza di massa mediante telecamere stradali, o persuasione di massa mediante targeting psicometrico. Può anche causare danni, sia quando funziona male sia quando causa effetti imprevisti. Potrebbe perfino giungere a destabilizzare i mercati, influenzare l'opinione pubblica, o accelerare la

[17] PAPA FRANCESCO, *Messaggio per la 57 giornata della pace*, Roma, 1° gennaio 2024.

[18] PAPA FRANCESCO, *Discorso del santo padre francesco ai partecipanti all'incontro dei "Minerva Dialogues" promosso dal dicastero per la cultura e l'educazione*, Città del Vaticano, 27 marzo 2023, https://www.vatican.va/content/francesco/it/speeches/2023/march/documents/20230327-minerva-dialogues.html.

[19] PAPA FRANCESCO, *Messaggio per la 58 giornata delle comunicazioni sociali*, Roma, 2024.

[20] PAPA FRANCESCO, *Messaggio per la 57 giornata della pace*, cit.

concentrazione della ricchezza nelle mani di quelli che controllano i dati o gli agenti» [21]. Tra i problemi che pone lo sviluppo della I.A. e in particolare di quella cosiddetta generalista, c'è anche in prospettiva quale effetto cumulato del suo utilizzo, una vera e propria "omogeneizzazione digitale" della conoscenza.

Se infatti il linguaggio della nuova disciplina è oggi quello della statistica e dell'ottimizzazione, e come scrive il Prof. Ferraris «quanto più cresce la conoscenza dei comportamenti umani attraverso i dati generati dai nostri comportamenti, tanto più questi comportamenti si rivelano prevedibili e uniformi» [22] bisogna incominciare a porsi seriamente il problema di un effetto progressivo di appiattimento ed omologazione culturale e cognitivo prodotto dai risultati generati dalla IA. Il rischio è che un ripetuto e prolungato apprendimento da parte dell'IA su *data set* analizzati con principi statistici potrebbe portare nel tempo a una sorta di "dittatura della gaussiana". Infatti i modelli probabilistici di analisi dei dati lavorano sulle possibilità che un certo risultato sia statisticamente più valido e cioè più probabile. Operano di fatto eliminando i risultati statisticamente posti agli estremi di una qualsiasi curva dell'apprendimento. Ora se questo metodo è sicuramente "una scorciatoia" che permette a questi agenti di arrivare rapidamente a risultati accettabili statisticamente, ciò naturalmente non significa che questi risultati siano desiderabili, al di là di un loro uso immediato in risposta ad una determinata richiesta. Infatti verrebbero tagliate tutte le ipotesi statisticamente meno frequenti creando dei *bias* omologativi nei percorsi della creazione della conoscenza nelle macchine. Sembra plausibile dice il Prof. Cristianini nel suo libro, che il «pregiudizio» (bias) possa entrare nella macchina attraverso l'uso di dati «trovati in natura», che quindi riflettono le disuguaglianze già esistenti nel mondo [23]. Basti pensare all'uso dell'IA nella scrittura. Le relazioni statistiche tra le parole validate attraverso il calcolo probabilistico sono influenzate dai data set di quanto pubblicato. Per cui per assurdo se gli agenti di produzione di contenuti (case editrici, giornali, etc.), favorissero un particolare modello di scrittura (ad esempio quello della fiction), o come già avviene una prevalenza linguistica ad esempio quella anglofona, avremmo un rafforzamento statistico di questa tipologia di scrittura nei data set di alimentazione dell'IA, con il risultato di produrre un rafforzamento delle risposte stilistiche e linguistiche di questo tipo da parte dell'IA. E se ciò corrispondesse nel lungo periodo anche a scelte degli agenti di produzione dell'IA, avremmo una progressiva eliminazione degli altri stili di scrittura e una progressiva omogeneizzazione culturale. Secondo un lavoro della University of Oxford, i modelli addestrati sui propri risultati producono risultati molto meno precisi e variegati dei dati di addestramento [24].

---

[21] N. CRISTIANINI, *op. cit.*, p. 205.

[22] M. FERRARIS, *op. cit.*, p. 135.

[23] N. CRISTIANINI, *op. cit.*, p. 98.

[24] T. CLABURN, *What is Model Collapse and how to avoid it*, in *The Register*, 26 gennaio 2024, https://www.theregister.com/2024/01/26/what_is_model_collapse/.

Inoltre secondo uno studio sul "pappagallo stocastico", realizzato da alcuni ricercatori della Washington University «la maggior parte della tecnologia linguistica [usata nei *Language Model – LM* che sono alla base di alcune IA generative come Chat-Gpt, *n.d.a.*] è costruita per soddisfare le esigenze di chi ha maggiori privilegi nella società, e cioè di chi ha le risorse economiche per acquistare un Google Home, Amazon Alexa o un dispositivo Apple con Siri installato, tecnologie che parlano con una tipologia di linguaggio adeguata al livello dei propri clienti. E quindi, quando i grandi LM codificano e rafforzano i pregiudizi predominanti, è molto probabile che i danni che ne conseguono ricadano sulle persone emarginate che, anche nelle nazioni ricche, è più facile che sperimentino forme di razzismo ambientale» [25].

Ancora più serio risulta il problema se lo analizziamo dal punto vista ad esempio della ricerca scientifica in campo farmacologico per i nuovi medicinali. I *data set* epidemiologici oggi riflettono nella stragrande maggioranza l'interesse delle *Big Pharma*, che li finanziano, per la realizzazione di medicinali che siano in grado di generare maggiori introiti economici e su più lunghi periodi, come ad esempio nel caso della cura del diabete rispetto alla ricerca di nuovi antibiotici. Ebbene in questo caso sarebbe facile prevedere che l'IA utilizzata nella ricerca scientifica in questo settore, nel tempo, produrrà risultati statisticamente in linea con questa premessa di mercato e quindi si rafforzerebbe il circuito vizioso aumentando i risultati a favore di una ricerca di nuovi medicinali destinati solo a curare alcune malattie, in particolare quelle con maggiori possibilità di profitti economici. Ma questo vale anche per i dati sanitari generali delle persone. Google, ad esempio, ha stretto un accordo controverso con Ascension Sistemi Sanitari per l'accesso alle cartelle cliniche dei pazienti ai fini della formazione diagnostica e altri sistemi di intelligenza artificiale medica, e ha inoltre pagato 2,1 miliardi di dollari per acquistare Fitbit, ancora una volta con un occhio alla raccolta di parametri e dati sanitari [26].

Considerato che l'IA attualmente, per come si è sviluppata la filiera digitale, è un derivato delle *Big Tech* che sono attualmente le uniche che dispongono dei fattori produttivi necessari (computer, algoritmi e *Big Data*), il rischio ulteriore è che i monopoli economici del digitale, si andranno a trasformare in veri e propri monopoli digitali della conoscenza che si potrebbero saldare con altri monopoli come quelli delle *Big Pharma* nel campo sanitario o quelli della logistica, aumentando gli effetti distorsivi della concorrenza ed esercitando sempre più un ruolo non soltanto nell'economia, ma nell'intera società, scollegato da ogni controllo e contrappeso democratico. Secondo uno studio della Vanderbilt University Law School «la concentrazione nel settore della tecnologia dell'intelligenza artificiale aumenta le

---

[25] E.M. BENDER et al., *On the Dangers of Stochastic Parrots: Can Language Models Be Too Big?*, in *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*, March 2021, pp. 610-623.

[26] T.N. NARECHANIA-G. SITARAMAN, *An Antimonoply Approach to Governing Artificial Intelligence*, n *Vanderbilt Law Research Paper*, No 24-9, November 2023; p. 18.

preoccupazioni sulla disuguaglianza economica nella società, perché non solo può portare ad avere un piccolo numero di aziende con un potere economico fuori misura, ma anche concentrare la ricchezza in un piccolo numero di individui: dirigenti e azionisti. Infine, la struttura del mercato della tecnologia IA, ai suoi vari livelli, è preoccupante per il futuro della democrazia. Infatti la concentrazione nell'intelligenza artificiale può dare a un numero relativamente piccolo di aziende un'enorme influenza sulle informazioni dell'ecosistema, sommandosi all'enorme influenza politica che ottengono dalla loro crescente ricchezza e potere» [27].

Basti pensare al fatto che un robot dopo milioni di operazioni in laparoscopia sarebbe irraggiungibile da qualunque chirurgo umano, sia per efficienza (24/7) che per efficacia. A quel punto non si laureerebbe più nessun chirurgo in quella specialità, ma avremmo solo operatori con abilità tecnica ma senza conoscenza. Si rischierebbe così anche di perdere la possibilità di innovare cambiando le tecniche operatorie. Perché la macchina sarebbe sì la più brava, ma ripetendo all'infinito e ottimizzando al massimo quello che già sa fare. Così come non ci sarebbe più nessuno stimolo per un giovane a studiare per 10 anni radiologia quando l'IA sarebbe in grado di fare meglio e a costi infinitesimali il suo lavoro. Così si avrebbe un'enorme concentrazione monopolistica nelle poche imprese proprietarie di quelle tecnologie. Ma questo sarà vero anche per un giornalista, per un notaio, per un attore, per un autista, per un pilota, etc.

Un'ulteriore conferma dei rischi, da non sottovalutare, deriva dal fatto che l'Intelligenza Artificiale «può anche essere usata per applicazioni militari, in modi che non vogliamo immaginare» [28].

E purtroppo abbiamo avuto recentemente conferma che non si tratta più di semplici speculazioni o immaginazioni ma di una realtà. Infatti secondo alcune recenti inchieste giornalistiche, [29] accreditate da diverse fonti militari israeliane, l'esercito di Tel Aviv nelle prime settimane di guerra a Gaza, ha utilizzato un'IA per decidere la lista degli obiettivi umani da eliminare nella striscia di Gaza. Questo lavoro è stato svolto da un'IA di nome Lavander che attraverso l'uso di Big Data sui cittadini palestinesi ha identificato migliaia di obiettivi umani sulla base di determinate caratteristiche. A detta delle stesse fonti israeliane questa IA aveva un margine di errore del 10%. Inoltre, mentre inizialmente i risultati dell'IA venivano rivisti da personale umano, per aumentare la velocità dei bombardamenti il controllo è stato successivamente limitato alla sola verifica del genere (maschile) dell'obiettivo da eliminare (per un tempo stimato dell'operato umano di 20 sec), lasciando quindi di fatto in autonomia alla macchina il compito della selezione dei target.

Inoltre una seconda IA, basata su *Big Data* di localizzazione, provvedeva a veri-

---

[27] *Ibidem*; T.N. NARECHANIA-G. SITARAMAN; p. 5.

[28] N. CRISTIANINI, *op. cit.*, p. 205.

[29] Y. ABRAHAM, *'Lavander': The AI machine directing Israel's bombing spree in Gaza*, in *+972 Magazine*, 3 aprile 2024, https://www.972mag.com/lavender-ai-israeli-army-gaza/.

ficare la presenza del target presso la sua abitazione e decidere quindi il momento in cui bombardare. In questa fase sono stati anche allentati i criteri etici di valutazione dei danni collaterali (vittime innocenti) alzando il numero di parecchie volte i precedenti parametri. Anche per questo secondo agente digitale il margine di errore è stato alto in relazione in particolare ai tempi tecnici tra l'identificazione della presenza e l'effettivo momento del bombardamento, con l'effetto che in numerosi casi il target selezionato non era più nella abitazione, al contrario dei suoi famigliari che sono stati perciò uccisi [30]. L'uso dell'IA per scopi militari da parte dell'esercito israeliano è quindi stato alla base dell'alto numero di morti di civili nelle prime settimane della guerra di Gaza.

2.3. I rimedi.

È evidente che, alla luce di questi potenziali rischi, oltreché in base a normali criteri di precauzione, bisognerà agire sul lato dei rimedi se si vuole utilizzare questa tecnologia in sicurezza e creare fiducia e ambienti consapevoli e favorevoli per l'uso dell'IA. Ultimamente qualcosa si sta facendo nell'ambito delle azioni di contenimento, tra le quali rientrano ad esempio i nuovi regolamenti emanati sull'IA.

L'Executive Order [31] emanato da Biden negli Usa, ad esempio, impone agli sviluppatori di alcuni sistemi di IA di condividere i risultati dei loro test e le informazioni più critiche con il governo degli Stati Uniti. Ciò in base al Defense Production Act del 1950, cui normalmente si ricorre in situazioni di emergenza nazionale o crisi produttiva. Il punto delicato rimane però che molti aspetti dell'EO si basano sulla cooperazione volontaria delle aziende tecnologiche. Inoltre, in quanto Ordine Esecutivo, non è fonte di nuove regole ma si limita ad avviare il processo per la loro adozione.

A ciò si aggiunge che l'EO non ha il rango di una legge del Congresso ed è revocabile dal prossimo presidente degli Stati Uniti.

L'Unione Europea ha recentemente raggiunto un faticoso accordo sull'IA ACT [32] che ha regole più stringenti ma rinvia la loro applicazione fra due anni. Un tempo infinito per una tecnologia come l'IA, che fa perdere di rilevanza e probabilmente efficacia al lavoro dell'UE.

Nel corso dei lavori delle diverse commissioni, nazionali e internazionali, che stanno lavorando alla realizzazione di codici etici o a regolamenti sull'intelligenza artificiale, vengono spesso fatti paralleli con i percorsi regolamentari che hanno coinvolto altre tecnologie come per esempio l'automobile. Io penso che da questo punto di vista sia molto utile il raffronto con quanto sviluppato cento anni fa nel

---

[30] Y. ABRAHAM, *'Lavander': The AI machine directing Israel's bombing spree in Gaza*, in *+972 Magazine*, 3 aprile 2024, https://www.972mag.com/lavender-ai-israeli-army-gaza/.

[31] *Ibidem*.

[32] https://www.europarl.europa.eu/doceo/document/A-9-2023-0188-AM-808-808_IT.pdf.

passaggio dall'aeronautica dei pionieri del volo, all'industria di massa dell'aviazione civile che oggi fa muovere in sicurezza miliardi di esseri umani.

Quando l'aeronautica è passata dalla fase iniziale dei pionieri ai primi utilizzi civili di massa (posta e trasporto persone), si è posto un problema di fiducia e di responsabilità. Cioè come fare affinché le persone si fidassero del nuovo mezzo tecnologico e quindi come stabilire meccanismi certi di responsabilità. Analogamente oggi si pone un tema di fiducia e responsabilità per l'uso di massa della tecnologia dell'IA. In aeronautica per prima cosa si sono delimitati spazi a terra (aeroporti) e in cielo (aerovie), in modo da poter usare questa nuova tecnologia in sicurezza. Questo degli ambiti o spazi di utilizzo credo sia un tema importante anche per la regolamentazione dell'IA. L'IA ACT dell'Unione Europea va in parte in questa direzione, quando ad esempio limita gli usi dell'IA nel settore del riconoscimento biometrico delle persone o pensa di regolamentare l'uso dei dati digitali nella sanità. È indubbio però che bisognerà lavorare ancora molto a livello internazionale e con più solerzia per regolamentare degli ambiti consentiti e delle limitazioni per l'utilizzo dell'IA. Ci sarà per questo bisogno di creare appositi enti regolatori internazionali, così come è stato progressivamente fatto per l'aeronautica civile, dove si possano condividere e standardizzare le regole di funzionamento dell'IA. La strada finora intrapresa presenta invece una pericolosa parcellizzazione a livello internazionale che ricalca il diverso punto di incontro di interesse tra le società private che gestiscono le IA (le BigTech) e gli stati nazionali o le entità sovranazionali di riferimento. Abbiamo infatti registrato una posizione sostanzialmente liberista e a favore di una sorta di autoregolamentazione delle imprese da parte degli Stati Uniti, che grazie a questa postura hanno guadagnato per le loro imprese una posizione dominante a livello mondiale nell'economia digitale che vogliono replicare nell'IA. Abbiamo invece una posizione regolatoria molto stringente da parte della UE, però vista da alcuni come un rischio per la crescita di queste tecnologie a livello europeo. E infine una posizione fortemente statalista e accentratrice da parte del regime comunista cinese. Queste diversità e separatezze andrebbero superate a favore di una regolamentazione mondiale condivisa e soprattutto di una standardizzazione tecnica e industriale dell'IA. Perché se questa sarà pervasiva della stragrande maggioranza delle attività umane, ci sarà bisogno di standard tecnici i più universali possibili come ci sono oggi per tecnologie come il GPS o il 5G, pena la mancanza di efficacia da un punto di vista tecnologico, e di efficienza economica e sociale. Così come sarebbe necessario che fossero create agenzie indipendenti per i controlli sulla gestione dell'IA, esattamente come si fa per la navigazione aerea (ICAO; etc.). Agenzie autonome che possano verificare la "navigazione digitale" della IA. Infatti come gli aeromobili per volare hanno bisogno di autorizzazioni che verifichino i parametri di sicurezza ma anche il loro percorso, così l'IA dovrebbe consentire ad agenti terzi di verificare i prerequisiti di sicurezza e la "direzione" di marcia.

Ci sarebbe bisogno a questo scopo anche di vere e proprie "scatole nere" che come negli aeroplani consentissero, laddove necessario, alle agenzie di controllo di verificare tutti i parametri di funzionamento dell'IA.

Infine bisognerebbe incominciare a prendere in considerazione la necessità di formare gli utenti, dando loro un vero e proprio "patentino" per utilizzare l'IA. Se oggi infatti riteniamo sia necessario un titolo rilasciato in base all'accertamento di alcuni parametri tecnico funzionali, per guidare un'automobile o un aereo, o una barca, perché non si dovrebbe immaginare un "patentino" per usare l'IA?

Esistono già numerosi indizi che ci dovrebbero portare a valutare questa ipotesi. Abbiamo infatti le prime evidenze scientifiche, secondo alcuni studi, di quanto l'utilizzo dei social, stia influenzando per esempio i comportamenti sociali dei giovani e in alcuni casi provocando loro anche danni psicologici. Perché dunque non considerare tra i rimedi ai rischi dell'IA anche l'attivazione di veri e propri percorsi formativi e attitudinali che consentano l'uso consapevole e quindi più sicuro di tali tecnologie per tutti?

Ma non basta però accontentarsi delle sole attività di contenimento e regolamentazione dell'IA, bisogna anche con decisione affrontare il tema della asimmetria tra i proprietari della tecnologia e noi utenti. Si tratta di contrastare il principio di disuguaglianza che è alla base: per noi utenti si tratta del nostro essere, la nostra "on life" come la definisce il Prof. Floridi [33], mentre per i proprietari della tecnologia si tratta del loro avere, dei loro profitti. Una differenza ontologicamente dirimente che impone una scelta soggettiva all'agire. Attualmente il vantaggio accumulato dalle Big Tech in termini di capitalizzazione, di asset tecnologici e soprattutto di dati digitali, è tale che è facilmente prevedibile che un simile strapotere determini con facilità dei nuovi monopoli anche nel settore dell'IA.

Per questo è importante immaginare e costruire una pluralità di IA che favoriscano una diversità di specie, che è un fondamentale principio di salvaguardia dettato dall'importanza dei beni in oggetto. La delicatezza dei beni e servizi nel perimetro dell'IA, come ad esempio la sanità, la mobilità, ma la stessa informazione e in definitiva il rischio di una collusione tra le società proprietarie delle IA con i governi per forme di controllo, spinge ad affiancare alla richiesta di regolamentazione e controlli anche una richiesta di partecipazione attiva della società nella realizzazione di forme diversificate e alternative di IA che rispondano prioritariamente ai bisogni dei cittadini/utenti e producano beni comuni digitali.

La pratica partecipativa del consenso informato (che si usa ad esempio nella bioetica in medicina), fornisce ad esempio uno strumento utile – ha scritto il Prof. Sebastiano Maffettone nella conclusione della ricerca "Cooperative Commons" – per conciliare fini sociali rilevanti con la legittimazione sociale, che in una liberaldemocrazia dipende dal consenso individuale. In questo modo le virtù deliberative della cittadinanza democratica si fondono con l'ideale-tipo della "sovranità del consumatore" che caratterizza il mercato concorrenziale. D'altra parte un ideale di giustizia distributiva è quello che prevede un equilibrio tra le pretese di equità e quelle di efficienza, nella prospettiva generale della tutela degli interessi del con-

[33] https://www.repubblica.it/dossier/tecnologia/onlife/2019/09/29/news/repubblica_onlife_luciano_floridi-237286128/.

traente più debole[34]. E nel contesto dell'intelligenza artificiale, «la *governance* cooperativa potrebbe essere uno strumento particolarmente utile non solo per affrontare la concentrazione e gli abusi di potere, ma anche per governare l'intelligenza artificiale in un modo che distribuisca la ricchezza in modo più equo e più coerente gli obiettivi e i valori dei suoi utenti»[35].

Bisogna dunque attraverso la partecipazione diretta dei cittadini favorire la nascita di una pluralità di IA che prevedano appunto un equilibrio tra equità ed efficienza.

3. Condividere i dati per costruire beni comuni digitali.

3.1. Un "New Deal" dei dati.

Per fare tutto ciò si deve partire da un bene essenziale per lo sviluppo dell'IA, un bene che è a disposizione delle persone che ne sono i produttori, anche se non ne dispongono autonomamente: i dati digitali. I dati digitali sono la indispensabile materia prima per far funzionare le IA, che però non hanno immediatamente valore, lo acquisiscono solo se interpretati; ciò non toglie che se non ci fossero i dati non ci sarebbero le interpretazioni, e gli enormi vantaggi economici che ne derivano.[36] Perché come ha ricordato recentemente Roberto Viola DG Connect dell'UE, più addestri (con i dati) un algoritmo e più questo avrà valore. Se quindi si permette ad altri algoritmi di addestrarsi sui nostri dati, avviene quello che gli esperti definiscono un trasferimento di valore[37] Possiamo paragonare le intelligenze artificiali che domani ci guideranno in una innumerevole quantità di ambiti della vita sociale ed economica, a dei bambini che per crescere e fornirci un servizio sempre più accurato hanno bisogno di alimentarsi: appunto di dati digitali.

Secondo il Professore e saggista israeliano Youval Harari[38] si sta creando addirittura una nuova visione del mondo, quasi una nuova religione: il datismo. Si tratta di un approccio strettamente formale all'umanità, che stima il valore delle esperienze umane in relazione al loro ruolo nei meccanismi di elaborazione. Secondo Harari quando si svilupperanno algoritmi che svolgeranno il medesimo compito in modo migliore – e più economico – le esperienze umane perderanno il loro valore. Il punto però non è solo come fare ad evitare di essere defraudati, o essere pagati per i nostri dati, come propone tra gli altri, Jaron Lanier[39]: ma soprattutto come fare ad usa-

---

[34] V. RINALDI, *Dalle Coop alle Co-App*, cit., 2019, p. 71.

[35] T.N. NARECHANIA-G. SITARAMAN, *op. cit.*, p. 50.

[36] M. FERRARIS, *op. cit.*, p. 79.

[37] *Corriere della Sera*, 12 febbraio 2024.

[38] Y.N. HARARI, Homo Deus. *Breve storia del futuro*, Firenze, 2017.

[39] J. LANIER, *La dignità ai tempi di internet*, Milano, 2014.

re i dati digitali per il bene comune e di conseguenza anche per il nostro benessere.

Per questo bisogna però partire dalla considerazione che i dati personali acquistano maggior valore quando vengono condivisi in forma aperta, trasparente e possibilmente democratica. Il punto chiave di partenza rimane comunque il valore condiviso dei dati perché solo tramite la condivisione il sistema può funzionare meglio e tendere al bene comune: i dati da soli non vanno da nessuna parte. Senza la loro condivisione non possono assurgere al grado di valore sociale e ancor di più di capitale sociale. «Perché è la natura stessa dei dati e della loro interpretazione a far sì che gli umani possano trarre vantaggio solo da dati aggregati, cioè da un atteggiamento cooperativo, mentre i dati individuali hanno di per sé poco valore» [40].

A monte del valore economico o sociale dei dati esiste un problema sul tema del "diritto di proprietà" che attiene a tale bene.

Secondo il Prof. Antonio Nicita si tratta di una sorta di «pervasiva ambiguità» [41] che da un punto di vista giuridico deriva in parte dalla natura digitale del bene, che essendo un "bene intangibile" in quanto tale può essere duplicato all'infinito e a costo zero nella sua forma originale, pur mantenendo per ogni detentore di una copia, lo stesso valore informazionale (assenza di rivalità nel consumo), e anche dal fatto che il suo valore si genera in relazione ad altri dati e attraverso attività di elaborazione matematica degli stessi.

Il dato digitale singolo, in quanto tale ha infatti un valore, come in generale nei beni relazionali o di rete proporzionale al numero dei partecipanti: se infatti in una rete telefonica abbiamo due soli utenti (la linea rossa della guerra fredda o un citofono interno a una casa) il valore della rete è sicuramente molto alto per coloro che la usano ma quasi nullo da un punto di vista del mercato.

Il Prof. Nicita si domanda, in relazione a ciò, se «quando rilasciamo un "consenso" all'uso del dato, stiamo assistendo o meno a un passaggio di proprietà su quello specifico uso. Per molti studiosi – dice Nicita- non è affatto così: i dati personali ceduti sarebbero una mera "delega" (di qui l'origine della tutela della privacy digitale come garanzia della inalienabilità e non negoziabilità del dato personale … creando involontariamente una garanzia di monopolio sull'uso economico del dato) … Riconoscere a chi generi un dato – prosegue – la proprietà dello stesso significherebbe rendere esplicita, su un vero e proprio mercato dei dati, la transazione … ma oggi questo tipo di transazioni esplicite tra l'originario produttore del dato e chi lo acquisisce per fini industriali, non avviene sul mercato» [42].

Proseguendo nel suo ragionamento il Prof. Nicita sostiene che «un altro modo per risolvere il problema è superare il (vecchio) principio della "delega" di un dato che resta non negoziabile, a favore della definizione di un diritto proprietario (cioè di controllo) sul dato, o meglio, su alcuni usi dello stesso ... già il diritto alla porta-

---

[40] M. FERRARIS, *op. cit.*, p 141.

[41] A. NICITA-M. DELMASTRO, *Big Data: come stanno cambiando il nostro mondo*, Bologna, 2019.

[42] *Ibidem.*

bilità (*del GDPR ndr*) risponde esattamente a questa logica: il dato "proprietario" viene "affittato" per un certo periodo di tempo a una certa piattaforma, ma può poi essere richiesto indietro dal titolare originario» [43].

In realtà lo stesso Nicita in altre parti del libro parla di copia dei dati, quindi duplicazione dell'asset, esattamente come su questa linea si è pronunciato a Bruxelles il CESE con il parere ([COM(2018) 233final] quando dice che: «I cittadini dovrebbero avere il diritto di accesso ai propri dati sanitari e devono essere loro a decidere se e quando condividerli. È essenziale tenere conto del regolamento generale sulla protezione dei dati, che garantisce ai cittadini il controllo sull'utilizzo dei propri dati personali, specialmente i dati sanitari. Il CESE suggerisce che un "diritto alla copia (gratuita)" potrebbe essere una forma attiva di tutela. Ciò riguarda tutti i dati generati dagli utilizzatori nell'interazione con le piattaforme digitali e permette ai cittadini di riutilizzare i propri dati. I dati originali sono l'unico valore utile per gli algoritmi e le piattaforme; essi devono essere considerati come un prodotto originale generato dall'utilizzatore che va tutelato ai sensi delle normative sulla proprietà intellettuale. Il "diritto alla copia (gratuita)" è un aiuto anche ai fini della tutela e della promozione della concorrenza, che oggi viene messa a dura prova dai sistemi impiegati dalle piattaforme digitali per espropriare dati e tracce personali» [44].

Dunque nel mondo digitale si opera a costi di transazione pari a zero e quindi una copia dei propri dati digitali non solo non costa ma non toglie nemmeno valore alla società che detiene per legge – l'originale dei dati. Quindi la condivisione dei dati è un gioco a sommatoria positiva: non toglie valore a chi detiene i dati e in più trasferisce analogo valore all'utente che ha generato i dati e ad altri che li volessero utilizzare insieme ai loro.

Su questo tema ha dato un importante contributo Alex Pentland, professore del Mit (Massachusetts Institute of Technology) di Boston, che ha lanciato a Davos nel 2007 un vero e proprio "*New Deal* dei Dati", basato sul fatto che "i dati vanno riconosciuti come beni dell'individuo". Per lui la soluzione migliore per rendere la condivisione di dati alla base del miglioramento del sistema pubblico è quella di creare "reti fiduciarie" [45]: la combinazione di un sistema informatico che registra il permesso dell'utente per tutti i dati raccolti e un contratto che specifica quello che si può fare con quei dati. Questo meccanismo è stato tra l'altro alla base dello sviluppo principale di una delle funzioni di successo del capitalismo di questi decenni: la finanziarizzazione globalizzata. Il sistema di trasferimento di denaro tra banche in tutto il mondo (Swift) funziona proprio in questa maniera ed è assolutamente affidabile e riservato.

La grande sfida del futuro è però di far sì invece che la condivisione dei dati degli utenti – in modo trasparente e certificato – possa contribuire al benessere della

---

[43] *Ibidem*.

[44] *Ibidem*.

[45] A. PENTLAND, *Fisica Sociale*, Milano, 2015.

collettività creando dei veri e propri "beni comuni digitali". Come ha scritto il Prof. Benkler: dobbiamo passare dai diritti di proprietà alla necessità di comprendere l'interazione necessaria tra proprietà e beni comuni. Dobbiamo comprendere finalmente che la tecnologia si può sviluppare anche attraverso il cooperativismo e così si può modellare anche la direzione del cambiamento tecnologico per consentire relazioni più stabili e più uguali. Proviamo a insegnare alle tecnologie la generosità e l'altruismo: perché non siamo nati egoisti [46].

3.2. Il contesto giuridico europeo sull'utilizzo e la condivisione dei dati.

Che i dati digitali fossero importanti i cittadini europei l'hanno incominciato a mettere a fuoco nel 2018 quando è entrato in vigore il nuovo regolamento sulla *privacy*. Il GDPR, *General Data Protection Regulation*, dava loro per la prima volta un nuovo diritto soggettivo: avere indietro una copia di tutti i dati digitali (in un formato digitale utilizzabile) da chiunque posseduti e con qualunque piattaforma generati, e soprattutto la possibilità di trasferirli a chiunque (portabilità dei dati) [47].

È stata dichiarata, come hanno detto alcuni, una guerra "a nostra insaputa" sulle nostre identità digitali che ha come fine non solo la creazione di centri di potere economico, ma anche l'indirizzamento dei comportamenti di massa in un circuito negativo che corre il serio rischio di minare le basi stesse della democrazia, come da noi fin qui conosciuta. L'Europa invece, con lungimiranza e decisione si è accorta di questa guerra "a nostra insaputa" e ha deciso di mettere un'arma nelle mani dei cittadini europei, creando con il GDPR un vero e proprio "porto dati" [48].

Quest'*arma* è appunto il regolamento europeo che è stato recepito nella legislazione nazionale da tutti i paesi della Unione. Il GDPR, all'art. 20, ha infatti creato un diritto soggettivo che riconosce a tutti i cittadini europei la "proprietà" di un "*digital twin*" dei loro dati, ovunque e con chiunque generati, attraverso il diritto a

---

[46] V. RINALDI, *op. cit.*

[47] Art. 20 (*Diritto alla portabilità dei dati*) del Reg. UE n. 679/2016: «1. L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:

a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera *a*), o dell'articolo 9, paragrafo 2, lettera *a*), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera *b*); e

b) il trattamento sia effettuato con mezzi automatizzati.

2. Nell'esercitare i propri diritti relativamente alla portabilità dei dati a norma del paragrafo 1, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.

3. L'esercizio del diritto di cui al paragrafo 1 del presente articolo lascia impregiudicato l'articolo 17. Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

4. Il diritto di cui al paragrafo 1 non deve ledere i diritti e le libertà altrui».

[48] Similitudine giornalistica con il "porto d'armi". *NdA*.

riceverne dal gestore una copia al fine di poterne disporre autonomamente. E, cosa ancora più significativa, eventualmente conferirla a terzi per un proprio vantaggio materiale o immateriale: compreso anche ad un *competitor* del gestore originario. Lo scopo dichiarato delle istituzioni europee è di favorire la competizione sul mercato dei dati digitali, in modo da sviluppare delle vere alternative allo strapotere dei *social network*. E quindi oggi oltre 448 milioni di europei possono disporre finalmente dei loro dati digitali e farne ciò che vogliono.

Questo nuovo diritto di disporre dei propri dati digitali in maniera autonoma rispetto al gestore degli stessi ha creato una profonda discontinuità con il meccanismo precedentemente in essere – *privacy* – perché ha determinato un positivo conflitto di interessi tra l'azienda – all'interno del cui perimetro fisico o digitale si è generato il dato digitale e che per questo li gestisce – e l'utente che li ha generati, mentre prima con la pratica impossibilità di disporre dei propri dati in maniera che fossero riutilizzabili nel mercato digitale sottraeva del valore all'utente. Basti pensare ai sensori corporei, sociali e ambientali che ci offriranno – come dice il professor Pentland del MIT – la possibilità di passare «dalla comprensione della realtà alla costruzione di nuove realtà» [49]. Un punto chiave, secondo Pentland, visto che i tuoi dati hanno più valore se puoi condividerli perché questa condizione consente a sistemi come la sanità pubblica di lavorare meglio per te. Conclude poi il suo ragionamento con la constatazione che dando alle persone il potere di controllare i dati che li riguardano, potremo avere una sorta di ambiente "democratizzato" di condivisione dei dati che ci consentirà di creare un mondo più sano, più verde e più pacifico [50]. La condivisione dei dati in forma diretta da parte dei cittadini aiuterebbe anche ad affrontare un altro tema che sta venendo sempre più a galla con la "datificazione" del mondo, e cioè la crescente mancanza di fiducia da parte delle persone di fronte al problema dei fake e all'uso dei loro dati a fini di profitto da parte delle BigTech. Questo problema ha anche un importante risvolto che riguarda la qualità dei dati che alimentano le IA e che si gioverebbe grandemente se i dati fossero conferiti volontariamente dai cittadini per la creazione di beni digitali sociali.

Dobbiamo quindi considerare i dati come un nuovo tipo di capitale: il capitale digitale [51].

Un ulteriore passaggio di questa strategia europea si è concretizzato nei primi mesi del 2024 quando è entrato in funzione anche in Italia il regolamento europeo sulla *governance* dei dati (DGA) [52]. Si tratta di un fondamentale tassello che finalmente consegna ai cittadini europei le regole con cui utilizzare i dati digitali per la creazione di un vero e proprio mercato europeo dei dati che «potrebbe essere cen-

---

[49] A. PENTLAND, *op. cit.*

[50] A. PENTLAND, *op. cit.*

[51] A. POSNER-E.G. WEYL, *Radical Markets*, Princeton (NJ), 2018, p. 224: «*In this view, data are much more like capital than labor*».

[52] Reg. UE n. 868/20222 (DGA).

trale per il rapido sviluppo della tecnologie di intelligenza artificiale» [53]. Lo scopo dichiarato è infatti quello «di migliorare le condizioni per la condivisione dei dati, creando un quadro armonizzato per gli scambi di dati e stabilendo alcuni requisiti di base per la *governance*» [54] degli stessi e «sviluppare (…) una società e un'economia dei dati antropocentriche, affidabili e sicure» [55]. Per arrivare a questo obiettivo il DGA prende in considerazione gli scambi di dati nel settore pubblico in quello privato e soprattutto nel settore *non profit*, definendo anche la possibilità di «sostenere obiettivi di interesse generale mettendo a disposizione quantità considerevoli di dati sulla base dell'altruismo dei dati» [56]. Questa ultima azione viene ulteriormente specificato è necessaria, in particolare, per aumentare la fiducia nella condivisione dei dati. Viene altresì specificato che l'utilizzo per obiettivi di interesse generale di dati messi a disposizione su base volontaria dagli interessati presenta grandi potenzialità per esempio nell'assistenza sanitaria, nella lotta ai cambiamenti climatici, per il miglioramento della mobilità, per il miglioramento della fornitura dei servizi pubblici, o in generale delle politiche pubbliche e il sostegno della ricerca scientifica. Si prevedono dunque specifiche figure di aggregatori di dati che detengano questi dati per valorizzarli attraverso specifici servizi di intermediazione degli stessi, e tra queste categorie di intermediari vengo identificati i soggetti che opereranno in base all'altruismo dei dati, e le cooperative di dati.

Nel DGA viene inoltre specificato che per «altruismo dei dati» si intende la condivisione volontaria di dati sulla base del consenso accordato dagli interessati al trattamento dei dati personali che li riguardano, o sulle autorizzazioni di altri titolari dei dati volte a consentire l'uso dei loro dati non personali, senza la richiesta o la ricezione di un compenso che vada oltre la compensazione dei costi sostenuti per mettere a disposizione i propri dati, per obiettivi di interesse generale.

Le cooperative di dati, viene inoltre chiarito, mirano a raggiungere una serie di obiettivi, in particolare a rafforzare la posizione dei singoli, affinché compiano scelte informate prima di acconsentire all'utilizzo dei dati, influenzando anche i termini e le condizioni, cui è subordinato l'utilizzo dei dati, in modo da offrire scelte migliori ai singoli membri del gruppo.

Si è aperto dunque, almeno in Europa, uno spazio concreto attraverso questi aggregatori di dati per far contare le scelte dei singoli sull'utilizzo dei loro dati digitali. Non solo per negoziare al meglio con i soggetti interessati ad utilizzarli, ma anche per poterne disporre a fini altruistici e quindi in direzione della creazione di beni comuni digitali destinati al benessere generale delle persone e non al profitto di pochi.

---

[53] *Considerando* n. 2, DGA.

[54] *Considerando* n. 3, DGA.

[55] *Ibidem.*

[56] *Ibidem.*

3.3. Il ruolo delle cooperative di dati e il mutualismo digitale.

Un ruolo importante in questo contesto potrebbe essere svolto in Italia dalle cooperative di dati e dal movimento cooperativo, a cui aderiscono oltre 12 milioni di persone [57] e che rappresenta una parte importante dell'economia nazionale.

Le cooperative di dati sono un soggetto naturalmente predisposto e particolarmente adatto per la creazione di data set con scopi sociali e qualsiasi cooperativa esistente, può a determinate condizioni, diventare, o dare vita, a una cooperativa di servizi di dati come previsto esplicitamente dal DGA. In primis perché sono un luogo di condivisione naturale e favorevole di dati tra i soci e le cooperative stesse, in quanto il socio produttore dei dati è anche e contemporaneamente il proprietario della cooperativa che li utilizza. Si determina dunque nella cooperativa una coincidenza di interessi tra socio e cooperativa stessa, che mette la cooperativa nella condizione più favorevole per l'uso dei dati per quei fini di riequilibrio sociale, difesa dei più deboli e scopi solidaristici che sono alla base del cooperativismo da più di 200 anni.

Secondo perché i principi di funzionamento e governance delle cooperative sono basati sul fondamento democratico di "una testa un voto", sulla mutualità e la solidarietà verso i soggetti più deboli, e la mancanza di profitto individuale, tutti elementi utili e necessari per il corretto funzionamento degli aggregatori dei dati come previsto dall'Unione Europea.

Il caso di specie delle "cooperative di dati" è un esempio particolarmente interessante perché facilita lo "*sharing*" fiduciario dei dati digitali in quanto presenta un'inversione rispetto al normale conflitto di interessi tra una società che detiene i dati digitali e un cliente che conferisce i suoi dati nell'utilizzo di un applicativo digitale, poiché questi sono due soggetti chiaramente distinti e legati esclusivamente da un vincolo contrattuale o da un semplice consenso (talvolta ottenuto obbligatoriamente a fronte del servizio erogato) i cui interessi rispetto al possesso dei dati possono divergere. Mentre nel caso di una cooperativa esiste una "convergenza di interessi" se non una vera e propria "sovrapposizione" in quanto i dati che si generano nell'interazione tra il socio e la cooperativa. Ad esempio nel sito di e-commerce si determina una sorta di "proprietà condivisa" dei dati generati nell'interazione tra il socio e la piattaforma digitale, in quanto il socio è anche proprietario della cooperativa e quindi, in quanto tale può determinare la governance dei suoi dati, a questa conferiti a fini mutualistici.

Il movimento cooperativo, ha però bisogno per svolgere questo ruolo di creatore di cooperative di dati, di innovare i principi fondanti della cooperazione estendendoli oltreché alle persone fisiche anche alla loro identità digitale: cioè ai dati da loro prodotti. Se, infatti, il principio di funzionamento base della cooperazione è quello di condividere un obiettivo da raggiungere in comune, è evidente che quando i dati digitali del socio divengono, grazie alla tecnologia, un valore – *asset* – utile per rag-

[57] Cfr. ALLEANZA DELLE COOPERATIVE ITALIANE, *L'associazione*, https://www.alleanzacooperative.it/l-associazione.

giungere questo stesso scopo questi dovrebbero rientrare nel perimetro cooperativo, attraverso un conferimento da parte dei soci alla cooperativa stessa. È un po' come se nei terreni di una cooperativa agricola si scoprisse un giacimento di petrolio o si ibridasse una nuova varietà di pianta da frutta. O come se una cooperativa industriale realizzasse un nuovo brevetto grazie all'opera di ingegno dei suoi soci. In tutti e due i casi, il nuovo valore – *asset* – andrebbe condiviso all'interno della proprietà cooperativa per lo sviluppo della stessa e la redistribuzione del valore generato tra i soci. In questo senso va dunque affermato e stabilito un vero e proprio nuovo principio cooperativo: quello della condivisione dei dati digitali «da parte dei soci nelle cooperative e delle cooperative tra di loro» [58].

Un nuovo principio che si può configurare come un aggiornamento/ estensione dell'identità cooperativa e dei principi e delle linee guida elaborate dall'ICA, International Co-Operative Alliance.

L'ICA infatti nell'emanare le nuove linee guida sui principi cooperativi vigenti dal Congresso di Manchester del 1995 si è posta il problema della nuova economia dei dati in termini di nuovi bisogni che sorgono in connessione alla gestione dei dati del singolo e si è domandata «come le cooperative possono accedere e recuperare il controllo su questi dati per usarli per lo sviluppo delle imprese cooperative» [59].

Il capitale digitale rappresentato dai dati per essere prodotto legalmente ha però bisogno che la cooperativa si attrezzi anche normativamente per il nuovo scopo e che il socio conferisca alla cooperativa il diritto di utilizzare i suoi dati digitali, sia quelli generati all'interno del rapporto mutualistico tra socio e cooperativa, sia quelli generati con terze parti. C'è dunque bisogno di una azione politica da parte delle associazioni cooperativistiche tesa all'aggiornamento e adeguamento dell'impianto stesso del rapporto mutualistico e della governance che in parte ne deriva.

Si pone dunque una questione relativa alla "mutualità digitale" o meglio al "nuovo valore mutualistico" generato grazie alle nuove tecnologie digitali e ai Big Data e alla sua iscrizione, anche statutaria, all'interno del perimetro delle regole e dei principi cooperativi.

La mutualità digitale si basa sul presupposto che ogni attività mutualistica che si svolge nella dimensione reale può avere un suo corrispondente nella rete. Quindi è necessario il riconoscimento giuridico che tutte le attività che vengono svolte in rete tra un socio e la cooperativa determinano ugualmente a quelle svolte nel mondo fisico, un'interazione mutualistica.

---

[58] Un simile principio di "condivisione dei dati" viene proposto ad esempio da Mayer-Schöberger e Ramge, nel libro *Reinventare il Capitalismo nell'era dei Big Data*: «i regolatori che vogliano garantire mercati competitivi dovrebbero imporre la condivisone dei dati (…) agli operatori di grandi dimensioni venga imposto di condividere tali dati(…) con i loro *competitor* (…) un mandato universale di condivisione sarebbe vantaggioso per entrambi» (V. MAYER SCHÖNBERGER-T. RAMGE, *Reinventare il capitalismo nell'era dei Big Data*, Milano, 2018, pp. 156-157).

[59] ICA (INTERNATIONAL COOPERATIVE ALLIANCE), *The Guidance Notes on the Cooperative Principles*, https://ica.coop/en/media/library/research-and-reviews/guidance-notes-cooperative-principles.

Può sembrare scontato e pleonastico ma non lo é: ancora oggi legalmente ai fini del calcolo della mutualità prevalente nell'ordinamento giuridico italiano, le attività svolte on line tra il socio e la cooperativa non si sa se contribuiscono o meno al conteggio mutualistico.

Essendo il socio il proprietario della cooperativa, questo è il modo corretto per saldare – ricongiungere – la proprietà del capitale digitale prodotto in cooperativa dal socio e la cooperativa stessa. Questa dicotomia avviene per un socio lavoratore in una cooperativa di tassisti piuttosto che per i soci di una cooperativa di utenti elettrici: i dati da loro prodotti e che riguardano la mobilità piuttosto che l'efficienza energetica sono sia della cooperativa che del socio.

Attraverso la "mutualità digitale" si avrebbe invece una ricongiunzione dei due diritti, quello in capo al socio e quello in capo alla cooperativa: un po' come nel caso della nuda proprietà e dell'usufrutto. Il principio della condivisione cooperativa dei dati è quindi una premessa necessaria per l'utilizzo trasparente e democratico dei dati, garantito dai valori e dai principi cooperativi: e soprattutto riguarderebbe una massa di oltre 12 milioni di cittadini in Italia [60] e un miliardo di soci cooperatori esistenti oggi nel mondo.

Per essere attuato il principio della condivisione cooperativa dei dati ha bisogno di includere negli statuti delle cooperative, tra gli scopi sociali e mutualistici, quello della condivisione dei dati tra socio e cooperativa. Si darebbe così la facoltà alla cooperativa di utilizzare e valorizzare i dati del socio al suo interno e anche di cederli, su delega espressa del socio, a terzi. Così facendo si metterebbe in grado la cooperativa di utilizzare a pieno il "capitale digitale" generato dai dati dei soci permettendo la creazione di un ecosistema digitale cooperativo. Non più solamente la possibilità di scambi tra cooperative, come è avvenuto finora attraverso la finanza o le merci e i servizi ma anche attraverso lo scambio e l'utilizzo condiviso dei dati digitali. Pensiamo che enorme valore, anche sociale oltre che economico, si potrebbe generare mettendo insieme i miliardi di dati che ogni minuto vengono acquisiti dalle cooperative: un immenso "giacimento di dati" che potrebbe consentire non solo una maggior efficienza delle imprese cooperative federate nell'ecosistema ma anche il raggiungimento di obiettivi di bene comune. Si tratterebbe di dare le gambe ad un modo completamente diverso di intendere la mutualità di sistema. Attraverso lo scambio dei dati, in forma anonima, riuscire ad avere delle raffigurazioni efficienti ed efficaci dei perimetri di sviluppo di nuovi servizi e nuovi business. Si potrebbero creare ad esempio sinergie tra cooperative per rendere possibile una reale economia circolare basata prima di tutto sullo scambio delle informazioni, sui materiali da riutilizzare, uno sviluppo di una mobilità integrata delle merci tra Grande Distribuzione Organizzata (GDO) e filiera cooperativa della logistica in modo da ridurre le emissioni di CO^2 oltreché rendere più competitivi i servizi cooperativi. Si potrebbe anche migliorare l'efficienza nei sistemi e nei servizi cooperativi di welfare, favorire sistemi intelligenti per la produzione e distribuzione di ener-

[60] *Ibidem*.

gie rinnovabili decentrate, favorire la mobilità sostenibile e trasformare i servizi per gli abitanti delle città a misura di un umanesimo digitale. Infine potremmo anche alimentare i sistemi di intelligenza artificiale con le giuste informazioni: cioè quelle da noi stessi fornite volontariamente in modo da consentire lo sviluppo di sistemi intelligenti il cui scopo sia il nostro benessere e non il profitto dell'imprenditore che li possiede.

Ridisegnare mutualismo e socialità utilizzando le competenze proprie della digital transformation, ha scritto il professor Paolo Venturi dell'Università di Bologna, è un passo ineludibile, ma altrettanto essenziale, è il consolidamento delle motivazioni e dei fini di coloro che lavorano in ambito sociale. Il governo dell'intelligenza artificiale, la creazione di piattaforme capaci di alimentare relazioni reali – non strumentali – e la nascita di nuove istituzioni digitali cooperative e inclusive, continua Venturi, diventano obiettivi a cui il Terzo settore – e la cooperazione – deve tendere affinché la comunità non venga sostituita con la comunanza e la felicità dall'utilità – di pochi [61].

4. Le cooperative di dati e l'Intelligenza Artificiale Sociale.

4.1. L'Intelligenza Artificiale Sociale.

L'IA sociale dovrebbe essere una tecnologia che risponde prioritariamente ai bisogni dei cittadini/utenti, la cui proprietà sia democratica, valorizzando il fattore umano. Una sorta di bene pubblico digitale. l'IA sociale dovrebbe caratterizzarsi da un punto di vista identitario come un soggetto collettivo a partecipazione volontaria, con governance democratica, caratterizzato dalla limitazione del profitto o non profit, mutualistico e solidaristico, e teso alla creazione di beni sociali digitali. L'IA sociale dovrebbe dunque utilizzare tutti i dati, liberamente conferiti dai cittadini, dalle associazioni del terzo settore, dalle cooperative e dalle istituzioni pubbliche, per produrre servizi e beni tesi al miglioramento del benessere dei cittadini.

Le cooperative di dati aggregando i dati (il capitale digitale) dei loro soci forniranno la base (democratica, mutualistica e non profit) per alimentare le IA sociali, destinate ad occuparsi non di produrre beni e servizi finalizzati al profitto individuale degli investitori e dei manager, ma a servire i bisogni delle persone e ad accrescere il benessere comune. In più i dati delle cooperative di dati, incorporando i valori cooperativi [62], forniranno una base qualitativa migliore per i "modelli fondativi" delle IAS, per quanto riguarda la mitigazione dei "*bias*" rispetto alle questioni

---

[61] P. VENTURI, *Nell'industria 4.0 la sfida è etica*, in *Corriere della Sera*, 12 settembre 2018, https://www.corriere.it/buone-notizie/18_settembre_12/paolo-venturi-nell-industria-40-sfida-etica-bcd93c7a-b68a-11e8-83fc-d7dcaceaa02b.shtml.

[62] Vedi FONDAZIONE IVANO BAERBERINI, *I valori e la cultura cooperativa*, https://fondazionebarberini.it/old/la-fondazione_valori-cooperativi.html.

di genere o relativamente ai collegamenti semantici rispetto alle disabilità.

Se prendiamo, ad esempio, il caso dell'Italia, milioni di cittadini ogni giorno producono miliardi di dati sui loro consumi e di conseguenza anche sulle loro abitudini. Se pensiamo ai dati sulla mobilità, si tratta di dati su milioni di chilometri percorsi ogni giorno, acquisiti ad esempio dalle scatole nere delle auto dei privati cittadini, o dai sensori a bordo delle auto stesse che dialogano con le case automobilistiche, che ogni giorno monitorando le strade e i conducenti possono consentire ad una IA sociale della mobilità di predire quali sono le strade più percorse e quando e dove si formano gli intasamenti, aiutando non solo i singoli cittadini a scegliere i percorsi migliori per i loro spostamenti ma anche le amministrazioni locali a programmare interventi per migliorare e ridurre i tempi di percorrenza, aumentare il trasporto pubblico, e sviluppare forme aggregative di trasporto collettivo efficiente e sostenibile, riducendo anche i costi ambientali del trasporto delle persone e delle cose in maniera significativa. Da i miliardi di dati sanitari acquisiti dai soggetti che operano nell'ambito della sanità, ospedali pubblici, medici di base, e dai cittadini con i loro referti clinici ma anche i loro consumi alimentari e i loro stili di vita, si potrebbero creare IA sociali tese a sviluppare servizi per il miglioramento della qualità della vita delle persone, la ricerca e l'uso di medicinali tesi al benessere delle persone e non al profitto delle Big Pharma, e soprattutto a spendere in maniera più efficace le risorse private e pubbliche in un paese a forte crescita delle classi anziane. I dati generati dai dati epidemiologici dei cittadini insieme ai loro referti diagnostici messi a disposizione dell'IA sociali della sanità permetterebbero di validare campagne di prevenzione mirate riducendone i costi e migliorandone l'efficacia. L'IA sociale potrebbe contribuire a realizzare una medicina di precisione (prevenzione delle patologie, diagnosi e cura personalizzata) non legata solo al profitto delle società che possiederanno l'IA ma a beneficio di tutti. Già oggi programmi scientifici come Brainteaser [63], integrando dati clinici, ambientali e dati generati dai pazienti attraverso app e sensori, sviluppa modelli predittivi di supporto per coloro che soffrono di sclerosi amiotrofica e sclerosi multipla e per i loro medici. Così come l'uso dell'IA sociale consentendo di migliorare la qualità delle immagini di Tac, radiografie e medicina nucleare, ridurrebbe i tempi di esposizione alle radiazioni del paziente e anche migliorerebbe le performance riducendo i tempi di attesa degli esami. delle operazioni realizzate con l'assistenza di *robot* e dell'IA fornirebbero conoscenza per poter fare la concorrenza con prodotti non profit alle società che lucrano sul loro strapotere tecnologico nella chirurgia robotica. Come pure se i cittadini italiani fornissero alle IA sociali per la transizione energetica i loro dati sui consumi energetici si potrebbero realizzare politiche di efficientamento energetico basate sull'uso programmato ed efficiente dell'energia, oggi impensabili e irrealizzabili, risparmiando miliardi euro e rendendo più sostenibile l'ambiente. Mettendo insieme i dati e le informazioni di carattere tecnico e scienti-

[63] Cfr. *Brainteaser Project (Bringing Artificial Intelligence home for a better care of amyotrophic lateral sclerosis and multiple sclerosis)*, https://brainteaser.health.

fico a disposizione del mondo universitario, insieme all'uso dei dati dei cittadini, si darebbe un enorme sviluppo a grandi aree di ricerca in moltissime discipline, mettendo le IA sociali in grado di competere con le IA del profitto, in campi come quello della ricerca sui nuovi farmaci seguendo una prassi che ha dimostrato di funzionare nel periodo del Covid, dove tutto il mondo scientifico ha condiviso tutte le informazioni con tutti con il risultato di salvare milioni di vite umane. Condividendo i dati delle agenzie pubbliche sulla meteorologia e il clima, e aggiungendo la partecipazione dei cittadini con i loro dati acquisiti dai loro sensori in tempo reale sulle condizioni climatiche e meteo locali, si potrebbero sviluppare IA sociali in grado di fornire modelli di previsioni più affidabili a livello locale sui fenomeni climatici avversi estremi e sul monitoraggio e la prevenzione del territorio. C'è insomma un immenso giacimento di dati e informazioni nel mondo dei soggetti dell'economia sociale, che sommato a quello delle istituzioni pubbliche, e con la partecipazione diretta e volontaria dei cittadini, consentirebbe ad un'IA sociale una serie infinita di correlazioni e soluzioni, creando un'enorme area di beni digitali comuni per il benessere e lo sviluppo sociale ed economico delle persone.

Inoltre bisogna considerare che un'IA che nasca nell'ambito dell'Economia Sociale sarebbe un *asset* importante nella strategia della competitività che dovrà guidare nei prossimi anni l'azione dell'Europa. È sempre più evidente, non solo nel campo dell'IA, che la competizione tra Stati Uniti, Cina ma anche Paesi Arabi sta aumentando e l'Europa sembra non aver ancora messo a fuoco gli strumenti su cui può realmente contare. Un'azione congiunta del mondo dell'Economia Sociale nel campo dell'IA sociale sarebbe sicuramente un investimento utile, intanto perché non esiste qualcosa di simile all'Economia Sociale negli Usa e tantomeno in Cina. Secondo perché si partirebbe con una potenzialità enorme non solo per la quantità di dati disponibili all'interno del perimetro dell'Economia Sociale, ma anche con una capacità tecnologica e computazionale unica che si trova all'interno del perimetro delle istituzioni universitarie pubbliche. Basti pensare ai supercomputers di Cineca in Italia. Quindi come fare perché questa sorta di nuovo "capitale digitale" rappresentato dai big data possa essere usato concretamente per alimentare l'IA sociale? Come fare a creare un valore realmente condiviso dai dati? Con chi costruire una strategia necessaria a far nascere un'IA Sociale?

4.2. Un'Alleanza per l'IA Sociale.

Non basta però per competere con le Big Tech nel settore delle tecnologie dell'IA, il solo movimento cooperativo. C'è bisogno di realizzare un concerto di intenti di più ampia scala che comprenda il vasto mondo dell'economia sociale e anche le Istituzioni pubbliche.

Bisognerà partire dai soggetti che nella società condividono i principi di autonomia, democrazia, mutualità e limitazione del profitto che devono essere alla base della IA sociale.

Soggetti di questo tipo in Europa fanno parte della cosiddetta «Economia Socia-

le»[64] nella quale si ritrovano diverse famiglie tra cui Fondazioni, cooperative, ong, associazioni del terzo settore, etc., dove ci sono i dati digitali di milioni di cittadini. A questi soggetti andrebbero affiancati tutti i soggetti del mondo della conoscenza e della ricerca, in primo luogo le Università, e gli attori istituzionali del sistema di ricerca di ricerca (Cun, Crui, Cnr, Conper, etc.), dove ci sono altri enormi giacimenti di dati e informazioni che dovrebbero essere messi a disposizione delle IA sociali. C'è bisogno di dare vita a una grande alleanza tra le organizzazioni dell'economia sociale e le Università (che possono inserire questa azione a pieno titolo nelle politiche legate all'impatto sociale della terza missione che tende a ricomprende sempre di più la produzione di beni pubblici sociali), per alimentare e far nascere IA sociali che rispondano ai bisogni dei cittadini e producono beni sociali per migliorare la qualità della vita. L'Alleanza tra questi mondi si dovrebbe cementare su un patto per un utilizzo condiviso ed etico dei dati per alimentare le IA sociali, basato su semplici presupposti, come quelli ad esempio delineati nel Manifesto di *Cooperative Commons* (2013)[65], nato non a caso da una collaborazione tra l'università LUISS e un'organizzazione dell'economia sociale, la Lega Nazionale delle Cooperative.

Al primo punto il Manifesto prevede che noi utenti: «Vogliamo usufruire dei vantaggi e degli sviluppi offerti dalla transizione digitale senza essere spossessati dei nostri dati e dei valori materiali e immateriali da essi rappresentati»[66], «Noi vogliamo che i nostri dati cooperino come già fanno i bits nella rete anche per produrre effetti nel mondo reale»[67] – e infine – «Noi vogliamo far cooperare i nostri dati e contenuti con i dati e i contenuti di tutti coloro i quali vogliano creare ulteriore valore materiale e immateriale in forma aperta, democratica e ripartirne gli effetti in forma mutualistica»[68].

Questa collaborazione tra Economia Sociale, Università e Istituzioni pubbliche dovrà essere finalizzata a far nascere uno o più "aggregatori di dati" come previsto dal DGA che possano mettere insieme l'enorme potenziale di dati e informazioni di questi soggetti per allenare IA sociali con il chiaro obiettivo di rispondere alle esigenze della società e alle principali sfide in ambito sanitario, ambientale, energetico, della mobilità, culturale. Favorire la nascita quindi con questi aggregatori di dati, di una sorta di "webfare" come lo descrive il Prof. Ferraris «che dovrebbe consentire agli utenti di capitalizzare e socializzare i propri dati… che devono venire anzitutto riconosciuti come "patrimonio dell'umanità»[69]. I principi etici condivisi

---

[64] EUR-LEX, voce *Econonia sociale*, in *Glossary of Summaries of EU legislation*, https://eur-lex.europa.eu/IT/legal-content/glossary/social-economy.html.

[65] Manifesto *Cooperative Commons*, in V. RINALDI, *op. cit.*, pp. 89-91.

[66] *Ibidem*.

[67] *Ibidem*.

[68] *Ibidem*.

[69] M. FERRARIS, *op. cit.*

negli aggregatori di dati in forma di cooperative, saranno i pilastri con cui verranno costruite le finalità operative delle IA sociali, i cui algoritmi opereranno in base a quegli stessi principi (democrazia, mutualità, solidarietà, mancanza di profitto, etc.), a garanzia per tutti i cittadini di un sistema tecnologico delle IA costruito a salvaguardia dell'interesse e del bene comune non solamente in senso normativo ma anche teleologico.

Naturalmente un'Alleanza per l'IA sociale dovrà porsi non solamente il problema del "capitale digitale" ma anche quello delle risorse economiche reali per raggiungere gli obiettivi prefissi.

La prima fonte di risorse sono le risorse pubbliche che il Governo ha deciso con il piano per il finanziamento dell'IA di mettere a disposizione. Bisognerebbe far in modo che venisse riconosciuto un canale dedicato, e magari preferenziale, per la realizzazione dell'IA sociale. Non dovrebbe essere difficile riferendosi alla normativa europea fare in modo che il Governo riconosca uno spazio all'interno delle risorse (oltre 1 miliardo di euro con il contributo di CDP Venture Capital) già stanziato per soggetti dell'economia sociale non profit che vogliano sviluppare IA sociale. Un secondo importante pilastro dovrebbe venire da quella parte di risorse che sono collocate all'interno del piano denominato «Repubblica digitale» [70] che è gestito dalle Fondazioni Bancarie (soggetti a pieno titolo facenti parte del mondo dell'economia sociale). All'interno dei bandi del programma dovrà trovare un adeguato spazio il tema dell'IA sociale.

Infine i soggetti *non profit* che intendessero partecipare all'Alleanza dovranno attivarsi con i cittadini per fare in modo che questi partecipino direttamente, non solo condividendo i loro dati digitali, ma conferendo anche le risorse economiche del loro 5x mille, in un grande programma di partecipazione popolare e democratica autofinanziato per la creazione di beni comuni digitali tramite le IA sociali.

Il recente accordo tra Open AI e News Corp per l'utilizzo a pagamento dei contenuti delle varie testate giornalistiche di proprietà di Murdoch per un valore di circa 250 milioni di dollari, mostra come si stia rapidamente sviluppando un mercato per i dati di qualità. Le cooperative di dati potrebbero, quindi, autofinanziare i propri modelli di IA Sociali, anche stringendo accordi di utilizzo dei propri "*Data Lake*" con soggetti terzi.

A queste risorse economiche andrebbe poi aggiunto, come detto, un importante *asset* che in Italia è pubblico ed è fortunatamente nelle mani delle istituzioni universitarie.

È la rete Europea pubblica dei supercomputer EuroHPC che ha l'obiettivo di creare un ecosistema di supercalcolo capace di garantire la sovranità tecnologica all'Europa e che ha ricevuto ingenti finanziamenti europei per oltre 8 miliardi euro.

---

[70] Cfr. sito istituzionale https://repubblicadigitale.gov.it, nel quale si trova precisato che «Repubblica Digitale è l'iniziativa nazionale che mira a ridurre il divario digitale e a promuovere l'educazione sulle tecnologie del futuro, supportando il processo di sviluppo del Paese. L'iniziativa è coordinata dal Dipartimento per la trasformazione digitale della Presidenza del Consiglio dei ministri».

Di questa rete fa parte il Consorzio Universitario Cineca (con sede a Bologna e che raccoglie 118 consorziati tra Università, Ministeri e istituzioni pubbliche) che dispone di uno tra i maggiori supercomputer europei [71]. Si tratta di Leonardo, sesto più potente HPC al mondo, grazie ai 250 milioni di miliardi di operazioni processate al secondo (246 *petaflop*) con una batteria di 14 mila GPU. Queste risorse computazionali pubbliche, riconoscendone la loro funzione sociale, dovrebbero riservare una quota del loro utilizzo per far funzionare gli algoritmi dell'IA sociali.

In questo modo come scrive il Prof. Ferraris «lo Stato potrà organizzare l'economia fondamentale (quella dei bisogni fondamentali) in collaborazione con le forme di auto-organizzazione delle comunità e con un Terzo settore potenziato» [72] e si potrà realizzare un ambiente favorevole e sicuro per l'utilizzo delle Intelligenza Artificiale guidata non più solo dal profitto individuale ma anche dal benessere comune.

[71] Da *Il Sole 24 ore*, Milano, 27 marzo 2024.

[72] M. FERRARIS, *op. cit.*

Capitolo X

Barriers to Geographic Data in Having a Data Cooperative: Satellites, Privacy, and the Dual Monopoly of States and Big Techs

Meem Arafat Manab-Nauani Schades Benevides[*]

Abstract: Why is it that geographic data, despite being commonplace, produced in a large amount every day, and in fact, also being easily accessible, still do not have many data collectives targeting them? In this short paper, we argue that geographic data, both from a technical and a legal perspective, are not afforded the protection they could be granted. With most satellites and GIS systems being confined in too few hands and the GDPR not including geolocational data among its list of sensitive personal data, it is increasingly difficult to sustain data collectives that target geolocational or geospatial data. We look at some of the data collectives that have been set up in the preceding years to cater to spatial data, and we show that the failure of these data collectives is a collective failure, as the required technologies to produce spatial data are owned by states and big techs and states, and that, paired with the lack of legal protection afforded to spatial data makes it exceedingly difficult to build a data collective or a data Trust that can secure independent data ownership of geographic data for users.

1. Introduction.

Data cooperatives and data trusts have been making a new resurgence, especially after the Data Governance Act came into force in the middle of 2022. Its article 2 defines these cooperatives as organized services for data intermediation, which will provide its members, either data subjects or SMEs or personal undertakings, with support for a wide range of data practices and rights. These supports cover the

[*] The individual sections of this essay have been jointly authored by both contributors.

facilitation of informed consent for data processing, correlating the members' interests with the purposes and conditions of data processing, and negotiation of terms and conditions on their behalf.[1] This definition gives leeway to a large number of services capable of being decentralized and member-owned through a data cooperative or a data Trust, including health services, agricultural productions, and business management. And this is where the surprising lack and faltering of geolocational data cooperatives come in. One-person undertakings, SMEs, and citizens all produce geographic data in a wide range, and then another stream of near-constant flow of geographic information can be traced to the satellites. Our argument shows that despite such affinity to personal lives, the path for geographic data to have data cooperatives is riddled with more difficulties when compared to, for instance, data cooperatives that deal with health data. The "strengthening" of individual positions that the Data Governance Act's Recital 31 promises to be a goal,[2] as our two-fold argument will show, is made significantly more intractable both from a technological and a legal reshaping of reality. Here, we will not use data Trusts and data cooperatives interchangeably, as the Data Governance Act only defines data cooperatives, and data Trusts, as discussed in previous literature,[3] broadly shares the same characteristics as cooperatives defined in the DGA.

2. Geographic Data.

What falls under the umbrella of geographic data from our point of view? Taking a cue from research is spatial data analysis, i.e. the most common methods of processing geographic data,[4] we assume geographic data to encompass any data that is implicitly or explicitly linked with a data subject's location on earth.[5] This naturally includes data generated from most GPS tracking devices, which then may or may not be further augmented with geographic information systems (GIS) software or satellite-produced images. With the advances in big data in particular, and also the introduction of location-based services that cater to needs as diverse as ordering food, ride-hailing, and even tracking your pets, we have more production and more use of geographic information at our fingertips. For our purpose, we will

[1] Art. 2 (Definitions), par. 1, No. 15, Reg. (EU) 868/2022 (*Data Governance Act*).

[2] Recital No. 31, Reg. 868/2022 (*Data Governance Act*).

[3] N. RADOSEVIC-M. DUCKHAM-M. SAIEDUR RAHAMAN-S. HO-K. WILLIAMS-T. HASHEM-Y. TAO, *Spatial data trusts: an emerging governance framework for sharing spatial data*, in *International Journal of Digital Earth*, Vol. 16, No. 1, 2023, pp. 1607-1639.

[4] A. SINGLETON-D. ARRIBAS BEL, *Geographic data science*, in *Geographical Analysis*, Vol. 53, No. 1, 2021, pp. 61-75.

[5] S. ELWOOD-M.F. GOODCHILD-D.Z. SUI, *Researching volunteered geographic information: Spatial data, geographic research, and new social practice*, in *Annals of the association of American geographers*, Vol. 102, No. 3, 2012, pp. 571-590.

not differentiate between geolocational data, geographic data, and geospatial data, as long as they are data directly linked with a data subject.

3. Technical Barriers.

Despite promising research that highlights data cooperatives as a desirable alternative to how big technological platforms treat geographic data, the reality is often far more crude and obstructive. For example, while Radosevic et al propose data sharing and accountability as desirable qualities,[6] with the bottleneck of only a handful of companies producing GPS trackers,[7] and then Google and Apple having established a dual monopoly over smartphones, sharing data generated by them through a data cooperative becomes genuinely impossible. States around the world, meanwhile, have long been using National Mapping and Cadaster Agencies (NMCAs)[8-9] for processing geographic data, but due to their top-down and often bureaucratic approach, they are seldom reliable for underdeveloped communities,[10] let alone data of individual data subjects. Notwithstanding these problems, we have seen the rise of socio-spatial networks such as Foursquare or Yelp, all to end in moderate to extreme failures.[11-12] To aggravate the already dire landscape, we also have tremendous overhead costs for spatial data governance, which, while still in cases profitable for big businesses, are often too overbearing for a smaller-sized data cooperative. The management of data from satellite systems as big as Europe's Copernicus program or NASA's LANDSAT is often far beyond the scope of what a data cooperative based on data subject's interests can pull off.[13]

---

[6] N. RADOSEVIC-M. DUCKHAM-M. SAIEDUR RAHAMAN-S. HO-K. WILLIAMS-T. HASHEM-Y. TAO, *Spatial data trusts: an emerging governance framework for sharing spatial data*, in *International Journal of Digital Earth*, Vol. 16, No. 1, 2023, pp. 1607-1639.

[7] NAVIXY, *Top 10 GPS tracker manufacturers*, available at https://www.navixy.com/blog/top-gps-tracker-manufacturers/, retrieved 12 April 2024.

[8] R. BENNETT-A. RAJABIFARD-I. WILLIAMSON-J. WALLACE. *On the Need for National Land Administration Infrastructures*, in *Land Use Policy*, Vol. 29, No. 1, 2012, pp. 208-219.

[9] M. SEIFERT-M. SALZMANN. *Cadastre* in W. KRESSE-D. DANKO (ed.), *Springer Handbook of Geographic Information*, Heidelberg: Springer International Publishing, 2022, pp. 581-611.

[10] N. GUPTA-S. BLAIR-R. NICHOLAS, *What We See, What We Don't See: Data Governance, Archaeological Spatial Databases and the Rights of Indigenous Peoples in an Age of Big Data*, in *Journal of Field Archaeology*, Vol. 45, No. sup 1, 2020, pp. S39-S50.

[11] J. FRITH-R. WILKEN, *Social shaping of mobile geomedia services: An analysis of Yelp and Foursquare*, in *Communication and the Public*, Vol. 4, No. 2, 2019, pp. 133-149.

[12] M. HOJATI-C. FARMER-R. FEICK-C. ROBERTSON, *Decentralized geoprivacy: leveraging social trust on the distributed web*, in *International Journal of Geographical Information Science*, Vol. 35, No. 12, 2021, pp. 2540-2566.

[13] S.C. ALVARADO, *The Regulation of the 'Open Data' Policy and Its Elements: The Legal Per-*

4. Legal Barriers.

A second criterion of barriers that all spatial data cooperatives must overcome is the lack of legal protection for geolocational data. On one hand, there is the continuous risk of re-identification of data subjects, vis-a-vis deanonymization and linking through various attributes.[14] Sometimes, the number of data subjects whose identity has been compromised can run up to hundreds or even thousands.[15] Notwithstanding, geolocational data is not considered a part of the special categories of data or sensitive data according to the GDPR, citing reasons such as it not constituting something personal for a data subject,[16] as opposed to sexual orientation or political beliefs, per se. At least in this regard, the United States has moved forward with tighter laws, with some states such as California[17] and Virginia[18] considering geographic location as sensitive data. It is indeed possible to profile and analyze a person based on the places they frequent, and its inclusion in the special category would be aptly befitting. We should note that someone's location can be used later to identify their sexual orientation or political beliefs, even though this purpose was not originally laid out. This fear was reaffirmed in the Article 29 Data Protection Working Party's Opinion 13/2011 on Geolocation services on smart mobile devices from 2011, where it states that «A behavioural pattern may also include special categories of data, if it for example reveal visits to hospitals and religious places, presence at political demonstrations or presence at other specific locations revealing data about for example sex life. These profiles can be used to take decisions that significantly affect the owner».[19] And indeed, this omission of geolocation from special category creates the biggest gap in creating data cooperatives for geographic data. A CJEU ruling from 2022 marks all data as sensitive when it can be used for later revelation of sensitive data,[20] and given that geolocation can always

---

spective of the EU Copernicus Programme, in *Space Law in a Networked World*, Brill Nijhoff, 2023, pp. 256-272.

[14] C. Culnane-A. Rubinstein-I. P. Benjamin-A. Teague, *Stop the Open Data Bus, We Want to Get Off*, 2019, arXiv:1908.05004v1.

[15] M. Douriez-H. Doraiswamy-J. Freire-C.T. Silva, *Anonymizing NYC Taxi Data: Does it Matter?*, in O. Zaiane-S. Matwin (ed.), *IEEE International Conference on Data Science and Advanced Analytics (DSAA)*, Montreal: IEEE, 2016, pp. 140-148.

[16] Information Governance Services, *Geolocation: The 'New Sensitive Data'?*, available at https://www.informationgovernanceservices.com/geolocation-the-new-sensitive-data/, retrieved 17 April 2024.

[17] California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), Cal. Civ. Code §§ 1798.140 (ae) and 1798.121.

[18] Virginia Consumer Data Protection Law (VCDPA), Va. Code § 59.1-517.

[19] Art. 29 Working Party, *Opinion 13/2011 on Geolocation services on smart mobile devices*, 16 May 2011, at 7.

[20] Case C-184/20, OT v Vyriausioji tarnybinės etikos komisija ECLI:EU:C:2022:601 para. 100.

be used for such revelation, data of this kind requires special attention. Despite the possibility of data linking through location that was admonished by the Article 29 Working Party in 2013,[21] the state of geolocation remained subject to later introspection, i.e. it would only be considered sensitive after it has been showed that some linking to other sensitive data has definitely been done. Given both the technical and the legal barriers in successful functioning of data cooperatives in light of the DGA, the lack of needed attention becomes more apparent. When we look at data cooperatives thriving in other fields, we see they either dealing with special categories of data (health data cooperatives, for example) or with some underprivileged domain-specific section of society (prison, farmers, etc.), both afforded at least some semblance of additional legal protection, and it is not realistic to expect characteristics such as data quality, data provenance, or data sovereignty without some added legal protection for geographic data.[22] A right step in the direction would be the immediate treatment of geographic data as a special category of its own. When geographic data is processed by data cooperatives, the data cooperatives themselves are required to «strengthen the position of individuals in making informed choices before consenting to data use, influencing the terms and conditions of data user organisations attached to data use in a manner that gives better choices to the individual members of the group or potentially finding solutions to conflicting positions of individual members of a group on how data can be used where such data relates to several data subjects within that group»,[23] because they have «as its main objectives to support its members in the exercise of their rights with respect to certain data, including with regard to making informed choices before they consent to data processing, to exchange views on data processing purposes and conditions that would best represent the interests of its members in relation to their data, and to negotiate terms and conditions for data processing on behalf of its members before giving permission to the processing of non-personal data or before they consent to the processing of personal data».[24] While, these definitions may, on the surface, seem to contradict our thesis, we are not denying the important role that data cooperatives can play. Theoretically, they should be able to maximize the positions of individuals, but our argument is that multiple practical limitations impede this maximization, and the efforts of data cooperatives remain conceptual at best, as shown by prior examples and also the bleak reality of current cooperatives dealing with geolocational data. All such data is intermediated by a few companies and some state-owned satellites, and without effectively removing

---

[21] ART. 29 WORKING PARTY, *Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation*, 13 May 2013.

[22] N. RADOSEVIC-M. DUCKHAM-M. SAIEDUR RAHAMAN-S. HO-K. WILLIAMS-T. HASHEM-Y. TAO, *Spatial data trusts: an emerging governance framework for sharing spatial data*, in *International Journal of Digital Earth*, Vol. 16, No. 1, 2023, pp. 1607-1639.

[23] Recital No. 31, Reg. (UE) 868/2022 (Data Governance Act).

[24] Art. 2 (Definitions), par. 1, No. 15, Reg. (UE) 868/2022 (Data Governance Act)

the intermediaries, or at any rate, without limiting their influence, data cooperatives that will deal with geographic data remain a tentative dream at best.

5. Conclusion.

While this short article may appear brooding or pessimistic in tone, that is only half of the narrative. There have been data cooperatives such as MIDATA[25] and Beneva[26] that use geographic data, and they have so far survived the test of time. But these cooperatives, we must restress, are focused on financial data or health data, i.e. some data that is already afforded additional legal protection. Besides, the narrower domain and push from either state or big companies (Beneva, for example, is financed by an insurance company) helps overcome most technical and economic difficulties. Hence, a narrower and well-protected domain can lead to some success in geographic data cooperatives. But, as long as most technologies for geographic data generation are gatekept by a few big companies and government organizations, and if personal geographic data is not treated as a special category/sensitive data, the cooperatives will have a hard time following up, depleting their meager resources. With the added risk of data being de-anonymized, the very existence of geographic data cooperatives cannot be guaranteed, as they would not be worth the trouble for most social entrepreneurs. It would need to be incentivized, and the first incentive can be entirely legal in nature as opposed to financial: which is the revising of GDPR's Article 9 (Processing of special categories of personal data) to directly include geolocation.

[25] N. SHADBOLT, *Midata: towards a personal information revolution*, in *Digital enlightenment yearbook*, 2013, pp. 202-224.

[26] E. BANZET, *Beneva Becomes First Canadian Insurer to Join the UN-Convened Net*, in *United Nations Environment Programme Finance Initiative*, 2023.

Capitolo XI

The cooperative model and the digital ecosystem: an alternative to platform capitalism?

Laura Tirabassi

Abstract: The digital transition has introduced new dimensions in our everyday life, creating complex hybrid realities where digital and physical spheres blend. Platforms, initially seen as participatory spaces promoting community engagement and free information exchange, have become intermediaries in personal data collection and analysis outlining new instances of capitalism within which users are crucial actors as both producers and consumers of data (Degli Esposti, 2015). The understanding of the current hybrid society thus calls for the observation of those principles and values embedded in platform infrastructures, the engagement paths and the mechanisms of data collection that constitute their primary economic asset. The investigation of the processes of platformization (Van Dijck, 2018), end-users' exploitation and their enclosure into digital walled gardens allow to critically envision the effect of platform capitalism and its implications in the diverse domain of contemporary society. To this extent, the present contribution aims to provide an overview on the complex scenario of digital platforms ruling the hybrid ecosystem, exploring its key actors as well as the proposed alternative of a decentralized infrastructure to ensure an open, ethical and user-centric digital environment thanks to a cooperative design (Scholz, 2016). Eventually, the case study of an electronic identity service in the Netherlands and the cooperative model within the public sphere as paths towards a fairer digital society are discussed.

1. Introduction.

Today, people are provided with new environments of experience by the digital

transition: needs, habits consumption paths as well as social imaginaries are shaped according to new possibilities and alternatives provided by the digital and technological tools introduced and adopted in our everyday life. The current hybrid reality, where the physical and the digital realms blur together within the flows of liquid globalizations, generates an increasing complexity in the diverse domains of contemporary political, economic and social organizations. Consumption and value creation processes encounter new transformations eventually resulting in creative destruction[1] and cultural lag[2] phenomena, both delivering tremendous changes in the material world as well as in the underlying economic, social and legal configurations. The concrete hybridization of the various domains of life sees the adoption of new devices that facilitates the mass collection of a vast quantity of personal information with different degrees of detail. Indeed, individuals regularly carry out practices of self-tracking through a number of sharing, feedback and self-exposure practices «to recirculate content as part of their identity and participation in social networks and communities[3]» within the engagement and participation frame. To date, the idea of a «quantified self» has penetrated the public debate until being commonly used to refer to the process of datafication i.e., those methods through which digital platforms render into data various practices, processes and aspects of human life that, thus far, have never been quantified in human history.[4] As a result, while platforms might be pictured as intermediary private actors allowing the interaction of different users and empowering them to shape their own service, products or even marketplace, the digital ecosystem gradually mold according to the logics of generating, engaging with and interpreting the knowledge collected and elaborated from personal data, benefiting from its materialization and representation. Whereas early visions on the potentialities of Web 2.0 as a new writing space[5] focused on an ideal participatory-based model able to offer mutual benefit to users and free circulation of information, enthusiasms have been counterbalanced by critical scholars who draw attention to the processes through which users' participation effectively occurs and the underlying values which orient and design the interaction modalities of the platform infrastructure. Before illustrating criticalities and implications of an increasingly hybrid context, it is fundamental to clarify what a platform is and how the digital environment has materially influenced and molded our capitalist economic system, eventually penetrating the current social fabric. Indeed, following a first section that sums up the main sociological approaches on digital prosumption and platform capitalism, this contribution presents the decen-

---

[1] J. SCHUMPETER, *Capitalism, Socialism, and Democracy*, New York, NY, 1942.

[2] W. F. OGBURN, *Social change with respect to cultural and original nature*, New York, NY, 1922.

[3] D. LUPTON, *Digital Sociology*, London, 2014, pp. 30-31.

[4] R. KITCHIN, *The Data Revolution: Big Data, Open Data, Data Infrastructures & Their Consequences*, London, 2014.

[5] J. D. BOLTER, *Writing space: Computers, hypertext, and the remediation of print*, II ed., London, 2011.

tralized, user-centric perspective offered by platform cooperativism model as an alternative in data management and use. To conclude, the related issues emerging in the public sphere with an on-topic case study are discussed.

2. What digital (plat)forms?

Platforms might be classified based on some evaluation criteria, such as the functions they implement, their purpose and size. Different platforms also provide different degrees of interaction, in both peer-to-peer and user-platform contexts, providing one or more functional purposes (i.e., transactional, network computing, services, social, entertaining, informational, financial). These combine at different levels of interactional depth, resulting in a wide variety of digital services and spaces (e.g. peer-to-peer marketplaces, hardware/software systems, matchmakers, exchanges, media and entertainment platforms, payment systems[6]). Platforms might therefore be grouped as super, large, middle and small according to the user scale (i.e. the number of active users within the platform), the types of operation involved and the restrictive ability of that specific platform to limit businesses or obstruct the connections of merchants with consumers.[7]

More generally, as sociologist José van Dijck explains, an online platform is a «programmable digital architecture designed to organize interactions between users– not just end users but also corporate entities and public bodies. It is geared towards the systematic collection, algorithmic processing, circulation, and monetization of user data[8]». The constituents of a platform anatomy are thus data, algorithms, interfaces, terms of use and a business model which define the operations through which the platform can create and capture economic value. More in detail, the core mechanisms of a platform life are datafication, commodification and selection, each of which cannot be analyzed as isolated but, rather, existing in a landscape of interconnected digital counterparts. Today, besides the prevailing platforms owned by the «Big Five» tech companies (Meta (Facebook), Apple, Microsoft, Alphabet (Google) and Amazon), «governments, incumbent (small and large) businesses, individual entrepreneurs, nongovernmental organizations, cooperatives, consumers, and citizens all participate in shaping the platform society's

[6] P. BELLEFLAMME-M. PEITZ, *Platforms: Definitions and Typology*, in P. BELLEFLAMME-M. PEITZ, *The Economics of Platforms: Concepts and Strategy*. Cambridge, 2021, pp. 10-40.

[7] G. WEBSTER-L. LASKAI-R. CREEMERS-J. COSTIGAN, *Translation: Guidelines for Internet Platform Categorization and Grading (Draft for Comment) – Oct. 2021*, DIGICHINA, 2022, https://digichina.stanford.edu/work/translation-guidelines-for-internet-platform-categorization-and-grading-draft-for-comment-oct-2021/ (30 April 2024).

[8] J. VAN DIJCK-T. POELL-M. DE WAAL, *The Platform Society. Public Values in a Connective World*, New York, NY, 2018, p. 4.

economic and social practices[9]». Rather than separate digital units coexisting in the same universe, the observation of the digital sphere as a living ecosystem allows to identify those norms, mechanisms and power relationships that outline platforms as interconnected and mutable actors, ultimately shaping and governing the digital society.

To date, the Western digital ecosystem has been mainly inhabited by two types of platforms: the platforms-infrastructure i.e., the «Big Five» group, and the sectoral platforms. The latter are also called «connectors» as they provide a digital service for one specific sector and depend on complementors namely, «organizations or individuals that provide products or services to end users *though* platforms, interlinking different «sides» and hence constituting multisided markets[10]». The criticality, here, emerges as private platforms, that present themselves as intermediaries aimed to facilitate the access to information and services, have been developing complex digital apparatuses where they eventually gain the monopoly on the data flows and end up as essential infrastructures that regulate and control the interaction among users, data and services, or simply what Van Dijck describes as a process of platformization.

3. The digital prosumer and its hidden costs.

The business model of sharing economy emphasizes the creative and empowering features of Web 2.0 and the figuratively flat infrastructure of platforms that, highlighting the horizontal feature of the hybrid network at stake, discourages the eye from noticing the unspoken labor necessary to produce and sustain the service offered. Within an increasingly hybridization of brick-and-mortar and digital spaces, the distinction between producers and consumers becomes undetectable. Indeed, there are no pure consumers benefiting from the digital service provided by a private platform but, rather, digital prosumers[11-12] that are simultaneously engaged in consumption and production processes[13]. These actors play a primary role in the digital economy as they constantly participate in interaction and data generation hence, they produce the premium value for the lifespan of any digital platform.

---

[9] J. VAN DIJCK-T. POELL-M. DE WAAL, *The Platform Society. Public Values in a Connective World*, cit., p. 4.

[10] J. VAN DIJCK-T. POELL-M. DE WAAL, *The Platform Society. Public Values in a Connective World*, cit., p. 17.

[11] A. TOFFLER, *The Third Wave*, New York, 1980.

[12] G. RITZER, *Prosumption: Evolution, Revolution, or Eternal Return of the Same?*, in *Journal of Consumer Culture*, 2014, 14, pp. 3-25.

[13] P. DEGLI ESPOSTI, *Essere prosumer nella società digitale. Produzione e consumo tra atomi e bit*, Milano, 2015.

The sharing economy system is grounded on and constantly promotes such duality, enabling the free exchange of goods and services through the double engagement of users as both producers and consumers. Traditional business models and intermediaries are now bypassed thanks to digital technologies and the Internet of Things. However, whereas prosumers are allowed to generate and manage their own goods, the spread and current reach of the sharing economy platforms reveals the significance of these key actors for the platform economy. Here resides the controversial nature of these apparently flat digital infrastructures: prosumers' work in the co-creation process of platform services and products remains unspoken and the platform ecosystem turns out to be composed of many contradictions as it appears equal but is hierarchical, it seems to serve public value but is primarily corporate and, even more importantly, it appears to promote bottom-up logic and consumer empowerment but does so through highly centralized paths that are opaque or deliberately obscure for its users.[14]

To conclude, prosumption perspective allows to observe new forms of work employment where consumers are also producers carrying out unpaid and socially unrecognized work, identifiable as a modern form of 'free labor'. Digital prosumers thus constitute the new group of exploited workers who produce economic value that turns into profit within and beyond the digital economy. Formulating it differently, a new stage of the capitalist system is introduced where profit is significantly increased by the simultaneous exploitation of both workers and consumers, or rather, working consumers[15] giving rise to a prosumer capitalism. By contrast, according to a more positive approach, digital environment and businesses generated by prosumption processes can be seen as spaces populated and controlled by prosumers themselves as they can actively and directly operate for their own benefit, rather than for the profitability of the companies of the platforms involved. The role of prosumers can thus be empowered by such opportunity of control exercised over what they prosume nurturing a democratic and co-operative digital ecosystem.[16]

4. Platforms and walled gardens.

However empowering and forward looking from a technologically optimistic perspective the digital environment results extremely invasive. Weber's iron cage

---

[14] J. VAN DIJCK, *Seeing the forest for the trees: Visualizing platformization and its governance*, in *New Media & Society*, 2021, Vol. 23, n. 9, pp. 2801-2819.

[15] P. DEGLI ESPOSTI-G. RITZER, *The Increasing and Invisible Impact of the Working Consumer on Paid Work*, in C. SUTER-J. CUVI-P. BALSIGER-M. NEDELCU, *The Future of Work*, Zurich, 2021, pp. 75-99.

[16] D. TAPSCOTT-A.D. WILLIAMS, *Wikinomics. How Mass Collaboration Changes Everything*, London, 2008.

of Weberian experienced by the individual in the industrial modernity, turns into a contemporary digital cage[17] that, although silent and invisible, is highly tighter and more binding; not only it engages with every aspect of life and is connected to past activities, but it is constantly alimented by the *lively data* collected through a variety of devices and digital tools, leaning towards particularly pervasive and asymmetrical forms of power e.g., the biopower produced by personal information gathering in the health sphere.[18] Online platforms are managed hierarchically by decisions made in the Silicon Valley and executed by black-box algorithms[19] providing their users with strictly interconnected and interdependent services and products generating what can be described as a walled garden. The walled garden metaphor highlights the closed traits and highly controlled environment of digital platforms as they are centralized, efficient and comfortable spaces, designed by the provider, where users are confined. The flow of information that circulates throughout and within the platform is thus centrally administrated, while users are often encouraged, if not required, to keep their activity within the confines of the platform, generating a limited exposure to external content. The idea of a walled garden is thus able to display the tendency to oligopolies and monopoly control that characterizes the platform ecosystem so far governed by private companies.

Within this frame, platforms can be described as digital re-programmable and data-driven infrastructures enabling the personalized and simplified interaction between end-users and complementors through collection, algorithmic processing, monetization and circulation of data.[20] They thrive on the increasing number of end-users as a higher number achieved causes what is defined as network effect,[21] which generates greater value, as well as significant capital accumulation thanks to the interaction paths. Accordingly, with the aim of progressively extracting data from its users, the platform utilizes a strategy of constant engagement and attraction, which translates users' activity into value, nurturing an exponential growth and hardening its gardens' walls. Finally, their multisided feature allows platform corporations to balance profits and efforts thanks to multiple-business branches. The penetrative capacity, the dynamicity, and the exponential growth of digital platforms currently position them at the center of public and private life of individuals. Entire economic key sectors and spheres of social life come influenced and

---

[17] R. SCHROEDER, *Big Data: Marx, Hayek, and Weber in a Data-Driven World*, in M. GRAHAM-W.H. DUTTON-M. CASTELLS, *Society and the Internet: How Networks of Information and Communication are Changing Our Lives*, Oxford, 2019.

[18] D. LUPTON, *Lively data, social fitness and biovalue: The intersections of health self-tracking and social media*, in J. BURGESS-A. MARWICK-T. POELL, *The sage handbook on social media*, London, 2015.

[19] F. PASQUALE, *The Black Box Society: The Secret Algorithms That Control Money and Information*, Cambridge, 2015.

[20] N. SRNICEK, *Platform Capitalism*, Cambridge, 2016.

[21] M.L. KATZ-C. SHAPIRO, *Systems Competition and Network Effects*, in *The Journal of Economic Perspectives*, 1994, Vol. 8, n. 2, pp. 93-115.

transformed according to such new infrastructure emphasizing how, one more time, «tools participate in shaping the world with us as we use them».[22] Platform capitalism thus poses new challenges within the rapidly transforming society, installing a top-down orchestration aimed at constantly achieving the value generated by the interaction with and among end-users. Moreover, as long as humans increasingly rely on algorithms,[23] the great questions running along the narrative is whether and to what extent this can be useful, powerful, harmful and fair to people's life. If «all data are people»[24] as well as data are *lively* themselves,[25] specific and urgent social aspects, such as equity, accessibility, fairness and transparency, need to be addressed when dealing with the public sphere. Conversely, the platform infrastructure assigns a crucial role to end-users since they are no more mere consumers of goods and services but, instead, they concretely participate in the economic process of goods' production as they are provided with the opportunity to act, connect and communicate through powerful means, reaching effective results within a seeming open landscape where the individual, or group of individuals, is given «a vantage point from which to act powerfully, a raised place to stand».[26]

Nevertheless, whereas platform capitalism might have contributed to decentralize many activities in the economic domain allowing its users to actively engage and circulate information and goods within its digital worlds, such change does not seem to correspond to an equivalent user-centric system since online platforms are centrally controlled by back-end server infrastructures eventually resulting into new forms of digital exploitation of the prosumer.[27]

5. The cooperative model as an alternative to platform capitalism.

5.1. Data as a commodity.

To shed light on possible alternatives to the platform capitalism driven ecosys-

---

[22] D. BOYD-K. CRAWFORD, *Critical questions for Big Data: Provocations for a cultural, technological, and scholarly phenomenon*, in *Information, Communication & Society*, 2012, Vol. 15, n. 5, p. 675.

[23] E. BOGERT-A. SCHECTER-R.T. WATSON, *Humans rely more on algorithms than social influence as a task becomes more difficult*, in *Sci Rep*, 2021, Vol. 11, n. 8028, pp. 1-9.

[24] M. ZOOK-S. BAROCAS-D. BOYD-K. CRAWFORD-E. KELLER-S.P. GANGADHARAN-A. GOODMAN-R. HOLLANDER-B.A. KOENIG-J. METCALF-A. NARAYANAN-A. NELSON-F. PASQUALE, *Ten simple rules for responsible big data research*, in *PLoS Computational Biology*, 2017, Vol. 13, n. 3, p. 2.

[25] D. LUPTON, *Lively data, social fitness and biovalue: The intersections of health self-tracking and social media*, cit.

[26] T. GILLESPIE, *The Platform Metaphor, Revisited*, Alexander von Humboldt Institute for Internet and Society, 2017, https://www.hiig.de/en/the-platform-metaphor-revisited/ (14 March 2024).

[27] E. PAPADIMITROPOULOS, *Platform Capitalism, Platform Cooperativism, and the Commons*, in *Rethinking Marxism*, 2021, Vol. 33, n. 2, pp. 246-262.

tem, it is imperative to change perspective on data and their digital domains. Indeed, on the other side of centralized Big-tech platform's model, is the incredibly democratic potential of a digital world able to foster open engagement processes, users' empowerment and bottom-up governance paths. An approach rooted in cooperative principles such as data valorization and emphasizing processes that, rather than to eradicate the contemporary platform economy, are aimed to propose different approaches and value design models to develop a varied and healthier digital ecosystem: a concrete endeavor to foster democratic digital environments in which data, so precious and valuable, become the passkey for a distributed and open governance of/by platforms *and* users.

Definitions of «Big Data» are as many as the new types of data[28] but an arguably exhaustive definition might be that they are «an imprecise description of a rich and complicated set of characteristics, practices, techniques, ethical issues, and outcomes all associated with data».[29] It can empower citizens and refine their relationship with the government agencies by means of more efficient, transparent and engaging public services. Nevertheless, while highlighting the benefits of this interdependence, such assumption must not fall into pure dataism[30] given that interpretation lays at the core of data analysis where more data does not stand for better data, especially as far as it represents the new «oil».[31]

Data valuation is highly dependent on the initial raw quality, on the context in which they are collected and on the ability to scale and generate profit from them. Accordingly, data can be redefined as a new commodity, a key resource in the digital economy since it is characterized by a low initial value that increases through refinement and analysis. Especially with regard to internet-related businesses, such mechanism gives rise to an economic model in which users do not effectively pay in monetary terms to benefit from a service or a product, rather, they do so through their consent to have data collected about themselves, thus, producing a new commodity. It is this immaterial characteristic that might cause a misleading understanding of the process producing this new commodity. Indeed, despite the absence of its raw value, «data can be replicated and distributed at negligible marginal costs, unlike physical goods requiring additional resources for each unit produced. This scalability affects pricing and value, as the cost to replicate data is minimal

---

[28] I. FOSTER-R. GHANI-R.S. JARMIN-F. KREUTER-J. LANE, *Big data and social science: data science methods and tools for research and practice*, New York, 2020.

[29] L. JAEPEC-F. KREUTER-M. BERG-P. BIEMER-P. DECKER-C. LAMPE-J. LANE-C. O'NEIL-A. USHER, *Big Data in Survey Research: AAPOR Task Force Report*, in *The Public Opinion Quarterly*, 2015, Vol. 79, n. 4, pp. 839-880.

[30] J.S. PEDERSEN, *The digital welfare state: Dataism versus relationshipism*, in J.S. PEDERSEN-A. WILKINSON, *Big Data: Promise, Application and Pitfalls*, Cheltenham, 2019, pp. 301-324.

[31] WORLD ECONOMIC FORUM, *Personal Data: The Emergence of a New Asset Class*, 2011, http://www.weforum.org/reports/ personal-data-emergence-new-asset-class (10 maggio 2024).

once the initial dataset is created».[32] Indeed, data as a commodity has intrinsic characteristics that no other type of product or exchange commodity currently possesses because although «data may be seen as the new oil that allows the system to hum along, (…) data is now the basis of the system and not simply a lubricant (…) it flows easily and quickly in many different directions. This is one of the qualities that makes data so valuable, but it also serves to make it highly dangerous».[33]

Starting from such assumption, the idea of a market for data might revitalize the dignity of data creators by means of a new "data dignity" which «translates the concept of human dignity that was central to defeating the totalitarianisms of the twentieth century to our contemporary context in which our data needs to be protected from new concentrations of power».[34] Additionally, data dignity does not call for a refusal of the network effects gains – in fact, it depends critically on big platforms – but instead, it introduces an informed attempt to maximize the benefits of digital platform architecture. Finally, and more importantly, to enable and make data dignity work, there is the need for an additional layer of organizations to mediate the process and bridge the gap between prosumers and data. These are the so-called «mediators of individual data», such as Data Cooperatives (introduced in the section 6.2. of this contribution) namely, organizations aimed at representing their members in a variety of forms through the negotiation of data royalties or wages, conferring the power of collective gains to the subjects who are the primary sources of the valuable data.[35]

5.2. The promises of platform cooperativism.

A promising option for individual data management to contrast the power exerted by digital platforms as intermediaries that facilitate, control and regulate the interaction between users, data and services within its digital infrastructure, is the cooperative model. A cooperative is «a voluntary association that is organized for the mutual benefit of a particular social, economic, and/or cultural agenda(s). (…) In cooperative enterprises, surpluses may be paid to members in the form of patronage returns proportional to the business done by each member of the cooperative».[36] Translated within the digital domain, platform cooperativism proposes an

---

[32] TODD HARBOUR, *The Paradox of Data: A Commodity Unlike Any Other*, Medium, 2024, https://medium.com/the-data-harbour/the-paradox-of-data-a-commodity-unlike-any-other-78690c3bf13d (10 maggio 2024).

[33] G. RITZER-J.M. RYAN-S. HAYES-M. ELLIOT-P. JANDRIĆ, *McDonaldization and Artificial Intelligence*, in *Postdigital Science and Education*, 2024, pp. 1-14.

[34] J. LANIER-E.G. WEYL, *A blueprint for a better digital society*, in *Harvard Business Review*, 2018, Vol. 26, p. 4.

[35] J. LANIER-E.G. WEYL, *A blueprint for a better digital society*, in *Harvard Business Review*, cit.

[36] P. DEGLI ESPOSTI, *Cooperatives*, in *The Wiley Blackwell Encyclopedia of Consumption and Consumer Studies*, Malden, MA, 2015, https://onlinelibrary.wiley.com/doi/10.1002/9781118989463.wbeccs078 (21 March 2014).

alternative to platform capitalism where platforms are owned and managed by the users, or better, prosumers themselves.

The cooperative frame provides platforms with new functions of cooperative structure i.e., members have a direct stake in the management of the data collected, the distribution of labour and the profits of the organization. More precisely, according to this frame, platform cooperative «is a mindset» where platform is intended as «a term used to describe an environment in which extractive or cooperative intermediaries offer their services or content».[37] As argued by Scholz, there are three parts comprising the concept of platform cooperativism: a) the implementation of a structural change that transfers the «technological heart» of sharing economy platforms (e.g., Uber, AirBnB or UpWork) to a different ownership model that is more consistent with democratic values; b) the principle of solidarity as the key component in the various forms of cooperatives, from multi-stakeholder to prosumer-owned platforms; c) the concepts of innovation and efficiency reframed to meet the shared common benefit of all, over the profit for the few. This practically results in direct ownership by workers which have a voice in the platform business decisions, sharing equally the profits generated by their work and the collection of data within a democratic co-operation system. Scholz points out that «platform capitalism is amazingly ineffective in watching out for people»[38] as the ownership of vast amounts of data and profits are concentrated in the hands of a few large companies, while the employees of these companies receive only a small portion of the value they create, and the end-users of the services provided, who contribute most to the generation of wealth by handing over ownership of the data provided with the use of the services, are totally dispossessed.

A good example of workers-owned cooperative platform is the one of Driver's Seat Cooperative, a driver-owned organization that enables drivers to benefit from their data collected on their working activity. This is possible as the pooling and analysis of data are fed back to workers who can thus organize their work according to these insights to optimize their incomes. Moreover, this cooperative platform is also able to sell the collected data to city agencies improving policy decisions and, even more importantly, redistributing back to members the profits from sales. Platform cooperative thus proposes an alternative to today's financialized capitalist model, where decisions are often taken by managers and investors, with little or no participation by workers and employees, with a resulting in large concentrations of wealth that can hardly be redistributed. It is aimed at providing member of the platforms with a different asset of the digital ecosystem where decisions are taken democratically by the members themselves, who have direct control over the man-

[37] T. SCHOLZ, *Platform cooperativism. Challenging the corporate sharing economy*, New York, NY, 2016, p. 14.

[38] T. SCHOLZ, *Platform cooperativism. Challenging the corporate sharing economy*, cit., p. 14.

agement of the platform, thus also increasing the multi-level permeability of the generated wealth and contributing to the creation of a new model of digital capitalism that is necessarily more sustainable in the long run.[39] After all, this is the promise of the fediverse, or federated network, where users can interact with each other across different servers allowing greater prosumers' control over their data while avoiding the need for central authority in a distributed network of networks.[40] The communication and exchange of information between multiple independent servers and software (e.g., Mastodon, Peertube, Pixelfed etc.) is possible thanks to the use of a shared protocol named ActivityPub. Many experts maintain that «the fediverse is heading in the right direction and operates in the way the original web (WWW) was designed to operate – as a distributed web of linked information»[41] as users can benefit from an increased control and freedom over their activity, since they are not bound to the platform profit-oriented architecture and its algorithms.

In other words, the proposed and evolving scenario of an alternative digital world to the current centralized platforms ecosystem, is the one of user-centric perspective in which interoperability, openness and de-centralization can weaken, if not defeat, network effects of centralized Big-Tech digital infrastructure and thus challenge platform capitalism.

6. Application of a user-centric approach in the hybrid public sphere.

In the hybrid public domain, infrastructures and services from the physical realm blur with the rapidly evolving landscape of digital platforms. If public services can be improved by digital tools that increase transparency, openness and facilitate citizens' involvement in decision-making processes, such tools do not guarantee an inclusive, diverse and informed public sphere given that «our diverse and heterogeneous cultural backgrounds make it difficult to recreate a unified public sphere, on or offline».[42] Nonetheless, the bureaucratic machine of public institutions has always depended on a variety of technological tools to manage the relations between citizens and the state, today «citizen data is one such tool» present-

---

[39] M.M. Bühler-I. Calzada-I. Cane-T. Jelinek-A. Kapoor-M. Mannan-S. Mehta-V. Mookerje-K. Nübel-A. Pentland-T. Scholz-D. Siddarth-J. Tait-B. Vaitla-J. Zhu, *Unlocking the Power of Digital Commons: Data Cooperatives as a Pathway for Data Sovereign, Innovative and Equitable Digital Communities*, in *Digital*, 2023, Vol. 3, n. 3, pp. 146-171.

[40] J. Anderlini-C. Milani, *Emerging Forms of Sociotechnical Organisation: The Case of the Fediverse*, in E. Armano-M. Briziarelli-E. Risi, *Digital Platforms and Algorithmic Subjectivities*, London, 2022, pp. 167-181.

[41] J. Ashford, *What Is the Fediverse, and Why Does It Matter?*, James Ashford, 2023, urly.it/3af1w, 29 April 2024.

[42] Z. Papacharissi, *The virtual sphere: The internet as a public sphere*, in *New Media & Society*, 2002, Vol. 4, n. 1, p. 22.

ing its by-design value system and operations, with «its affordances and limits».[43] From a user-centric perspective that strongly relates to the ideas of citizenship, commonality and accessibility, the opportunity presented by data in the digital space might enhance participation in public affairs and improve public services thanks to the greater interaction between citizens and institutions.

In this final section, among opportunities and challenges, a study case of a decentralized, attribute-based identification system and the following reflection on Data Cooperatives in the European regulatory framework are discussed as instances of a cooperative, distributed model for data valorization and citizen-prosumers' empowerment in the public sphere.

6.1. I Reveal My Attributes: the case of IRMA system.

With the aim to contribute to the development of infrastructures that are designed to govern the digital worlds on the basis of public values, the opportunity provided by an electronic identification service (eIDs) called IRMA (acronym for I Reveal My Attributes) is explored, as an example of decentralized, attribute-based, nonprofit and nonstate (DAN) system implemented in the Netherland. This DAN-eIDs' architecture is built on the idea that few eID systems allow users' control over which piece of information they give away in each different transactions or contexts.[44]

IRMA platform differs from centralized identification service such as Facebook Login as attributes of the users are stored locally on their devices rather than in a central database. Whereas social network sites (SNS) act as intermediaries that store and manage data flows usually without a defined user's control over what information is shared, in the IRMA App, after collecting their attributes, users actively choose to disclose them directly to the verifier avoiding the involvement of the issuer during the authentication process. Indeed, while Facebook Login collect extensive data from the user's authentication activities, possibly combining such data to profile the user or as primary source for targeted advertising, the Dutch public platform provides the user with the possibility to decide which attribute to reveal following the specific requirements of the verifier. Finally, the user-centric approach of this DAN-eIDs is displayed in its design, built on the principle of data minimization. Whereas many SNS log in procedure, such as Facebook Login, involve extensive data sharing and might include personal and behavioral data with purposes that go beyond the immediate authentication procedure, the IRMA App allows users to disclose only necessary attributes, enhancing users' privacy protection as well as providing a procedure that better aligns with the General Data Protection Regulation (GDPR) requirements.

---

[43] J. BURRELL-R. SINGH-P. DAVISON, *Keywords of the Datafied State*, Data & Society, 2024, p. 27, https://ssrn.com/abstract=4734250.

[44] J. VAN DIJCK-B. JACOBS, *Electronic identity services as sociotechnical and political-economic constructs*, in *New Media & Society*, 2020, Vol. 22, n. 5, pp. 896-914.

As the reported example of a decentralized, non-profit identification service shows, the issue of eIDs, just like other digital services, cannot be restricted to technical and legal compliance questions, but should be faced within the context of «(geo)political positioning – particularly in Europe which finds itself squeezed between centralized data systems run by governments, companies or, at best, public-private partnerships[45] (…) they are sensitive political-economic choices that raise questions of power and control in governing a digital society».[46] The opportunity of a decentralized, attribute-based, non-profit system may thus provide European members with an effective alternative to be effective actors within the global digital framework, able to counterbalance the power exercised by private market players that, as van Dijck puts it, are shaping the platform ecosystem and its architecture, leaving little room for civil society actors.

6.2. The evolving European scenario of Data Cooperatives in the public sphere.

Another instance to offer citizens the opportunity to regain control over their data is to provide them with the possibility to choose over its use while benefitting from the right to share its value. New data governance models emerge, aimed at mitigating the tension between data openness and data control, and making data accessible without sacrificing producers' power over it.

Within this frame, a step forward in democratizing the digital ecosystem has been embraced by the European Commission, with the purpose of redirecting the unprecedented potential of data towards the benefit of individuals, society and institutions throughout its governance and regulation. More in detail, the proposal is to move forward from the idea of data as a commodity, to data as «"a value" available to all, as a key factor of growth, wealth and development, for the entire society, including citizens, public administrations, enterprises and other public and private bodies».[47] Indeed, if the actions of public sector bodies should pursue the public good and interests to benefit the community, the valorization of data results unavoidably linked to such public interest. The Data Governance Act defines a set of rules for providers of data intermediation services to ensure that they will function as trustworthy organizers of data sharing. A possibly crucial role is presented by Data Cooperatives as they might enable open data models thanks to their digital architecture designed to create personal data stores ultimately aimed at the mutual benefit. By rebalancing the asymmetry between data

[45] J. VAN DIJCK-B. JACOBS, *Electronic identity services as sociotechnical and political-economic constructs*, cit. p. 897.

[46] J. VAN DIJCK-B. JACOBS, *Electronic identity services as sociotechnical and political-economic constructs*, cit. p. 911.

[47] F. BRAVO, *Data Governance Act and Re-Use of Data in the Public Sector*, in *European Review of Digital Administration & Law (ERDAL)*, 2022, Vol. 3, n. 2, p. 14.

subjects (i.e., those producing personal data) and data users (i.e., those using data to develop a service or product), Data Cooperatives might thus offer an opportunity to data subjects to organize and collectively participate in the decision-making processes on data usage, aiming at «the empowerment of individuals through collective use of their own personal data»,[48] and a promising direction to withstand data colonialism.[49] To do so, an essential first will be to affirm individuals' data rights into legislation and regulations, allowing them to negotiate and informedly choose terms and conditions. The entities designed to process data are indeed those registered as 'data-altruism organizations recognized in the Union' namely, entities of not-for-profit character that «meet transparency requirements as well as offer specific safeguards to protect the rights and interests of citizens and companies who share their data».[50]

In this regard, the role of Public Administration might be crucial to empower citizens and value their data in the public domain as it might act «in the public interest, as an intermediary, in the logics of re-use of data which it holds for its institutional purposes, while preserving the protection of the subjects to whom these data refer to who, thanks to the action of public administration, can enjoy an enhanced system that protects their rights».[51] However, a valorization of data processed by public authorities will require a congruent fine-tuning of concrete measures to create the fertile ground for cooperative modelling actions, such as the establishment of common European Data Spaces that «are envisioned as sovereign, trustworthy and interoperable data sharing environments where data can flow within and across sectors, in full respect of data.[52]

Nonetheless, Data Cooperatives have their limits for successful adoption since they require significant community engagement and trust to establish and maintain the cooperative organization,[53] plus a potential misuse of data might occur if it is not managed properly.[54] A vivid discussion, embracing academics', policy makers' and experts' endeavor to jointly develop a European regulatory framework and govern the digital ecosystem is thus essential to protect the citizen-prosumers, to

---

[48] A. PENTLAND-T. HARDJONO, *Data Cooperatives*, in A. PENTLAND-A. LIPTON-T. HARDJONO (eds.), *Building the New Economy: Data as Capital*, Cambridge, MA, 2020, pp. 19-35.

[49] G. PEREIRA-N. COULDRY, *Data Colonialism Now: Harms and Consequences*, in THE TIERRA COMÚN NETWORK, *Resisting Data Colonialism: A Practical Intervention*, Amsterdam, 2023, pp. 38-44.

[50] EUROPEAN COMMISSION, *Data Governance Act explained*, Shaping Europe's digital future, 2024, urly.it/3af1_, 18 May 2024.

[51] F. BRAVO, *Data Governance Act and Re-Use of Data in the Public Sector*, cit., p. 18.

[52] EUROPEAN COMMISSION, *A European Strategy for Data*, Brussels, 19 February 2020, COM (2020)66 final.

[53] J. PIERSON, *Digital platforms as entangled infrastructures: Addressing public values and trust in messaging apps*, in *European Journal of Communication*, 2021, Vol. 36, n. 4, pp. 349-361.

[54] G. GRABHER-J. KÖNIG, *Disruption, embedded. A Polanyian framing of the platform economy*, in *Sociologica*, 2020, Vol. 14, n. 1, pp. 95-118.

build an accountable, transparent and trustworthy public sphere, as well as to achieve, both in the private and public sectors, a «good governance»[55] in the transforming hybrid reality.

7. Conclusions.

This contribution has attempted to provide an introductory description of the intricate dynamics characterizing the digital ecosystem. In detail, the criticalities of the increasingly hybrid society have been illustrated and analyzed exploring the current traits of digital prosumers' exploitation, the main characteristics of the platformization process and the emerging conceptual framework that understand data as bounded to their generated value. To this extent, platform cooperativism has been discussed as a possible alternative to the implications of the digital economy, within which the working consumers' perspective[56] highlights the need for a horizontal organizational model to prevent a digital space where the pitfalls of digital exploitation "are either neutralized, ignored, or accepted as indispensable or inevitable components of this new capitalism».[57]

Reasonably, the centralized platform-oriented ecosystem and the de-centralized user-oriented model illustrated might replicate the intrinsic quality of «the internet as facilitating two dialectically antagonistic tendencies of competition and cooperation. The hegemonic competitive form of contemporary social relations thrives on the network structure of the internet but also gives rise to an emerging cooperative potentiality».[58] Within this frame, the lens of cultural lag highlights how the tremendous changes happening in one aspect of culture does not encounter coincident transformations in another aspect or, in other words, how the platformization process has already produced crucial transformations both in the private and public spheres without a corresponding appropriate regulatory framework within the European public context.

The analysis of digital platforms and the hybrid landscape they inhabit should thus be open to a broader debate on the current alternatives that might mitigate the effects of a profit-oriented digital economy penetrating individuals' private and public life, in the view of a democratically regulated digital ecosystem where «citizens would have the power to control their personal data and wield democratic

---

[55] M. BOVENS, *Public Accountability*, in E. FERLIE-L.E. LYNN-C. POLLITT, *The Oxford Handbook of Public Management*, Oxford, 2009, pp. 182-208.

[56] P. DEGLI ESPOSTI-G. RITZER, *The Increasing and Invisible Impact of the Working Consumer on Paid Work*, cit.

[57] E. FISHER, *Contemporary technology discourse and the legitimation of capitalism*, in *European Journal of Social Theory*, 2010, Vol. 13, n. 2, p. 236.

[58] C. FUCHS, *Internet and Society: Social Theory in the Information Age*, New York, NY, 2008.

control over what happens to collective data flows and repositories».[59] In this regard, given the limits of a successful digital cooperative model due to the implementation in different national contexts, an appropriate regulation framework would be supported by a common endeavor on data literacy on both the side of public bodies and citizens, as an essential first step to facilitate the development of equipped digital cooperative alternatives addressed to informed and engaged citizens.

To conclude, aware of the contradictions, challenging features and limits of digital cooperative models for data intermediation,[60-61] the user-centric perspective of cooperativism represent an opportunity to equipe the civil society with both the knowledge and tools to navigate the complexities of the digital age and mitigate the monopolistic tendency of platform capitalism, with the aim to foster a solid, resilient and fairer hybrid society.

[59] J. VAN DIJCK-T. POELL-M. DE WAAL, *The Platform Society. Public Values in a Connective World*, cit. p. 140.

[60] P. GASPER, *Are workers' cooperatives the alternative to capitalism*, in *International Socialist Review*, 2014, Vol. 93.

[61] T. SCHOLZ, *Platform cooperativism. Challenging the corporate sharing economy*, cit.

Capitolo XII

Intermediari di dati e cooperative di dati nell'ambito del *Data Governance Act*: verso un nuovo approccio nella gestione dei dati?

Stefano Torregiani

Abstract: During the last decade, the European legislator intervened many times in order to shape a data management system that would simultaneously allow the protection of individuals and the exploitation of the enormous potential deriving from the correct processing of data. In this regard, the most ambitious piece of EU legislation currently in force is certainly Regulation (EU) 2022/868, known as the Data Governance Act, due to the innovative «European» data governance model it enacts. This paper will focus on the analysis of one of the issues that could prove to be fundamental in the context of this new system, that is, the data intermediary, because it gives us the chance to evaluate where European data law is heading. By focusing on data cooperatives as a special category of intermediary, we will attempt to understand whether the time is ripe for a new approach to data protection.

1. Introduzione.

Di fronte alla rivoluzione cibernetica che ha travolto la nostra società [1], il legislatore europeo si è mosso introducendo una vasta gamma di provvedimenti di carattere normativo finalizzati a orientare lo sviluppo tecnologico verso la salvaguardia sia dei diritti e delle libertà dei cittadini degli Stati membri, sia della sovranità dell'Unione europea.

[1] A. SIMONCINI, *L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà*, in *BioLaw Journal – Rivista di BioDiritto*, 2019, 1, p. 63 ss.

Uno degli ambiti in cui le istituzioni eurounitarie si sono dimostrare più attive in termini di produzione legislativa è stato, ed è tuttora, quello che in dottrina viene definito «*data law*», corrispondente all'insieme dei corpi normativi diretti a disciplinare la gestione, la circolazione e la protezione dei dati [2].

Prendendo come riferimento temporale l'ultima decade, l'ordinamento europeo in materia di dati si è inizialmente evoluto verso un metodo di regolazione basato su una dicotomia fondativa tra i dati a carattere personale e i dati a carattere non personale. Segnatamente, il graduale percorso di costituzionalizzazione che ha contrassegnato il diritto alla protezione dei dati personali nel continente europeo ha portato dapprima alla cristallizzazione di una disciplina particolarmente protettiva con riguardo ai dati personali [3], da ultimo culminata con l'entrata in vigore del Regolamento (UE) 2016/679, anche noto con l'acronimo anglosassone di GDPR [4]. Sul versante opposto, invece, la fattispecie del dato non personale ha trovato definitiva positivizzazione nel contesto continentale solo con l'approvazione del Regolamento (UE) 2018/1807 relativo alla libera circolazione dei dati non personali all'interno dell'Unione europea [5].

Il quadro ordinamentale così consolidatosi è stato ben presto messo a dura prova dal mutamento di paradigma generato dagli sviluppi tecnologici più recenti [6]: la realizzazione di strumenti che consentono, con grande velocità e facilità, di individuare modelli ricorrenti e corrispondenze nascoste nell'ambito di grandi insiemi di dati [7], per un verso, ha portato a un maggiore accentramento di potere in capo ad attori, sia pubblici che privati, aventi sede al di fuori dell'UE [8], e, per un altro ver-

---

[2] T. STREINZ, *The Evolution of European Data Law*, in P. CRAIG-G. DE BÚRCA (eds.), *The Evolution of EU Law*, Oxford University Press, 2021, p. 902 ss. Sull'esigenza di un ordinamento costituzionale dei dati, si veda: S. CALZOLAIO, *Vulnerabilità della società digitale e ordinamento costituzionale dei dati*, in *Rivista italiana di informatica e diritto*, 2023, 2, pp. 13 ss.

[3] O. POLLICINO-M. BASSINI, *Commento all'art. 8 CdfUE*, in R. MASTROIANNI-O. POLLICINO-S. ALLEGREZZA-F. PAPPALARDO-O. RAZZOLINI (a cura di), *Carta dei diritti fondamentali dell'Unione europea*, Milano, 2017, p. 132 ss.

[4] S. CALZOLAIO, *Protezione dei dati personali*, in R. BIFULCO-A. CELOTTO-M. OLIVETTI (a cura di), *Digesto delle Discipline Pubblicistiche*, Utet giuridica, 2017, p. 598 ss.

[5] Per un approfondimento su tale peculiare fattispecie di dato, sia consentito rinviare a S. TORREGIANI, *Il dato non personale alla luce del Regolamento (UE) 2018/1807: tra anonimizzazione, ownership e Data by Design*, in *federalismi.it*, 2020, 18, p. 317 ss.

[6] A. SIMONCINI-S. SUWEIS, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in *Rivista di filosofia del diritto*, 2019, 1, pp. 87-106.

[7] J.-E. MAI, *Big data privacy: The datafication of personal information*, in *The Information Society*, 2016, Vol. 32, n. 3, p. 192 ss.; M. OROFINO, *Trattamento dei dati personali e libertà di espressione e di informazione*, in L. CALIFANO-C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, 2017, p. 508 ss.

[8] EUROPEAN COMMISSION, *Commission Staff Working Document, Impact Assessment Report Ac-*

so, sta mettendo fortemente in crisi la capacità della legislazione continentale di garantire un'adeguata protezione dei dati personali e una fruttuosa valorizzazione delle informazioni prodotte in territorio europeo.

Le perplessità circa l'attitudine di tale normativa a orientare lo sviluppo di sistemi di gestione dei dati nella maniera più proficua e costruttiva possibile per il vecchio continente hanno spinto il legislatore a intervenire nuovamente nell'oramai affollato ambito del *data law* europeo. Fra gli atti normativi di recente introduzione assume rilievo centrale il Regolamento (UE) 2022/868 relativo alla governance europea dei dati, meglio noto con il nome di «*Data Governance Act*» (di seguito, anche DGA)[9].

Nella mente delle istituzioni unionali, il *Data Governance Act* rappresenta il primo pilastro per la realizzazione di un modello «europeo» di *governance* dei dati, ossia di un differente approccio nella gestione delle informazioni che si discosti dalle altre realtà attualmente dominanti lo scenario internazionale, evitando in tal modo di rimanere vittima di un neocolonialismo digitale[10].

Sebbene il concetto di *data governance* europea non possa di certo ridursi ad un unico provvedimento normativo[11], il Regolamento (UE) 2022/868 rappresenta un tassello fondamentale all'interno del complesso mosaico che compone la *governance* in quanto atto trasversale e fondativo di un modello volto a incentivare una (ri)distribuzione equanime del valore ricavabile dai dati tra tutti i soggetti che contribuiscono alla loro generazione e, conseguentemente, orientato a impedire che le informazioni prodotte in territorio continentale possano divenire una risorsa solamente per autorità o industrie extraeuropee[12].

Nello strumentario che il DGA predispone al fine di promuovere una politica di condivisione dei dati finalizzata a un ottimale sfruttamento delle informazioni all'interno dell'Unione rientra anche l'intermediazione dei dati, intesa quale attività diretta alla instaurazione di un collegamento tra coloro che, da un lato, generano e trattano dati e chi, dall'altro, desidera accedere a tali dati per fini commerciali o non commerciali. In tale contesto, riveste dunque un ruolo cruciale la figura del-

---

companying the document Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act) Brussels, 25 November 2020, SWD(2020)295 final, p. 1.

[9] Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724, Regolamento sulla governance dei dati (GU L 152 del 3 giugno 2022).

[10] A. IANNUZZI, *La governance europea dei dati nella contesa per la sovranità digitale: un ponte verso la regolazione dell'intelligenza artificiale*, in *Studi parlamentari e di politica costituzionale*, 2021, Anno 54, n. 209, p. 50.

[11] A. IANNUZZI, *I regolamenti intersettoriali per l'istituzione dei «data spaces»: Data Governance Act e Data Act*, in S. CALZOLAIO-A. IANNUZZI-E. LONGO-M. OROFINO-F. PIZZETTI, *La regolazione europea della società digitale*, Torino, 2024, p. 107 ss.

[12] T. TOMBAL, *Economic Dependence and Data Access*, in *International Review of Intellectual Property and Competition Law (IIC)*, 2020, Issue 51, n. 1, p. 70 ss.

l'intermediario di dati in quanto, collocandosi nella posizione mediana tra i due opposti versanti dell'economia dei dati, riuscirebbe a stimolare enormemente la circolazione delle informazioni nell'Unione europea.

Il presente contributo mira ad approfondire la rilevante tematica dei servizi di intermediazione dei dati nel tentativo di comprendere quale impatto essi potrebbero avere sul sistema economico e giuridico europeo. Nello specifico, i servizi di intermediazione possono potenzialmente condurre verso una auspicabile rivisitazione degli attuali meccanismi di gestione dei dati, specie a carattere personale, sempre meno effettivi ed efficaci innanzi ai nuovi rischi derivanti dall'impiego delle più recenti tecnologie dell'informazione e della comunicazione [13].

A tal proposito, in una realtà *data-intensive* in cui si corre il pericolo di aumentare drasticamente l'asimmetria informativa tra chi genera i dati e chi li tratta per finalità proprie, può svolgere una funzione (costituzionalmente) essenziale una *species* di intermediario dei dati, sempre individuata dal DGA, ossia le cooperative di dati, il cui scopo primario è quello di salvaguardare i diritti e gli interessi di coloro i quali ricoprono la posizione che potremmo definire «debole» nell'ambito delle *value chains* dei dati.

In tal senso, sebbene il *Data Governance Act* sia concepito come disciplina recessiva rispetto al GDPR [14], l'ambito di applicazione riservato al Regolamento del 2022 – concernente indistintamente dati personali e non personali – lascia uno spazio di intervento, soprattutto al giurista, per riconsiderare le concrete modalità di protezione dei dati relativi alle persone fisiche nel contesto di un sistema di *governance* capace di coniugare lo sviluppo della *data economy* con il valore primario della tutela dei diritti individuali [15].

---

[13] Per una disamina dei rischi connessi allo sviluppo della tecnologia, si veda: E. LONGO, *La disciplina del "rischio digitale"*, in S. CALZOLAIO-A. IANNUZZI-E. LONGO-M. OROFINO-F. PIZZETTI, *La regolazione europea della società digitale*, Torino, 2024, p. 53 ss.

[14] Eloquente il tal senso l'art. 1, par. 3 del DGA, il quale prevede che: «Il diritto dell'Unione e nazionale in materia di protezione dei dati personali si applica a qualsiasi dato personale trattato in relazione al presente regolamento. In particolare, il presente regolamento non pregiudica i regolamenti (UE) 2016/679 e (UE) 2018/1725 e le direttive 2002/58/CE e (UE) 2016/680, anche per quando riguarda i poteri e le competenze delle autorità di controllo. In caso di conflitto tra il presente regolamento e il diritto dell'Unione in materia di protezione dei dati personali o il diritto nazionale adottato conformemente a tale diritto dell'Unione, prevale il pertinente diritto dell'Unione o nazionale in materia di protezione dei dati personali. Il presente regolamento non crea una base giuridica per il trattamento dei dati personali e non influisce sui diritti e sugli obblighi di cui ai regolamenti (UE) 2016/679 e (UE) 2018/1725 o alle direttive 2002/58/CE o (UE) 2016/680».

[15] Tale esigenza appare sempre più pressante alla luce della diffusione dell'idea di «riutilizzo dei dati», specie se personali, negli atti istituzionali dell'Unione, rinvenibile, oltre che all'interno del DGA, nella Proposta di Regolamento del Parlamento europeo e del Consiglio sullo spazio europeo dei dati sanitari del 3 maggio 2022 (COM(2022)197 final), il cui obiettivo è quello di creare il primo spazio europeo dei dati ipotizzato nel quadro della strategia europea per i dati utile a garantire l'uso primario e secondario dei dati sanitari elettronici.

2. Il nuovo modello «europeo» di *data governance*.

In linea con la «Strategia europea per i dati» da cui deriva [16], il *Data Governance Act* ha l'obiettivo di promuovere la creazione di uno «spazio unico europeo di dati» (*common European data space*) inteso quale «mercato interno dei dati nel quale questi ultimi possano essere utilizzati indipendentemente dal loro luogo fisico di conservazione nell'Unione, nel rispetto della normativa applicabile» [17]. Se durante i primi sviluppi dell'era digitale (Web 2.0) il nostro continente è rimasto a guardare mentre le altre potenze prendevano iniziativa, con questo ulteriore intervento il legislatore ambisce a superare gli ostacoli che ancora impediscono la piena realizzazione dell'immenso potenziale contenuto nelle informazioni generate dalle persone fisiche e giuridiche presenti in territorio europeo [18].

Il DGA rappresenta, dunque, il primo passo concreto verso la costruzione di tale spazio comune europeo, composto a sua volta da sottospazi settoriali che rappresentano il vero «*core tissue of an interconnected and competitive data economy in the EU*» [19]. All'interno di siffatto ecosistema, la condivisione dei dati favorisce un ampliamento della gamma di utilizzatori di dati in settori aventi ad oggetto attività economiche, strategiche o di pubblico interesse per l'Unione [20].

Lo spazio comune di dati si dovrebbe ipoteticamente tradurre in un sistema infrastrutturale e regolamentare di matrice continentale su cui le imprese private e gli enti pubblici possano fare affidamento per la gestione delle informazioni in loro possesso. Una volta implementato, esso consentirebbe la nascita di meccanismi di *governance* capaci di declinare i principi europei in materia di trattamento e gestione dei dati in misure legislative, amministrative e contrattuali idonee ad indirizzare lo sviluppo di ambienti sicuri di condivisione e accesso ai dati senza che i confini (digitali) dei singoli Stati membri possano costituire un ostacolo [21].

---

[16] COMMISSIONE EUROPEA, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, "Una strategia europea per i dati"*, Bruxelles, 19 febbraio 2020, COM(2020) 66 final.

[17] *Considerando* n. 2 del DGA.

[18] EUROPEAN COMMISSION, *Commission Staff Working Document, Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act)*, cit., p. 1.

[19] *Ibid*., p. 11.

[20] COMMISSIONE EUROPEA, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, "Una strategia europea per i dati"*, cit., pp. 5-6. La Commissione distingue nove spazi specifici in ragione della loro particolare rilevanza per gli interessi europei: manifattura, green deal, mobilità, sanità, finanza, energia, agricoltura, pubblica amministrazione, competenze.

[21] EUROPEAN COMMISSION, *Regulatory scrutiny board opinion, Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act)*, (SEC(2020) 405), p. 1.

Il termine *governance* è in questo senso evocativo di una presa di coscienza da parte del legislatore delle difficoltà che si frappongono alla regolazione di un settore così complesso come quello dei dati. La costruzione di uno spazio dinamico e interconnesso per lo scambio, la circolazione e il conseguente sfruttamento del patrimonio digitale continentale richiede un approccio multidimensionale che affianchi alle disposizioni giuridiche, norme tecniche e organizzative capaci di modellare «procedimenti di condivisione, accordi e standard tecnici, fino all'istituzione di strutture e processi per la condivisione dei dati in modo sicuro, anche attraverso soggetti terzi» [22]. Da ciò deriva anche una differente modalità di normazione dove, al classico metodo verticale puramente prescrittivo, viene anteposto un approccio collaborativo tra legislatore, settore privato e membri della collettività, al fine di consentire la maturazione di regole tarate in maniera più puntuale sul contesto di operatività dei soggetti coinvolti [23].

Nei documenti inerenti ai lavori preparatori antecedenti all'approvazione del DGA si avverte in maniera chiara l'intenzione di creare lo spazio comune europeo al fine di fornire una valida alternativa al cosiddetto «*Integrated Platform Model*» che costituisce il modello di trattamento di dati implementato dalle *big tech* extra-europee e consolidatosi, per lo più, grazie a una regolamentazione indulgente, se non del tutto assente [24]. L'accumulo di potere che deriva dalla messa in atto del modello delle piattaforme integrate, oggi predominante nella *data economy* e tendente verso la concentrazione di enormi quantità di dati nei *server* di pochi potenti attori, costituisce un grave pericolo sia per la protezione delle persone fisiche con riguardo al trattamento dei loro dati personali [25], sia per la concorrenza nel mercato europeo [26].

La volontà di prevenire il rafforzamento dell'oligarchia dei giganti della tecnologia ha spinto, dunque, verso un modello improntato ad una logica spiccatamente ridistributiva [27]. La divisione delle funzioni e la compartecipazione di più attori

---

[22] A. IANNUZZI, *La governance europea dei dati nella contesa per la sovranità digitale*, cit., p. 39.

[23] A. WERNICK-C. OLK-M. VON GRAFENSTEIN, *Defining Data Intermediaries – A Clearer View through the Lens of Intellectual Property Governance*, in *Technology and Regulation*, 2020, p. 66.

[24] EUROPEAN COMMISSION, *Commission Staff Working Document, Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act)*, cit., pp. 19-20.

[25] Alcune fra le piattaforme digitali più note si sono rese spesso protagoniste di episodi di violazione della normativa a tutela dei dati personali. A titolo di esempio, si richiamano i provvedimenti adottati dal Garante italiano per la protezione dei dati personali volti a sanzionare Facebook (Provvedimento del 10 gennaio 2019, Registro dei provvedimenti n. 5 (doc. web n. 9080914)) e Tik Tok (Provvedimento del 22 gennaio 2021, Registro dei provvedimenti n. 20 (doc. web n. 9524194)), o quello della Commission nationale de l'informatique et des libertés (CNIL) con cui è stata sanzionata Google (Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC).

[26] K.A. BAMBERGER-O. LOBEL, *Platform Market Power*, in *Berkeley Technology Law*, 2017, *Journal* 32, n. 3, pp. 1083-1087.

[27] EUROPEAN COMMISSION, *Commission Staff Working Document, Impact Assessment Report Ac-*

economici nella formazione delle catene di valore dei dati aspira a proporsi quale alternativa «europea» alla centralizzazione nella raccolta e nell'analisi dei dati delle grandi piattaforme digitali[28], riducendo drasticamente le opportunità di concentrazione e, conseguentemente, la creazione di monopoli e oligopoli [29].

La chiave di volta di questo rinnovato modello risiede nei meccanismi di condivisione dei dati che consentono di affiancare alla logica ridistributiva una logica collaborativa: il *data sharing*, strumento di politica economico-giuridica capace di incrementare il flusso di informazioni fra Stati membri e, di riflesso, l'accesso degli utenti, funge da perfetto grimaldello per scardinare lo *status quo* in cui ristagna la *governance* dei dati attuale. La messa a disposizione volontaria da parte del detentore, direttamente o tramite un intermediario, in favore di soggetti esterni alla propria organizzazione assume una carica propulsiva enorme per la circolazione delle informazioni nel territorio europeo [30].

La trasformazione dei dati da «sottoprodotto» ad asset autonomo e prezioso ha messo in evidenza la necessità di adottare politiche efficaci con riguardo alla loro condivisione. Il riutilizzo dei dati – ossia l'uso per una finalità diversa dalla originale – ha dimostrato di poter avere un valore e un impatto maggiori per la collettività, da un punto di vista sia economico che sociale, rispetto a quanto ne abbia l'utilizzo primario [31]. Al contempo però, proprio questa fondamentale capacità di analisi dei dati necessita di infrastrutture e di competenze che, spesso, non sono presenti all'interno dell'ente che li ha raccolti e trattati in prima istanza. Per tale motivo la condivisione potrebbe rappresentare un volano per la *data economy*, specie se si considera che essa può interessare differenti soggetti a seconda del modello operativo adottato. Il *data sharing*, infatti, può realizzarsi orizzontalmente quando avviene tra enti in concorrenza tra loro, in quanto operanti nello stesso mercato;

---

companying the document Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act), cit., pp. 19-20.

[28] Con riguardo ai profili inerenti all'applicazione della normativa sulla protezione dei dati personali alle piattaforme, si veda: E. GARZONIO, *Responsabilità degli ISP rispetto al trattamento automatizzato dei dati personali con finalità di comunicazione politica: applicabilità del GDPR alle piattaforme social*, in *MediaLaws*, 2019, 2, p. 190 ss.

[29] *Ibid*., pp. 10-11.

[30] Il fatto che la messa a disposizione sia volontaria, non implica necessariamente che la stessa debba in ogni caso essere gratuita. Anzi, soprattutto nel settore privato dove le disposizioni regolamentari non possono arrivare ad imporre un vero e proprio obbligo di *disclosure*, l'incentivo della remunerazione economica è assolutamente lecito, al pari di qualsiasi altro vantaggio, commerciale o non commerciale, di cui possa beneficiare l'ente privato disposto a condividere.

In aggiunta, dalla definizione di *data sharing* esula qualsiasi concessione di accesso che non risulti il frutto di una determinazione libera del detentore, sicché l'accesso dettato da provvedimenti delle autorità o per verifiche previste da disposizioni normative non potrà considerarsi come condivisione di dati.

[31] OECD, *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Reuse across Societies*, Paris, 2019, p. 17.

verticalmente se intercorre tra organizzazioni che hanno già un rapporto di collaborazione, generalmente perché ricoprono posizioni differenti nella stessa filiera di produzione e distribuzione; esternamente nei casi in cui l'ente permette l'accesso a operatori che si trovano al di fuori dal settore di mercato in cui agisce e che possono offrire un servizio sia su commissione che per interesse proprio [32].

Le esperienze di *data sharing* già realizzate negli Stati membri hanno dimostrato di poter offrire benefici importanti sia dal punto di vista individuale, con maggiore visibilità sul mercato e riduzione dei costi di transazione per la singola impresa, che collettivo poiché fra le principali esternalità positive che si accompagnano ad una massiccia condivisione dei dati figurano un deciso passo in avanti verso la definizione di standard comuni europei, minori barriere in entrata ai mercati e una funzione di supporto essenziale per l'innovazione tecnologica [33].

Malgrado i benefici anzidetti, il *data sharing* non è mai veramente decollato in ambito europeo. La realtà dei fatti restituisce uno spaccato in cui al timore di perdere vantaggi competitivi a causa della rivelazione di informazioni di carattere confidenziale o strategico corrisponde uno smisurato accumulo di dati nei cosiddetti «*data silos*» dove ristagnano per un tempo indefinito senza essere condivisi con altri attori al fine di trarre beneficio dalla relativa cooperazione [34]. Al mantenimento di tale situazione anti-economica contribuisce un quadro normativo in materia di dati finora di ardua comprensione, specie con riguardo alla qualificazione della natura del dato, alle conseguenze derivanti dalla involontaria re-identificazione delle persone fisiche e al riconoscimento dei diritti spettanti a chi ha contributo alla creazione dell'informazione [35].

Nella fattispecie, al fine di aggirare le barriere legali, commerciali, culturali e tecniche frutto della politica di *non-sharing by default* oggi dominante, il DGA si focalizza su specifiche situazioni la cui assenza di regolamentazione ha spesso condotto a soluzioni non ottimali o a squilibri di mercato. In primo luogo, esso punta a incrementare il riutilizzo di quelle informazioni detenute dalle pubbliche amministrazioni che, in quanto gravate da diritti altrui, non sono sottoposte all'obbligo di divulgazione imposto dalla Direttiva *Open Data* [36]. In secondo luogo,

---

[32] Altre distinzioni si basano sul grado di apertura consentito dal detentore dei dati – che può essere più o meno limitato, sino ad arrivare alla modalità *open data* – oppure ai mezzi utilizzati, dal punto di vista sia giuridico (contratti di licenza), sia tecnico (API, piattaforme, *marketplace, algorithm-to-the-data, privacy-preserving computation*).

[33] EUROPEAN COMMISSION, *Commission Staff Working Document, Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act)*, cit., p. 15.

[34] A. WERNICK-C. OLK-M. VON GRAFENSTEIN, *Defining Data Intermediaries*, cit., pp. 65-66.

[35] OECD, *Enhancing Access to and Sharing of Data*, cit., pp. 70-71.

[36] Capo II del DGA. Nello specifico, si tratta di informazioni detenute da enti pubblici che sono protette per motivi di riservatezza commerciale, riservatezza statistica; protezione dei diritti di proprietà intellettuale di terzi o protezione dei dati personali.

come anticipato, il Regolamento predispone un meccanismo normativo teso a costruire un clima di fiducia nei confronti di chi svolge servizi di intermediazione dei dati, perno del sistema [37]. Infine, sempre in un'ottica di stimolo alla circolazione dei dati, il provvedimento introduce una nuova modalità di condivisione delle informazioni, denominata *data altruism*, consistente nella disinteressata messa a disposizione di dati personali da parte delle persone fisiche e di dati non personali da parte di quelle giuridiche in favore di soggetti pronti ad utilizzarli per finalità di interesse generale [38].

I paragrafi che seguono si focalizzeranno su alcuni degli aspetti più interessanti toccati dal *Data Governance Act* in specifico riferimento alla tematica degli intermediari dei dati e all'enorme impatto che questa peculiare figura soggettiva potrebbe avere sul mercato digitale europeo.

3. Gli intermediari di dati nel *Data Governance Act*: tra accessorietà formale e indispensabilità sostanziale.

Nella configurazione del *data sharing* tratteggiata dal legislatore europeo si possono distinguere due tipologie di figure. Da un lato, compaiono quelle essenziali, in assenza delle quali non sarebbe possibile alcuna condivisione, mentre dall'altro, si trovano quelle eventuali, la cui presenza non è indispensabile per lo scambio di dati, anche se possono agevolare significativamente tale attività. All'interno della prima di queste due categorie rientrano sicuramente quelli che il DGA designa come «titolari dei dati» (*data holders*) e come «utenti dei dati» (*data users*) [39].

In particolare, il titolare dei dati coincide con la persona fisica o giuridica che «ha il diritto di concedere l'accesso a determinati dati personali o dati non personali o di condividerli» [40]. Nell'ambito del ciclo di trasferimenti seguito dalle informazioni, il *data holder* incarna quel soggetto che ha la facoltà – giuridica o di fatto – di interrompere o reindirizzare il flusso dei dati, indipendentemente dal suo effetti-

---

[37] Capo III del DGA.

[38] Capo IV del DGA. Il *data altruism* – come ulteriore canale aperto dal DGA al fine di incentivare la circolazione delle informazioni convogliandole in grandi *pool* che fungano da carburante per un migliore sfruttamento del patrimonio digitale europeo – costituisce la massima espressione del principio di solidarietà nella *data economy*, giacché riconosce alle persone fisiche e alle persone giuridiche la facoltà di, rispettivamente, acconsentire al trattamento dei propri dati personali o permettere l'utilizzo dei propri dati non personali, non per finalità individuali, ma nell'interesse della collettività, nel tentativo di produrre benefici diffusi per la società intera.

[39] Tale assunto pare deducibile dall'art. 2, p.to 10) del DGA ove la condivisione di dati viene definita come: «la fornitura di dati da un interessato o un titolare dei dati a un utente dei dati ai fini dell'utilizzo congiunto o individuale di tali dati, sulla base di accordi volontari o del diritto dell'Unione o nazionale, direttamente o tramite un intermediario, ad esempio nel quadro di licenze aperte o commerciali, dietro compenso o a titolo gratuito».

[40] Art. 2, punto 8) del DGA.

vo contributo dal punto di vista della raccolta o della definizione del contenuto dell'informazione.

Il DGA rimane tuttavia ambiguo in merito al corretto inquadramento giuridico di siffatto attore: se il termine inglese «*holder*» suggerisce l'adesione a quello che è stato definito «*facts-based approach*», dove le nozioni di possesso o detenzione non assumono un rilievo *stricto sensu* giuridico, i diritti potestativi di concessione dell'accesso o di condivisione lasciano propendere per un contrapposto «*rights-based approach*» [41].

Per converso, il titolo di utente dei dati spetta a quei soggetti che nel contesto del *data sharing* possono vantare un diritto di accesso sui dati detenuti dall'*holder* e che possono utilizzarli per finalità commerciali o non commerciali [42]. Rientrano in tale definizione persone fisiche, enti pubblici, ricercatori, organizzazioni non governative e imprese operanti nello stesso o in un diverso settore rispetto al titolare [43], che, mossi dallo scopo di estrarre valore aggiunto dai dati, sono i principali fautori dei benefici individuali e collettivi derivanti dalla condivisione [44].

Nel gruppo delle figure eventuali rientrano, invece, i soggetti che offrono servizi di intermediazione di dati.

A dispetto del loro carattere formalmente accessorio, nel modello di condivisione dei dati in commento la funzione degli intermediari, quale cerniera di collegamento tra i due attori necessari descritti in precedenza, è destinata a diventare un elemento caratterizzante del sistema europeo: sebbene, come detto, il *data sharing* possa prendere forma anche tramite la condivisione diretta tra titolare e utente, l'intermediario riveste una posizione decisiva all'interno del peculiare paradigma europeo di *data governance* in quanto tassello aggiuntivo «capace di offrire un approccio alternativo all'attuale modello commerciale per le piattaforme tecnologiche integrate» [45].

Il compito principale assolto dall'intermediario in esame è quello di agevolare l'incontro tra l'interesse del titolare dei dati a condividere e quello dell'utente dei dati ad avere accesso alle informazioni. In genere, al di là del modello continentale,

---

[41] AA.VV., *White Paper on the Data Governance Act*, in *CiTiP Working Paper, KU Leuven Centre for IT & IP Law*, 2021, pp. 10-13.

[42] Art. 2, punto 9) del DGA.

[43] EUROPEAN COMMISSION, *Impact Assessment on enhancing the use of data in Europe. Report on Task 1 – Data governance, prepared for the European Commission* (SMART 2020/694 | D2), p. 40.

[44] OECD, *Enhancing Access to and Sharing of Data*, cit., p. 35.

[45] COMMISSIONE EUROPEA, *Proposta di regolamento del Parlamento europeo e del Consiglio relativo alla governance europea dei dati (Atto sulla governance dei dati)*, Bruxelles, 25 novembre 2020, Com(2020)767 final, p. 6. Il medesimo concetto è ribadito nel testo finale del DGA ove al *considerando* n. 32 si prevede, fra l'altro, che: «Sia in situazioni in cui la condivisione di dati avviene tra due imprese sia quando ha luogo tra impresa e consumatore, i fornitori di servizi di intermediazione dei dati dovrebbero offrire una modalità nuova, "europea", di governance dei dati, garantendo una separazione, nell'economia dei dati, tra fornitura, intermediazione e utilizzo dei dati».

rientra in tale categoria una gamma di soggetti del tutto eterogenea poiché le attività di intermediazione differiscono a seconda dell'utenza, del tipo di dati coinvolti e dell'eventuale inclusione di servizi a valore aggiunto. Fra gli esempi più rilevanti nell'ambito della condivisione fra privati, meritano di essere menzionati i *data marketplaces* che raccolgono dati da numerosi *data holders* al fine di permettere il riutilizzo agli utenti, le *industrial data platforms* che offrono un ambiente virtuale sicuro e con regole comuni per lo scambio di informazioni tra le imprese partecipanti, i *personal information management services* (PIMS) il cui scopo principale è quello di garantire maggiore controllo e potere agli individui tramite mezzi tecnici che permettono di esercitare i diritti loro riconosciuti in maniera più effettiva e rapida, le *trusted third parties* dove l'intermediario ricopre l'incarico di ente certificatore con il compito di attestare la sussistenza di tutti i requisiti in materia, fra l'altro, di *privacy*, di sicurezza e di infrastruttura in capo alle organizzazioni partecipanti e, infine, le *data cooperatives* dove la gestione dei dati, specie personali, viene espletata al fine di riequilibrare l'asimmetria informativa che spesso pesa sugli interessati [46].

La forma adottata assume particolare rilievo con riguardo ai servizi che l'intermediario è in grado di offrire poiché, oltre al *matchmaking* tra *holder* e *user* e alla certificazione dell'avvenuta transazione, possono aggiungersi delle peculiarità capaci di rendere il *data sharing* tramite intermediazione estremamente appetibile per le imprese. Fra queste, degne di nota sono la predisposizione di clausole contrattuali standard, l'elaborazione dei dati al fine di convertirli in un formato comune o di anonimizzare informazioni personali o confidenziali, fino ad arrivare a servizi che consentono al titolare dei dati di mantenere un ampio controllo sulle informazioni condivise per mezzo di misure tecniche che garantiscono la conoscenza dell'identità di chi accede e le modalità con cui i dati vengono trattati [47]. In tal senso, l'intermediario si caratterizza come quel soggetto che, anche ricorrendo ad apposite clausole *smart* di gestione dei dati [48], mette a disposizione di titolari e utenti un sistema di *data governance* che, grazie alla conformità alla normativa europea conferita per impostazione predefinita, consente un flusso massivo, in entrata e in uscita, di informazioni essenziali per le politiche pubbliche, le attività di impresa e lo sviluppo della ricerca.

---

[46] EUROPEAN COMMISSION, *Impact Assessment on enhancing the use of data in Europe*, cit., pp. 38-40.

[47] EUROPEAN COMMISSION, *Commission Staff Working Document "Guidance on sharing private sector data in the European data economy", Accompanying the document Communication from the Commission to the European Parliament, the Council, the European economic and social Committee and the Committee of the Regions "Towards a common European data space"*, Brussels, 25 april 2018, SWD(2018) 125 final, p. 11.

[48] Per un approfondimento in merito alle implicazioni giuridiche legate alla diffusione degli smart contracts, si veda: C. BOMPREZZI, *Implications of Blockchain-Based Smart Contracts on Contract Law*, in *Luxembourg Legal Studies*, 2021, Vol. 23, pp. 47-73.

Tornando nel contesto del Reg. (UE) 2022/868, la versione «europea» di intermediario predisposta dal testo di legge gode di una libertà di azione piuttosto circoscritta, specie in virtù dell'introduzione dell'obbligo di neutralità sullo stesso gravante [49]. Eloquente in tal senso il *considerando* n. 33 del DGA nella parte in cui stabilisce che: «Un elemento essenziale attraverso il quale aumentare la fiducia e il controllo dei titolari dei dati, interessati e utenti dei dati nei servizi di intermediazione dei dati è la neutralità dei fornitori di servizi di intermediazione dei dati riguardo ai dati scambiati tra titolari dei dati o interessati e utenti dei dati». In ossequio a tale requisito, l'intermediario deve limitarsi ad instaurare una connessione tra titolare e utente, senza poter poi impiegare i dati che entrano nella sua disponibilità per finalità diverse dal semplice *sharing*, salva tuttavia la possibilità di utilizzo delle informazioni ricevute per il miglioramento dei propri servizi [50].

In primo luogo, tale aspetto implica che, se un'organizzazione desidera operare in qualità di intermediario in aggiunta ad altri servizi già parte del suo *business*, dovrà necessariamente procedere in via preventiva a una separazione strutturale del proprio organigramma [51]. Prescrizioni di questo tenore mirano sia a evitare la comparsa di conflitti di interesse fra gli intermediari che potrebbero sfruttare la loro posizione di privilegio per entrare nel mercato in cui operano i titolari e gli utenti, sia a disincentivare l'ingresso in questa nuova fetta di mercato di attori che hanno già a loro disposizione grandi quantità di dati.

In secondo luogo, l'obbligo di neutralità impone l'applicazione del principio di non discriminazione al fine di prevenire la creazione di regimi di trattamento differenziati a seconda del tipo di *holder* o *user* interessato a partecipare (*openness obligation*) [52], o del contenuto dei dati trattati (*zero knowledge platform approach*), salvo un controllo, seppur limitato, volto a contrastare condotte criminali che potrebbero consumarsi per il tramite dell'intermediario [53].

---

[49] F. CALOPRISCO, *Data Governance Act. Condivisione e "altruismo" dei dati*, in *Associazione Italiana Studiosi di Diritto dell'Unione europea (AISDUE), Focus "Servizi e piattaforme digitali"*, 2021, 3, p. 68.

[50] Così sempre il *considerando* n. 33 del DGA.

[51] Art. 12, lett. *a)* del DGA. Particolarmente rilevante al riguardo risulta ancora il *considerando* n. 33 che, oltre a parlare di «separazione strutturale tra il servizio di intermediazione dei dati e qualsiasi altro servizio fornito, in modo tale da evitare conflitti di interessi», specifica che: «Le condizioni commerciali, compresa la fissazione dei prezzi, per la fornitura dei servizi di intermediazione dei dati non dovrebbero essere subordinate al fatto che un potenziale titolare dei dati o utente dei dati utilizzi altri servizi forniti dallo stesso fornitore di servizi di intermediazione dei dati o da un'entità collegata, tra cui l'archiviazione, l'analisi, l'intelligenza artificiale o altre applicazioni basate sui dati, e, in caso affermativo, dalla misura in cui il titolare dei dati o gli utenti dei dati utilizzino tali altri servizi», prescrivendo un obbligo di neutralità a tuttotondo.

[52] EUROPEAN COMMISSION, *Commission Staff Working Document, Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act)*, cit., pp. 25-27.

[53] Questo è quanto emerso durante le consultazioni preliminari. A tal proposito, si veda il *Work-*

Da tali osservazioni è possibile dedurre che l'intermediario europeo dovrebbe assumere un atteggiamento piuttosto passivo, agendo da ponte tra titolare e utente per mezzo degli strumenti tecnici, giuridici o di altro tipo utili alla instaurazione di un rapporto commerciale di condivisione dei dati, ma senza privilegiare i propri interessi o quelli di alcuni solamente fra i partecipanti. Per tale ragione, pur rientrando nella definizione generale di intermediario, non sono considerati tali ai sensi del capo III del DGA quelli che servono gruppi chiusi di *holder* e *user* o che consentono solamente l'utilizzo dei dati detenuti da un unico titolare e quelli che aggregano, arricchiscono o trasformano i dati aggiungendovi valore sostanziale [54].

Al contempo però, il requisito della neutralità può servire l'ulteriore scopo di impedire alle *Big Tech* di entrare in questo nuovo settore di mercato dove il vantaggio competitivo di cui già godono in virtù della loro posizione causerebbe una illegittima alterazione della concorrenza. Come è stato osservato, il DGA pone le condizioni per la creazione di una «nicchia di mercato» popolata da imprese europee [55], specie piccole e medie, che sia indipendente da «qualsiasi operatore che detenga un grado significativo di potere di mercato» [56].

Siffatta caratterizzazione della figura dell'intermediario risponde all'esigenza di infondere fiducia nella condivisione dei dati in seno al mercato digitale europeo. La possibilità di fare affidamento su una figura intermedia a cui è vietato entrare in concorrenza con gli altri operatori potrebbe rivelarsi determinante al fine di stimolare un flusso dei dati efficiente, caratterizzato da costi di transazione contenuti, elevata qualità e standard comuni. In sostanza, lo sviluppo dell'ecosistema digitale europeo passa anche attraverso la figura mancante dell'intermediario di dati: se il *data sharing* rappresenta il mezzo che permetterà all'Unione europea di realizzare un modello differente, è possibile sostenere che l'intermediario, mentre «inventa» e determina l'infrastruttura di *governance* del digitale, ricoprirà il ruolo di pilota, poiché è su questi che grava il compito di separare chiaramente la fornitura, l'intermediazione e l'utilizzo dei dati e di creare un ambiente aperto, equo e democratico che sia capace di accantonare, o almeno affiancare, il sistema delle grandi piattaforme [57].

---

shop on labels for or certification of providers of technical solutions for data exchange: Summary of discussions, del 12 maggio 2020, pp. 2-4. Sembra deporre in tal senso anche l'art. 12 lett. *c*) del DGA nella parte in cui prevede che: «i dati raccolti su qualsiasi attività di una persona fisica o giuridica ai fini della fornitura del servizio di intermediazione dei dati, compresi la data, l'ora e i dati di geolocalizzazione, la durata dell'attività e i collegamenti con altre persone fisiche o giuridiche stabiliti dalla persona che utilizza il servizio di intermediazione dei dati, sono utilizzati solo per lo sviluppo di tale servizio di intermediazione dei dati, il che può comportare l'uso di dati per l'individuazione di frodi o a fini di cibersicurezza».

[54] Siffatte esclusioni sono espressamente disposte dall'art. 2, n. 11, del DGA nella parte in cui definisce i «servizi di intermediazione di dati».

[55] A. IANNUZZI, *La governance europea dei dati nella contesa per la sovranità digitale*, cit., pp. 42-44.

[56] *Considerando* n. 27 del DGA.

[57] *Considerando* n. 32 del DGA.

Alla luce di ciò, non può che essere accolta positivamente la scelta di affidare a un attore come l'intermediario di dati il ruolo di cardine del modello europeo. La predisposizione di un «filtro» nell'ambito dei flussi di informazioni consentirebbe di superare alcuni fra i più spinosi problemi caratterizzanti l'analisi e il riutilizzo dei dati [58]. La strutturazione dei servizi di intermediazione prospettata nel DGA si rivela estremamente preziosa per quella consistente porzione del mercato continentale costituita da piccole e medie imprese, le quali si trovano costantemente costrette a fronteggiare serie difficoltà con riguardo alla corretta identificazione dei dati che possono essere condivisi o riutilizzati senza infrangere norme di legge o accordi privati [59]. In tal senso, l'intermediazione, malgrado la sua accessorietà, appare un elemento indispensabile per aumentare la fiducia nei confronti della condivisione, per promuovere standard specifici per ogni settore a beneficio dell'interoperabilità e, infine, per procedere a una maggiore distribuzione del potere di mercato.

4. Le cooperative di dati come *species* di intermediario: tratti comuni e tratti distintivi.

Il requisito della neutralità previsto dal DGA potrebbe richiedere una lettura parzialmente diversa con riguardo a quelle particolari tipologie di intermediari il cui obiettivo non risiede solamente nella promozione dello scambio di dati, ma altresì nella facilitazione dell'esercizio dei diritti e nella salvaguardia degli interessi di determinate tipologie di soggetti che decidono di condividere i dati personali che li riguardano o i dati non personali a loro disposizione.

---

[58] Fra le problematiche più impattanti nel mondo della gestione dei dati, oltre alla protezione dei dati personali, figurano sicuramente: la corretta qualificazione del dato, le misure di de-identificazione (specie l'anonimizzazione e la pseudonimizzazione) e la proprietà o l'accesso ai dati. Si vedano, al riguardo: S. STALLA-BOURDILLON-A. KNIGHT, *Anonymous data v. Personal Data – A false debate: an EU perspective on anonymization, pseudonymization and personal data*, in *Wisconsin International Law Journal*, 2016; G. D'ACQUISTO-M. NALDI, *Big data e privacy by design. Anonimizzazione, pseudonimizzazione, sicurezza*, Torino, 2017; A. GALIANO-A. LEOGRANDE-S.F. MASSARI-A. MASSARO, *I dati non personali: la natura e il valore, in Rivista italiana di informatica e diritto*, 2020, 1, p. 1 ss.; C. IRTI, *Personal Data, Non-Personal Data, Anonymised Data, Pseudonymised Data, De-identified Data*, in R. SENIGAGLIA-C. IRTI-A. BERNES (eds.), *Privacy and Data Protection in Software Service*, Springer, 2022; C. FOGLIA, *Il dilemma (ancora aperto) dell'anonimizzazione e il ruolo della pseudonimizzazione nel GDPR*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali tra libertà e regole del mercato. Commentario al Regolamento UE n. 679/2016 e al d.lgs. n. 101/2018*, 2019, pp. 309-332; P. OHM, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, in *UCLA Law Review*, 2010, Vol. 57, p. 1701 ss.; AA.VV., *Data Ownership and Access to Data. Position Statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the Current European Debate*, in *Max Planck Institute for Innovation & Competition Research Paper* No. 16-10, 2016.

[59] EUROPEAN COMMISSION, *Commission Staff Working Document "Guidance on sharing private sector data in the European data economy"*, cit., p. 1.

Sotto questo aspetto, appare particolarmente interessante approfondire il tema di quella singolare figura che all'interno della complessa categoria dell'intermediario dei dati, come declinata nell'ambito del *Data Governance Act*, viene identificata come «cooperativa di dati», giacché in riferimento alla stessa il Regolamento (UE) 2022/868 sembra prevedere (o quantomeno sembra aprire alla possibilità di contemplare) una caratterizzazione parzialmente differente.

In quella che potrebbe essere letta come una prima tassonomia normativa dei servizi di intermediazione di dati, l'art. 10 del DGA fa riferimento a tre distinte tipologie di intermediari. Compaiono, segnatamente, i servizi di intermediazione tra i titolari dei dati e i potenziali utenti dei dati, i servizi di intermediazione tra persone fisiche e potenziali utenti dei dati, e, da ultimo, i servizi di cooperative di dati, le quali, in sostanza, vantano caratteristiche in parte differenti rispetto alle prime due classi di intermediari [60].

Anche sotto il profilo definitorio si percepisce una chiara volontà legislativa di distinguere le diverse tipologie, laddove, nell'articolo in cui sono accorpate tutte le definizioni rilevanti ai fini dell'applicazione del Regolamento 2022/868, compaiono simultaneamente sia la definizione di «servizio di intermediazione dei dati» [61], sia quella di «servizi di cooperative di dati» [62].

In proposito, l'art. 2, n. 15, del DGA fissa, sebbene indirettamente, i tratti caratterizzanti della cooperativa di dati, la quale consiste in una «struttura organizzativa costituita da interessati, imprese individuali o da PMI, che sono membri di tale struttura, avente come obiettivi principali quelli di aiutare i propri membri nell'esercizio dei loro diritti in relazione a determinati dati, anche per quanto riguarda il compiere scelte informate prima di acconsentire al trattamento dei dati, di procedere a uno scambio di opinioni sulle finalità e sulle condizioni del trattamento dei dati che rappresenterebbero al meglio gli interessi dei propri membri in relazione ai loro dati, o di negoziare i termini e le condizioni per il trattamento dei dati per conto dei membri prima di concedere l'autorizzazione al trattamento dei dati non personali o prima che essi diano il loro consenso al trattamento dei dati personali».

In sostanza, gli aspetti che contraddistinguono la cooperativa di dati sono riconducibili a due profili: da un lato, quello organizzativo e, dall'altro, quello teleologico.

Per quanto concerne il primo profilo, la cooperativa deve consistere in una «struttura organizzativa» – elemento che appare come l'unica aggiunta significativa rispetto alla definizione contenuta nella proposta di regolamento [63] – all'interno

---

[60] Analoga distinzione compare nei *considerando* da 28 a 31 del DGA.

[61] Art. 2, n. 11, del DGA.

[62] Art. 2, n. 15, del DGA.

[63] Sebbene nella proposta originaria non fosse presente una specifica definizione dei servizi delle cooperative dei dati all'interno dell'art. 2 – come del resto non compariva neanche quella di servizi di intermediazione – la descrizione delle cooperative dal punto di vista sostanziale era presente all'interno del proposto art. 9 (corrispondente all'art. 10 del testo definitivo) ove alla lett. *c*) veniva stabilito che fra i servizi condivisione dei dati soggetti a una procedura di notifica rientravano: «servizi di coo-

della quale possono rientrare solamente specifiche tipologie di soggetti, ossia quelli che ricoprono la posizione debole, dal punto di vista contrattuale, nel contesto dell'economia digitale: gli interessati, le imprese individuali o le piccole e medie imprese; tutte entità che spesso non hanno modo di incidere significativamente sulle decisioni prese dalle *Big Tech* [64].

In riferimento al secondo profilo, l'attività della cooperativa deve avere come scopo l'ausilio ai membri della struttura con riguardo all'esercizio dei diritti concernenti i dati di loro pertinenza, la valorizzazione di un confronto costruttivo tra le diverse posizioni che possono emergere in seno alla cooperativa e l'attività di negoziazione preventiva di termini e condizioni per il trattamento dei dati.

Peraltro, essendo siffatti obiettivi espressamente definitivi come principali, la cooperativa potrebbe anche soddisfare ulteriori esigenze dei membri della struttura, purché conformi alla natura di organizzazione cooperativa.

In questo senso, è proprio la qualificazione giuridica dell'intermediario che consente di tracciare la distinzione tra i servizi offerti dalle cooperative di dati e gli altri servizi definiti alle lett. *a)* e *b)* dell'art. 10 del DGA. Sebbene rischi di sovrapposizione potrebbero ravvisarsi anche con riguardo alla figura di intermediario di cui alla lett. *a)*, relativa alla prestazione dei servizi in favore di titolari dei dati e utenti dei dati [65], la corretta demarcazione della linea di confine rimane più difficoltosa tra l'area di intervento degli intermediari di cui alla lett. *b)* e l'area di intervento degli intermediari di cui alla lett. *c)*, relativa ai servizi offerti delle cooperative di dati.

Entrambe le tipologie di intermediario, infatti, vantano come tratto qualificante la prestazione di servizi aventi come finalità il tendenziale riequilibrio della asimmetria informativa a danno di una specifica gamma di soggetti, interessati e piccole imprese, che nell'epoca della datificazione si è intensificata a dismisura [66].

---

perative di dati, vale a dire servizi che aiutano interessati o imprese individuali, microimprese o piccole e medie imprese, che sono membri della cooperativa o che conferiscono alla cooperativa il potere di negoziare i termini e le condizioni per il trattamento dei dati prima di dare il loro consenso, a compiere scelte informate prima di acconsentire al trattamento dei dati, e che prevedono meccanismi di scambio di opinioni sulle finalità e sulle condizioni del trattamento dei dati che rappresenterebbero al meglio gli interessi degli interessati o delle persone giuridiche».

[64] Eloquente al riguardo il *considerando* n. 31 del DGA che, nel periodo finale, prevede che: «Le cooperative di dati potrebbero altresì rappresentare uno strumento utile per imprese individuali e PMI che, in termini di conoscenze in materia di condivisione dei dati, sono spesso equiparabili ai singoli individui».

[65] Al riguardo, il *considerando* n. 28 del DGA, nel definire l'attività di tale intermediario, che rimane sempre diretta a instaurare rapporti commerciali ai fini della condivisione dei dati tra un numero indeterminato di interessati e di titolari dei dati, da un lato, e gli utenti dei dati, dall'altro, contempla espressamente la possibilità che tale servizio sia offerto «anche per l'esercizio dei diritti degli interessati in relazione ai dati personali».

[66] J. VAN DIJCK, *Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology*, in *Surveillance and Society*, 2014, Vol. 12, n. 2, p. 197 ss.; M. MARTONI, *Datificazione dei nativi digitali. Una prima ricognizione e alcune brevi note sull'educazione alla cittadinanza digitale*, in *federalismi.it*, 2020, 1, p. 119 ss.

I fornitori di servizi di intermediazione dei dati di cui alla lett. *b)* dell'art 10 del DGA possono prestare i loro servizi esclusivamente a beneficio di persone fisiche, siano esse «interessati» ai sensi del GDPR che intendono mettere a disposizione i propri dati personali [67], siano esse persone fisiche che intendono mettere a disposizione dati non personali in loro possesso [68].

Ciononostante, dal testo del DGA si percepisce una spiccata propensione di questa tipologia di intermediario per l'offerta di attività di assistenza utile alla tutela dei dati a carattere personale: oltre all'inciso conclusivo della lett. *b)* ove è presente la precisazione relativa all'esercizio dei diritti degli interessati di cui al Reg. (UE) 2016/679, anche il *considerando* n. 30 identifica quale finalità di siffatti intermediari quella di «rafforzare la capacità di agire degli interessati e, in particolare, il controllo dei singoli individui in merito ai dati che li riguardano», in particolare «gestendone la concessione e la revoca del consenso al trattamento dei dati, il diritto all'accesso ai propri dati, il diritto alla rettifica dei dati personali inesatti, il diritto alla cancellazione o "diritto all'oblio", il diritto alla limitazione del trattamento e il diritto alla portabilità dei dati, che consente agli interessati di trasferire i propri dati personali da un titolare del trattamento a un altro». Attività che potrebbero essere proposte anche attraverso consulenza [69].

Similmente, l'operato delle cooperative di dati converge verso il rafforzamento della «posizione dei singoli individui, affinché compiano scelte informate prima di acconsentire all'utilizzo dei dati, influenzando i termini e le condizioni, stabiliti dalle organizzazioni di utenti dei dati» [70], dunque, sempre in ottica di un intermediario che funge da strumento tramite il quale è possibile gestire in maniera migliore le proprie informazioni in una realtà estremamente complessa [71].

Stante la comunanza dell'aspetto finalistico testé analizzato, appaiono allora due, fondamentalmente, gli elementi peculiari che contribuiscono a definire la cooperativa di dati come *species* autonoma nell'ambito degli intermediari dei dati delineati dal DGA.

---

[67] Nel definire la figura dell'interessato, l'art. 2, n. 7, del DGA rinvia all'art. 4, n. 1, del GDPR, il quale lo descrive come una «persona fisica identificata o identificabile».

[68] Rimane sempre molto acceso il dibattito dottrinale in tema di proprietà dei dati (altresì con riguardo a quelli di carattere non personale), anche se la maggioranza della dottrina sembra restia rispetto alla possibilità di introdurre una privativa in riferimento ai dati; sul punto si vedano: J. DREXL, *Legal Challenges of the Changing Role of Personal and Non-Personal Data in the Data Economy*, in *Max Planck Institute for Innovation and Competition Research Paper* No. 18-23, 2018, pp. 23-25; W. KERBER, *A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis*, in *Joint Discussion Paper Series in Economics by the Universities of Aachen, Gießen, Göttingen, Kassel, Marburg, Siegen*, No. 37-2016; T. FIA, *La tutela dei dati non personali: accesso, proprietà e regolamentazione*, in *Nuovo Notiziario Giuridico*, 2019, 1, p. 60 ss.

[69] *Considerando* n. 30 del DGA.

[70] *Considerando* n. 31 del DGA.

[71] D. POLETTI, *Gli intermediari dei dati*, in *European Journal of Privacy Law & Technologies*, 2022, 1, pp. 54-56.

Il primo concerne la forma della «struttura organizzativa» che può fornire i servizi della cooperativa di dati. In proposito, è stato correttamente notato che, in assenza di un chiaro riferimento alla forma societaria, essa può assumere una delle diverse conformazioni che l'organizzazione cooperativa può adottare nel contesto europeo [72]. A tale riguardo, risulta dirimente il principio mutualistico che connota l'attività dell'organizzazione cooperativa [73]: se già di per sé il prototipo «europeo» di intermediario di dati rappresenta una modalità di *governance* dei dati alternativa e innovativa rispetto all'esistente, la cooperativa di dati sembra allontanarsi in misura ancor più significativa dalle dinamiche capitalistiche del mercato digitale attuale [74]. In questo senso, l'inclusione delle cooperative di dati nel novero degli intermediari operata dal DGA offre una preziosa opportunità per l'affermazione di un rinnovato mutualismo [75], in un contesto, quello digitale, ove il recupero di valori fondanti per il nostro costituzionalismo come il principio solidaristico, pluralistico e di sussidiarietà hanno sino ad oggi faticato a imporsi [76].

Il secondo elemento qualificante riguarda, invece, i beneficiari delle prestazioni offerte dalla cooperativa, i quali devono cumulare contestualmente il requisito soggettivo, consistente nell'essere interessati o imprese individuali o PMI, e il requisito di appartenenza, relativo alla partecipazione alla struttura organizzativa in qualità di membro.

In definitiva, gli elementi distintivi delle cooperative di dati testé descritti lasciano intravedere, in una prospettiva che suggerisce un ritorno al costituzionalismo più tradizionale, un primo tentativo del legislatore di garantire maggiore tutela alle persone, fisiche e giuridiche, «europee», anche tramite strumenti di matrice aggregativa, dove la volontà del singolo si assomma a quella degli altri al fine di acquisire maggiore valore, senza però perdere la propria insostituibile individualità[77].

5. Osservazioni conclusive: verso un nuovo approccio nella gestione dei dati?

Le disposizioni del *Data Governance Act* dedicate alle cooperative di dati resti-

---

[72] F. Bravo, *Le cooperative di dati*, in *Contratto e impresa*, 2023, 3, pp. 3-4.

[73] L. Petrone, *Il mercato digitale europeo e le cooperative di dati*, in *Contratto e impresa*, 2023, 3, p. 12.

[74] F. Bravo, *Le cooperative di dati*, cit., pp. 7-8.

[75] Aa.Vv., *Le cooperative e le sfide dell'innovazione digitale: il neo mutualismo in dieci tesi*, documento manifesto di Legacoop e Fondazione PICO, pp. 4-6.

[76] G. Scotti, *Alla ricerca di un nuovo costituzionalismo globale e digitale: il principio di solidarietà "digitale"*, in *Forum di Quaderni Costituzionali*, 2021, 2, p. 399 ss.

[77] Sia consentito rinviare a S. Torregiani, *Il Data Act: una versione europea del Data Nationalism?*, in *Rivista italiana di informatica e diritto*, 2023, 2, p. 131 ss.

tuiscono una categoria di intermediario *sui generis*, contraddistinta da peculiarità fortemente innovative nel vasto panorama dei soggetti deputati al governo dei dati.

Fra le più importanti, va annoverata senz'altro quella che è stata definita come «*governance* duale», sintagma utilizzato per descrivere la facoltà concessa dalle cooperative di dati di consentire, contestualmente, la *governance* individuale del singolo membro sui suoi dati (personali o non personali) e la *governance* collettiva esercitata dalla cooperativa sulla base delle decisioni formatesi in seno al gruppo [78]. In tal modo si aggiungerebbe una ulteriore e nuova dimensione, quella collettiva, nel contesto del controllo delle proprie informazioni: tramite la predisposizione di una strumentazione tecnica e giuridica apposita, sarebbe possibile guadagnare quel potere di negoziazione e di influenza che il diritto dei dati europeo non è mai riuscito a garantire completamente ai singoli interessati e alle piccole imprese, neanche per mezzo dell'ingente apparato di autorità amministrative competenti nell'ambito dell'economia digitale [79].

Tale nuova dimensione sembra trovare un aggancio all'interno del DGA grazie al *considerando* n. 31, specie se raffrontato con la versione inizialmente proposta, giacché non è ora più rinvenibile il riferimento al fatto che «i diritti a norma del Reg. (UE) 2016/679 possono essere esercitati soltanto a titolo individuale e non possono essere conferiti o delegati a una cooperativa di dati» [80]. Tale emendamento permetterebbe dunque di ampliare i poteri e le facoltà della cooperativa di dati con riguardo alla possibilità di attuare una *governance* collettiva delle informazioni dei membri ad essa appartenenti [81].

Ciononostante, l'interpretazione sistematica delle disposizioni sulle cooperative di dati sembra ridimensionare questo promettente e rinnovato approccio alla gestione delle informazioni.

La collocazione all'interno della categoria degli intermediari di dati sembra imporre anche alle cooperative il rispetto delle condizioni che sono generalmente richieste a tutte le tipologie individuate dall'art. 10 del DGA, comprese quelle tese a garantire la neutralità degli intermediari. Una esegesi restrittiva del provvedimento normativo rischierebbe in tal senso di ostacolare enormemente il potenziale delle cooperative di dati le quali, pur trovandosi nella posizione migliore per accrescere il controllo degli interessati con riguardo ai propri dati, potrebbero essere costrette a ridurre il loro operato alla mera ricezione e trasmissione delle informazioni, corredata eventualmente dall'offerta di una consulenza preventiva [82].

---

[78] F. BRAVO, *Le cooperative di dati*, cit., pp. 5-6.

[79] Per un approfondimento in merito alle autorità oggi operanti, si veda S. CALZOLAIO, *Autorità indipendenti e di governo della società digitale*, in S. CALZOLAIO-A. IANNUZZI-E. LONGO-M. OROFINO-F. PIZZETTI, *La regolazione europea della società digitale*, Torino, 2024, p. 83 e ss.

[80] *Considerando* n. 24 della Proposta di DGA (COM(2020) 767 final).

[81] F. BRAVO, *Le cooperative di dati*, cit., p. 31 ss.

[82] L. PETRONE, *Il mercato digitale europeo e le cooperative di dati*, cit., p. 14.

Sarebbe stato pertanto auspicabile inserire all'interno del Regolamento una esplicita deroga all'obbligo di neutralità, quantomeno nella misura in cui lo stesso impedisce a detta tipologia di intermediari di adempiere fino in fondo alle proprie funzioni: dovrebbe essere garantito alle cooperative un margine di utilizzo più ampio dei dati conferiti dai membri, in maniera tale da assicurare maggiori benefici per tutti i partecipanti, in linea con il principio solidaristico [83]. Solo in questo modo, forzando l'interpretazione letterale o, meglio ancora, tramite una modifica normativa, le cooperative dei dati rappresenteranno uno strumento estremamente prezioso e valido per approdare verso una nuova modalità di gestione dei dati e, quando personali, verso un nuovo approccio alla tutela della *privacy* [84].

In effetti, in seno al DGA si percepisce un embrionale cambio di prospettiva consistente, fra l'altro, in una tendenza alla «mercificazione» del dato [85], il quale è ora divenuto oggetto diretto della regolazione [86].

Nello specifico, malgrado il DGA non intervenga direttamente in materia di tutela delle persone fisiche con riguardo al trattamento dei loro dati personali – in ossequio alla base giuridica prescelta (art. 114 del TFUE) e alla dichiarata prevalenza del GDPR – il complessivo modello europeo di *data governance* racchiude il potenziale per una riconsiderazione della anacronistica impostazione della normativa europea, ancora legata a concetti oramai divenuti obsoleti.

La *governance* europea ha infatti ad oggetto anche i dati personali: non viene plasmata una disciplina destinata a proteggere le persone fisiche nell'ambito del trattamento delle informazioni che le riguardano, ma viene regolata la gestione di tali informazioni in qualità di asset autonomo e slegato dall'entità cui inerisce [87]. Ci si sta allontanando da una logica eminentemente protezionistica attraverso l'ado-

---

[83] F. BRAVO, *Le cooperative di dati*, cit., p. 17.

[84] Preme in proposito osservare che all'interno del DGA sono sparsi alcuni elementi normativi che legittimerebbero una interpretazione favorevole a una deroga alla neutralità, quantomeno nella sua lettura più rigida, imposta agli intermediari. Oltre a quelle citate nell'ambito del presente lavoro, di particolare interesse sono passaggi come quello alla lett. *m*) dell'art. 12 del DGA, ove viene imposto agli intermediari che offrono servizi agli interessati (dunque, non necessariamente alle sole cooperative) di agire nell'interesse superiore di questi ultimi, prestando la propria opera non in maniera «equidistante» come vorrebbe una neutralità pura, ma curando gli interessi di una delle due parti messe in contatto.

In ogni caso, preme ribadire l'idea che specifiche previsioni eccezionali per le cooperative di dati sarebbero state quantomeno opportune.

[85] D. POLETTI, *Gli intermediari dei dati*, cit., p. 51.

[86] Tendenza che era già stata ravvisata, invero, con riguardo ai dati non personali. Sul punto, si veda il *Parere del Comitato economico e sociale europeo (CESE) sulla «Comunicazione della Commissione al Parlamento europeo e al Consiglio – Linee guida sul regolamento relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea»* adottato il 25 settembre 2019.

[87] AA.VV., *White Paper on the Data Governance Act*, cit., pp. 54-55.

zione di una strategia che, tramite meccanismi di *governance*, riesca a trarre massimo beneficio dalle potenzialità offerte dalla digitalizzazione del mercato interno senza per questo sacrificare la tutela dei dati personali [88].

Sono ormai numerose le voci che in dottrina sottolineano la fragilità del sistema di protezione dei dati oggi operante in Europa e la necessità di avviare una nuova stagione nella gestione di tali informazioni. Lo sviluppo e l'impiego massivo delle tecnologie moderne, in particolare dell'Intelligenza Artificiale, impone l'obbligo di prendere in considerazione anche l'interesse collettivo alla gestione, alla protezione e al corretto utilizzo dei dati; interesse la cui tutela può essere efficacemente esercitata da un organo esponenziale in grado di conciliare le differenti prospettive emergenti in seno alla collettività di riferimento e in grado di contrattare alla pari con chi i dati li tratta per le proprie finalità [89].

A fortiori, dunque, valgono le considerazioni suesposte in merito alla centralità della funzione che potrebbero ricoprire le cooperative di dati. Similmente a quanto accaduto tra Ottocento e Novecento quando nacquero i primi sindacati per fronteggiare una realtà nuova, oggi, innanzi a una rivoluzione epocale, potrebbe essere il momento opportuno per delegare la cura dei nostri diritti e dei nostri interessi a un apposito organismo collettivo [90].

Malgrado ciò, le istituzioni, specialmente se preposte alla tutela dei dati personali [91], rimanendo ancorate a una visione anacronistica della realtà digitale, rischiano di rallentare il processo di mutamento che il *data law* europeo deve necessariamente intraprendere in quanto, nell'epoca della datificazione [92], non è più possibile proteggere le informazioni personali in assenza di una *data governance* adeguata. Sfortunatamente si fatica ancora a cogliere il passaggio concettuale insito nell'impianto del DGA dove la *governance* dei dati, nata come costola della protezione delle informazioni a carattere personale, si amplia e diviene un corpo più grande che ingloba tutte le altre dimensioni legate al mondo dei dati, compresa la protezione di quelli personali da cui origina.

---

[88] F. BRAVO, *Le cooperative di dati*, cit., p. 22.

[89] A. MANTELERO, *Rilevanza e tutela della dimensione collettiva della protezione dei dati personali*, in *Contratto e impresa / Europa, 2015*, 1, pp 137 ss.

[90] T. HARDJONO-A. PENTLAND, *Data Cooperatives: Towards a Foundation for Decentralized Personal Data Management,* in *MIT Connection Science, 2019*, pp. 10-11.

[91] Si vedano, in proposito, le critiche mosse in EDPB-EDPS, *Parere congiunto EDPB-EDPS 03/2021 sulla proposta di regolamento del Parlamento europeo e del Consiglio relativo alla governance europea dei dati (Atto sulla governance dei dati)*, Versione 1.1, 9 giugno 2021, e in EDPB, *Dichiarazione 05/2021 relativa all'atto sulla governance dei dati alla luce degli sviluppi legislativi*, 19 maggio 2021, ove le Autorità hanno rimarcato la dogmatica superiorità della disciplina in materia di protezione dei dati personali allo scopo di ottenere una modifica, fra l'altro, della definizione di dati personali e di titolare dei dati.

[92] Per una disamina dell'impatto sul diritto costituzionale e sulle strutture sociali delle tecnologie digitali, si veda, E. LONGO, *La ricerca di un'antropologia costituzionale della società digitale*, in *Rivista italiana di informatica e diritto*, 2023, 2, p. 147 ss.

Sebbene siano maturi i tempi per avviare una transizione in tal senso, il percorso che il diritto dei dati europeo si accinge a intraprendere si rivelerà certamente lungo e tortuoso, principalmente in ragione dell'insistenza di parte delle istituzioni unionali nel rivendicare la dogmatica «superiorità» normativa del GDPR, che, se non opportunamente declinata nel contesto della *data governance*, diverrà lettera morta, mentre la protezione dei dati personali rischia di rimanere un astratto anelito normativo.

Capitolo XIII

Appunti sulla «fornitura» di dati personali e non personali nelle cooperative di dati

Giovanni Di Ciollo

Abstract: The purpose of this paper is to analyze the legal nature of the act of "provisioning" personal data in the context of data intermediation services and, in particular, data cooperatives, as governed by Regulation (EU) 2022/868, offering a unified reading of the regime of exploitation, in this matter, of personal and non-personal data.

1. Le cooperative di dati, i servizi di intermediazione di dati e i soggetti del *Data Governance Act.*

Il Regolamento (UE) 2022/868, nell'ottica di agevolare la condivisione di dati tanto tra privati, tanto tra l'amministrazione e i privati, ha provveduto a normare taluni aspetti dell'attività svolta dai fornitori di servizi di intermediazione di dati, introducendo, in particolare, la figura della cooperativa di dati [1].

[1] Cfr. F. BRAVO, *Le cooperative di dati*, in *Contratto e impresa*, 2023, 3, p. 757 ss.; L. PETRONE, *Il mercato digitale europeo e le cooperative di dati*, *ivi*, p. 800 ss. In generale, sui servizi di intermediazione dei dati, si rinvia a F. BRAVO, *Intermediazione di dati personali e servizi di* data sharing *dal GDPR al* Data Governance Act, in *Contratto e impresa Europa*, 2021, 1, p. 199 ss.; D. POLETTI, *Gli intermediari dei dati*, in *European Journal of Privacy & Law Technologies*, 2022, 1, p. 45 ss.; A. MORACE PINELLI, *Dalla* Data Protection *alla* Data Governance*: il Regolamento UE 2022/868*, in *La nuova giurisprudenza civile commentata*, 2024, 2, p. 486 ss. Sul mercato dei dati, cfr. G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, in *Rivista trimestrale di diritto pub-*

Le cooperative di dati sono definite all'art. 2, par. 1, n. 15, *Data Governance Act* (di seguito DGA) quali «servizi di intermediazione dei dati offerti da una struttura organizzativa costituita da interessati, imprese individuali o da PMI, che sono membri di tale struttura» [2]; la norma prosegue descrivendo le finalità principali perseguite da tali enti, individuando, nello specifico: (i) la prima, di più accentuata componente personalistica, consistente nello svolgimento di attività volte a coadiuvare i propri membri nell'esercizio dei loro diritti in relazione a determinati dati, anche personali, nonché svolgere attività informativa nei confronti di costoro [3]; (ii) la seconda, più spiccatamente rivolta al mercato dei dati, la quale si sostanzia nella facoltà di negoziare i termini e le condizioni per il trattamento dei dati per conto dei membri prima di concedere l'autorizzazione al trattamento dei dati non personali o prima che gli interessati diano il loro consenso al trattamento dei dati personali.

Non sembra, tuttavia, che il legislatore unionale abbia inteso tipizzare diverse categorie di cooperative di dati, essendosi limitato ad esemplificarne, piuttosto, alcune delle esplicazioni maggiormente rilevanti [4]. Una scelta di segno contrario, difatti, apparirebbe come irragionevolmente arbitraria, non ritenendosi che la finalità, perseguita dalla cooperativa, di rafforzare la posizione dei propri membri, in fase di negoziazione delle condizioni di trattamento dei dati personali e non, sia incompatibile con le attività volte ad informare o coadiuvare costoro nell'esercizio delle prerogative vantate su tali dati, e viceversa.

I servizi di intermediazione di dati sono definiti all'art. 2, par. 1, n. 11, DGA, quali servizi che mirano ad instaurare rapporti commerciali ai fini della condivisione dei dati tra un numero indeterminato di interessati e di titolari dei dati, da un lato, e gli utenti dei dati, dall'altro, anche al fine di coadiuvare gli interessati nell'esercizio dei loro diritti in relazione ai dati personali. I fornitori di servizi di intermediazione devono mantenere una posizione di neutralità rispetto ai soggetti coinvolti (interessati, titolari dei dati e utenti dei dati) [5]. Sono esclusi dalla disciplina dettata per i servizi di intermediazione i soggetti che, pur esercitando attività di intermediazione di dati, non creano un rapporto commerciale tra potenziali utenti dei dati, da un lato, e interessati e titolari dei dati, dall'altro, *ivi* nonché i soggetti che esercitano attività di intermediazione di contenuti protetti da diritto d'autore [6]. Sono del pari espressamente esclusi «servizi che ottengono dati dai titolari dei dati e li aggregano, arricchiscono o trasformano al fine di aggiungervi un valore sostan-

blico, 2022, 4, p. 971 ss.; L. LIONELLO, *La creazione del mercato europeo dei dati: sfide e prospettive*, in *Rivista del commercio internazionale*, 2021, 3, p. 675 ss.

[2] Cfr. *considerando* n. 31, di medesimo tenore.

[3] Cfr. anche *considerando* n. 30.

[4] Per una ricognizione delle diverse tipologie di cooperative di dati concepite nell'esperienza estera, anche prima di tale intervento normativo, si rinvia a F. BRAVO, *Le cooperative di dati*, cit., p. 768 ss.

[5] Cfr. *considerando* n. 33.

[6] Cfr. *considerando* n. 29.

ziale e concedono licenze per l'utilizzo dei dati risultanti agli utenti dei dati, senza instaurare un rapporto commerciale tra i titolari dei dati e gli utenti dei dati» [7], e quelli che «sono utilizzati esclusivamente da un titolare dei dati per consentire l'utilizzo dei dati detenuti da tale titolare dei dati, oppure che sono utilizzati da varie persone giuridiche all'interno di un gruppo chiuso» [8].

Per i servizi di intermediazione di dati non è prevista una specifica veste giuridica, limitandosi il regolamento a menzionare «una struttura organizzativa costituita da interessati, imprese individuali o da PMI» [9]; similmente, non è sancita a monte una forma per la cooperativa di dati, benché sia stato osservato dai primi commentatori della normativa che «la "società cooperativa" – nelle diverse declinazioni che può assumere – sia il soggetto fisiologicamente chiamato a ricoprire il ruolo di "cooperativa di dati", quantomeno nel nostro ordinamento e in quello europeo» [10].

Nel testo normativo sono introdotte nuove figure. Ci si riferisce, innanzitutto, al "titolare dei dati", definito, al n. 8 dell'art. *de quo*, come la persona fisica o giuridica, diversa dall'interessato, titolare del diritto a concedere l'accesso o condividere dati personali o non personali. Vi è poi l'"utente dei dati", definito al n. 9 come la persona fisica o giuridica che ha accesso legittimo a dati personali e non, ed è titolare del diritto di utilizzare tali dati a fini commerciali o non commerciali.

È interessante osservare la diversità dell'approccio definitorio tra il GDPR e il DGA [11]. L'interessato, a norma dell'art. 4, par. 1, n. 1, GDPR, è individuato nella persona fisica identificata o identificabile cui si riferisce una data informazione, denominata "dato personale". Di contro, il titolare dei dati è definito quale il soggetto, diverso dall'interessato, titolare del diritto di compiere determinate attività (condivisione e fornitura dell'accesso) nei riguardi di informazioni: si osserva che l'elencazione delle attività che qualificano un soggetto quale titolare dei dati appare tutt'altro che esauriente, essendo opportuno integrarle, in virtù del rinvio operato dall'art. 2, par. 1, n. 12, DGA, con la definizione di trattamento contenuta nell'art. 3, par. 1, n. 2, Reg. (UE) 2018/1807, la quale non si discosta da quella offerta dal GDPR in relazione ai dati personali. Si rileva, inoltre, la totale diversità tra la figura del titolare del trattamento, individuato nel soggetto che predispone le finalità e i mezzi del trattamento di dati personali (art. 1, par. 1, n. 7, GDPR) e l'utente dei dati (art. 2, par. 1, n. 9, DGA), il quale è il soggetto che «ha accesso legittimo a determinati dati personali o non personale e che ha diritto anche a norma del regolamento (UE) 2016/679 in caso di dati personali, a utilizzare tali dati a fini commerciali o

---

[7] Ne deriva, dunque, l'inapplicabilità della normativa ai grandi operatori del mercato digitale che raccolgono, aggregano e trasformano i dati per poi sfruttarli economicamente, anche concedendoli in licenza a soggetti terzi, cfr. A. MORACE PINELLI, *Dalla* Data Protection *alla* Data Governance, cit., p. 493.

[8] *Considerando* n. 28.

[9] Cfr. art. 2, par. 1, n. 15, DGA.

[10] Cfr. F. BRAVO, *Le cooperative di dati*, cit., p. 760.

[11] Per un'analisi delle diverse sfumature semantiche tra la versione inglese e italiana del testo del regolamento, cfr. F. BRAVO, *Intermediazione di dati personali*, cit., p. 202 ss.

non commerciali». Le figure delineate dal DGA possono sovrapporsi con quelle del GDPR: il titolare dei dati può essere anche il titolare del trattamento, nelle ipotesi in cui a quest'ultimo sia concesso condividere o fornire l'accesso (a terzi utenti dei dati) ai dati personali già raccolti presso l'interessato sulla base delle condizioni di liceità del trattamento che di volta in volta vengono in rilievo; del pari, il titolare del trattamento può coincidere con l'utente dei dati, nei casi in cui a costui sia concesso l'uso dei dati per finalità commerciali e non commerciali.

Orbene, dal costante accostamento, nel testo del DGA, degli interessati e dei titolari dei dati, appare di tutta evidenza la volontà del legislatore unionale di trattare unitariamente un fenomeno che involge soggetti titolari di situazioni giuridiche radicalmente differenti, nonché latori di interessi di natura profondamente diversa. Difatti, il corpo normativo oggetto di disamina – a differenza del GDPR – è volto a disciplinare un fenomeno di rilievo primariamente economico, stante la definizione summenzionata di servizio di intermediazione, il quale richiede l'instaurazione di un rapporto commerciale tra titolari dei dati e interessati, da un lato, e utenti dei dati, dall'altro [12]. Tanto, peraltro, non è escluso neanche per quei servizi di intermediazione volti ad agevolare gli interessati nell'esercizio dei diritti loro attribuiti dal GDPR, per i quali, rimarca il *considerando* n. 30 del DGA, «è importante che il modello commerciale di tali fornitori garantisca che non vi siano incentivi disallineati che incoraggino i singoli individui a utilizzare tali servizi per mettere a disposizione più dati che li riguardano di quanto non sia nel loro stesso interesse».

Senz'altro, tale intervento normativo si inserisce nella nuova *stagione* [13] dello studio del diritto alla tutela dei dati personali, incentrato per lo più sul fenomeno dello sfruttamento economico di tali entità [14] e, più in genere, delle informazioni, in virtù della loro sempre crescente rilevanza nei traffici economici.

2. Il diritto alla tutela dei dati personali tra persona e mercato.

Leggendo il Reg. (UE) n. 679/2016, si ha la chiara impressione che la posizione di centralità, nella normativa, sia occupata dalla persona – l'interessato – in luogo

[12] Cfr. *considerando* n. 28 del DGA.

[13] I riferimenti sono rispettivamente a G. ALPA, *Le stagioni del contratto*, Bologna, 2012, pp. 34-35 e V. RICCIUTO, *L'equivoco della* privacy, Napoli, 2022, pp. 12-13, il quale, riprendendo le riflessioni espresse da Giovanni Battista Ferri in ID., *Le stagioni del contratto e le idee di Guido Alpa*, in *Riv. dir. comm.*, 2013, 2, p. 205 ss., sottolinea l'importanza di una disamina degli istituti in chiave storica e diacronica, così approcciando la disamina dell'avvicendamento dei concetti di riservatezza, *privacy*, autodeterminazione informativa, tutela dei dati personali, in una prospettiva evolutiva che tenga conto dei cambiamenti socio-economici che, parallelamente, hanno accompagnato il diverso intendimento di tali concetti giuridici.

[14] Sul tema la letteratura è copiosissima. Si segnalano, in particolare, i seguenti recenti volumi: F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Milano, 2018; N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, 2019.

dei dati personali, nonostante la stessa si professi, per definizione legislativa, come posta *a tutela dei dati personali*. È del resto stato osservato che oggetto di tutela della normativa sia l'individuo, sebbene questa sia mediata dalla protezione dei suoi attributi, ovverosia i dati personali, trattati alla stregua di estrinsecazione della persona [15].

Tale concezione si evince, in primo luogo, dal fatto che la normativa – già dalla direttiva 95/46/CE – è sbilanciata in favore dell'interessato, del tutto omettendo di analizzare qualsivoglia sua condotta che possa, anche in astratto, essere lesiva di interessi del titolare del trattamento, stante l'asimmetria strutturale che connota la posizione dell'interessato, ben più debole rispetto al titolare del trattamento. Eloquente, in tal senso, la formulazione dell'art. 82 GDPR, il quale, al primo paragrafo, enuncia i regimi di responsabilità del titolare e del responsabile del trattamento, senza alcun riferimento a forme di responsabilità dell'interessato. Ulteriore esempio dello sbilanciamento nella formulazione delle norme, come volte a garantire esclusivamente l'interessato, si rinviene nella formulazione dell'art. 5, par. 1, lett. *a*), il quale recita: «I dati personali trattati in modo lecito, corretto e trasparente *nei confronti dell'interessato*»; il tenore letterale della disposizione porta a chiedersi se i principi menzionati – in particolare quello di correttezza – debbano essere applicati a tutti i soggetti coinvolti nelle attività di trattamento, ovvero esclusivamente nei confronti degli autorizzati, responsabili e titolari del trattamento [16].

Oltre allo sbilanciamento a livello positivo, ha contribuito a rafforzare l'idea della normativa *privacy* come normativa posta a tutela della persona una confusione dogmatica tra il diritto alla tutela dei dati personali, il diritto alla riservatezza e il diritto all'identità personale [17]. Ancor prima della Direttiva 95/46/CE, difatti, il dibattito dottrinale era andato a identificare nella *privacy*, intesa come riservatezza, il mezzo per eccellenza per tutelare e, di converso, realizzare, la personalità dell'individuo [18]. Tale convincimento, del resto, è stato rafforzato dall'espresso richiamo,

---

[15] G. ALPA, *La «proprietà» dei dati personali*, in N. ZORZI GALGANO, *Persona e mercato dei dati*, cit., p. 16; similmente, S. RODOTÀ, *Conclusioni*, in *Trattamento dei dati e tutela della persona*, Milano, 1998, p. 295.

[16] Sul tema, sia consentito rinviare a G. DI CIOLLO, *Il principio di correttezza*, in F. BRAVO (a cura di), *Dati personali. Protezione, libera circolazione e governance – 1. Principi*, Pisa, 2023, p. 121 ss.

[17] Per una ricognizione dell'evoluzione dell'approccio alla riservatezza in relazione alla tutela dei dati personali, cfr. V. RICCIUTO, *L'equivoco della* privacy, cit., p. 18 ss.; V. CUFFARO, *Il diritto europeo sul trattamento dei dati personali e la sua applicazione in Italia: elementi per un bilancio ventennale*, in V. CUFFARO-R. D'ORAZIO-V. RICCIUTO, *I dati personali nel diritto europeo*, Torino, 2019, p. 3 ss.

[18] Cfr. V. RICCIUTO, *L'equivoco della* privacy, cit., p. 31; G.B. FERRI, *Persona e privacy*, in *Persona e formalismo giuridico. Saggi di diritto civile*, Rimini, 1987, p. 274 ss. Sul tema, cfr. R. PARDOLESI, *Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e discontinuità*, in ID. (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003, p. 1 ss.; S. NIGER, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Padova, 2006, *passim*; F. BRAVO, *Il "diritto" a trattare i dati personali nello svolgimento dell'attività economica*, Milano, 2018, p. 13 ss.

da parte dell'art. 1, l. 31 dicembre 1996, n. 675, alla tutela della *riservatezza* e dell'*identità personale*, il quale ha contribuito a delineare «un quadro confuso e, in buona sostanza, superato già dal riconoscimento, in termini assai chiari e definiti, dei "nuovi" diritti della personalità (riservatezza ed identità personale) da parte della giurisprudenza e della dottrina» [19]. Ancora oggi, del resto, l'autorità di controllo nazionale [20], quella europea [21], nonché la giurisprudenza domestica [22], tendono a concepire la tutela dei dati personali come strumento per attuare la tutela della persona e, in particolare, il diritto alla riservatezza. Orbene, senz'altro la tutela approntata dalla normativa sulla *privacy* si presta, nel concreto, ad essere lo strumento privilegiato e più efficace per tutelare la riservatezza di colui che la ritenga violata. Tuttavia, Il testo del GDPR, di particolare analiticità e spiccato tecnicismo, è per lo più privo di riferimenti alla tutela morale della persona: anche alla luce dei successivi interventi normativi inerenti la dimensione patrimoniale dei dati personali, sembra opportuno rivalutare la primazia delle considerazioni valoriali e morali che sovente sono associate alla normativa sulla *privacy*.

Con l'emanazione del GDPR, il diritto alla tutela dei dati personali ha acquisito confini più definiti, quale diritto autonomo e distinto rispetto al diritto alla riservatezza e all'identità personale [23], espressamente riconosciuto dall'art. 8 della Carta

---

[19] V. RICCIUTO, *L'equivoco della* privacy, cit., p. 31. Si osserva che una parte dei commentatori ha invece sin dall'inizio sottolineato la diversità del diritto alla tutela dei dati personali rispetto al diritto alla riservatezza e all'identità personale, cfr. E. GIANNANTONIO, Commento *sub* art. 1, in E. GIANNANTONIO-M.G. LOSANO-V. ZENO ZENCOVICH (a cura di), *La tutela dei dati personali. Commentario alla legge n. 675/1996*, Padova, 1997, pp. 5-6; v. pure, ID., *Responsabilità civile e trattamento dei dati personali*, in *Dir. inf.*, 1999, 6, p. 1036.

[20] Il richiamo alla tutela del diritto alla riservatezza o all'identità personale è presente in modo diffuso nella produzione provvedimentale dell'autorità (cfr., *ex multis*, GPDP, *Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o per scopi di ricerca storica*; ID., Provv. 7 marzo 2024, in *https://garanteprivacy.it*, doc. *web* n. 10007098). Significativo che, in occasione del conferimento al presidente dell'autorità, prof. Pasquale Stanzione, del premio "Dekra Safety Award 2021", il relativo comunicato stampa pubblicato sul sito del garante reciti: «Un riconoscimento per l'impegno dell'Autorità da lui presieduta nella tutela del diritto alla riservatezza dei cittadini», cfr. GPDP, Provv. 19 novembre 2021, *ivi*, doc. *web* n. 9720604.

[21] EDPS, *Opinion 4/2017*, punto 17, nel quale i traffici economici aventi ad oggetto i dati personali sono, ad avviso di chi scrive inopportunamente, paragonati al traffico di organi umani.

[22] Cfr., *ex multis*, Cass. civ., sez. I, ord. 13 dicembre 2021, n. 39531, nella cui parte motiva si discorre, relativamente alla situazione giuridica scaturente dalla normativa *privacy*, come di "diritto alla riservatezza".

[23] Il riferimento a tale diritto era, di contro, assente tanto nella l. n. 675/1996, tanto nella Direttiva n. 46/95/CE. Quanto al termine "*privacy*", codesto, nel discorso giuridico italiano, ormai si riferisce all'insieme di norme poste a tutela dei dati personali, e non può più essere semplicemente accostato alla nozione di "riservatezza"; sul tema, cfr. V. RICCIUTO, *L'equivoco della privacy*, pp. 24 ss.; V. CUFFARO, *Il diritto europeo sul trattamento dei dati personali e la sua applicazione in Italia*, cit., p. 4 ss.; P. TANDA, *I nuovi orizzonti della nozione di* privacy *e la patrimonializzazione dei dati personali da parte dei* social network, in *Diritto e processo amministrativo*, 2020, 3, p. 736 ss.; G. PINO, *Giudizi*

dei diritti fondamentali dell'Unione europea, e che – senz'altro legato ad altri – occupa un vertice autonomo nel prisma dei diritti della personalità; come più approfonditamente esposto nel paragrafo che segue, tale diritto si connota di una marcata rilevanza sul piano economico, che, ulteriormente, lo distingue dal diritto alla riservatezza e all'identità personale, elaborati in seno alla teorica dei diritti della personalità [24], i quali, tradizionalmente, mal si conciliano con considerazioni di ordine patrimoniale.

Anche i dati personali, tuttavia, sono considerati attributi immateriali della persona [25] e la loro disciplina è da ricondurre nell'alveo dei diritti della personalità [26], che intrinsecamente attribuisce rilievo privilegiato, nel fenomeno giuridico in oggetto, che pur coinvolge multipli soggetti, alla posizione del titolare del diritto in parola; e ciò in quanto tale categoria di diritti sembra porsi – quale proiezione dei più alti valori della persona costituzionalmente riconosciuti [27] – su un piano superio-

---

di valore e dottrine civilistiche. Il caso dei diritti della personalità, in *Diritto & questioni pubbliche*, 2022, 2, pp. 133-134. L'ambiguità del termine era già stata rilevata da risalente dottrina prima ancora dell'emanazione della direttiva sulla protezione dei dati personali, cfr. S. RODOTÀ, *Protezione dei dati e circolazione delle informazioni*, in *Riv. crit. dir. priv.*, 1984, p. 4.

[24] A. DE CUPIS, *I diritti della personalità*, in *Trattato dir. civ. comm.*, diretto da A. CICU e F. MESSINEO, 2ª ed., Milano, 1982, pp. 283 ss., 399 ss.

[25] Con tale espressione ci si riferisce alle manifestazioni della personalità, morali o materiali, *oggetto* dei diritti della personalità stessi, fra i quali rientrano, ad esempio, «*il nome, l'immagine, e altri elementi evocativi della dell'identità*», G. RESTA, *Autonomia privata e diritti della personalità*, Napoli, 2005, p. 4; ID., *Dignità, persone, mercati*, Torino, 2014, p. 96 ss., pp. 123-124; A. DE CUPIS, *I diritti della personalità*, in *Trattato dir. civ. comm.*, diretto da A. CICU e F. MESSINEO, 2ª ed., Milano, 1982, *passim*; V. ZENO ZENCOVICH, *I negozi sugli attributi della personalità*, in *Dir. inf.*, 1998, 4-5, p. 545 ss.

[26] Diffusamente, sul tema, si segnalano i seguenti contributi: A. DE CUPIS, *I diritti della personalità*, in A. CICU-F. MESSINEO (diretto da), *Trattato dir. civ. comm.*, 2ª ed., Milano, 1982; G. RESTA, *Autonomia privata e diritti della personalità*, cit.; V. ZENO-ZENCOVICH, voce *Personalità (diritti della)*, in *Digesto civ.*, XIII, Torino, 1995, p. 430 ss.; ID., *I diritti della personalità*, in N. LIPARI-P. RESCIGNO (diretto da), *Diritto civile*, I, *Fonti, soggetti, famiglia*, I, *Le fonti e i soggetti*, Milano, 2009, p. 496 ss.; P. RESCIGNO, voce *Personalità (diritti della)*, in *Enc. giur.*, XXIII, Roma, 1991, p. 1 ss.; D. MESSINETTI, voce *Personalità (diritti della)*, in *Enc. dir.*, XXXIII, Milano, 1983, p. 355 ss. P. VERCELLONE, voce *Personalità (diritti della)*, in *Nov. dig.it.*, XXII, Torino, 1965, p. 1083 ss.

[27] Cfr. C.M. BIANCA, *Diritto civile*, I, *La norma giuridica*, *i soggetti*, 2ª ed., Milano, 2002, p. 139 ss. Gli attributi della persona, definiti come «un *modo di essere fisico o morale della persona*», sono ritenuti, dalla dottrina tradizionale, privi di immediata rilevanza economica, per cui se ne predica la natura di diritto *non patrimoniale*, cfr. A. DE CUPIS, *I diritti della personalità*, cit., p. 51, nonché C.M. BIANCA, *op. cit.*, p. 147. Altresì, è ritenuto sussistente un obbligo gravante sulla generalità di non ledere i diritti della personalità, per cui se ne predica il carattere dell'*assolutezza*, cfr. A. DE CUPIS, *op. cit.*, pp. 51-52; similmente, C.M. BIANCA, *op. cit.*, p. 147. Alpa contesta il carattere di assolutezza del diritto alla tutela dei dati personali rilevando l'esistenza, nel Regolamento, di diverse graduazioni della tutela approntata dalla normativa a seconda della dimensione dell'impresa che tratta i dati, cfr. G. ALPA, *La «proprietà» dei dati personali*, cit., p. 16; invero, tuttavia, riflessioni analoghe possono operarsi per tutti quei diritti della personalità la cui tutela si estrinseca nella regolamentazione della circolazione e sfruttamento degli attributi che ne costituiscono proiezione, come nell'ipotesi del diritto al

re, tali da ritenerli tendenzialmente sottratti financo alla disponibilità del titolare degli stessi [28].

Ordunque, il diritto alla tutela dei dati personali ha da subito ereditato gran parte delle riflessioni svolte intorno ai diritti della personalità, in particolare, per quanto di interesse in tale scritto, quelle che tradizionalmente rifuggono la reificazione degli attributi della personalità [29] – e, come corollario, guardano con sospetto ai fenomeni economici nei quali tali siano convolti – e quelle che hanno visto in tale di-

---

riserbo delle persone note, per cui si rinvia a M. PROTO, *Il diritto e l'immagine*, Milano, 2012, p. 230 ss. L'immanenza dei diritti della personalità, rispetto alle normative che ne attuano la tutela, è stata del resto sostenuta da autorevole dottrina, secondo la quale i diritti della personalità appartengono «all'individuo in via originaria», tale per cui le norme specificamente preposte a disciplinare gli stessi si limitano ad attuare (in positivo o in negativo) una tutela già presupposta dall'ordinamento, cfr. M. GIORGIANNI, *La tutela della riservatezza*, in *Riv. trim. dir. proc. civ.*, 1970, 1, p. 20 ss. Nel secolo scorso, il dibattito sulla consistenza dei diritti della personalità è stato assai vivace e le differenti teorie (monista e pluralista; si rinvia, per una disamina delle diverse posizioni, a G. PINO, *Teorie e dottrine dei diritti della personalità. Uno studio di meta-giurisprudenza analitica*, in *Materiali per una storia della cultura giuridica*, 2003, 1, p. 255 ss.) avevano soprattutto la funzione di individuare la norma violata, a fini risarcitori, cfr. G. ALPA-G. RESTA, *Le persone e la famiglia*, 1, *Le persone fisiche e i diritti della personalità*, 2ª ed., in R. SACCO (diretto da), *Tratt. dir. civ.*, Torino, 2019, p. 274 ss. Per quanto concerne i diritti della personalità, il dibattito è ormai storicizzato, stante la rilevanza costituzionale degli stessi (cfr. D. MESSINETTI, *Personalità (diritti della)*, cit., p. 395) e la pacifica risarcibilità dei danni patrimoniali e non patrimoniali derivanti dalla lesione di interessi costituzionalmente protetti, cfr. C.M. BIANCA, *Diritto civile*, 5, *La responsabilità*, 3ª ed., Milano, 2021, p. 562 ss.

[28] Più nello specifico, dei diritti della personalità si sono storicamente predicati quattro attributi fondamentali: *intrasmissibilità*, *indisponibilità, irrinunciabilità* e *imprescrittibilità*, cfr. A. DE CUPIS, *I diritti della personalità*, cit., p. 85 ss.; V. ZENO ZENCOVICH, voce *Personalità (diritti della)*, cit., pp. 430 ss. Il connotato dell'intrasmissibilità trova la sua ragion giustificatrice nella stretta inerenza di tali diritti alla persona, intesa nella sua dimensione materiale e intellettuale. Non ritenendosi ammissibile il trasferimento dei diritti della personalità, se ne predica, più in generale, l'indisponibilità; corollario dell'indisponibilità è l'irrinunciabilità del diritto, stante la persistenza del connotato di inerenza alla persona per il solo fatto che essa esiste; speculare al tratto dell'irrinunciabilità è quello dell'imprescrittibilità dei diritti della personalità, secondo cui essi non possono estinguersi per inerzia del titolare.

Occorre osservare che, sul connotato dell'indisponibilità, plurime autorevoli voci ne hanno contemperato la portata, offrendo molteplici soluzioni che in tal sede non si possono neanche sinteticamente richiamare, limitandoci a rinviare ai contributi più rilevanti, cfr. A. DE CUPIS, *I diritti della personalità*, cit., p. 93 ss.; G. RESTA, *Autonomia privata e diritti della personalità*, cit., p. 250 ss.; G. RESTA, *Contratto e diritti fondamentali*, in G. D'AMICO (a cura di), *Contratto*, Milano, 2021, p. 299 ss.; A. NICOLUSSI, voce «*Autonomia privata e diritti della persona*», in *Enc. dir.*, *Annali*, IV, Milano, 2011, p. 137 ss.; V. ZENO ZENCOVICH, *I negozi sugli attributi della personalità*, cit., p. 545 ss.

[29] La concezione spiccatamente personalistica e valoriale dei diritti della personalità ne postula l'estraneità dal novero dei diritti *patrimoniali*; sul punto, dottrina autorevole ha rimarcato «l'inestimabilità pecuniaria dei beni interiori alla persona», cfr. A. DE CUPIS, *I diritti della personalità*, cit., p. 55. La questione assume rilievo, oltre che per i fenomeni negoziali inerenti ai diritti della personalità, anche in relazione ai profili successori dei diritti della personalità, per cui si rinvia a G. RESTA, *L'oggetto della successione: I diritti della personalità*, in G. BONILINI (diretto da), *Trattato di diritto delle successioni e donazioni*, I, *La successione ereditaria*, Milano, 2009, p. 729 ss.

ritto ulteriore misura volta a garantire l'inviolabilità morale della persona.

Tuttavia, è stato rilevato in dottrina come l'idea dell'inconciliabilità dei rapporti patrimoniali con i diritti della personalità sia priva di adeguato riscontro fattuale e non condivisibile sul piano dogmatico [30], tanto che gli sforzi di risolvere le aporie derivanti dall'indubbia «patrimonializzazione» dei diritti della personalità, più che fare lumi sul fenomeno, hanno disvelato la fragilità dell'assunto di partenza; di conseguenza, è stato affermato che la "componente patrimoniale", suscettibile di sfruttamento economico [31], dei diritti della personalità, faccia intrinsecamente parte di codesti [32].

Ciò non di meno, in un contesto così eterogeneo, appare prudente resistere alla tentazione di estendere automaticamente alla materia della tutela dei dati personali conclusioni già tratte nell'ambito di altri diritti della personalità, tenendo a mente che la più autorevole dottrina, nello studio degli aspetti successori dei diritti della personalità, ha ammonito sulla configurabilità di ricostruzioni tanto valide quanto tra loro incompatibili, ritenendo di non trascurare l'eventualità che per diversi diritti della personalità valgano soluzioni differenti [33].

3. Dall'interessato al dato personale.

Dagli interventi normativi in materia *privacy* successivi all'emanazione del GDPR, si evince l'attenzione del legislatore europeo non più orientata (in via principale) alla tutela della debole posizione dell'interessato – o, ancor di più, della di lui personalità morale – bensì rivolta al dato personale stesso e alla regolamentazione delle vicende inerenti alla sua *circolazione*, con un approccio apparentemente agnostico rispetto a considerazioni di ordine valoriale che hanno strenuamente caratterizzato – e in parte continuano a caratterizzare – il dibattito sulla tutela dei dati personali.

Occorre però evidenziare che tale prospettiva non costituisce un *novum* di recente conio. Già l'art. 1, par. 2, direttiva 95/46/CE, sanciva il principio di libera circolazione dei dati personali, il quale non poteva essere compresso per motivi connessi alla tutela dei diritti e delle libertà fondamentali delle persone fisiche; significativa-

---

[30] Cfr. G. RESTA, *Autonomia privata e diritti della personalità*, cit., p. 241 ss.

[31] Cfr. G. RESTA, *Autonomia privata e diritti della personalità*, cit., p. 260 ss.; v. pure V. ZENO-ZENCOVICH, *Profili negoziali degli attributi della personalità*, in *Dir. inf.*, 1993, 4-5, p. 549. L'ambito dove la disponibilità a titolo oneroso è più lampante è quello del diritto allo sfruttamento economico dell'icona personale, per cui si rinvia a M. PROTO, *Il diritto e l'immagine*, cit., p. 98 ss.

[32] Cfr. V. RICCIUTO, *I dati personali come oggetto di operazione economica. La lettura del fenomeno nella prospettiva del contratto e del mercato*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati*, cit., p. 104 ss., in particolare nota a piè di pagina n. 14.

[33] A. ZACCARIA, *Diritti extrapatrimoniali e successione. Dall'unità al pluralismo nelle trasmissioni per causa di morte*, Padova, 1988, p. 13.

mente, tuttavia, tale inciso non è apparso nel recepimento domestico di tale direttiva [34], concorrendo a mettere in sordina il discorso sulla rilevanza economica di tale fenomeno. Il principio, oggi contenuto nell'art. 1, par. 3, GDPR, acquisisce rinnovato e privilegiato rilievo, essendo volto a valorizzare il dato personale, nel contesto del mercato europeo, come entità suscettibile di essere proficuamente coinvolto in operazioni di rilievo economico e commerciale [35].

Un importante intervento normativo, sul punto, si rinviene nella direttiva 2019/770/UE la quale, recepita con il d.lgs. 4 novembre 2021, n. 173, ha previsto espressamente all'art. 3, par. 1, confluito nell'art. 135-*octies*, co. 4, c. cons., l'ipotesi di somministrazione di servizi o contenuti digitali a fronte della «fornitura» di dati personali all'operatore economico, il quale è autorizzato a trattarli per fini diversi dalla mera prestazione del servizio [36].

Del pari, il *Data Governance Act*, presuppone, alla base del funzionamento dei servizi di intermediazione di dati, l'attività di "condivisione", definita all'art. 2, par. 1, n. 10, quale «la *fornitura di dati* da un interessato o un titolare dei dati a un utente dei dati ai fini dell'utilizzo congiunto o individuale di tali dati, sulla base di accordi volontari o del diritto dell'Unione o nazionale, direttamente o tramite un intermediario, ad esempio nel quadro di licenze aperte o commerciali, dietro compenso o a titolo gratuito».

Le normative in commento menzionano l'attività di *fornitura* di dati personali, senza tuttavia qualificarla giuridicamente, e lasciando intendere la centralità, a tal fine, del consenso al trattamento dei dati personali. Deve tuttavia menzionarsi che le recenti riforme hanno riaperto il dibattito sulla natura giuridica del consenso al

---

[34] Cfr. V. RICCIUTO, *I dati personali come oggetto di operazione economica*, cit., p. 105 ss.

[35] Come del resto espressamente previsto dal *considerando* n. 9 del GDPR, il quale valorizza il principio di libera circolazione dei dati personali all'interno dell'Unione proprio alla luce delle attività economiche connesse al trattamento dei dati che potrebbero risentire da misure volte a limitare la circolazione dei dati. Cfr., sul punto, V. RICCIUTO, *L'equivoco della privacy*, cit., p. 48 ss. Sul rapporto tra tutela dei dati personali e libera circolazione dei dati, è stato rimarcato in dottrina che il primo di tali diritti subisce il contemperamento con altri diritti fondamentali di pari rango, in conformità con il principio di proporzionalità; sul punto, diffusamente, si richiamano S. RODOTÀ, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Riv. crit. dir. priv.*, 1997, p. 583 ss.; G. ALPA, *La normativa sui dati personali. Modelli di lettura e problemi esegetici*, in *Dir. inf.*, 1997, 4-5, p. 718 ss.; F. BRAVO, *Il "diritto" a trattare i dati personali nello svolgimento dell'attività economica*, cit., p. 10 ss.; V. RICCIUTO, *L'equivoco della privacy*, cit., p. 50 ss.; E. TOSI, *Circolazione dei dati personali tra contratto e responsabilità*, Milano, 2023, p. 79 ss.

[36] Per un estensivo commento del recepimento, cfr. S. PAGLIANTINI, *L'attuazione minimalista della dir. 2019/770/UE: riflessioni sugli artt. 135* octies-*135* vicies ter *c.cons. La nuova disciplina dei contratti b-to-c per la fornitura di contenuti e servizi digitali*, in *Le nuove leggi civili commentate*, 2022, 6, p. 1499 ss.; v. pure V. VERSACI, *Il valore negoziale dei dati personali del consumatore: spigolature sul recepimento della direttiva 2019/770/UE in una prospettiva comparata*, in E. CREMONA-F. LAVIOLA-V. PAGNANELLI (a cura di), *Il valore economico dei dati personali tra diritto pubblico e diritto privato*, Torino, 2022, p. 155 ss.

trattamento dei dati personali [37], del quale appare opportuno ripercorrere i punti salienti.

4. La natura del consenso al trattamento dei dati personali.

Sulla natura del consenso hanno riscosso particolare favore due tesi, seppur sostenute con sfumature diverse.

Una tesi, sulla scorta dell'indubbia rilevanza economica del dato personale, e dell'alterità tra il diritto alla riservatezza e il diritto alla tutela dei dati personali, attribuisce al consenso natura dispositiva-negoziale, tramite il quale i dati personali, reificati in entità dotate di propria oggettività e qualificabili come beni giuridici, sono immessi in circolazione e possono divenire oggetto di prestazioni a titolo oneroso [38], secondo schemi, anche contrattuali, compatibili con la normativa *privacy* [39].

Un'altra tesi [40], attribuisce al consenso valore di atto autorizzatorio, in quanto vol-

---

[37] Per una ricognizione delle diverse posizioni, cfr. S. MAZZAMUTO, *Il principio del consenso e il problema della revoca*, cit., p. 1021 ss.; F. BRAVO, *Il "diritto" a trattare i dati personali nello svolgimento dell'attività economica*, cit., p. 15 ss., in particolare note a piè di pagina nn. 19-20; più in generale, nell'ambito dei diritti della personalità, cfr. G. RESTA, *Autonomia privata e diritti della personalità*, cit., p. 250 ss.

[38] V. ZENO-ZENCOVICH, *Una lettura comparatistica della L. 675/1996 sul trattamento dei dati personali*, in V. CUFFARO-V. RICCIUTO-V. ZENO-ZENCOVICH (a cura di), *Trattamento dei dati e tutela della persona*, cit., p. 168 ss.; *ivi* pure G. OPPO, *Sul consenso dell'interessato*, p. 123 ss. e V. CUFFARO, *A proposito del ruolo del consenso*, p. 121; v. pure V. ZENO-ZENCOVICH, voce *Cosa*, in *Dig. civ.*, IV, Torino, 1989, p. 438 ss.; ID., voce *Informazione (profili civilistici)*, in *Digesto civ.*, IX, Torino, 1993, p. 421 ss.; ID., *Sull'informazione come "bene" (e sul metodo del dibattito giuridico)*, in *Riv. crit. dir. priv.*, 1999, p. 485 ss.; A. DE FRANCESCHI, *La circolazione dei dati personali tra privacy e contratto*, Napoli, 2017, p. 68 ss. Nello specifico, è tracciato un parallelismo tale per cui i dati personali si pongono, rispetto alla persona, così come la singola immagine si pone rispetto al ritratto: «E come il rapporto fra soggetto e suo ritratto può atteggiarsi in svariati modi (sotto forma di uno *ius arcendi*, sotto forma di una privativa, oggetto di una obbligazione, di indifferenza giuridica), considerazioni non dissimili sembrano potersi estendere ai dati personali», V. ZENO-ZENCOVICH, *Una lettura comparatistica della L. 675/1996*, cit., p. 168.

[39] Secondo gli esponenti che più autorevolmente hanno sostenuto tale ricostruzione, il paradigma contrattuale emerge quando l'attività di trattamento è coinvolta in un rapporto sinallagmatico di carattere patrimoniale, cfr. V. ZENO-ZENCOVICH, *Una lettura comparatistica della L. 675/1996*, cit., p. 168 ss.; V. RICCIUTO, *L'equivoco della privacy*, cit., p. 153 ss. È stato rilevato che l'atto dispositivo presenta, quantomeno in astratto, gli elementi strutturali del contratto, cfr. G. OPPO, *Sul consenso dell'interessato*, cit., p. 123, mentre alcuni autori si sono spinti a qualificare in termini squisitamente contrattuali anche la mera attività di trattamento a fronte della prestazione del consenso, pur qualificando il fenomeno *de quo* come lecita intrusione nella sfera giuridica dell'interessato e non atto traslativo di diritti sul dato, cfr. F. BILOTTA, *Consenso e condizioni generali di contratto*, in V. CUFFARO-V. RICCIUTO (a cura di), *Il trattamento dei dati personali*, II, *Profili applicativi*, Torino, 1999, p. 89 ss.

[40] Cfr. D. MESSINETTI, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *Riv. crit. dir. priv.*, 1998, p. 350 ss.; S. PATTI, Commento *sub* art. 23, in C.M. BIANCA-F.D. BUSNELLI (a cura di), *Commentario al d.lgs. 30 giugno 2003, n. 196 ("Codice della* privacy*")*, in *I*

to ad elidere il divieto preesistente al trattamento dei dati personali del soggetto, e in quanto tale inidoneo a realizzare una vicenda dispositiva-traslativa; una volta venuto meno l'obbligo di astensione, riconosce tuttavia al consenso ha altresì la funzione di determinare i perimetri della fattispecie circolatoria [41].

Quest'ultima ricostruzione appare la più persuasiva. Difatti, tra le situazioni giuridiche di cui l'interessato è titolare, ai sensi del GDPR, non sembra esservi la facoltà di disporre direttamente dei dati personali in favore di un altro soggetto. Tale facoltà, difatti, presupporrebbe una relazione di appartenenza in termini proprietari tra il dato personale e l'interessato che, tuttavia, non si rinviene. Difatti, la conformazione della normativa *privacy*, rende evidente che in capo al titolare del trattamento fa capo la *preesistente* facoltà di trattare i dati personali conformemente alle condizioni di liceità previste [42]; in particolare, il consenso, dunque, si configura come «ostacolo» che

---

libri de Le nuove leggi civili commentate, Padova, 2007, p. 553; E. GIANNANTONIO, *Trattamento di dati e responsabilità civile*, cit., p. 1036-1037; A. DI MAJO, *Il trattamento dei dati personali tra diritto sostanziale e modelli di tutela*, in V. CUFFARO-V. RICCIUTO-V. ZENO-ZENCOVICH (a cura di), *Trattamento dei dati e tutela della persona*, cit., pp. 230-231; F. BRAVO, *Lo "scambio di dati personali" nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto*, in *Contratto e impresa*, 2019, 1, p. 34 ss.; ID., *Le condizioni di liceità del trattamento di dati personali*, in G. FINOCCHIARO (a cura di), *Protezione dei dati personali in Italia, Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018*, Bologna, 2019, p. 140 ss.; C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, Torino, 2021, p. 74 ss. Similmente, più in generale sui diritti della personalità, A. DE CUPIS, *I diritti della personalità*, cit., p. 93 ss. Diversa questione, estranea allo scopo del presente scritto, se il consenso autorizzatorio a sua volta sia qualificabile come negozio giuridico o atto giuridico in senso stretto, per cui si rinvia a S. PATTI, *op. cit.*, p. 554, nota a piè di p. n. 339.

[41] Cfr. D. MESSINETTI, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, cit., p. 352. È stato correttamente osservato che, nella prassi, il consenso come dispositivo "negoziale" svolge una funzione assai limitata, stante la conformazione del consenso, nei traffici giuridici, in termini *adesivi*, sulla base di finalità, modalità e caratteristiche del trattamento stabilite unilateralmente dal titolare del trattamento, cfr. F. BRAVO, *Il "diritto" a trattare i dati nello svolgimento dell'attività economica*, cit., pp. 17-18; in termini analoghi, S. PATTI, Commento *sub* art. 23, cit., p. 554 ss.

[42] Cfr. F. BRAVO, *Il "diritto" a trattare i dati nello svolgimento dell'attività economica*, cit., p. 51 ss. Tale prospettiva, dunque, pur attribuendo al consenso efficacia autorizzatoria, non qualifica l'attività di trattamento come intrinsecamente illecita (in senso opposto, ponendo l'accendo sulla funzione della normativa quale strumento volto a impedire l'indebita altrui ingerenza nella sfera personale, cfr. D. MESSINETTI, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, cit., p. 346; S. PATTI, Commento *sub* art. 23, cit., p. 553). Del resto, nell'odierna conformazione della disciplina *privacy*, il consenso ha perduto la sua posizione di centralità, essendo oggi solo una tra le diverse ed equipollenti condizioni di liceità del trattamento (cfr. F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, cit., p. 130 ss.); di conseguenza, appare inopportuno un paragone del consenso al trattamento dei dati personale al consenso dell'avente diritto di cui all'art. 50 c.p., valorizzato da alcuni commentatori, in quanto il primo, a differenza del secondo, non si pone come unica – o, tra le altre, privilegiata – tecnica per rendere lecita la "violazione" della sfera della persona: l'esistenza di molteplici condizioni di liceità del trattamento, congiuntamente al riconoscimento del principio di libera circolazione dei dati, priva l'attività di trattamento dello stigma di riprovevolezza e antigiuridicità che di contro si attaglia alle condotte di rilievo penale scriminate dall'art. 50 c.p. In generale, sul tema, v. F. BRAVO, *Il "diritto" a trattare i dati nello svolgimento dell'attività economica*, cit., p. 57 ss.

l'ordinamento pone al fine di meglio contemperare l'interesse al trattamento e sfruttamento dei dati personali da parte del titolare del trattamento con le esigenze di autodeterminazione informativa dell'interessato [43]. In tali termini, il consenso non ha effetti traslativi del diritto alla tutela dei personali (inteso nella sua facoltà di disposizione *ivi* ipotizzata) che, dunque, si affievolisce in capo all'interessato venendosi a costituire, di contro, in capo al titolare del trattamento, speculari situazioni giuridiche relativamente ai dati dell'interessato [44]; la sua funzione si limita nel rendere lecita l'attività di trattamento che, per talune fattispecie, il legislatore ha ritenuto subordinare al controllo preventivo dell'interessato [45].

Né, del pari, possono trarsi altre conseguenze analizzando la struttura dei diritti dell'interessato che, in diversa misura, si rivolgono *direttamente* ai dati personali, suggerendo l'esistenza di una situazione giuridica che possa attribuite poteri *immediati* di disposizione degli stessi. Nello specifico, tali diritti si pongono come misure di reazione [46] volte a conformare le attività di trattamento al volere dell'interessato, nei limiti in cui tale facoltà gli è attribuita dalla normativa e non costituiscono, di contro, strumenti volti a *creare* fattispecie di circolazione dei dati personali; difatti, gli stessi *presuppongono* un'esistente attività di trattamento [47] che, invece, sarebbe assente nell'ipotesi del consenso quale puro atto dispositivo: in tal caso, il trattamento sarebbe *conseguenza* della prestazione del consenso; la diversità strutturale e teleologica dei diritti dell'interessato rispetto all'ipotizzato atto di disposizione mediante consenso non consente, dunque, di tracciare utili parallelismi.

Preso atto dall'impossibilità di rinvenire, nella normativa sulla *privacy*, norme attributive di situazioni giuridiche di appartenenza sui dati personali in capo all'interessato [48], appare irrilevante porsi la questione sui confini della disponibilità si sif-

---

[43] Cfr. F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, cit., pp. 141-142.

[44] Cfr. G. RESTA, *Revoca del consenso ed interesse al trattamento nella legge sulla protezione dei dati personali*, in *Riv. crit. dir. priv.*, 2000, 2, p. 307.

[45] Cfr. F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, p. 142 ss. Tale ricostruzione si oppone a quella che, invece, tende a costruire il rapporto tra interessato e dato personale in termini di appartenenza, cfr., sul tema, F. CAFAGGI, *Qualche appunto su circolazione, appartenenza e riappropriazione dei dati personali*, in *Danno e resp.*, 1998, 7, p. 613 ss.

[46] Cfr. D. MESSINETTI, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, cit., p. 346, il quale identifica nei diritti dell'interessato il potere di reazione a fronte della violazione del comando giuridico di astensione, di cui rimarca il carattere obiettivo; nello specifico, discendendo tale obbligo da una norma qualificata imperativa, lo stesso esprime la sua cogenza anche nei confronti del soggetto stesso (D. MESSINETTI, voce «*Personalità (diritti della)*», cit., pp. 361-362); cogenza che verrebbe bene con la prestazione del consenso, il quale fa decadere il divieto di astensione (cfr. D. MESSINETTI, *op. ult. cit.*, pp. 403-404).

[47] Cfr. F. BRAVO, *Il "diritto" a trattare i dati nello svolgimento dell'attività economica*, cit., p. 54 ss.

[48] Di converso, nella disamina della posizione del titolare del trattamento, è stato rimarcato che non sia configurabile neanche in capo a costui una situazione di «titolarità» sui dati trattati, e che il "diritto" a trattare i dati consiste nel diritto a porre in essere «operazioni» sugli stessi, cfr. F. BRAVO, *Il "diritto" a trattare i dati nello svolgimento dell'attività economica*, cit., p. 109.

fatto ipotizzato diritto, se suscettibile di essere coinvolto in vicende meramente obbligatorie o reali.

5. La «fornitura» di dati personali e non personali: fattispecie strutturalmente diverse ovvero in rapporto di specialità?

La dottrina a sostegno della tesi del consenso quale atto autorizzatorio ha specificato che rilievo patrimoniale può essere attribuito, nei fenomeni negoziali *de quibus* ove si assiste a "scambi" di dati personali, non ai dati stessi, bensì all'atto autorizzatorio al trattamento [49].

L'affermazione appare coerente con l'impianto argomentativo appena ricostruito, nella quale il dato personale non è *direttamente* oggetto di fenomeni di patrimonializzazione.

Sia tuttavia consentita una riflessione di ordine fattuale.

Solitamente, essendo posto l'accento sull'attività compiuta dal titolare del trattamento sui dati, si descrive la prima delle attività che lo connotano con il termine

---

[49] Cfr. F. BRAVO, *Il commercio elettronico dei dati personali*, T. PASQUINO-A. RIZZO-M. TESCARO (a cura di), *Questioni attuali in tema di commercio elettronico*, Napoli, 2020, pp. 118-119; ID., *Lo "scambio di dati personali"*, cit., p. 34 ss.; C. IRTI, *Consenso "negoziato"*, cit., p. 90 ss. Una volta ricostruita in tali termini la natura del consenso, si è posto il problema della sua qualificazione in seno al rapporto contrattuale. Secondo autorevole dottrina, non può configurarsi la patrimonializzazione del consenso autorizzatorio, in quanto lo stesso si pone, in termini di scansione logica della fattispecie, su un piano antecedente rispetto all'accordo contrattuale, dacché, invertendo la scansione dei due momenti, il consenso andrebbe a configurarsi quale oggetto di obbligazione, in aperto contrasto con il requisito di libertà e incoercibilità del consenso, cfr. G. RESTA, *I dati personali oggetto del contratto. Riflessioni sul coordinamento tra la Direttiva (UE) 2019/770 e il Regolamento (UE) 2016/679*, in A. D'ANGELO-V. ROPPO (diretto da), *Annuario del contratto*, 2018, p. 145. Sulla scorta di tale ricostruzione, Irti ha qualificato la manifestazione del consenso autorizzatorio quale "prestazione" cui è subordinata la promessa contrattuale di offerta di servizi o contenuti digitali, ricondotta allo schema dell'art. 1333 c.c., cfr. C. IRTI, *op. cit.*, p. 102 ss. Scettico, nei confronti di tale ricostruzione, V. RICCIUTO, *L'equivoco della privacy*, cit., p. 144 ss., il quale, assumendo una prospettiva di consenso quale atto dispositivo inseribile *a pieno titolo* in un contesto contrattuale, negando che la manifestazione del consenso, una volta convenuta quale controprestazione, cessi di essere libera. È stato del resto osservato che l'art. 7 GDPR, impone di tenere conto, ai fini della valutazione della libertà della manifestazione del consenso, della circostanza che l'esecuzione di un contratto sia condizionata alla prestazione del consenso, senza però inserire un vero e proprio divieto, (cfr. A. DE FRANCESCHI, *La circolazione dei dati personali*, cit., p. 74). Per un'approfondita disamina sulla questione e ulteriori ipotesi ricostruttive, cfr. C. ANGIOLINI, *Lo statuto dei dati personali. Uno studio a partire dalla nozione di bene*, Torino, 2020, p. 208 ss. Su un diverso piano, anche a voler ammettere la configurabilità della manifestazione del consenso quale oggetto dell'obbligazione, non è chiaro se per lo stesso possa predicarsi il carattere di patrimonialità di cui all'art. 1174 c.c. Se tale questione non si pone in una visione del consenso quale atto dispositivo di diritti (anche) di natura patrimoniale, il connotato della patrimonialità non sembra di contro rinvenirsi, quanto meno con medesimo nitore, nel consenso quale atto autorizzatorio: al contrario, come si vedrà, la rilevanza patrimoniale potrebbe attribuirsi ai dati personali stessi, sebbene non nell'accezione comunemente intesa.

"raccolta", anche se – salvo i casi in cui il titolare sia già nella disponibilità degli stessi – i dati raccolti sono, in effetti, stati previamente comunicati dall'interessato al titolare del trattamento.

Dunque, l'uso dell'espressione «fornitura di dati» [50], sposta la prospettiva dal lato dell'interessato, il cui ruolo, come si è detto, giuridicamente sembrerebbe limitarsi a quello di acconsentire al trattamento. Oltre a ovvie considerazioni sul fatto che tale cambio di registro linguistico è indice di una maggior attenzione, da parte del legislatore, nei confronti del dato personale in sé, appare opportuno fare delle osservazioni in punto di diritto e sondare se, effettivamente, il ruolo l'interessato si limita ad una passiva attività autorizzatoria, oppure involge altro.

In sede di studio delle interferenze tra il fenomeno successorio [51] e il regime di circolazione dei dati personali dopo la morte dell'interessato, è stato precisato che l'appartenenza di una *res*, anche immateriale, all'asse ereditario deve essere saggiata esclusivamente sulla scorta della configurabilità, su di essa, di diritti di natura patrimoniale; a tal proposito, si è ritenuto che nella normativa sulla *privacy* non fossero rinvenibili diritti di natura patrimoniale sui dati personali e che, dunque, l'esistenza o meno di informazioni di carattere personale nel bene immateriale-informazionale, non ha altra conseguenza che far soggiacere tale bene *anche* alla disciplina sulla *privacy*, la quale, come visto, attribuisce all'interessato facoltà limitate di controllo su quelle informazioni qualificabili come dati personali.

In tal modo, si verifica una stratificazione di regimi giuridici che, invece che escludersi a vicenda, concorrono a determinare i perimetri di uso e circolazione di determinate entità.

Ordunque, così come in ambito successorio la qualificabilità o meno di una *res* immateriale, anche meramente informazionale, come dato personale, nulla dice sulla sua appartenenza all'asse ereditario, sembrerebbe che medesime conclusioni possano trarsi per la «fornitura» di dati personali: la normativa sulla *privacy* è ricondotta, dunque, a cornice regolatoria di un fenomeno di rilevanza strettamente *personale* e, per ciò, inidonea a individuare compiutamente il regime di circolazione, anche nei traffici commerciali delle informazioni qualificabili come dati personali.

In breve, esiste il diritto alla tutela dei dati personali, che si esplica negli strumenti approntati dalla normativa sulla *privacy*, ma non sembra per questo sussistere un generico diritto *sui* propri dati personali, che ne consenta il diretto coinvolgimento in fenomeni contrattuali da parte del titolare di tale diritto: al più, occorrerà sondare la configurabilità di diritti, più in generale, sulle informazioni.

Il DGA non qualifica in termini giuridici né la fornitura di dati personali, né la fornitura di dati non personali, benché, pur adoperando terminologie diverse, sovente pone tali attività sullo stesso piano. Sarebbe erroneo, a parere di chi scrive, fermarsi

---

[50] In inglese «*provision of data*», tanto nel DGA, tanto nella Direttiva (UE) 2019/770.

[51] Cfr. G. Di Ciollo, *Il trattamento dei dati personali delle persone decedute. Note in ambito successorio*, in *Ciberspazio e diritto*, 2020, 3, p. 528 ss.

alla diversità terminologica tra interessato e titolare dei dati, tra consenso al trattamento dei dati personali e autorizzazione al trattamento dei dati non personali, per affermare, in modo definitivo, la diversità strutturale delle fattispecie in questione.

Al contrario, proprio il fatto che le fattispecie sono trattate in modo tendenzialmente omogeneo – ferme le peculiarità proprie della normativa sulla *privacy* che si concretizzano, ad esempio, in servizi di intermediazione volti a coadiuvare gli interessati nell'esercizio dei propri diritti – appare opportuno ricostruire il fenomeno negoziale *de quo* in termini tendenzialmente unitari.

Ordunque, occorrerebbe, a livello sistematico, ricostruire la disciplina riguardante l'intermediazione di *informazioni*, applicabile a tutti i servizi di intermediazione di dati e, solo in un secondo momento, sondare le differenze sul regime circolatorio di quelle informazioni qualificabili come dati personali. Indicazioni in tal senso possono del resto ricavarsi dall'art. 2, par. 2, Direttiva (UE) 2018/1807 sulla libera circolazione dei dati non personali nell'unione europea, il quale specifica: «Qualora i dati personali e non personali all'interno di un insieme di dati siano indissolubilmente legati, il presente regolamento lascia impregiudicata l'applicazione del regolamento (UE) 2016/679».

Non essendo possibile, in tal sede, ricostruire il regime di circolazione dei dati non personali [52], può tuttavia evidenziarsi che la fattispecie della fornitura di dati personali nelle cooperative di dati – e in generale, nei rapporti di rilevanza economica consistenti nella «fornitura» di dati personali – si delinea come una fattispecie complessa che involge da un lato un fenomeno contrattuale, eventualmente di natura dispositiva, inerente le informazioni – uniforme per dati personali e dati non personali – e il consenso al trattamento dei dati personali come *quid pluris* necessario per rendere lecita la circolazione di informazioni qualificabili come dati personali.

In dottrina è stato osservato che, nelle ipotesi di fornitura di dati in un contesto contrattuale si attribuirebbe al cessionario una «licenza d'uso» dei dati personali stessi [53]. Tale tesi presuppone la configurabilità di una situazione giuridica soggettiva sui dati personali; pur ammettendo siffatta eventualità, tale situazione giuridica non potrebbe scaturire dalla normativa sulla *privacy* e andrebbe rinvenuta altrove: la medesima, si ipotizza, dalla quale si fa discendere il «diritto» al trattamento dei dati non personali. Qualora, di contro, si dovesse ritenere che nessuna forma di reificazione sia configurabile sulle informazioni, allora l'atto di fornitura di dati personali va a coincidere con la prestazione del consenso autorizzatorio, cui si accompagna, pattiziamente, l'obbligazione di mero *facere* consistente nel rendere disponibili al titolare del trattamento tali dati.

---

[52] Per osservazioni sul punto cfr. F. BRAVO, *Intermediazione di dati personali*, cit., p. 241; più approfonditamente, sul tema, cfr. A. VIGORITO, *I dati non personali: modelli di attribuzione e circolazione*, in *Riv. crit. dir. priv.*, 2020, 3, p. 369 ss.

[53] Cfr. C. ALVISI, *Dati personali e diritti dei consumatori*, in V. CUFFARO-R. D'ORAZIO-V. RICCIUTO, *I dati personali nel diritto europeo*, Torino, 2019, p. 675; in toni dubitativi, F. BRAVO, *Il commercio elettronico dei dati personali*, cit., p. 118.

6. Differenze tra «consenso» e «autorizzazione».

Si è delineata una proposta ricostruttiva che scinde il conferimento di informazioni – atto di primaria rilevanza patrimoniale nel fenomeno negoziale in oggetto – e la necessità, per le informazioni qualificabili come dati personali, del coinvolgimento del consenso al trattamento dei dati personali, nello schema negoziale ai fini del perfezionamento della fattispecie di fornitura di dati.

L'uso, da parte del DGA, dei termini «consenso» e «autorizzazione», rispettivamente per i dati personali e non personali, suggerirebbe che medesime considerazioni debbano trarsi in merito alla natura dell'atto di autorizzazione. Sebbene un approfondimento sul conferimento di dati non personali appare essere la sede più opportuna per la disamina della natura giuridica di tale atto, possono comunque svolgersi utili considerazioni dal raffronto dello stesso con il consenso al trattamento dei dati personali.

Mentre codesto ultimo atto è volto a sollevare il limite legalmente posto per il trattamento di date informazioni e non vi si riconosce attitudine dispositiva sui dati personali, non sembra rinvenirsi, nell'ordinamento, un preesistente limite al trattamento di dati non personali; né tale limite può ricavarsi *a contrario* dalla definizione di «autorizzazione» [54], la quale si identifica nell'atto di «conferimento agli utenti dei dati del diritto al trattamento dei dati non personali» [55]. Non soffermandoci troppo sulla diversità lessicale tra la formulazione dell'atto di autorizzazione quale atto di «conferimento di diritti» – implicante una vicenda dispositiva del diritto al trattamento dei dati non personali per il quale apparirebbe prima opportuno sondarne il perimetro di configurabilità– e il consenso quale atto di «assenso (...) che i dati personali che lo riguardano siano oggetto di trattamento» [56], si evidenzia che essere titolari del «diritto» a trattare dati non personali non implica necessariamente l'esistenza di un diritto di controllo esclusivo di tali informazioni che si atteggi in termini analoghi al consenso al trattamento dei dati personali.

In assenza di siffatto regime di controllo esclusivo configurabile in capo al titolare di dati non personali, appare chiara la diversità tra consenso e autorizzazione. Non potendo l'autorizzazione al trattamento dei dati non personali atteggiarsi quale atto *stricto sensu* autorizzatorio, nell'accezione *supra* data al consenso al trattamento dei dati personali, ovverosia di atto volto ad elidere un limite legale al trattamento di dati non personali, lo stesso va sostanzialmente a coincidere con l'elemento dell'accordo contrattuale in cui si esplica la vicenda dispositiva inerente ai dati non personali [57], coincidenza che, invece, non si è ritenuta configurabile in relazione alla fornitura di dati personali.

---

[54] Art. 2, par. 1, n. 6, DGA.

[55] Art. 2, par. 1, n. 6, DGA.

[56] Art. 4, par. 1, n. 1, GDPR.

[57] Tanto nel caso la vicenda dispositiva consista nel trasferimento o la costituzione di diritti di uti-

7. Le cooperative di dati tra delega di diritti e conferimento di dati.

Nel testo della proposta di Regolamento della Commissione era prevista, per le cooperative di dati, il divieto di «delega» o «conferimento» dei diritti dell'interessato a cooperative di dati, rimarcando che gli stessi fossero esercitabili solo «a livello individuale» [58]. L'inciso è scomparso nel testo definitivo del Regolamento, il cui *considerando* n. 31 ora recita «i diritti a norma del Regolamento (UE) 2016/679 sono diritti personali dell'interessato e che quest'ultimo non può rinunziarvi».

È stato dunque osservato che «mentre il divieto della rinunzia, quale tipico atto abdicativo, implichi l'impossibilità del conferimento in società (atto con efficacia reale), esso non preclude invece la stipula di un contratto di mandato (con rappresentanza), in quanto atto con mera efficacia obbligatoria» [59].

Occorre chiedersi se anche il consenso sia atto delegabile. Alcuni hanno opinato in senso negativo adducendo, da un lato, che le cooperative di dati svolgono un ruolo di rilevanza commerciale limitato, in ambito *privacy*, principalmente volto a coadiuvare gli interessati nelle attività prodromiche alla manifestazione del consenso o a trasmettere a terzi la manifestazione di volontà di costoro e, dall'altro, la natura del consenso al trattamento dei dati personali quale atto personalissimo non delegabile [60]. Altrove, si è osservato che il consenso non costituisce atto personalissimo [61], che il limite alla delegabilità dei diritti derivanti dal GDPR alle cooperative di dati, originariamente previsto dal *considerando* n. 24 della Proposta di Regolamento sulla *Governance* europea dei dati, è venuto meno nel testo definitivo, pur essendo ribadita la non conferibilità, in termini "reali", dei diritti scaturenti dal GDPR e che, in ogni caso, era già ammessa, tanto nella prassi quanto per espresso riconoscimento normativo, la delega per l'esercizio dei diritti dell'interes-

---

lizzazione delle informazioni, tanto nel caso il contratto in questione non preveda diritti di uso delle informazioni ma si risolva nella mera messa a disposizione delle informazioni. Tale ultima ipotesi postula l'inconfigurabilità di diritti sulle informazioni, fuori dai casi espressamente previsti dalla legge quali, ad esempio, le privative industriali; di conseguenza, non si potrebbe discorrere, secondo tale ricostruzione, di atto dispositivo – ovverosia di atto di trasferimento o costituzione di diritti – delle informazioni, se non in senso atecnico, non essendo a monte configurabile un diritto su codeste entità. Tale ricostruzione, tuttavia, sembra porsi in contrasto con la definizione di «autorizzazione» offerta dal DGA la quale sembra implicare – tracciando un parallelismo con la funzione che il consenso svolge in ambito *privacy* – un limite giuridico all'uso dei dati personali non personali detenuti da un soggetto; del pari, il «titolare dei dati» è colui che vanta diritti, a norma dell'art. 2, par. 1, n. 8, DGA, sui dati non personali: di contro, ove non si ritenessero configurabili diritti sui dati non personali, titolare dei dati è colui che, meramente, ne ha la materiale disponibilità.

[58] *Considerando* n. 24; cfr. F. BRAVO, *Intermediazione di dati personali*, cit., pp. 244-245.

[59] G. RESTA, *Pubblico, privato e collettivo nel sistema europeo di governo dei dati*, cit., p. 993.

[60] Cfr. G. RESTA, *op. ult. cit.*, pp. 993-994, il quale mostra perplessità nei confronti dell'impostazione adottata dal DGA.

[61] Essendo previsto che, per i minori d'età, il consenso sia manifestato dai genitori, cfr. F. BRAVO, *Intermediazione di dati personali*, cit., p. 245; ID., *Le cooperative di dati*, cit., p. 793.

sato [62]. Ci limitiamo ad osservare che apparirebbe più coerente con l'impianto del DGA ammettere, in linea di principio, la delegabilità del consenso e, specularmente, del potere di revoca dello stesso, posto che le esigenze di controllo preventivo che sono ricondotte a tale atto sembrerebbero frustrate dalla pacifica delegabilità, tra gli altri, del diritto di accesso o alla portabilità dei dati i quali, come dimostrato dalla prassi [63], sono idonei a spostare ingenti masse di dati personali verso il delegato o anche verso altri titolari (che abbiano una base giuridica legittimante il trattamento). Tale controllo dunque si sostanzierebbe non nell'esclusione della facoltà di delega, ma nella negoziazione di termini di delega specifici, oltre che nella libera recedibilità da tale pattuizione, stante l'irrinunziabilità delle posizioni giuridiche che hanno origine dal GDPR. Del resto, è stato condivisibilmente rimarcato in dottrina che la dimostrata fragilità – nella realtà dei traffici economici – di un potere di controllo *individuale* nei confronti dei propri dati, rende particolarmente opportuna la previsione, introdotta dal DGA, di una forma di controllo *collettivo* sulla circolazione dei dati dei membri, esercitato dall'intermediario [64].

È stato evidenziato che «La logica stessa di una compagine con scopo mutualistico suggerirebbe l'opportunità di riconoscere un conferimento dei dati con correlativi poteri dispositivi in capo alla società» [65]. Come si è visto, tuttavia, non è possibile offrire una risposta a tale interrogativo guardando esclusivamente alla normativa *privacy*, essendo necessario prima sondare *tout court* il regime di circolazione delle informazioni. Qualora sia ammessa la possibilità di conferire informazioni in una cooperativa di dati, dovrà necessariamente ammettersi, in linea di principio, anche la possibilità di conferire quelle informazioni qualificabili come dati personali [66], ferma, in ogni caso, l'applicabilità della normativa *privacy*, la cui interferenza (ad esempio, tramite revoca del consenso che si accompagna all'atto di conferimento) può ben essere idonea a svuotare di contenuto l'atto di conferimento, con conseguenza sul regolamento contrattuale in cui tale consenso è inserito [67].

---

[62] Cfr. F. BRAVO, *Le cooperative di dati*, cit., p. 791 ss.

[63] Ci si riferisce al modello commerciale adottato dall'azienda *Weople*, la quale, beneficiaria di delega all'esercizio dei diritti dell'interessato, richiede poi a molti esercenti di servizi in linea copia dei dati ai sensi dell'art. 20 GDPR. Si rinvia, per un esame più approfondito, a F. BRAVO, *Intermediazione di dati personali*, cit., p. 215 ss.

[64] Cfr. F. BRAVO, *Le cooperative di dati*, cit., p. 784 ss.

[65] G. RESTA, *Pubblico, privato e collettivo nel sistema europeo di governo dei dati*, cit., p. 993.

[66] Nonostante, secondo la ricostruzione proposta, non sia configurabile in capo all'interessato un diritto esclusivo allo sfruttamento economico dei propri dati personali, si osserva che, più in generale, sono note all'ordinamento ipotesi di conferimento di diritti derivati di sfruttamento di attributi della personalità, cfr. G. RESTA, *Autonomia privata e diritti della personalità*, cit., p. 340, in nota.

[67] In generale, sulla conformazione di contratti in cui è convenuto il consenso quale controprestazione, v. G. VERSACI, *Il valore negoziale dei dati personali del consumatore: spigolature sul recepimento della direttiva 2019/770/UE in una prospettiva comparata*, in *Riv. dir. priv.*, 2022, 2, p. 207 ss. Sulla configurabilità di conferimento in società di diritti sugli attributi della personalità, v. G. RESTA, *Autonomia privata e diritti della personalità*, cit., p. 323 ss., in particolare nota a piè di pagina n. 185.

Concepire le cooperative di dati come organizzazioni che operano esclusivamente sulla base della delega all'esercizio di diritti, non appare del tutto soddisfacente se non per quelle il cui oggetto sociale è offrire servizi nei confronti degli interessati; al contrario, per quelle il cui oggetto sociale consta in uno sfruttamento, anche in termini economici, delle informazioni riferite alla persona, attribuire rilevanza immediata all'informazione, nella vicenda negoziale, sembrerebbe la soluzione più appropriata. Ammessa la configurabilità dello schema negoziale complesso descritto per i dati personali, la remunerazione del contributo mutualistico ben potrebbe avvenire tramite l'istituto dei ristorni di cui all'art. 2545-*sexies* c.c., strumento di remunerazione dei soci per i conferimenti effettuati alla cooperativa.

8. Riflessioni conclusive.

È evidente che gli ultimi interventi normativi a livello europeo hanno inteso attribuire un maggior ruolo ai dati personali quali entità oggetto di sfruttamento economico di pregnante rilevanza.

In assenza di indicazioni positive sul regime di circolazione delle informazioni, la dottrina più risalente ha cercato di spiegare i fenomeni che implicano un grado di oggettivazione dei dati personali guardando esclusivamente alla normativa *privacy* o, al più, traendo spunti dal diritto industriale e dallo studio sullo sfruttamento economico degli attributi della personalità.

Tuttavia è oggi palese l'inadeguatezza di tale normativa, da sola, a fornire una soddisfacente giustificazione giuridica ai fenomeni *de quibus*: al contrario, il moltiplicarsi degli interventi normativi relativi ai dati non personali offre l'occasione per rileggere il fenomeno della fornitura di dati personali e non personali in chiave unitaria. In tale ottica, la normativa *privacy* è restituita alla sua originaria area di appartenenza, ovverosia quella di normativa volta a regolare gli aspetti prevalentemente *personalistici* del trattamento dei dati personali: le aporie che tanto adontano la dottrina, più che da un'incompatibilità ontologica tra dimensione patrimoniale e diritti della personalità, sembrano germinare dall'inadeguatezza della lente scelta ai fini dell'osservazione del fenomeno della patrimonializzazione dei dati personali. Al contrario, una ricostruzione del regime di sfruttamento delle informazioni che tenga conto dei recenti interventi normativi può consentire di spiegare più efficacemente anche i fenomeni negoziali in cui sono coinvolti i dati personali.

Capitolo XIV

Cooperative di dati e *data evaluation*

Francesco Checcacci-Louis Botros[*]

Abstract: The evolution of digital technologies has generated an increasing amount of data and greater complexity in their management and use, as well as new ways of generating value for organizations that hold and come into possession of them. Data cooperatives, by promoting resource sharing, can offer an innovative approach to managing and enhancing data among the various entities participating in the project. This article aims to focus on the identification and evaluation of data as the main asset and the profitability derived from their management. Through a literature review and analysis of a case study, the paper highlights the methodologies and tools for data evaluation.

1. Introduzione.

In un'epoca caratterizzata dalla digitalizzazione e dall'espansione delle tecnologie dell'informazione, i dati sono diventati una risorsa cruciale e un asset fondamentale per le aziende in tutti i settori. Considerati come il «nuovo petrolio» [1], i dati hanno acquisito un valore significativo non solo come strumento per l'innovazione e la competitività, ma anche come merce con un proprio mercato specifico. In questo contesto, diventa necessario per le aziende e tutti gli *stakeholder* trattare i dati non più solo come una risorsa operativa, ma come veri e propri asset.

In aggiunta, rimane cruciale considerare la crescente importanza che i dati assumono nell'ambito del machine learning come risorsa per il training degli algo-

[*] I singoli paragrafi del presente scritto sono da attribuire, congiuntamente, ad entrambi gli autori.

[1] C. ARTHUR, *Tech giants may be huge, but nothing matches big data*, in *The Guardian*, 2013.

ritmi. In tale contesto il valore generato non deriva dal dato stesso, quanto più dalle informazioni che emergono dal trattamento congiunto dei dati. Quanto detto è coerente con l'opinione di alcuni autori Reilly e Schweihs che evidenziano «l'informazione, nella sua forma più basilare, è qualcosa che può essere consumato dalle persone e fornisce intuizioni su uno o più argomenti». Di conseguenza il valore attribuito ad un dato dipende dai benefici generati dall'utilizzo dell'informazione stessa, diventa quindi rilevante «differenziare tra informazione che possiede/non possiede valore» [2].

In tale contesto, il concetto di valore del dato assume un ruolo ancora più rilevante per le cooperative di dati, concepite come ecosistema collaborativo in cui diverse entità forniscono i propri dati, mettendoli a fattore comune, per il beneficio collettivo. La necessità di attribuire un valore economico-monetario al dato, sia per valorizzare il singolo contributo sia per valorizzare l'insieme complessivo dei dati, è una delle principali sfide che emerge dalle caratteristiche distintive di queste entità. Il presente elaborato, pertanto, ha la finalità di illustrare i diversi approcci valutativi che possono essere applicati nella stima del valore economico attribuibile al dato.

Entrando nello specifico, attraverso una revisione della letteratura esistente, si analizzeranno le varie tecniche di valutazione utilizzate sulla base delle specifiche caratteristiche e il contesto di utilizzo dei dati. Questo studio mira a fornire una comprensione approfondita di come questi diversi approcci possano essere applicati per quantificare il valore dei dati, sottolineando al contempo i rispettivi punti di forza e le sfide. In aggiunta, il documento esplorerà un caso pratico che illustra l'applicazione di queste metodologie di valutazione in un contesto reale, dimostrando l'importanza pratica e le implicazioni di una corretta valutazione dei dati.

In conclusione, questo lavoro mira a contribuire significativamente al dibattito accademico e professionale sulla valutazione dei dati, suggerendo direzioni future per la ricerca e la prassi in questo campo in rapida evoluzione.

2. *Review* della letteratura.

2.1. Le cooperative di dati.

La cooperativa dei dati si basa sulla collaborazione volontaria tra individui che uniscono i dati da loro acquisiti a vantaggio dei membri del gruppo o della comunità. La ragione che giustifica la volontà collaborativa dei soci consiste nel plusvalore derivante dall'utilizzo congiunto dei dati in un unico pool. La funzione principale della cooperativa dei dati si concretizza nel garantire ai suoi membri il possesso e il controllo dei propri dati personali, offrendo loro in cambio il servizio di raccol-

[2] R.F. REILLY-R. P. SCHWEIHS, *Valuing intangible assets*, McGraw Hill Professional, 1998.

ta, gestione e protezione dei dati attraverso il proprio archivio personale o all'interno della cooperativa stessa [3].

Uno degli aspetti chiave della governance dei dati e della relazione tra le cooperative di dati e i loro membri sta nel come vengono raccolti, memorizzati e analizzati i dati personali e non personali; infatti, mentre alcune cooperative desiderano garantire ai propri membri il controllo totale dei dati conferiti, altre cooperative creano un pool di dati in cui questi vengono resi anonimi e aggregati. La finalità di una cooperativa di dati risiede nella possibilità di ottenere benefici (quali ad esempio un risparmio di costi) correlati all'aggregazione e all'elaborazione condivisa dei dati disponibili. Tuttavia, non tutte le cooperative perseguono gli obiettivi economici e di monetizzazione, alcune tipologie di cooperative sono interessate ad utilizzare i dati per il bene comune, ad esempio, donandoli per la ricerca. Altre cooperative, invece, sono organizzate in modo da consentire ai propri membri di monetizzare individualmente i dati [4], permettendo di utilizzare l'insieme dei dati per poter offrire sul mercato prodotti a maggior valore aggiunto [5].

In tale contesto il concetto di valore del dato ha un ruolo fondamentale per lo sviluppo delle cooperative di dati. La cooperativa di dati si forma grazie all'aggregazione dei dati a seguito del "conferimento" degli stessi da parte dei soci iscritti. Ne consegue pertanto comprendere bene, prima di entrare nel merito dei possibili metodi di valutazione da adottare, definire alcune caratteristiche indispensabili per poter dire che il dato ha valore.

Una prima caratteristica da analizzare è il volume dei dati. Una prima interpretazione potrebbe vedere la qualità di un aggregato di dati come direttamente proporzionale alla loro massa. Nonostante la ratio dietro a tale scelta possa sembrare sensata, tale interpretazione non tiene conto della presenza di potenziali repliche di dati al suo interno, che ne causerebbero una diluzione, riducendone, pertanto, il valore.

Una seconda caratteristica è la diversità e la ricchezza di elementi che compongono il dato, in particolare da più elementi è composto il dato, maggiori saranno le informazioni che si potranno costruire tramite la combinazione di questi dati. Inoltre, dati con più elementi diversi tra loro hanno maggior probabilità di essere utili allo scopo della cooperativa.

Il dato è considerabile come un bene intangibile, ovvero, come discusso ampiamente nella letteratura scientifica attuale, i dati presentano caratteristiche comuni con le tecnologie, con i brevetti e con altre forme di asset intangibili.

Così come i brevetti, anche i dati possono essere oggetto di diritti di utilizzazione economica ad essi collegati, che possono essere ceduti o acquistati. Come le

---

[3] T. HARDJONO-A. PENTLAND, MIT *Connection Science Data Cooperatives: Towards a Foundation for Decentralized Personal Data Management*, 2019.

[4] E. BIETTI-A. ETXEBERRIA-M. MANNAN, J. WONG, *Data Cooperatives in Europe: A Legal and Empirical Investigation*, 2021.

[5] S. GIRISH-M. AVERY, *Data cooperative: Enabling meaningful collective negotiation of data rights for communities* (December 1, 2022), in SSRN, disponibile online all'url https://ssrn.com/abstract=4414473.

tecnologie, possono invece essere ceduti in licenza a più soggetti. Il fattore che differenzia il dato dagli altri *asset* intangibili è la loro produzione poiché i dati non sono creati in laboratorio, ma sono spesso generati automaticamente, come sottoprodotto dell'attività economica [6]. Anche se lo stoccaggio e l'analisi dei dati possono essere costosi, la loro produzione di solito non lo è.

Un bene intangibile è valorizzabile quando presenta le seguenti caratteristiche: *a*) identificabilità; *b*) controllo; *c*) possibilità di generare benefici economici futuri.

Un bene intangibile soddisfa il criterio di identificabilità nella definizione dell'attività immateriale quando: (i) è separabile, ossia capace di essere separata o scorporata dall'entità e venduta, trasferita, data in licenza, locata o scambiata, sia individualmente che insieme al relativo contratto, attività o passività; oppure (ii) deriva da diritti contrattuali o altri diritti legali indipendentemente dal fatto che tali diritti siano trasferibili o separabili dall'entità o da altri diritti e obbligazioni.

Una entità legale ha il controllo di un bene intangibile se ha il potere di usufruire dei benefici economici futuri derivanti dalla risorsa in oggetto e può, inoltre, limitare l'accesso a tali benefici da parte di terzi.

La capacità dell'entità di controllare i benefici economici futuri derivanti da un'attività immateriale trae origine, in genere, da diritti legali tutelabili in sede giudiziale. I benefici economici futuri derivanti da un'attività immateriale possono includere: *a*) i proventi originati dalla vendita di prodotti o servizi; *b*) i risparmi di costo; *c*) altri benefici derivanti dall'utilizzo dell'attività da parte della società.

In letteratura viene ampiamente discusso come il valore generato dai dati non derivi dal dato preso singolarmente, quanto più dall'insieme di dati o *dataset*, in cui quest'ultimo si inserisce. In questo contesto, è utile presentare la nozione di «*Shapley Value*» [7], che nasce dalla teoria dei giochi cooperativi e viene frequentemente applicata nell'ambito dell'analisi dei dati. Nello specifico, si tratta di una metrica che permette di assegnare un valore a ciascun dato presente all'interno di un dataset, evidenziando il contributo di ciascuno di essi allo specifico fine perseguito. L'ampia adozione di questo metodo di valutazione dei dati trova fondamento nella sua applicabilità come schema di allocazione del profitto generato dall'intero *dataset* sul singolo dato. Nonostante il calcolo dello *Shapley Value* fornisca numerosi vantaggi, non sempre il suo calcolo è di facile esecuzione, specialmente all'aumentare della dimensione del *dataset* [8].

Nella valutazione dei dati è fondamentale quindi considerare le loro proprietà, tra cui la commerciabilità. A questo proposito, Nash afferma che i dati sono «*non-rival*», poiché possono essere consumati simultaneamente da più parti [9]. La non rivalità dei dati è un aspetto che rende complessa la loro valutazione. Farboodi e

---

[6] L. VELDKAMP, *Valuing Data as an Asset*, in *Review of Finance*, 2023, pp. 1545-1562.

[7] A. GHORBANI-J. ZOU, *Data Shapley: Equitable Valuation of Data for Machine Learning.*

[8] R. JIA *et. al*., *towards Efficient Data Valuation Based on the Shapley Value*.

[9] KIM S. NASH, *CIOs Consider Putting a Price Tag on Data*, Springer, 2014.

Veldkamp affermano su questo tema che se l'acquirente paga un prezzo P per ogni unità di dati acquistati, il venditore guadagnerà un valore maggiore di P per ogni unità di dati ceduti, poiché concede all'acquirente di possedere i dati ma non in esclusività dato che ne rimane ancora proprietario [10].

I dati possono essere considerati un bene «intermedio» poiché grazie alla loro proprietà, potenzialmente, le società riescono a creare valore attraverso l'utilizzo di altri *asset* (i.e. il ruolo dei dati può essere quello di permettere alle aziende di scegliere tecniche di produzione migliori), o più semplicemente i dati possono acquisire valore se combinati con altri dati, in quanto una volta aggregati generano informazioni aventi varie possibilità di utilizzo.

Altra considerazione rilevante che viene spesso sottolineata in letteratura da diversi autori, tra cui Adams e Gounardes [11] è la libertà attraverso la quale i dati sono generati e scambiati. In particolare, viene portato alla luce il processo attraverso il quale dati personali sensibili, dati demografici, finanziari, sanitari, dati relativi alle attività, dati di consumo vengano forniti gratuitamente alle aziende dagli individui. Pertanto, la discussione sui pro e contro dell'uso aziendale dei dati forniti liberamente, è in una fase di evoluzione.

Anche la titolarità dei dati è un concetto molto discusso in fase di evoluzione. Alcune località, come l'Unione Europea e il Regno Unito, hanno approvato leggi sul diritto d'autore delle banche dati [12].

Un ulteriore aspetto che risulta essenziale menzionare nell'ambito della valutazione dei dati consiste nella perdita di valore degli stessi. Infatti, per attribuire un valore preciso ad ogni singolo dato, è fondamentale in primis determinarne la vita utile. A tal proposito Maryam Farboodi e Laura Veldkamp sostengono che «il tasso di ammortamento dei dati è determinato specificamente dalla persistenza e dalla volatilità dell'ambiente in cui i dati vengono impiegati per effettuare previsioni» [13]. Affermano cioè che il tasso di ammortamento è differente rispetto al contesto. Per cui, ad esempio, i dati relativi al flusso degli ordini di una azienda, che sono altamente volatili, avranno un tasso di deprezzamento diverso rispetto ai dati sui codici postali dei clienti, che persistono per anni. Oltre a variare in base al contesto di riferimento, secondo Choi i piani di ammortamento dei dati, dovrebbero riflettere la volatilità dei flussi finanziari attesi da quest'ultimi. A titolo esemplificativo, i dati i cui benefit attesi risultano più volatili, dovranno essere ammortizzati più veloce-

---

[10] M. FARBOODY-L. VELDKAMP, *A Model of the data economy*, in *National Bureau of economic research*, 2021.

[11] E. ADAMS-A. GOUNARDES, *A tax on data could fix New York's budget*, in *The Wall Street Journal*, 1st June 2020; IRS, *Intangible property valuation guidelines*, 2020.

[12] N. DUCH BROWN-B. MARTENS-F. MUELLER LANGER, *The economics of ownership, access and trade in digital data*, 2017 (*JRC Digital Economy Working Paper 2017-01)*, in SSRN, disponibile all'url https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2914144.

[13] M. FARBOODY-L. VELDKAMP, *A Model of the data economy*, in *National Bureau of economic research*, 2021.

mente. Al contrario gli asset i cui flussi sono meglio prevedibili subiranno un ammortamento meno aggressivo nei primi periodi [14].

In linea con quanto esposto in precedenza risulta altrettanto importante menzionare il contributo fornito da Wakeman [15], il quale afferma che in presenza di incertezza relativa all'andamento futuro dei flussi associati ad un dato il metodo di ammortamento prediletto è il «*accelerated amortization method*». Quest'ultimo consente di ammortizzare il costo di un bene più rapidamente rispetto ai metodi tradizionali. Ad arricchire il punto di vista precedentemente menzionato sono Berg, Waegenaere e Wielhouwer [16], che confermano la superiorità del suddetto metodo, ma aggiungono che in determinate circostanze a prevalere è lo «*straight line method*», il quale prevede che i costi di acquisizione/produzione di un cespite vengano equamente distribuiti durante l'intera vita utile del cespite. In particolare, quest'ultimo è quello favorito considerando determinati fattori di natura temporale, tributaria, oltre che di incertezza relativa all'andamento dei flussi finanziari futuri.

In conclusione, le cooperative di dati offrono un modello di collaborazione volontaria che favorisce l'unione e l'utilizzo congiunto dei dati per creare valore per i membri del gruppo. Questa forma di collaborazione si basa sul possesso e il controllo dei dati personali dei membri, garantendo loro servizi di raccolta, gestione e protezione dei dati. Dal punto di vista economico, le cooperative di dati consentono di ottenere economie di scala nella domanda e nell'offerta, riducendo i costi di aggregazione e di elaborazione dei dati e creando opportunità per il commercio di dati di alta qualità. Tuttavia, la valutazione qualitativa dei dati richiede un'attenzione approfondita, considerando non solo il volume ma anche la diversità dei dati. È importante considerare le diverse scelte di governance dei dati, incluse le modalità di raccolta, memorizzazione e analisi dei dati personali, così come gli obiettivi economici e di monetizzazione delle cooperative di dati. La valutazione dei dati implica anche una riflessione sulle loro proprietà e sul loro valore come risorsa intermedia che può creare valore attraverso l'utilizzo di altri *asset*. Infine, nella valutazione dei dati, emerge l'importanza di considerare la vita utile dei dati, inclusa la loro persistenza e volatilità, e adottare metodi di ammortamento adeguati a riflettere il valore temporale e finanziario associato ai dati. Nel complesso, le cooperative di dati rappresentano un'interessante forma di collaborazione che può portare a benefici economici e garantire un controllo più efficace e consapevole dei dati personali.

---

[14] W.W. CHOI-S.S. KWON-G.J. LOBO. *Market valuation of intangible assets*, in *Journal of Business Research*, 49 (1), 2000, pp. 35-45.

[15] L.M. WAKEMAN, *Optimal tax depreciation*, in *Journal of accounting and economis*, 1980, pp. 213-237.

[16] M. BERG-A. WAEGENAERE-J. WIELHOUWER, *Optimal tax depreciation with uncertain future cash-flows*, in *European Journal of Operational Research*, 2001, pp. 197-209.

2.2. Valutazione di dati.

Mike Fleckenstein, Ali Obaidi e Nektaria Tryfona asseriscono che il metodo di valutazione dei dati «attualmente [più diffuso], è simile alle tecniche di valutazione consentite per altri *asset* immateriali, come brevetti, diritti d'autore o *software*» [17]In altre parole, i metodi di valutazione su cui vige maggiore consenso in letteratura per i dati sono i medesimi utilizzati per la valutazione degli asset immateriali. In particolare, i metodi di valutazione più frequentemente utilizzati sono:

(i) *Modelli di Mercato*, attraverso i quali i dati vengono valutati basandosi su ciò che il mercato è disposto a pagare, considerando il potenziale di reddito, il valore di mercato delle aziende orientate ai dati, e il costo delle perdite di dati.

(ii) *Modelli Economici*, che si concentrano sull'impatto economico dei dati, come l'utilizzo dei dati del censimento per migliorare l'allocazione delle risorse o l'efficacia delle politiche pubbliche. Questi modelli sono spesso impiegati dai governi per determinare il valore della divulgazione dei dati pubblici.

(iii) *Modelli Dimensionali*, i quali considerano specifiche caratteristiche dei set di dati, come la qualità, il volume, la varietà, e il contesto di utilizzo. Questi modelli valutano come i dati vengono utilizzati e integrati all'interno delle organizzazioni per migliorare le operazioni o i servizi.

Inoltre, gli autori sottolineano che le aziende considerano il valore dei dati non solo per l'uso interno ma anche nel contesto di acquisizioni aziendali, dove i dati possono rappresentare una parte significativa del valore di un'azienda. Il valore dei dati viene approcciato da molteplici angolature che riflettono la loro importanza crescente nell'economia moderna. Questi modelli offrono diversi metodi per quantificare il valore dei dati, che variano in base agli obiettivi specifici, al contesto di utilizzo e alle caratteristiche intrinseche dei dati stessi.

Facendo riferimento ai modelli di mercato, Veldkamp individua diversi approcci di valutazione del dato. In primis l'approccio del costo, l'approccio tradizionale per valutare gli *asset*, che prevede di tenere in considerazione il costo di produzione. Tuttavia, per i dati, il costo può essere difficile da determinare, specialmente per i dati acquisiti attraverso transazioni interne. Questi dati non hanno un prezzo di transazione e la loro produzione, come specificato in precedenza, è un sottoprodotto dell'attività economica, che rende difficile la loro valutazione. Attraverso un esempio l'autrice suggerisce il concetto di "*Data Barter*": visti i benefici significativi che le grandi aziende traggono dai dati dei clienti, un'idea potenziale per valutare i dati è quella di considerare lo sconto che il cliente può ricevere grazie ai dati da esso forniti. Riconoscendo quanto una società può ridurre il prezzo di un bene ad un cliente in cambio dei suoi dati e misurando successivamente questa differenza di prezzo, si potrebbe valutare il costo effettivo della produzione dei dati [18].

---

[17] M. FLECKENSTEIN, A. OBAIDI, N. TRYFONA, *A Review of Data Valuation Approaches and Building and Scoring a Data Valuation Model*, in *Harvard data science review*, 2023.

[18] L. VELDKAMP, *Valuing Data as an Asset*, cit.

Secondo questo approccio, un investitore non spenderebbe per un asset una somma superiore a quella necessaria per sostituirne l'utilità, alla quale si aggiungerebbe un profitto o un rendimento aggiuntivo richiesto per incentivare una terza parte ad effettuare la sostituzione del bene. È inoltre chiaro che in molti casi il costo del bene immateriale potrebbe non essere rappresentativo dei benefici futuri che lo stesso potrebbe generare, il che rende il metodo potenzialmente non adatto a stimarne un valore di mercato [19].

L'Approccio del Reddito permette di valutare i dati quando questi permettono di generare un profitto. Il valore dei dati dovrebbe essere il valore attuale della somma dei ricavi che genera. Tuttavia, isolare il ricavo dei dati dagli altri ricavi è la sfida principale. In molti casi, i dati possono essere utilizzati per scopi multipli e separare i ricavi derivanti dai dati può essere difficile. Come specificato in precedenza le aziende potrebbero vendere prodotti e servizi a un prezzo inferiore rispetto ai costi per acquisire più clienti e dati nel lungo periodo [20]. Rodov e Leliaert si espongono a riguardo presentando un metodo di valutazione che si basa sui flussi incrementali che derivano dall'utilizzo dei dati nell'attività operativa di un'entità. In particolare, il metodo da essi proposto si basa su una stima di flussi di reddito futuri derivanti dall'utilizzo dell'immobilizzazione immateriale. Una volta determinati i flussi finanziari derivanti dall'utilizzo dei dati, simulando un'operatività aziendale priva dei dati oggetto di valutazione, «i flussi vengono poi scontati utilizzando metodi di attualizzazione» [21]. Il punto di debolezza principale associato a questo metodo di valutazione consiste nell'incertezza derivante dalle stime di flussi futuri generati dai dati. Infatti, a meno che non siano basati su ipotesi razionali queste valutazioni rischiano di dare vita a rappresentazioni poco coerenti con il valore reale dei dati.

Relativamente all'approccio reddituale, un altro approccio applicabile è un metodo reddituale/ibrido secondo cui un asset può essere valutato sulla base del valore attuale dei risparmi di costo che si originano grazie al possesso dell'asset stesso piuttosto che dal sostenere, in virtù di un accordo ipotetico, pagamenti relativi ad un canone di *royalty* verso un potenziale licenziante. Il valore di un set di dati può quindi essere stimato in base all'attualizzazione dei flussi futuri di *royalty* attribuibili ad esso (al netto delle imposte), prendendo come periodo di riferimento per la valutazione un orizzonte temporale corrispondente alla vita utile residua dell'*asset* e come tasso di sconto un tasso espressivo del rischio specifico attribuito all'intangibile oggetto di valutazione.

Altro approccio è il cosiddetto Metodo «*With-and-without*» che si basa sulla quantificazione dell'impatto che avrebbe la sostituzione di un *asset* (set di dati nel

---

[19] DELOITTE, *Data valuation: Understanding the value of your data assets*, 2020.

[20] M. FARBOODI-D. SINGAL-L. VELDKAMP-V. VENKATESWARAN, *Valuing Financial Data*, in *NBER (National Bureau of Economic Research), working paper*, 2022, disponibile all'url https://www.nber.org/papers/w29894.

[21] I. RODOV-P. LELIAERT, FiMIAM: *Financial method of intangible assets measurement*, in *Journal of Intellectual Capital*, 2002, pp. 323-336.

caso specifico) sui flussi di cassa (ipotizzando che tutti gli altri asset necessari per far funzionare l'attività siano presenti e abbiano la stessa capacità produttiva in entrambi gli scenari). I ricavi previsti, le spese operative e i flussi di cassa vengono calcolati in scenari "con" e "senza" l'*asset*, e la differenza dei flussi di cassa tra le due opzioni è utilizzata per stimare il *fair value* dell'*asset* stesso. In concreto, la stima dei risultati differenziali attesi può essere operata confrontando i redditi o flussi di cassa attesi di una società che dispone del database con quelli di una medesima impresa che ne è sprovvista, oppure quantificando in modo diretto i risultati differenziali attesi.

Le aziende sfruttano tecniche avanzate di analisi per comprendere appieno i dati e per concederli in licenza. In particolare, sul mercato si verificano scambi di dati tra partecipanti, che permettono aggregazione e creazione di valore. Si ritiene che con il maturare dei mercati, le transazioni di dati rappresenteranno un metodo efficace ai fini della valutazione del fair value degli *asset* stessi. Da qui, attraverso l'approccio di mercato la stima del valore di un set di dati si effettuerebbe facendo riferimento ai prezzi e alle altre informazioni desunte da transazioni aventi ad oggetto *set* di dati con le medesime caratteristiche. Il più noto tra i criteri appartenenti a questa categoria è quello delle transazioni comparabili, che si esplicita facendo rifermento ai prezzi o ai multipli impliciti sul mercato, negoziati per attività simili e comparabili. Il criterio dei multipli di borsa, tra i metodi di mercato, richiede invece che sia quantificabile il valore del *database* deducendo i valori correnti di tutte le attività diverse dal core *asset* oggetto di stima. L'applicazione di questo criterio può risultare molto complessa qualora gli intangibili core siano più di uno, e di conseguenza debbono essere separati i relativi valori.

3. Analisi empirica.

3.1. Presentazione di un caso.

Di seguito è illustrato un possibile approccio empirico per la stima del valore corrente teorico di un database di contatti che si è generato nel corso degli anni grazie ad un programma di fidelizzazione dei clienti (di seguito "*Database*") composto da informazioni anagrafiche, preferenze di acquisto ed altre informazioni rilevanti per possibili azioni di *marketing* e commerciali.

La società ha diversi modi per monetizzare i dati da essa raccolti: (i) utilizzare i dati per personalizzare le campagne di *marketing* e quindi orientare maggiormente lo sviluppo dei prodotti verso quelli più appetibili dai propri clienti; (ii) cedere tali dati ad aziende terze.

Il processo di valutazione si è articolato nelle seguenti fasi: (1) analisi e comprensione dei dati; (2) scelta del metodo di valutazione; (3) identificazione e sviluppo di scenari utilizzo dati.

3.2. Analisi e comprensione dei dati.

Il primo passo in qualsiasi processo di valutazione è la comprensione del bene oggetto di stima. Nel caso specifico, si è proceduto a svolgere un inventario del Database, analizzando nel dettaglio le principali caratteristiche e le modalità con cui sono sfruttati. In dettaglio, durante tale fase è opportuno procedere ad analizzare i seguenti elementi: (i) qualità dei dati, intesa come rilevanza, aggiornamento, accuratezza e tipo; (ii) fonte, *governance*, metodo di raccolta, implicazioni sulla *privacy*; (iii) copertura della popolazione, dati di tracciamento; (iv) domanda di mercato; (v) disponibilità di dati simili.

In molti casi, scopriamo che le organizzazioni sono ostacolate nei loro sforzi per monetizzare efficacemente i loro dati perché non comprendono dove si trovano tutti i loro dati. Scoprire tutti i dati può richiedere l'aggiornamento e il mantenimento di un registro dell'inventario dei dati dell'azienda. Una volta identificati i dati, il management dovrebbe esplorare e categorizzare i loro attributi chiave. La comprensione degli attributi chiave può aiutare nello sviluppo di qualsiasi caso d'uso per massimizzare l'impatto dei dati sulla crescita, redditività e rischio dell'organizzazione.

3.3. Scelta del metodo di valutazione.

La scelta del criterio valutativo da applicare per la stima del valore di mercato del Database è stata effettuata tenendo conto delle caratteristiche intrinseche dell'*asset* stesso, il quale si ritiene essere fonte primaria di generazione di flussi finanziari e valore di conseguenza.

Come evidenziato precedentemente, i dati sono equiparabili ai beni intangibili, ancorché con caratteristiche uniche, possono essere valutati con gli approcci tradizionali.

3.3.1. *Metodi reddituali.*

In pratica, per valutare il valore di un *database*, ad esempio, si determinano i ricavi e i costi associati all'asset e si calcola il reddito specifico derivante dal database tramite la differenza tra i ricavi e i costi. Successivamente, si attualizza il reddito specifico ad un tasso che riflette il rischio associato all'asset. Questo tasso di attualizzazione deve essere adeguato per riflettere le fluttuazioni del mercato o di altra natura, come la tecnologia o l'impatto della legislazione sull'utilizzo del *database*.

In generale, il metodo reddituale determina un valore per il *database* basato sui flussi finanziari futuri che l'*asset* può generare. Questo approccio assume che il valore di un asset immateriale sia determinato dalla sua capacità di generare reddito futuri e non dal solo costo di acquisto.

L'impiego del metodo reddituale richiede la quantificazione precisa dei ricavi e dei costi associati all'*asset*, nonché un'attenta valutazione dei rischi che potrebbero influenzare tale valore nel tempo. Inoltre, questo metodo è soggetto ad alcune limi-

tazioni: ad esempio, la valutazione basata sul reddito può dipendere da previsioni e stime future che non possono sempre essere accurate, in particolare in mercati in evoluzione rapida.

Nonostante queste limitazioni, il metodo reddituale rappresenta comunque uno dei metodi migliori per la valutazione di *asset* immateriali, in quanto tiene conto dei benefici economici futuri che un asset può generare e, quando utilizzato correttamente, può fornire una valutazione affidabile e oggettiva del valore dell'*asset*.

3.3.2. *Metodi di mercato.*

Oggi, le aziende stanno utilizzando analisi avanzate per comprendere più a fondo i loro dati e per identificare modalità di concessione in licenza a terzi. Inoltre, all'interno di vari ecosistemi, vengono sviluppati scambi di dati affinché i partecipanti al mercato possano aggregare e scambiare beni dati, e le aziende partecipanti possano scambiarsi dati per creare ancora più valore per le loro imprese. Man mano che le aziende continuano a esplorare i loro dati e a sviluppare modelli per transare in questa categoria di beni, queste transazioni possono essere utilizzate per derivare indicazioni di mercato sul valore. Come con altri beni, esisteranno sfide di comparabilità del valore, ma con la maturazione dei mercati e l'identificazione di più modi per transare, si crede che le transazioni di dati saranno comunemente utilizzate per valutare i beni dati.

L'approccio basato sui multipli, e in particolare sull'utilizzo di transazioni comparabili, è un altro metodo comunemente utilizzato nella valutazione degli *asset*, come il *database* di una società. In questo approccio, il valore degli *assets* viene stimato confrontando i prezzi delle transazioni comparabili definiti dai mercati regolamentati o dalle negoziazioni private, al fine di determinare un valore di mercato per l'attività della società.

A differenza dell'approccio reddituale, il metodo dei multipli non tiene conto dei dati storici o previsionali, né dei dati del bilancio dell'azienda. Al contrario, i multipli vengono calcolati rapportando il valore di mercato degli assets selezionati per un indicatore numerico o economico, come ad esempio il numero di utenti o di contatti associati all'asset.

Per quantificare il valore economico di un *database*, ad esempio, è possibile fare riferimento al valore corrente di *asset* simili detenuti da società comparabili e rapportare tale valore con uno specifico indicatore numerico, come il numero di contatti. Il multiplo così stimato è possibile utilizzarlo per stimare il valore dell'asset della società stessa in considerazione del numero di contatti della società specifica.

Questo processo consente di stimare il valore economico del *database*, utilizzando transazioni comparabili al fine di determinare un valore di mercato obiettivo. Tuttavia, l'approccio basato sui multipli presenta alcune limitazioni, come l'affidabilità delle fonti, la difficoltà di individuare transazioni comparabili in diversi mercati o settori, o la difficoltà di trovare un indicatore numerico economico adeguato per la specifica attività.

In generale, l'approccio basato su multipli può fornire un utile complemento all'approccio reddituale, ma richiede comunque un'attenta considerazione delle circostanze specifiche dell'asset in questione.

3.3.3. *Metodo* with-and-without.

Un altro metodo per stimare il valore dei dati è quello basato sui flussi differenziali nel caso in cui i dati dovessero essere sostituiti (assumendo che tutti gli altri beni necessari per operare l'azienda siano presenti e abbiano la stessa capacità produttiva). I ricavi previsti, le spese operative e i flussi di cassa vengono calcolati in scenari "con" e "senza" i dati, e la differenza tra i flussi di cassa nei due scenari viene utilizzata per stimare il valore dei dati.

3.4. Identificazione e sviluppo di scenari utilizzo dati.

Il processo di valutazione dei dati permette di identificare nuovi casi d'uso, che vanno da nuove applicazioni commerciali a utilizzi alternativi e difensivi dei dati. Gli approcci di valutazione in ogni caso saranno determinati dagli usi esistenti e potenziali dei dati.

Ai fini della valutazione è stato applicato:

I. – il metodo "*with or without*" che prevede la stima da parte del management di due scenari, uno nel quale il business beneficia dell'utilizzo dei dati e uno nel quale non può beneficiare dell'utilizzo dei dati. In ciascuno degli scenari sono stati stimati relativi flussi di cassa. Pertanto, gli *input* di tale modello sono i seguenti:

(i) la vita utile attesa dell'*asset* (dato) (che può essere determinata da una comprensione approfondita delle sue caratteristiche);

(ii) flussi di cassa dello scenario "*with*";

With		**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Ricavi		100	110	121	133	146	149	152	155	158	162
	yoy%		*10%*	*10%*	*10%*	*10%*	*2%*	*2%*	*2%*	*2%*	*2%*
Costi		(60)	(63)	(66)	(69)	(73)	(74)	(76)	(77)	(79)	(81)
	yoy%		*5%*	*5%*	*5%*	*5%*	*2%*	*2%*	*2%*	*2%*	*2%*
EBITDA		**40**	**47**	**55**	**64**	**73**	**75**	**76**	**78**	**80**	**81**
D&A			(11)	(11)	(11)	(11)	(11)	(11)	(11)	(11)	(11)
EBIT		**40**	**36**	**44**	**53**	**62**	**64**	**65**	**67**	**68**	**70**
Imposte	*27,90%*	(11)	(10)	(12)	(15)	(17)	(18)	(18)	(19)	(19)	(20)
NOPAT		**29**	**26**	**32**	**38**	**45**	**46**	**47**	**48**	**49**	**50**
D&A		-	11	11	11	11	11	11	11	11	11
Delta CCN		(8)	(9)	(11)	(13)	(15)	(15)	(15)	(16)	(16)	(16)
Capex		(100)	-	-	-	-	-	-	-	-	-
FCFO		**(79)**	**28**	**32**	**36**	**41**	**42**	**43**	**44**	**45**	**45**

(iii) flussi di cassa dello scenario "*without*";

Without		**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Ricavi		77	85	93	102	113	115	117	120	122	124
yoy%			*10%*	*10%*	*10%*	*10%*	*2%*	*2%*	*2%*	*2%*	*2%*
Costi		(60)	(63)	(66)	(69)	(73)	(74)	(76)	(77)	(79)	(81)
yoy%			*5%*	*5%*	*5%*	*5%*	*2%*	*2%*	*2%*	*2%*	*2%*
EBITDA		**17**	**22**	**27**	**33**	**40**	**41**	**41**	**42**	**43**	**44**
D&A			-	-	-	-	-	-	-	-	-
EBIT		**17**	**22**	**27**	**33**	**40**	**41**	**41**	**42**	**43**	**44**
Imposte	*27,90%*	(5)	(6)	(8)	(9)	(11)	(11)	(12)	(12)	(12)	(12)
NOPAT		**12**	**16**	**19**	**24**	**29**	**29**	**30**	**30**	**31**	**32**
D&A		-	-	-	-	-	-	-	-	-	-
Delta CCN		(3)	(4)	(5)	(7)	(8)	(8)	(8)	(8)	(9)	(9)
Capex		-	-	-	-	-	-	-	-	-	-
FCFO		**9**	**11**	**14**	**17**	**21**	**21**	**22**	**22**	**22**	**23**

(iv) tasso di attualizzazione coerente con la configurazione del flusso di cassa.

With or without		**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Flusso di cassa differenziale		**(88)**	**16**	**18**	**19**	**21**	**21**	**21**	**22**	**22**	**22**
Discount period		*0,5*	*1,5*	*2,5*	*3,5*	*4,5*	*5,5*	*6,5*	*7,5*	*8,5*	*9,5*
Discount factor	*10%*	*0,95*	*0,87*	*0,79*	*0,72*	*0,65*	*0,59*	*0,54*	*0,49*	*0,44*	*0,40*
Flusso di cassa attualizzato		**(84)**	**14**	**14**	**14**	**13**	**12**	**11**	**11**	**10**	**9**
Valore corrente database	**25**										

Il valore attuale del flusso di cassa differenziale rappresenta pertanto il valore corrente attribuibile al *database*;

II. – il modello "*relief from royalty*": tale metodo prevede l'identificazione di un tasso di *royalty* ipotetico da pagare ad un terzo per l'uso dei dati, in uno scenario ipotetico in cui i dati non fossero direttamente in suo possesso ma di proprietà di un terzo. Pertanto, gli *input* di tale modello sono i seguenti:

(i) la vita utile attesa dell'asset (dato) (che può essere determinata da una comprensione approfondita delle sue caratteristiche);

(ii) tassi di crescita del fatturato legati al tasso di *royalty* (compresa l'analisi delle caratteristiche);

(iii) la redditività del modello di *business* utilizzando i dati come variabile chiave;

Eur/mln

Relief from royalty		**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Ricavi		100	110	121	133	146	149	152	155	158	162
yoy%			*10%*	*10%*	*10%*	*10%*	*2%*	*2%*	*2%*	*2%*	*2%*
Royalty rate	*5%*	**5**	**5**	**6**	**6**	**7**	**7**	**7**	**7**	**8**	**8**
Costi di mantenimento		(1)	(1)	(1)	(1)	(1)	(1)	(1)	(1)	(1)	(1)
Flusso di royalty netto		**4**	**4**	**5**	**5**	**6**	**6**	**6**	**6**	**7**	**7**
Imposte	*27,90%*	(1)	(1)	(1)	(1)	(2)	(2)	(2)	(2)	(2)	(2)
Flusso di royalty post tax		**3**	**3**	**3**	**4**	**4**	**4**	**5**	**5**	**5**	**5**
Discount period		*0,5*	*1,5*	*2,5*	*3,5*	*4,5*	*5,5*	*6,5*	*7,5*	*8,5*	*9,5*
Discount factor	*10%*	*0,95*	*0,87*	*0,79*	*0,72*	*0,65*	*0,59*	*0,54*	*0,49*	*0,44*	*0,40*
Valore attuale		**3**	**3**	**3**	**3**	**3**	**3**	**2**	**2**	**2**	**2**
Valore corrente database	**25**										

(iv) tassi di *royalty* comparabili con l'aggiunta di un tasso di sconto, che misura il rischio atteso del modello di *business*.

Il valore attuale del flusso di *royalty* netto rappresenta il valore corrente attribuibile al *database*.

4. Conclusione.

La valutazione dei dati come asset immateriale presenta molte sfide e limiti. I metodi tradizionali di valutazione degli asset possono non essere sufficientemente adattati per catturare il valore complesso e mutevole dei dati. Anche se esistono diverse metodologie, come l'approccio al costo o al reddito, ciascuna presenta criticità. Ad esempio, l'approccio al costo potrebbe sottovalutare il valore dei dati, ignorando l'impatto dei dati stessi sulle operazioni aziendali. D'altra parte, l'approccio al reddito potrebbe essere difficoltoso da applicare a dati non monetizzati direttamente o soggetti a flussi finanziari non determinabili con precisione. Inoltre, la natura mutevole e dinamica dei dati, insieme alla loro crescente importanza economica, aggiunge ulteriori complicazioni. La valutazione dei dati richiede un'analisi approfondita delle fonti, della qualità e del potenziale di utilizzo dei dati stessi, oltre a considerazioni su *privacy*, sicurezza e conformità normativa. Le nuove sfide emergono anche dalla natura stessa dei dati come asset immateriali. Mentre altri asset immateriali come brevetti o marchi registrati possono essere valutati con maggior precisione, i dati sono più sfuggenti e soggetti a variazioni imprevedibili nel loro valore nel tempo. Inoltre, la mancanza di standardizzazioni e metodologie consolidate può rendere la valutazione dei dati un'operazione soggettiva e poco definita.

Tuttavia, nonostante queste sfide, il valore dei dati continua a crescere, con le aziende che li utilizzano sempre più come fonte di vantaggio competitivo e innovazione. Il riconoscimento del valore dei dati è fondamentale per guidare decisioni aziendali informate e sfruttare appieno il potenziale di questo *asset* intangibile.

Capitolo XV

El impacto del *big data* en el derecho societario: la importancia de la cooperativa de datos

Mauricio Boretto

Abstract: One of the most important measures proposed by the Data Governance Regulation is to establish rules allowing the development of favourable conditions for the exchange of data; creating an European data market. For this reason, this regulatory framework has ruled as main idea the figure of "data intermediates", who can be consulted by the parties about the exchange of data; one of whose alternatives is "data cooperative". The combined application of these cooperatives and the Big Data in the administration and management of data, has strongly influenced the development of the companies' business strategies.

1. Punto de partida.

La Unión Europea (en adelante, UE), a través del Reglamento 2022/868 del Parlamento Europeo y del Consejo de 30 de mayo relativo a la *gobernanza europea de datos*, vino a reconocer enfáticamente al "dato" [1] – y a su regulación – como una

[1] Art. 2, inc. 1, Reglamento 2022/868: *Se entiende por "datos" toda representación digital de ac-*

pieza esencial del desarrollo presente y futuro de la sociedad; erigiéndose claramente en una prioridad desde el punto de vista político-institucional [2].

Se dice con razón que los "datos" constituyen un *activo social*. En efecto, a medida que la sociedad y sus diversos actores – como son los ciudadanos, las universidades, las empresas y la propia administración pública – se han ido digitalizando, sus actividades – tanto económicas cuanto sociales, políticas y culturales, entre otras – se rigen cada vez más por el uso de tecnologías que, precisamente, necesitan de estos "datos" para funcionar. Véase, por ejemplo, que la inteligencia artificial, la Internet de las Cosas, el *big data*, el *blockchain* y, en general, cualquier otra tecnología, necesitan de "datos" para operar.

Sin "datos" suficientes, utilizados adecuada y hasta estratégicamente, tanto Europa como cualquier país del mundo, no podrían desarrollar su máximo potencial, limitando el acceso de los ciudadanos a los diversos servicios de calidad, sean estos tecnológicos, educativos, económicos, sanitarios, culturales, ambientales, jurídicos, entre otros; dificultando, de esta manera, el progreso, la competitividad, la innovación y el bienestar de la comunidad a la que pertenecen.

Existe una realidad que la UE no desconoce [3] y que ha motivado el dictado del Reglamento 2022/868:

Sabe que los datos son un recurso esencial para que las *startups* y las *PyMES* europeas puedan desarrollar nuevos productos y servicios. Además, la disponibilidad de datos es fundamental para entrenar a los sistemas de inteligencia artificial, como así también para alimentar el uso de gemelos digitales [4].

---

tos, hechos o información, así como su recopilación, incluso como grabación sonora, visual o audiovisual. Para analizar la definición de "dato" como bien jurídico ver la opinión de G. RESTA, *I dati personali oggetto del contratto Riflessioni sul coordinamento tra la direttiva (UE) 2019/770 e il regolamento (UE) 2016/679*, in G. RESTA-V. ZENO ZENCOVICH (a cura di) *Governance of/Throug big data – Vol. II*, *Consumatori e Mercato 13*, Roma, 2023, p. 661.

[2] Por ejemplo, con la adopción del *GDPR (Reglamento General de Protección de Datos UE 2016/679)* en vigor desde hace años, la UE se ha posicionado como un faro relevante en materia de datos personales, consagrando, por ejemplo, el derecho de todo interesado a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

[3] S. HEREDIA QUERRO, *Hacia un mercado europeo de datos: el nuevo régimen de los Intermediarios (neutrales) de Datos*, 15/01/2024, *opinión*, https://abogados.com.ar/hacia-un-mercado-europeo-de-datos-el-nuevo-regimen-de-los-intermediarios-neutrales-de-datos/34073.

[4] Los gemelos digitales o "*digital twins*"son un modelo virtual que refleja con exactitud un objeto físico, proceso o sistema. Se utilizan para realizar simulaciones y estudiar el comportamiento de un producto digital, para después adaptar las soluciones al producto real de una manera eficiente (https://www.repsol.com/es/energia-futuro/tecnologia-innovacion/gemelos-digitales/index.cshtml). El término "gemelo digital" es una forma sencilla de describir un modelo virtual en tiempo real de un dispositivo o proceso físico existente en el mundo real. Básicamente, la creación de un modelo virtual de sistemas complejos del mundo real permite a desarrolladores, planificadores y otras partes interesadas visualizar esos sistemas, evaluar su viabilidad, realizar pruebas y ajustar la construcción de las versiones del mundo real, lo que puede ahorrar tiempo y gastos e incluso evitar fallas. Por ejemplo,

Es consciente que un pequeño número de grandes empresas de tecnología de China y Estados Unidos posee gran parte de los datos del mundo, lo que puede reducir los incentivos para que surjan, crezcan e innoven en la UE empresas basadas en los datos.

No ignora la elevada concentración existente en la prestación de servicios en la nube y de infraestructuras de datos, y de ciertos desequilibrios de mercado en relación con el acceso a los datos y su utilización, lo que termina afectando a las *PyMEs* europeas. Este problema se ilustra bien con el caso de las plataformas: un pequeño número de actores pueden acumular grandes cantidades de datos que les permiten obtener información importante y ventajas competitivas gracias al volumen y la variedad de los datos que poseen. Además, se afecta la competencia en los mercados en casos específicos, no solo en el mercado relevante *per se* de provisión de servicios de plataformas digitales, sino también en los distintos mercados específicos de bienes y servicios que también son cubiertos por la plataforma, en particular, si la plataforma está activa en dichos mercados conexos (*spillover effects*) [5].

Además del cuidado y respeto de los datos personales y la regulación de las plataformas, han comenzado a aparecer grandes cantidades de datos industriales (datos no personales), datos públicos, y también nuevas formas de tratamiento y gestión de los mismos. Pero ¿cuántos datos?, ¿dónde están almacenados? La UE indica que el volumen de datos producidos en el mundo escalará desde los 33 zettabytes en 2018 hasta los 175 zettabytes en 2025 – es decir 6X de crecimiento –. Actualmente, el 80% del tratamiento y el análisis de estos datos tiene lugar en centros de datos y en instalaciones informáticas centralizadas, y el 20% restante en objetos conectados inteligentes (IoT) como vehículos, electrodomésticos, robots y en otros tipos de instalaciones informáticas cercanas al usuario: *Edge Computing*. La UE asume que este mix 80/20 se invertirá tan pronto como en 2025.

En este contexto, precisamente, se ha procurado dotar a los "datos" – en su condición de activo esencial – de reglas de uso claras, buscando promover una óptima protección y una compartición segura de los mismos dentro del mercado europeo. A tal fin, y como política institucional fundamental, se ha dictado la normativa regulatoria que estamos analizando – el Reglamento 2022/868 – capaz de brindar la seguridad jurídica que se necesita para el desarrollo de aquellos objetivos claves.

El texto en análisis se enfoca en intercambios voluntarios y comerciales de datos, a la vez que busca impulsar el desarrollo de nuevos intermediarios europeos, que faciliten el intercambio de datos entre tenedores – *data holders* – y usuarios – *data users* –, pero de manera neutral, es decir, sin procesar esa información para un fin propio o corporativo; en función de una expresa prohibición de integración ver-

---

Un gemelo digital, o *digital twin*, es una réplica virtual realizada a imagen y semejanza de un producto: la turbina de un avión, la fachada de un edificio, etc.

[5] Los economistas suelen utilizar el término de derrame (*spillover*) para capturar la idea de que algunos individuos o empresas se benefician (o perjudican) indirectamente de ciertas actividades o acciones realizadas por otros.

tical y *cross-subsidies*[6] – en castellano: *subsidios cruzados*[7] – del art. 12[8].

[6] S. Heredia Querro, *Hacia un mercado europeo de datos: el nuevo régimen de los Intermediarios (neutrales) de Datos*, 15/01/2024, *opinión*, https://abogados.com.ar/hacia-un-mercado-europeo-de-datos-el-nuevo-regimen-de-los-intermediarios-neutrales-de-datos/34073.

[7] Utilizamos aquí esta expresión en sentido metafórico. En efecto, suele utilizarse para describir aquellos mecanismos universales usados para transferir vía precio un ingreso de un sector de la población a otro, para así darle acceso a algún bien o servicio que de otra forma no lo tendría. En su concepción más general implica una "transferencia de costos" donde algunos o todos los costos de un producto/servicio se trasladan a otro. En otras palabras, el subsidio cruzado responde a la idea de transferencia de recursos o costos de un segmento del mercado a otro.

[8] *Condiciones para la prestación de servicios de intermediación de datos*. La prestación de servicios de intermediación de datos a que se refiere el artículo 10 estará sujeta a las condiciones siguientes: *a) Los proveedores de servicios de intermediación de datos no podrán utilizar los datos en relación con los que presten sus servicios para fines diferentes de su puesta a disposición de los usuarios de datos y prestarán los servicios de intermediación de datos a través de una persona jurídica distinta; b) las condiciones contractuales comerciales, incluidas las relativas a los precios, para la prestación de servicios de intermediación de datos a un titular de datos o a un usuario de datos no podrán depender de que el titular de datos o el usuario de datos utilice otros servicios prestados por el mismo proveedor de servicios de intermediación de datos o por una entidad relacionada con él, y, de utilizarlos, no podrán depender de en qué grado el titular de datos o el usuario de datos utilice dichos servicios; c) los datos recogidos sobre cualquier actividad de una persona física o jurídica a efectos de la prestación de un servicio de intermediación de datos, incluidas la fecha, hora y geolocalización, la duración de la actividad y las conexiones que el usuario del servicio de intermediación de datos establezca con otras personas físicas o jurídicas, solo se utilizarán para el desarrollo de ese servicio de intermediación de datos, lo que puede implicar la utilización de datos para la detección de fraudes o para fines de ciberseguridad, y se pondrán a disposición de los titulares de datos, previa petición; d) los proveedores de servicios de intermediación de datos intercambiarán los datos en el mismo formato en el que los reciban de parte del interesado o del titular de datos, únicamente los convertirán en formatos específicos con el fin de mejorar la interoperabilidad intrasectorial e intersectorial o si así lo solicita el usuario de datos o si así lo exige el Derecho de la Unión o si es necesario a efectos de la armonización con las normas internacionales o europeas en materia de datos y ofrecerán a los interesados o a los titulares de datos una posibilidad de exclusión en relación con dichas conversiones, a menos que el Derecho de la Unión obligue a realizar dicha conversión; e) los servicios de intermediación de datos podrán incluir la oferta de herramientas y servicios específicos adicionales a los titulares de datos o los interesados con el objetivo específico de facilitar el intercambio de los datos, por ejemplo, el almacenamiento temporal, la organización, la conversión, la anonimización y la seudonimización, siempre que tales herramientas y servicios solo se utilicen previa solicitud o aprobación expresas del titular de datos o del interesado, y que las herramientas de terceros ofrecidas en ese contexto no se utilicen para otros fines; f) los proveedores de servicios de intermediación de datos velarán por que el procedimiento de acceso a sus servicios, incluidos los precios y las condiciones de servicio, sea equitativo, transparente y no discriminatorio, tanto para los interesados como para los titulares de datos y los usuarios de datos; g) los proveedores de servicios de intermediación de datos dispondrán de procedimientos para impedir prácticas fraudulentas o abusivas de las partes que deseen obtener acceso a través de sus servicios de intermediación de datos; h) los proveedores de servicios de intermediación de datos se asegurarán en caso de insolvencia, de la continuidad razonable de la prestación de sus servicios de intermediación de datos y, cuando esos servicios de intermediación de datos incluyan el almacenamiento de datos, dispondrán de los meca-*

Así las cosas, esta nueva regulación trae consigo un novedoso enfoque ante la posibilidad de que los datos – personales o no – puedan ser compartidos entre los actores económicos y sociales para alentar el crecimiento de la sociedad y de la economía digitales en Europa; siempre que sea de una forma segura y en un marco democrático y de respeto a los derechos y a las libertades de los ciudadanos.

Sin perjuicio de lo expuesto, no puede afirmarse que la UE no hubiera considerado importante la regulación de los datos con anterioridad al mismísimo Reglamento 2022/868.

En efecto, durante estos últimos años la UE creó un marco jurídico de "datos", aunque lo circunscribió fundamentalmente a la protección de los datos personales [9]

---

nismos de garantía necesarios para que los titulares de datos y los usuarios de datos puedan acceder a sus datos, transferirlos o recuperarlos y, cuando presten esos servicios de intermediación entre interesados y usuarios de datos, para permitir que los interesados ejerzan sus derechos; i) los proveedores de servicios de intermediación de datos adoptarán las medidas adecuadas para garantizar la interoperabilidad con otros servicios de intermediación de datos, entre otros, mediante normas abiertas de uso común en el sector en el que operen los proveedores de servicios de intermediación de datos; j) los proveedores de servicios de intermediación de datos aplicarán las medidas técnicas, jurídicas y organizativas adecuadas para impedir el acceso a datos no personales o su transferencia cuando dicho acceso o transferencia sean ilícitos con arreglo al Derecho de la Unión o al Derecho nacional del Estado miembro correspondiente; k) los proveedores de servicios de intermediación de datos informarán sin demora a los titulares de datos en caso de transferencia, acceso o utilización no autorizados de los datos no personales que haya compartido; l) los proveedores de servicios de intermediación de datos tomarán las medidas necesarias para garantizar un nivel de seguridad adecuado en relación con el almacenamiento, el tratamiento y la transmisión de los datos no personales, y también garantizarán el más elevado nivel de seguridad en relación con el almacenamiento y la transmisión de información sensible desde el punto de vista de la competencia; m) los proveedores de servicios de intermediación de datos que ofrezcan servicios a los interesados actuarán en el mejor interés de estos cuando faciliten el ejercicio de sus derechos, en particular, informándolos y, cuando corresponda, asesorándolos de manera concisa, transparente, inteligible y fácilmente accesible sobre los usos previstos de los datos por los usuarios de datos y las condiciones generales aplicables a dichos usos antes de que los interesados presten su consentimiento; n) cuando los proveedores de servicios de intermediación de datos proporcionen herramientas para obtener el consentimiento de los interesados o el permiso para tratar los datos facilitados por los titulares de datos, especificarán, cuando corresponda, el territorio del tercer país en el que se pretenda usar los datos y proporcionarán a los interesados herramientas tanto para otorgar como para retirar su consentimiento, y a los titulares de datos, herramientas tanto para conceder como para retirar los permisos para tratar los datos; o) los proveedores de servicios de intermediación de datos conservarán un registro de la actividad de intermediación de datos.

[9] Se entiende por "datos personales" *toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona* (art. 4, inc. 1, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos).

a través del *Reglamento General de Protección de Datos* (RGPD) [10]; generando un exitoso estándar mundial en la materia [11].

Hoy, claramente, a través del Reglamento 2022/868 ha dado un paso muy importante hacia adelante, en dirección a la regulación de todo tipo de datos aunque no sean personales, o sea, datos puramente industriales, medioambientales, agrícolas, financieros, empresariales, entre muchos otros.

Una última aclaración.

Las nuevas reglas no implican una regulación omnicomprensiva de todos los aspectos jurídicos que afectan a los datos como activo social. El objetivo principal ha sido establecer un marco regulatorio que confiera mayor seguridad jurídica al dato digital en determinados aspectos, como es la promoción de un mercado europeo de datos y la fijación de reglas claras para incentivar la puesta en común de determinadas categorías de datos [12].

Sin perjuicio de ello, de lo que no cabe duda, es que las nuevas normas europeas sobre la materia suponen indefectiblemente un cambio de enfoque y un nuevo paradigma que tendrán seguramente un impacto relevante – entre otros aspectos – en la forma de actuar de las *empresas a la hora de la toma de decisiones*; tema de nuestro especial interés y al cual nos referiremos a continuación.

---

[10] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

[11] El profesor Fabio Bravo se refiere a los "datos personales" como verdaderos instrumentos de poder y de control: "*I dati personali sono divenuti oggetto di crescente attenzione da parte di istituzioni e di imprese, per la straordinaria capacità di sviluppo che essi comportano. La possibilità di ricavare informazioni dalla loro analisi consente di godere di indiscutibili vantaggi in termini di potere e di controllo in molteplici ambiti, tra cui quello del mercato (c.d. business intelligence, behavioural advertising), quello finanziario (FinTech, TechFin), quello politico (anche con riguardo alla manipolazione a fini elettorali quello "governativo". I dati personali hanno inoltre una forte attitudine ad essere utilizzati in modelli di business profondamente redditizi, già esplorati nella prassi degli affair*". En castellano: "*Los datos personales se han convertido en objeto de creciente atención por parte de instituciones y empresas, por la extraordinaria capacidad de desarrollo que implican. La posibilidad de extraer información de su análisis permite disfrutar de ventajas indiscutibles en términos de poder y de control en múltiples ámbitos, entre ellos el del mercado (c.d. business intelligence, behavioural advertising), el financiero (FinTech, TechFin) el político (también en lo que respecta a la manipulación con fines electorales), el "gubernativo". Los datos personales también tienen una fuerte aptitud para ser utilizados en modelos de negocio profundamente rentables, ya explorados en la práctica de los negocios*" (F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in *Contratto e impresa Europa*, 2021, 1, pp. 208-209).

[12] L. LOPEZ LAPUENTE, *La nueva regulación europea de los datos: como dar forma al futuro digital de Europa*, in *Actualidad Jurídica Uría Menéndez*, 61, pp. 50/71 https://www.uria.com/es/publicaciones/8350-la-nueva-regulacion-europea-de-los-datos-como-dar-forma-al-futuro-digital-de-eu.

2. Importancia de los "datos" y de su regulación.

La nueva regulación revela, evidentemente, que la digitalización de Europa constituye una prioridad institucional por varios motivos [13].

Por un lado, la UE es consciente que los datos – personales y no personales – son claves para habilitar nuevos productos y servicios basados en tecnologías disruptivas como la inteligencia artificial o el *blockchain*; de tal modo de hacer que la producción sea más eficiente y de brindar mejores herramientas para combatir nuevos desafíos sociales. Por ejemplo, durante la crisis del COVID-19 se apreció cómo, en el área de la salud, los datos pudieron contribuir a brindar una mejor atención médica, optimizar los tratamientos personalizados y ayudar a curar enfermedades.

Por otro lado, está claro que los datos tienen un importante papel en materia de competencia en el mercado. En efecto, la UE considera también a los datos como un poderoso motor para la innovación empresarial, la creación de nuevos puestos de trabajo; constituyéndose en un recurso fundamental para las empresas emergentes y las *PyMes*, favoreciendo – de esta manera – el desarrollo de una economía europea competitiva.

En este sentido, preocupa que la acumulación de datos en unos pocos agentes económicos pueda obstaculizar el desarrollo de nuevas empresas – sobre todo aquellas con un componente tecnológico importante – las cuales, sin el acceso a los mismos, pueden verse limitadas en su capacidad de producción o en su potencial de crecimiento.

Desde este diagnóstico, y de acuerdo con la imperiosa necesidad de mejorar el "manejo de los datos", es que surge la *Estrategia Europea de Datos* [14], a través de la cual la Comisión Europea está adoptando una serie de medidas para intentar capitalizar verdaderamente este enorme potencial.

El objetivo principal de la Estrategia es, por lo tanto, poner a disposición más datos en el ámbito de la UE y establecer medidas – muchas de ellas normativas – para permitir a los actores europeos – empresas, investigadores, sector público y también ciudadanos – que puedan compartirlos con confianza y que sean técnicamente fáciles de reutilizar.

Una de las medidas adoptadas en este sentido en el marco de la *Estrategia Europea de Datos*, es crear las condiciones adecuadas para que exista un mercado europeo de datos en el que estos puedan intercambiarse y compartirse de una manera segura y fiable, promoviendo así su compartición. Este objetivo se pretende consolidar, precisamente, a través de la nueva regulación que estamos analizando: el *Re-*

---

[13] F. CALOPRISCO, *Data Governance Act. Condivisione e 'altruismo' dei dati*, in *Quaderni Aisdue*, 2021, 2, Napoli, 2022, p. 169.

[14] La estrategia de datos se centra en poner a las personas en primer lugar en el desarrollo de la tecnología y en la defensa y promoción de los valores y derechos europeos en el mundo digital – https://digital-strategy.ec.europa.eu/es/policies/strategy-data.

glamento de Gobernanza de Datos, que se aprobó en mayo de 2022. Sin seguridad jurídica en el intercambio de datos y *sin la intervención de intermediarios seguros y fiables*, resulta difícil que las empresas e instituciones accedan a los datos necesarios que les permitan avanzar en materia de investigación, innovación, desarrollo y aplicación eficiente de las nuevas tecnologías, productos y servicios.

En resumen, este Reglamento pretende generar un mercado europeo de datos confiable y transparente, que facilite el intercambio entre los distintos actores.

A tal efecto se regula, entre otros aspectos, la figura del *intermediario de datos* que analizaremos en el acápite siguiente.

3. Los servicios de intermediación de datos como mecanismo para crear un mercado europeo de datos.

3.1. Introducción.

Como dijimos, una de las importantes medidas propuestas por el *Reglamento de Gobernanza de Datos* es fijar las reglas que permitan el desarrollo de condiciones favorables para el intercambio de datos, es decir, establecer las bases adecuadas para el funcionamiento de un mercado europeo de datos.

La propia idea implica un cambio de paradigma normativo en la UE, en la medida en que se aborda por primera vez y de forma tan específica el "intercambio de datos" entre empresas como un objetivo recomendable, que debe promoverse, aunque sujeto – claro está – a ciertos límites y reglas relativas a la protección de datos [15] y al Derecho de la competencia [16].

---

[15] Véase, a modo de ejemplo, lo expuesto en los considerandos 5 y 23 del Reglamento (UE) 2022/88: (5) "*Se requieren medidas de la Unión para incrementar la confianza en el intercambio de datos mediante el establecimiento de mecanismos adecuados que permitan a los interesados y los titulares de datos ejercer control sobre los datos que les conciernen y para abordar otros obstáculos al buen funcionamiento y la competitividad de la economía basada en los datos. Esta acción debe entenderse sin perjuicio de las obligaciones y los compromisos establecidos en los acuerdos comerciales internacionales celebrados por la Unión. Un marco de gobernanza de la Unión debe tener como objetivo generar confianza entre los particulares y las empresas en relación con el acceso a los datos, su control, intercambio, utilización y reutilización, especialmente mediante el establecimiento de mecanismos adecuados que permitan a los interesados conocer y ejercer de forma significativa sus derechos y, en lo relativo a la reutilización de determinados tipos de datos que obren en poder de organismos del sector público, la prestación de servicios a los interesados, a los titulares de datos y a los usuarios de datos, por parte de los proveedores de servicios de intermediación de datos, así como la recogida y el tratamiento de datos cedidos con fines altruistas por personas físicas y jurídicas. En particular, una mayor transparencia en cuanto a la finalidad de la utilización de los datos y las condiciones en que las empresas los almacenan puede contribuir a aumentar la confianza*" y (23) "*Para impulsar la confianza en la economía de los datos de la Unión es esencial que las garantías relativas a los ciudadanos de la Unión y al sector público y las empresas de la Unión garanticen que se ejerza control sobre sus datos estratégicos y sensibles, y que se respeta el Derecho, los valores y las normas*

Para crear este mercado, el Reglamento elige como idea rectora regular la figura de los *intermediarios* [17] a los que pueden acudir las partes para el intercambio de datos.

---

de la Unión en cuanto a la seguridad, la protección de datos y la protección de los consumidores, entre otros aspectos. A fin de impedir el acceso ilícito a los datos no personales, los organismos del sector público, las personas físicas o jurídicas a las que se haya concedido el derecho a reutilizar datos, los proveedores de servicios de intermediación de datos y las organizaciones reconocidas de gestión de datos con fines altruistas deben adoptar todas las medidas razonables para impedir el acceso a los sistemas en los que se almacenen los datos no personales, tales como el cifrado de datos o las políticas corporativas. Para ello, debe garantizarse que los organismos del sector público, las personas físicas o jurídicas a las que se haya concedido el derecho a reutilizar datos, los proveedores de servicios de intermediación de datos y las organizaciones reconocidas de gestión de datos con fines altruistas deben acatar todas las normas técnicas, códigos de conducta y certificaciones pertinentes de la Unión".

[16] Véase, a modo de ejemplo, lo expuesto por los considerandos 20 y 37 del Reglamento (UE) 2022/88: (20) "*Además, a fin de preservar la competencia leal y la economía de mercado abierta, resulta de vital importancia salvaguardar los datos protegidos de carácter no personal, en particular, los secretos comerciales, pero también los datos no personales que constituyan contenidos protegidos por derechos de propiedad intelectual, frente a un acceso ilícito que entrañe riesgo de robo de esta última o de espionaje industrial. A fin de garantizar la protección de los derechos o los intereses de los titulares de datos, los datos no personales que deban protegerse del acceso ilícito o no autorizado de conformidad con el Derecho de la Unión o nacional y que obren en poder de organismos del sector público, deben poder transferirse a terceros países únicamente cuando ofrezcan garantías adecuadas para su utilización. Dichas garantías adecuadas deben incluir como requisito que el organismo del sector público transmita los datos protegidos a un reutilizador únicamente cuando este contraiga obligaciones contractuales en interés de la protección de los datos. Todo reutilizador que tenga intención de transferir los datos protegidos a un tercer país debe cumplir las obligaciones establecidas en el presente Reglamento, incluso después de dicha transferencia. A fin de velar por el correcto cumplimiento de estas obligaciones, el reutilizador también ha de aceptar, por lo que respecta a la resolución judicial de litigios, las competencias del Estado miembro al que pertenezca el organismo del sector público que haya permitido la reutilización*" y (37) "*Los proveedores de servicios de intermediación de datos deben adoptar, asimismo, medidas para garantizar el cumplimiento del Derecho de la competencia y disponer de procedimientos a tal efecto. Este es el caso de determinadas situaciones en las que el intercambio de datos permite a las empresas estar al corriente de las estrategias de mercado de sus competidores reales o potenciales. La información sensible desde el punto de vista de la competencia suele incluir detalles sobre datos de clientes, precios futuros, costes de producción, cantidades, facturación, ventas o capacidades*".

[17] Los *Data intermediaries* (DIs) son un nuevo intermediario neutral entre los usuarios y los tenedores de datos, con distintos modelos de negocios (públicos o privados, *for profit o non-profit*), que cobran suscripciones para acceder a data sets centralizados, o comisiones por transacciones. Surgen de la mano del movimiento de *Open Banking* (como *trusted third parties*, como ilustra el *UK Open Banking Implementation Entity*), o como custodios de datos como el *Genomic England Project*, ofreciendo ambientes seguros para análisis de datos o auditoría de datos, aunque la doctrina afirma que no está tan claro qué otros servicios – aparte de intermediación – podrán ofrecer. Los DIs pueden estar estructurados como organizaciones con data servers centralizados, o totalmente descentralizadas como *Ocean Protocol*. Los DIs pueden ofrecer servicios de valor agregado como seguridad, autenticación, prevención de fraude, anonimización o seudonimización, además de *regulatory compliance services*, o servicios de gestión de información personal. También es posible que los DIs no compartan ni

La definición del servicio de intermediación se confía al art. 2, inc. 11, Reglamento 2022/868, que expresa que consiste en un "*un servicio destinado a establecer, mediante medios técnicos, jurídicos o de otro tipo, relaciones comerciales con el fin de compartir datos entre un número indeterminado de interesados y titulares de datos, por una parte, y los usuarios de los datos, por otra, también para el ejercicio de los derechos de los interesados en relación con los datos personales*".

En suma, estos intermediarios facilitan el *intercambio de los datos* entre un número indeterminado de titulares de datos y los potenciales usuarios de estos. En otras palabras, recaban datos de una parte cedente (interesada en trasmitir) y los ceden a terceros receptores (interesados en adquirir); debiendo generar confianza en esta interactuación para el adecuado funcionamiento del *mercado de datos*.

Con este objetivo principal, deben:

– apoyar y fomentar las prácticas de intercambio voluntario de datos entre empresas;

– facilitar la aparición de nuevos ecosistemas basados en datos independientes de cualquier operador con un nivel importante de poder de mercado;

– posibilitar el acceso no discriminatorio a la economía de los datos para todas las empresas, independientemente de su tamaño, en particular, para las *PyMes* y las empresas emergentes con limitados medios financieros, jurídicos o administrativos.

A este respecto, se subordina la actividad de intermediación al cumplimiento de ciertos principios.

Por ejemplo:

Para garantizar que los interesados y los titulares de datos, así como los usuarios, tengan un mayor control sobre el acceso a sus datos y su utilización, se fomenta la elaboración de códigos de conducta a escala de la Unión Europea, en los que intervengan las partes interesadas. De este modo, independientemente de que el intercambio de datos tenga lugar entre empresas o entre una empresa y el consumidor, los proveedores de servicios de intermediación de datos deben ofrecer una forma novedosa de gobernanza que establezca una separación en la economía de los datos entre el suministro, la intermediación y la utilización.

Asimismo, los proveedores de servicios de intermediación deben ofrecer una infraestructura técnica específica para la interconexión de los interesados y los titulares de datos con los usuarios. A este respecto, reviste especial importancia configurar dicha infraestructura de tal manera que *las PyMes* y las empresas emergentes no encuentren obstáculos técnicos o de otro tipo para su participación en la economía de los datos.

---

manipulen datos, sino que simplemente ofrezcan una infraestructura tecnológica para interconectar a distintos sujetos y usuarios de datos. Los DIs también pueden ser *data marketplaces* – como AWS Data Exchange-, u orquestar ecosistemas de datos abiertos, como propone el considerando 32 de la Ley de Gobernanza de Datos (DGA) a través de las cooperativas de datos europeas como *Salus Coop, PolyPoly.coop, MIDATA*, etc (S. HEREDIA QUERRO, *Hacia un mercado europeo de datos: el nuevo régimen de los Intermediarios (neutrales) de Datos*, 15/01/2024, *opinión*, https://abogados.com.ar/hacia-un-mercado-europeo-de-datos-el-nuevo-regimen-de-los-intermediarios-neutrales-de-datos/34073).

Vemos algunos ejemplos de *intermediarios de datos* [18].

(i) Deutsche Telekom.

Con su Data Intelligence Hub, Deutsche Telekom ofrece un mercado de datos en el que las empresas pueden gestionar, proporcionar y monetizar de forma segura información de buena calidad, por ejemplo datos de producción, para optimizar procesos o cadenas de valor completas.

Telekom asume el papel de administrador neutral y garantiza la soberanía de los datos mediante una gestión descentralizada de los mismos. Actualmente, más de 1.000 usuarios de más de 100 empresas diferentes están activos en la plataforma.

(ii) Dawex.

Es una empresa francesa que se describe a sí misma como un "mercado global de datos". Dawex no compra ni vende datos, pero reúne a empresas interesadas en monetizar y reutilizar datos, y fomenta la transparencia entre proveedores y usuarios de datos garantizando que se comuniquen y realicen la transacción directamente en su plataforma.

Dawex desarrolló una serie de herramientas para ayudar tanto a los proveedores como a los usuarios de datos a comprender, evaluar y comunicarlos.

Las herramientas de visualización (por ejemplo, mapas de calor, mapas de árbol) brindan a los usuarios de datos información diferente sobre un conjunto de datos completo que se puede compartir de forma segura antes de que se complete una transacción. Las herramientas de muestreo generan automáticamente muestras de datos representativas basadas en algoritmos para evitar cualquier sesgo. Los usuarios y proveedores de datos se comunican mediante una herramienta de mensajería integrada en la plataforma.

Además, Dawex apoya la negociación del acuerdo contractual mediante términos modelo que pueden generarse automáticamente.

(iii) Api-Agro.

Es un centro de intercambio de datos agrícolas que utiliza la tecnología Dawex.

Esta tecnología fomenta un ecosistema agrícola que involucra a numerosos actores y un intermediario neutral (la plataforma Api-Agro) donde existe una clara separación entre el rol de intermediación y otras actividades relacionadas con el uso de los datos.

Api-Agro no monetiza los datos, sino que funciona como un tercero neutral que conecta a los titulares y usuarios de los datos.

3.2. Categorías de *intermediarios*.

Según el *Reglamento (UE) 2022/868*, los intermediarios de datos pueden categorizarse en las siguientes tres tipologías [19]:

---

[18] https://digital-strategy.ec.europa.eu/en/policies/data-governance-act-explained.

[19] D. POLETTI, *Gli intermediari dei dati*, 1 EJPLT, 2022, p. 45-56. DOI: https://doi.org/10.57230/EJPLT221DP.

i. *Prestadores de servicios de intermediación entre los "titulares de datos" y los potenciales "usuarios de datos"*.

Se prevé que puedan prestar sus servicios tanto en intercambios bilaterales como multilaterales o que, incluso, puedan crear plataformas o bases de datos que faciliten el intercambio y el uso común de los mismos.

Quedan incluidos los "*servicios de intermediación entre los titulares de datos y los usuarios de datos hipotéticos, incluida la puesta a disposición de medios técnicos o de otro tipo para permitir dichos servicios; que podrán incluir intercambios de datos bilaterales o multilaterales o la creación de plataformas o bases de datos que permitan el intercambio o el uso conjunto de los datos, así como el establecimiento de otra infraestructura específica para la interconexión de los titulares de datos con los usuarios de los mismos*".

Se trata de una tipología que sigue el modelo de los *data marketplaces*. Estos proveedores de servicios de intercambio de datos deben reducir los costes de transacción combinando fuentes de datos y conectando a usuarios y proveedores. Quedan excluidos de la definición los operadores que recogen datos de fuentes externas para ofrecer servicios, sin establecer una relación directa entre titulares y usuarios de los datos. Queda claro entonces que, este primer tipo de intermediario, se refiere a la relación entre los titulares de los datos y los usuarios de los datos.

ii. *Prestadores de servicios de intermediación entre los "interesados" que deseen facilitar sus datos personales o las personas humanas que deseen facilitar datos no personales y los potenciales "usuarios de datos"*.

Este es un aspecto novedoso y de gran interés jurídico. Se introduce así de forma expresa la posibilidad de que "interesados" pongan a disposición de terceros, incluidas empresas, sus datos personales – además de los no personales – para su intercambio. Concretamente, esta categoría es la de los proveedores de "*servicios de intermediación entre interesados que desean poner a disposición sus datos personales o personas físicas que desean poner a disposición datos no personales y usuarios potenciales de los datos, incluida la puesta a disposición de medios técnicos o de otro tipo para permitir dichos servicios, en particular permitiendo el ejercicio de los derechos de los interesados contemplados en el Reglamento (UE) 2016/679*" [20].

Incluye a los proveedores que ofrecen sus servicios a los interesados, que no deben tratar ni añadir valor a los datos, sino que tienen por objeto reforzar la capacidad de actuación de los interesados y, en particular, el control de los particulares sobre los datos que les conciernen. Estos proveedores ayudan a las personas en el ejercicio de sus derechos en virtud del *Reglamento General de Protección de Datos* ("RGPD") ya citado; en efecto, tienen la capacidad de gestionar la concesión y revocación del consentimiento para el tratamiento de datos, así como el ejercicio de los derechos reconocidos por el Reglamento.

---

[20] Del Parlamento Europeo y el Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

En este contexto, es importante que el modelo empresarial de dichos proveedores garantice que no existan incentivos no alineados que animen a las personas a utilizar dichos servicios para poner a disposición más datos sobre ellos de los que se encuentran en su propio interés.

Parece existir entre los prestadores de servicios y los interesados una relación jurídica de carácter fiduciario a la que se vincula la obligación para los primeros de actuar en el mejor interés de los segundos, garantizando que los datos tratados no se utilicen para fines distintos o ilícitos.

A primera vista, no está claro si este tipo de organizaciones coincide con (o más bien engloba) los sistemas de gestión de la información (los c.d. PIMS, *Personal Information Management Systems*[21]); que permiten a los interesados gestionar sus datos personales en sistemas de almacenamiento seguros, locales o en línea y com-

[21] El concepto PIMS ofrece un nuevo enfoque en el que los individuos son los "titulares" de su propia información personal. Los PIMS permiten a las personas gestionar sus datos personales en sistemas de almacenamiento seguros, locales o en línea y compartirlos cuando y con quién elijan. Los individuos podrían decidir qué servicios pueden utilizar sus datos y qué terceros pueden compartirlos. Esto permite un enfoque centrado en el ser humano de los datos personales y de los nuevos modelos de negocio, protegiendo contra técnicas ilegales de seguimiento y elaboración de perfiles que tienen como objetivo eludir los principios clave de protección de datos. Existe un interés creciente en nuestras "sociedades digitales" por saber cómo los individuos pueden controlar mejor sus datos personales. Una encuesta del Eurobarómetro de marzo de 2019 reveló que la mitad de los encuestados (51%) sentían que solo tenían un control parcial sobre la información que proporcionaban en línea, mientras que el 30% creía que no tenían ningún control. Sólo el 14% de los encuestados pensaba que tenía el control total. Una encuesta estadounidense de 2019 incluso mostró que el 80% de los encuestados sentían que no tenían el control de sus datos personales. En la Unión Europea, el artículo 8 de la Carta de la UE consagra la protección de los datos personales como un derecho fundamental de toda persona y el Reglamento General de Protección de Datos de la UE (RGPD) tiene como objetivo facultar a las personas para que tengan el control de sus datos. Para ello se necesitan herramientas y servicios prácticos y eficaces. Los datos personales se recopilan constantemente en el entorno digital, lo que lleva a que las personas dejen huellas digitales. El RGPD establece varios derechos de los interesados, como el derecho de acceso y rectificación de datos personales. Sin embargo, la arquitectura actual de los servicios de la sociedad de la información dificulta que las personas tengan control total sobre cómo se utilizan sus datos, quién debe tener acceso a ellos y cómo establecer restricciones y objeciones efectivas al procesamiento de datos. Una característica básica de un concepto común de PIMS es proporcionar control de acceso y un sendero de acceso. Los individuos, los proveedores de servicios y las aplicaciones necesitarían autenticarse para acceder a un centro de almacenamiento personal. Esto permite a las personas rastrear quién ha tenido acceso a su comportamiento digital. Las personas pueden personalizar qué categorías de datos quieren compartir y con quién. Otros elementos generalmente comunes de PIMS son el almacenamiento seguro de datos, las transferencias seguras de datos (transportar datos de forma segura entre sistemas y aplicaciones) y la interoperabilidad y portabilidad a nivel de datos. Hay varios ejemplos de iniciativas y proyectos que afirman tener funciones PIMS. *Nextcloud* permite a personas y organizaciones utilizar sus propios servicios en la nube para compartir archivos y servicios de colaboración, así como compartir archivos entre diferentes servidores de *Nextcloud*. Las personas pueden instalar el software gratuito y de código abierto o recibir el software como servicio (SaaS) de proveedores profesionales. Muchas universidades, gobiernos y empresas ya emplean *Nextcloud* (ver https://www.edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-32020-personal-information_en).

partirlos cuando lo deseen y con partes que consideren fiables, creando "espacios" para los datos personales.

iii. *Prestadores de servicios de cooperativas de datos*.

Su objetivo principal es brindar asistencia a *sus miembros* en el ejercicio de sus derechos con respecto a determinados datos; ofreciendo servicios de apoyo y asesoramiento.

Estas cooperativas buscan también reforzar la posición de las personas para que tomen decisiones informadas antes de dar su consentimiento al uso de los datos, influyendo en los términos y condiciones establecidas por las organizaciones de usuarios de datos, a las que está subordinada la utilización; convirtiéndose, en este sentido, en una herramienta útil para las empresas individuales, las microempresas y las *PyMes*.

Volveremos *infra* con un análisis particular de la *cooperativa de datos*.

3.3. Contornos del *servicio de intermediación de datos*.

En otro orden de cosas, otro de los enfoques novedosos para la regulación digital europea introducidos por este Reglamento, es que el servicio de intermediación de datos que se promueve aparece como un "intercambio disruptivo", regulando el concepto de "titular de datos", entendiendo como tal a toda persona jurídica (pública o privada) o persona humana que no sea el interesado con respecto al dato específico en cuestión que, de conformidad con la normativa de la UE o la legislación nacional aplicable, "*tenga derecho a conceder acceso a determinados datos personales o no personales o a compartirlos*". Se trata, por tanto, de un concepto que reconoce a esa persona humana o jurídica determinadas facultades de decisión y explotación sobre los datos, abriendo distintas posibilidades sobre las facultades de disposición e, inclusive, sobre el reconocimiento de derechos relativos a la propiedad de los datos.

Como se expresó anteriormente, el marco de gobernanza de datos generado por la UE tiene como fin prioritario el de generar confianza entre los particulares y las empresas en relación con el acceso a los datos, su control, intercambio, utilización y reutilización. Precisamente, para contribuir a aumentar dicha confianza en la figura de los *prestadores de servicios de intercambio*, el Reglamento fija requisitos y deberes fiduciarios significativos para que estos prestadores puedan iniciar y desarrollar su actividad. Cuanto mayor sea la transparencia, seguridad y proporcionalidad en la actividad de estos intermediarios, la UE considera que se aumentará la confianza y se incrementará el mercado europeo y el intercambio de datos.

Entre los requisitos y condiciones que se exigen, se encuentran los siguientes:

la obligación de identificarse y notificar su actividad a la autoridad competente que le corresponda

la prohibición de que utilicen los datos – cuya intermediación promueven – para fines diferentes de su "puesta a disposición" a favor de terceros. No pueden, por

tanto, explotar los datos a los que accedan para "fines personales" distintos de la propia intermediación [22]

también se les exige intercambiar los datos en el mismo formato en el que los reciban, permitiéndoles únicamente adaptarlos a formatos específicos con el fin de mejorar su interoperabilidad, con lo que se excluye la posibilidad de que los intermediarios ejecuten tareas tales como la "consultoría" sobre los datos como parte de esta actividad.

A mayor abundamiento, entre otros diversos requisitos que impone la Reglamentación a los *prestadores del servicio*, se encuentran los siguientes:

---

[22] El profesor Fabio Bravo explica la importancia de la "*finalità esclusiva, neutralità, separazione strutturale nella fornitura dei servizi*", al referirse al "*fornitori del servizio di condivisione dei dati*" en el *GDPR (Reglamento UE 2016/679)*. En tal sentido, expresa: "*Per arginare rischi di abusi da parte dell'infomediario, che sarebbero drasticamente lesivi non solo dei diritti fondamentali dell'interessato, ma – nella prospettiva del legislatore europeo – soprattutto di quella fiducia considerata necessaria per la realizzazione del mercato dei dati, occorre che all'intermediario sia preclusa la facoltà di utilizzare i dati per fini diversi ed ulteriori da quelli concernenti il servizio di condivisione dei dati. Così il considerando n. 26 rimarca che «Un elemento essenziale per infondere fiducia e garantire maggiore controllo ai titolari e agli utenti dei dati nei servizi di condivisione dei dati è la neutralità dei fornitori del servizio di condivisione dei dati riguardo ai dati scambiati tra titolari e utenti dei dati. È pertanto necessario che i fornitori di servizi di condivisione dei dati agiscano solo in qualità di intermediari nelle transazioni e non utilizzino per nessun altro fine i dati scambiati (...)». La riferita neutralità comporta una necessaria «separazione strutturale tra il servizio di condivisione dei dati e qualsiasi altro servizio fornito, in modo tale da evitare problemi di conflitto di interessi. Ciò significa che il servizio di condivisione dei dati dovrebbe essere fornito mediante un'entità giuridica distinta dalle altre attività di tale fornitore di servizio di condivisione dei dati. I fornitori di servizi di condivisione dei dati che agiscono da intermediari tra i singoli individui, quali i titolari dei dati, e le persone giuridiche dovrebbero inoltre avere l'obbligo fiduciario nei confronti dei singoli individui di garantire che agiscono nel migliore interesse dei titolari dei dati»*". En castellano: "*Para limitar los riesgos de abusos por parte de los infomediario, que serían drásticamente perjudiciales no solo para los derechos fundamentales del interesado, sino también – desde la perspectiva del legislador europeo – con respecto a la confianza que se considera necesaria para la realización del mercado de datos, debe prohibirse al intermediario el uso de los datos para fines distintos de los relacionados con el servicio de intercambio de datos. Así, el considerando nro. 26 señala que «Un elemento esencial para infundir confianza y garantizar un mayor control a los titulares y usuarios de datos en los servicios de intercambio de datos es la neutralidad de los proveedores de servicios de intercambio de datos respecto a los datos intercambiados entre los titulares y los usuarios de los datos. Por consiguiente, los proveedores de servicios de intercambio de datos deben actuar únicamente como intermediarios en las transacciones y no utilizar los datos intercambiados para ningún otro fin (...)». La neutralidad mencionada implica una separación estructural necesaria entre el servicio de intercambio de datos y cualquier otro servicio prestado, con el fin de evitar conflictos de intereses. Esto significa que el servicio de intercambio de datos debería prestarse a través de una entidad jurídica distinta de las demás actividades de dicho proveedor de servicios de intercambio de datos. Los proveedores de servicios de intercambio de datos que actúan como intermediarios entre las personas, como los titulares de datos, y las personas jurídicas también deben tener la obligación fiduciaria frente a los particulares de garantizar que actúan en el mejor interés de los titulares de datos»*" (F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in *Contratto e impresa Europa*, 2021, 1, pp. 245-246).

– el acceso a sus servicios y sus precios deben ser equitativos, transparentes y no discriminatorios,

– deben disponer de procedimientos de detección de prácticas fraudulentas o abusivas.

También se impone a los Estados miembros de la UE el deber de designar autoridades nacionales específicas de supervisión de estos prestadores, con facultades de suspender o hacer cesar su actividad e, incluso, imponerles sanciones.

Finalmente, cabe agregar que la UE ha creado un *Registro de servicios de intermediación de datos*. El mismo se puede consultar en https://digital-strategy.ec.europa.eu/es/policies/data-intermediary-services.

Este registro de servicios de intermediación de datos de la UE se ha establecido en el marco de la Ley de Gobernanza de Datos (DGA), como un pilar clave de la estrategia europea de datos que establece un marco de gobernanza para promover la confianza en el intercambio de datos entre individuos y empresas.

Se debe tener en cuenta que:

– los intermediarios de datos funcionarán como terceros neutrales que conectan a individuos y empresas con usuarios de datos;

– si bien pueden cobrar por facilitar el intercambio de datos entre las partes, no pueden utilizar directamente los datos que intermedian para obtener beneficios financieros (por ejemplo, vendiéndolos a otra empresa o utilizándolos para desarrollar su propio producto sobre la base de estos datos);

– los intermediarios de datos deberán cumplir requisitos estrictos para garantizar esta neutralidad y evitar conflictos de intereses.

En la práctica, esto significa que habrá una separación estructural entre el servicio de intermediación de datos y cualquier otro servicio prestado (es decir, deben estar separados legalmente). Además, las condiciones comerciales (incluidos los precios) para la prestación de servicios de intermediación no deben depender de si un titular potencial de datos o un usuario de datos está utilizando otros servicios. Los datos y metadatos adquiridos solo pueden utilizarse para mejorar el servicio de intermediación de datos.

La página web citada mantiene un registro público de todos los proveedores de servicios de intermediación de datos que ofrecen sus servicios en la Unión Europea, indicándose los países donde están registrados.

Por ejemplo:

(i) Dataspace Europe OY (Finlandia) [23];

(ii) NIDHAS Adatközvetítő Korlátolt Felelősség, Társaság (Hungría) [24].

[23] https://ec.europa.eu/newsroom/dae/redirection/document/101189.

[24] https://ec.europa.eu/newsroom/dae/redirection/document/104469.

4. La cooperativa de datos.

4.1. Punto de partida: ¿Por qué una "cooperativa" de datos?

Sin duda alguna, la respuesta se vincula al concepto mismo de *cooperativismo*.

El cooperativismo es un movimiento social que define la cooperación de sus miembros en el ámbito económico y social como un medio para lograr que sus asociados, integrados en asociaciones voluntarias que se denominan cooperativas, obtengan mayores beneficios para satisfacer sus necesidades.

El movimiento cooperativo es ahora una fuerza económica que extiende sus intereses a las personas de menores recursos, promoviendo la inclusión financiera de estos, lo que crea oportunidades para el desarrollo social, económico y ambiental.

El cooperativismo no tiene ánimo de lucro y es muy importante para todos los países ya que fomenta la participación de las personas de todos los niveles económicos en la creación de una economía sana.

Entre las características del cooperativismo, cabe destacar las siguientes:

– impulsa el apoyo mutuo entre asociados;
– facilita la igualdad entre los asociados;
– promueve la solidaridad entre los participantes;
– estimula el esfuerzo individual y la motivación compartida;
– permite un sistema democrático y justo;
– fortalece la responsabilidad social y con el medio ambiente;
– facilita la definición de metas y objetivos comunes entre los cooperativistas.

Aplicados estos conceptos a la temática de la "administración de los datos", permite afirmar que la idea de una "cooperativa de datos" se traduce en una estructura organizacional formada por trabajadores, consumidores o entidades que en conjunto deciden fundarla para tener la disposición y control compartidos de los datos y gestionarlos democráticamente para servir a los miembros de la cooperativa y a la propia comunidad.

Por lo tanto, una cooperativa de datos es una empresa caracterizada por la *gobernanza* democrática de los datos, en la que el uso de tecnologías digitales apoya el consumo, el intercambio entre pares y la producción de bienes y servicios dentro de una comunidad, y maximiza la generación y distribución de valor dentro de la misma; centrándose básicamente en las necesidades de los miembros.

En estos términos, queda claro cómo una cooperativa de datos aparece como un instrumento idóneo para la *provisión del servicio de intercambio de datos*. En efecto, su objetivo es ayudar a las pequeñas empresas y a los empresarios individuales a acceder o procesar grandes cantidades de datos, garantizar *una gobernanza* participativa compartida entre empresas y empresarios en su gestión – es decir, entre "contribuyentes", usuarios y beneficiarios-, negociar los términos y condiciones para el procesamiento de datos, tomar decisiones informadas sobre su uso y resolver disputas entre múltiples usuarios de los mismos datos.

Por último, la estructura cooperativa aparece como una alternativa óptima para

compartir los costos del mantenimiento y gestión de datos, las tecnologías, etc.; en beneficio de sus miembros.

Ejemplificamos, sintéticamente, con dos casos.

Por un lado, una importante cooperativa de datos que existe hoy en día es la Cooperativa Europea de Datos (EDC)[25], que es el punto de entrada único para miles de datos sobre recaudación de fondos, inversiones y desinversiones. En este caso específico, el uso de una plataforma con una metodología estandarizada permite obtener estadísticas paneuropeas coherentes y comparables útiles para informar mejor a los gestores de fondos, inversores, políticos, reguladores y otras *partes interesadas*.

Por el otro, siempre con el objetivo de lograr una mejor comprensión acerca de cómo funciona el "modelo cooperativo" aplicado al manejo de datos, cabe contrastarlo con el "modelo capitalista".

Para ello utilizaremos un ejemplo que da Fabio Bravo con respecto a una particular cooperativa de datos: *Driver's Seat.* En este sentido, explica el profesor italiano: "*Entre las diferentes cooperativas de datos, presentes en diferentes sectores (por ejemplo, el de la salud, los transportes, la agricultura, la gig economy), se señala «Driver's Seat», una "data cooperativa" americana que opera en el sector de los transportes, con servicios de "ride-sharing" (análogos al modelo Uber) y de "delivering" a través de riders (análogos al modelo Glovo o Deliveroo), gestionados sin embargo en forma de cooperativa, según las lógicas mutualistas, y no según el modelo capitalista tradicional. Los miembros de las cooperativas de datos utilizan una aplicación específica, con la que ejercen el control sobre los datos generados en la prestación del servicio, determinando si los comparten y cuándo. Los datos recopilados se analizan a partir de la información cooperativa de la que forman parte, con el fin de maximizar el beneficio para los miembros, con el fin de aprovechar los datos en su beneficio, en términos monetarios y no monetarios. Mientras que en los modelos capitalistas los análisis de los datos relativos a la prestación del servicio (de ride-sharing, de food-delivering, etc.) se realizan en beneficio de la misma sociedad que desarrolla actividades de empresa, con el fin de hacer más eficiente el proceso de producción y maximizar los beneficios, con resultados que a menudo perjudican a los trabajadores, en el modelo mutualista, el análisis de los datos recogidos en el ejercicio de la actividad se realiza esencialmente en favor del trabajador individual, así como de la propia cooperativa y de terceros. El trabajador – por ejemplo – podrá beneficiarse del análisis de los datos generados por el sistema para aumentar en su propio beneficio la eficiencia en la*

[25] La Cooperativa Europea de Datos (EDC) es una iniciativa conjunta desarrollada por *Invest Europe* y sus socios de asociación nacionales para recopilar datos de la industria a nivel europeo sobre la actividad (recaudación de fondos, inversiones y desinversiones) y el impacto económico (empleo, volumen de negocios, EBITDA y CAPEX). La plataforma EDC es propiedad y está gestionada conjuntamente por las asociaciones de capital privado y de capital riesgo de Europa. Es la base de datos más completa de las estadísticas europeas de capital privado y capital riesgo.

prestación del servicio, identificando las franjas horarias más rentables, las rutas más rentables y las formas más rentables de remuneración (en el transporte de personas o bienes, por ejemplo, si es más ventajosa la remuneración calculada en función del tiempo empleado o de la distancia recorrida), etc. También podrá valorizar en términos monetarios los datos si, a través de la cooperativa, se conceden (en forma agregada) a terceros, públicos o privados" [26].

4.2. La *cooperativa de datos* y el Reglamento 2022/868.

El Reglamento 2022/868, en su art. 2 inciso 15, define a la cooperativa de datos en tanto intermediario *como* "*aquella estructura organizativa constituida por interesados, empresas unipersonales o pymes pertenecientes a dicha estructura, cuyos objetivos principales sean prestar asistencia a sus miembros en el ejercicio de los derechos de estos con respecto a determinados datos, incluida la asistencia por lo que respecta a la adopción de decisiones informadas antes de consentir el tratamiento de datos, intercambiar opiniones sobre los fines del tratamiento de datos y las condiciones que mejor representen los intereses de sus miembros en relación con los datos de estos, y negociar las condiciones contractuales para el tratamiento de datos en nombre de sus miembros antes de conceder permiso para el tratamiento de datos no personales o antes de dar su consentimiento para el tratamiento de datos personales*".

---

[26] "*Tra le diverse cooperative di dati, presenti in diversi settori (tra cui, ad esempio, quello della salute, dei trasporti, dell'agricoltura, della gig economy), si segnala «Driver's Seat», una data coopeative americana operante nel settore dei trasporti, con servizi di "ride-sharing" (analoghi al modello Uber) e di "delivering" tramite riders (analoghi al modello Glovo o Deliveroo), gestiti tuttavia in forma di cooperativa, secondo le logiche mutualistiche, e non secondo il modello capitalistico tradizionale. I members della data cooperative utilizzano un'app specifica, con cui esercitano il controllo sui dati generati nella fornitura del servizio, stabilendo se e quando metterli in condivisione. I dati raccolti sono poi analizzati dalla data cooperative di cui fanno parte, al fine di massimizzare il vantaggio per i members, nell'ottica di una valorizzazione dei dati medesimi a loro vantaggio, in termini monetari e non. Mentre nei modelli capitalistici le analisi dei dati relativi alla fornitura del servizio (di ride-sharing, di food-delivering, et similia) vengono effettuate a vantaggio della società stesa che svolge attività di impresa, al fine di rendere il processo produttivo più efficiente e di massimizzare il profitto, con risultati che spesso sono a discapito dei lavoratori, nel modello mutualistico l'analisi dei dati raccolti nello svolgimento dell'attività viene svolta essenzialmente a favore del singolo lavoratore, oltre che della cooperativa medesima e dei soggetti terzi. Il lavoratore – ad esempio – potrà giovarsi dell'analisi dei dati generati dal sistema per incrementare a proprio vantaggio l'efficienza nella fornitura del servizio, individuando le fasce orare più redditizie, i percorsi più redditizi e le modalità più redditizie di remunerazione (nel trasposto di persone o cose, ad esempio, se sia più vantaggiosa la remunerazione calcolata in base al tempo impiegato o alla distanza percorsa), etc. Potrà anche valorizzare in termini monetari i dati qualora, tramite la cooperativa, siano concessi (in forma aggregata) a soggetti terzi, pubblici o privati*" (F. BRAVO, *Le cooperative di dati*, in *Contratto e impresa*, 2023, 3, p. 757 ss., y in *Progetto di terza missione*, *Cooperative di dati*, Università di Bologna, Saggi, pp. 13 y 14 – https://site.unibo.it/cooperative-di-dati/it/attivita-di-ricerca/pubblicazioni).

A su turno, el considerando 31 del mismo Reglamento 2022/868 expresa que: "*Las cooperativas de datos tratan de alcanzar varios objetivos, en particular, reforzar la capacidad de las personas para que tomen decisiones con conocimiento de causa antes de dar su consentimiento a la utilización de los datos, influyendo en las condiciones contractuales de las organizaciones usuarias de datos en relación con la utilización de los datos de tal manera que se proporcionen mejores opciones a los distintos miembros del grupo o, en su caso, encontrando soluciones a las posiciones en conflicto de los miembros de un grupo sobre la manera de utilizar los datos cuando estos atañen a varios interesados de ese grupo*".

La transformación digital que se avecina en los distintos sectores de la actividad económica se basará en una utilización intensiva de datos específicos y rigurosos.

La masa crítica de información necesaria sólo se alcanzará si todos los agentes participan de una forma consciente y voluntaria. Deben estar convencidos en que el aprovechamiento de los datos va a ser muy positivo para el sector de que se trate y que los beneficios que se generen repercutirán de forma proporcional a los distintos eslabones y agentes que lo componen.

Las instituciones de datos son organizaciones que administran datos en nombre de otros, a menudo con fines públicos, educativos o benéficos. Por ello, la "administración de datos" no es cuestión menor y se vincula fuertemente no solo con la toma de decisiones, sino también con respecto a cuestiones colaterales, no menos importantes, tales como 1). – quién tiene acceso a los datos, 2). – con qué fines y 3). – en beneficio de quién.

Solo así se comprende el valor y se limita el daño que la divulgación o compartición de los datos pueden ocasionar.

En este contexto, la cooperativa de datos – como una de las opciones en el servicio de intermediación – aparece como una interesante alternativa desde que importa la aplicación del *modelo cooperativo* a un ámbito tan sensible como es el *manejo de los datos*.

Es que, el modelo cooperativo, permite generar confianza al promover la colaboración entre sus *miembros* acerca de la compartición y el uso de los datos que los ayude a tomar las mejores decisiones posibles, dentro de un marco de seguridad.

En efecto, pensar en un *modelo cooperativo de recopilación y tratamiento de datos*, permite compartir entre sus miembros información propia con la de otros miembros – vinculados a la misma o similar actividad, empresarial o no – e inclusive, con fuentes externas, que posibilite optimizar la toma de decisiones, en función de los datos almacenados.

El modelo cooperativo aparece, sin duda alguna, como instrumento eficaz en este sentido basado, repetimos, en la confianza de sus integrantes.

De esta manera la *cooperativa,* como estructura organizacional, tiene una indudable utilidad práctica en la *intermediación de datos* toda vez que:

– empodera a los individuos dándoles el control sobre los datos que comparten y monetizando efectivamente esos mismos datos. Volveremos más adelante sobre este último aspecto;

– a través de estos controles, las cooperativas de datos establecen un ecosistema de confianza;

– la asignación efectiva de los ingresos de una cooperativa de datos entre sus miembros, aunque es un reto, es primordial para la ampliación y el mantenimiento de la propia cooperativa. En efecto, al agregar los datos individuales, una cooperativa mejora su poder de negociación y puede obtener un mejor precio por los datos agrupados;

– aparece como un esquema eficaz de asignación de ingresos al estilo *Robin-Hood* que compensa a los "pobres en privacidad" a expensas de los "ricos en privacidad" [27]; concepto que también desarrollaremos *infra*;

– finalmente, como intermediario en el servicio de datos, la cooperativa puede encontrar soluciones comunes sobre cómo se utilizan, cuando hay posiciones opuestas dentro de un mismo grupo [28].

Dicho esto, y así como existen las *cooperativas de consumo* – que se forman para adquirir o producir por cuenta de la cooperativa, artículos de consumo de uso personal y del hogar para ser distribuidos entre los asociados – o las *cooperativas de trabajo* – que agrupan a trabajadores manuales o intelectuales, quienes aportan su trabajo o profesión para la realización de actividades económicas, con el objeto de proveerles fuentes permanentes de trabajo y distribuir los excedentes entre sus asociados –; cabe preguntarse:

¿Por qué no aplicar el modelo cooperativo a los datos como mecanismo de generación de valor estratégico para que sus miembros optimicen las decisiones que deben tomar?

La respuesta afirmativa se impone [29].

---

[27] https://es.weforum.org/agenda/2022/02/la-clave-para-disenar-cooperativas-de-datos-sostenibles/.

[28] Data Governance Act: le regole per il mercato interno dei dati, Associazione fra le società italiane per azioni, Approfondimenti, N. 4 del 2022, http://www.assonime.it/, https://www.astrid-online.it/static/upload/appr/approfondimenti-4-2022.pdf.

[29] Especialmente para Italia, en virtud de lo dispuesto por el art. 45 de su Constitución, que expresa: "*La República reconoce la función social de la cooperación de carácter mutualista y sin finalidad de especulación privada. La Ley promueve y favorece el aumento de la misma con los medios más adecuados y asegura, a través de los controles oportunos, su carácter y sus finalidades. La Ley provee a la protección y al desarrollo del artesanado*". En tal sentido explica Luca Petrone: "*La cooperativa, come modello societario, infatti, risponde a principi diversi rispetto alle altre società di capitali. E questa diversità viene legittimata a livello costituzionale dall'art. 45, attraverso il quale viene espressamente disposto che «la Repubblica riconosce la funzione sociale della cooperazione a carattere di mutualità e senza fini di speculazione privata. La legge ne promuove e favorisce l'incremento con i mezzi più idonei e ne assicura, con gli opportuni controlli, il carattere e le finalità». Il favore costituzionale per la cooperazione è dovuto essenzialmente a due ragioni, ossia la tutela delle posizioni economicamente deboli e l'articolazione e diffusione del potere economico che tale modello societario consente, traducendo sul terreno economico i principi di democraticità, uguaglianza e solidarietà che sono alla base del nostro ordinamento giuridico30. Modello, questo, antitetico rispetto a quello adottato da quegli operatori economici che fanno del trattamento del dato il relativo core business con logiche spiccatamente capitalistiche*" (L. Petrone, *Il mercato digitale europeo e le coope-*

La disponibilidad de cantidades masivas de datos de los consumidores – una consecuencia ineludible de la economía digital-, junto con el rápido desarrollo de métodos para explotarlos con el fin de tomar decisiones empresariales inteligentes, ha impulsado la innovación no sólo en la forma en que las empresas realizan sus negocios, *sino también en la manera de recopilar los datos*.

En los últimos años se ha observado un creciente interés por las cooperativas de datos, también conocidas como una de las especies de *instituciones de datos ascendentes* [30], que recopilan datos compartidos voluntariamente por miembros individuales y monetizan los datos agrupados en beneficio de toda la comunidad de miembros.

---

rative di dati, in *Contratto e impresa*, 2023, 3, p. 800 ss. y in *Progetto di terza missione*, *Cooperative di dati*, Saggi, Università di Bologna, p. 11, https://site.unibo.it/cooperative-di-dati/it/attivita-di-ricerca/pubblicazioni). En castellano: "*La cooperativa, como modelo societario, responde a principios diferentes a los de otras sociedades de capital. Y esta diversidad está legitimada constitucionalmente por el art. 45, mediante el cual se establece expresamente que «la República reconoce la función social de la cooperación con carácter de mutualidad y sin fines de especulación privada. La ley promoverá y favorecerá su incremento por los medios más idóneos y garantizará, con los controles oportunos, su carácter y su finalidad». El apoyo constitucional a la cooperación se debe esencialmente a dos razones, a saber, la protección de las posiciones económicamente débiles y la articulación y difusión del poder económico que permite este modelo de sociedad, traduciendo en el terreno económico los principios de democracia, igualdad y solidaridad que son la base de nuestro ordenamiento jurídico. Modelo, este, antitético respecto al adoptado por aquellos operadores económicos que hacen del tratamiento del dato el relativo core business con lógicas marcadamente capitalistas*".

[30] La mayoría de las organizaciones tienen procesos de gobernanza de datos (formas de tomar decisiones sobre los datos que recopilan y conservan). Sin embargo, hay instituciones que tienen procesos que permiten a las personas (generalmente aquellas que han generado los datos o a quienes se refieren los datos) participar activamente en esos procesos de gobernanza de datos. En este sentido se habla de "*instituciones de datos ascendentes*" como aquellas que se vinculan especialmente con el hecho de incluir a las personas en la toma de decisiones. Muchas de estas instituciones de datos son el resultado de iniciativas comunitarias, una institución de datos creada por un gobierno, una empresa o una gran organización filantrópica que permitiera a las personas participar activamente en la toma de decisiones también se consideraría una institución de datos ascendente. La cooperativa "Swash" – que veremos más adelante en este trabajo – emplea la toma de decisiones delegada en torno a los datos en su esfuerzo por construir una 'economía digital nueva, más justa y más equilibrada'. Después de descargar la extensión del navegador Swash, los usuarios pueden definir individualmente: qué datos se recopilan sobre ellos y sus hábitos de navegación, quién los recopila, el nivel de transformación para preservar la privacidad que se aplica a esos datos y su nivel preferido de anonimato. Posteriormente, Swash "trabaja en segundo plano" para recopilar, agregar y vender datos en "Streamer Marketplace" y distribuir las ganancias entre sus miembros. De igual manera, la cooperativa "Driver's Seat" – que vemos también más adelante en este monografía-, al descargar la aplicación, los conductores de la economía colaborativa pueden decidir individualmente combinar sus datos de conducción con datos de otros conductores para obtener información valiosa. Luego, Driver's Seat trabaja para vender estos datos a agencias municipales en nombre de los conductores y distribuye las ganancias entre los miembros (https://theodi.org/news-and-events/blog/what-are-bottom-up-data-institutions-and-how-do-they-empower-people/).

En este último sentido, o sea, *la monetización de los datos*, cabe decir que un sistema de asignación de ingresos determina cómo se deben distribuir los ingresos monetizados entre los miembros de la cooperativa. La aplicación de un sistema eficaz es fundamental para su mantenimiento, ya que genera un círculo virtuoso beneficioso. Crea incentivos para que los miembros compartan datos de alta calidad, lo que a su vez da lugar a datos agregados de alta calidad; esto aumenta el valor de mercado de los datos agrupados y, por tanto, los ingresos de la cooperativa, lo que en última instancia se traduce en una mejor compensación para los miembros.

Para diseñar un sistema eficaz de asignación de ingresos, las cooperativas deben tener en cuenta las contribuciones de datos de los miembros individuales, cuestión que depende tanto de la calidad como de la cantidad de los datos compartidos.

También son importantes los incentivos económicos de los socios para participar y compartir datos útiles y de alta calidad.

Por otro lado, los incentivos de los miembros para compartir datos dependen, a su vez, del esquema de asignación de ingresos empleado por la cooperativa. Si la compensación proporcionada por un esquema es considerada poco atractiva por los miembros, entonces naturalmente se abstendrán de compartir datos. Además, para que una cooperativa sea sostenible, una característica deseable de un esquema de asignación es que no cree incentivos perversos para que los miembros se separen y formen grupos más pequeños [31].

En cuanto a los esquemas de asignación de ingresos, un esquema intuitivo y natural consiste en distribuir los ingresos totales de la cooperativa entre sus miembros en proporción a su aportación individual de datos. Aunque este esquema es atractivo y aparentemente justo, no siempre es eficaz, ya que, en primer lugar, no tiene en cuenta la sensibilidad de los miembros a la hora de compartir sus datos y, en segundo lugar, no ofrece suficientes incentivos a los miembros que tienen una sensibilidad relativamente alta a la privacidad.

El diseño de un sistema eficaz requiere ajustes de tipo *Robin-Hood* en la compensación a los miembros. Es decir, el sistema debe proporcionar un trato preferente a los miembros "pobres en privacidad", como los que son muy sensibles a la privacidad, a expensas de los miembros "ricos en privacidad". Sin embargo, este trato no puede ser demasiado desigual, ya que podría resultar gravoso en la medida en que los miembros ricos en privacidad decidan separarse de la cooperativa.

Como institución, las cooperativas de datos son atractivas porque ofrecen datos frescos de los consumidores obtenidos de forma abierta, no discriminatoria y respetando la privacidad, tras compensar debidamente a los miembros. Un esquema atractivo de asignación de ingresos es la columna vertebral de una cooperativa de datos próspera y la clave para ayudarla a desarrollar todo su potencial [32].

Por último, existe otra ventaja en la utilización del *modelo cooperativo* vincula-

[31] https://es.weforum.org/agenda/2022/02/la-clave-para-disenar-cooperativas-de-datos-sostenibles/.

[32] https://es.weforum.org/agenda/2022/02/la-clave-para-disenar-cooperativas-de-datos-sostenibles/.

do a la *manera en que se gestionan los datos*. En efecto, en vez depender de un tercero – que puede ser una gran corporación multinacional que "manipula", "controla" o "vende" abusivamente los datos que suministra –, en el caso de la cooperativa, se depende de una estructura organizada sobre la base de la solidaridad de sus miembros; quienes comparten la información recopilada, que ha sido proporcionada por los propios integrantes.

Conforme a lo expuesto, se puede apreciar cómo, la cooperativa, aparece como un instrumento idóneo para recuperar el control de una materia prima – el dato – que se ha convertido en los tiempos que vivimos en el ingrediente clave para los nuevos negocios.

Veamos algunos ejemplos de cooperativa de datos para comprender la lógica de funcionamiento de este particular *intermediario del servicio de intercambio de datos*.

(i) *Salus.Coop.*

En el ámbito de la salud es el caso de *SALUS.COOP*, una cooperativa de donantes de datos para la investigación para el Bien Común.

Se lee en la web de esta cooperativa [33] que "*la investigación nos permite generar información que una vez analizada se convierte en la evidencia necesaria para la toma de decisiones. Desde Salus.Coop impulsamos la investigación como vehículo de transformación social. Los datos son el nuevo patrimonio personal y social. El uso que hacemos es determinante a la hora de dibujar el mapa de la realidad que nos rodea. Por eso desde Salus.Coop trabajamos cada día para garantizar el anonimato y el impacto social positivo de los proyectos a los que nutren. A través de la App Salus.Coop conectamos donantes e investigadores de forma segura: el control es del donante, los datos son anónimos y el recercaire sólo accede a lo que se indica en el acuerdo, que es sencillo y transparente*".

En definitiva, *Salus.coop* tiene como objetivo legitimar los derechos de los ciudadanos a controlar sus propios registros de salud, al tiempo que facilita el intercambio de datos para acelerar la innovación en la investigación en salud.

Parte de la premisa según la cual, el futuro de la salud depende significativamente del potencial de combinar, integrar y compartir datos de salud de diferentes fuentes. Sin embargo, la decisión de compartir los datos requiere medir muchos riesgos, que incluyen la privacidad, la seguridad e incluso el posible mal uso de los mismos.

Cabe preguntarse, entonces, ¿En quién confiamos para hacer estos juicios?

Aunque los ciudadanos europeos poseen legalmente sus datos sanitarios, en la práctica – a menudo – no pueden acceder a ellos ni controlar su uso. Esto está obstaculizando la innovación en la asistencia sanitaria y ralentizando la investigación.

Ante este escenario aparece *Salus.Coop*.

(ii) *Polypoly.*

[33] https://www.salus.coop/intercooperacio/.

Otro tanto ocurre con *Polypoly*[34]. Se trata de un sistema económico revolucionario para datos cuya estructura descentralizada garantiza el uso justo de los datos sin infringir los derechos de ningún usuario. La tecnología central que hace esto posible es el PolyPod. La computación perimetral y el principio de descentralización que la acompaña son los aspectos clave del polyPod. Todo esto, combinado, crea un modelo altamente escalable, seguro y rentable.

Para que la Internet de las cosas sea sostenible se necesitan bases sólidas: el PolyPod garantiza que los datos nunca tengan que salir del dispositivo portátil, reloj inteligente, automóvil u otro dispositivo IoT que captura datos en primer lugar.

Pensar en este nuevo paradigma permite a los desarrolladores crear funciones sobre el PolyPod con la ayuda de bloques de construcción simples.

Por último, pero no menos importante, esto también significa beneficio mutuo para las empresas, que pueden reducir significativamente los costos de almacenamiento y eliminar los que han surgido como resultado del *RGPD*, sin mencionar el riesgo de una violación de datos. Al mismo tiempo, se generan conocimientos de datos de mayor calidad, procedentes de clientes que no tienen que ceder sus datos.

Así es como se ve un intercambio de datos rentable con un usuario de PolyPod.

Ahora bien, con el fin de potenciar la visión impulsada con el propósito de inventar un nuevo sistema económico para datos, aparece otro concepto: el *PolyVerse* o *Poliverso*, el cual se compone de tres entidades: La Fundación, La Empresa y La Cooperativa. Las tres entidades cumplen una función diferente, pero están conectadas para garantizar que el equilibrio de intereses combinados contribuya a construir una economía de datos que sea eficiente, compatible con la privacidad y sostenible.

Polypoly Enterprise se centra en los intereses económicos y los requisitos de la economía, Polypoly Foundation se centra en los requisitos gubernamentales y un marco regulatorio para el uso justo de los datos. La Cooperativa Polypoly está centrada en los ciudadanos y representa sus intereses, especialmente en lo que respecta a la riqueza generada a partir de sus datos. Las tres entidades cumplen una función diferente, pero la combinación garantiza que el equilibrio nunca se incline a favor de los intereses de un grupo en particular. Las tres entidades se controlan mutuamente para asegurarse de que el equilibrio de poder se distribuya equitativamente.

Polypoly Enterprise: crea soluciones para emprendedores. Los modelos de negocio digitales exitosos se basan en datos. Actualmente, Europa está perdiendo su capital de datos a manos de monopolios extranjeros y las empresas europeas son dependientes y se ven privadas gradualmente de acceso a modelos de negocio que impulsan la economía digital. La solución: una economía de datos descentralizada. La cooperativa Polypoly proporciona la base técnica: el PolyPod. Desarrolla herramientas y productos para una fácil transición a una economía de datos descentralizada. Los empresarios podrán liberarse de los monopolios de datos, protegiendo así sus modelos existentes y construyendo nuevos modelos digitales.

Fundación Polypoly: comprende las necesidades de los funcionarios públicos.

[34] https://www.eu-startups.com/directory/polypoly-2/.

Europa también está perdiendo su capital de datos a manos de monopolios extranjeros. Como resultado, las empresas europeas quedan aisladas de sus clientes. La privacidad de los datos de los ciudadanos está desprotegida y los Estados europeos están perdiendo el dinero de los contribuyentes. De esta manera, se ayuda a los gobiernos a construir una economía de datos descentralizada para Europa. La infraestructura técnica la proporciona una cooperativa de ciudadanos europeos que utilizan el PolyPod. El *RGPD* está incluido en su código. El PolyPod protege eficazmente a los ciudadanos europeos y libera a las empresas europeas de la dependencia de los monopolios de datos. De ello se deduce que los impuestos sobre las ganancias generadas por el capital de datos europeo se devuelven a Europa.

Cooperativa Polypoly: Representa los intereses de todos los ciudadanos. La idea central de toda cooperativa es lograr unirlos. Desde esta óptica se persigue una suerte de "soberanía" sobre los datos. A tal efecto, se desarrolla la base técnica para una economía de datos descentralizada: el PolyPod, que pertenece a todos los miembros de la Cooperativa. El PolyPod está disponible para todos los ciudadanos, permitiéndoles reclamar la soberanía de sus datos. El PolyPod almacena los datos de los usuarios en sus dispositivos finales personales, de los que nunca sale. Los ciudadanos pueden elegir, de esta manera, cómo poner a disposición sus datos, ya sea como donación o en alquiler. Si se intercambia dinero, la cooperativa recibe un pequeño porcentaje que se distribuye entre todos los miembros de la cooperativa.

Igual de importantes son estas otras *cooperativas de datos*:

(iii) *Driver's Seat.*

Es una cooperativa de conductores que recopila datos relacionados con el trabajo a partir de los teléfonos inteligentes de los conductores de la economía sumergida.

Se lee en su web (https://www.driversseat.co/):

"*Lanzamos Driver's Seat hace cinco años para ayudar a los trabajadores a recibir salarios más altos cada día, combatir el uso por parte de las empresas de la gestión algorítmica con tecnología que los trabajadores construyen ellos mismos, incorporar datos honestos a la fuerza laboral y la formulación de políticas de transporte, y construir un negocio de propiedad cooperativa para sostener nuestra misión. Hemos logrado grandes avances hacia todos esos objetivos:*

Miles de conductores de transporte y repartidores aumentaron su salario y al mismo tiempo recuperaron el control de su trabajo mediante el uso de la transparencia salarial, el seguimiento de tiempo y millas, la información de mercado de colaboración abierta y las herramientas de recomendaciones de IA de la aplicación Driver's Seat.

Organizaciones de trabajadores como Rideshare Drivers United, Los Deliveristas Unidos, Colorado Independent Drivers Union y SEIU utilizaron nuestros conjuntos de datos agregados para defender políticas a favor de los trabajadores y luchar contra la desinformación de las empresas.

Los planificadores de transporte de la ciudad de San Francisco, UC Berkeley y Fehr and Peers se asociaron con nosotros para analizar la conexión entre el salario de los trabajadores autónomos y los resultados ambientales y de transporte.

Construimos un modelo de tecnología que es de propiedad cooperativa y está dirigida por sus usuarios y beneficiarios".

Explica con claridad el profesor Fabio Bravo la utilidad de esta "cooperativa de datos" de la siguiente manera: "*La agregación de los datos de tráfico generados por los múltiples "drivers" o "riders", con su análisis de datos, permite – por ejemplo – a los organismos públicos desarrollar políticas específicas sobre la viabilidad, el tráfico y el desarrollo urbano. A favor de empresas comerciales, en cambio, el análisis de los datos generados por Diver's Seat podría utilizarse para planificar y decidir sobre la posible apertura de puntos de venta por parte de establecimientos comerciales y la necesidad o no de adquirir zonas adicionales para el estacionamiento de los autores de clientes, en una realidad urbana marcada por el creciente desarrollo del e-commerce y del food delivery, que podrían comprometer la bondad de los análisis de business plan realizados según técnicas más tradicionales*" [35].

(iv) *Resonate.*

Es una cooperativa propiedad de músicos y sus mecenas.

También se lee en su web (https://resonate.coop/):

"*Una plataforma de música que todos podemos controlar. Es el primer servicio de transmisión de música de propiedad comunitaria. Una plataforma cooperativa de múltiples partes interesadas, gobernada democráticamente por nuestros miembros: artistas, oyentes y trabajadores*".

(v) *Swash.*

Recopila datos de navegación por Internet de particulares.

Se lee en su web (https://support.swashapp.io/hc/en-us/articles/19218801718801-What-is-Swash):

"*Swash permite a las personas ganar dinero siendo ellos mismos en línea. Swash es un portal de ganancias en línea donde puedes ganar puntos por estar activo y completar tareas en línea. Canjee sus ganancias por efectivo, tarjetas de regalo y criptomonedas o elija donar a causas en las que cree. Ya sea que esté navegando por la web, viendo anuncios o compartiendo opiniones, merece que le agradezcan sus esfuerzos. Al compartir las ganancias de sus contribuciones con usted, Swash está aquí para crear juntos un ecosistema digital más saludable y sostenible. Además de los usuarios habituales de Internet, Swash consta de una amplia red de colaboradores interconectados que incluyen:*

marcas que publican anuncios

---

[35] *L'aggregazione dei dati di traffico generata dai molteplici "drivers" o "riders", con relativa data analysis, consente – ad esempio – ad enti pubblici di sviluppare mirate politiche sulla viabilità, sul traffico, sullo sviluppo urbano. In favore di società commerciali, invece, l'analisi dei dati generati da Diver's Seat potrebbe essere utilizzata per pianificare e decidere in ordine all'eventuale apertura di punti vendita da parte di esercizi commerciali e alla necessità o meno di acquisire ulteriori aree da destinare al parcheggio delle autori dei clienti, in una realtà urbana segnata dal crescente sviluppo dell'e-commerce e del food delivery, che potrebbero compromettere la bontà delle analisi di business plan effettuate secondo tecniche più tradizionali* (F. BRAVO, *Le cooperative di dati*, cit., p. 14).

empresas que compran y analizan datos
científicos de datos que construyen modelos
desarrolladores que innovan en la pila Swash
organizaciones benéficas que reciben sus donaciones".

5. El *Big data*.

5.1. Introducción.

En la era digital se han generado cantidades abrumadoras de información. Estas cantidades de datos han llegado a ser inmensamente valiosas para las grandes *empresas*: por primera vez, las empresas pueden integrar datos dispares en fuentes significativas para que los algoritmos de inteligencia artificial interpreten y comprendan comportamientos.

El *big data* se puede definir como: "*activos de información de gran volumen o variedad que exigen formas rentables e innovadoras de procesamiento de información y permiten una mejor comprensión, toma de decisiones y automatización de procesos*"[36].

Los datos juegan un papel muy importante en la interpretación de información valiosa en torno a los objetivos empresariales y a las preferencias de los clientes. Si se analizan correctamente, pueden explicar mucho sobre nuestro comportamiento, personalidades e historias. Las empresas pueden aprovecharlos para mejorar productos, estrategias comerciales y campañas de marketing.

La importancia del *big data* ha existido por años, pero sólo en los últimos tiempos se han desarrollado las tecnologías necesarias para analizar – con velocidad y eficiencia – grandes conjuntos de datos. Es más, a medida que los datos recopilados – estructurados o no[37] – vayan aumentando, podrán ser examinados, inclusive, para predecir el futuro.

El *big data* ha cambiado la forma en que, incluso las empresas más pequeñas,

---

[36] https://blog.up.edu.mx/que-es-el-big-data-y-como-te-ayudara-a-tomar-decisiones-estrategicas-para-tu-empresa – Universidad Panamericana – febrero 2020.

[37] Los datos no estructurados se pueden pensar como datos que no se gestionan de forma activa en un sistema transaccional; por ejemplo, los datos que no viven en un sistema de gestión de bases de datos relacionales (RDBMS). Los datos estructurados se pueden pensar como registros (o transacciones) en un entorno de base de datos; por ejemplo, las filas de una tabla de una base de datos SQL. No hay preferencia en cuanto a si los datos están estructurados o no estructurados. Ambos disponen de herramientas que permiten a los usuarios acceder a la información. Los datos no estructurados sólo tienen una mayor abundancia que los datos estructurados. Algunos ejemplos de datos no estructurados son: a. – *Medios enriquecidos*. Datos de medios y entretenimiento, datos de vigilancia, datos geoespaciales, audio, datos meteorológicos. b. – *Colecciones de documentos.* Facturas, registros, correos electrónicos, aplicaciones de productividad. c. – *Internet de las cosas.* Datos de sensores, datos de teletipos. d. – *Análisis. Aprendizaje automático, inteligencia artificial (IA).* Hasta la llegada del almacenamiento basado en objetos, la mayoría, si no todos, de estos datos no estructurados se almacenaban en sistemas basados en archivos (https://www.netapp.com/es/data-storage/unstructured-data/what-is-unstructured-data/).

hacen negocios a medida que la recopilación e interpretación de datos se vuelven más accesibles. Nuevas tecnologías innovadoras y rentables van surgiendo y mejorando constantemente, razón por la cual resulta más fácil para cualquier organización implementar soluciones mediante *big data*.

5.2. Aplicaciones del *big data* en los negocios.

Como el *big data* procesa y analiza grandes conjuntos de datos que permiten obtener información valiosa y útil para la toma de decisiones, su importancia radica en que permite a las empresas obtener una visión más completa de sus clientes, mejorar su eficiencia y reducir costos. Con el uso de las tecnologías *big data* se busca convertir gran cantidad de datos en conocimiento útil, por lo que es necesario contar con herramientas que permitan analizar, procesar y almacenar todos los *inputs* recogidos.

En efecto, el uso y la comprensión del *big data* es una ventaja competitiva crucial para las empresas en tanto estas pueden recopilar datos de la realidad económica, comercial, financiera y social existentes en torno a la compañía, como así también, almacenar la información suministrada por los clientes, a la que los competidores no tienen acceso.

En otras palabras, el uso de herramientas de *big data* es importante por varias razones:

– Para tomar decisiones más informadas y basadas en hechos concretos.

– Para identificar tendencias y patrones en tiempo real que pueden ser de gran valor.

– Mejorar la eficiencia, optimizar procesos y reducir costos, siempre en base a los datos.

– Personalizar la experiencia del cliente, utilizando todo tipo de datos obtenidos de los mismos clientes.

El *big data* presenta, entonces, una gran cantidad de nuevas vías de crecimiento, desde ideas y soluciones innovadoras hasta modificaciones en la interacción con los clientes.

A tal efecto, hay que tener en cuenta tres aspectos: la *automatización, la información detallada y la toma de decisiones basada en datos*.

(i) *Automatización*

El *big data* tiene el potencial de mejorar la eficiencia interna y las operaciones a través de la automatización robótica de procesos. Enormes cantidades de datos en tiempo real pueden analizarse inmediatamente e integrarse en los procesos comerciales con el fin de efectuar tomas de decisiones automatizadas.

Ante infraestructuras escalables y la disminución de costos de computación en nube, la automatización de la recopilación y el almacenamiento de datos se encuentra al alcance de las empresas.

(ii) *Perspectivas a profundidad*

El *big data* también se puede utilizar para descubrir oportunidades ocultas, desconocidas antes de poder analizar grandes conjuntos de datos. Los conjuntos de da-

tos complejos incluso pueden emplearse para desarrollar nuevos productos o mejorar los existentes. Los datos de propiedad dentro del mercado pueden resultar de gran valor en el panorama competitivo.

(iii) *Toma de decisiones más rápida y mejor*

Gracias a la velocidad de la tecnología de análisis de datos, junto con la capacidad de analizar nuevas fuentes de datos, las empresas hoy en día pueden analizar estratégicamente información al instante y tomar decisiones inteligentes e informadas.

5.3. ¿Cómo aprovechar el potencial del *big data*?

El mercado de análisis es enorme: más del 40% de las grandes organizaciones han invertido en estrategias de *big data* desde el 2012. Sin embargo, con un sinfín de conjuntos de datos posibles por administrar, puede ser abrumador saber dónde o cómo comenzar [38].

Por lo tanto, antes de elegir e implementar una solución de *big data*, las organizaciones deben considerar los siguientes puntos:

(i) *Equipo experimentado de big data*

Se debe reunir un equipo de expertos en recopilación, análisis y estrategias de datos para que elaboren un enfoque ideal de *big data* capaz de generar aciertos para la empresa. Este equipo debe incluir personas que entiendan de métodos analíticos modernos y sepan manipular grandes conjuntos de datos, y consultores experimentados que comprendan los objetivos comerciales generales.

(ii) *Identificación de metas*

Contar con los objetivos correctos es crucial para implementar con éxito una solución de *big data*. Los datos y los análisis deben alinearse correctamente con los objetivos definitivos de la organización (es decir, mayores ganancias, reconocimiento de marca, participación en el mercado).

(iii) *Recopilación de los datos correctos*

Una vez que se hayan definido los objetivos comerciales estratégicos, el siguiente paso consiste en tener plena comprensión de los datos antes de su aplicación. Identificar, captar y rastrear los datos correctos representará el eje de todo el proceso. Utilizar conjuntos incorrectos de datos puede conllevar consecuencias indeseables y conducir a la empresa hacia una dirección equivocada.

Los analistas profesionales de datos deben estar capacitados para convertir (o traducir) grandes cantidades de datos en información valiosa con eficiencia y precisión.

Asimismo, los resúmenes de datos fácilmente comprensibles ayudan a los equipos de apoyo a procesar rápidamente los análisis de datos y ejecutar decisiones comerciales rápidas.

---

[38] https://blog.up.edu.mx/que-es-el-big-data-y-como-te-ayudara-a-tomar-decisiones-estrategicas-para-tu-empresa.

5.4. Herramientas de *big data*.

Analizada la importancia de los datos para las empresas, cabe mencionar algunas herramientas de Big Data para procesar y almacenar datos [39]:

(i) *Hadoop*

Una de las herramientas más populares que se utiliza para almacenar y procesar grandes conjuntos de datos es el Hadoop, un software de código abierto que funciona en *clusters* de servidores y permite el procesamiento distribuido de datos. Es muy útil para empresas que necesitan procesar grandes cantidades de datos y hacer análisis en tiempo real.

(ii) *Spark*

Otra herramienta de código abierto que se utiliza para procesar grandes volúmenes de datos en tiempo real es Spark. Es una herramienta muy rápida y escalable, y se utiliza en aplicaciones como análisis de datos, procesamiento de imágenes y aprendizaje automático.

(iii) *MongoDB*

Es una base de datos NoSQL que se utiliza para almacenar grandes volúmenes de datos de manera eficiente y escalable. MongoDB es muy popular en aplicaciones web y móviles, y es ideal para almacenar datos no estructurados.

(iv) *Tableau*

Es una herramienta de visualización de datos que permite a los usuarios crear gráficos y tablas interactivas a partir de grandes conjuntos de datos. Es muy fácil de usar y se integra con otras herramientas de análisis de datos como Hadoop y Spark.

(v) *Apache Kafka*

Es una plataforma de *streaming* de datos que se utiliza para procesar y analizar grandes volúmenes de datos en tiempo real. Kafka es muy útil para empresas que necesitan analizar datos en tiempo real, como las empresas de publicidad en línea.

Es importante aclarar que cada una de estas herramientas tiene un propósito específico y es ideal para empresas que necesitan procesar grandes cantidades de datos y hacer análisis en tiempo real.

6. La Cooperativa de datos como instrumento eficaz para optimizar la utilización del *big data* en el ámbito del derecho societario.

6.1. Introducción.

Frente a la amplia utilización de las tecnologías de la información y comunicación (TICs) en las actividades de las empresas, resultaba llamativa la lentitud para incorporarlas al plano societario, esto es, al funcionamiento de los órganos societa-

[39] https://www.teclab.edu.ar/las-5-mejores-herramientas-big-data-para-tu-empresa/.

rios, a la documentación, a la contabilidad y a las comunicaciones societarias.

La demora puede haberse debido tanto a cuestiones culturales cuanto a dudas existentes sobre la confiabilidad de las nuevas tecnologías en la materia.

Hoy, con la incesante evolución tecnológica, la incorporación de las nuevas generaciones al quehacer societario, y particularmente después de la experiencia de la Pandemia, esas barreras han sido superadas y no se advierte impedimento para hacer plena aplicación del "principio de equivalencia funcional" entre actos físicos o materiales con actos virtuales en materia societaria [40].

No obstante, el desafío no se limita a pasar de lo analógico a lo digital sino que conlleva pretensiones más profundas como el ámbito de los sistemas de control, la ejecución automática y las decisiones mediante aplicación de la inteligencia artificial.

Pero la cuestión no termina allí.

En efecto, también el *Big Data* ha impactado fuertemente en el derecho societario con distintos enfoques que, perfectamente, podrían ser canalizados a través de las *cooperativas de datos* como instrumento de recolección, almacenamiento y gestión de datos para la toma de decisiones estratégicas desde el punto de vista empresarial.

6.2. Alianzas estratégicas empresariales.

Cuando nos referimos a fusiones, gobierno corporativo y alianzas estratégicas, se advierte la creciente influencia de los datos en la toma de decisiones empresariales.

Efectivamente, los datos han venido a desarrollar un papel crítico en la optimización de fusiones y adquisiciones, la mejora de la gobernanza corporativa y la toma de decisiones claves en alianzas empresariales estratégicas [41].

El impacto del *Big Data* en las prácticas de fusiones y adquisiciones ha sido revolucionario. Las empresas han experimentado un cambio significativo en su enfoque gracias a la capacidad de aprovechar datos inteligentes para evaluar con mayor precisión en tiempo real *el valor de los activos y pasivos* relacionados con las empresas que son objeto de interés.

La aplicación del análisis avanzado de datos permite llevar a cabo una evaluación detallada de los riesgos y oportunidades vinculados a cualquier transacción.

De esta manera, el *Big Data* proporciona a las empresas la capacidad necesaria de evaluar la rentabilidad potencial de una fusión, identificar sinergias que pueden ser explotadas y descubrir riesgos ocultos en los datos financieros. Este nivel de

---

[40] F. DUBOIS, *Los impactos tecnológicos en las sociedades comerciales, ¿Se está configurando un nuevo modelo "societario tecnológico"?*, in https://favierduboisspagnolo.com/trabajos-de-doctrina/los-impactos-tecnologicos-en-las-sociedades-comerciales/.

[41] C.A. PUENTE ROSERO, *Big Data y Derecho Societario: Potenciando el futuro de Fusiones, Gobierno Corporativo y Alianzas Estratégicas*, in *X-PedientesEconómicos*,Vol. 7, 18, 2023, pp. 23-41 – Vista de Big Data y Derecho Societario: Potenciando el futuro de Fusiones, Gobierno Corporativo y Alianzas Estratégicas (supercias.gob.ec).

análisis en tiempo real añade un grado de profundidad y precisión que hasta hace poco resultaba inalcanzable.

Esta tecnología ha emergido, entonces, como una herramienta esencial en el ámbito de las fusiones y adquisiciones, ofreciendo nuevas perspectivas y ventajas estratégicas para las distintas empresas.

Desde esta óptica, adquiere particular importancia que esos datos económicos, financieros, de mercado – entre otros – puedan ser almacenados, conservados, clasificados estratégicamente y hasta gestionados democráticamente en el seno de una misma estructura organizativa; creada con el objetivo de suministrar oportunamente esa información a sus propios miembros – cuando la necesiten – con el fin de tomar la mejor decisión empresarial posible.

Véase, en este sentido, como la aplicación del *modelo cooperativo para la recolección, el almacenamiento y la compartición de datos* económicos y financieros del mercado, hace posible que estructuras societarias que forman parte de la *cooperativa de datos o que se vinculan a la misma,* puedan crear un *modelo avanzado de asesoramiento* – a través de las herramientas de *big data* y los *datos compilados* – para optimizar las decisiones que deben tomarse sobre la conveniencia (o no) de fusionarse con otras corporaciones o adquirir (o no) el paquete de control accionario de las mismas.

Sin los datos necesarios y sin la tecnología que permita analizarlos estratégicamente, la decisión adoptada puede ser errática e ineficiente. A través de la *cooperativa de datos* creada a tal efecto, ello puede evitarse.

Reiteramos.

A través del *big data*, se puede realizar una evaluación precisa del *valor real* de una empresa. Esto implica un análisis exhaustivo de sus activos, pasivos, flujos de efectivo y proyecciones financieras sustentados en datos que va a proporcionar la *cooperativa*; quien los ha obtenido – principalmente – de sus propios miembros – aunque también puede hacerlo de fuentes externas-, que luego son compartidos a los integrantes para que resuelven óptimamente tal o cual problema.

Las predicciones basadas en datos "administrados" de esta manera, suelen resultar más fiables y sólidas en comparación con las estimaciones tradicionales (que suelen "alimentarse" *solamente* de fuentes externas).

A mayor abundamiento, el Big Data también desempeña un papel esencial en la identificación y gestión proactiva de los riesgos asociados con una fusión o adquisición. Esto abarca la detección temprana de riesgos financieros, legales y operativos que podrían surgir durante un proceso de reorganización societario.

Pensemos, entonces, en la importancia del rol de la cooperativa, quien además de compilar los datos, los proporciona a sus miembros; asistiéndolos en la toma de la decisión que, sustentada en el análisis de esa información, les permitirá analizar si realmente les conviene o no fusionarse o adquirir el *take over accionario* de la otra compañía.

Recordemos en este sentido que, la capacidad de tomar medidas preventivas en tiempo real, permite a las empresas mitigar ciertos riesgos antes de que se convier-

tan en obstáculos insuperables posteriores, por ejemplo, en la hora previa a decidir la adquisición de otras unidades económicas.

6.3. Optimización de las decisiones para un mejor resultado de la gestión empresarial.

El modelo cooperativo y el *big data* pueden también desempeñar un papel clave en materia de colaboración empresarial entre distintas compañías para la generación de información abundante y de calidad.

Nos referimos a la compartición y uso de los datos obtenidos en una determinada actividad – compilados y gestionados por la cooperativa de datos – que los ayude a tomar mejores decisiones dentro de un marco de seguridad.

Pensemos, por ejemplo, en varias empresas dedicadas a la actividad agrícola que forman parte de una *cooperativa de datos* y que, gracias a la información meteorológica y sobre los mercados de cereales que esta almacena junto con los datos proporcionados por fuentes externas (por ejemplo, los provenientes de satélites, estaciones meteorológicas e información de los mercados), hace posible la creación de modelos de predicción y asesoramiento avanzados que les permite a sus socios contar con los datos necesarios para conocer con mayor precisión qué granos sembrar, en que época del año, tomar medidas de prevención en caso de sequía o inundaciones, especular sobre la rentabilidad de la cosecha, etc.

Un claro ejemplo de cuanto decimos [42] es el caso de las Cooperativa Agroalimentaria de España, que representa y defiende a casi cuatro mil cooperativas agrarias, que reúnen a más de un millón de socios y ganaderos.

HISPATEC [43] desarrolla tanto servicios como tecnología digital y Big Data para el sector agroalimentario español desde el año 1986 y siempre ha tenido una fuerte conexión con las empresas cooperativas.

Estas entidades buscan consolidar el concepto "cooperativas de datos" como germen de la colaboración entre distintos agentes del sector agroalimentario para la generación de información abundante y de calidad. Para este objetivo se apoyan especialmente en la hoja de ruta que marca la *Estrategia para la Digitalización del sector agroalimentario y forestal y del medio rural* elaborado por el Ministerio de Agricultura, Pesca y Alimentación español.

En el marco de este plan, el papel de las cooperativas será el de "*agregadores de datos*".

Otro pilar fundamental de esta táctica es la creación de un Código de Conducta para el intercambio de datos en la agricultura, pactado entre los principales representantes de agricultores, cooperativas y el resto de los agentes a nivel europeo. En él se establecen las bases contractuales que ampararán las relaciones de intercambio de información entre los distintos operadores.

---

[42] https://www.revistatransformaciondigital.com/2019/03/26/cooperativa-de-datos/.

[43] https://www.hispatec.com/.

Cabe calificar entonces como *estratégica*, la labor que puede desempeñar en este ámbito la *cooperativa de datos*.

En efecto, los miembros de la cooperativa, prácticamente, dependen de sí mismos a la hora de contar con la información que necesitan, desde que son ellos mismos – si bien a través de la estructura cooperativa – los que gestionan y controlan democráticamente y en un marco de igualdad dicha información esencial.

7. Palabras finales.

La normativa que hemos analizado a lo largo de estas líneas da cuenta del objetivo primordial del Reglamento 2022/88 y sus diversas iniciativas: convertir a la Unión en líder de una sociedad dirigida por los datos, mediante la creación de un mercado único de datos que permita que estos fluyan libremente por la UE y entre sectores, en beneficio de las empresas, los investigadores y las Administraciones públicas.

Con tal finalidad, esta nueva regulación propone un cambio de paradigma y de enfoque en el tratamiento y gestión de los datos, que no puede soslayarse, si es que se quiere estar a la altura de una nueva realidad social, económica, cultural y empresarial; tremendamente influenciada por las nuevas tecnologías.

En este contexto, si la nueva generación de empresarios – especialmente los emprendedores – desean optimizar sus resultados desde el punto de vista económico, financiero, ambiental y social, es evidente que no podrán mantenerse al margen de este fenómeno imparable.

Capitolo XVI

Le cooperative di dati nel *Data Governance Act*: analisi normativa e ricerca di modelli attuativi compatibili

Fiorella Albanese

Abstract: By analysing the legislative framework of data broker activities, this paper traces the main characteristics of data cooperatives and highlight their statutory contradictions (mainly related to the data cooperatives' legal form and structure). The purpose of this analysis is ultimately to identify the compatibilities between data cooperatives and other (pre-existing) cooperative corporations.

1. Introduzione.

Il 30 maggio 2022 è stato approvato il Reg. (UE) 2022/868 del Parlamento Europeo e del Consiglio relativo alla *governance* europea dei dati [1] (di seguito, "Rego-

[1] Il DGA si colloca nell'ambito di una serie di misure annunciate nella Strategia europea sui dati

lamento sulla *governance* dei dati", o "*Data Governance Act*" o "DGA") che ha definito le regole e le condizioni che l'Europa ha adottato in materia di *data sharing*, individuando tre principali pilastri: il riutilizzo dei dati pubblici, i servizi di intermediazione di dati, l'altruismo dei dati.

Per quanto attiene al secondo pilastro (i servizi di intermediazione dei dati), lo scopo declamato dal Regolamento è quello di aumentare la fiducia nei servizi di intermediazione e condivisione dei dati, riducendo le asimmetrie di potere e informazione, al fine di offrire un nuovo modo "europeo" di gestire i dati attraverso la separazione tra la fornitura, l'intermediazione e l'uso dei dati nell'economia [2].

In ossequio a tale obiettivo, il DGA stabilisce requisiti armonizzati per una fornitura affidabile dei servizi di intermediazione dei dati, regolamentando e delineando i contorni di un nuovo soggetto: l'infomediario [3], vale a dire il fornitore dei servizi di condivisione dei dati.

2020. Nell'ambito della Strategia, la Commissione ha descritto la visione di uno Spazio comune europeo dei dati, vale a dire un mercato unico per i dati in cui essi possano essere utilizzati indipendentemente dal luogo in cui sono fisicamente conservati nell'UE in conformità con la legge applicabile.

[2] Oltre a disciplinare i requisiti dei servizi di intermediazione dei dati, il Regolamento introduce poi una procedura di notifica per i servizi di intermediazione. In conformità al principio del Paese d'origine, il fornitore invia la notifica solo all'autorità designata nello Stato in cui si trova il suo stabilimento principale o il suo rappresentante legale. La notifica ha un contenuto tassativo ed è una dichiarazione dell'intenzione di fornire i servizi di intermediazione (nonché la rappresentazione delle informazioni indicate nel Regolamento). Non è richiesta alcuna decisione esplicita o atto amministrativo da parte dell'autorità competente e il fornitore può iniziare a operare dopo la notifica, in tutti gli Stati membri.

Se il fornitore di servizi cessa l'attività, deve notificarlo all'autorità competente entro 15 giorni e, in caso di modifiche alle informazioni fornite, deve notificarlo entro 14 giorni.

Il prestatore dei servizi può anche chiedere all'autorità competente di rilasciare un certificato che attesti il rispetto delle condizioni per la fornitura di servizi di cui agli artt. 10 e 11 del DGA. Una volta ricevuta tale conferma, il fornitore può utilizzare la denominazione di "fornitore di servizi di intermediazione di dati stabilito nell'Unione" e il logo comune adottato dalla Commissione.

Gli Stati membri sono tenuti a designare una o più autorità incaricate di notificare i fornitori di servizi di intermediazione dei dati e di monitorare e controllare il rispetto delle condizioni stabilite dal DGA. Gli Stati membri devono inoltre prevedere sanzioni per le violazioni del DGA, in particolare almeno per le infrazioni delle disposizioni riguardanti:

– l'obbligo di notifica dei fornitori di servizi di intermediazione dati ai sensi dell'art. 11;

– le condizioni per la fornitura di servizi ai sensi dell'art. 12.

Le autorità competenti devono essere giuridicamente distinte e funzionalmente indipendenti da qualsiasi intermediario di dati. I dirigenti e il personale responsabile non devono essere coinvolti in alcun modo nella fornitura dei servizi che valutano (ciò non esclude l'uso di tali servizi per le attività dell'autorità o per scopi personali). Devono svolgere i loro compiti in modo imparziale, trasparente, coerente, affidabile e tempestivo. Devono disporre di risorse finanziarie e umane adeguate, comprese le competenze e le risorse tecniche necessarie.

[3] Prendiamo in prestito la terminologia utilizzata dalla prof.ssa Poletti Dianora (cfr. Cfr. D. POLETTI, *Gli intermediari di dati*, in *European Journal of Privacy Law & Technologies*, 2022, 1, pp. 45-56, consultabile al sito https://universitypress.unisob.na.it/ojs/index.php/ejplt/article/view/1623/1092) per riferirci agli intermediari di dati in genere. Si precisa che i termini infomediario, intermediario, e fornitore di servizi di intermediazione sono utilizzati del testo come sinonimi.

L'infomediazione DGA *compliant* può assumere tre principali declinazioni e riguardare:

a) i servizi di intermediazione tra i titolari dei dati e i potenziali utenti dei dati;

b) i servizi di intermediazione tra interessati che intendono mettere a disposizione i propri dati personali o persone fisiche che intendono mettere a disposizione dati non personali e potenziali utenti dei dati;

c) i servizi di cooperative di dati [4].

Sull'ultima categoria di infomediari, le cooperative di dati, si concentra il presente lavoro che, muovendo dalla ricostruzione del quadro normativo, intende tracciare gli argini entro i quali si sviluppa la figura delle cooperative di dati al fine di identificarne: l'ambito di applicazione della norma; la veste giuridica (o le vesti giuridiche) compatibile; il ventaglio di attività esercitabili e conseguentemente i modelli di *business* percorribili.

2. Definizione della cooperativa di dati.

Il *Data Governance Act* non dà una definizione delle cooperative di dati ma definisce i «servizi di cooperative di dati» come quei «servizi di intermediazione dei dati offerti da una struttura organizzativa costituita da interessati, imprese individuali o da PMI, che sono membri di tale struttura, avente come obiettivi principali quelli di aiutare i propri membri nell'esercizio dei loro diritti in relazione a determinati dati, anche per quanto riguarda il compiere scelte informate prima di acconsentire al trattamento dei dati, di procedere a uno scambio di opinioni sulle finalità e sulle condizioni del trattamento dei dati che rappresenterebbero al meglio gli interessi dei propri membri in relazione ai loro dati, o di negoziare i termini e le condizioni per il trattamento dei dati per conto dei membri prima di concedere l'autorizzazione al trattamento dei dati non personali o prima che essi diano il loro consenso al trattamento dei dati personali» [5].

Pertanto il legislatore europeo identifica il servizio da essi erogato in particolare focalizzando l'attenzione sui seguenti elementi:

---

[4] All' art. 10 del DGA sono disciplinati i tre sottogruppi di servizi di intermediazione dei dati (i primi due distinti in base alla qualità dei dati – personali e/o non personali – e ai soggetti messi in relazione dall'attività di intermediazione):

a) servizi di intermediazione tra i titolari dei dati e i potenziali utenti dei dati (aventi ad oggetto dati non personali);

b) servizi di intermediazione tra interessati che intendono mettere a disposizione i propri dati personali o persone fisiche che intendono mettere a disposizione dati non personali e potenziali utenti dei dati (aventi ad oggetto dati personali e/o misti, quindi aventi ad oggetto dati personali e non);

c) servizi di cooperative di dati (non meglio identificati con riguardo a oggetto e soggetti posti in relazione dall'intermediazione).

[5] Cfr. art. 2, par 1, n. 15).

(i) i servizi di cooperative di dati sono servizi di intermediazione [6];

(ii) sono offerti da una struttura organizzativa costituita da interessati, imprese individuali o da PMI, i quali sono membri di tale struttura;

(iii) la struttura ha come obiettivo principale (che ne costituisce l'attività caratterizzante) aiutare i propri membri nell'esercizio dei loro diritti in relazione a determinati dati e l'aiuto può concretarsi:

– nell'assistenza per compiere scelte informate prima di acconsentire al trattamento dei dati;

– nel procedere a uno scambio di opinioni sulle finalità e sulle condizioni del trattamento dei dati che rappresenterebbero al meglio gli interessi dei propri membri in relazione ai loro dati;

– nel negoziare i termini e le condizioni per il trattamento dei dati per conto dei membri prima di concedere l'autorizzazione al trattamento dei dati non personali o prima che essi diano il loro consenso al trattamento dei dati personali.

3. Il rapporto fra i servizi di cooperative di dati e i servizi di intermediazione.

3.1. Definizione e contenuto dei servizi di intermediazione dei dati.

Il primo degli elementi definitori sussume i servizi delle cooperative di dati fra quelli di intermediazione di dati. Questa sussunzione genera qualche dubbio di impatto ermeneutico attesa la necessità di stabilire in quale misura le disposizioni previste per gli intermediari dei dati si estendano anche alle cooperative di dati (nel rispetto delle peculiarità di queste ultime).

Per comprendere le difficoltà collegate a questa operazione interpretativa occorre rinviare alla definizione di servizio di intermediazione (che in qualche misura traccia i contorni anche dei servizi di cooperative di dati che ne sono un sottogruppo).

All'art. 2 del DGA il legislatore europeo definisce il «servizio di intermediazione dei dati» come «un servizio che mira a instaurare, attraverso strumenti tecnici, giuridici o di altro tipo, rapporti commerciali ai fini della condivisione dei dati tra un numero indeterminato di interessati e di titolari dei dati, da un lato, e gli utenti dei dati, dall'altro, anche al fine dell'esercizio dei diritti degli interessati in relazione ai dati personali». La norma valorizza in particolare:

– l'instaurazione di rapporti commerciali finalizzati alla condivisione di dati fra fornitori di dati [7] e utenti di dati;

---

[6] Cfr. art. 10 DGA.

[7] Con la locuzione "fornitore di dati" ci si intende riferire, nel presente lavoro, ai soggetti che, nell'ambito della disciplina DGA, mettono a disposizione i dati per l'intermediazione e pertanto gli interessati e i titolari di dati.

– che l'intermediazione avviene tra un numero indeterminato di interessati/titolari dei dati e gli utenti.

La norma prosegue dettando delle esclusioni (riguardanti attività, materie e caratteristiche di servizi che non si sussumono nei SID)[8].

Riassumendo, dunque, i servizi di intermediazione dei dati (di seguito, per brevità, i "SID") sono precipuamente servizi di condivisione dei dati che mirano ad instaurare un rapporto commerciale fra la domanda di dati (utenti dei dati) e l'offerta di dati (interessati/titolari di dati).

Gli elementi definitori presenti all'art. 2 costituiscono un laconico estratto[9] di quanto più diffusamente il legislatore europeo lascia intendere nei *considerando*: da una lettura complessiva emergono infatti ulteriori elementi e caratteristiche che saranno evidenziati nel prosieguo.

3.2. I principi di neutralità, separazione e indipendenza e il divieto (apparente) di erogazione dei servizi accessori.

I margini all'interno dei quali sono confinate le attività di cui si sostanziano i SID sono tracciati in modo incerto: non è chiaro fino a che punto i fornitori di SID possano spingersi, andando oltre l'attività principale (la pura intermediazione fra

[8] Si tratta, in particolare, delle esclusioni riguardanti: i) alcune tipologie di attività che comportano l'elaborazione dei dati (come aggregazione arricchimento e trasformazione) senza instaurare un rapporto commerciale tra titolari dei dati e utenti dei dati, di cui si dirà *infra*; ii) alcune materie (dati protetti dal diritto di autore); iii) i servizi destinati a un solo titolare dei dati, a un numero determinato di titolari o comunque all'interno di un gruppo chiuso; iv) i servizi offerti da enti pubblici non miranti a instaurare rapporti commerciali.

[9] La definizione *ex* art. 2 è infatti un *patchwork* fra i *considerando* nn. 28 e 29:

– i SID instaurano «rapporti commerciali ai fini della condivisione dei dati tra un numero indeterminato di interessati e di titolari dei dati, da un lato, e gli utenti dei dati, dall'altro, anche per l'esercizio dei diritti degli interessati in relazione ai dati personali» (*considerando* n. 28);

– «Ciò escluderebbe i servizi che ottengono dati dai titolari dei dati e li aggregano, arricchiscono o trasformano al fine di aggiungervi un valore sostanziale e concedono licenze per l'utilizzo dei dati risultanti agli utenti dei dati, senza instaurare un rapporto commerciale tra i titolari dei dati e gli utenti dei dati» (*considerando* n. 28);

– «Il presente regolamento non dovrebbe riguardare i servizi il cui obiettivo principale è l'intermediazione di contenuti protetti da diritto d'autore» (*considerando* n. 29);

– «Ciò escluderebbe altresì i servizi che sono utilizzati esclusivamente da un titolare dei dati per consentire l'utilizzo dei dati detenuti da tale titolare dei dati, oppure che sono utilizzati da varie persone giuridiche all'interno di un gruppo chiuso, anche nel quadro di rapporti con i fornitori o i clienti o di collaborazioni contrattualmente stabiliti, in particolare quelli aventi come obiettivo principale quello di garantire le funzionalità di oggetti o dispositivi connessi all'internet delle cose» (*considerando* n. 28);

– «Il presente regolamento non dovrebbe applicarsi ai servizi offerti da enti pubblici così da facilitare il riutilizzo di dati protetti, detenuti da diversi enti pubblici conformemente al presente regolamento, o l'utilizzo di eventuali altri dati, nella misura in cui tali servizi non abbiano l'intenzione di creare rapporti commerciali» (*considerando* n. 29).

domanda e offerta di dati), e lambire attività ulteriori di elaborazione e processo dei dati (di seguito chiameremo queste attività i "servizi accessori"), che ne renderebbero molto più interessante l'offerta.

Le disposizioni del Regolamento su questo tema risultano ambigue e ai limiti del contraddittorio.

Muovendo anzitutto dall'analisi delle disposizioni limitative, i principi di neutralità e separazione tracciati dall'art. 12, par. 1, lett. *a*) [10] stabiliscono che: «il fornitore di servizi di intermediazione dei dati non utilizza i dati per i quali fornisce servizi di intermediazione dei dati per scopi diversi dalla messa a disposizione di tali dati agli utenti dei dati e fornisce servizi di intermediazione dei dati attraverso una persona giuridica distinta».

La disposizione sembrerebbe valorizzare la purezza del servizio di intermediazione, escludendo che il fornitore del servizio possa effettuare utilizzi dei dati che vadano oltre la messa a disposizione dei dati stessi (principio c.d. di neutralità); il fornitore dei servizi accessori sui dati deve separarli strutturalmente dall'intermediazione dei dati, creando un soggetto giuridico distinto (principio c.d. di separazione) [11]. La lettura che di questa norma ricorrentemente viene data [12] va nel senso

---

[10] L'articolo disciplina le «Condizioni per la fornitura di servizi di intermediazione dei dati».

[11] Del medesimo tenore anche il *considerando* n. 32.

Sull'interpretazione del principio di neutralità di cui all'art. 12, par. 1, lett. *a*), DGA per le cooperative di dati, cfr. F. BRAVO, *Le cooperative di dati*, in *Contratto e impresa*, 2023, 3, pp. 757-799, disponibile anche al sito: https://site.unibo.it/cooperative-di-dati/it.

[12] In questo senso: G. CAROVANO-M. FINCK, *Regulating data intermediaries: The impact of the Data Governance Act on the EU's data economy*, consultabile al sito: https://doi.org/10.1016/j.clsr.2023.105830; E. BIETTI-M. MANNAN, *Data Cooperatives in Europe: A Legal and Empirical Investigation White Paper created as part of The New School's Platform Cooperativism Consortium and Harvard University's Berkman Klein Center for Internet & Society Research Sprint*, December 2021, consultabile al sito: https://cyber.harvard.edu/sites/default/files/2022-02/Data_Cooperatives_Europe-group2.pdf, dove viene data un'interpretazione del concetto di "neutralità" come inteso a escludere deliberatamente un'ampia varietà di altri fornitori di servizi, che sviluppano prodotti aggiungendo valore ai dati: «*Intermediation is clearly the operative word here, as the proposal only applies to providers who are 'neutral' and whose main business objective is to legally (and potentially technically) connect data holders and data users, as well as assist in their transaction of data assets. It deliberately excludes a wide variety of other service providers, including cloud services, content intermediaries, data brokers and businesses that develop products by adding value to data. Instead, three types of data sharing services are mentioned: (1) intermediaries that facilitate B2B data-sharing, to enable bilateral data exchanges or pooling to allow joint exploitation of data; (2) intermediaries that facilitate C2B data-sharing, by making technical means available for businesses to access individual data subjects' data, and (3) data cooperatives that facilitate data subjects or MSMEs better realizing their rights, specifically by negotiating terms with data users prior to giving consent to use, helping them make informed consent decisions and fostering dialogue between them on data processing purposes and conditions*». Condivide questa soluzione interpretativa anche S. GIRISH-M. AVERY, *Data cooperative: Enabling meaningful collective negotiation of data rights for communities*, consultabile al sito: https://ssrn.com/abstract=4414473 o http://dx.doi.org/10.2139/ssrn.4414473 in cui si sottolinea come la legge preclude potenzialmente anche le attività che aggiungono valore ai dati aggregati allo scopo di venderli: «*The*

di escludere qualunque servizio accessorio [13] ad eccezione di quelli espressamente ammessi dalle lett. *c*), *d*) ed *e*) del medesimo art. 12 [14], vale a dire:

(i) uso dei dati sulle attività (data, ora, geolocalizzazione, durata dell'attività, collegamenti con altre persone) per lo sviluppo del servizio di intermediazione dei dati, e la loro messa a disposizione dei titolari dei dati su richiesta;

(ii) conversione dei dati in formati specifici solo allo scopo di migliorare l'interoperabilità a livello intrasettoriale e intersettoriale, se richiesto dall'utente dei dati, se prescritto dal diritto dell'Unione o per garantire l'armonizzazione con le norme internazionali o europee in materia di dati, con facoltà per gli interessati/titolari dei dati di non partecipare a tali conversioni (a meno che la conversione non sia prescritta dal diritto dell'Unione);

(iii) offerta di servizi supplementari come la conservazione temporanea, la cura, la conversione, l'anonimizzazione e la pseudonimizzazione, fermo restando che tali strumenti e servizi sono utilizzati solo su richiesta o approvazione esplicita del tito-

---

act [Data Governance Act, *n.d.a.*] *also potentially precludes the activities of cooperatives like Drivers' Seat which add value to aggregated driver data for the purpose of selling it*».

Nel senso contrario, della possibilità di conferire valore aggiunto ai dati, cfr. S. MEHTA-M. DAWANDE-V. MOOKERJEE, *Can data cooperatives sustain themselves?*, 2021, consultabile all'indirizzo: https://blogs.lse.ac.uk/businessreview/2021/08/02/can-data-cooperatives-sustain-themselves/.

Sull'interpretazione del principio di neutralità di cui all'art. 12, par. 1, lett. *a*), DGA per le cooperative di dati cfr. F. BRAVO, *Le cooperative di dati*, in *Contratto e impresa*, 2023, 3, cit.

[13] Giova rilevare che il problema dei servizi accessori riguardando tanto i dati personali quanto quelli non personali non può essere *bypssato* da una previa anonimizzazione dei dati. Il DGA difatti ammette, laddove lo richieda e quindi acconsenta l'interessato, l'anonimizzazione da parte dell'infomediario (e quindi anche della cooperativa) dei dati personali. Tuttavia neppure l'eventuale anonimizzazione dei dati personali (ammesso che tale operazione trasformi il dato personale in un dato non personale) può superare il tema della neutralità/separazione.

[14] Art. 12, lett. *c*), *d*) ed *e*):

«*c)* i dati raccolti su qualsiasi attività di una persona fisica o giuridica ai fini della fornitura del servizio di intermediazione dei dati, compresi la data, l'ora e i dati di geolocalizzazione, la durata dell'attività e i collegamenti con altre persone fisiche o giuridiche stabiliti dalla persona che utilizza il servizio di intermediazione dei dati, sono utilizzati solo per lo sviluppo di tale servizio di intermediazione dei dati, il che può comportare l'uso di dati per l'individuazione di frodi o a fini di cibersicurezza, e sono messi a disposizione dei titolari dei dati su richiesta;

d) il fornitore di servizi di intermediazione dei dati agevola lo scambio dei dati nel formato in cui li riceve da un interessato o da un titolare dei dati, li converte in formati specifici solo allo scopo di migliorare l'interoperabilità a livello intrasettoriale e intersettoriale, se richiesto dall'utente dei dati, se prescritto dal diritto dell'Unione o per garantire l'armonizzazione con le norme internazionali o europee in materia di dati e offre agli interessati o ai titolari dei dati la possibilità di non partecipare a tali conversioni, a meno che la conversione non sia prescritta dal diritto dell'Unione;

e) i servizi di intermediazione dei dati possono comprendere l'offerta di strumenti e servizi supplementari specifici ai titolari dei dati o agli interessati allo scopo specifico di facilitare lo scambio dei dati, come la conservazione temporanea, la cura, la conversione, l'anonimizzazione e la pseudonimizzazione, fermo restando che tali strumenti e servizi sono utilizzati solo su richiesta o approvazione esplicita del titolare dei dati o dell'interessato e gli strumenti di terzi offerti in tale contesto non utilizzano i dati per altri scopi».

lare dei dati o dell'interessato e gli strumenti di terzi offerti in tale contesto non utilizzano i dati per altri scopi.

3.3. Il requisito della commercialità e l'ammissibilità dei servizi accessori.

Se le condizioni per la fornitura dei servizi di intermediazione dei dati risultano così stringenti, l'art. 2, par. 1, n. 11) e i *considerando* [15] aprono a tutt'altro scenario.

Il *considerando* n. 28, richiamato peraltro dall'art. 2, par. 1, n. 11), espressamente afferma che non possono considerarsi SID: «i servizi che ottengono dati dai titolari dei dati e li aggregano; [li] arricchiscono o [li] trasformano al fine di aggiungervi un valore sostanziale e concedono licenze per l'utilizzo dei dati risultanti agli utenti dei dati, *senza instaurare un rapporto commerciale* tra i titolari dei dati e gli utenti dei dati» [16].

Il *discrimen* fra attività accessorie rientranti nell'ambito di applicazione della disciplina dei SID e attività escluse è rappresentato dal rapporto commerciale che deve instaurarsi fra interessati [17]/titolari di dati e utenti dei dati.

Il Regolamento non definisce il "rapporto commerciale", rinviando in questo modo a un concetto convenzionale di commercialità tutt'altro che pacifico:

(i) cos'è un rapporto commerciale e cosa comporta riferirlo alla relazione fra fornitori di dati e utenti dei dati [18]? In particolare è necessario che il rapporto commer-

---

[15] Che pure, va ricordato, non hanno una efficacia vincolante ma un valore interpretativo.

[16] Analogamente, sempre secondo il *considerando* 28, sono esclusi: «i servizi di archiviazione sul *cloud*; [i servizi] di analisi; [i servizi] di *software* per la condivisione dei dati; [i servizi] di *web browser*; [i servizi] di *plug-in* per *browser*; [i servizi] di un servizio di posta elettronica». L'esclusione viene perimetrata da una condizione, ossia che «tali servizi si limitino alla messa a disposizione di strumenti tecnici per gli interessati o per i titolari dei dati ai fini della condivisione di dati con altri». Tuttavia viene precisato che «la fornitura di tali strumenti non mira né a instaurare un *rapporto commerciale* tra i titolari dei dati e gli utenti dei dati né a consentire al fornitore di servizi di intermediazione dei dati di acquisire informazioni in merito all'instaurazione del rapporto commerciale ai fini della condivisione dei dati». Non è chiaro se questa ulteriore precisazione sia un'ultronea condizione (rispetto a quella di cui alla nota precedente) oppure un'inferenza.

I summenzionati servizi, esclusi dalla gamma dei SID tutte le volte in cui essi si limitino alla mera messa a disposizione di strumenti che consentano agli interessati/titolari dei dati di condividere dati con altri senza instaurare rapporti commerciali, sembra invece che siano sussumibili fra i SID allorquando si generi un rapporto commerciale (fra produttori di dati – interessati/titolari – e utenti dei dati).

[17] Nella disposizione citata, invero, non vengono menzionati gli interessati.

[18] Intorno al concetto di attività commerciale si è stratificata una consolidata letteratura giuridica, da cui è possibile attingere elementi per interpretare il concetto di "rapporto" commerciale. Rimangono tuttavia dei margini di dubbio sulla contestualizzazione del rapporto riferito alla relazione fra: i fornitori di dati e gli utenti dei dati. Le incertezze interpretative inerenti la locuzione non riguardano soltanto i servizi accessori atteso che il rapporto commerciale fra fornitori di dati e utenti dei dati caratterizza, a monte, la definizione e quindi l'essenza stessa, dei servizi di intermediazione dei dati (ed ha pertanto delle ricadute applicative sulla configurazione del rapporto fra fornitori di dati/soci della cooperativa di dati e la cooperativa di dati stessa, cfr. nota 61).

ciale avvenga direttamente (quindi sia "diretto") fra fornitori di dati e utenti di dati?

(ii) la commercialità si esprime solo in termini di ricavi?

(iii) la commercialità deve essere estesa a ciascun servizio accessorio?

(iv) *quid iuris* in caso di servizi accessori parzialmente gratuiti, questi sono sufficienti ad assorbire tutta l'attività dell'intermediario e a collocarla complessivamente al di fuori della disciplina della DGA [19]?

(v) ove si erogassero servizi accessori gratuiti per gli interessati (e i titolari di dati) e a pagamento per i soli utenti dei dati, saremmo ancora innanzi a infomediari tenuti al rispetto delle norme DGA? [20].

Le disposizioni contenute all'art. 2, par. 1, n. 11). lett. *a*) e nei *considerando* citati, hanno quindi riportato, nell'alveo di applicazione degli artt. 10 e ss., i servizi che, in assenza di tali precisazioni e in ossequio al disposto di cui all'art. 12, avrebbero dovuto sicuramente considerarsi esclusi dalla definizione di SID e che invece adesso costringeranno l'interprete allo sforzo ermeneutico di distinguere le situazioni ricadenti nell'ambito di applicazione del DGA da quelle che ne sono escluse.

Il tema summenzionato ha delle ricadute tutt'altro che marginali, oltre che per i fornitori di SID in generale, anche per le cooperative di dati, che saranno approfondite nel prosieguo, sul profilo:

– sia della disciplina applicabile, atteso che l'interpretazione che la Corte di giustizia dovesse dare decreterà il perimetro di applicazione dei vincoli imposti dal DGA sui SID e quindi alle cooperative di dati;

---

[19] Cfr. G. CAROVANO-M. FINCK, *Regulating data intermediaries: The impact of the Data Governance Act on the EU's data economy*, cit., che nell'evidenziare il dubbio sull'accezione da dare al rapporto commerciale fra interessati/titolari e utenti si interroga della sorte dei servizi misti (a pagamento e gratuiti) «*The DGA does not define what a commercial relationship is, raising the question of how existing DIS offered for free (or only partially for free) by private operators ought to be classified*» e rilevando altresì come richiedere relazioni commerciali dirette potrebbe creare uno spazio per strategie di elusione, ad esempio nel caso in cui un fornitore di servizi di dati, attraverso l'aggregazione, l'arricchimento, le inferenze, la combinazione di tali dati con dati sintetici o altri mezzi, conceda successivamente in licenza agli utenti dei dati il prodotto dei dati risultante al fine di interrompere il diretto rapporto commerciale tra titolari/interessati e utenti e dunque di sottrarsi all'applicazione dei vincoli imposti dalla DGA ai SID: «(…) *Furthermore, requiring direct commercial relationships might create room for circumvention strategies as a service provider can transform the data it holds through aggregation, enrichment, inferences, mixture with synthetic data or other means and later licence the resulting data product to data users to break the direct commercial relationship between data holders/subjects and users*». Queste le considerazioni da cui muovono le critiche al requisito della neutralità (requisito a cui il DGA ha dato grande rilievo) e alla sua concreta valorizzazione da parte del mercato.

[20] Laddove poi l'analisi si sposti, dagli infomediari in generale, alle cooperative di dati, i quesiti sulla commercialità si moltiplicano ulteriormente: ove il servizio accessorio che aggiunge valore ai dati forniti (analisi, aggregazione etc.) sia erogato a beneficio dei fornitori di dati (quindi non degli utenti) sia pure a fronte di un corrispettivo, tale servizio deve considerarsi interno o esterno al perimetro della commercialità, atteso che la relazione di commercialità non si istaura fra fornitore di dati e un utente (terzo), ma il fornitore di dati assume in questo caso il duplice ruolo di fornitore dei dati grezzi e utente dei dati modificati?

– sia con riguardo al tema dei modelli di *business* (sul profilo giuridico e economico-sostenibile) applicabili ai SID e, per esteso alle cooperative di dati.

L'elemento della commercialità dei rapporti fra interessati/titolari dei dati e utenti dei dati assume quindi un'indubbia centralità nel tracciare una distinzione sostanziale fra le attività incluse fra i SID e quelle che non lo sono.

4. Struttura e natura giuridica della cooperativa di dati.

4.1. Natura giuridica della cooperativa di dati.

Esaminato l'elemento definitorio che, sussumendo i servizi erogati dalle cooperative di dati fra i SID, rinvia alla disciplina dell'intermediazione dei dati, occorre passare all'analisi della struttura della cooperativa di dati al fine di identificarne la natura giuridica.

La natura giuridica della cooperativa di dati, infatti, non viene espressamente tracciata, tuttavia la scelta terminologica del legislatore europeo (che, nell'introdurre fra i fornitori di servizi di intermediazione dei dati un sottogruppo di soggetti, ha deciso di definirli "cooperative" di dati) ha generato non poche perplessità.

Se da una parte si potrebbe ritenere che il riferimento terminologico (alla "cooperativa" dei dati) non possa essere aspecifico e privo di implicazioni giuridiche, dovendo riconoscere a questa scelta linguistica un intenzionale e chiaro riferimento alla società cooperativa (che, ferme restando le variabili riconducibili alle peculiarità esistenti di sistema giuridico in sistema giuridico, conserva un nucleo essenziale riconosciuto unanimemente a livello europeo e che ruota intorno al concetto di mutualità), dall'altra parte è nutrita la posizione dottrinale che, al contrario, ammette ulteriori soluzioni che vanno oltre le società cooperative [21].

---

[21] In questo senso cfr. F. BRAVO, *Le cooperative di dati*, cit., «ciò lascia intuire che la fornitura di "servizi di cooperative di dati" possa essere svolta, eventualmente, anche in forme diverse da quella societaria, benché la "società cooperativa" – nelle diverse declinazioni che può assumere – sia il soggetto fisiologicamente chiamato a ricoprire il ruolo di "cooperativa di dati", quantomeno nel nostro ordinamento e in quello europeo. Si pensi ad esempio all'ipotesi in cui la "struttura organizzativa" venga "costituita" nella forma delle associazioni temporanee di imprese (ATI) o dei raggruppamenti temporanei di impresa (RTI) o, ancora, nella forma delle "reti di imprese", che svolgano "servizi di intermediazione di dati" mediante logiche di "cooperazione" a beneficio dei propri membri. Il concetto di "cooperativa di dati" non è rigidamente determinato nel DGA e apre la strada a forme soggettive diverse. Del resto il legislatore europeo, volutamente sintetico su tale aspetto, ha scelto di porre l'accento sull'elemento oggettivo, la fornitura del "servizio", e non sulla natura soggettiva del fornitore: nel far ciò ha però definito i "servizi di cooperative di dati" senza mai menzionare la "società cooperativa", facendo generico riferimento a una organizzazione strutturata costitutiva dai "membri" che la compongono, da individuarsi nelle persone fisiche a cui i dati si riferiscono («interessati», ai sensi del Reg. UE 679/2016), alle imprese individuali o alle piccole e medie imprese (PMI), che abbia come "obiettivi principali" il supporto ai propri "membri" in relazione all'uso dei dati che verrà effettuato nella fornitura del servizio».

Si veda inoltre anche M. MICHELI-E. FARRELL-B. CARBALLA SMICHOWSKI-M. POSADA SÁNCHEZ-

4.2. L'elenco dei membri della struttura.

L'unica norma che rasenta il tema della natura giuridica [22] delle cooperative di

S. SIGNORELLI-M. VESPE, *Mapping the landscape of data intermediaries Emerging models for more inclusive data governance*, 2023, pubblicato all'indirizzo https://publications.jrc.ec.europa.eu/repository/handle/JRC133988 «*Even if this is not often acknowledged when addressing data intermediaries, cooperatives are a distinct type of enterprise, different from private companies, NGOs and public bodies – and they can have either a for-profit, or a notfor – profit business model, depending on how they are implemented* (Mannan et al., 2022)», il contributo prosegue rilevando come la prassi avrebbe fatto emergere una tendenza delle cooperative di dati esistenti verso la condivisione dei dati per il perseguimento di risultati di interesse pubblico e non allo scopo di stabilire relazioni commerciali, in questo modo collocando le realtà esistenti più verso l'etichetta di organizzazioni per l'altruismo dei dati (*Data Governance Act compliant*) che non di "intermediario di dati" (proteso alla realizzazione di rapporti commerciali), in particolare il modello di *business* ricorrente sembra per ora essere basato sulla destinazione di eventuali redditi ricavati dalla condivisione dei dati con terze parti a garanzia della sostenibilità dell'iniziativa (e quindi la conseguente qualificazione come organizzazioni di altruismo dei dati secondo la DGA):«*Depending on how they are implemented in practice, specific use cases of data cooperatives might fall either under the label of 'data altruism organisations recognised in the Union' (RDAOs), or neither of the two. The definition of data cooperatives in Chapter III of the DGA (as one type of DISP) mainly highlights how they can support the realisation of individual objectives for the participating members. On the other hand, from the literature and engagement with the external experts during a workshop, we have found a greater emphasis on their facilitation of collective data management and on public interest goals. Since data cooperatives are often established to support data sharing for public-interest outcomes, and not for the purpose of establishing commercial relationships, they might also fall under the label of data altruism organisations recognised by the Union. If income is earned by sharing data with third parties, it is often used to ensure the sustainability of the initiative, so they would still qualify as data altruism organisations according to the DGA*».

Interessante la posizione di J. BALOUP-E. BAYAMLIOĞLU-A. BENMAYOR-C. DUCUING, *White Paper on Data Governance Act*, 2021, pubblicato all'indirizzo: https://www.researchgate.net/publication/352690055 che evidenzia come l'allora proposta della DGA non fosse chiara su cosa concretamente la nozione di "cooperativa di dati" implicasse in termini di forma giuridica e tipo di organizzazione, in particolare valorizzando la circostanza che l'articolo 2 della proposta facesse riferimento alla *membership* e quindi a un concetto di "adesione" che avrebbe potuto suggerire anche la considerazione di organizzazioni senza scopo di lucro come le associazioni oltre che le società cooperative: «*The DGA proposal is unclear on what the notion of 'data cooperative' concretely entails in terms of legal form and type of organisation. As the article in the proposed text on data cooperatives refers to "membership", this could suggest that they are envisaged as a non-profit type of organisation such as associations or cooperative societies. Yet, the DGA proposal provides no clear guidance about the legal form and the nature of this newly enacted entity, in contrast for instance with the clear requirement for data altruism organisations to be not-for-profit in order to be registered as such (see Section 5 below). In this respect, there is also no link made to 'European Cooperative Society' as a recognised legal form at the EU level. Cooperatives, as part of the European social model and the Single Market, have received strong recognition and support in various key EU documents. Under the EU acquis, the European Cooperative Society (ECS) aims to reduce existing cross-border obstacles for cooperatives and facilitate operation across European borders. It complements the legislation on European Companies (Societas Europaea or SE) laying out the general framework for a European public limited company*».

[22] Invero si tratta di una disposizione da cui è possibile inferire indizi sulle vesti giuridiche compatibili/incompatibili.

dati è contenuta nella definizione di cui al più volte richiamato art. 2, laddove, riferendosi alla loro struttura organizzativa, afferma che essa è «costituita da interessati, imprese individuali o da PMI, i quali sono membri di tale struttura».

Non è chiaro se questo elenco di membri debba interpretarsi come esclusivo (la cooperativa deve essere costituita solo ed esclusivamente da gruppi di interessati e/o gruppi di imprese individuali e/o gruppi di PMI) oppure come esemplificativo ed aperto anche ad altri soggetti (la cooperativa può essere costituita da qualunque PF o PG – ivi inclusi soggetti pubblici- purché fra questi soggetti vi siano anche gruppi di interessati e/o gruppi di imprese individuali e/o gruppi di PMI).

L'interpretazione "esclusiva" (che sembra quella suggerita dalla lettera della norma) impone che soggetti giuridici come le persone giuridiche (di seguito, per brevità "PG") di grandi dimensioni o gli enti pubblici siano esclusi dalla compagine sociale della cooperativa di dati, a meno che non creino appositi veicoli, con le caratteristiche della PMI (l'unica delle tre categorie di membri della struttura a non essere unipersonale), per partecipare alla cooperativa di dati.

La seconda soluzione interpretativa potrebbe invece aprire la strada alla partecipazione, nella cooperativa di dati, anche di PG, non necessariamente ricadenti nell'ambito delle PMI, così come alla partecipazione diretta di soggetti pubblici [23].

4.3. La *membership* degli interessati e il superamento della lettura restrittiva dei principi di neutralità, separazione e indipendenza.

L'elenco poc'anzi richiamato, contemplando gli interessati (oltre che le imprese individuali e le PMI) quali membri della struttura giuridica, consente di tracciare una significativa discriminante fra la cooperativa di dati e gli intermediari di dati [24] e di superare l'ostacolo ermeneutico che poteva essere rappresentato da una lettura rigorosa dei principi di indipendenza [25], neutralità e separazione [26].

---

[23] Il tema verrà ripreso *infra*, par. 4.4.

[24] Il *discrimen* potrebbe avere significative ricadute sulla stratificazione interpretativa inerente le norme riguardanti gli infomediari e la loro applicazione agli intermediari di dati c.d. puri (quelli alla cui struttura interessati e titolari di dati non partecipano) e alle cooperative di dati.

[25] Il concetto di indipendenza può inferirsi dal *considerando* n. 27 che, letto in combinato disposto con l'art. 12, par. 1, lett. *a*), sembra delineare una figura di intermediario di dati (puro) terza e neutrale rispetto agli altri soggetti coinvolti nella dinamica dell'intermediazione: «I servizi di intermediazione dei dati specializzati, che sono indipendenti dagli interessati, dai titolari dei dati e dagli utenti dei dati, potrebbero facilitare l'emergere di nuovi ecosistemi basati sui dati indipendenti da qualsiasi operatore che detenga un grado significativo di potere di mercato, prevedendo nel contempo un accesso non discriminatorio all'economia dei dati per le imprese di tutte le dimensioni, in particolare le PMI e le start-up con mezzi finanziari, giuridici o amministrativi limitati».

È evidente che laddove gli interessati (e i titolari di dati) fossero membri della struttura dell'intermediario risulterebbe difficile conciliare questa sovrapposizione con un concetto di indipendenza.

[26] I principi di neutralità e separazione, letti in combinato disposto col principio di indipendenza, possono essere intesi non solo come riferiti alle attività (cfr. par. 3.2), ma a monte come volti a sepa-

Il DGA con questo tassello precisa che, nell'ambito delle cooperative di dati, gli interessati e i titolari dei dati (imprese individuali e PMI), non sono entità separate dalla cooperativa ma la costituiscono, poiché ne sono i membri/soci/associati.

Questa precisazione normativa estende quindi l'ambito dei fornitori di SID (laddove si tratti di cooperative di dati) anche a veicoli giuridici non del tutto indipendenti, neutrali e separati dai soggetti interessati e/o titolari dei dati.

4.4. I requisiti della struttura dei fornitori di SID e l'applicabilità alle cooperative di dati: la commercialità e l'ammissibilità di una cooperativa di dati ente pubblico/organizzazione per l'altruismo dei dati.

L'analisi della struttura delle cooperative di dati deve essere integrata con l'esame delle disposizioni previste, per tali aspetti, dalla disciplina degli infomediari in genere.

Nell'ambito delle norme riguardanti gli intermediari, il legislatore aggiunge l'ulteriore elemento della commercialità dei rapporti fra interessati/titolari dei dati e utenti dei dati, ammettendo fra i fornitori di servizi di intermediazione di dati:

– gli enti pubblici [27], allorquando abbiano l'«intenzione di creare rapporti commerciali» (giacché in mancanza di tale "intenzione" si esula dall'ambito applicativo del Regolamento) [28];

– nonché le organizzazioni per l'altruismo dei dati, ma solo allorquando i servizi che erogano creino (o per usare la terminologia del Regolamento "puntino" a creare) un rapporto commerciale tra potenziali utenti dei dati, da un lato, e interessati e titolari dei dati che mettono a disposizione i dati per motivi altruistici, dall'altro [29].

---

rare i soggetti posti in relazione nella dinamica dell'intermediazione (interessati/titolari di dati e utenti dei dati) dal fornitore di SID per assicurare un elevato livello di indipendenza dello stesso ed aumentare la fiducia.

[27] Il *considerando* n. 27 ammette infatti che «I fornitori di servizi di intermediazione dei dati, che possono includere anche enti pubblici, che offrono servizi che collegano i diversi soggetti dispongono del potenziale per contribuire alla messa in comune efficiente dei dati come pure all'agevolazione della *condivisione bilaterale* dei dati».

Al successivo *considerando* n. 29 si precisa però che «Il presente regolamento non dovrebbe applicarsi ai servizi offerti da enti pubblici così da facilitare il riutilizzo di dati protetti, detenuti da diversi enti pubblici conformemente al presente regolamento, o l'utilizzo di eventuali altri dati, nella misura in cui tali servizi non abbiano l'intenzione di creare rapporti commerciali».

[28] Cfr. l'art. 2 par. 1, n. 11, lett. *d*) e il *considerando* n. 29.

[29] Il legislatore europeo invero, con riguardo al rapporto fra SID e organizzazioni per l'altruismo dei dati, si esprime sempre in termini negativi affermando che le «organizzazioni per l'altruismo dei dati [...] non dovrebbero essere considerate offrire servizi di intermediazione dei dati a condizione che tali servizi non creino un rapporto commerciale tra potenziali utenti dei dati, da un lato, e interessati e titolari dei dati che mettono a disposizione i dati per motivi altruistici, dall'altro» (*considerando* n. 29). Ancora più chiaramente all'art. 15 rubricato "Deroghe" si legge che «Il presente capo [dedicato ai servizi di intermediazione dei dati, *n.d.a.*] non si applica alle organizzazioni per l'altruismo dei dati

Potenzialmente, quindi, anche un ente pubblico e un'organizzazione per l'altruismo dei dati (e, per l'effetto, anche un'associazione senza scopo di lucro)[30], laddove generino un rapporto commerciale fra fornitori di dati (interessati/titolari) e utenti di dati, possono erogare SID e quindi considerarsi un infomediario.

Il requisito della commercialità ripropone, in questo contesto, le medesime problematiche rilevate nel precedente paragrafo (nel contesto delle attività costituenti SID), avendo il legislatore europeo omesso di chiarire cosa voglia intendere con «creare rapporti commerciali fra interessati/titolari di dati e utenti».

Una parte della dottrina interpreta il requisito della commercialità, riferendolo al veicolo giuridico, come ostacolo all'ammissione di fornitori di SID (e quindi anche di cooperative di dati) che abbiano la veste di enti pubblici o di enti senza scopo di lucro[31] (essendo questi enti, pubblici o privati, assorbiti dalla disciplina delle organizzazioni per l'altruismo dei dati)[32]; altra parte della dottrina evidenzia come la

---

riconosciute o ad altre entità senza scopo di lucro nella misura in cui le loro attività consistono nel cercare di raccogliere, per obiettivi di interesse generale, dati messi a disposizione da persone fisiche o giuridiche sulla base dell'altruismo dei dati, a meno che tali organizzazioni e entità non puntino a stabilire relazioni commerciali tra un numero indeterminato di interessati e titolari dei dati, da un lato, e utenti dei dati, dall'altro».

[30] Ai sensi dell'art. 18 infatti l'organizzazione per l'altruismo dei dati per poter essere registrata, deve avere i seguenti requisiti: *a)* svolgere attività di altruismo dei dati; *b)* essere una persona giuridica costituita a norma del diritto nazionale per conseguire obiettivi di interesse generale, stabiliti nel diritto nazionale, ove applicabile; *c)* operare senza scopo di lucro ed essere giuridicamente indipendente da qualsiasi entità che operi a scopo di lucro; *d)* svolgere le proprie attività di altruismo dei dati mediante una struttura funzionalmente separata dalle sue altre attività; *e)* rispettare il codice di cui all'art. 22, par. 1, al più tardi entro 18 mesi dopo la data di entrata in vigore degli atti delegati di cui a tale paragrafo.

[31] Lo sostiene, sia pure in senso critico, E. BIETTI-M. MANNAN, *Data Cooperatives in Europe: A Legal and Empirical Investigation White Paper created as part of The New School's Platform Cooperativism Consortium and Harvard University's Berkman Klein Center for Internet & Society Research Sprint*, cit., «*By saying that negotiating and dialogue-building activities fall within the purview of for-profit data cooperatives – the only type of data cooperative recognized by the DGA – it distracts from the efforts of other actors involved in these activities and contributes to its commercialization*» che, nel riferirsi alle attività delle cooperative, afferma incidentalmente che l'unico tipo di cooperativa ammessa dalla DGA è quella con scopo di lucro.

Analogamente e sempre in senso critico S. GIRISH-M. AVERY, *Data cooperative: Enabling meaningful collective negotiation of data rights for communities*, cit., che evidenzia come la legge sulla *governance* dei dati dell'UE definisca le cooperative di dati in modo limitante in quanto non riconosce le cooperative di dati senza scopo di lucro, peraltro già esistenti nella prassi «*The EU Data Governance act defines data cooperatives and clarifies that they have 'fiduciary duties' however such a definition is limiting as it does not fit in cooperatives that seek to pool and process aggregated data and fails to recognise non-profit data cooperatives that exist, both in the EU (e.g., Salus) and beyond (e.g., MIDATA)*».

[32] In realtà questa conclusione è tutt'altro che pacifica. In attesa che il Regolamento venga applicato e che la giurisprudenza chiarisca gli aspetti rimasti offuscati, non è da escludersi che residui un cono d'ombra, sottratto alla disciplina dei SID e delle organizzazioni per l'altruismo dei dati, nell'ambito del quale molti servizi collaterali all'intermediazione (e per estensione i loro fornitori) potrebbero ricadere. Fra di essi probabilmente i servizi che non generano rapporti commerciali (qualun-

formulazione dei *considerando* (sono esclusi … laddove non creino rapporti commerciali…) al contrario ammetta anche gli enti pubblici e/o associazioni senza scopo di lucro [33] (perdendo altrimenti significato la delimitazione della deroga ai soli enti pubblici e organizzazioni per l'altruismo dei dati che non generano rapporti commerciali).

Invero il requisito della commercialità, più che riferito alla natura giuridica del veicolo (che quindi è irrilevante se sia o meno commerciale o altruistica), sembra riguardi, come sottolinea la lettera delle disposizioni che lo menzionano, la relazione che l'intermediazione dei dati (qualunque sia il veicolo prescelto dall'intermediario: società commerciale, ente pubblico, associazione senza scopo di lucro

---

que cosa ciò voglia dire) ma che al contempo non sono organismi per l'altruismo dei dati (entità peraltro che, diversamente dai fornitori di SID, non sono obbligate a qualificarsi come organizzazioni per fini altruistici se non allo scopo di fruire della condivisione dei dati donati per tale scopo).

[33] Che si ritroverebbero in alcuni casi, ad essere sussumibili sotto la duplice etichetta di cooperative di dati (od anche più in generale fornitori di SID) e organizzazioni di altruismo dei dati. Accennano a questo tema M. MICHELI-E. FARRELL-B. CARBALLA SMICHOWSKI-M. POSADA SÁNCHEZ-S. SIGNORELLI-M. VESPE, *Mapping the landscape of data intermediaries Emerging models for more inclusive data governance*, cit., ove si ritiene plausibile che le cooperative, a seconda di come sono implementate, possano avere un modello di *business* con o senza scopo di lucro. Analogamente J. BALOUP-E. BAYAMLIOĞLU-A. BENMAYOR-C. DUCUING, *White Paper on Data Governance Act*, cit., che facendo leva sul concetto di *membership* ritiene che le organizzazioni senza scopo di lucro possano costituire la veste giuridica della cooperativa di dati. A valorizzare la natura anfibia delle cooperative di dati (profit e no-profit) E. BIETTI-M. MANNAN, *Data Cooperatives in Europe: A Legal and Empirical Investigation White Paper created as part of The New School's Platform Cooperativism Consortium and Harvard University's Berkman Klein Center for Internet & Society Research Sprint*, cit.: «Alcune cooperative cercano di isolarsi dal mercato adottando uno *status no profit*: ciò consente loro di godere di sgravi fiscali (a seconda della giurisdizione) e di accedere a sovvenzioni, finanziamenti governativi, ecc. Tuttavia, è probabile che questa forma di finanziamento non sia sufficiente, da sola, a coprire i costi sostanziali dello sviluppo e della commercializzazione del *software*. Altre cooperative operano come entità commerciali, il che apre la possibilità di ricevere finanziamenti da un maggior numero di attori del mercato. Ciò può includere l'inclusione di investitori esterni come categoria distinta di soci all'interno della cooperativa, che detengono una classe distinta di azioni, nonché l'emissione di obbligazioni cooperative, titoli di partecipazione e certificati senza diritto di voto. Ci sono inoltre diversi casi in cui le cooperative agricole sono "diventate pubbliche", costituendo una filiale che si quota in borsa o addirittura quotando le proprie azioni (spesso privilegiate) in borsa. Per alcuni, queste "cooperative imprenditoriali" continuano a svolgere la funzione di rimediare a un mercato mal funzionante, mentre per altri questa deriva dal modello cooperativo tradizionale, che diluisce la proprietà e il controllo dei soci, comporta il rischio di demutualizzazione. La demutualizzazione si riferisce al processo degenerativo attraverso il quale una cooperativa perde il suo carattere democratico e il suo scopo mutualistico. Sebbene esista una ricca letteratura sull'argomento, per i nostri scopi è sufficiente dire che essi contribuiscono all'erosione della differenza delle cooperative rispetto alle controparti aziendali. Il fatto che possano coesistere motivazioni economiche non lucrative, imprenditoriali e altre motivazioni economiche ibride dimostra, in senso più ampio, l'ambivalenza politica delle cooperative, comprese le cooperative piattaforma. di assunzione di capitale. D'altro canto, è stato criticato il fatto che le cooperative, comprese le cooperative di piattaforma, non siano in grado di svincolarsi dalla logica dei mercati capitalistici» (traduzione a cura dell'a.).

etc.) deve generare fra fornitori di dati (interessati/titolari di dati) e utenti dei dati [34].

Anche spostando l'analisi sulla commercialità del rapporto fornitori di dati/utenti, rimangono tuttavia poco chiari i profili già visti nel paragrafo precedente (cosa deve intendersi con il concetto di commercialità? In caso di fornitori di SID che eroghino servizi accessori, in parte onerosi, in parte gratuiti, la mera presenza dei servizi gratuiti colloca automaticamente il fornitore in un cono d'ombra ove non trova applicazione né la disciplina dei SID né quella sull'altruismo dei dati? Cosa deve intendersi con generare un rapporto commerciale fra fornitori di dati e utenti dei dati? Questo rapporto deve essere "diretto"?).

Prescindendo dalla soluzione da dare al tema della commercialità, ove ipotizzassimo di ricadere in una delle casistiche di ente pubblico (o di organizzazione per l'altruismo dei dati) che abbia l'«*intenzione di creare rapporti commerciali*», in questo caso, dunque, rientreremmo in una delle residuali ipotesi in cui la cooperativa di dati potrebbe assumere la veste di ente pubblico (o di organizzazione per l'altruismo dei dati); questa ipotesi (in particolare per quanto riguarda l'ente pubblico) si ricollega al tema strutturale summenzionato (*supra*, parr. 4.2 e 4.3), e in specie all'interpretazione da dare all'elenco dei membri della cooperativa di dati. La lettura esclusiva – cui poc'anzi si accennava (i membri della cooperativa possono essere solo interessati e/o imprese individuali e/o PMI) – risulta difatti sconfessata dall'ipotesi residuale da cui muoviamo e ciò in quanto lo Stato e gli altri Enti Regionali e Locali (gli *shareholder* di un ente pubblico e quindi i membri della cooperativa di dati – ente pubblico) non sono sussumibili in alcuna delle tre categorie [35]

---

[34] Sembra darlo per scontato M. MICHELI-E. FARRELL-B. CARBALLA SMICHOWSKI-M. POSADA SÁNCHEZ-S. SIGNORELLI-M. VESPE, *Mapping the landscape of data intermediaries Emerging models for more inclusive data governance*, cit., laddove rileva che fra gli obiettivi principali dei requisiti della DGA (e in specie quelli di neutralità e separazione) vi sia quello di non fare dipendere il modello di *business* di un fornitore di SID dal fatto di trarre profitto diretto dalle informazioni che sta condividendo, cosicché gli unici beneficiari del valore dei dati siano i fornitori di dati e gli utenti di dati, non i fornitori di servizi di intermediazione che consentono la condivisione dei dati: «*A key objective of these DGA requirements is for data holders/subjects to know that the business model of a DISP does not depend on making a direct profit from the information it is sharing. The only beneficiaries of the data value shall be the data suppliers and selected/known data users, not the intermediation services providers that enable the data sharing. This set of conditions clearly distinguishes DISPs from those large online platforms that qualify as gatekeepers according to the Digital Markets Act, as well as from other kinds of data intermediaries that do not meet the DGA criteria*».

[35] Va ricordato infatti che l'art. 2, par. 1, n. 17) e 18) definisce: l'ente pubblico come «le autorità statali, regionali o locali, gli organismi di diritto pubblico o le associazioni formate da una o più di tali autorità oppure da uno o più di tali organismi di diritto pubblico».

E gli organismi di diritto pubblico come «gli organismi che hanno le caratteristiche seguenti: *a*) sono istituiti per soddisfare specificatamente bisogni d'interesse generale e non hanno carattere industriale o commerciale; *b*) sono dotati di personalità giuridica; *c*) le loro attività sono finanziate in modo maggioritario dallo Stato, da autorità regionali o locali o da altri organismi di diritto pubblico, o la loro gestione è soggetta alla supervisione da parte di tali autorità o organismi, oppure sono dotati di un organo di amministrazione, di direzione o di vigilanza in cui più della metà dei

di membri della cooperativa di dati [36]. Sembrerebbe quindi che l'unica lettura che concilia le due norme (quella che non esclude radicalmente gli enti pubblici e quella che elenca i membri delle cooperative di dati) sia quella che interpreta l'elenco dei membri nel senso di ammettere, oltre alle categorie richiamate dalla lettera della norma, anche ulteriori soggetti e fra di essi, quantomeno, gli *shareholder* di un ente pubblico.

4.5. (*segue*) Il requisito dell'apertura dei servizi.

Fra le disposizioni riguardanti la struttura degli infomediari in genere che meritano attenzione vi sono quelle che escludono, dall'ambito applicativo della disciplina dei SID, i servizi destinati ad essere utilizzati da un gruppo chiuso o da un titolare di dati per consentire l'uso dei suoi dati [37].

Questa disposizione ha un significativo impatto concorrenziale, atteso che impedisce agli infomediari DGA *compliant* di scegliere i fornitori di dati e quindi di creare degli ecosistemi formati da intese fra i fornitori di dati.

Considerate le differenze fra l'intermediario di dati puro e la cooperativa di dati [38], appare di tutta evidenza come questa potenziale apertura a qualunque titolare di dati, nelle due casistiche, abbia degli effetti strutturali diversi:

– mentre nel caso di un infomediario puro, che è un soggetto distinto dai fornitori di dati, l'accesso di questi ultimi ai SID avviene all'interno della dinamica che è la stessa che normalmente si instaura fra soggetti terzi (committente del servizio vs fornitore del servizio) e pertanto teorizzare dei SID aperti non ha peculiari riflessi sulla struttura dell'infomediario stesso;

– nel caso di una cooperativa di dati, poiché i fornitori di dati (interessati e titolari di dati) partecipano alla struttura (della cooperativa di dati), assicurare il servizio di intermediazione a qualunque titolare (e quindi assicurare la *membership* a chiunque)

---

membri è designata dallo Stato, da autorità regionali o locali o da altri organismi di diritto pubblico».

[36] Resterebbero invero «gli organismi di diritto pubblico» (poiché le associazioni formate «da una o più di tali autorità» riconduce a entità aventi fra i propri membri lo Stato e gli Enti Regionali e Locali), i quali tuttavia si caratterizzano (secondo la definizione DGA) per il fatto di non avere «carattere industriale o commerciale».

[37] In questo senso art. 2, par. 1 n. 11, lett. *c*), e *considerando* n. 28, DGA.

Sono difatti escluse le piattaforme di scambio dati utilizzate da un unico titolare per consentire l'utilizzo dei dati da parte di terzi e le piattaforme dati dell'*Internet of things* sviluppate esclusivamente per garantire funzionalità dei dispositivi connessi e consentire servizi a valore aggiunto.

Si pone in linea con questo requisito l'art. 12, lett. *f*), DGA.

[38] D'ora innanzi quando ci si riferisce all'intermediario (o informediario) "puro" si vuole rimarcare la differenza, evidenziata nel paragrafo 4.3, fra questi e la cooperativa di dati (anch'essa intermediario di dati, ma peculiare). Mentre il primo (l'intermediario di dati puro) ha una struttura separata, neutra e anche indipendente dai fornitori di dati, la seconda (la cooperativa di dati) si caratterizza per una *membership* formata anche da fornitori di dati (oltre che interessati, espressamente richiamati nell'elenco dei membri, anche titolari di dati, quali potrebbero essere imprenditori individuali e PMI).

nonché impedire una selezione fra di essi (il gruppo chiuso di titolari), comporta che la disposizione abbia un impatto sulla struttura della cooperativa di dati stessa.

Per riassumere, dunque, le disposizioni sulla struttura della cooperativa di dati sin ora analizzate, pur restando laconiche [39] (in quanto non aiutano ad individuare la natura giuridica della cooperativa dei dati o comunque a definire in modo certo lo spazio entro il quale si esercita la libertà di scelta del veicolo da impiegare), lasciano intendere che:

(i) i fornitori di dati possono/devono essere membri della struttura della cooperativa;

(ii) la cooperativa di dati, al ricorrere di certe condizioni, potrebbe identificarsi con un organismo per l'altruismo dei dati;

(iii) la cooperativa di dati, al ricorrere di certe condizioni, potrebbe identificarsi con un ente pubblico e pertanto, fra i suoi membri possono partecipare lo Stato, le Regioni, gli Enti locali od eventualmente altri enti pubblici;

(iv) la cooperativa di dati, in quanto intermediario di dati, deve restare aperta all'accesso dei potenziali titolari di dati [40].

---

[39] Sulla critica alla vaghezza del concetto di cooperativa di dati cfr. J. BALOUP-E. BAYAMLIOĞLU-A. BENMAYOR-C. DUCUING, *White Paper on Data Governance Act*, cit.; E. BIETTI-M. MANNAN, *Data Cooperatives in Europe: A Legal and Empirical Investigation White Paper created as part of The New School's Platform Cooperativism Consortium and Harvard University's Berkman Klein Center for Internet & Society Research Sprint*, cit.: «*Of particular relevance to cooperatives and the cooperative movement at large is the fact that the DGA advances a specific, and arguably muddled, conception of what data cooperatives are. As mentioned above, data cooperatives are defined in the proposal by three possible functions, without providing a clear, general definition*». Della medesima opinione anche EDPB, *Parere congiunto EDPB-GEPD 03/2021 sulla proposta di regolamento del Parlamento europeo e del Consiglio relativo alla governance europea dei dati (Atto sulla governance dei dati)*, disponibile all'indirizzo: https://www.edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032021-proposal_it, dove viene sottolineato (al par. 128) che «il concetto di "servizi di cooperative di dati", introdotto nell'articolo 9, paragrafo 1, lettera c) della proposta, resta poco chiaro in termini di natura e di obblighi. A questo riguardo è opportuno introdurre una definizione chiara di questi fornitori di servizi di condivisione dei dati e dei rispettivi obblighi applicabili, onde evitare qualsiasi incertezza giuridica nella fornitura di tali servizi».

[40] Altro requisito di struttura previsto per gli infomediari riguarda l'indeterminatezza del numero di interessati/titolari di dati: ai fornitori di SID infatti è richiesto di frapporsi tra un numero indeterminato di titolari/soggetti dei dati e gli utenti dei dati.

Questa precisazione ricorre in almeno tre disposizioni del Regolamento: l'art. 2, par. 1, n. 11, DGA, l'art. 15 del DGA e il *considerando* n. 28.

La precedente formulazione della bozza di DGA, al *considerando* n. 22 (l'antenato dell'attuale *considerando* n. 28) conteneva un riferimento a un termine diverso («indefinito» anziché «indeterminato»), ma soprattutto era riferita sia ai fornitori di dati (interessati/titolari dei dati) che agli utenti dei dati; (forse anche per questa ragione) la precedente versione ha subito un'espressa censura da parte del "Parere congiunto EDPB-GEPD 03/2021 sulla proposta di regolamento del Parlamento europeo e del Consiglio relativo alla *governance* europea dei dati". La nuova disposizione cambia la terminologia ma soprattutto riferisce il requisito della indeterminatezza ai soli fornitori di dati e non anche agli utenti.

5. Cooperative di dati e società cooperative preesistenti.

5.1. Il problema della compatibilità tra cooperativa di dati e società cooperativa *tout court*.

Delineati i controversi contorni del quadro normativo che disciplina le cooperative di dati, nel prosieguo analizzeremo la compatibilità fra questo nuovo soggetto e la società cooperativa, ipotizzando delle soluzioni che possano rappresentare modelli di *business* al contempo DGA *compliant* e sostenibili.

Il ricorso a un veicolo avente la natura giuridica di società cooperativa, come precedentemente accennato, rappresenta la soluzione, a livello strutturale, apparentemente più lineare e al contempo quella suggerita (almeno così sembrerebbe) dal legislatore, se non altro per la scelta terminologica operata (che menziona le "cooperative" dei dati) [41].

È oscuro il valore semantico che il legislatore europeo intendeva sottolineare introducendo il concetto di indeterminatezza (critici sul punto anche G. CAROVANO-M. FINCK, *Regulating data intermediaries: The impact of the Data Governance Act on the EU's data economy*, cit.) e in specie se tale richiamo volesse solo evocare l'esclusione dei servizi destinati ad essere utilizzati da un gruppo chiuso o da un titolare di dati per consentire l'uso dei suoi dati (ci si riferisce all''art. 2, par. 11, lett. *c*), e al *considerando* n. 28 che escludono esplicitamente i servizi destinati ad essere utilizzati da un gruppo chiuso o da un titolare di dati per consentire l'uso dei suoi dati), oppure se l'intento fosse quello di introdurre un requisito ulteriore rimasto tuttavia inespresso. Il potenziale semantico di questo termine rimane anch'esso affidato all'interpretazione della giurisprudenza europea.

[41] Il modello della società cooperativa va incontro al requisito dell'accesso non discriminatorio e aperto a una platea potenzialmente illimitata di fornitori di dati: il principio sancito all'art. 2528 c.c., difatti, nel prevedere un capitale variabile (non determinato in un ammontare definito) per le società cooperative, consente la possibilità di ingresso di nuovi soci in qualsiasi momento e senza particolari formalità (senza quindi l'intervento di un notaio), salva l'approvazione da parte dell'organo amministrativo, che deve verificare la presenza dei requisiti previsti dallo statuto coerentemente con lo scopo mutualistico e l'attività svolta.

Una tale lettura viene proposta anche da G. CAROVANO-M. FINCK, *Regulating data intermediaries: The impact of the Data Governance Act on the EU's data economy*, cit.

Sembrerebbe sottintenderlo anche L. PETRONE, *Il mercato digitale europeo e le cooperative di dati*, cit.: «Non solo la finalità mutualistica sarebbe confacente all'obiettivo di creare un mercato digitale europeo che sia distante dal modello adottato oltreoceano, bensì anche altri principi tipici del modello cooperativo, come il principio della parità di trattamento tra soci e della "porta aperta" che trovano espresso riconoscimento legislativo rispettivamente agli artt. 2516 e 2528 c.c.; principi, quelli appena citati che garantirebbero l'idoneità dell'organismo cooperativo a soddisfare astrattamente il medesimo bisogno in un numero indeterminato di soggetti, assicurando loro un trattamento equo e paritario ed evidenziandone la naturale inclinazione a porsi a servizio di quanti appartengono alla categoria prevista nell'atto costitutivo».

Tuttavia rimangono delle difficoltà nella conciliazione col modello della società cooperativa che, pur meritevoli di approfondimento, non saranno oggetto della presente trattazione. Ci si riferisce in particolare ai rapporti di scambio mutualistico fra la società cooperativa e i soci che la compongono e alla concretizzazione di questo scambio all'interno della cooperativa di dati in considerazione:

– del requisito della commercialità nell'ambito della cooperativa di dati (ossia l'esigenza per

Le principali difficoltà invero sorgono nella ricerca di una compatibilità fra le attività esercitate dalle cooperative di dati (cfr. par. 3) così come perimetrate dai limiti imposti ai SID dal principio di neutralità e il modello della società cooperativa, specie ove la società cooperativa sia preesistente.

Le cooperative di dati infatti potrebbero nascere come società cooperative costruite *ex novo* e *ad hoc* per lo svolgimento delle attività di SID oppure sfruttare strategicamente la struttura di società cooperative preesistenti, il loro avviamento, i loro dati, mediante una conversione delle stesse in cooperative di dati [42].

Nel paragrafo seguente saranno trattati gli aspetti che ostacolano, in particolare, quest'ultima soluzione, la quale avrebbe potuto rappresentare una strategia promettente per la diffusione delle cooperative di dati.

5.2. La conversione di una società cooperativa preesistente in cooperativa di dati.

Il principale ostacolo alla conversione di una società cooperativa preesistente in una cooperativa di dati è rappresentato dalla delimitazione dei trattamenti di dati prevista dalla disciplina dei SID.

L'interpretazione che – valorizzando i principi di neutralità, separazione e indipendenza – esclude i servizi accessori [43] limita fortemente l'attività degli infomediari e le loro prospettive di *business* [44] e ciò in quanto le elaborazioni dei dati volte ad aggiungere valore agli stessi sono quelle che aumentano la possibilità di attirare fornitori di dati ma soprattutto utenti. L'attrazione di domanda e offerta è infatti determinante per la costruzione di un mercato di dati tale da poter beneficiare di economie di scala e ridurre i costi (pochi fornitori di dati vuol dire pochi dati e conseguentemente pochi utenti).

Questi limiti rischiano pertanto, oltre che di ostacolare l'emergere di cooperative di dati create *ad hoc* ed *ex novo* (attesa la difficoltà di avviare un'attività senza

---

quest'ultima di creare un rapporto commerciale fra fornitori di dati/soci della società cooperativa e utenti dei dati e non quindi fra fornitori di dati/soci e società cooperativa di dati);

– nonché delle limitazioni apparentemente imposte agli infomediari in generale nell'erogazione di servizi accessori.

[42] Attraverso la creazione di un nuovo "livello di dati". In questo senso M. MICHELI-E. FARRELL-B. CARBALLA SMICHOWSKI-M. POSADA SÁNCHEZ-S. SIGNORELLI-M. VESPE, *Mapping the landscape of data intermediaries Emerging models for more inclusive data governance*, cit.

[43] Ci si riferisce a quei servizi volti ad aggregare arricchire e trasformare i dati forniti da interessati/titolari di dati «al fine di aggiungervi un valore sostanziale e concedono licenze per l'utilizzo dei dati risultanti agli utenti dei dati», di cui si è parlato ampiamente ai parr. 3.2 e 3.3.

[44] L'ostacolo purtroppo non può essere superato anche laddove si tenesse nella debita considerazione il requisito commerciale (ossia anche nel caso in cui si riconoscesse la sussumibilità dei servizi accessori nell'ambito dei SID ove instaurassero «*un rapporto commerciale tra i titolari dei dati e gli utenti dei dati*»), in quanto le difficoltà interpretative connesse al tema della commercialità, sintanto che non verranno dipanate, rappresentano un rischio per l'operatore che intenda configurarsi quale cooperativa di dati.

attrattive per il mercato degli utenti dei dati e per l'adesione dei fornitori di dati), soprattutto di frenare la trasformazione delle cooperative esistenti in cooperative di dati (specie laddove si tratti di cooperative aduse a erogare servizi che comportano processare i dati).

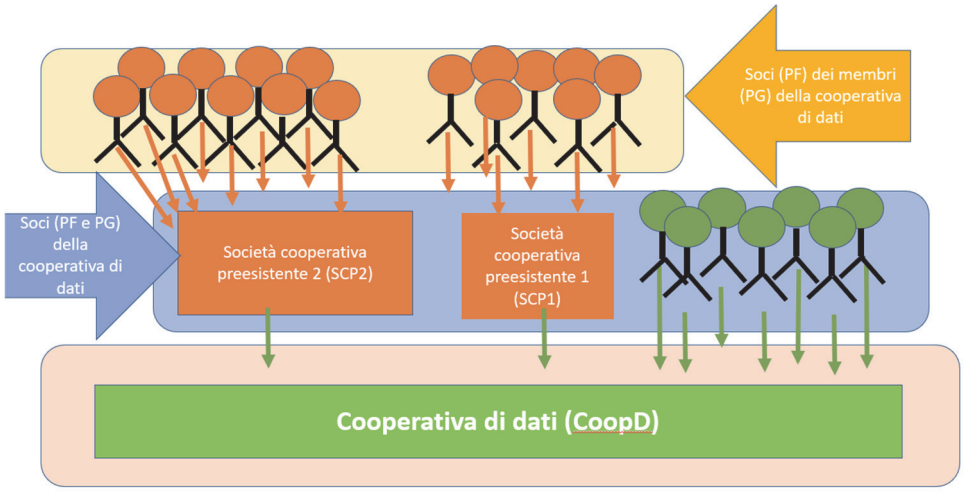
5.3. La *membership* delle cooperative preesistenti.

Una possibile soluzione – a metà strada fra cooperativa di dati *ad hoc* e cooperativa di dati frutto della conversione della società cooperativa preesistente – che al contempo consentirebbe di conciliare la limitazione dei servizi accessori e il coinvolgimento di realtà preesistenti, potrebbe essere rappresentata dalla partecipazione della cooperativa preesistente quale membro/titolare di dati della cooperativa di dati.

Nell'ambito della società cooperativa preesistente continuerebbero a essere offerti (o si attiverebbe *ex novo* l'offerta di) servizi accessori (analisi, aggregazione, manipolazione etc.) in favore dei propri membri cosicché i dati (anche personali) originari fatti confluire nella società cooperativa preesistente dagli originari interessati, da una parte, unitamente ai dati (personali o non) che rappresentano il prodotto dell'elaborazione dei servizi accessori effettuata dalla società cooperativa preesistente, dall'altra, costituirebbero i *data asset* forniti dalla cooperativa preesistente alla cooperativa di dati attraverso la *membership* (e, si accennerà, previo consenso espresso dei singoli interessati).

In sostanza il modello potrebbe schematizzarsi come di seguito.

Tabella 1: Descrizione dei livelli



La Tabella 1 descrive la struttura del modello che si ripartisce su tre livelli:

1) cooperativa di dati;

2) membri diretti: soci della cooperativa di dati (soci persone fisiche e soci persone giuridiche);

3) membri indiretti: soci delle persone giuridiche membri della cooperativa di dati.

La soluzione della *membership* di società cooperative preesistenti, se da una parte libera la cooperativa di dati dal problema esegetico dei servizi accessori (collegato al requisito della commercialità, spostando questa attività all'interno dei singoli membri), dall'altra non è priva di insidie applicative, limitazioni ed ostacoli.

Anzitutto, poiché la cooperativa di dati (come qualunque altro intermediario di dati DGA *compliant*) deve assicurare l'accesso indiscriminato ai potenziali interessati/titolari di dati, sembrerebbe vietato limitare l'accesso a cooperative preesistenti selezionate (perché gradite) e negando la partecipazione alle altre (magari perché concorrenti dell'entità capofila del progetto istitutivo della cooperativa di dati). Questo potrebbe fortemente disincentivare l'interesse delle cooperative preesistenti stesse alla creazione di un *network* all'interno di una cooperativa di dati aperta all'accesso di potenziali concorrenti [45].

Inoltre la soluzione, benché proposta per superare il principio di neutralità, rischia comunque di inciampare sui collegati principi di indipendenza e separazione.

Come difatti già rilevato, l'art. 12, par. 1, lett. *a*), prevede che gli intermediari non utilizzino i dati oggetto dei SID: «per scopi diversi dalla messa a disposizione di tali dati agli utenti dei dati» e i SID sono forniti «attraverso una persona giuridica distinta», richiedendo, nel caso si offrano servizi accessori, di separarli strutturalmente dall'intermediazione dei dati, creando un soggetto giuridico separato.

A questa disposizione si ricollega una gamma di soluzioni interpretative variegata [46], fra le quali anche quella che considera la mera separazione giuridica della cooperativa di dati dalla cooperativa preesistente (fornitore di dati e fornitore di servizi accessori sui dati) una condizione non sufficiente ad assicurare il rispetto

---

[45] Una incidentale menzione del tema si trova in S. GIRISH-M. AVERY, *Data cooperative: Enabling meaningful collective negotiation of data rights for communities*, cit., dove parlando della scalabilità delle cooperative si evidenziano le complessità della gestione di grandi cooperative di dati, complessità connesse principalmente alla difficoltà di rappresentare una vasta gamma di membri. All'uopo viene richiamato l'esempio di Driver's Seat (una cooperativa di proprietà di autisti fondata nel 2019 per aiutare a collettivizzare la *gig economy*), ove è sorto il problema della competizione degli autisti per le corse più remunerative (a fronte della limitatezza delle risorse, nel caso di specie rappresentate dalle aree geografiche con domanda di taxi).

[46] Quantomeno nel caso delle cooperative di dati, queste letture non possono arrivare a escludere la *membership* del fornitore di dati (interessato/titolare di dati) rispetto alla cooperativa di dati (che peraltro parrebbe uno dei requisiti delle cooperative di dati stesse).

dei requisiti imposti agli infomediari ove non accompagnata da una separazione sostanziale [47]. Una tale interpretazione tuttavia, quantomeno per quanto attiene alla cooperativa di dati, pare doversi escludere, atteso che laddove il legislatore europeo ha inteso imporre un'indipendenza e separazione anche sostanziale, lo ha espresso chiaramente [48].

Anche sposando la soluzione interpretativa che ammette una mera separazione fra veicoli, rimane aperto il problema della difficoltà di accentrare, in capo a un solo veicolo separato, i servizi accessori [49].

Non può poi essere ignorata la summenzionata lettera dell'art. 2 DGA che espressamente contempla, fra i membri della cooperativa, le persone fisiche, le imprese individuali e le PMI: la lettura più angusta lascerebbe fuori le società cooperative di grandi dimensioni. Tuttavia si è evidenziato, nel par. 4 come l'elenco dei membri meriti una lettura più generosa, l'unica in grado di conciliarsi con le disposizioni che si occupano degli enti pubblici.

Da ultimo la soluzione della *membership* delle società cooperative preesistenti, senza ulteriori correttivi, avrebbe comunque il limite [50]:

a) di generare dei comparti stagni all'interno della cooperativa di dati, rappresentati dal rapporto asfittico intercorrente fra ciascuna delle società preesistenti e i

---

[47] La separazione sostanziale sicuramente viene meno nel caso in cui sia offerta ad alcuni membri della cooperativa la possibilità di fornire servizi accessori e dati frutto di servizi accessori.

[48] Le disposizioni sull'indipendenza sostanziale sono principalmente tre:

– quella già vista di cui al *considerando* n. 27, riferita all'indipendenza dei fornitori di SID rispetto a interessati e titolari (si è già avuto modo di argomentare le ragioni per cui tale disposizione sia difficile da applicare alle cooperative di dati);

– il *considerando* n. 44 che si occupa dell'indipendenza delle autorità competenti dai fornitori di SID;

– l'art. 26 DGA, richiamato dall'art. 13, che sancisce indipendenza delle autorità competenti dai fornitori di SID.

[49] La separazione del soggetto cui vengono demandati servizi accessori apre infatti ad ulteriori riflessioni relative al suo rapporto con la cooperativa di dati. Ipotizziamo che nell'ambito della cooperativa di dati questo soggetto, che effettua elaborazioni sui dati (previo consenso degli interessati ove si discuta di dati personali e autorizzazione del titolare dei dati ove fossero dati non personali), si configuri, a sua volta, come un titolare di dati membro della cooperativa di dati. In tale ipotesi questo fornitore dei servizi accessori sui dati (in qualità di titolare di dati e membro della cooperativa di dati), in ragione del requisito dell'apertura dei servizi di cui all'art. 2, par. 1 n. 11, lett. *c*), e *considerando* n. 28, DGA (per approfondimenti cfr. par. 4.5) non può avere l'esclusiva sui servizi accessori all'interno della cooperativa di dati, non potendo quest'ultima creare gruppi chiusi di titolari di dati in ragione dell'espressa esclusione dai SID dei «servizi utilizzati esclusivamente da un titolare dei dati per consentire l'utilizzo dei dati detenuti da tale titolare dei dati, oppure utilizzati da varie persone giuridiche all'interno di un gruppo chiuso». Questa situazione, di fatto, potrebbe limitare la possibilità di accentrare, sia pure in capo a un veicolo separato, i servizi accessori di elaborazione sui dati.

[50] Beninteso, guardando la questione da un'altra prospettiva, questi apparenti limiti potrebbero considerarsi l'unica tutela per le società preesistenti dal rischio concorrenziale cui si è accennato nel presente paragrafo.

propri membri, e ciò in quanto confinando i servizi accessori al livello delle società preesistenti, non si verificano scambi ad esempio:

– fra gli interessati membri della società cooperativa preesistente 1 (di cui alla Tabella 1, di seguito per brevità "SCP1") e la società cooperativa preesistente 2 (di cui alla Tabella 1, di seguito per brevità "SCP2");

– e, viceversa, fra gli interessati membri di SCP2 e la società SCP1;

– fra gli interessati membri diretti della cooperativa di dati e SCP1 ed SCP2 [51];

b) di impedire una gestione accentrata di servizi accessori che consenta l'aggregazione ed elaborazione dei dati complessivi affluiti direttamente o indirettamente nella cooperativa di dati [52].

5.4. Le cooperative di dati quali spazi di dati.

Il primo limite potrebbe essere superato dall'implementazione di un'organizzazione tecnico-giuridica (della cooperativa di dati) [53] che consenta a ciascun interessato (membro diretto o indiretto della cooperativa) di mettere i propri dati (attraverso una specifica manifestazione del proprio consenso) [54] a disposizione dei trattamenti (di aggregazione, analisi, ricerca etc.) effettuati da una, o più, società cooperative preesistenti (di seguito "SCP") a sua/loro volta membro/i della cooperativa di dati.

Si verrebbe a generare in questo modo una rete sinergica di soggetti che svolgono ruoli e attività differenti e che interagiscono all'interno della cooperativa di dati [55].

Una simile rete di competenze, nel settore dei dati, è conosciuta come spazio di dati (c.d. "*data spaces*"), ecosistemi giuridici e tecnico-organizzativi in cui le in-

---

[51] Mentre non si vedono ostacoli a ipotizzare che un interessato, socio di una cooperativa preesistente, possa fruire, anche gratuitamente, dei servizi (accessori) sui dati erogati da parte della cooperativa preesistente di cui è membro, è invece più difficile comprendere in quale misura un interessato, membro diretto della cooperativa di dati oppure socio della cooperativa di dati preesistente SCP1, possa fruire dei servizi sui dati eventualmente erogati della cooperativa preesistente SCP2 con la quale l'interessato non ha rapporti di *membership*.

[52] Cfr. nota 49.

[53] Sposando l'interpretazione secondo cui la natura giuridica della cooperativa di dati (e quindi dell'organizzazione che stiamo ipotizzando) possa essere la più variegata (società di capitali, ivi inclusa la società cooperativa, ente pubblico, ente no profit etc., sul tema cfr. parr. 4.2 e 4.3), ipotizziamo la soluzione che sembra più semplificata di una cooperativa di dati con natura di società a responsabilità limitata.

[54] Questo comporterebbe l'implementazione di un'infrastruttura tecnico giuridica molto complessa e stratificata che consenta agli interessati, membri diretti e indiretti della cooperativa di dati, oltre che, a monte, di manifestare un consenso specifico per ciascuno dei trattamenti e delle attività trasversali svolte dalle società cooperative preesistenti, a valle di separare le posizioni garantendo la pronta limitazione o inibizione del trattamento in caso di revoca del consenso.

[55] S.r.l.

formazioni (siano o meno dati personali) possono fluire ed essere condivise in modo efficiente e sicuro [56], all'interno di uno spazio dove interagiscono diversi soggetti [57], in particolare:

(i) i fornitori di dati (personali e non personali): vale a dire gli interessati o i titolari dei dati;

(ii) gli utenti dei dati: vale a dire i soggetti interessati ad utilizzare i dati;

(iii) i fornitori di servizi: vale dire soggetti che forniscono servizi sui dati (elaborazione dei dati, analisi, sintesi, etc.) messi a disposizione dagli interessati o dai titolari di dati;

(iv) gli utenti dei servizi di dati: vale a dire i soggetti in favore dei quali sono destinati i servizi sui dati o il dato-prodotto elaborato dal fornitore di servizi;

(v) il fornitore dello spazio di dati: vale a dire il soggetto che mette a disposizione la tecnologia e l'infrastruttura su cui si basa lo spazio di dati;

(vi) l'intermediario di dati: vale a dire il soggetto che mette in relazione fornito-

---

[56] L'incentivo allo sviluppo di *Data Spaces* (e in particolare di *Data Spaces* sicuri) è in linea con gli ambiziosi piani politici del Decennio Digitale dell'Unione, che mirano a plasmare il futuro dell'Europa entro il 2030. In particolare il *Data Governence Act* pone le basi per una disciplina degli spazi di dati destinata ad essere completata attraverso delle normative specifiche per la regolazione dei settori strategici che al momento sono stati individuati nelle seguenti materie: Agricoltura, Patrimonio culturale, Energia, Finanza, Green Deal, Salute, Lingua, Settore manifatturiero, Media, Mobilità, Pubblica amministrazione, Ricerca e innovazione, Competenze, Turismo. Per maggiori dettagli si invita alla consultazione del sito della Commissione europea ed in particolare: COMMISSIONE EUROPEA, *Plasmare il futuro digitale dell'Europa*, *Spazi comuni europei di dati*, disponibile all'indirizzo: https://digital-strategy.ec.europa.eu/it/policies/data-spaces. Ulteriori approfondimenti in M.PAGE-G. CECCONI, *European data spaces and the role of data.europa.eu*, disponibile all'indirizzo https://data.europa.eu/sites/default/files/report/Data_Spaces_Panel_Report_EN.pdf.

Nella primavera del 2024 il Parlamento europeo e il Consiglio hanno raggiunto un accordo politico sulla proposta della Commissione di uno spazio europeo dei dati sanitari (la bozza della proposta è disponibile all'indirizzo: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:197:FIN).

Per approfondimenti in generale sugli spazi di dati si vedano: S. SCERRI- T.TUIKKA-I.L. DE VALLEJO-E. CURRY, *Common European Data Spaces: Challenges and Opportunities*, in S. SCERRI- T. TUIKKA-I.L. DE VALLEJO-E. CURRY (a cura di), *Data Spaces*, 2022, disponibile al sito https://doi.org/10.1007/978-3-030-98636-0_16; B. OTTO, *The Evolution of Data Spaces*, in B. OTTO-M. TEN HOMPEL-S. WROBEL (a cura di), *Designing Data Spaces*, 2022, disponibile all'indirizzo https://doi.org/10.1007/978-3-030-93975-5_1; T. MARGONI-C. DUCUING-L. SCHIRRU, *Data Property, Data Governance and Common European Data Spaces*, in *Tijdschrift voor Informatica, Telecommunicatie en Recht*, 2023, disponibile all'indirizzo: https://ssrn.com/abstract=4428364 or http://dx.doi.org/10.2139/ssrn.4428364; N. ZINGALES, *Data Collaboratives, Competition Law and the Governance of EU Data Spaces,* 2021, disponibile all'indirizzo: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3897051; W. LI-P.QUINN, *The European Health Data Space: An expanded right to data portability?*, in *Computer Law & Security Review*, 52, 2024, 105913, disponibile all'indirizzo: https://doi.org/10.1016/j.clsr.2023.105913.

[57] Per esemplificare il funzionamento di uno spazio di dati complesso si rinvia ai risultati del progetto DS4Skills un progetto in corso di realizzazione. DS4Skills è un consorzio. Per approfondimenti si rinvia all'indirizzo: https://www.skillsdataspace.eu/what-is/.

ri di dati e gli utenti di dati e che supporta i suoi membri nell'esercizio dei propri diritti sui dati.

I ruoli dei soggetti summenzionati, nell'ambito dello spazio di dati, sono peraltro suscettibili di scambio e sovrapposizione, ad esempio:

(i) il titolare dei dati, nella misura in cui rielabora i dati dei propri soci/membri (come nella ipotesi di SCP1), potrebbe diventare un fornitore di servizi all'interno dello spazio di dati;

(ii) l'interessato potrebbe concedere l'uso dei propri dati per fruire dei servizi offerti da fornitori di servizi e quindi diventare, all'interno dello spazio di dati, un utente dei servizi;

(iii) l'utente dei dati potrebbe, una volta ottenuta la concessione dell'uso degli stessi, rielaborarli e fornire servizi sui dati.

Poiché la cooperativa di dati si differenzia dall'intermediario di dati puro (in quanto si caratterizza per l'adesione alla sua struttura di fornitori di dati) diventa plausibile ipotizzare (accanto al tradizionale ruolo assunto dall'intermediario puro, che si sostanzia in una partecipazione allo spazio di dati, marginale e tendenzialmente neutra, quale mero intermediario fra una domanda di dati e una offerta di dati) la configurazione di uno "spazio di dati-cooperativa di dati", ossia uno spazio di dati che coincide, in larga parte, con la cooperativa di dati, la quale ingloba, attraverso la *membership*, i fornitori di dati e di servizi.

Mentre infatti il ruolo dell'intermediario puro di dati è *naturaliter* creato per collocarsi all'interno di uno spazio di dati, ricoprendo la funzione precipua di collegare, in modo neutro e imparziale, fornitori di dati e utenti dei dati (essendo questi tre soggetti separati fra loro), la cooperativa di dati non ha questo ruolo neutro e imparziale in particolare nei confronti dei fornitori di dati (che ne sono membri).

La cooperativa di dati fungerebbe quindi essa stessa (parzialmente) da spazio di dati, fagocitando (nel senso di associarli) oltre che i fornitori di dati (propri membri) anche i fornitori di servizi (o meglio i fornitori di dati che svolgono il ruolo di fornitori di servizi sui dati), favorendo il dinamismo fra i ruoli dei propri membri (diretti e indiretti) e ammettendo che l'interessato possa, esprimendo il proprio specifico consenso in tal senso, beneficiare dei servizi dei vari "membri- fornitori di servizi" (diventando in questo modo, un utente dei servizi).

La soluzione che si propone, dunque, fonde una parte della struttura dello spazio di dati con la soluzione della *membership* delle società cooperative preesistenti di cui si parlava nel precedente paragrafo, moltiplicando i membri (persone giuridiche), di modo da pervenire, all'interno della cooperativa di dati, alla costruzione di una rete di società (*ex novo* o preesistenti) che si integrano a livello orizzontale (effettuando le medesime attività) o a livello verticale (poiché svolgono attività e servizi diversi, sia pur tra loro collegati).

In un tale contesto le possibili dinamiche, all'interno dello spazio di dati-cooperativa di dati, potrebbero aprire maggiori opportunità di *business* e arricchire l'offerta dei servizi resi disponibili oltre che agli interessati anche agli utenti, rendendo appetibile, per gli interessati, la partecipazione alla cooperativa di dati e per

gli utenti l'acquisto dei dati e dei servizi offerti, in questo modo compensando gli apparenti limiti posti all'offerta dei SID.

5.5. L'accentramento dei servizi accessori.

L'ultimo dei limiti della *membership* delle società preesistenti citato potrebbe invero essere superato facendo leva sulle norme che ammettono la possibilità per gli infomediari di erogare servizi accessori, ipotizzando un'interpretazione del requisito della commercialità che si concili con le richiamate peculiarità delle cooperative di dati (in particolare quella rappresentata dal rapporto strutturale intercorrente fra di esse e i titolari di dati).

La soluzione che si propone è di riconoscere che il rapporto commerciale fra titolari dei dati (nonché membri della cooperativa di dati) e utenti dei dati, nella cooperativa di dati, si genera a valle dell'erogazione di servizi accessori accentrati [58] e che pertanto alla cooperativa di dati è consentito erogare servizi accessori aventi a oggetto i dati che i propri membri, diretti o indiretti, abbiano consentito a conferire per tale scopo.

Una volta che il servizio accessorio sia stato erogato (i dati sono stati aggregati analizzati etc.), il prodotto di tale servizio, di cui i membri (diretti o indiretti) della cooperativa di dati beneficiano, si converte eventualmente in un *asset* di dati suscettibile a sua volta di essere intermediato e quindi di generare un rapporto commerciale fra gli interessati/titolari di dati che vi hanno partecipato (eventualmente prevedendo in favore di questi ultimi una remunerazione) e gli utenti dei dati.

Diversamente argomentando, la disposizione in materia di servizi accessori ammissibili nella misura in cui generino un rapporto commerciale fra interessati/titolari di dati e utenti di dati resterebbe lettera morta [59].

Questa lettura potrebbe inoltre, in alcuni casi, aprire alla possibilità di una conversione di cooperative preesistenti in cooperative di dati [60], sebbene residuino problemi interpretativi e applicativi che non sono stati approfonditi in questa sede ma che meriterebbero una trattazione a sé stante [61].

---

[58] Ovviamente a condizione che vi sia, da parte degli interessati i cui dati siano stati messi a disposizione dai titolari di dati, espressa manifestazione del consenso da parte di ciascun interessato, membro diretto o indiretto della cooperativa di dati.

[59] Atteso che non residuano altri margini applicativi percorribili.

[60] Cfr. par. 5.2.

[61] Non sono stati in questa sede approfonditi, *ex multis*, i seguenti temi:

1) quale è il titolo in virtù del quale la cooperativa di dati dispone dell'*asset* dei dati dei fornitori di dati. In particolare tali *asset* sono dei conferimenti veri e propri (acquisiti come capitale sociale), dei versamenti "mediante altre utilità" (acquisiti al patrimonio netto della società), ovvero sono messi a disposizione della cooperativa di dati mediante una licenza, od altro contratto?

2) definito il titolo in ragione del quale la cooperativa di dati mette in condivisione l'*asset* dei dati, come si delinea il rapporto commerciale (diretto) fra fornitori di dati e utenti di dati, all'interno del-

6. Brevi cenni conclusivi.

La normativa DGA che avrebbe fra i suoi scopi quello di incentivare la costruzione di un nuovo e alternativo mercato di dati rischia, con le limitazioni imposte, di boicottare fortemente il suo scopo primario atteso che, a oltre sei mesi dalla sua applicabilità, la ricerca delle soluzioni e dei modelli *di business* in grado di assicurare al contempo la *compliance* e la sostenibilità economica delle cooperative di dati continua a rappresentare una sfida.

Le scelte normative operate dal Regolamento unitamente alla vaghezza con cui sono stati tracciati limiti ed esclusioni rischiano di mettere in pericolo le cooperative già esistenti (molte delle quali basate su modelli di *business no profit latu sensu*) [62] ma anche di ostacolare l'emergere di nuove cooperative di dati e quindi di non far mai decollare questo nuovo soggetto [63] (considerata peraltro la difficoltà interpretativa connessa già solo alla comprensione dei requisiti giuridici necessari ad assicurarne la *compliance*).

Il ruolo di interpreti non può che andare nel senso di cercare e proporre delle soluzioni ermeneutiche in grado di incoraggiare la tenuta giuridico-economica di un soggetto che deve ancora vedere la luce, auspicando che la giurisprudenza comunitaria voglia andare oltre le apparenti vulnerabilità evidenziate dalla lettera delle disposizioni del Regolamento e accogliere, fra le soluzioni possibili, quelle che consentano di dare delle opportunità di sopravvivenza alle neonate cooperative di dati.

---

la cooperativa di dati, ove i fornitori di dati sono anche membri della struttura dell'intermediario. Diventa infatti complesso ipotizzare un rapporto diretto fra fornitori di dati (soci della cooperativa di dati) e utenti dei dati (ossia clienti della cooperativa di dati), attesa la necessità di mediazione della cooperativa di dati stessa nel rapporto commerciale;

3) come si struttura la remunerazione dei fornitori di dati/soci per avere condiviso il proprio *asset* di dati (distribuzione di utili? o mediante delle fee?);

4) in caso di utilizzo dello schema della società cooperativa come veste giuridica della cooperativa di dati, come si struttura il rapporto mutualistico fra la società/cooperativa di dati e i suoi soci, anche in considerazione dell'importanza che riveste la generazione del rapporto commerciale fra fornitori di dati e utenti (cfr. nota 41, ultimo periodo)?

[62] In questo senso S. GIRISH-M. AVERY, *Data cooperative: Enabling meaningful collective negotiation of data rights for communities*, 2022 (disponibile al sito: https://ssrn.com/abstract=4414473 o http://dx.doi.org/10.2139/ssrn.4414473), che rilevano: «*The EU Data Governance act defines data cooperatives and clarifies that they have 'fiduciary duties' however such a definition is limiting as it does not fit in cooperatives that seek to pool and process aggregated data and fails to recognise non-profit data cooperatives that exist, both in the EU (e.g., Salus) and beyond (e.g., MIDATA)*».

[63] Un soggetto dotato di armi spuntate: che nasce con l'obbiettivo di potenziare la posizione degli interessati ma che non è in grado di fornire alcuna proposta appetibile per attirare i potenziali membri non essendo neppure posto nella condizione di elaborare i dati per conto degli stessi.

Capitolo XVII

La valorizzazione dei dati in dimensione collettiva: tra cooperative di dati e reti di imprese

Carlo Basunti

Abstract: The paper analyses the provision of data cooperative services, recently regulated in the Data Governance Act (EU Reg. 868/2022). The DGA, especially with the introduction of the mentioned services, aims to address the distortion of competition within the digital market, reshaping the balance among the players. In this context, the essay investigates the role of consent in the circulation of data within data cooperatives and the possibility of using the subjective form of business networks to provide data cooperative services.

1. La *European Strategy for Data*: alcune premesse.

Nell'odierna società dell'informazione, è innegabile l'enorme potenziale racchiuso nei dati. La normativa europea relativa alla protezione dei dati personali è permeata da un'insopprimibile tensione tra la tutela della persona umana con i suoi diritti fondamentali [1] e la libera circolazione dei dati stessi. Si tratta di due contrap-

[1] Il diritto alla protezione dei dati di carattere personale, come è noto, ha conosciuto una consacrazione a livello europeo, in posizione autonoma rispetto al diritto alla vita privata e familiare, nella Carta dei diritti fondamentali dell'Unione europea all'art. 8 – oltre che nell'art. 16 TFUE – ed è, senza

poste esigenze, entrambe sottese alle scelte di politica legislativa europee, che devono necessariamente trovare una corretta composizione.

La progressiva instaurazione di un mercato interno che, oltre alla libera circolazione di merci, persone, servizi e capitali, promuove anche quella relativa ai dati, determina un complesso quadro giuridico dello svolgimento dei rapporti economici, ed impone una (ri)lettura del fenomeno che presti una puntuale attenzione anche agli aspetti di carattere prettamente patrimoniale. Può, dunque, dirsi superato l'approccio tradizionale alla materia, focalizzato esclusivamente sul contesto dei diritti assoluti, notoriamente caratterizzati da indisponibilità, imprescrittibilità e assolutezza. Precisamente, una simile impostazione garantista non deve essere del tutto abbandonata – il diritto alla *privacy*, nella sua odierna accezione di diritto all'autodeterminazione informativa [2], rimane pur sempre un diritto della personalità con tutte le conseguenze, *in primis* in termini di tutela, che ne derivano –, ma deve essere rivista alla luce dell'attuale scenario economico, dando quindi opportuno rilievo alle più moderne dinamiche di mercato ed accettando il ruolo centrale assunto dai dati personali nella prospettiva dei rapporti obbligatori [3]. L'interprete non può, dunque, oggi, limitarsi ad un'esegesi del fenomeno in chiave meramente personalista, ma deve essere pronto a cogliere le potenzialità (dello sfruttamento) dei dati, mantenendo saldi i profili di protezione della persona umana – che certo non possono essere obliterati – e saggiando altresì i possibili schemi negoziali nei quali tali dati possono fare il loro ingresso.

Pare essere proprio questa la linea tracciata dal Reg. (UE) 2016/679 (GDPR) che, sin dall'art. 1, nel porre l'obiettivo di proteggere i diritti e le libertà fondamentali delle persone fisiche, con particolare riguardo al diritto alla protezione dei dati personali,

---

dubbio, annoverabile tra quei diritti soggettivi che, secondo la fortunata espressione di Francesco Galgano, sono «trovati dal diritto oggettivo», ossia «diritti dell'uomo che si considerano esistenti indipendentemente da ogni norma giuridica che li riconosca e che il diritto oggettivo si limita a garantire» e che costituiscono un catalogo aperto: in questo senso, F. GALGANO, *Trattato di diritto civile*, vol. I, III ed., Padova, 2014, p. 171.

[2] Sul tema v. G. FINOCCHIARO, *Il quadro d'insieme sul regolamento europeo sulla protezione dei dati personali*, in ID. (opera diretta da), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, 2019, p. 1 ss.

[3] Il tema è ampiamente indagato dalla dottrina: tra i volumi che si occupano di tali questioni cfr. F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Milano, 2018; N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, 2019; V. RICCIUTO, *L'equivoco della* privacy. *Persona* vs *dato personale*, Napoli, 2022; ID.-C. SOLINAS (a cura di), *Forniture di servizi digitali e* «pagamento» *con la prestazione dei dati personali: un discusso profilo dell'economia digitale*, Milano, 2022; C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, Torino, 2021; A. DE FRANCESCHI, *La circolazione dei dati personali tra* privacy *e contratto*, Napoli, 2017; S. THOBANI, *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, Milano, 2018; C. SOLINAS, *Autonomia privata e regolazione pubblica nel trattamento dei dati personali*, Bari, 2022; G. VERSACI, *La contrattualizzazione dei dati personali dei consumatori*, Napoli, 2020; F.G. VITERBO, *Protezione dei dati personali e autonomia negoziale*, Napoli, 2008.

aggiunge che «la libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali». Tale disposizione deve essere letta in combinato disposto con il *Considerando* n. 4 del GDPR che, chiaramente, afferma la natura non tiranna del diritto alla protezione dei dati personali che, infatti, non è una «prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità» [4].

Le disposizioni richiamate sono espressione dell'idea di fondo dell'intero *corpus* normativo che si pone oggi nella dialettica tra persona e mercato. La poliedricità della libertà di circolazione dei dati deve essere inquadrata sia con riguardo agli interessi dei privati di sfruttamento dei dati per fini prettamente economici – anche nel caso in cui la pubblica amministrazione agisca *iure privatorum* – sia con riguardo a quelli di soggetti pubblici (anche) nel perseguire il fine del benessere sociale e, più in generale, ogniqualvolta l'utilizzo dei dati sia diretto allo svolgimento di compiti e funzioni di interesse pubblico. In quest'ottica, tra i diritti e gli interessi, che di volta in volta vengono in gioco, nessuno può risultare *ex se* superiore, ma si deve sempre operare un rigoroso bilanciamento al fine di comprendere, nel caso concreto, quale tra essi debba prevalere. Con riferimento al diritto o interesse che, nella specie, risulterà recessivo, non si potranno, comunque, ammettere limitazioni che incidano sul suo nucleo essenziale: ogni compressione dovrà essere adeguatamente ponderata e dovrà rappresentare il frutto del vaglio di proporzionalità.

Nella direzione di una adeguata valorizzazione e promozione dello sfruttamento dei dati, si inserisce la Strategia europea per i dati [5] che intende porre le basi per assicurare all'Unione europea un ruolo guida nell'economia sempre più *data driven*, rendendola così un vero punto di riferimento [6] per lo sfruttamento dei vantaggi derivanti da un sapiente utilizzo dei dati non solo a livello imprenditoriale, ma anche nel settore pubblico. In questo senso, emergono diversi aspetti di particolare rilevanza come, ad esempio, nuovi assetti delle relazioni pubblico-privato; nuovi equilibri tra il potere pubblico e i diritti dei singoli; nuovi compiti per le pubbliche amministrazioni e nuovi diritti per i privati; nonché la definizione del nuovo ruolo ricoperto dalle PA nell'attuale contesto sociale ed economico basato sulla circolazione dei dati [7].

---

[4] Chiarisce la portata ed il tenore letterale del *Considerando* n. 4 GDPR e della funzione sociale affermata dalla disposizione A. RICCI, *Sulla «funzione sociale» del diritto alla protezione dei dati personali*, in *Contr. e impr.*, 2017, 2, spec. p. 598 ss.

[5] COMMISSIONE EUROPEA, Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Una Strategia europea per i dati*, Bruxelles, 19 febbraio 2020 [COM (2020) 66 *final*].

[6] Il fatto che l'Unione europea si ponga, già grazie al GDPR, progressivamente, come punto di riferimento per le normative inerenti alla tutela del diritto alla protezione dei dati personali, può rinvenirsi, ad esempio, nella normativa californiana sul tema, ossia il *California Consumer Privacy Act* (CCPA) del 2018, come modificato dal *California Privacy Rights Act* (CPRA) del 2020.

[7] V. F. BRAVO-J. VALERO TORRIJOS, *Data in the Public Sector and Data Valorisation*, in F. BRAVO-J.

Attraverso importanti investimenti nelle tecnologie e nelle infrastrutture di prossima generazione da un lato, così come nell'alfabetizzazione ai dati, dall'altro, l'UE tratteggia un quadro in cui la (tutela della) persona in quanto tale non perde la centralità che, a ragione, deve caratterizzarla, ma in cui è manifesta la convinzione che, attraverso l'uso dei dati, tanto il settore privato quanto quello pubblico, ognuno secondo le proprie specificità, possano disporre di strumenti per adottare decisioni migliori e conoscere così nuove linee di sviluppo.

I dati, del resto, rappresentano *assets* di valore strategico, ben potendo essere copiati pressocché a costo zero e per il fatto che il loro utilizzo da parte di un soggetto non ne impedisce il contemporaneo uso da parte di un altro. Gli stessi dati possono, infatti, essere trattati simultaneamente da più persone o organizzazioni, anche per finalità differenti, purché determinate, esplicite e legittime. Tale natura non rivale dei dati, unitamente al fatto che essi costituiscono attributi della personalità, ne impone, tra l'altro, una esclusione dalle logiche di apprensione di tipo proprietario e dalla possibilità di effettuare scambi, aventi ad oggetto dati, tramite il modello del contratto ad effetti reali [8]. Se, infatti, con riguardo agli scambi che hanno ad oggetto dati non personali, si può ricorrere ai concetti ormai collaudati nell'ambito della disciplina della proprietà intellettuale, quando ci si riferisce a dati personali non ci si può distaccare dall'apparato di tutele fornito, per i diritti fondamentali, a livello europeo [9].

VALERO TORRIJOS (eds.), *Data Governance, Open Data and Data Protection in the Public Sector (Monographic Section)*, in *Eur. Rev. of Digital Administration & Law (ERDAL)*, 2022, 2, p. 5 in cui gli Autori evidenziano come questi rappresentino «*issues that highlight the new dimension of data valorisation*» e che assumono rilevanza «*both on their own and as part of a global vision*».

[8] Sul tema cfr. le riflessioni di G. ALPA, *La "proprietà" dei dati personali*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, cit., p. 11 ss.; e l'impostazione critica di F. BRAVO, *La «compravendita» di dati personali?*, in *Dir. internet*., 2020, 3, p. 531 ss.; anche in F. BRAVO-J. VALERO TORRIJOS, *Data in the Public Sector and Data Valorisation*, cit., p. 7; ed in F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al* Data Governance Act, in *Contr. e impr. Europa*, 2021, 1, p. 203 in cui, nel commentare l'introduzione della figura soggettiva del titolare dei dati (*data holder*) da parte del *Data Governance Act*, si esprimono preoccupazioni per tale «cambio di paradigma che rischia di essere un preludio all'introduzione, per via normativa, di una reificazione dei dati personali, quali entità giuridicamente rilevanti *ex se* più che quali attribuiti della persona»; v. pure V. ZENO ZENCOVICH, *Do "Data Markets" Exist?*, in *Media Laws*, 2019, 2, spec. p. 25 ss. in cui vengono espresse attente puntualizzazioni sul concetto di "*ownership*" riferito ai dati personali: in questo senso, da un punto di vista semantico, l'A. afferma: «*"Ownership" is not a notion which is engraved in some sacred tables. It is the result of centuries, millennia of theoretical, religious, political, social, economic evolution*» e aggiunge: «*ownership is a concept quite different from proprieté or from Eigentum*»; J.S. BERGÉ-S. GRUMBACH-V. ZENO ZENCOVICH, *The 'Datasphere', Data Flows beyond Control, and the Challenges for Law and Governance*, in *European J. of Comp. Law and Governance*, 2018, 2, p. 144 ss.; P.B. HUGENHOLTTZ, *Against "data property"*, in G. GHIDINI-H. ULLRICH-P. DRAHOS (eds.), *Kritika: Essays on Intellectual Property*, Cheltenham-Northampton, 2018, p. 48 ss.; e B.J. EVANS, *Much Ado About Data Ownership*, in *Harvard J. of Law & Tech*., 2011, 25, p. 78 secondo cui «*different assets call for different forms of ownership*».

[9] V. F. BRAVO, *Data Governance Act and Re-Use of Data in the Public Sector*, in F. BRAVO -J.

Il disegno strategico del legislatore europeo, indirizzato alla creazione e, soprattutto, ad una efficace regolamentazione del mercato unico digitale a livello unionale si compone di diversi interventi normativi. Tra questi, al di là del GDPR, si annoverano il *Digital Services Act* (DSA) [10]; il *Digital Markets Act* (DMA) [11]; il *Data Act* [12]; l'*AI Act* [13]; ed il *Data Governance Act* (DGA) [14], applicabile dal 24 settembre 2023.

Il DGA, in particolare, fa riferimento tanto ai dati di carattere personale quanto a quelli non personali (accomunati nella definizione di cui all'art. 2) e mira alla elaborazione di un sistema di *governance* dei dati a livello europeo che, nel pieno rispetto dei diritti fondamentali della persona, crei un clima di fiducia per gli operatori del mercato dei dati – singoli individui, imprese e pubbliche amministrazioni –, arginando lo strapotere nelle mani delle c.d. *Big Tech* e favorendo così scambi affidabili ed equi di dati. In questo senso, tale Regolamento tende a riequilibrare l'assetto di poteri che si è delineato sino ad oggi sul mercato digitale, caratterizzato dall'accumulo di un'enorme quantità di dati da parte di un esiguo numero di grandi

---

VALERO TORRIJOS (eds.), *Data Governance, Open Data and Data Protection in the Public Sector (Monographic Section)*, cit., pp. 32-33 che, nell'approfondire il riutilizzo dei dati (anche) personali da parte delle pubbliche amministrazioni, afferma: «*when it comes to personal data one cannot identify an ownership of the public sector bodies or other entities holding personal data nor can contracts on the re-use of personal data have as their object the "sale" of data: when it comes to personal data that are not anonymised, one will have to take into account the specific aspects of the GDPR's regulations*», precisando poi che «*this must not lead to the conclusion that personal data cannot be the object of contracts regulating their use, but rather that the adopted contractual solutions must be compliant with the specific nature of the fundamental right attributed to the data subject. Personal data can be the temporarily used for legitimate and specific purposes and in compliance with the principles indicated by the GDPR (including those of lawfulness, transparency and fairness, data minimisation, purpose limitation, storage limitation), which (also) have a limitative scope of contractual autonomy, to safeguard the rights and fundamental freedoms of the data subject*».

[10] Reg. (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022, relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (Regolamento sui servizi digitali).

[11] Reg. (UE) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022, relativo a mercati equi e contendibili nel settore digitale e che modifica le Direttive (UE) 2019/1937 e (UE) 2020/1828 (Regolamento sui mercati digitali).

[12] Reg. (UE) 2023/2854 del Parlamento europeo e del Consiglio del 13 dicembre 2023, riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il Regolamento (UE) 2017/2394 e la Direttiva (UE) 2020/1828 (regolamento sui dati).

[13] Reg. (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale).

[14] Reg. (UE) 2022/868 del Parlamento europeo e del Consiglio del 30 maggio 2022, relativo alla *governance* europea dei dati e che modifica il Reg. (UE) 2018/1724 (Regolamento sulla *governance* dei dati).

imprese, secondo un modello di sostanziale oligopolio, al fine di incentivare l'emersione e di dare rilievo a *start-up* e PMI.

Questa prospettiva merita sicuro apprezzamento in quanto una tale concentrazione di potere nelle mani di pochi non solo mina il corretto funzionamento del mercato nel suo insieme, ma pone altresì in pericolo, tra gli altri, il diritto alla *privacy* e l'autonomia contrattuale dei singoli.

Nella creazione di una intelaiatura tra dimensione privata, pubblica e collettiva di sfruttamento dei dati, il DGA si snoda lungo tre direttrici: (i) il riutilizzo dei dati [15], ossia la possibilità per le persone fisiche e giuridiche di utilizzare dati che sono nella disponibilità di enti pubblici, perseguendo finalità commerciali o non commerciali, ma, comunque, differenti rispetto a quelle su cui si è fondato il primo trattamento. La possibilità di riutilizzo dei dati deve essere, ragionevolmente, ristretta nell'ambito di quelle operazioni che reimpieghino i dati a beneficio della collettività, trattandosi, pur sempre, di dati gestiti da enti pubblici con fondi pubblici; (ii) i servizi di intermediazione dei dati [16], per mezzo dei c.d. fornitori di servizi di intermediazione di dati, instaurando rapporti commerciali inerenti ai dati tra gli utenti e quei soggetti che raccolgono e utilizzano tali dati; (iii) l'altruismo dei dati, nel quale si percepisce una forte eco del principio normativo di solidarietà [17], relativo

---

[15] Sul tema, cfr. F. BRAVO-J. VALERO TORRIJOS (eds.), *Data Governance, Open Data and Data Protection in the Public Sector (Monographic Section)*, cit., p. 5 ss.

[16] I servizi di intermediazione dei dati, elencati all'art. 10 DGA, sono: «a) servizi di intermediazione tra i titolari dei dati e i potenziali utenti dei dati, compresa la messa a disposizione di mezzi tecnici o di altro tipo per consentire tali servizi (…); b) servizi di intermediazione tra interessati che intendono mettere a disposizione i propri dati personali o persone fisiche che intendono mettere a disposizione dati non personali e potenziali utenti dei dati, compresa la messa a disposizione di mezzi tecnici o di altro tipo per consentire tali servizi, permettendo in particolare l'esercizio dei diritti degli interessati di cui al regolamento (UE) 2016/679; c) servizi di cooperative di dati»; il considerando n. 27 DGA afferma che: «si prevede che i servizi di intermediazione dei dati svolgano un ruolo essenziale nell'economia dei dati, in particolare nel sostenere e promuovere pratiche volontarie di condivisione dei dati tra imprese o nell'agevolare la condivisione dei dati nell'ambito degli obblighi stabiliti dal diritto dell'Unione o nazionale. Essi potrebbero diventare strumenti che agevolano lo scambio di quantità considerevoli di dati pertinenti. I fornitori di servizi di intermediazione dei dati, che possono includere anche enti pubblici, che offrono servizi che collegano i diversi soggetti dispongono del potenziale per contribuire alla messa in comune efficiente dei dati come pure all'agevolazione della condivisione bilaterale dei dati». In argomento, cfr. F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al* Data Governance Act, cit., p. 199 ss.; ID., *Data Governance Act and Re-Use of Data in the Public Sector*, cit., p. 15 ss. parla di «*key role of data intermediaries*»; D. POLETTI, *Gli intermediari dei dati*, in *European J. of Privacy Law & Tech*., 2022, 1, p. 46 ss.; anche in ID., *Gli intermediari dei dati*, in A. MORACE PINELLI (a cura di), *La circolazione dei dati personali. Persona, contratto e mercato*, Pisa, 2023, p. 105 ss.

[17] Sul principio di solidarietà, inquadrato quale principio normativo, cfr. G. ALPA, *Solidarietà. Un principio normativo*, Bologna, 2022; ID., *I principi generali*, Milano, 2023, p. 256 ss.; v. anche la ricostruzione del principio offerta da S. RODOTÀ, *Solidarietà. Un'utopia necessaria*, Roma-Bari, 2014; P. RESCIGNO, *Solidarietà e diritto*, Napoli, 2006; N. LIPARI, *"Spirito di liberalità" e "spirito di solidarietà"*, in *Riv. trim. dir. e proc. civ*., 1997, 1, p. 1 ss.; F.D. BUSNELLI, *Il principio di solidarietà e*

alla condivisione volontaria di dati per finalità altruistiche di interesse generale che vadano oltre la mera compensazione dei costi sostenuti per mettere a disposizione tali dati, come, ad esempio, l'assistenza sanitaria, la lotta ai cambiamenti climatici, il miglioramento della mobilità, l'agevolazione dell'elaborazione, produzione e divulgazione di statistiche ufficiali, il miglioramento della fornitura di servizi pubblici, l'elaborazione di politiche pubbliche e la ricerca scientifica.

Tra i servizi di intermediazione dei dati – i cui fornitori possono essere anche enti pubblici e che sono destinati ad avere un ruolo strategico nell'economia dei dati, (anche) quali strumenti atti ad agevolare lo scambio di considerevoli quantità di dati –, il *Data Governance Act* prevede, *ex* art. 10, lett. c), i «servizi di cooperative di dati» [18], su cui, in questa sede, si intende focalizzare l'attenzione. Tali servizi, e, si noti, non le cooperative di dati in sé, vengono definiti, giusta l'art. 2, par. 1, n. 15, DGA come «servizi di intermediazione dei dati offerti da una struttura organizzativa costituita da interessati, imprese individuali o da PMI, che sono membri di tale struttura, avente come obiettivi principali quelli di aiutare i propri membri nell'esercizio dei loro diritti in relazione a determinati dati, anche per quanto riguarda il compiere scelte informate prima di acconsentire al trattamento dei dati, di procedere a uno scambio di opinioni sulle finalità e sulle condizioni del trattamento dei dati che rappresenterebbero al meglio gli interessi dei propri membri in relazione ai loro dati, o di negoziare i termini e le condizioni per il trattamento dei dati per conto dei membri prima di concedere l'autorizzazione al trattamento dei dati non personali o prima che essi diano il loro consenso al trattamento dei dati personali».

Un simile modello organizzativo si contrappone, dunque, a quello tradizionalmente capitalistico e, fondandosi su logiche di stampo mutualistico rappresenta la massima esplicazione della strada che, con il *Data Governance Act*, l'Unione europea procede a delineare. Si tratta, a ben vedere, di una costante di lungo corso nella storia dell'umanità: la ricerca mutualistica, da parte di individui, gruppi e popolazioni intere, di soluzioni comuni a problemi comuni di varia entità [19]. Questo mec-

---

"l'attesa della povera gente", oggi, in *Riv. trim. dir. e proc. civ*., 2013, 2, p. 413 ss.; M. TAMPIERI, *La riscoperta del principio di solidarietà*, in *Jus Civile*, 2020, 3, p. 612 ss.; B. BERTARINI, *Il principio di solidarietà tra diritto ed economia. Un nuovo ruolo dell'impresa per uno sviluppo economico inclusivo e sostenibile*, Torino, 2020; A. APOSTOLI, *La svalutazione del principio di solidarietà: crisi di un valore fondamentale per la democrazia*, Milano, 2012; F. POLACCHINI, *Doveri costituzionali e principio di solidarietà*, Bologna, 2017; sul principio di solidarietà applicato al tema della protezione dei dati personali, cfr. F. BRAVO, *Il principio di solidarietà in materia di protezione dei dati personali nelle decisioni del Garante e della Corte di cassazione*, in *Contr. e impr.*, 2023, 2, p. 405 ss.; ID., *Il principio di solidarietà*, in ID. (a cura di), *Dati personali. Protezione, libera circolazione e* governance – Vol. 1., *Principi*, Pisa, 2023, p. 541 ss.; ID., *Il principio di solidarietà tra* data protection *e* data governance, in *Dir. inf*., 2023, 3, p. 481 ss.

[18] Cfr. l'analisi critica della disciplina giuridica sul tema delle cooperative di dati alla luce del DGA di F. BRAVO, *Le cooperative di dati*, in *Contr. e impr.*, 2023, 3, p. 757 ss.

[19] M.C. PASTOR SEMPERE, *La nueva economía social del dato (ESD)*, in *Rev. Jur. de Econ. Soc. y Coop*., 2022, 41, p. 35 osserva che «*desde siempre han existido fórmulas de autoayuda y solidaridad*

canismo, dunque non sconosciuto, viene oggi calato nello scenario digitale, al fine di mantenere entro i binari della giustizia [20] – o, almeno, di un'idea di giustizia – il progresso economico.

È, dunque, questo il contesto in cui mira ad inserirsi la presente indagine, volta ad un inquadramento e ad un'analisi del ruolo delle cooperative di dati e delle opportunità che l'impiego di tale modello dischiude nel solco della Strategia europea per i dati e delle *rationes* ad essa sottese. In quest'ottica, lo scopo di questo lavoro è quello di affrontare alcune delle principali criticità che emergono dalle norme dettate sul tema dal legislatore europeo.

Segnatamente, si intende indirizzare l'analisi in una duplice prospettiva. Dapprima, l'obbiettivo è quello di indagare il concreto atteggiarsi del consenso al trattamento dei dati nell'ambito delle operazioni poste in essere da una cooperativa di dati, con particolare riguardo alla problematica ipotesi in cui il membro della cooperativa, che autorizza quest'ultima a trattare i dati sia un *data holder* (nuova categoria giuridica soggettiva prevista ai sensi dell'art. 2, par. 1, n. 8, DGA) e non un *data subject* (la cui definizione è notoriamente ricavabile da quella di «dato personale», ai sensi dell'art. 2, par. 1, n. 1, GDPR). In seguito, alla luce dell'indeterminatezza del concetto di cooperativa di dati con riferimento alle forme soggettive adottabili nella fornitura di tali servizi di intermediazione, ci si propone di ricercare strutture organizzative che, al di là di quella della società cooperativa, possano essere utilizzate, in *compliance* con il DGA, per fornire i servizi di cooperative di dati. Nello specifico, si valuterà se le reti di imprese possono rappresentare una soluzione in tal senso idonea nonché una scelta efficace nel raggiungimento degli obbiettivi di promozione del mercato digitale posti dal legislatore europeo attraverso la Strategia europea per i dati.

Lo sviluppo del mercato interno (anche) tramite la circolazione e lo sfruttamento dei dati può, senz'altro, dirsi ineludibile e merita di essere incentivato. Tale sviluppo deve, tuttavia, essere improntato ad una idea di economia digitale sostenibile [21] e, a tal fine, la persona umana deve godere di una tutela adeguata. Non potreb-

---

mediante las cuales individuos, grupos y poblaciones enteras, han buscado y logrado soluciones comunes a problemas comunes de variadas magnitudes y alcances. Con la Revolución Industrial, surgieron como respuesta casi automática: el común, o la gente en términos coloquiales, constituyó organizaciones socioeconómicas y de autodefensa con bases asociativas como las asociaciones, cooperativas, y mutuales, iniciándose así la construcción de un sector con rasgos específicos, que los economistas de finales del primer tercio del S. XIX denominaron Economía Social» e, in questo quadro, le cooperative di dati rappresentano, dunque, «*la última expresión "digital" de una constante a lo largo de la historia de la humanidad*»; sempre in prospettiva storica, M.T. BODIE, *The Law of Employee Data: Privacy, Property, Governance*, in *Indiana Law J*., 2022, 2, spec. p. 712 sottolinea che «*collecting and using data about workers is endemic to employment relationships throughout history*»; parimenti, I. AJUNWA-K. CROWFORD-J. SCHULTZ, *Limitless Worker Surveillance*, in *California Law Rev*., 2017, 3, p. 735 ss.

[20] Sul tema, v. per tutti N. LIPARI, *Elogio della giustizia*, Bologna, 2021.

[21] In argomento, v. M.C. PASTOR SEMPERE, *Economia Digital Sostenible*, Cizur Menor (Navarra),

be, infatti, dirsi sostenibile uno sviluppo che, unicamente indirizzato al profitto delle imprese e per le imprese, prescinda dalla protezione dei diritti della persona e dalla tutela multilivello ad essa accordata dal legislatore europeo. In tal senso, il *framework* delineato dalla *European Strategy for Data* e, in particolare dal DGA, soprattutto attraverso le cooperative di dati, pare potersi apprezzare per l'attenzione dedicata, nell'ambito della *data economy*, alla valorizzazione delle potenzialità dei dati, tramite modelli di *business* che evitino abusi (o, quantomeno, siano ideati per evitarli), a garanzia dei «diritti inviolabili dell'uomo, sia come singolo, sia nelle formazioni sociali ove si svolge la sua personalità» (art. 2 Cost.).

2. L'utilizzo dei dati in chiave mutualistica attraverso le cooperative, nell'opera di "*digital market reshaping*".

Il *Data Governance Act*, come si è accennato, fa riferimento ai servizi di cooperative di dati e non procede a definire e a disciplinare puntualmente le cooperative di dati *ex se*. Pertanto, la mancanza di una circoscrizione della forma soggettiva utilizzabile, lascia libera la strada a diverse forme di svolgimento di tali servizi, nonostante appaia chiaro che la forma societaria e, segnatamente, quella della società cooperativa sia il modello *standard* cui riferire le cooperative di dati [22].

Le società cooperative [23], cui il codice civile dedica il titolo VI del Libro V, so-

2020; e J. GUTIÉRREZ VICÉN, *Una economía digital sostenible*, in *Trama y Text*., 2016, 31, p. 97 in cui sottolinea come ci troviamo immersi in «*un nuevo paradigma «tecno-económico», que es el responsable del paso definitivo del capitalismo industrial al capitalismo posindustrial o «capitalismo informacional*»».

[22] V. F. BRAVO, *Le cooperative di dati*, cit., p. 760 che, sul punto, fa riferimento alla possibilità di svolgere tali servizi «nella forma delle associazioni temporanee di imprese (ATI) o dei raggruppamenti temporanei di impresa (RTI) o, ancora, nella forma delle "reti di imprese", che svolgano "servizi di intermediazione di dati" mediante logiche di "cooperazione" a beneficio dei propri membri» e aggiunge: «del resto il legislatore europeo, volutamente sintetico su tale aspetto, ha scelto di porre l'accento sull'elemento oggettivo, la fornitura del "servizio", e non sulla natura soggettiva del fornitore: nel far ciò ha però definito i «servizi di cooperative di dati» senza mai menzionare la "società cooperativa"», sia altresì consentito il rinvio a C. BASUNTI, *Nuove prospettive di valorizzazione dei dati in dimensione collettiva: le cooperative di dati (e le reti di imprese)*, in *Contr. e impr*., 2024, 3, p. 926 ss. in cui tale aspetto viene in particolare trattato con riguardo alle reti di imprese.

[23] La letteratura in tema di società cooperative è vastissima. Ci si limita in questa sede a richiamare, F. GALGANO, *Trattato di diritto civile*, vol. IV, III ed., Padova 2015, p. 689 ss.; ID.-R. GENGHINI, *Il nuovo diritto societario. Le nuove società di capitali e cooperative*, in F. GALGANO (diretto da), *Tratt. dir. comm. e dir. pubbl. econ*., III ed., t. I, Padova, 2006, p. 923 ss.; G. BONFANTE, *Imprese cooperative*, in *Comm. c.c. Scialoja – Branca*, a cura di Galgano, *Libro V*, *Del lavoro, artt. 2511-2545*, Bologna-Roma, 1999; ID., voce *Società cooperative*, in *Enc. dir., Annali*, t. 2, Milano, 2008, p. 1087 ss.; ID., *La società cooperativa*, in *Tratt. dir. comm*., diretto da Cottino, Padova, 2014; ID., *La nuova società cooperativa*, Bologna, 2010; L.F. PAOLUCCI, *Imprese cooperative e mutue assicuratrici*, in P. RESCIGNO (diretto da), *Tratt. dir. priv*., vol. 17, *Impresa e lavoro*, t. III, II ed., Torino, 2010; G. RA-

no notoriamente caratterizzate da un fine non lucrativo, ma mutualistico, o, comunque, almeno prevalentemente mutualistico e, quindi, prevalentemente non lucrativo. Lo scopo mutualistico – che, pur richiamato dalle norme codicistiche di cui agli artt. 2511 ss., anche dopo la riforma operata dal d.lgs. 17 gennaio 2003, n. 6, non ha conosciuto una esplicita definizione legislativa, rimanendo un dato inespresso del sistema, deputato all'interpretazione – caratterizza causalmente le società cooperative e le differenzia sul piano funzionale da quelle lucrative. Le cooperative, siano esse a mutualità prevalente o no e, quindi, fiscalmente agevolate o meno, rientrano tutte in un disegno unitario e si basano necessariamente sulla mutualità e, dunque, sulla possibilità di far conseguire ai soci beni, servizi o occasioni di lavoro a condizioni migliori di quelle di mercato, e non sul conseguimento e riparto di utili patrimoniali in proporzione al capitale conferito. Del resto, l'indicazione sociale di "cooperativa" può essere utilizzata, *ex* art. 2515, co. 2, c.c., solo da società che hanno scopo mutualistico e, inoltre, i criteri seguiti per tale scopo devono essere indicati specificamente, *ex* art. 2545 c.c., dagli amministratori e dai sindaci della società in occasione dell'approvazione del bilancio di esercizio.

Un simile modello, trasposto nel mercato digitale, permette agli interessati di esercitare più efficacemente i loro diritti sui dati, organizzandosi in una dimensione collettiva, fondata sull'aiuto reciproco in ottica mutualistica, potendo così contare su una organizzazione strutturata e non mostrandosi più solo come persone singole al cospetto dei *Big Players*, in una assoluta asimmetria contrattuale.

Il vero vantaggio ottenuto dai soci non si sostanzia tanto, almeno in un primo momento, in termini strettamente monetari, quanto nella consapevolezza delle dinamiche del trattamento e, in generale, del mercato dei dati nonché dell'uso secondario dei dati [24] e, quindi, con riferimento al *modus operandi*, al fine di non subire lesioni, nell'esercizio del diritto all'autodeterminazione informativa. Del resto, il settore è tutt'ora caratterizzato da un forte grado di opacità che determina, il più delle volte, una inconsapevolezza generalizzata nell'acconsentire all'utilizzo di un "prodotto" dotato di valore economico, *rectius*, capace, attraverso le operazioni di trattamento, di fornire un vantaggio economico. Gli obblighi di informazione devono, dunque, rappresentare, un elemento imprescindibile del trattamento affinché il *data subject* non renda il suo consenso una mera "presa d'atto" della sussistenza

---

CUGNO, *La società cooperativa*, in V. BUONOCORE (diretto da), *Tratt. dir. comm*., Sez. IV, Tomo 9, Torino, 2006; M.C. TATARANO, *La nuova impresa cooperativa*, in A CICU-F. MESSINEO-L. MENGONI (già diretto da), P. SCHLESINGER (continuato da), *Tratt. dir. civ. e comm*., Milano, 2011; G. TATARANO, *L'impresa cooperativa*, in A CICU-F. MESSINEO-L. MENGONI (già diretto da), P. SCHLESINGER (continuato da), *Tratt. dir. civ. e comm*., Milano, 2002; A. BASSI, *Delle imprese cooperative e delle mutue assicuratrici*, in P. SCHLESINGER (diretto da), *Il c.c. Comm., Artt. 2511-2548*, Milano, 1988; D.U. SANTOSUOSSO (a cura di), *Delle società. Dell'azienda. Della concorrenza*, in E. GABRIELLI (diretto da), *Comm. del c.c., Artt. 2511-2574*, Torino, 2014; M.J. MORILLAS JARILLO-M.I. FELIU REY, *Curso de cooperativas*, Madrid, 2018.

[24] V. G. RESTA, *Pubblico privato, collettivo nel sistema europeo di governo dei dati*, in ID.-V. ZENO-ZENCOVICH (a cura di), *Governance of/through Big Data*, vol. II, Roma, 2023, p. 619.

del trattamento, privando così tale consenso della fondamentale caratteristica della (reale) libertà.

Nell'atto costitutivo della società dovranno essere determinati i criteri che verranno utilizzati per ricompensare i soci in misura proporzionale alla quantità e qualità dello scambio mutualistico prestato, proprio come l'art. 2545 *sexies* c.c. stabilisce per i ristorni delle cooperative genericamente intese. I servizi di intermediazione dei dati offerti dalla cooperativa e basati sui dati (personali e non personali) vengono così offerti a beneficio dei soci della cooperativa e, eventualmente, anche inseriti in logiche negoziali con soggetti terzi. In tal modo, si ha una massima valorizzazione dello scambio mutualistico, sulla base dell'apporto dato ai singoli soci a vantaggio della cooperativa e, quindi, di tutti i soci della stessa.

La combinazione tra criterio quantitativo e criterio qualitativo appare particolarmente pregnante nell'ambito specifico delle cooperative di dati. In questo campo, infatti, si potrà senz'altro dare maggior rilievo al socio che ha cooperato non solo "di più", ma anche "meglio". Precisamente, non si può avere unicamente riguardo alla quantità di dati forniti, perché la *data quality* è di assoluta importanza.

Sebbene oggigiorno sia particolarmente agevole raccogliere ingenti quantità di dati, il profilo qualitativo degli stessi presenta importanti ricadute sul trattamento da effettuarsi. Affinché i dati forniti dai soci siano realmente utili agli altri soci – come pure alla cooperativa nei rapporti con i terzi –, essi devono rispettare, in particolare, il principio di esattezza [25]. Solo in tal guisa, infatti, i dati possono divenire un *asset* strategico per operare sul mercato. In una cooperativa di dati, i vari soci sono particolarmente incentivati a condividere *high quality data* dal momento che, dalla condivisione di tale tipologia di dati, ne deriva, *in primis*, una elevata qualità del complesso di dati raccolti e trattati, aumentandone così il valore (economico in un'ottica di mercato e funzionale per le attività dei soci), e, successivamente, un accrescimento del ri(s)torno per i singoli membri della cooperativa.

Si pensi, ad esempio, ad una cooperativa di dati che svolge un servizio di *ride-hailing*: è evidente come: a) per i singoli soci possa essere vantaggioso solo l'utilizzo di dati esatti relativi al traffico, alla quantità di clienti in attesa in un determinato posto, al numero di *drivers* già al lavoro in una certa zona, e così via; b1) per la cooperativa in sé sarà particolarmente facile, disponendo di dati esatti, destare l'interesse di soggetti privati che operano sul mercato digitale e poter instaurare con loro rapporti contrattuali riferiti ai dati, dal momento che tali soggetti potrebbero operare (anche) attraverso studi statistici inerenti alle abitudini e agli spostamenti di grandi quantità di persone cui poter, in seguito, offrire determinati servizi in modo mirato; b2) la cooperativa potrebbe altresì interfacciarsi con soggetti pubblici che intendano conoscere con precisione le infrastrutture maggiormente utilizzate ed i luoghi più frequentati per fasce orarie, come pure le emissioni di Co2 nell'arco

[25] Su tale principio sia consentito il rinvio a F. AVVEDUTO-C. BASUNTI, *Il principio di esattezza*, in F. BRAVO (a cura di), *Dati personali. Protezione, libera circolazione e* governance – Vol. 1., *Principi*, cit., p. 263 ss.

delle varie giornate, così da poter attuare nuove opere per il tessuto urbano e porre in essere oculate politiche di sicurezza pubblica e di tutela ambientale.

Tutte queste potenzialità di utilizzo dei dati e di connessa crescita della cooperativa – e dei suoi soci – verrebbero frustrate laddove i dati raccolti non fossero rispettosi del principio di esattezza.

Va da sé che le società cooperative mirano comunque ad assumere un ruolo sul mercato digitale, nell'intento di divenire competitive nei confronti delle società di stampo capitalistico. Sia le cooperative sia le società lucrative sono caratterizzate dall'esercizio in comune di una attività economica sulla base di un programma imprenditoriale indirizzato (quantomeno) a coprire i costi con i ricavi. Le prime, tuttavia, (anche) attraverso la condivisione mutualistica dei dati, conoscono una responsabilizzazione particolarmente pregnante ed hanno alla base una amministrazione etica – *stewardship*[26] – dei dati che rappresentano la loro risorsa principale, garantendo, nella loro attività, la massima tutela dei soci e dei loro diritti nonché un utilizzo responsabile dei dati. Le cooperative di dati rappresentano, in questo senso, l'espressione dell'opera, che si potrebbe definire di "*digital market reshaping*", che il DGA mira ad attuare. Una simile politica, non è certo diretta a negare le potenzialità (anche economiche) che i dati racchiudono che, anzi, si intendono valorizzare, ma è volta ad uno sfruttamento consapevole, etico e responsabile di tale, non più tanto nuova, risorsa, a beneficio non solo di una cerchia ristretta di soggetti, ma di una più ampia pletora di individui, e finanche della società tutta.

In questa direzione, il DGA ridisegna gli equilibri tra gli agenti del mercato digitale, ridistribuendo il potere dalle grandi compagnie – che hanno innegabilmente contribuito a causare il c.d. *data divide* e l'esclusione digitale di vari soggetti – ad individui singolarmente intesi, *start-up* e *communities*. A tal fine, le cooperative di dati puntano sulla garanzia di processi decisionali democratici e di un'equa distribuzione dei benefici risultanti dallo sfruttamento dei dati, creando in tal guisa quel clima di fiducia che è essenziale affinché i soggetti possano essere incentivati all'utilizzo mutualistico dei dati nell'ambito dei servizi di cooperative di dati. Il

---

[26] Cfr. E. BIETTI-A. ETXEBERRIA-M. MANNAN-J. WONG, *Data Cooperatives in Europe: A Legal and Empirical Investigation*, *White Paper created as part* of *The New School's Platform Cooperativism Consortium and Harvard University's Berkman Klein Center for Internet & Society Research Sprint*, December 2021, in *https://cyber.harvard.edu/sites/default/files/2022-02/Data_Cooperatives_Europe-group2.pdf*, p. 8; W. HALL-AL., *Exploring legal mechanism for data stewardship*, *Working group final report*, in *https://www.adalovelaceinstitute.org/wp-content/uploads/2021/03/Legal-mechanisms-for-data-stewardship_report_Ada_AI-Council-2.pdf*, p. 52 dove si inquadrano le «*data cooperatives as cooperative organisations (whatever their legal form) that have as their main purpose the stewardship of data for the benefit of their members, who are seen as individuals (or data subjects). This is in contrast to stewardship of data primarily or exclusively for the benefit of the community at large*», e si precisa: «*that is not to say that a cooperative whose aim is to benefit its members might not also benefit wider society (…). Indeed, where members see the wider benefits as their own priorities (as with philanthropic giving), the distinction between members' benefits and social benefits may be hard to discern*».

meccanismo di *governance* sotteso alle cooperative di dati, fondato sullo stesso potere decisionale in capo ai soci, tutti posti sullo stesso piano, e sulla valorizzazione condivisa dei dati, in ottica collettiva, a beneficio di tutti, può certamente determinare quel clima di fiducia di cui si è detto.

Le sfide che la transizione digitale impone possono essere efficacemente affrontate – e le opportunità da essa offerta possono, d'altro canto, essere colte – attraverso il «neomutualismo» [27], nella sua moderna declinazione di «neomutualismo digitale».

Il menzionato intento del legislatore europeo di contrastare il sostanziale oligopolio affermatosi nel settore della circolazione dei dati, si esplica, tra l'altro, nella valorizzazione di nuove forme di *business* basate sul modello mutualistico, capaci sia di offrire adeguata tutela all'interessato (o al titolare dei dati) sia di acquisire un ruolo di rilievo nell'economia *data based*. In tale quadro, l'agire attraverso la mutualità, che costituisce l'essenza stessa della cooperazione, riempiendo di significato il rapporto sociale, diviene espressione di vita democratica nella *societas* ai tempi dell'informazione [28].

L'impostazione spiccatamente democratica della cooperativa rinviene un importante pilastro nel sistema di voto capitario che, nonostante abbia conosciuto nel tempo un affievolimento a livello di imperatività a fronte dell'ampliarsi dei confini dell'autonomia statutaria [29], rimane il regime legale di riferimento che differenzia tale tipologia di società dal modello "plutocratico" delle società lucrative. Giusta l'art. 2538, co. 2 c.c., ogni socio cooperatore ha diritto ad un voto a prescindere dal valore della sua quota o dal numero di azioni possedute, ad eccezione, prosegue il co. 3 della norma, delle persone giuridiche alle quali l'atto costitutivo può attribuire un numero maggiore di voti (comunque non superiore a cinque). I soci della cooperativa (di dati) si trovano, dunque, tutti sullo stesso piano nell'amministrazione della società e nell'assunzione di decisioni relative all'utilizzo dei dati collazionati dalla cooperativa, evitando sperequazioni e posizioni di primazia.

---

[27] Il riferimento è a P. VENTURI-F. ZANDONAI, *Neomutualismo. Ridisegnare dal basso competitività e* welfare, Milano, 2022; sulle connessioni tra neomutualismo (digitale) e cooperative (di dati), v. F. BRAVO, *Le cooperative di dati*, cit., p. 764 ss. e *passim*, a p. 766, l'Autore afferma: «mi pare che la cornice teorica del mutualismo digitale possa ben interpretare, sul piano economico, l'introduzione del modello giuridico delle cooperative di dati quale fattore di sviluppo per la *data governance*». Sull'aspetto etico alle base delle società cooperative, cfr. M. FRANZONI, *Etica del legislatore nel governo dell'impresa cooperativa*, in *Riv. trim. dir. e proc. civ*., 1993, 2, spec. p. 501 ss.

[28] In argomento, v. F. BRAVO, Ubi societas ibi ius *e fonti del diritto nell'età della globalizzazione*, in *Contr. e impr.*, 2016, 6, p. 1344 ss. che cala il brocardo «*ubi societas ibis ius*» nel contesto delle piattaforme digitali; ID., *Le sfide della globalizzazione per il diritto nell'età postmoderna. Aspetti teorici e approccio metodologico alla luce della teoria ordinamentale di Santi Romano*, in M.A. STEFANELLI (a cura di), *Dopo la globalizzazione: sfide alla società e al diritto*, Torino, 2017, p. 199 ss.; T.E. FROSINI, *Il costituzionalismo nella società tecnologica*, in *Dir. inf*., 2020, 3, p. 465 ss.; ID., *L'ordine giuridico del digitale*, in *Giur. cost*., 2023, 1, p. 377 ss.

[29] Per un'indagine relativa a tali aspetti, cfr. G. MARASÀ, *Voto plurimo, voto maggioritario e cooperative*, in *Banca, borsa, tit. cred*., 2016, 1, p. 1 ss.

Questo aspetto, cui fa eco anche il principio di parità di trattamento dei soci di cui all'art. 2516 c.c., appare di particolare rilievo nel settore specifico della *data protection* in cui a circolare sono i dati (anche personali, e quindi attributi della personalità). L'accento viene, in tal guisa, posto sulla funzione sociale del diritto alla protezione dei dati personali e, con riguardo ai dati genericamente intesi, si enfatizza la prospettiva solidaristica in cui le operazioni di trattamento devono rientrare.

Si aggiunga poi il principio della c.d. "porta aperta" che, previsto *ex* art. 2528 c.c., norma da leggersi in combinato disposto con gli artt. 2521, co. 3, n. 6, 2424 e 2527 c.c., cala nel contesto cooperativo la regola di cui all'art. 1332 c.c. [30]. Tale principio, che esalta la specificità delle cooperative nel perseguire lo scopo mutualistico, in un'ottica democratica e solidaristica, rende la cooperativa una struttura aperta in cui possono entrare tutti i soggetti portatori dei medesimi interessi, previsti nell'atto costitutivo della società. Ciò non deve apparire però il fondamento di una posizione dell'aspirante socio qualificabile come diritto soggettivo: gli amministratori non sono obbligati all'accoglimento della domanda di ammissione di un terzo, anche se in possesso di tutti i requisiti previsti dalla legge e dallo statuto. Gli amministratori sono, invero, tenuti ad effettuare un concreto vaglio di ammissibilità e opportunità, e, quindi, a non respingere in modo arbitrario le richieste di adesione, in quanto un simile potere sopprimerebbe di fatto la possibilità di ammissione, precludendo, seppur in via traversa, l'ingresso di nuovi soci. Si deve, in quest'ottica, valorizzare adeguatamente la prospettiva contrattuale dell'ammissione del nuovo socio: trattasi infatti di un atto di autonomia contrattuale che attiene alla formazione (progressiva) del contratto di società e richiede, pertanto, l'accordo tra le preesistenti parti del rapporto ed il nuovo contraente. Il principio della c.d. "porta aperta" non tutela tanto l'interesse dei terzi all'ingresso nella cooperativa, quanto l'interesse dei soci al rafforzamento numerico del gruppo cooperativo [31].

A maggior ragione in una cooperativa di dati, è sicuramente interesse dei soci che il vincolo tra loro sussistente sia aperto all'adesione di nuove parti, proprio per il fatto che nuovi soci apporterebbero nuovi dati, e tanto più cospicua è la quantità (unitamente alla qualità) di dati che la cooperativa può utilizzare, quanto più solida è la posizione della stessa sul mercato e di maggiore utilità la partecipazione ad essa da parte dei singoli. Se generalmente, infatti, il principio della "porta aperta" è

---

[30] Afferma F. GALGANO, *L'impresa cooperativa fra autogestione e autocrazia*, in *Dem. e dir.*, 1982, 3, p. 83 che il principio della porta aperta rappresenta il «ripudio della regola capitalistica per la quale il potere di decidere dipende dalla ricchezza posseduta ed è proporzionale ad essa», inoltre, a p. 90, l'Autore sottolinea che tale principio deve essere sempre verificato nella sua effettività, in rapporto alla concreta struttura organizzativa della cooperativa; v. anche ID., *Persone giuridiche*, in ID. (a cura di), *Comm. c.c. Scialoja-Branca*, *Libro I, Persone e famiglia*, artt. 11-35, II ed., Bologna-Roma, 2006; in argomento v. anche M. MAGGIOLO, *Clausole di apertura e «porta aperta» nei procedimenti di adesione a contratti plurilateriali*, in *Riv. dir. civ*., 2010, 6, p. 783 ss.

[31] V. sul punto F. GALGANO-R. GENGHINI, *Il nuovo diritto societario. Le nuove società di capitali e cooperative*, cit., p. 957 ss.

funzionale ad una migliore gestione delle risorse della cooperativa per gli scopi mutualistici perseguiti, nell'ambito digitale risulta essenziale per la cooperativa disporre di una grande quantità di dati – i dati presi singolarmente o raccolti in quantità limitate non hanno di per sé particolare utilità – sia per erogare servizi realmente utili ai propri soci sia per interfacciarsi con soggetti terzi in logiche negoziali.

Il modello cooperativo, la cui funzione sociale conosce il *favor* costituzionale *ex* art. 45, ben potrebbe adattarsi al mondo digitale, mirando da un lato, alla tutela di soggetti che, sul mercato, rivestono una posizione di debolezza e, dall'altro, ponendosi come alternativa alla società capitalistica, tramite il superamento della logica, unicamente indirizzata a massimizzare i profitti, che imperversa nel settore.

Le cooperative di dati possono rappresentare, dunque, un modello capace di stabilire una *governance* democratica delle operazioni di trattamento dei dati, grazie ad una concreta applicazione del principio di solidarietà, promuovendo l'imprenditoria digitale unitamente al benessere sociale e creando così un *digital ecosystem* più equo, egualitario ed inclusivo.

3. Il consenso (ed i consensi) nell'ambito della cooperativa di dati.

3.1. Il consenso al trattamento dei dati ed il consenso espresso in occasione delle delibere assembleari: profili distintivi.

Nella cooperativa di dati, i vari soci-interessati del trattamento (o titolari dei dati) acconsentono a che la società utilizzi i loro dati per i fini e con i modi stabiliti nello statuto e definiti di volta in volta dall'assemblea. Tale consenso rappresenta la condizione di liceità [32] (*ex* art. 6, par. 1, lett. a) e, eventualmente, *ex* art. 9, par. 2,

[32] Sulle condizioni di liceità del trattamento, v. F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, in G. FINOCCHIARO (opera diretta da), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, cit., p. 110 ss.; D. POLETTI, *Le condizioni di liceità del trattamento dei dati personali*, in *Giur. it*., 2019, 12, p. 2783 ss.; ID., *Art. 6 GDPR. Liceità del trattamento*, in R. D'ORAZIO-G. FINOCCHIARO-O. POLLICINO-G. RESTA (a cura di), *Codice della* privacy *e* data protection, Milano, 2021, p. 191 ss.; M. DELL'UTRI, *Principi generali e condizioni di liceità del trattamento dei dati personali*, in V. CUFFARO-R. D'ORAZIO-V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, p. 179 ss.; con particolare riguardo al consenso al trattamento dei dati, *ex multis*, v. P. GALLO, *Il consenso al trattamento dei dati personali come prestazione*, in *Riv. dir. civ*., 2022, 6, p. 1054 ss.; C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, cit.; P. MANES, *Il consenso al trattamento dei dati personali*, Padova, 2001; A. SPATUZZI, *Contratto di fornitura di servizi digitali e ruolo del consenso al trattamento dei dati personali*, in *Notar*., 2021, 4, p. 371 ss.; V. BACHELET, *Il consenso oltre il consenso: dati personali, contratto, mercato*, Pisa, 2023; E. TOSI, *Circolazione dei dati personali tra contratto e responsabilità: riflessioni sulla fragilità del consenso e sulla patrimonializzazione dei dati personali nella società della sorveglianza digitale*, Milano, 2023; S. THOBANI, *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità*, in *Eur. dir. priv*., 2016, 2, p. 513 ss.; G. COMANDÈ, *Leggibilità algoritmica e consenso al trattamento dei dati personali*, in *Danno e resp.*, 2022, 1, p. 33 ss.; A. VI-

lett. a) GDPR) che la cooperativa-titolare del trattamento deve soddisfare affinché lo stesso possa essere considerato lecito, e quindi, libero, specifico, informato ed inequivocabile.

Nel quadro delineato dal *Data Governance Act*, appare particolarmente rilevante l'onere in capo ai fornitori di servizi di intermediazione di dati – e fra questi, le cooperative di dati – del rispetto dei principi posti a tutela dell'interessato, tra i quali, sicuramente, quello di liceità. È infatti cruciale, affinché gli obbiettivi sottesi al DGA possano essere soddisfatti, la creazione di un clima di massima fiducia per i *data subjects* e per i *data holders* con cui i fornitori dei menzionati servizi si interfacciano. A maggior ragione in un contesto nel quale pare possibile affermare che il consenso non costituisca più la prima, nel senso di prioritaria base giuridica del trattamento, potendosene rinvenire altre più idonee a tutelare l'interessato (e oggi anche il titolare dei dati), e, dunque, sembri perdere la sua centralità nell'alveo delle condizioni di liceità del trattamento, l'indagine sulla validità dello stesso deve essere sottoposta a criteri particolarmente rigorosi [33].

Il rapporto di fiducia che di certo non si è creato nelle relazioni tra *Big Tech* e interessati e al quale mirano, tra gli altri, le cooperative di dati, deve necessariamente affondare le sue radici nell'informazione che viene garantita a tutti quei soggetti che, tramite il consenso, autorizzano il titolare all'utilizzo dei dati anche al fine di inserire tale utilizzo dei dati (e, preme sottolinearlo, non i dati in sé) in logiche contrattuali [34]. Segnatamente, la fiducia ingeneratasi per mezzo e nei confronti delle cooperative di dati, permetterà (o, quantomeno, dovrebbe permettere) ad un sempre più ampio numero di individui di voler assumere la qualità di socio della cooperativa. Questo, sia in vista dei vantaggi che i soci possono ottenere dalle operazioni di *data pooling* e *data sharing* attuate dalla cooperativa sia per il fatto che la gestione, pur potendo essere indirizzata anche a sfruttamenti contrattuali e, quindi, prettamente economici, dei dati a disposizione, si muoverà comunque lungo binari etici.

I soci della cooperativa di dati possono, infatti, aspirare ad un adeguato e chiaro ri(s)torno derivante dal loro consenso, unito a quello degli altri soci, all'utilizzo dei dati. Tale fattore non ha certo un'analoga incidenza nel rapporto con le grandi imprese il cui *core business* è lo sfruttamento (il più delle volte, cieco) dei

---

VARELLI, *Il consenso al trattamento dei dati personali nell'era digitale: sfide tecnologiche e soluzioni giuridiche*, Napoli, 2019.

[33] *Amplius* per questa tesi, sia consentito il rinvio a C. BASUNTI, *La (perduta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali*, in *Contr. e impr.*, 2020, 2, p. 860 ss.

[34] La ricostruzione del consenso-condizione di liceità come consenso di tipo autorizzatorio, idoneo a rimuovere un ostacolo posto dall'ordinamento al preesistente potere del titolare, viene efficacemente fornita da F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, cit., p. 140 ss.; ID., *Lo "scambio di dati personali" nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto*, in *Contr. e impr*., 2019, 1, spec. p. 40 ss.

dati per fini di profitto, in cui i dati stessi, e quindi le persone di cui questi ultimi rappresentano attributi della personalità, vengono annichiliti a "merce di scambio". Inoltre, sulla base delle scelte di politica del diritto espresse nel DGA, l'utilizzo dei dati viene anche finalizzato al benessere sociale tramite un loro sapiente impiego in favore di enti pubblici, improntati alla sostenibilità e al progresso comune. Comunque, pure nel caso in cui la cooperativa si proponesse anche un utilizzo dei dati in ambito negoziale, ciò avverrebbe sulla base dei solidi principi etici propri della cooperativa, chiariti nell'atto costitutivo così come nel contratto costitutivo e, pertanto, condivisi da tutti i soci. Qualsiasi vantaggio, ottenuto sul mercato dalla cooperativa, si tradurrebbe in un vantaggio per il socio che otterrebbe, direttamente o indirettamente, grazie alla aggregazione con altri soggetti, benefici concreti ben superiori a quelli che riceverebbe agendo come singolo nel "mercato dei forti".

Come è stato evidenziato [35], nell'ambito delle cooperative di dati, si determina un controllo duale sui dati: una *governance* collettiva in capo alla società accanto ad una, imprescindibile, *governance* individuale, in capo all'interessato o titolare dei dati. Un tale sistema non è, infatti, volto a privare il *data subject* o il *data holder* del controllo sui dati, ma, al contrario, a potenziare le tutele loro offerte grazie al controllo ulteriore e maggiormente specializzato degli intermediari.

Il DGA, pur essendo indirizzato ad ampliare le possibilità di utilizzo dei dati, si mostra sul punto attento a vestire di concretezza quegli strumenti di autodeterminazione e controllo sui dati – su tutti, il consenso al trattamento – che, delineati dal GDPR, si sono spesso mostrati solo formali [36].

Il consenso al trattamento dei dati deve però essere distinto dal consenso fornito dal socio alla formazione della volontà della società cooperativa.

Il consenso espresso nel contesto di maggioranze necessarie all'approvazione di delibere assembleari è funzionalmente diverso dal consenso-condizione di liceità. In proposito, si è espressa la Corte di Cassazione in un caso di trattamento illecito

---

[35] In questo senso F. BRAVO, *Le cooperative di dati*, cit., p. 762 ss. e *passim*.

[36] Si consenta ancora il rinvio a C. BASUNTI, *La (perduta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali*, cit., spec. pp. 881-882 in cui si è sostenuto che nei vari casi in cui via sia uno squilibrio di potere, inteso in senso lato, possa operare «una presunzione (relativa) di non effettività (e quindi non libertà) del consenso prestato»; in questo senso v. anche EDPB, *Linee guida 5/2020 sul consenso ai sensi del Regolamento (UE) 2016/679. Versione 1.1.*, adottate il 4 maggio 2020, pp. 9-10 in cui si afferma che «data la dipendenza risultante dal rapporto datore di lavoro/dipendente, è improbabile che l'interessato sia in grado di negare al datore di lavoro il consenso al trattamento dei dati senza temere o rischiare di subire ripercussioni negative come conseguenza del rifiuto. È improbabile che il dipendente sia in grado si rispondere liberamente, senza percepire pressioni (…). Di conseguenza il Comitato ritiene problematico per il datore di lavoro trattare i dati personali dei dipendenti attuali o futuri sulla base del consenso, in quanto è improbabile che venga prestato liberamente»; parimenti si era espresso il GRUPPO DI LAVORO *EX* ART. 29, *Linee guida sul consenso ai sensi del Regolamento 2016/679*, adottate il 28 novembre 2017, come adottate e modificate da ultimo il 10 aprile 2018, pp. 7-8.

effettuato da una cooperativa sui dati di un socio lavoratore [37]. Nella fattispecie, si è evidenziata la presenza di un'asimmetria tra la cooperativa e il lavoratore, stante il timore di quest'ultimo di ripercussioni negative in caso di mancata prestazione del consenso al trattamento dei dati, idoneo a minare la libertà (e, quindi, la validità) del consenso eventualmente prestato. La S.C. ha in questa sede chiarito che nonostante il rapporto in questione avesse natura associativa e, dunque, alla formazione della volontà dell'ente contribuissero gli stessi soci tramite le delibere assembleari, il trattamento dei dati non poteva considerarsi legittimo se fondato sulle decisioni dell'assemblea e sulla maggioranza emersa in seno ad essa. Il consenso al trattamento dei dati, infatti, deve essere circondato da idonee garanzie, tali da determinare un'adeguata ponderazione e consapevolezza dell'interessato, sicuramente incompatibili con eventuali condizionamenti che possono emergere nei rapporti di lavoro e nelle delibere assembleari. In questo senso, «il consenso è validamente prestato solo se espresso liberamente e specificamente in riferimento a un trattamento chiaramente individuato» [38].

Affinché il trattamento sia lecito, in ambito lavorativo, sul datore di lavoro incombe un onere probatorio particolarmente gravoso: egli deve dimostrare, puntualmente, anche sulla scorta del principio di *accountability*, che il consenso è stato espresso liberamente e, quindi, la non sussistenza di ripercussioni negative sui dipendenti (attuali o futuri) in caso di mancata prestazione del consenso stesso. Nella fattispecie vagliata dalla Corte di cassazione, la partecipazione al concorso era obbligatoria per tutti i soci lavoratori e, pertanto, in seguito alla decisione dell'assemblea, si deve escludere la libertà del consenso (al trattamento) prestato dai soci, tenuto conto del duplice ruolo da essi rivestito: membri dell'assemblea con diritto di voto in merito alle decisioni della società-titolare ed interessati al trattamento [39].

Nella cooperativa di dati si intersecano, dunque, più piani che devono essere tra loro ben differenziati al fine di porre in essere trattamenti leciti. Le decisioni prese dall'assemblea, e quindi dalla società, non possono sovrapporsi alla decisione di un socio di prestare il proprio consenso quale valida base giuridica del trattamento. L'indagine deve sempre riguardare il caso concreto, valutando le effettive circostanze in cui operano i consensi nell'ambito dell'azione della cooperativa, ma te-

---

[37] Il riferimento è a Cass., 1° giugno 2022, n. 17911, in *Giur. it*., 2022, 12, p. 2597 ss., con nota di S. THOBANI. Il caso riguarda la pubblicazione, da parte di una società cooperativa, sulla bacheca aziendale, di dati relativi ai soci in merito a contestazioni disciplinari unitamente alle relative valutazioni effettuate dalla cooperativa stessa, mediante l'uso di "faccine" nell'ambito di un concorso a premi per i soci lavoratori, finalizzato ad incentivare condotte meritevoli tra i soci e la cui partecipazione era per loro obbligatoria.

[38] Così Cass., 1° giugno 2022, n. 17911, cit.

[39] Cfr. S. THOBANI, *Consenso al trattamento e delibere assembleari*, in *Giur. it*., 2022, 12, p. 2601, dove l'Autrice afferma: «rispetto al trattamento dei dati con finalità di valutazione dell'operato dei lavoratori, il socio lavoratore riveste dunque due separati ruoli: quello di socio, che partecipa alle decisioni dell'ente titolare del trattamento, e quella di lavoratore, come interessato».

nendo ben presente che «i due piani di *governance*, individuale e collettiva, rimangono distinti» [40].

Pertanto, anche con riguardo al consenso al trattamento dei dati, i fornitori di servizi di intermediazione dei dati, e tra questi le cooperative di dati, devono agire nell'architettura normativa delineata dal GDPR e dal DGA, garantendo una tutela adeguata all'interessato ed ai suoi diritti fondamentali. Le cooperative di dati devono infatti operare (anche) in funzione di una tutela collettiva per i *data subjects* ed i *data holders* che rivestono il ruolo di soci, offrendo loro una maggiore protezione rispetto a quella che otterrebbero agendo come singoli sul mercato, nella rete di rapporti contrattuali che caratterizza i fenomeni circolatori in cui vengono inseriti, con le dovute peculiarità, i dati.

3.2. Sulla limitazione delle finalità nell'ambito della circolazione dei dati tra interessato, impresa e cooperativa di dati.

Nell'ambito delle cooperative di dati, si è visto, possono ricoprire la qualità di soci sia *data subjects* (ai sensi del GDPR) sia *data holders* (ai sensi del DGA). Se, nel primo caso, l'autorizzazione all'utilizzo dei dati può efficacemente essere prestata attraverso il consenso al trattamento, dovendosi, dunque, incentrare l'analisi circa la liceità del trattamento sulla validità dello stesso, nel secondo caso, laddove vi sia un'impresa (ad esempio, impresa individuale o rientrante nella categoria delle PMI) che intenda conferire in cooperativa i dati raccolti nella sua attività imprenditoriale, la situazione diventa più complessa [41].

Nell'ultimo caso prospettato, la validità del trattamento posto in essere dall'impresa deve essere indagata con particolare attenzione e risultano necessarie maggiori accortezze. Può infatti presentarsi la situazione in cui un'impresa che opera sul mercato (anche) trattando dati sia membro di una cooperativa di dati ed intenda condividere, nell'ambito di tale cooperativa, i dati collazionati. Una simile operazione può certamente essere inclusa nell'ambito dell'ampia definizione di «trattamento» enunciata giusta l'art. 2, par. 1, n. 2), GDPR [42] e, pertanto, deve trovare giustificazione su un'idonea base giuridica. Tra queste, il consenso sembra essere quella che, fisiologicamente, può essere utilizzata, ma si deve comprendere come si atteggi in simili fattispecie.

A ben vedere, avremo, a monte, un consenso prestato da un soggetto qualifica-

---

[40] Così, condivisibilmente, F. BRAVO, *Le cooperative di dati*, cit., p. 790.

[41] Tale problematica viene posta in luce da F. BRAVO, *Le cooperative di dati*, cit., p. 798.

[42] Ai sensi della norma, può essere considerato come «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione».

bile come interessato che autorizza l'impresa-titolare del trattamento ad effettuare operazioni di trattamento sui suoi dati. L'impresa acquisisce, dunque, il consenso e, nel trattare i dati dell'interessato, assumendo altresì la qualifica di *data holder*, decide, a sua volta, a valle, di acconsentire all'utilizzo di tali dati da parte di una cooperativa di dati di cui è membro.

A parere di chi scrive, il problema che emerge in casi come quello qui ipotizzato deve essere ricondotto al principio di limitazione delle finalità di cui all'art. 5, par. 1, lett. b), GDPR ai sensi del quale i dati personali devono essere «raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali». Si determina, infatti, un intreccio di consensi-autorizzazioni, l'uno susseguente all'altro, dove il primo deve necessariamente essere in grado di giustificare il secondo, così da renderlo valido.

Posto che il (primo) consenso, conferito dall'interessato all'impresa, deve essere rispettoso delle note caratteristiche espresse dall'art. 4, par. 1, n. 11), GDPR – e, dunque, deve essere libero, specifico, informato e inequivocabile –, altrimenti il trattamento non sarà lecito (in mancanza di un'altra valida base giuridica *ex* art. 6 GDPR), è proprio tale consenso a dover reggere, giustificandolo, l'atto con cui l'impresa autorizza la cooperativa ad accedere ai dati e a porre in essere operazioni di trattamento.

In tal guisa, la cooperativa tratta lecitamente i dati di interessati che non hanno con la stessa un contatto diretto, e questo in forza di una intelaiatura di atti autorizzatori che tendono a finalità ben chiare.

L'impresa-titolare del trattamento, nel definire *ab initio* le finalità ed i mezzi del trattamento che intende effettuare, è tenuta ad informare adeguatamente l'interessato sul punto. Da un lato, si garantisce così il principio di trasparenza, in modo che l'interessato possa compiere scelte libere, in quanto informate, esercitando il proprio diritto all'autodeterminazione informativa, dall'altro, si permette al titolare una corretta e ponderata organizzazione delle operazioni di trattamento da effettuarsi, agendo nel rispetto del principio di *accountability*. Inoltre, il titolare valuterà così la necessità e la proporzionalità del trattamento[43] in base al rapporto tra gli obiettivi che intende perseguire e la compressione dei diritti in gioco e, segnatamente, di quello alla protezione dei dati personali. In questo senso, si potranno comprendere i dati che, in forza delle finalità preventivate, devono essere trattati, limitando opportunamente la portata del trattamento.

---

[43] V. EDPS, *Quick-guide to necessity and proportionality*, del 28 gennaio 2020; e EDPS, *Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*, del 19 dicembre 2019. Sul tema, si consenta il rinvio a C. BASUNTI, *Il principio di proporzionalità*, in F. BRAVO (a cura di), *Dati personali. Protezione, libera circolazione e* governance – *Vol. 1., Principi*, cit., p. 411 ss.

Laddove, pertanto, un'impresa intenda autorizzare la cooperativa di cui è membro ad accedere e a trattare i dati raccolti da interessati nell'ambito della propria attività, dovrà chiarire in modo adeguato agli interessati la finalità che intende perseguire così che questi ultimi decidano consapevolmente in merito. Va da sé che la cooperativa potrà trattare unicamente i dati di quegli interessati che abbiano, a monte, prestato il proprio consenso per tale finalità determinata, esplicita e legittima, *rectius*, l'impresa potrà concedere l'accesso solo ai dati di questi interessati.

Potrebbe anche verificarsi il caso in cui l'impresa diventi membro della cooperativa in un momento successivo rispetto alla raccolta del consenso da parte di taluni interessati di cui (già) tratta i dati personali. In tale fattispecie, ove per ovvie ragioni non si è potuto prestare un consenso riferito anche allo sfruttamento dei dati da parte della cooperativa, dovranno essere esaminate le finalità su cui si è fondato il consenso prestato dall'interessato, al fine di vagliarne la compatibilità con quelle sorte successivamente e, segnatamente, la possibilità di utilizzo dei dati da parte della cooperativa.

L'impresa-titolare potrebbe, infatti, sulla scorta del principio di *accountability*, riscontrare tale compatibilità tra le finalità e non richiedere un ulteriore consenso all'interessato, dal momento che il legislatore europeo ha previsto [44] la possibilità di trattamento dei dati personali per finalità ulteriori rispetto a quelle per le quali i dati sono stati inizialmente raccolti, purché compatibili con queste ultime. Diversamente, l'impresa sarà tenuta a chiedere un ulteriore consenso all'interessato (o trovare una nuova e diversa base giuridica) in modo da ottenere l'ulteriore autorizzazione ad un utilizzo dei dati in questo senso, rendendo così lecito il trattamento. Le sarà, invece, preclusa la possibilità di conferire in cooperativa i dati personali di coloro che non abbiano prestato tale ulteriore consenso.

Si delinea, pertanto, una sorta di differenziazione delle logiche di utilizzo dei dati raccolti da parte dell'impresa, in cui solo una parte dei dati potrà essere sfruttata (anche) dalla cooperativa in base alle logiche mutualistiche che le sono proprie.

Dovrà essere effettuato, caso per caso, il c.d. *compatibility assessment* [45] dal momento che, se le ulteriori finalità risultano essere incompatibili con quelle per le quali i dati sono stati inizialmente raccolti, il trattamento potrà comunque essere effettuato solamente in presenza di un ulteriore atto autorizzativo (e, dunque, un ulteriore consenso dell'interessato, informato delle nuove finalità) oppure in presenza di un atto legislativo unionale o di uno Stato membro che costituisca una misura necessaria e proporzionata per la salvaguardia degli obiettivi di cui all'art. 23, par. 1, GDPR. Tale vaglio si baserà, tra gli altri, sui criteri elencati all'art. 6, par. 4, GDPR [46] cui il titolare del trattamento dovrà rifarsi.

---

[44] V., in particolare, gli artt. 5, par. 1, lett. b) e 6, par. 4 GDPR, il *Considerando* n. 50 GDPR, nonché l'art. 7 della Convenzione 108+ ed il relativo *Explanatory Report*, al punto 49.

[45] Al riguardo v. GRUPPO DI LAVORO *EX* ART. 29, *Opinion 03/2013 on purpose limitation*, *adopted on 2 April 2013*, spec. p. 20 ss.

[46] Ai sensi dell'art. 6, par. 4 GDPR, il titolare del trattamento, tra gli altri, deve tener conto «a) di

Nelle cooperative di dati, si aggiunge il fatto che il modello di utilizzo dei dati raccolti segue logiche etiche che avvantaggia la cooperativa in sé, i propri soci e finanche la collettività nella sua interezza. Ciò si pone certamente in linea con il menzionato art. 5, par. 1, lett. b), GDPR giusta il quale, finalità (ulteriori) di archiviazione per il pubblico interesse, di ricerca scientifica o storica, e di carattere statistico – tutte finalità indirizzate al bene comune – non sono incompatibili con quelle iniziali. Una cooperativa di dati ben potrebbe, infatti, perseguire tali finalità e utilizzare in queste direzioni (anche) i dati conferiti dall'impresa che, divenuta membro della cooperativa, ne concede a quest'ultima la possibilità di trattarli.

Si aggiunga che l'impresa ottiene dei vantaggi dalla partecipazione alla cooperativa, grazie allo sfruttamento mutualistico dei dati, e tali vantaggi potrebbero essere, seppur indirettamente, rivolti anche agli interessati che con l'impresa si sono rapportati: ad esempio, in termini di (maggiori e migliori) servizi offerti nell'ambito del rapporto che lega i soggetti del trattamento. Questo pare essere un elemento da tenere in debita considerazione nel *compatibility assessment* delle finalità.

In questo quadro, si nota come la normativa *privacy* lasci margini di manovra per la possibilità di utilizzare i dati raccolti per finalità ulteriori rispetto a quelle per le quali è stato prestato, inizialmente, il consenso, rimettendo la decisione in merito (e, di conseguenza, la relativa responsabilità) in capo al titolare del trattamento. Inoltre, i servizi di cooperative di dati si presentano come un nuovo paradigma di utilizzo dei dati che merita di essere incentivato, soprattutto per i benefici che può apportare alla società. Tuttavia, dovrà comunque essere adottata una particolare cautela nel vagliare la compatibilità delle finalità ulteriori. Infatti, la meritevolezza del *cooperative model* e la sua promozione sul mercato digitale non può certo condurre ad un irragionevole restringimento delle tutele offerte al *data subject* ed alla libertà di cui deve godere nell'esercizio del proprio diritto all'autodeterminazione informativa.

4. Quali possibili forme soggettive per la fornitura di servizi di cooperative di dati?

4.1. I servizi di cooperative di dati nella forma delle reti di imprese.

Il *Data Governance Act* non circoscrive il campo delle possibili forme soggettive che il fornitore di servizi di cooperative di dati, quali servizi di intermediazione

---

ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto; b) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento; c) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9, oppure se siano trattati dati relativi a condanne penali e a reati ai sensi dell'articolo 10; d) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati; e) dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione».

dei dati di cui all'art. 10 DGA, può assumere. Lo stesso *Considerando* n. 31 DGA fa genericamente riferimento ad un «gruppo» del quale i singoli individui che lo compongono devono conoscere un rafforzamento della propria posizione. Inoltre, al di là di singoli interessati, ai sensi della definizione di servizi di cooperative di dati, giusta l'art. 2, par. 1, n. 15), DGA, anche imprese individuali o PMI possono essere membri della struttura organizzativa fornitrice del servizio di intermediazione. Pare quindi possibile, sulla scorta delle larghe maglie del dettato normativo, lasciare aperta la strada a formazioni sociali ulteriori rispetto a quella della società cooperativa che, pur rimanendo il punto di riferimento più immediato per l'interprete e, se vogliamo, fisiologico, non necessariamente deve escludere altri modelli organizzativi che con altrettanta efficacia possano fornire i servizi di cooperative di dati [47].

La forma del contratto di rete tra imprese [48] sembra poter essere un efficace schema entro il quale inserire i servizi di cooperative di dati.

Come è noto, il contratto di rete è stato introdotto nel nostro ordinamento con la l. 9 aprile 2009, n. 33 e successive modifiche, di conversione, con modificazioni, del d.l. 10 febbraio 2009, n. 5, recante misure urgenti a sostegno dei settori industriali in crisi. Nella prospettiva legislativa, il contratto di rete – definito "transtipico" [49] – è un contratto plurilaterale, formale (redatto per atto pubblico o scrittura privata autenticata), a contenuto obbligatorio che ha ad oggetto l'esercizio in comune di una o più attività economiche «allo scopo di accrescere, individualmente e collettivamente, la propria capacità innovativa e la propria competitività sul mercato» (art. 3, co. 4-*ter*, l. n. 33/2009). Con la rete di imprese si attua un insieme di relazioni caratterizzate da una, almeno tendenziale, stabilità tra imprese che restano tra loro distinte, ma che possono essere concorrenti e tra le quali sussiste una interdipendenza ed emerge un'esigenza di coordinamento [50].

---

[47] Pone in luce tale aspetto del DGA F. BRAVO, *Le cooperative di dati*, cit., p. 759 ss.

[48] Tra i molteplici Autori che si sono occupati del tema, si rinvia a G. SPOTO, *I contratti di rete tra imprese*, Torino, 2017; F. CAFAGGI-P. IAMICELI-G.D. MOSCO (a cura di), *Il contratto di rete per la crescita delle imprese*, Milano, 2012; P. IAMICELI (a cura di), *Le reti di imprese e i contratti di rete*, Torino, 2009; F. BRIOLINI-L. CAROTA-M. GAMBINI (a cura di), *Il contratto di rete. Un nuovo strumento di sviluppo per le imprese*, Napoli, 2013; C. GARILLI, *Contratto di rete e diritto* antitrust, Torino, 2017; P. ZANELLI, *Reti e contratto di rete*, Padova, 2012.

[49] Così F. CAFAGGI, *Il contratto di rete e il diritto dei contratti*, in F. MACARIO-C. SCOGNAMIGLIO (a cura di), *Reti di impresa e contratto di rete: spunti per un dibattito*, in *Contr*., 2009, 10, p. 919 ss.; F. CAFAGGI, *Il nuovo contratto di rete:* "Learning by doing"*?*, in *Contr*., 2010, 12, p. 1144; ID.-P. IAMICELI, *Contratto di rete. Inizia una nuova stagione di riforme?*, in *Obbl. e contr*., 2009, 7, p. 597 ss.

[50] Cfr. la definizioni fornita da P. IAMICELI, *Le reti di imprese: modelli contrattuali di coordinamento*, in F. CAFAGGI (a cura di), *Reti di imprese tra regolazione e norme sociali*, Bologna, 2004, p. 128 secondo cui la rete di imprese è «quell'insieme di relazioni di tipo cooperativo e tendenzialmente stabili tra due o più imprese formalmente e giuridicamente distinte, anche concorrenti, tra le cui attività esista o si generi una qualche interdipendenza ed emerga un'esigenza di coordinamento, alla quale la rete risponda ricorrendo a strumenti di governo diversi, formali e informali, contrattuali e non»; tale definizione risente dell'influenza della definizione di *networks* fornita da H. COLLINS, *Introduction:*

Il fenomeno delle reti tra imprese si inserisce a pieno titolo nel dialogo tra economia e diritto [51] in una prospettiva poliedrica [52], ponendosi come strumento che, dotato di una, seppur non particolarmente nitida, cornice legislativa, affonda le sue radici nel diritto dei contratti e dell'impresa e presenta importanti ricadute sul mercato, oggi anche digitale.

La rete opera in un contesto ibrido, caratterizzato dalla ineludibile compresenza degli elementi propri, da un lato, del mercato e dei connessi scambi che ivi avvengono, contraddistinti da azioni poste in essere, per interessi propri, dell'agente, in un'ottica antagonista, e, dall'altro, dall'organizzazione gerarchica – *hierarchy* – nella quale i soggetti operano in un ordine, con ruoli ben definiti da un superiore gerarchico, stabilendo un sistema autoritativo [53]. In altri termini, si potrebbe affer-

---

The Reseach Agenda of Implicit Dimensions of Contracts, in D. CAMPBELL-H. COLLINS-J. WIGHTMAN (eds.), *Implicit Dimension of Contracts: Discrete, Relational and Network Contracts*, Oxford-Portland, 2003, pp. 19-20.

[51] R.M. BUXBAUM, *Is "Network" a Legal Concept?*, in *J. of Inst. And Theor. Economics*, 1993, 4, p. 698 ss. si interrogava sui possibili risvolti di interesse giuridico delle reti, per poi concludere a p. 704 affermando nettamente che: «*"Network" is not a legal concept*»; in netto contrasto si pone M. GRANIERI, *Il contratto di rete: una soluzione in cerca del problema?*, in F. MACARIO-C. SCOGNAMIGLIO (a cura di), *Reti di impresa e contratto di rete: spunti per un dibattito*, cit., p. 936; sul punto, v. F. MACARIO, *Il "contratto" e la "rete": brevi note sul riduzionismo legislativo*, in ID.-C. SCOGNAMIGLIO (a cura di), *Reti di impresa e contratto di rete: spunti per un dibattito*, cit., p. 952, sottolinea che quello relativo alla reti di imprese sia un «fenomeno di matrice socio-economica che reclama (…) una disciplina articolata» e ne ricerca un inserimento nelle categorie tradizionali del diritto privato attraverso una declinazione nella disciplina del contratto, della responsabilità aquiliana e nelle regole della concorrenza, ossia nella materia *antitrust*; v. anche A. LOPES-F. MACARIO-P. MASTROBERARDINO (a cura di), *Reti di imprese. Scenari economici e giuridici*, Torino, 2007. Con riferimento alla relazione tra economia e diritto, è di primaria importanza G. CALABRESI, *Il futuro del* Law and Economics. *Saggi per una rimeditazione ed un ricordo*, F. FIMMANÒ-V. OCCORSIO (a cura di), *Presentazione* di E. AL MUREDEN; sul punto v. anche G. ALPA, *Il futuro di* Law & Economics*: le proposte di Guido Calabresi*, in *Contr. e impr.*, 2016, 3, p. 597 ss.; E. AL MUREDEN, *Il futuro del* Law and Economics *nel pensiero di Guido Calabresi*, in *Riv. dir. civ*., 2018, 3, p. 778 ss.

[52] Emblematiche le pagine di G. CALABRESI-A.D. MELAMED, *Property rules, liability rules and inalienability: one view of the cathedral*, in *Harvard Law Rev*., 1972, 85, p. 1089 ss. in cui, al fine di spiegare la complessità della realtà giuridica, si ricorre alla metafora della cattedrale di Rouen, dipinta da Monet nelle differenti visuali, determinate dai toni di luce che si susseguono nell'arco della giornata.

[53] In argomento, v. G. TEUBNER, Coincidentia Oppositorum*: Hybrid Networks Beyond Contract and Organisation*, in M. AMSTUTZ-G. TEUBNER (a cura di), *Networks. Legal Issues of Multilateral Co-operation*, Oxford-Portland, 2009, p. 3 ss.; W.W. POWELL, *Neither Market nor Hierarchy: Network Forms of Organization*, in *Research in Org. Behavior*, 1990, 12, p. 295 ss.; G.S. GEIS, *The Space Between Markets and Hierarchies*, in *Virginia Law Rev*., 2009, 1, p. 99 ss.; O.E. WILLIAMSON, *Markets and Hierarchies: Analysis and Antitrust Implications: A Study in the Economics of Internal Organization*, New York, 1975; F. CAFAGGI, *Contractual Networks and the Small Business Act: Towards European Principles?*, in *Eu. Rev. Contr. Law*, 2008, 4, p. 493 ss., spec. pp. 495-496, in cui si afferma: «*Contractual networks are hybrid forms of organizations located between markets and hierarchies. Networks differ from market contracting because the participants are not impersonal agents but well identified players chosen on the basis of resource complementaries. They permit resources*

mare che il contesto è quello in cui la concorrenza incontra la cooperazione.

Le reti di imprese si sono proposte, sin dagli esordi, come schema di *business* strategicamente destinato in particolare alle piccole e medie imprese, permettendo loro di agire sul mercato superando i propri limiti dimensionali. Si tratta di un modello indirizzato a governare l'interdipendenza tra le imprese preservandone, ad un tempo, l'indipendenza.

Le singole imprese in rete possono avvalersi delle proficue relazioni tra loro sussistenti, mantenendo una piena autonomia ed indipendenza, ma migliorando il proprio posizionamento competitivo. In tal guisa, infatti, le imprese, per mezzo delle sinergie create attraverso la forma reticolare, possono diventare più innovative e competitive sul mercato, sempre più globalizzato, in cui i *Big Players* godono di una posizione di assoluto privilegio.

Tale aspetto, caratterizzante le reti di imprese, preme sottolinearlo, si pone pienamente in linea, nell'ambito della circolazione e della *governance* dei dati, con la *ratio* sottesa al DGA di arginare i fenomeni sostanzialmente oligopolistici delle grandi imprese, nell'ottica di creare proficui margini di azione per le PMI. Pare infatti che si tratti di finalità che, seppur da punti di vista differenti, hanno riguardo al medesimo problema e tentano di offrire opportune soluzioni. Proprio per tale ragione, i due sistemi legislativi meritano, a parere di chi scrive, di essere posti a dialogo tra loro, per comprendere se realmente l'uno è, come appare, complementare all'altro nel settore digitale.

Il progressivo abbattimento dei confini nazionali del mercato, che ne ha determinato un'apertura su scala mondiale, ha reso quantomai utile la condivisione di informazioni e competenze. La circolazione del *know-how* in una prospettiva di reciprocità e collaborazione può risultare la chiave per valorizzare massimamente gli *assets* a disposizione di ciascuna impresa. Un simile sistema di aggregazione di imprese, dotato di profonda flessibilità, appare efficace per far fronte alle sfide che la globalizzazione impone in termini di innovazione e competitività sui mercati non solo nazionali.

Soprattutto per le PMI, la possibilità di competere efficacemente su un mercato di tale portata passa necessariamente attraverso la condivisione di conoscenze, progettualità, capacità e costi. In questo senso, la rete di imprese permette ai singoli aderenti di conservare la propria autonomia così da poter investire per finalità mirate e utili per le rispettive attività, senza che sia necessario costituire un nuovo soggetto giuridico (c.d. rete-soggetto contrapposta alla c.d. rete-contratto), autonomo centro di imputazione di rapporti giuridici attivi e passivi, nonostante ne sia prevista la possibilità, attraverso l'iscrizione nella sezione ordinaria del registro delle imprese nella cui circoscrizione è stabilita la sede.

Se, da un lato, non è necessaria la costituzione di un soggetto di diritto a sé, aspetto questo che differenzia ontologicamente la rete di imprese dalla società coo-

---

bundling that markets are unable to achieve. They differ from hierarchies because enterprises are autonomous and legally independent even if they may be economically dependent».

perativa – anche nella veste di fornitori di servizi di cooperative di dati –, dall'altro, il profilo fiduciario rimane centrale. Il rapporto di fiducia nell'ambito della rete, indirizzato allo svolgimento in comune del programma di rete, plasma in modo particolare il rapporto tra gli imprenditori aderenti che mirano al loro progresso, ben consapevoli del fatto che quest'ultimo deriva (con maggior facilità) da quello della rete nel suo complesso. Un saldo legame fiduciario rappresenta la chiave di volta per una cooperazione stabile e vincente: per la crescita sia dei singoli sia della rete, *rectius*, per la crescita dei singoli attraverso la crescita della rete.

L'architettura della rete di imprese si mostra, dunque, come un modello la cui utilità in termini di sviluppo imprenditoriale può essere calata nel contesto attuale, caratterizzato da un mercato globalizzato che si muove lungo le direttrici dell'innovazione tecnologica. L'accesso e la possibilità di operare proficuamente sul mercato digitale comportano un impegno costante da parte degli agenti, tenuti, al fine di mantenere competitività, sempre più spesso, a muoversi in anticipo. Ecco perché un'azione coordinata di più soggetti, depositari di conoscenze specifiche, può, in tale settore, esplicare la massima utilità.

Affinché una rete di imprese possa, in *compliance* con il *Data Governance Act*, rivestire il ruolo di fornitore di servizio di cooperativa di dati, pare opportuno sottolineare che l'attenzione debba essere incentrata sui singoli membri della rete e sui loro diritti. Se, infatti, le cooperative di dati sono, tra l'altro, deputate all'aiuto dei relativi membri nel far valere le facoltà loro riconosciute dall'ordinamento giuridico con particolare riferimento all'esercizio dei diritti in relazione a determinati dati, a maggior ragione se di carattere personale, tale fondamentale aspetto non può certo essere tralasciato, e neppure compresso, in forza di una differente forma organizzativa adottata. L'*agere* nel settore della circolazione dei dati (anche personali) significa muoversi, al contempo, anche in vista di una adeguata protezione dei dati stessi, così come delineata dal GDPR. Inoltre, il DGA enfatizza l'importanza di un libero esercizio dei diritti sui dati anche attraverso l'istituzione dei servizi di intermediazione dei dati e, tra questi, dei servizi di cooperative di dati, chiamate ad operare (anche) in questa direzione.

La rete che intenda offrire il servizio di cooperativa di dati dovrà altresì aiutare le singole imprese a compiere scelte informate prima di autorizzare l'accesso a determinati dati personali o non personali o, comunque, la loro condivisione; dovrà inoltre procedere a scambi di opinioni in merito alle finalità e condizioni del trattamento dei dati, negoziandone i termini se del caso, avendo sempre riguardo ai soggetti aderenti alla rete e ai loro precipui interessi così da valorizzarli al meglio.

Pertanto, il puntuale rispetto di quanto richiesto dal DGA per i servizi di cooperative di dati, a partire dalla definizione offertane giusta l'art. 2, par. 1, n. 15) del Regolamento stesso, rappresenta un elemento imprescindibile al fine di poter inquadrare la rete di imprese come modello per le cooperative di dati.

Di più, il rapporto di fiducia che lega i vari membri di una cooperativa di dati (imprese parti di una rete o soci di una società cooperativa) affonda le proprie radici nella possibilità, in capo ad ognuno, di potenziare la propria posizione soggetti-

va, grazie ad una forma di aggregazione con risvolti di utilità pratica per i singoli membri sia in termini di competitività sul mercato sia sotto il profilo di un più agile esercizio dei diritti sui dati. Tale prospettiva di *empowerment*[54] del *data subject* e del *data holder* deve essere tenuta in massima considerazione.

Sebbene, a differenza della società cooperativa, nell'ambito del contratto di rete non sia previsto un fine mutualistico, il disegno comune in base al quale le varie imprese hanno prestato la propria adesione, deve comunque essere impostato in modo tale non solo da promuovere la crescita della rete complessivamente intesa, ma anche da garantire adeguati benefici per i singoli membri, sostanzialmente, in un'ottica solidaristica. Tali benefici devono essere intesi in senso lato: infatti, essi non devono necessariamente essere di diretto carattere economico, ma possono concretizzarsi anche nella circolazione di capacità e conoscenze, nella creazione di nuove opportunità lavorative, nella possibilità di posizionarsi con successo su mercati prima non esplorati dal singolo membro, nel reciproco aiuto per rispettare la normativa in tema di *data protection*, nell'ideazione di nuove prospettive imprenditoriali, e così via. Si tratta, dunque, di un'impostazione strategica di sviluppo che presta particolare attenzione ai componenti della rete e che deve essere fatta propria anche dalla rete di imprese che intenda proporsi come intermediario dei dati. In altri termini, sembra possibile affermare che, da questo punto di vista, il *modus operandi* della rete si avvicina molto a quello della società cooperativa.

Inoltre, la rete deve occuparsi della *governance* collettiva dei dati forniti dagli aderenti e da questi puntualmente definita, facendo sempre salva la dimensione di *governance* individuale che permane in capo alle singole imprese. Queste ultime sfrutteranno i dati cui hanno accesso, in forza di un'idonea base giuridica, non solo per i propri interessi, ma anche e soprattutto per quelli dei soggetti aderenti. Starà poi ad essi stabilire gli obiettivi e le concrete modalità con cui ricevere i vantaggi derivanti dal sistema reticolare attraverso il programma di rete e la scelta in merito alla creazione di una rete-soggetto o di una rete-contratto, flessibilità, quest'ultima, mancante in una società cooperativa. Le imprese che aderiscono alla rete partecipano in modo diretto ed autonomo, a maggior ragione se non è stato costituito un ente giuridico a sé stante, alla gestione comune delle risorse in vista delle finalità contrattualmente stabilite. Il modello di sviluppo della rete di imprese è infatti di tipo autonomo, anche se connesso alla attività posta in essere dagli altri soggetti aderenti. In tal guisa, pare rimanere in capo alle imprese un maggior controllo sull'utilizzo dei dati che si mettono a disposizione della rete nel complesso. Il fatto che la rete intervenga laddove necessario per la crescita collettiva (e dei singoli attraverso l'impegno collettivo di rete), nonché contrattualmente stabilito, e lasci ampi margini di individualismo agli aderenti, sembra rendere questo modello organizzativo, particolarmente indicato a garantire non solo la *governance* collettiva, ma anche e soprattutto quella individuale.

---

[54] Cfr. D. POLETTI, *Gli intermediari dei dati*, cit., p. 56; e F. BRAVO, *Le cooperative di dati*, cit., pp. 784 e 786.

Ai fini del presente discorso, appare utile chiedersi se sia la forma di rete-contratto sia quella di rete soggetto possano costituire un valido modello di cooperativa di dati, in altri termini, se sia necessaria la costituzione di una entità distinta dagli aderenti.

A ben vedere, la distinzione tra le due forme reticolari attiene alle modalità con cui le imprese intendono collaborare per meglio assumere capacità innovativa e competitività sul mercato: trattasi, dunque, di differenti modelli organizzativi della rete, adottati nell'ambito della libertà di iniziativa economica. Le singole imprese si accordano sulla base dei reciproci disegni imprenditoriali così da costituire il sistema reticolare che maggiormente può essere utile per la loro crescita ed il loro posizionamento in modo da veicolare l'offerta alla ricerca di nuovi sbocchi commerciali, rafforzando quelli già in essere.

Non pare che la scelta sul tipo di rete possa avere una qualche incidenza, almeno in astratto, sulla possibile compatibilità con la cooperativa di dati. Non si vede perché debba essere necessaria la costituzione di un nuovo soggetto di diritto per la fornitura di un servizio di cooperativa di dati: del resto, nessuna disposizione legislativa presenta previsioni in tal senso.

Il vaglio di compatibilità dovrà, piuttosto, essere indirizzato in concreto, per valutare se la specifica rete di imprese (sia essa rete-soggetto o rete-contratto) si presenta *compliant* i) con il quadro generale a tutela dei diritti e libertà fondamentali con particolare riguardo al diritto alla protezione dei dati personali delineato dal GDPR; ii) con quanto il DGA prevede specificamente in materia di servizi di intermediazione dei dati e, tra questi, dei servizi di cooperative di dati. In merito a quest'ultimo aspetto, sarà piuttosto facile trovare similitudini tra le finalità sottese al contratto di rete e al DGA sotto il profilo della promozione della crescita delle PMI sul mercato dove imperano le grandi società. Più attenta dovrà, invece, essere la valutazione sul concreto operare della rete quale fornitrice di servizi di cooperative di dati con particolare riguardo alla tutela e all'ausilio nell'esercizio dei diritti delle singole imprese-*data holders*, nonché ad una amministrazione etica dei dati raccolti, che si discosti dalle logiche che hanno caratterizzato il mercato digitale sin dalla sua nascita, e si muova lungo il percorso del neomutualismo digitale.

4.2. La condizione di cui all'art. 12, lett. a), DGA tra società cooperative e reti di imprese.

Nella regolamentazione dei servizi di intermediazione dei dati, assume un ruolo centrale l'art. 12 DGA con le condizioni ivi stabilite, che devono essere rispettate per la fornitura di tali servizi.

Un soggetto che voglia essere riconosciuto come fornitore di servizi di intermediazione dei dati e che voglia utilizzare tale titolo nelle sue comunicazioni scritte ed orali deve, *ex* art. 11, par. 9, DGA, inviare relativa richiesta all'autorità competente la quale, previa verifica, dichiarerà la conformità all'art. 11 DGA ed il rispetto delle condizioni *ex* art. 12 DGA. Affinché i fornitori, che hanno ottenuto la di-

chiarazione di conformità al DGA e che quindi sono inseriti in un registro pubblico tenuto ed aggiornato regolarmente a cura della Commissione europea, possano essere facilmente riconoscibili e identificabili in tutta l'Unione, *ex* art. 11, par. 9, DGA, essi vengono dotati di un logo comune, stabilito dalla Commissione europea con atti di esecuzione [55]. Tale logo dovrà essere esposto sempre in modo chiaro sia nelle comunicazioni *online* sia in quelle *offline* dell'intermediario nell'esercizio della propria attività di intermediazione.

Nell'alveo delle menzionate condizioni che i fornitori dei servizi di intermediazione dei dati – e quindi anche di servizi di cooperative di dati – devono rispettare, particolare interesse suscita quella *sub* lett. a) [56] ai sensi della quale «il fornitore di servizi di intermediazione dei dati non utilizza i dati per i quali fornisce servizi di intermediazione dei dati per scopi diversi dalla messa a disposizioni di tali dati agli utenti di dati e fornisce servizi di intermediazione dei dati attraverso una persona giuridica distinta». Si nota che tale prima condizione impone due requisiti agli erogatori dei servizi: da un lato, richiede una netta separazione dal punto di vista dei soggetti agenti tra fornitore del servizio ed utilizzatore dei dati oggetto del servizio; dall'altro, richiede l'unicità dello scopo di utilizzo dei dati per i quali il servizio viene offerto.

---

[55] Sul punto la Commissione europea è intervenuta, nell'ambito dell'attuazione dell'atto sulla *governance* dei dati, introducendo tali loghi comuni per aiutare i portatori di interessi a individuare facilmente i fornitori di servizi di intermediazione dei dati e le organizzazioni per l'altruismo dei dati riconosciute nell'Unione. I loghi in tutti i formati e tutte le lingue sono scaricabili liberamente: v. COMMISSIONE EUROPEA, *Loghi per gli intermediari di dati e le organizzazioni per l'altruismo dei dati riconosciute nell'Unione*, 9 agosto 2023, *https://digital-strategy.ec.europa.eu/it/library/logos-data-intermediaries-and-data-altruism-organisations-recognised-union*. Cfr. anche F. BRAVO, *Le cooperative di dati*, cit., pp. 780-781.

[56] La disposizione si completa con il *Considerando* n. 33 DGA secondo cui «è pertanto necessario che i fornitori di servizi di intermediazione dei dati agiscano solo in qualità di intermediari nelle transazioni e non utilizzino per nessun altro fine i dati scambiati. Le condizioni commerciali, compresa la fissazione dei prezzi, per la fornitura dei servizi di intermediazione dei dati non dovrebbero essere subordinate al fatto che un potenziale titolare dei dati o utente dei dati utilizzi altri servizi forniti dallo stesso fornitore di servizi di intermediazione dei dati o da un'entità collegata, tra cui l'archiviazione, l'analisi, l'intelligenza artificiale o altre applicazioni basate sui dati, e, in caso affermativo, dalla misura in cui il titolare dei dati o gli utenti dei dati utilizzino tali altri servizi. Ciò renderà altresì necessaria una separazione strutturale tra il servizio di intermediazione dei dati e qualsiasi altro servizio fornito, in modo tale da evitare conflitti di interessi. Ciò significa che il servizio di intermediazione dei dati dovrebbe essere fornito mediante una persona giuridica distinta dalle altre attività di tale fornitore di servizi di intermediazione dei dati». Per un inquadramento v. L. VON DITFURTH, *Datenmärkte, Datenintenmädiare un der Data Governance Act. Eine Analyse der europäischen Regulierung von B2B-Datenvermittlungsdiensten*, Berlino-Boston, 2024, spec. p. 338 ss.; a p. 340 l'A. afferma che: «*von größter Bedeutung ist das Neutralitätsprinzip, das grundlegend die Erbringung von Datenvermittlungsdiensten prägen soll*», e poi specifica: «*das Neutralitätsprinzip* weist *dabei im Wesentlichen zwei Facetten auf. Zum einen soll die Neutralität der Datenvermittler in Bezug auf die Daten sichergestellt werden, die zwischen Dateninhabern und Datennutzern über ihre Dienste geteilt werden Zum anderen sieht Art. 12 DGA zu einem gewissen Grad eine unabhängige und neutrale Marktstellung der Datenvermittler vor*».

Questa condizione concerne il requisito della neutralità che si richiede ai fornitori dei servizi di intermediazione, intesa come elemento essenziale al fine di accrescere la fiducia ed il controllo dei titolari dei dati, interessati ed utenti dei dati nell'ambito di tali servizi. Essa riflette, dunque le scelte di politica legislativa attuate attraverso il *Data Governance Act* e mira a rispondere al timore che i *data holders* e i *data subjects* possano perdere il controllo sui dati una volta che ne hanno autorizzato l'accesso o il trattamento. Si intende quindi aumentare la fiducia nei confronti degli intermediari così da promuoverne l'operato, facendo loro acquisire col tempo un più ampio ventaglio di soggetti interessati al servizio.

Seppur l'intento sia apprezzabile, la condizione di cui all'art. 12, lett. a), DGA finisce per avere un rilevante effetto limitativo per gli intermediari dei dati.

La neutralità imposta dalla norma non renderebbe possibile per l'intermediario utilizzare i dati raccolti a beneficio degli stessi soggetti da cui i dati sono stati raccolti, ma unicamente per metterli a disposizione di soggetti diversi (gli utenti dei dati richiamati dalla disposizione e la cui definizione si rinviene giusta l'art. 2, n. 9) DGA)[57]. L'intermediario subirebbe una forte limitazione, assumendo un ruolo più che altro passivo, utile solamente a mettere in contatto *data holders* e interessati con i *data users*, essendo esclusa ogni possibile interferenza sui dati raccolti.

Un simile inquadramento se, forse, può trovare un fondamento rispetto ad imprese di grandi dimensioni e contesti in cui vi sia un alto rischio di *cross-data usage*, esso non risulta affatto ragionevole con riferimento ai servizi di cooperative di dati, improntate ad una logica mutualistica e solidaristica[58]. Nell'ambito della cooperativa di dati, i dati ivi conferiti (precisamente, l'accesso ad essi tramite il consenso al trattamento) devono primariamente essere funzionali alla crescita dei singoli soci la cui volontà di far parte della cooperativa si giustifica in forza dei vantaggi a loro derivanti dall'unione con altri soggetti.

Questo discorso, a parere di chi scrive, sembra valere sia nel caso in cui i servizi di cooperative di dati siano erogati nella forma soggettiva della società cooperativa sia della rete di imprese. Sicuramente la società cooperativa, ontologicamente, richiede un utilizzo delle risorse (in questo caso i dati) a vantaggio dei propri soci e non può, pertanto, comprendersi una esclusività di scopo in altra direzione. Si impone, come evidenziato in dottrina[59], una interpretazione elastica della norma così

---

[57] Secondo la definizione fornita dal DGA, si definisce utente dei dati «una persona fisica o giuridica che ha accesso legittimo a determinati dati personali o non personali e che ha diritto, anche a norma del regolamento (UE) 2016/679 in caso di dati personali, a utilizzare tali dati a fini commerciali o non commerciali».

[58] Condivisibilmente sul punto, F. BRAVO, *Le cooperative di dati*, cit., p. 774 ss.; e G. RESTA, *La dimensione collettiva dei dati personali*, in *Parole chiave*, 2023, 1, spec. p. 107.

[59] In questo senso, F. BRAVO, *Le cooperative di dati*, cit., p. 775 secondo il quale: «si potrebbe intervenire a livello interpretativo, applicando in maniera non rigida la "condizione" concernente l'obbligo di separazione soggettiva tra (fornitore del servizio di) cooperativa di dati e utilizzatore di dati, volta a sterilizzarne l'applicazione in considerazione della natura mutualistica della cooperativa, al

da rendere il quadro offerto dal DGA compatibile con le disposizioni in tema di società cooperative.

Parimenti, le imprese che aderiscono ad una rete che svolge servizi di intermediazione di dati (e, quindi, anche di cooperativa di dati) mirano ad una loro crescita principalmente in termini di posizionamento sul mercato. Anche in questo caso, quindi, è la prospettiva di un ritorno concretamente apprezzabile che indirizza gli aderenti verso il contratto di rete e che permette un accesso comune ai dati nella loro disponibilità. Di più, nel caso del contratto di rete, le imprese, con una certa facilità, potrebbero assumere ruoli differenti, finalizzando il disegno complessivo all'elusione della norma. La rete e la sua funzione, nelle troppo strette maglie dell'art. 12, lett. a) DGA, verrebbero frustrate, così come lo spirito che permea l'intera normativa sulla *data governance*, proiettato a favorire massimamente la circolazione e lo sfruttamento dei dati e, tramite ciò, lo sviluppo dei singoli e della società.

4.3. Le ripercussioni in tema di concorrenza.

È ormai chiara da diversi anni l'attenzione del legislatore europeo per le piccole e medie imprese e per il loro sviluppo, nell'ottica di dare concretezza al principio "*Think Small First*" [60]. Anche il *Data Governance Act*, in senso lato, può essere ricompreso in questo quadro.

Lungo questo percorso, l'Unione europea ha deciso di includere nelle proprie politiche l'incentivo alla cooperazione tra imprese – a maggior ragione se di piccole o medie dimensioni – per sfruttare al meglio il potenziale che il mercato offre, anche in una prospettiva transfrontaliera, alle PMI.

---

fine di far salve le norme tipiche della società cooperativa, che devono essere coordinate a livello di sistema con quelle frettolosamente inserite, sul punto, nel *Data Governance Act*»; secondo l'A., non essendo del tutto soddisfacente operare sul versante interpretativo, «si dovrebbe forse intervenire opportunamente in via normativa – in sede europea o in sede nazionale, a livello di coordinamento della disciplina domestica con quella unionale –, chiarendo in maniera più dettagliata le peculiarità della disciplina della *data governance* con riguardo al caso di specifico delle "cooperative di dati", facendo salva l'utilizzabilità dei dati da parte di quest'ultima, nello spirito mutualistico che la contraddistingue e la contrappone al modello più tipicamente capitalistico»; in argomento v. anche le preoccupazioni di H. RICHTER, *Looking at the Data Governance Act and Beyond: How to Better Integrate Data Intermediaries in the Market Order for Data Sharing*, in *Grur int*., 2023, 5, spec. p. 466 che afferma: «*as a consequence, the principle of strict data neutrality may effectively lead to less innovation because DISs will either disappear or not even enter the market*».

[60] V. in particolare COMMISSIONE DELLE COMUNITÀ EUROPEE, Comunicazione al Consiglio, al Parlamento europeo, al Comitato economico e sociale europeo e al Comitato delle regioni, "*Pensare anzitutto in piccolo*" (Think Small First) *Uno* "Small Business Act" *per l'Europa*, Bruxelles, 30 settembre 2008. COM (2008) 394 definitivo/2. Tale documento sostituisce COMMISSIONE DELLE COMUNITÀ EUROPEE, Comunicazione al Consiglio, al Parlamento europeo, al Comitato economico e sociale europeo e al Comitato delle regioni, *"Una corsia preferenziale per la piccola impresa". Alla ricerca di un nuovo quadro fondamentale per la Piccola Impresa (un* "Small Business Act" *per l'Europa)*, Bruxelles, 25 giugno 2008. COM (2008) 394/definitivo.

Va da sé, tuttavia, che pur con il condivisibile *favor* per la cooperazione tra imprese – anche sotto la forma della rete di imprese – non si può considerare il contratto di rete una deroga ai principi propri della libera concorrenza sul mercato che sono dotati di rilevanza costituzionale e informano in maniera trasversale l'intero ordinamento, così come il sistema unionale. L'incentivo verso simili forme di aggregazione presenta sì enormi vantaggi per la crescita delle imprese, per il benessere dei consumatori e per il progresso della società complessivamente intesa, ma a condizione che venga proiettato in senso pro-concorrenziale e non per eludere la normativa *antitrust*. Per le reti di imprese, risulta dunque di particolare importanza un vaglio, caso per caso, di compatibilità con la normativa, nazionale ed unionale a tutela della concorrenza, anche nel caso in cui forniscano servizi di intermediazione dei dati. L'accordo tra i retisti deve essere puntuale nella definizione di un progetto comune e dell'oggetto su cui si incentrerà la collaborazione tra le imprese, chiarendo le finalità sottese come pure le modalità di realizzazione. Il contratto deve risultare effettivamente indirizzato ad accrescere la capacità innovativa e la competitività dei membri della rete e non deve costituire uno strumento, direttamente o indirettamente, funzionale a falsare la concorrenza e, di conseguenza, a porsi in contrasto con la *ratio* stessa dell'istituto [61].

La cooperazione, seppur si presenti come semanticamente opposta al concetto di competizione, laddove correttamente inquadrata e rispettosa dell'apparato normativo in tema di concorrenza, può costituire uno strumento utile per aumentare il dinamismo dei mercati [62]. Il rischio che emerge è la possibilità che un accordo che nasce con l'intento di aiutare soggetti che singolarmente individuati non avrebbero la possibilità di competere sul mercato, divenga uno strumento capace di minare il

---

[61] Sul punto cfr. quanto precisato da AGCM, *Comunicazione relativa all'istituto delle reti di imprese, così come disciplinate dall'articolo 3, comma 4-*ter*, del decreto legge n. 5/2009, come convertito in legge n. 33/2009, e s.m.i*., del 16 maggio 2011, in *Boll. Autorità conc. merc*., 17 maggio 2011, provv. n. 22362; su tale comunicazione v. A. GENOVESE, *Contratto di rete e disciplina* antitrust, in *Contr. e impr*., 2012, 3, p. 725 ss. Parimenti, con riguardo alle società cooperative, v. COMMISSIONE DELLE COMUNITÀ EUROPEE, Comunicazione al Consiglio, al Parlamento europeo, al Comitato economico e sociale europeo e al Comitato delle regioni, *Sulla promozione delle società cooperative in Europa*, Bruxelles, 23 febbraio 2004. COM (2004) 18 definitivo. In argomento, v. A. NERVI, *Contratto di rete e disciplina* antitrust, in *Riv. dir. impr*., 2016, 1, p. 81 ss.; e M. BENGTSSON-S. KOCK, *"Coopetition" in Business Network – to Cooperate and Compete Simultaneously*, in *Ind. Market Management*, 2000, 29, p. 411 ss.

[62] In questo senso M. LIBERTINI, *Contratto di rete e concorrenza*, in *Giust. civ*., 2014, 2, p. 406 dove l'A. afferma: «la cooperazione, sul piano concettuale, è il contrario della competizione. Tuttavia, in realtà complesse come sono quelle dei mercati odierni, la cooperazione fra alcune imprese indipendenti, se vista in una prospettiva sistemica, può essere anche uno strumento atto ad aumentare la concorrenzialità complessiva nei mercati»; *amplius* sul rapporto tra tutela della concorrenza e libertà contrattuale cfr. ID., *Contratto e concorrenza*, in *Enc. dir*., *I Tematici*, Milano, 2021, 1, p. 264 ss.; con riferimento alla applicazione della normativa *antitrust* nel contesto del mercato digitale, v. ID., *Il Regolamento europeo sui mercati digitali e le norme generali in materia di concorrenza*, in *Riv. trim. dir. pubbl*., 2022, 4, p. 1069 ss.; e ID., *Digital markets and competition policy. Some remarks on the suitability of the antritrust toolkit*, in *Orizzonti del dir. comm*., 2021, 1, p. 337 ss.

regolare funzionamento della concorrenza. Anche il DGA che, come si è visto, è indirizzato a dare nuova voce alle piccole e medie imprese, non può certo rappresentare l'occasione per falsare la concorrenza, creando indebite posizioni di vantaggio. E questo, preme sottolinearlo, anche laddove si abbia riguardo ad imprese di dimensioni particolarmente piccole: tale fattore non costituisce, evidentemente, ragione di deroga alla normativa *antitrust*, e neppure una presunzione di compatibilità con quest'ultima. Del resto, il DGA ha tra i suoi obiettivi proprio quello di riequilibrare il mercato digitale, arginando il potere delle *Big Tech*, ed intervenendo, dunque, sul piano concorrenziale: qualsiasi operazione imprenditoriale diretta a creare un contesto di mercato ostile per altri agenti – anche se, questa volta, a vantaggio di coloro che prima erano "deboli" – si porrebbe allora in netto contrasto con la nuova normativa europea.

Pare possibile affermare che il controllo (del rispetto) dei profili concorrenziali con riguardo alle reti di imprese che intendano fornire servizi di cooperative di dati debba essere particolarmente accurata. La rete di imprese è, per definizione, composta da imprese e quindi, nel prisma dei soggetti del trattamento dei dati, da *data holders*. Tali soggetti, tendenzialmente, hanno a disposizione quantità di dati di gran lunga maggiori rispetto ai *data subjects* cui si riferiscono i dati oggetto di trattamento. Le imprese-titolari dei dati possono infatti avere nella loro disponibilità una mole di dati che, seppur non sconfinata come quella delle maggiori multinazionali dell'IT (spesso riunite nell'acronimo GAFAM, relativo a Google, Apple, Facebook, Amazon, Microsoft), dal momento che parliamo, principalmente, di PMI, può comunque avere un rilievo non indifferente. In altri termini, con riguardo alle società cooperative che erogano servizi di cooperative di dati, al di là della possibilità che siano costituite (anche) da persone giuridiche, è possibile rinvenire casi in cui siano formate unicamente da persone fisiche. Una simile evenienza non è configurabile nelle reti di imprese. Si deve, pertanto, tenere presente che l'unione di più imprese, che operano nel mercato dei dati e che possono trattare (molti) dati di altrettanti interessati, può, almeno potenzialmente, incidere in misura maggiore, anche in negativo, sulla concorrenza.

Certamente, è necessario prestare attenzione alle ricadute nell'ambito della concorrenza sia laddove una società cooperativa fornisca servizi di cooperative di dati sia laddove tale servizio venga erogato da una rete di imprese. Tuttavia, in questo secondo caso, il rispetto della normativa *antitrust* deve essere tenuto in massima considerazione.

Quanto affermato deve essere visto nello specchio della *compliance* sia con le norme – nazionali ed europee – in tema di concorrenza sia con il *Data Governance Act* complessivamente inteso e, soprattutto, con riferimento alla *ratio* ad esso sottesa, relativa alla promozione dell'accesso ai dati e ad un loro utilizzo consapevole da parte delle PMI, capace, tra l'altro, di creare fiducia nei confronti del mercato digitale. Le cooperative di dati mirano, infatti, ad un utilizzo etico dei dati raccolti: tale genere di utilizzo non può che andare di pari passo (anche) con un puntuale rispetto delle regole della concorrenza.

Dunque, il titolare del trattamento, nel suo operato, dovrà rispettare (e dimostra-

re di aver rispettato) anche la disciplina della concorrenza che, in un certo qual modo, viene attratta dalla *data protection law*, rientrando così sotto l'egida del principio di *accountability*.

Il vaglio cui le cooperative di dati, a maggior ragione nel caso in cui abbiano la forma della rete di impresa, è, *in primis*, quello in rapporto agli artt. 101 [63] e 102 TFUE nonché alla l. n. 287/1990 [64]. La rete, infatti, potrebbe creare, sulla base del legame tra le imprese, una posizione di supremazia collettiva di cui si potrebbe profittare a danno dei consumatori e degli altri agenti del mercato. Non è difficile pensare che la collaborazione più o meno accentrata tra i retisti possa tradursi con una certa facilità in comportamenti abusivi. A maggior ragione ricordando che la disciplina sulle reti di imprese – seppur volta ad incentivare l'operato delle PMI, soggetti che naturalmente dovrebbero essere incoraggiati a definire alleanze tramite reti – rimane aperta alle imprese di tutte le dimensioni.

Si tratta, tra l'altro, di un terreno fertile per un'attenta applicazione della clausola generale di buona fede che, nel guidare il comportamento dei contraenti, può determinare obblighi di protezione in chiave filoconcorrenziale per il corretto andamento dei traffici [65].

La valutazione non può avvenire unicamente, soprattutto nell'odierno mercato globalizzato, dal punto di vista territoriale, ma deve avere riguardo all'ambito settoriale in cui la rete opera. Sarà necessario avvalersi di articolate analisi economiche di settore, indirizzate a comprendere se, effettivamente, l'accordo abbia ad oggetto o l'effetto «di impedire, restringere o falsare il gioco della concorrenza all'interno del mercato interno» (art. 101, co. 1, TFUE). In tal caso, l'accordo dovrà es-

---

[63] Sul tema cfr. COMMISSIONE EUROPEA, *Linee direttrici sull'applicabilità dell'art. 101 del Trattato sul funzionamento dell'Unione europea agli accordi di cooperazione orizzontale*, 2011/C 11/01, in particolare in prospettiva fisiologica, par. 2 in cui si legge che «gli accordi di cooperazione orizzontale possono determinare vantaggi economici sostanziali, in particolare se combinano attività, competenze o attivi complementari. La cooperazione orizzontale tra imprese può costituire uno strumento idoneo a condividere i rischi, ridurre i costi, aumentare gli investimenti, mettere in comune il *know-how*, aumentare la qualità e la varietà dei prodotti e lanciare più rapidamente le innovazioni sul mercato».

[64] La normativa italiana sul tema, notoriamente, rappresenta una trasposizione sul piano nazionale di quanto già sancito a livello europeo. Parimenti è avvenuto negli altri Stati membri: a titolo di esempio, si richiama, nell'ordinamento spagnolo, la *Ley 15/2007, de 3 de julio, de Defesa de la Competencia* che riforma il primigeneo sistema basato sulla *Ley 16/1989, de 17 de julio, de Defesa de la Competencia* ed il cui art. 1 rappresenta una semplice traduzione dell'art. 101 TFUE. Su tale intervento normativo v. per tutti L. PAREJO ALFONSO-A. PALOMAR OLMEDA (eds.), *Derecho de la competencia. Estudios sobre la Ley 15/2007, de 3 de julio, de Defesa de la Competencia*, Madrid, 2008. Con riguardo al rapporto tra diritto della concorrenza e accordi tra imprese nell'ordinamento spagnolo cfr. R.A. SÁNCHEZ, *Economía colaborativa y derecho* antitrust, in *CEF Legal. Rev. Práctica de der. Com. y casos prácticos*, 2018, 214, p. 35 ss.

[65] Cfr. F. LONGOBUCCO, *Obblighi di protezione e regole di concorrenza nella contrattazione di (e tra) impresa (e)*, in *Contr. e impr. Europa*, 2010, 1, p. 41 ss.; ID., *Abuso di dipendenza economica e reti di imprese*, in *Contr. e impr*., 2012, 2, p. 391.

sere considerato nullo di pieno diritto, purché non si rientri nel campo di applicazione dall'art. 101, co. 3, TFUE che prevede alcune deroghe in forza del bilanciamento con i benefici economici comunque prodotti da determinati accordi anticompetitivi.

Anche il giudizio sullo sfruttamento abusivo di una posizione dominante, eventualmente ricoperta dalla rete di imprese, dovrà avvenire in concreto, dovendosi vagliare non solo, e non tanto, il fatto che la rete detenga una posizione dominante sul mercato, ma un indebito sfruttamento di tale posizione, non semplicemente utile per ottenere "giusti" profitti.

Lo scambio della conoscenza e delle informazioni riveste un ruolo strategico nell'ambito della rete e spesso costituisce proprio l'oggetto del programma di rete. Tale scambio, che può avvenire sia direttamente da parte dei retisti sia tramite una struttura comune, da un lato, può aiutare le imprese a diminuire i costi, ad allocare più proficuamente i prodotti e, più in generale, agire in modo più efficace sul mercato, dall'altro, può dar luogo ad effetti restrittivi della concorrenza, in particolare, con riferimento alla possibilità per le imprese di conoscere le strategie imprenditoriali di quelle che sono (anche) proprie concorrenti. La riduzione dell'incertezza strategica sul mercato comporta, infatti, il pericolo di una limitazione della concorrenza.

Attualmente, il diritto della concorrenza deve essere calato nel contesto digitale e, quindi, anche nell'ambito delle cooperative di dati, al fine di vagliare i casi in cui determinati accordi (come un contratto di rete) tra imprese possano falsare il corretto funzionamento del mercato. Si tratta di una sfida attuale che investe le logiche degli scambi e che risente del sempre più largo impiego di algoritmi [66] e di sistemi di intelligenza artificiale, nonché dello sfruttamento dei *Big Data* [67]. Si nota come il contesto digitale sia, almeno potenzialmente, idoneo ad acuire i rischi di condotte imprenditoriali contrarie alla normativa *antitrust*. Risulta perciò fondamentale un'analisi accurata, da effettuarsi caso per caso, volta a comprendere se un accordo tra imprese possa porsi in contrasto con la regolamentazione della concorrenza.

---

[66] Secondo G. SARTOR, *Le applicazioni giuridiche dell'intelligenza artificiale. La rappresentazione della conoscenza*, Milano, 1990, p. 5, l'algoritmo può essere inteso come «una sequenza di prescrizioni o "istruzioni" che indica in modo preciso e non ambiguo i passi da compiere per risolvere correttamente, a partire da determinate informazioni, un certo tipo di problema (se la soluzione esiste), in un tempo finito. Dalla complessità e potenza degli algoritmi e delle loro sequenze si ottiene un'intelligenza artificiale più o meno evoluta. Per poter essere eseguiti da un elaboratore, gli algoritmi (termine spesso usato per indicare applicazioni della IA) vanno formulati in appositi linguaggi formali, i c.d. linguaggi di programmazione».

[67] Sul rapporto tra sfruttamento dei *Big Data* e tutela della concorrenza cfr. L. CALZOLARI, *La collusione fra algoritmi nell'era dei* big data*: l'imputabilità alle imprese delle "intese 4.0" ai sensi dell'art. 101 TFUE*, in *Media Laws*, 2018, 3, p. 219 ss.; A. PARZIALE, *Regulating Algorithms in The European Data-Driven Economy: The Role of Competition Law and Civil Liability*, in *Op. Jur. in Comp*., 2020, 1, p. 97 ss.; F. DÍEZ ESTELLA, *Google, Internet y Derecho de la Competencia: ¿viejas reglas para nuevos mercados?*, in *CEF Legal. Rev. Práctica de der. com. y casos prácticos*, 2014, 163-164, p. 5 ss.

Non è sempre vero che per normare nuovi fenomeni serva un nuovo diritto[68], ma spetta al giurista, attribuendo rilevanza al quadro d'insieme, adattare soluzioni consolidate alle situazioni che si creano con la diffusione, sempre più capillare, delle nuove tecnologie.

Dunque, il diritto della concorrenza, applicato al settore digitale, deve fungere da guida per gli operatori del mercato. La normativa relativa alla *data governance* deve, pertanto, dialogare con la disciplina della concorrenza perché solo in tal guisa potranno essere perseguite realmente le finalità ad essa sottese. In un contesto in cui le logiche di mercato si intersecano inscindibilmente con i diritti della persona, la cui tutela deve comunque permanere come esigenza fondamentale del sistema nella sua sempre più complessa architettura, il DGA appare sempre più come il tassello di un mosaico che non può essere preso singolarmente, e astratto dal contesto di riferimento.

La fornitura di servizi di intermediazione di dati, e quindi anche di cooperative di dati, deve essere tenuta sotto controllo (anche) in prospettiva concorrenziale a prescindere dalla forma soggettiva assunta dal soggetto erogante. Si tratta pur sempre di soggetti che, collazionando rilevanti quantità di dati, si propongono di assumere un ruolo non indifferente sul mercato digitale. Il fatto che tali soggetti siano rispettosi di quelle che rappresentano le idee di fondo del DGA, non può certo essere lasciato al caso, ma deve essere il frutto di un vaglio attento e puntuale. L'utilizzo etico dei dati da parte delle cooperative di dati, che caratterizza la fornitura di tali servizi, deve essere declinato anche in ottica proconcorrenziale in modo tale che la prospettiva di tutela non sia verticalizzata unicamente verso la persona umana, ma anche verso l'equilibrio ed il corretto funzionamento del mercato (digitale).

[68] Così, condivisibilmente, G. FINOCCHIARO, *Riflessioni su diritto e tecnica*, in *Dir. inf.*, 2012, 4-5, p. 838.

Capitolo XVIII

Il ruolo delle cooperative di dati per lo sviluppo delle *small and medium sized enterprises* tra mercato unico digitale e strategia europea dei dati

Angelo Francini

Abstract: The study aims to represent how the EU's legal regulation of the ongoing digital transformation can constitute an opportunity for growth for SMEs, the strengthening of which can contribute to the development of the digital single market. Taking the assumption from the European Data Strategy, the work focuses attention on the advantages, in terms of better access to data and the ability to develop new services based on them, which can derive for SMEs from participation in data cooperatives. data, a new collective entity which, due to the mutualistic spirit that characterizes it, can profoundly innovate the data market.

1. Osservazioni introduttive. *Platform economy* e *Big data*: la necessità di una regolamentazione giuridica europea.

La trasformazione digitale sta modificando radicalmente la vita quotidiana[1],

[1] Vastissima la dottrina in materia; *ex multis*: B. BERTARINI, *European Union Digital Single Market. Legal Framework and Challenges*, Milano, 2023; F.A. BELLA, *Tecnologie innovative nel settore salute tra scarsità delle risorse e differenziazione: alla ricerca di un equilibrio difficile*, in *Federalismi*, n. 2/2020; B. BERTARINI, *Il quadro giuridico per il mercato unico digitale*, in *Percorsi Costituzionali*, n. 1/2018; D. CROCCO-G. NEGRI, *La digitalizzazione della società moderna: incidenze e refluenze della tecnologia digitale sulle istituzioni pubbliche e il diritto nell'esperienza italiana*, Napoli,

coinvolgendo tanto le persone, nella loro sfera pubblica e in quella privata [2], singolarmente e come collettività, quanto le imprese, i mercati e la Pubblica Amministrazione [3]: «il mondo si va organizzando proprio attraverso 'assemblaggi di un'era digitale Globale» [4].

Quella che si può definire come Quarta Rivoluzione Industriale o Industria 4.0 [5] ha determinato, e sempre più determinerà, incisivi cambiamenti nell'economia, nella politica, nella cultura, negli ordinamenti giuridici e nella società nel suo complesso (c.d. *e-society*), grazie ad Internet [6] che svolge «il ruolo di infrastruttura por-

---

2016; P. DEGLI ESPOSTI, *Essere prosumer nella società digitale: produzione e consumo tra atomi e bit*, Milano, 2015; K. KELLY, *New Rules for the New Economy*, London, 1999; P.A. MERCIER-F. PLASSARD-V. SCARDIGLI, *La società digitale: le nuove tecnologie nella vita quotidiana*, Venezia, 1984.

[2] G. ALPA, *La "proprietà" dei dati personali*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, 2019, p. 11.

[3] E. DE MARCO, *Introduzione*, in E. DE MARCO (a cura di), *Accesso alla rete e uguaglianza digitale*, Milano, 2008, p. 2. L'A. nell'affermare come la digitalizzazione stia «erompendo» nella vita di tutti i giorni, afferma come questa stia incidendo su «aspetti della vita sociale, di interrelazioni individuali e di gruppo, di rapporti dei soggetti con le pubbliche autorità». In tema, si rinvia a O. POLLICINO-T.E. FROSINI-E. APA-M. BASSINI (a cura di), *Diritti e libertà in Internet*, Milano, 2017.

[4] S. RODOTÀ, *Una Costituzione per internet?*, in *Politica del diritto*, 3/2010, p. 345. In tema, anche R BALDWIN, *La grande convergenza. Tecnologia informatica, Web e nuova globalizzazione*, trad. it., Bologna, 2018, p. 11, che afferma come «Il modo con cui la rivoluzione delle tecnologie dell'informazione e della comunicazione (ICT) ha trasformato la globalizzazione e il suo impatto sul modo sono assai semplici da intuire, ma per spiegarli è necessario collocarli nella giusta prospettiva. Partiamo da qualche fatto. La globalizzazione compì un balzo in avanti negli anni '80 dell'Ottocento, quando la macchina a vapore e la pace globale ridussero i costi di trasporto dei beni. La globalizzazione fece poi un secondo grande balzo verso la fine del secolo scorso, quando le ICT ridussero radicalmente il costo del trasferimento delle idee... questi due avanzamenti – chiamiamoli rispettivamente "vecchia" e "nuova" globalizzazione ebbero effetti sostanzialmente differenti sulla geografia economica mondiale. Dall'inizio del IXI secolo, la caduta dei costi commerciali alimentò un ciclo di scambi commerciali, industrializzazione e crescita, che ha prodotto una dei più drammatici rovesciamenti di fortune: le antiche civiltà asiatiche e mediorientali, che da quattro millenni dominavano il modo, in meno di due secoli furono soppiantate dagli odierni Paesi ricchi. Questo esisto, che gli storici definiscono "grande divergenza" spiega come tanto potere economico, politico, culturale e militare venne e concentrarsi in poche mani. A partire dal 1990 la tendenza si invertì bruscamente; la posizione di supremazia economica dei Paesi ricchi, creatasi in un secolo di ascesa, si vanificò in due soli decenni. Oggi la loro quota è ritornata al livello del 1914. Questa tendenza, che potremmo definire "grande convergenza" è certamente il fatto economico dominante degli ultimi due o tre decenni. Essa è all'origine di gran parte dell'avversione per la globalizzazione nutrita da una parte della popolazione dei Paesi ricchi, e del carattere aggressivo assunto recentemente dalle realtà etichettabili come mercati emergenti».

[5] Il riferimento è, per tutti, a L. FLORIDI, *La rivoluzione dell'informazione. Come l'infosfera sta trasformando il mondo*, Milano, 2017.

[6] E. MAESTRI, *Lex informatica*, Napoli, 2015, p. 49. L' A. afferma «La rete internet è la manifestazione più eclatante di una tecnologia capace non solo di modificare la configurazione dei rapporti sociali ad ogni livello, dai rapporti tra individui ai rapporti tra potere pubblico e cittadino, ma anche di assumere dimensioni globali. Un mutamento così radicale da abbattere lo spazio ed il tempo e da ridurre la persona ad un flusso di dati», similmente anche M. CASTELLS, *La nascita della società in re-*

tante della nascente digital economy, di motore fondamentale della crescita di efficienza dei sistemi economici» [7].

L'integrazione tra la già ampia disponibilità di tecnologie digitali della Terza Rivoluzione Industriale (o Rivoluzione Digitale) e le innovazioni successive, quali l'IA, l'editing del genoma, la realtà virtuale e aumentata, la robotica, la blockchain, i quantum computing e la stampa 3D, favorisce la crescente diffusione di sistemi cyberfisici (*cyber-physical system* o CPS), con l'inserimento nei processi lavorativi affidati agli individui di macchine "intelligenti" e connesse ad Internet che possono arrivare a guidare la produzione e modificarne gli esiti, a seconda degli input esterni, e, se ben governate, ad innalzare il livello della qualità della vita [8]. Detta integrazione comporta necessariamente ingenti investimenti per l'introduzione delle nuove tecnologie e l'indispensabile ammodernamento ed adeguamento delle infrastrutture esistenti [9].

L'utilizzo dei servizi digitali, inizialmente a supporto di quelli tradizionali ma sempre più con finalità di effettiva sostituzione, sta facendo emergere nuove figure professionali, come gli sviluppatori di applicazioni, i produttori di dispositivi mobili, i cloud providers e i programmatori di hardware e software dotati di IA [10].

Nel processo di digitalizzazione, ricoprono un ruolo centrale le Piattaforme telematiche, perno di sviluppo della c.d. *Platform economy* [11], termine con cui si ri-

---

te, Milano, 2014, p. 22. In tema, si veda anche R. BALDWIN, *La grande convergenza. Tecnologia informatica, Web e nuova globalizzazione*, Bologna, 1999, ove l'A. afferma come «la capacità di inviare idee attraverso cavi, quasi senza costi, quasi ovunque, innescò una serie di riforme pratiche di lavoro e di management, come pure nelle relazioni tra imprese, fornitori e clienti. I metodi di lavoro e la progettazione dei prodotti si modificarono al fine di rendere al produzione più modulare e quindi più facile da coordinare a distanza... Là dove la rivoluzione del vapore impiegò decenni per trasformare la globalizzazione, la rivoluzione ICT impiegò anni».

[7] P. GARRONE-S. MARIOTTI (a cura di), *L'economia digitale*, Bologna, 2001, p. 23. Gli A., sempre a p. 23, non mancano, tra l'altro, di «esprimere anche preoccupazione: ad esempio che in relazione alla natura, ai contenuti e alle modalità di diffusione dei servizi distribuiti via internet possano manifestarsi nuove asimmetrie, e più in generale rischi di esclusione di larghe fasce di popolazione. E che non siano affatto improbabili, a causa dell'assenza di mediazioni istituzionali nell'uso della rete, rischi di violazione della privacy, di uso improprio dei dati personali, di diffusione di usi criminosi», tutte problematiche che si ripresentano ancor più in modo pressante con le nuove e più moderne tecnologie.

[8] A. SORO, *Uomini e macchine. Protezione dati per un'etica del digitale*, intervento al Convegno *Uomini e macchine. Protezione dati per un'etica del digitale* del 30 gennaio 2018 e disponibile al link web http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7598686.

[9] F. DI PORTO-E. SCOTTI, *La trasformazione digitale*, in E. BANI-F. DI PORTO-G. LUCHENA-E. SCOTTI, *Lezioni di Diritto dell'economia*, Torino, 2023, p. 276.

[10] G. DI FEDERICO, *Digitalizzazione dei servizi sanitari e Unione Europea: uno sguardo d'insieme sullo stato dell'arte e sulle sfide future*, in C. BOTTARI (a cura di), *La salute del futuro. Prospettive e nuove sfide del diritto sanitario*, Bologna, 2020, p. 28.

[11] In tema di *Platform economy*, si rinvia, *ex multis*, a: P. FALLETTA, *La trasparenza amministrativa in rete: le nuove piattaforme digitali per la diffusione di contenuti informativi*, in *Rivista trimestra-*

chiamano «*to all economic activity arising out of actual or intended commercial transactions in the internal market and facilitated directly or indirectly by online platforms, in particular online intermediation services and online search engines*» [12].

Infatti, «negli anni più recenti (la c.d. *Platform economy*) ha rappresentato, se-

---

le di diritto pubblico, n. 2/2021; M. MIDIRI, *Le piattaforme e il potere dei dati (Facebook non passa il Reno)*, in *Il Diritto dell'informazione e del l'informatica*, n. 2/2021; M.C. CAUSARANO, *Le piattaforme "online" e la tutela degli utenti digitali al tempo della pandemia*, in *Persona e Mercato*, n. 4/2020; X. CHEN-W. TIAN-X. ZHAO, *The Literature Review of Platform Economy, in Scientific Programming*, New York, 2020; F. KOEN-A. VAN WAES-P. PELZER-M. SMINK-R. VAN EST, *Safeguarding Public Interests in the Platform Economy*, in *Policy and Internet*; n. 3/2020; O. LUKIANENKO-A. NIAMESHCHUK, *Development of the Platform Economy in the Global Digital Environment*, in *International Economic Policy*, n. 32-33/2020; R. PETRUSO, *Osservazioni su contratti algoritmi e tutela del consumatore nell'economia di piattaforma*, in *Annuario di diritto comparato e di studi legislativi*, n. 1/2020; G. PETRUZZELLA, *Riflessioni sul mutamento del diritto della concorrenza nell'economia delle piattaforme e dei "Big Data"*, in *Annuario di diritto comparato e di studi legislativi*, n. 1/2020; S.K. SASIKUMAR-S. KANIKKA, *Digital Platform Economy: Overview, Emerging Trends and Policy*, in *Perspectives Productivity*, n. 3/2020; S. DIAMOND-N. DRURY-A. LIPP-A. MARSHALL-S. RAMAMURTHY, *The future of banking in the platform economy*, in *Strategy & Leadership*, n. 6/2019; M. DUFVA-R. KOIVISTO-L. ILMOLA-SHEPPARD-S. JUNNO, *Anticipating Alternative Futures for the Platform Economy*, in *Technology Innovation Management Review*, n. 9/2017; D. MCKEE, *The platform economy: natural, neutral, consensual and efficient?*, in *Transnational Legal Theory*, n. 4/2017; M. KENNEY-J. ZYSMAN, *The Rise of the Platform Economy*, in *Issues in Science and Technology*, n. 3/2016; M.E. BUCALO, *I servizi delle piattaforme "online" fra giurisprudenza sovranazionale e interna e necessità di regolazione dell'economia collaborativa. Riflessioni a partire dal caso Airbnb*, in *Federalismi*, n. 22/2020; E. GRAMANO, *Digitalisation and work: challenges from the Platform-economy*, in *Contemporary Social Science*, 4/2020; F. LAGIOIA-G. SARTOR, *Profilazione e decisione algoritmica: dal mercato alla sfera pubblica*, in *Federalismi*, n. 11/2020; I. PAIS, *La Platform Economy: aspetti metodologici e prospettive di ricerca*, in *Rivista internazionale di scienze sociali*, n. 1/2019; A. PALMIERI, *Profili giuridici delle piattaforme digitali: la tutela degli utenti commerciali e dei titolari di siti web aziendali*, Torino, 2019; C. SZYMANSKI, *Gli approcci alla "Platform Economy" nel diritto del lavoro americano*, in *Diritti lavori mercati*, n. 3/2019. Per la Scienza economica, si rinvia agli studi di «*two sided markets*» di J.C. ROCHET-J. TIROLE, *Platform competition in two-sided markets*, in *Journal of the European Economic Association*, 1/2003; e *Two-sided markets: a progress report*, in *RAND Journal of Economics*, n. 3/2006, pp. 645-667, in cui gli Autori specificano che «*we define a two-sided market as one in which the volume of transactions between end-users depends on the structure and not only on the overall level of the fees charged by the platform. A platform's usage or variable charges impact the two sides' willingness to trade once on the platform and, thereby, their net surpluses from potential interactions; the platforms' membership or fixed charges in turn condition the end-user's presence on the platform. The platforms' fine design of the structure of variable and fixed charges is relevant only if the two sides do not negotiate away the corresponding usage and membership externalities. Conceptually, the theory of twosided markets is related to the theories of network externalities and of (market or regulated) multi-product pricing. From the former, initiated by Katz and Shapiro (1985, 1986) and Farrell and Saloner (1985, 1986), it borrows the notion that there are noninternalized externalities among end-users. From the latter, it borrows the focus on price structure and the idea that price structures are less likely to be distorted by market power than price levels*».

[12] EUROPEAN COMMISSION, *Commission Decision On setting up the Group of Experts for the Observatory on the Online Platform Economy*, Brussels, 26 april 2018, C(2018) 2393 *final*.

condo un'espressione usata ormai nel linguaggio corrente, una "innovazione epocale". Il modello di business centrato sulla piattaforma si è diffuso in molte aree dell'economia. In più l'evoluzione tecnologica ha prodotto una differenziazione tra le varie tecnologie, dalle piattaforme di prima generazione come Google e Yahoo alla creazione di mercati online come eBay o Amazon fino alla più recente generazione che ha interessato l'economia dei servizi (da Uber a Lyft a Airbnb a Taskrabbit alle piattaforme di crowdfunding o sociale lending solo per fare qualche esempio…)» [13].

Appare, quindi, rilevante analizzare come il legislatore europeo stia dedicando sempre maggiore attenzione agli effetti economici e alle implicazioni sociali che discendono dalla digitalizzazione poiché «*reaping the benefits and addressing the challenges of the digital age requires narrowing the gap between technological developments and public policy*» [14].

Infatti, le tecnologie dell'informazione e della comunicazione (ICT) oltre a creare «opportunità di sviluppo per la trasformazione di interi settori produttivi sulla base di nuovi modelli di *business*» [15], a modificare l'agire della PA [16] e delle im-

---

[13] L. AMMANATI, *Verso un diritto delle piattaforme digitali?*, in *Federalismi*, n. 7/2019, p. 2.

[14] ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, *Going digital: shaping policy, improving lives*, 2019, Paris, p. 18.

[15] G. GAGGIANI, *Il quadro normativo del Mercato Unico Digitale*, in F. ROSSI DAL POZZO (a cura di), *Mercato Unico Digitale, dati personali e diritti fondamentali*, Milano, 2020, p. 13. In tema, si rimanda anche a N. VETTAS, *Competition and Regulation in Markets for goods and Services: A Survey with emphasis on Digital Markets*, in *Economics without Borders, Economic Research for European Policy Challenges*, 2021, p. 194.

[16] La dottrina giuridica in materia di eGovernment è assai ampia: tra tutti si vedano: F. LAUS, *Preparedness e once only nella digitalizzazione della PA: focus sul settore sanitario*, in *European Review of digital administration & Law*, n. 2/2021; L. SCIANNELLA, *"E-government" e accessibilità ai servizi: il "Single Digital Gateway"*, in *Ambientediritto.it*, n. 1/2021; G. SGUEO, *Tre idee di "design" per l'amministrazione digitale*, in *Giornale di diritto amministrativo*, n. 1/2021; G. SGUEO, *La democrazia digitale*, in *Giornale di diritto amministrativo*, n. 2/2021; P. CLARIZIA, *La digitalizzazione della pubblica amministrazione Commento a dec. legge 16 luglio 2020 n. 76 (Misure urgenti per la semplificazione e l'innovazione digitale)*, in *Giornale di diritto amministrativo*, n. 6/2020; D. FUSCHI, *Accesso telematico e utilizzo dei dati nell'"e-government"*, in *Diritto pubblico comparato ed europeo*, n. 4/2020; P. PIRAS, *Il tortuoso cammino verso un'amministrazione nativa digitale*, in *Il Diritto dell'informazione e dell'informatica*, n. 1/2020; F. FAINI, *Il volto dell'amministrazione digitale nel quadro della rinnovata fisionomia dei diritti in rete*, in *Il Diritto dell'informazione e dell'informatica*, n. 4-5/2019; R. TITOMANLIO, *L'amministrazione digitale: norme costituzionali e principi organizzativi*, in *GiustAmm.it: norme costituzionali e principi* organizzativi, in *GiustAmm.it*, n. 10/2019; B. CAROTTI, *Il correttivo al Codice dell'amministrazione digitale: una metariforma Commento a d.lg. 13 dicembre 2017, n. 217*, in *Giornale di diritto amministrativo*, n. 2/2018; P. COLITTI, *La digitalizzazione della Pubblica Amministrazione tra innovazioni tecniche, riforme legislative e piena realizzazione dell'archiviazione digitale*, in *Rivista Amministrativa della Repubblica Italiana*, n. 11-12/2018; E. DE GIOVANNI, *Il codice dell'Amministrazione digitale: genesi, evoluzione, principi costituzionali e linee generali*, in *Rassegna dell'avvocatura dello stato*, n. 3/2018; D.U. GALETTA, *La Pubblica Amministrazione nell'era delle ICT: sportello digitale unico e intelligenza artificiale al servizio della trasparenza*

prese e a costituire il fondamento dei sistemi economici innovativi moderni [17] «sono solite interagire con il diritto non solo offrendogli strumenti di intervento innovativi, ma altresì inducendolo a modificare le proprie regole per governare le realtà economiche, sociali e politiche a loro volta plasmate dal cambiamento tecnico scientifico» [18]. L'evoluzione tecnologica, dunque, coinvolge anche «gli istituti giuridici [che] subiscono, infatti, ai nostri giorni pressioni e trasformazioni di significativa entità, dovendosi adattare e riadattare continuamente a contesti tecnologici non facilmente riconducibili alle categorie di teoria generale conosciute» [19].

L'Unione Europea ha cercato, nel tempo, tanto di porsi «alla testa dell'economia digitale globale» [20], quanto di creare un *mercato unico digitale* [21] ove i Network e i servizi digitali possano prosperare, conscia che in assenza di ciò l'industria europea o «si digitalizzerà, o cesserà di esistere» [22], e già con il Regolamento (UE) 2019/1150 (*Platform to Business*) del Parlamento europeo e del Consiglio del 20

---

e dei cittadini?, in *Ciberspazio e Diritto*, n. 3/2018; F. ZHAO-J. WALLIS-M. SINGH, *E-government development and the digital economy: A reciprocal relationship*, in *Internet Research*, n. 3/2015; C. BAITINI, *Un'introduzione ai servizi di "eGovernment"*, in *Amministrare*, n. 1/2013; D. ARDUINI-F. BELOTTI-F.M. DENNI-M.G. GIUNGATO, *L'innovazione nelle Amministrazioni Pubbliche. Evidenza sulla diffusione dell'eGovernment in Italia*, in *Economia e politica industriale*, n. 2/2008. Sottolinea L. SCIANNELLA, *"E-government" e accessibilità ai servizi: il "Single Digital Gateway"*, in *Ambientediritto.it*, n. 1/2021, p. 459, che «un assunto che sembra particolarmente calzante per la spesa nel campo ICT e, in particolare, per quella destinata ai processi di digitalizzazione della Pubblica Amministrazione, suscettibile non solo di consentire allo Stato di migliorare l'efficienza della funzione di bilancio, ma anche, nel medio-lungo periodo, di trasformare l'architettura stessa della policy pubblica, nella direzione di rendere la stessa più accessibile e meno onerosa dal punto di vista finanziario. Difatti, la digitalizzazione sposta l'amministrazione verso una dimensione di piattaforma, su cui interagiscono cittadini e servizi pubblici, comportando una necessaria e parallela trasformazione degli attuali modelli organizzativi, cui si lega un radicale ripensamento della modalità di gestione dei flussi di dati».

[17] B. BERTARINI, *La regolazione giuridica della digitalizzazione quale strumento di crescita*, in S. DOMINELLI-G.L. GRECO (a cura di), *I mercati dei servizi fra regolazione e governance*, Torino, p. 97.

[18] M. MAGGIOLINO, *I big data e il diritto Antitrust*, Milano, 2018, p. 5.

[19] M.A. STEFANELLI, *La nuova Strategia europea per le PMI. Innovazioni giuridiche digitali: la Piattaforma europea "Fit for the future" e i "Digital Innovation Hub"*, in *Innovazione e Diritto*, 3/2020, p. 3.

[20] COMMISSIONE EUROPEA, *Strategia per il mercato unico digitale in Europa*, Brussels, 6 maggio 2015, COM (2015), 192 *final*, p. 3 (*Introduzione – perché abbiamo bisogno di un mercato unico digitale*).

[21] COMMISSIONE EUROPEA, *Strategia per il mercato unico digitale in Europa*, cit., p. 3. Ove si definisce un mercato unico digitale come «Il mercato unico digitale è un mercato in cui è garantita la libera circolazione delle merci, delle persone, dei servizi e dei capitali e in cui, quale che sia la loro cittadinanza o nazionalità o il luogo di residenza, persone e imprese non incontrano ostacoli all'accesso e all'esercizio delle attività online in condizioni di concorrenza leale e potendo contare su un livello elevato di protezione dei consumatori e dei dati personali». In dottrina, il rinvio, per tutti, è a M.A. STEFANELLI, *European SMEs and the Digital Single Market The Dynamics of New Regulation*, Milano, 2023.

[22] COMITATO ECONOMICO E SOCIALE EUROPEO, *Parere sulla Comunicazione della Commissione* "*Una nuova Strategia industriale per l'Europa"*, Brussels, 28 ottobre 2020, 2020/C 364/15, p. 2.

giugno 2019 (Regolamento P2B), ha inteso introdurre un insieme di norme, armonizzate a livello europeo, a tutela degli utenti commerciali e dei titolari di siti web aziendali che si servono dei fornitori di servizi di intermediazione online e dei motori di ricerca online per offrire beni e servizi ai consumatori.

Posto, infatti, che tali servizi di intermediazione «possono essere cruciali per il successo commerciale delle imprese che [li] utilizzano (…)per raggiungere i consumatori» [23], il Regolamento disciplina le relazioni tra le piattaforme online e gli altri soggetti dell'ecosistema digitale precisando che «Al fine di sfruttare pienamente i vantaggi dell'economia delle piattaforme *online* è importante che le imprese possano avere fiducia nei servizi di intermediazione online con cui instaurano rapporti commerciali, in primo luogo perché l'incremento delle intermediazioni delle transazioni attraverso i servizi di intermediazione online, alimentati da forti effetti indiretti di rete basati su dati, conduce a un aumento della dipendenza da tali servizi degli utenti commerciali, in particolare le microimprese, piccole e medie imprese (PMI) per raggiungere i consumatori» [24].

L'evoluzione tecnologica non consiste solo nei cambiamenti introducibili nei processi produttivi e nella vita quotidiana, fino alla costituzione del Metaverso, ovvero di un sistema di realtà virtuali interconnesse in maniera persistente, ma anche e soprattutto nella disponibilità di enormi quantità di dati, *Big Data* (o Mega Dati) [25], ribattezzati come dei veri e propri «giacimenti petroliferi del Terzo Millennio» e «definiti come grandi aggregazioni di dati digitali, ovvero frammenti elementari di informazioni, spesso di carattere personale, che non possono essere processati e analizzati con i tradizionali strumenti di analisi» [26] per la loro grandezza e numerosità e che sono elaborabili solo con mezzi adeguati, anch'essi frutto della stessa evoluzione, al punto che le tecnologie dell'informazione e della comunicazione sono diventate «il fondamento medesimo di tutti i sistemi economici innovativi moderni» [27].

---

[23] *Considerando* n. 2 del Regolamento europeo del 20 giugno 2019, n. 1150.

[24] *Considerando* n. 2 del Regolamento europeo del 20 giugno 2019, n. 1150.

[25] In tema di *Big Data* la dottrina giuridica è molto vasta; *ex multis* si rinvia a: R. DE LAURENTIIS, *Economia digitale*, Torino, 2021; M. SINISI, *Uso dei Big Data e principio di proporzionalità*, in *Federalismi*, n. 8/2020; C. CASONATO, *Potenzialità e sfide dell'intelligenza artificiale*, in *BioLaw Journal – Rivista di BioDiritto*, n. 1/2019; M. MAGGIOLINO, *I Big Data e il Diritto Antitrust*, cit.; F. MATASSOGLIO, *Big Data: impatto sui servizi finanziari e sulla tutela dei dati personali*, in M.T. PARACAMPO (a cura di), *FinTech: introduzione ai progili giuridici di un mercato univo tecnologico dei servizi finanziari*, Torino, 2017 e a F. DI PORTO, *Big Data e concorrenza*, in *Concorrenza e mercato*, n. 23/2016, C. PAPA, *Antropologia dell'impresa*, Milano, 1999.

[26] B. RABAI, *I "Big Data" nell'ecosistema digitale: tra libertà economiche e tutela dei diritti fondamentali*, in *Amministrare*, n. 3/2017, p. 407.

[27] COMMISSIONE EUROPEA, *Strategia per il mercato unico digitale in Europa*, cit., p. 3. Si richiama anche COMMISSIONE EUROPEA, *Verso una florida economia basata sui dati*, Brussels, 2 luglio 2014, COM (2014) 442 *final*, p. 5, Ove ci si riferisce ai Big Data come «a grandi quantità di dati di tipo diverso prodotti a grande velocità da numerosi tipi di fonti. La gestione di questi dataset ad elevata va-

Si rendono, perciò, necessari specifici interventi in quanto «è dato empirico di immediata percezione come lo sviluppo esponenziale della tecnologia digitale imprima un dirompente cambiamento nel modo d'essere delle relazioni sociali ed economiche. Nell'universo digitale si delineano oggi, e domani ancor di più, i lineamenti essenziali dell'identità individuale e si raccolgono e conservano dati personali di ogni sorta; lineamenti e dati della persona sono divenuti, in pari tempo, asset fondamentali delle attività economiche e commerciali che si svolgono sul mercato digitale e non» [28].

2. La Comunicazione della Commissione europea del 19 febbraio 2020, *Una strategia europea per i dati*: perno delle iniziative per la digitalizzazione dell'UE.

Lo sviluppo del mercato digitale, come detto, ormai al centro della vita quotidiana di imprese e persone in conseguenza anche dell'accelerazione impressa dalla pandemia, ha indotto il legislatore europeo a proporre norme regolatrici.

La Commissione Europea ha emanato il 15 dicembre 2020 un *Digital Package*, sviluppato nel *Digital Market Act* (DMA *Proposal*) [29] e nel *Digital Service Act* (DSA Proposal) [30], che «*would include one pillar aiming at deepening the internal market and clarifying the responsibilities of digital services*» [31]. Le suddette propo-

riabilità e in tempo reale impone il ricorso a nuovi strumenti e metodi, quali ad esempio potenti processori, software e algoritmi»; si richiama, altresì, COMMISSIONE EUROPEA, *Verso uno spazio comune europeo dei dati*, Brussels, 5 aprile 2018, COM (2018) 232 *final* afferma come «l'innovazione guidata dai dati è un motore essenziale per la crescita e l'occupazione, in grado di accrescere la competitività europea sul mercato globale». Secondo l'International Data Corporation il mercato delle tecnologie e dei servizi Big Data è cresciuto del 22,6% dal 2015 al 2020, raggiungendo i 58,9 miliardi di dollari. Il tasso di crescita ha seguito un ritmo pari a 6 volte quello dell'intero mercato delle ICT (INTERNATIONAL DATA CORPORATION, *Worldwide Big Data Technology and Services Forecast, 2016-2020*, 2024). Il valore economico dei dati, anche di quelli personali, incide anche sulla tutela della concorrenza in quanto la quantità di dati posseduta e le diverse possibilità di accesso a questi non solo possono determinare la qualità dei servizi offerti dagli operatori economici ma anche favorire la costituzione di posizioni dominanti sul mercato e precludere lo sviluppo di imprese concorrenti per l'impossibilità, o, comunque, la difficoltà, di accesso ai dati.

[28] G. MARINO, *La "successione digitale*", in *Osservatorio del diritto civile e commerciale*, n. 1/2018, p. 167.

[29] COMMISSIONE EUROPEA, *Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo a mercati equi e contendibili nel settore digitale (legge sui mercati digitali)*, Brussels, 15 dicembre 2020, COM (2020) 842 *final*.

[30] COMMISSIONE EUROPEA, *Proposta di Regolamento del Parlamento Europeo e del Consiglio relativo a mercati equi e contendibili nel settore digitale (legge sui mercati digitali)*, cit.

[31] S.B. MICOVA-A. DE STREEL, *Digital Services Act. Deepening the internal market and clarifying responsabilities for digital services*, Report CERRE – Centre on Regulation Europe, December 2020, p. 7.

ste, fondate sull'art. 114 del TFUE, «appaiono in realtà riduttive rispetto ai progetti inizialmente diffusi. Secondo l'idea originaria, infatti la Commissione mirava ad articolare una proposta normativa strutturata in tre pilastri. Il primo concerneva la regolamentazione dei servizi digitali (il *Digital Service Act*, DSA); il secondo conteneva una disciplina dei mercati di gitali (il *Digital Market Act*, DMA); il terzo (il c.d. *New Competition Tool*) avrebbe consentito di munire le autorità antitrust di uno strumento di azione rapida, maggiormente rispondente alle caratteristiche dei mercati digitali» [32].

Successivamente, la proposta relativa al c.d. *New Competiton Toll* è venuta meno [33], cosicché il *Digital Package* è risultato composto solamente dalle prime due proposte; con esse la Commissione europea ha inteso «stabilire un apparato normativo unico in tutta la UE che renda il digitale uno spazio più aperto e sicuro nel rispetto dei valori e dei princìpi fondamentali dell'Unione» [34]: le proposte «mirano, da un lato, ad aumentare l'innovazione e la competitività europea e, dall'altro, a rendere la rete più equa e aperta e porre un argine allo strapotere di quei pochi colossi privati che la dominano (le c.d. *Big Tech*); tutto ciò mediante una protezione effettiva dei diritti degli utenti nonché delle imprese e piattaforme di piccole e medie dimensioni. Così facendo si colma una vistosa lacuna del sistema giuridico europeo, il cui quadro normativo in tema di servizi e mercati digitali è tuttora dettato da un atto, la direttiva 2000/31/CE sul commercio elettronico ormai del tutto inadeguato, malgrado i numerosi interventi chiarificatori della Corte di Giustizia in sede interpretativa, a regolare un settore che si è sviluppato e modificato in modo dirompente nell'ultimo ventennio» [35].

Le proposte trovano il loro fondamento nella Comunicazione della Commissione del 19 febbraio 2020, *Una strategia europea dei dati* [36], che delinea le misure politiche ed indica gli investimenti necessari affinché l'Europa possa effettivamente svolgere un ruolo strategico e di guida nell'economia dei dati ed hanno, poi, portato all'emanazione del Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio, del 14 settembre 2022, relativo a mercati equi e contendibili nel settore digita-

---

[32] G. CONTALDI, *il DMA (Digital Market Act) tra tutela della concorrenza e protezione dei dati personali*, in *Ordine internazionale e diritti umani*, n. 2/2021, p. 292.

[33] G. CONTALDI, *il DMA (Digital Market Act) tra tutela della concorrenza e protezione dei dati personali*, cit., p. 293. L'A. specifica che «Non sono noti i motivi per i quali la Commissione ha ritenuto superflua l'introduzione di un nuovo meccanismo di enforcement della normativa antitrust. Si può, pertanto, solo ipotizzare che la scelta sia stata determinata dal peculiare rapporto intercorrente tra la nuova proposta normativa e la disciplina esistente nel Trattato».

[34] N. ZORZI GIUSTINIANI, *Governing the ungoverned. Recenti proposte europee e internazionali per regolare il digitale*, in *Nomos*, n. 3/2020, p. 1.

[35] N. ZORZI GIUSTINIANI, *Governing the ungoverned. Recenti proposte europee e internazionali per regolare il digitale*, cit., p. 1.

[36] COMMISSIONE EUROPEA, *Una strategia europea per i dati*, Brussels, 19 febbraio 2020, COM (2020) 66 *final*.

le (DMA)[37], e del Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali (DSA)[38].

Con l'adozione della Strategia europea dei dati, la Commissione, sottolineata l'importanza imprescindibile dei dati quali «linfa vitale dello sviluppo economico, base di molti nuovi prodotti e servizi»[39] e fonte di «guadagni in termini di produttività ed efficienza delle risorse in tutti i settori economici»[40], evidenzia come, attraverso la gestione dei dati, il cui volume è in rapida crescita a livello mondiale, dai 33 zettabyte del 2018 ai 175 zettabyte previsti nel 2025[41], l'Unione Europea possa «divenire un modello di riferimento per una società che, grazie ai dati, dispone di strumenti per adottare decisioni migliori, a livello sia di imprese sia di settore pubblico» in quanto «L'Europa digitale dovrebbe riflettere le migliori qualità europee ed essere aperta, equa, diversificata, democratica e sicura»[42].

L'innovazione guidata dai dati può comportare grandi benefici per i cittadini, in tutti gli ambiti, dalla medicina[43], alla tutela dell'ambiente, grazie ad un consumo energetico più consapevole, alle nuove soluzioni di mobilità e alla tracciabilità dei prodotti, dei materiali e degli alimenti.

La Strategia sollecita a tenere conto prioritariamente delle diverse tipologie di dati, prevedendo modalità di trattamento differenziate per quelli personali dei cittadini, i quali «daranno fiducia alle innovazioni basate sui dati e le faranno proprie solo se saranno convinti che la condivisione dei dati personali nell'UE sarà soggetta in ogni caso alla piena conformità alle rigide norme dell'Unione in materia di protezione dei dati»[44], e per i dati industriali non personali e dati pubblici.

In merito ai dati personali, l'Unione ha già definito il presupposto per la fiducia digitale dei cittadini con il Regolamento generale sulla protezione dei dati (GDPR)[45]

---

[37] Per tutti, il riferimento è a P. MANZINI, *Il Digital Market Act decodificato*, in P. MANZINI-M. VELLANO (a cura di), *Unione Europea 2020 – I dodici mesi che hanno segnato l'integrazione europea*, Milano, 2021.

[38] G. CAGGIANO, *La proposta di Digital Services Act per la regolazione dei servizi e delle piattaforme online nel diritto dell'Unione europea*, in *I Post di AISDUE*, 2021; G.M. RUOTOLO, *Le proposte di disciplina di digital services e digital markets della Commissione del 15 dicembre 2020*, in *DPCE on line*, n. 4/2020.

[39] COMMISSIONE EUROPEA, *Una strategia europea per i dati*, cit., p. 3.

[40] COMMISSIONE EUROPEA, *Una strategia europea per i dati*, cit., p. 3.

[41] COMMISSIONE EUROPEA, *Una strategia europea per i dati*, cit., p. 2 che riprende lo studio di INTERNATIONAL DATA CORPORATION, *DataAge 2025 – The Digitization of the world*, 2018.

[42] COMMISSIONE EUROPEA, *Una strategia europea per i dati*, cit., p. 1.

[43] Il riferimento, per tutti, è a C. BOTTARI (a cura di), *La salute del futuro. Prospettive e nuove sfide del diritto sanitario*, Bologna, 2020; C. BOTTARI, *Profili innovativi del sistema sanitario*, Torino, 2018 e a C. BOTTARI-G. DE VERGOTTINI, (a cura di), *La sanità elettronica*, Bologna, 2018.

[44] COMMISSIONE EUROPEA, *Una strategia europea per i dati*, cit., p. 1.

[45] Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla*

mentre per i dati non personali, che «dovrebbero essere disponibili a tutti, siano essi soggetti pubblici o privati, piccoli o grandi, *start-up* o colossi» [46], ha adottato diverse disposizioni volte a dare stimolo all'incremento dell'economia dei dati [47] allo scopo di creare un contesto politico attraente, cosicché entro il 2030 la quota UE dell'economia dei dati (dati conservati, elaborati e utilizzati proficuamente in Europa) corrisponda almeno al suo peso economico e permetta all'Europa di «mantenersi tra i leader mondiali dell'economia digitale, sostenendo la crescita delle imprese europee su scala mondiale» [48].

La Strategia rimarca la grande «opportunità offerta dai dati per il bene sociale ed economico, poiché i dati, a differenza della maggior parte delle risorse economiche, possono essere copiati pressoché a costo zero e il loro utilizzo da parte di una persona o di un'organizzazione non ne impedisce l'utilizzo simultaneo da parte di un'altra persona o organizzazione» [49].

Nel delineare la situazione esistente, la Commissione sottolinea come sia necessario che l'Europa affronti «in maniera concertata questioni che vanno dalla connettività all'elaborazione e alla conservazione dei dati, dalla potenza di calcolo alla cibersicurezza» anche per «migliorare le proprie strutture di governance per la gestione dei dati e ampliare i propri pool di dati di qualità disponibili per l'utilizzo e il riutilizzo» [50] con l'obiettivo anche di eliminare «in tempi rapidi delle differenze fondamentali che separano il mondo online dal mondo *offline* al fine di abbattere le barriere che bloccano l'attività online attraverso le frontiere» [51].

Pur in presenza del ristretto gruppo di grandi imprese tecnologiche (Big Tech) detentrici di buona parte dei dati disponibili a livello mondiale, la Strategia delinea un quadro favorevole allo sviluppo delle aziende europee basate sui dati in quanto «Una gran parte dei dati del futuro proverrà da applicazioni industriali e professionali, ambiti di interesse pubblico o applicazioni dell'Internet delle cose di uso quotidiano» ovvero da «settori in cui l'UE è particolarmente competitiva» [52].

---

libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). In tema, il rinvio è, per tutti, a F. BRAVO (a cura di), *Dati personali. Protezione, libera circolazione e governance. – Vol. 1. Principi*, Pisa, 2023.

[46] COMMISSIONE EUROPEA, *Una strategia europea per i dati*, cit., p. 1.

[47] Tra queste, si citano: il Regolamento sulla libera circolazione dei dati non personali, Regolamento (UE) 2018/1807, il Regolamento sulla cibersicurezza, Regolamento (UE) 2019/881, e la Direttiva sull'apertura dei dati, Direttiva (UE) 2019/1024. In tema di Economia digitale, si rimanda, tra gli alti a R. DE LAURENTIIS, *Economia digitale*, cit.

[48] COMMISSIONE EUROPEA, *Strategia per il mercato unico digitale in Europa*, cit., p. 3.

[49] COMMISSIONE EUROPEA, *Una strategia europea per i dati*, cit., p. 5.

[50] COMMISSIONE EUROPEA, *Una strategia europea per i dati*, cit., p. 1.

[51] COMMISSIONE EUROPEA, *Sulla revisione intermedia della Strategia per il mercato unico digitale. Un mercato unico digitale connesso per tutti*, Brussels, 10 maggio 2017, COM (2017), 228 *final*, p. 3 (*Introduzione*).

[52] COMMISSIONE EUROPEA, *Una strategia europea per i dati*, cit., p. 3.

L'obiettivo europeo, come detto, dovrebbe essere quello di «creare uno spazio unico europeo di dati – un autentico mercato unico di dati, aperto ai dati provenienti da tutto il mondo – nel quale sia i dati personali sia quelli non personali, compresi i dati commerciali sensibili, siano sicuri e le imprese abbiano facilmente accesso a una quantità pressoché infinita di dati industriali di elevata qualità, che stimolino la crescita e creino valore» [53].

La politica pubblica risulta strategica al fine di incentivare la domanda di prodotti basati sui dati secondo una duplice linea d'azione.

Direttamente, sia potenziando la capacità del settore pubblico di utilizzare i dati nei processi decisionali e nei servizi pubblici sia rendendo accessibili le informazioni da questo detenute, secondo l'impostazione ormai consolidata dell'UE [54] che mira ad aumentare sempre più la quota di dati prodotti dalle Pubbliche Amministrazioni di cui deve essere garantita l'accessibilità, come attestano la direttiva sull'apertura dei dati [55], di recente sottoposta a revisione, e altre normative settoriali, tutte basate sull'assunto che trattandosi di dati prodotti con denaro pubblico, dovrebbero essere utilizzati a beneficio della società.

Indirettamente, innovando ed adeguando le disposizioni e le politiche di settore affinché valorizzino le opportunità offerte dai dati e non costituiscano ostacolo o disincentivo al loro uso.

Lo spazio unico europeo dei dati dovrebbe favorire il superamento delle criticità che ancora permangono ed ostacolano l'effettiva diffusione della condivisione dei dati tra imprese.

Il potenziale economico di tale condivisione, infatti, è condizionato da timori derivanti dalla diffidenza reciproca tra gli operatori economici per un utilizzo dei dati non conforme agli accordi contrattuali, dal rischio di perdere un vantaggio concorrenziale, dalla mancanza di chiarezza giuridica e dal timore dell'appropriazione indebita dei dati da parte di terzi e dette criticità sono avvertite in particolare dalle PMI che, per le loro stesse dimensioni, molto spesso non riescono a far fronte alla disomogenea disponibilità di dati che, talvolta, continua a caratterizzare zone diverse dell'UE, e si trovano in posizione subalterna rispetto alle grandi piattaforme online, in cui un numero esiguo di operatori può accumulare grandi quantità di dati, traendo informazioni importanti e vantaggi competitivi dalla ricchezza e dalla varietà dei dati in proprio possesso ed incidendo sulla contendibilità dei mercati: di quello dei servizi di piattaforma ma anche dei vari mercati specifici dei beni e dei servizi offerti dalla piattaforma, in particolare se quest'ultima è essa stessa attiva su tali mercati collegati, imponendo unilateralmente condizioni per l'accesso ai dati e il loro utilizzo.

---

[53] COMMISSIONE EUROPEA, *Una strategia europea per i dati*, cit., p. 5.

[54] A partire dall'adozione della Direttiva 2003/98/CE relativa al riutilizzo dell'informazione del settore pubblico.

[55] Direttiva (UE) 2019/1024, che abroga la direttiva 2003/98/CE rivista dalla direttiva 2013/37/UE.

La realizzazione di una strategia europea dei dati che garantisca una regolazione giuridica efficace è, dunque, una necessità e la Commissione ha individuato in quattro Pilastri i punti più significativi per giungere all'obiettivo, e cioè «Un quadro di governance intersettoriale per l'accesso ai dati e il loro utilizzo», «Abilitatori: investimenti nei dati e rafforzamento delle infrastrutture e delle capacità europee per l'hosting, l'elaborazione e l'utilizzo dei dati, l'interoperabilità», «Competenze: fornire strumenti alle persone, investire nelle competenze e nelle PMI» e «Spazi comuni europei di dati in settori strategici e ambiti di interesse pubblico».

Il terzo Pilastro, in particolare, riprende l'attenzione specifica da tempo riservata dall'Europa alle *Small and Medium sized Enterprises*, ancora oggi mancanti di un contesto omogeneo di natura normativa [56], e mira a definire misure specifiche per sviluppare le capacità delle PMI [57] e delle start-up, fornendo «consulenza giuridica e normativa per sfruttare appieno le numerose opportunità derivanti dai modelli di business basati sui dati» [58]. Attraverso i programmi Orizzonte Europa e Europa digitale ed i Fondi strutturali e d'investimento, verranno offerte alle «PMI dell'economia dei dati opportunità di un migliore accesso ai dati e di sviluppo di nuovi servizi e applicazioni basati sui dati» [59] proprio in ragione del fatto che queste imprese sono «Esposte ad una concorrenza profondamente trasformata dal processo di digitalizzazione dell'economia, [e] hanno comunque un ruolo fondamentale da svolgere nell'ambito della duplice transizione digitale ed ecologica dell'UE al fine di raccogliere le sfide che ci attendono» [60].

---

[56] M.A. STEFANELLI, *Small and Medium sized Enterprises e mercato unico digitale nella regolamentazione giuridica europea*, in *Percorsi Costituzionali*, n. 1/2018, p. 230. Ci si riferisce allo *Small Business Act per l'Europa* (Comunicazione della Commissione europea "*Una corsia preferenziale per la piccola impresa*". *Alla ricerca di un nuovo quadro fondamentale per la piccola impresa – Small Business Act per l'Europa*), al posteriore *Riesame dello Small Business Act per l'Europa* (COM (2011) 78 *final*); alla *Carta europea per le PMI* (Consiglio di Feira, 19-20 giugno 2000), e alla *Relazione annuale di attuazione della Carta europea per le piccole imprese* del 7 marzo 2011, COM (2011) 122 *final*.

[57] Ai sensi dell'art. 2 dell'Allegato alla Raccomandazione della Commissione del 6 maggio 2003 relativa alla *Definizione delle microimprese, piccole e medie imprese*, sono microimprese quelle imprese che occupano meno di 10 persone e realizzano un fatturato annuo o una totale di bilancio annuo non superiori a 2 milioni di euro; sono piccole imprese quelle imprese che occupano meno di 50 persone e realizzano un fatturato annuo o una totale di bilancio annuo non superiori a 10 milioni di euro; sono medie imprese quelle imprese che occupano meno di 250 persone e realizzano un fatturato annuo che non supera i 50 milioni di euro oppure il cui totale di bilancio annuo non supera i 43 milioni di euro.

[58] COMMISSIONE EUROPEA, *Una strategia europea per i dati*, cit., p. 24.

[59] COMMISSIONE EUROPEA, *Una strategia europea per i dati*, cit., p. 24.

[60] COMITATO ECONOMICO E SOCIALE EUROPEO, Parere "*L'IA nelle micro, piccole e medie imprese (MPMI)*", Brussels, 10 gennaio 2022, INT/945, p. 1, (Punto 1.2). In tema di transizione ecologica, il rimando è a B. BERTARINI, *Il finanziamento pubblico e privato dell'European Green Deal*, in *AmbienteDiritto*, 1/2022.

3. *Data Governance Act* e l'opportunità delle cooperative di dati per le PMI.

Seguendo un approccio condiviso a livello europeo, «andrebbero, quindi, considerate con attenzione le competenze digitali di cui dovrebbero disporre i cittadini e le imprese (in particolare le PMI) per interagire con il nuovo quadro proposto in materia di digitalizzazione» [61].

La diffusione di competenze digitali, infatti, potrebbe favorire meccanismi concorrenziali sui mercati digitali e circoscrivere la capacità di controllo del flusso di dati generato sugli stessi, attualmente esercitata da un ristretto numero di aziende globali tanto ampiamente da rendere trasversale a tutti i sistemi giuridici la riflessione sulla necessità di una regolamentazione del mercato digitale che miri a garantire la concorrenza, senza soffocare l'innovazione e il benessere generale dei consumatori [62].

Perseguendo gli obiettivi della Strategia europea dei dati, il legislatore europeo si è proposto di integrare la logica prevalentemente protezionistica, che caratterizza le disposizioni già assunte per regolamentare il trattamento dei dati personali, con un'impostazione di maggiore valorizzazione dei dati, personali e non [63].

Rilevante in tal senso è l'iniziativa dedicata alla *European Data Governance*, disciplinata nel *Data Governance Act* (DGA), il Reg. UE n. 868/2022, che riconosce come, per «cogliere le opportunità offerte dall'era digitale attuale, un prerequisito fondamentale è regolamentare l'accesso ai dati e il loro utilizzo (…) rafforza[ndo] l'accesso all'utilizzo dei dati da parte dei consumatori e delle imprese e [garantendo], ove necessario, l'accessibilità dei dati per le istituzioni pubbliche». L'Unione, si prefigge quindi «di liberare il valore dei dati generati da oggetti connessi in Europa eliminando gli ostacoli all'accesso ai dati stessi, sia per gli enti pubblici che per quelli privati» [64], «garantire l'equità nell'ambiente digitale consentendo ai consumatori e alle imprese di avere un maggiore controllo sui loro dati, precisando chi può avervi accesso e a quali condizioni; promuovere un mercato dei dati competitivo "liberando una grande e preziosa quantità di dati industriali"; aprire opportunità di innovazione basata sui dati; e rendere i dati mag-

---

[61] Comitato Economico e Sociale Europeo, Parere *sulla digitalizzazione nel coordinamento della sicurezza sociale: facilitare la libera circolazione nel mercato unico*, Brussels, 23 aprile 2024, C/2024/2486, p. 4, Punto 3.5.

[62] M. Dietrich-T. Vinje, *The European Commission's proposal for a Digital Markets Act, In search of a "golden standard" for appropriate ex ante regulation of large digital players*, in *Computer Law Review International*, n. 2/2021, p. 33.

[63] F. Bravo, *Le cooperative di dati*, in *Contratto e impresa*, 2023, 3, p. 757 ss., testo disponibile al link https://site.unibo.it/cooperative-di-dati/it (ivi, p. 1).

[64] Comitato Economico e Sociale Europeo, Parere *riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (normativa sui dati)* [COM (2022) 68 final – 2022/0047 (COD)] (2022/C 365/04), Brussels, 23 settembre 2022, p. 2, Punto 2.1.

giormente accessibili a tutti»[65]. Il DGA specifica «quali soggetti possono ricavare valore dai dati e a quali condizioni, oltre a garantire un'equa ripartizione del valore dei dati tra gli operatori dell'economia dei dati e nei loro contratti, nel rispetto dei legittimi interessi delle imprese e dei singoli cittadini che investono in prodotti e servizi basati sui dati. Infine, le nuove norme proposte conferiscono ai consumatori e alle imprese la possibilità di avere voce in capitolo su come possono essere impiegati i dati generati dai loro prodotti connessi»[66].

Precipua attenzione è riservata alle PMI in quanto «Attualmente, molte PMI non hanno accesso ai dati che contribuiscono a generare quando utilizzano apparecchiature dell'Internet degli oggetti, che possiedono o hanno in locazione o in *leasing*, o i servizi correlati. Inoltre, le PMI e le startup innovative non riescono a creare valore aggiunto sotto forma di nuovi prodotti e servizi complementari per gli utenti di apparecchiature dell'Internet degli oggetti poiché non hanno la possibilità di entrare in possesso dei dati generati da tali dispositivi. Ciò indebolisce le prestazioni del mercato unico digitale»[67]. Scopo «della proposta è invertire le recenti tendenze del mercato che hanno portato al consolidamento dell'*economia di Internet* e generato monopoli dei dati in diversi settori, ad es. l'assistenza sanitaria e l'industria automobilistica. Questo continuo incremento dei dati necessita di attenzione e impone di regolamentare la portata delle condizioni abusive di utilizzo dei dati»[68].

Per superare detta situazione, «L'economia dei dati deve essere creata in modo da consentire alle imprese, in particolare alle microimprese e alle piccole e medie imprese (PMI) (…) e alle *start-up*, di prosperare, garantendo neutralità dell'accesso ai dati e portabilità e interoperabilità dei dati, ed evitando effetti di dipendenza (*lock-in*)»[69] e i dati debbano essere, quindi, «reperibili, accessibili, interoperabili e riutilizzabili (principi FAIR per i dati), garantendo nel contempo un elevato livello di cibersicurezza. Laddove esista parità di condizioni nell'economia dei dati, le imprese competono sulla qualità dei servizi e non sulla quantità dei dati che controllano»[70] e, grazie ad una solida *governance* siano rispettate le necessarie «condizioni per il riutilizzo dei dati protetti da applicarsi agli enti pubblici che, a norma del diritto nazionale, sono designati come competenti per consentire o negare l'accesso

---

[65] COMITATO ECONOMICO E SOCIALE EUROPEO, Parere *riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (normativa sui dati)*, cit., p. 2, Punto 2.3.

[66] COMITATO ECONOMICO E SOCIALE EUROPEO, Parere *riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (normativa sui dati)*, cit., p. 2, Punto 3.1.

[67] COMITATO ECONOMICO E SOCIALE EUROPEO, Parere *riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (normativa sui dati)*, cit., p. 2, Punto 3.2.

[68] COMITATO ECONOMICO E SOCIALE EUROPEO, Parere *riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (normativa sui dati)*, cit., p. 2, Punto 2.3.

[69] *Considerando* n. 2 del Regolamento (UE) 2022/868 del Parlamento e del Consiglio, del 30 maggio 2022 *relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (Regolamento sulla governance dei dati)*.

[70] *Ibidem*.

per il riutilizzo, e dovrebbe lasciare impregiudicati i diritti e gli obblighi relativi all'accesso a tali dati. Tali condizioni dovrebbero essere non discriminatorie, trasparenti, proporzionate e oggettivamente giustificate e allo stesso tempo non dovrebbero limitare la concorrenza, con un'attenzione specifica alla promozione dell'accesso a tali dati da parte delle PMI e delle *start-up*» [71].

Quanto riportato, nell'ottica della valorizzazione dell'impresa di dimensioni minori, vera «spina dorsale dell'economia dell'UE», [72] rappresenta «la sfida del futuro su cui si celebrerà la grandezza o si certificherà il fallimento dell'Unione nel campo dell'economia digitale, non essendo più possibile ignorare l'incredibile capacità di sviluppo che i dati, anche personali, possono generare» [73].

Il DGA, infatti, prendendo l'avvio dal Regolamento UE 2016/679 (GDPR), che disciplina la tutela dei dati personali ma anche le condizioni e i limiti per la loro circolazione, detta una serie di regole che mirano a favorire la condivisione dei dati, personali e non, pur nel rispetto delle esigenze di protezione che le singole tipologie richiedono, secondo più direttrici, tra cui: il riutilizzo dei dati prodotti dalla PA, la destinazione dei dati per finalità altruistiche e i servizi di intermediazione per lo scambio dei dati.

Dopo aver delineato, nel Capo II, una serie di norme che disciplinano il riutilizzo di determinati dati in possesso della PA, richiamandosi alla Direttiva Open Data, il DGA dedica il Capo III ad un nuovo modello di impiego dei dati, inserendo il servizio di intermediazione tra la fornitura e l'utilizzo.

Prevedendo come «i servizi di intermediazione dei dati svolgano un ruolo essenziale nell'economia dei dati, in particolare nel sostenere e promuovere pratiche volontarie di condivisione dei dati tra imprese o nell'agevolare la condivisione dei dati nell'ambito degli obblighi stabiliti dal diritto dell'Unione o nazionale. Essi potrebbero diventare strumenti che agevolano lo scambio di quantità considerevoli di dati pertinenti. I fornitori di servizi di intermediazione dei dati, che possono includere anche enti pubblici, che offrono servizi che collegano i diversi soggetti dispongono del potenziale per contribuire alla messa in comune efficiente dei dati come pure all'agevolazione della condivisione bilaterale dei dati. I servizi di interme-

---

[71] *Considerando* n. 15 del Regolamento (UE) 2022/868 del Parlamento e del Consiglio, del 30 maggio 2022 *relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (Regolamento sulla governance dei dati)*.

[72] COMMISSIONE EUROPEA, *Una strategia per le PMI per un'Europa sostenibile e digitale,* Brussels, 10 marzo 2020, COM (2020) 103 *final*, p. 1 (*Introduzione*). Ove si afferma come «L'Europa può contare su 25 milioni di piccole e medie imprese (PMI) (…): danno lavoro a circa 100 milioni di persone, generano più della metà del PIL dell'Europa e svolgono un ruolo chiave garantendo un valore aggiunto in tutti i settori dell'economia» e ancora «forniscono i due terzi dei posti di lavoro, offrono opportunità di formazione in vari settori e regioni, anche per lavoratori poco qualificati, e sostengono il benessere della società, non da ultimo nelle zone remote e rurali».

[73] L. PETRONE, *Il mercato digitale europeo e le cooperative di dati*, in *Contratto e impresa*, 2023, 3, pp. 800 ss., testo disponibile al link https://site.unibo.it/cooperative-di-dati/it (ivi, p. 7).

diazione dei dati specializzati, che sono indipendenti dagli interessati, dai titolari dei dati e dagli utenti dei dati, potrebbero facilitare l'emergere di nuovi ecosistemi basati sui dati indipendenti da qualsiasi operatore che detenga un grado significativo di potere di mercato, prevedendo nel contempo un accesso non discriminatorio all'economia dei dati per le imprese di tutte le dimensioni, in particolare le PMI e le start-up con mezzi finanziari, giuridici o amministrativi limitati. Ciò sarà particolarmente importante nel contesto della creazione di spazi comuni europei di dati, ossia quadri interoperabili specifici o settoriali o intersettoriali di norme e prassi comuni per condividere o trattare congiuntamente i dati, anche ai fini dello sviluppo di nuovi prodotti e servizi, della ricerca scientifica o di iniziative della società civile. I servizi di intermediazione dei dati potrebbero includere la condivisione bilaterale o multilaterale dei dati o la creazione di piattaforme o banche dati che consentano la condivisione o l'utilizzo congiunto dei dati, nonché l'istituzione di un'infrastruttura specifica per l'interconnessione di interessati e titolari dei dati con gli utenti dei dati» [74].

All'art. 2, n. 11, il DGA fornisce la relativa definizione del «servizio che mira a instaurare, attraverso strumenti tecnici, giuridici o di altro tipo, rapporti commerciali a fini di condivisione dei dati tra un numero indeterminato di interessati e di titolari di dati, da un lato, e gli utenti dei dati dall'altro, anche al fine dell'esercizio dei diritti degli interessati in relazione ai dati personali».

Secondo la terminologia del GDPR, dunque, il servizio ha la finalità di far instaurare relazioni commerciali tra gli interessati, ossia le persone fisiche cui si riferiscono i dati, e i titolari, ovvero le persone giuridiche, incluse le PA, o fisiche (diverse dagli interessati) che hanno il diritto di concedere l'accesso a determinati dati o la loro condivisione, ed i c.d. *data users*, vale a dire i soggetti (persone fisiche o giuridiche) che hanno l'accesso legittimo a determinati dati e che hanno diritto di utilizzarli per fini commerciali o non commerciali (art. 2).

Enunciate le definizioni, l'art. 10 illustra tre tipologie di servizio di intermediazione, caratterizzate da diverse finalità e per le quali il DGA indica anche strumenti specifici, sempre delineando un soggetto neutrale rispetto agli altri coinvolti nello scambio, con funzioni di facilitatore della condivisione dei dati.

La prima tipologia mette in contatto titolari e utenti dei dati per finalità commerciali di scambio, avvalendosi di piattaforme telematiche, che permettono anche l'utilizzo congiunto dei dati, oppure approntando infrastrutture specifiche per l'interconnessione di titolari ed utenti dei dati, tutte soluzioni auspicate dal DGA in quanto funzionali a ridurre i costi di transazione.

Un'altra tipologia di servizio di intermediazione, invece, mette in contatto i potenziali utenti di dati con gli interessati, agevolando questi ultimi nell'esercizio dei

---

[74] *Considerando* n. 27 del Regolamento (UE) 2022/868 del Parlamento e del Consiglio, del 30 maggio 2022 *relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (Regolamento sulla governance dei dati)*.

diritti loro riconosciuti dal GDPR, come, ad esempio, la concessione o la revoca del consenso al trattamento dei dati, la rettifica dei dati personali inesatti, la cancellazione, il diritto all'oblio o alla portabilità [75].

In detta relazione, gli intermediari svolgono una funzione di supporto nell'assicurare la possibilità di un maggior controllo dei dati da parte degli interessati e sono anche tenuti a garantire che gli utenti trattino i dati con la dovuta diligenza e non per scopi diversi o illeciti. Per svolgere più efficacemente il servizio, gli intermediari dovrebbero creare spazi riservati al trattamento, in modo da evitare che i dati personali possano essere trasmessi a terzi. Il DGA specifica che gli spazi di dati personali potrebbero contenere il nome, l'indirizzo, la data di nascita dell'interessato, nonché dati generati dall'utilizzo di un servizio *on line* o da un oggetto connesso all'*Internet of things* o, ancora, informazioni verificate sull'identità dell'interessato, quali numeri di passaporto o conti bancari (*considerando* n. 30) [76].

La terza tipologia di servizio di intermediazione comprende, infine, i servizi resi da cooperative di dati.

Anche se non riporta una definizione di "cooperativa di dati", è possibile affermare che proprio il DGA, per la prima volta, assegna un ruolo nell'ambito dell'economia digitale al modello della società cooperativa, già ampiamente diffuso nel mondo dell'impresa in vari settori dell'economia, anche molto diversi tra loro.

La cooperativa di dati può essere considerata un *unicum* nel panorama della *data governance*, in ragione delle sue peculiari caratteristiche, derivanti dall'essenza stessa di essere cooperativa, che potrebbero consentire ai cittadini di esercitare potere negoziale per l'uso dei dati.

Si tratta di «una struttura organizzativa costituita da interessati, imprese individuali o da PMI, che sono membri di tale struttura, avente come obiettivi principali quelli di aiutare i propri membri nell'esercizio dei loro diritti in relazione a determinati dati, anche per quanto riguarda il compiere scelte informate prima di acconsentire al trattamento dei dati, di procedere a uno scambio di opinioni sulle finalità e sulle condizioni del trattamento dei dati che rappresenterebbero al meglio gli interessi dei propri membri in relazione ai loro dati, o di negoziare i termini e le condizioni per il trattamento dei dati per conto dei membri prima di concedere l'autorizzazione al trattamento dei dati non personali o prima che essi diano il loro consenso al trattamento dei dati personali» (art. 2, par. 1, n. 15, DGA).

La cooperativa di dati si fonda sulla condivisione volontaria e collaborativa dei propri dati personali da parte di individui a vantaggio dell'appartenenza al gruppo o alla comunità e consente agli stessi individui di acquisire, in tal modo, una migliore comprensione delle loro attuali condizioni economiche, sanitarie e sociali, attraver-

---

[75] ASSONIME, *Data Governance Act: le regole per il mercato interno dei dati*, approfondimento 4/2022, disponibile al link https://www.astrid-online.it/rassegna/2022/23-12-2022-n-365.html.

[76] ASSONIME, *Data Governance Act: le regole per il mercato interno dei dati*, cit.

so un modello di controllo dei dati di tipo collettivo da cui consegue anche la monetizzazione dei dati raccolti a beneficio dell'intera comunità dei membri, seppur circoscritta in ragione proprio del tipo di società che deve, per sua stessa natura, limitare il lucro soggettivo dei singoli soci [77].

Anche per le cooperative di dati, il servizio di intermediazione ha lo scopo primario di assistere gli interessati nell'effettuare una scelta consapevole sull'utilizzo dei propri dati e di supportarli nell'individuazione di soluzioni comuni sulle modalità di utilizzo, laddove vi siano posizioni contrastanti all'interno di uno stesso gruppo, ma proprio la specificità del modello cooperativo garantirebbe ai soci la certezza di mantenerne il controllo.

A sua volta, l'attività degli intermediari è sottoposta a controllo tramite un sistema di notifica obbligatoria all'autorità nazionale competente (art. 11) ed il rispetto di una serie di obblighi e requisiti volti a scongiurare un uso improprio dei dati (art. 12). In particolare, l'intermediario deve: assicurare che la procedura di accesso al servizio sia equa, trasparente e non discriminatoria (anche per quanto riguarda i prezzi e le condizioni di servizio); garantire un adeguato livello di sicurezza per la conservazione dei dati e per prevenire pratiche fraudolente o abusive da parte dei soggetti che richiedono l'accesso; agevolare lo scambio dei dati nel formato in cui li riceve e convertirli in formati specifici solo allo scopo di migliorarne l'interoperabilità, intrasettoriale e intersettoriale.

4. Osservazioni conclusive: le PMI tra Industria 5.0 e Neo mutualismo digitale, un connubio possibile?

In conclusione, riprendendo il *considerando* n. 31 del DGA, se, da un lato, «Le cooperative di dati mirano a raggiungere una serie di obiettivi, in particolare a rafforzare la posizione dei singoli individui, affinché compiano scelte informate prima di acconsentire all'utilizzo dei dati, influenzando i termini e le condizioni, stabiliti dalle organizzazioni di utenti dei dati, cui è subordinato l'utilizzo dei dati, in modo da offrire scelte migliori ai singoli membri del gruppo, o trovando possibili soluzioni alle posizioni contrastanti dei singoli membri di un gruppo in merito alle modalità di utilizzo dei dati laddove tali dati riguardino più interessati», dall'altro, «potrebbero altresì rappresentare uno strumento utile per imprese individuali e PMI che, in termini di conoscenze in materia di condivisione dei dati, sono spesso equiparabili ai singoli individui».

Una cooperativa è immaginabile come «*an enabler for SMEs to harness the vast potential of IIoT analytics despite limitations in capital, expertise, and IT resources*» in grado di «*draw together the capabilities of an SME ecosystem and*

[77] A PENTLAND-T. HARDJONO, *Data cooperatives*, in *Building the New Economy*, p. 2. Disponibile al link https://wip.mitpress.mit.edu/pub/pnxgvubq/release/2.

concentrate them in a data cooperative that also acts as a legal entity owned by the SMEs» apparendo quale «*a viable solution to foster data sharing among SMEs and to enable innovative analytics solutions*» [78].

Infatti, «Le PMI non traggono (…) ancora pieno beneficio dai dati, la linfa vitale dell'economia digitale. Molte di esse non sono consapevoli del valore dei dati che creano e non sono sufficientemente tutelate né preparate per la futura economia agile basata sui dati. (…). La scelta di una strategia imprenditoriale digitale suscita spesso dubbi nelle PMI tradizionali, che hanno altresì problemi a sfruttare i grandi repertori di dati a disposizione delle grandi imprese, rifuggono da strumenti e applicazioni avanzati (…)e risultano nel contempo vulnerabili alle minacce informatiche» [79].

Sempre più, dunque, «Si avverte la necessità di sostenere le piccole e medie imprese (PMI) che intendono avvalersi della trasformazione digitale nei loro processi produttivi» [80], anche ricorrendo e attribuendo un ruolo chiave ai Poli europei dell'innovazione digitale, strumenti introdotti con il Regolamento (UE) 2021/694, che potrebbero consentire alle PMI di beneficiare di servizi di consulenza in materia digitale, stimolando «un'ampia adozione delle tecnologie digitali avanzate da parte dell'industria, in particolare le PMI» [81] e favorendole nel arrivare ad essere «*more competitive with regard to their business/production processes, products or services by using digital technologies*» [82].

I Poli europei dell'innovazione digitale, quali soggetti selezionati a «fornire direttamente o assicurare l'accesso a competenze tecnologiche e strutture di sperimentazione, come attrezzature e strumenti software, allo scopo di rendere possibile la trasformazione digitale dell'industria, nonché agevolare l'accesso ai finanziamenti» [83], potranno, in combinato anche con le cooperative di dati, sostenere davvero la digitalizzazione delle PMI, processo che continua a presentarsi ancora «come un procedimento in itinere, non privo di ostacoli o di rischi» [84].

Infatti, anche se le piattaforme online possono costituire un'opportunità di «promozione economica e commerciale importante», le «pratiche svantaggiose per gli

---

[78] H. BAARS-A. TANK-P. WEBER-H. G. KEMPER-H. LASI-B. PEDELL, *Cooperative Approaches to Data Sharing and Analysis for Industrial Internet of Things Ecosystems*, in *AppliedScience*, n. 11/2021, p. 15.

[79] COMMISSIONE EUROPEA, *Una strategia per le PMI per un'Europa sostenibile e digitale*, cit., p. 4.

[80] *Considerando* n. 16 del Regolamento UE 2021/694 del 29 aprile 2021 che istituisce *il programma Europa digitale*.

[81] *Considerando* n. 17 del Regolamento UE 2021/694 del 29 aprile 2021 che istituisce *il programma Europa digitale*.

[82] A. CRUPI-N. DEL SANTO-A. DI MININ-G. GREGORI, *The digital transformation of SMEs. A new knowledge broker called the digital innovation hub*, in *Journal of Knowledge Management*, 2020, n. 6, p. 1264.

[83] Art. 2, punto 5, del Regolamento UE 2021/694 del 29 aprile 2021 che istituisce *il programma Europa digitale*.

[84] M.A. STEFANELLI, *La nuova Strategia europea per le PMI. Innovazioni giuridiche digitali: la Piattaforma europea "Fit for the future" e i "Digital Innovation Hub"*, cit., p. 6.

utilizzatori professionali (quali, ad esempio, il *delisting* di prodotti o servizi senza il dovuto preavviso o senza effettiva possibilità di ricorso)» [85] e «la mancanza di trasparenza, ad esempio per quanto riguarda le posizioni e i risultati delle ricerche, e la mancanza di chiarezza per quanto riguarda alcune normative o politiche applicabili» sono tuttora un freno rilevante alla digitalizzazione delle PMI in ragione anche della circostanza che «Una percentuale significativa di controversie tra utenti professionali e piattaforme online resta irrisolta, il che può creare importanti effetti negativi per le imprese interessate» [86].

Stante l'imprescindibile necessità che le PMI attuino un profondo ed intenso processo di digitalizzazione delle proprie attività per crescere e prosperare sul mercato, potrà rivelarsi «essenziale adottare un approccio da PMI a PMI. Il numero crescente di PMI giovani, esperte nell'uso delle tecnologie, può aiutare le imprese industriali più affermate ad adeguare il proprio modello di business e a sviluppare nuove forme di lavoro per l'era digitale» [87], attuando quasi una sorta di patto generazionale tra imprese che condividono la stessa dimensione minore.

La normativa contenuta nel *Digital Data Act* e, in particolare, le cooperative di dati appaiono quali strumenti utili per bilanciare l'economia mondiale dei dati, attraverso il raggiungimento di un equilibrio tra le parti interessate, e per promuovere un contesto economico in cui anche le aziende europee più piccole e con minore influenza sul mercato possono accedere al mercato dei dati [88].

Sempre nella logica di valorizzazione delle PMI e «Al fine di attuare con successo il quadro di governance dei dati» [89], la Commissione, all'art. 29 del DGA, prevede tra i componenti del neo-istituito Comitato europeo per l'innovazione in materia di dati, il rappresentante dell'UE per le PMI o un rappresentante nominato dalla rete dei rappresentanti per le PMI.

Il contesto attuale sembra pronto per la creazione di istituzioni collettive che rappresentino i diritti dei dati degli individui, quali, appunto, le cooperative di dati che, in quanto soggetto collettivo, possono costituire un potente strumento per negoziare servizi e sconti migliori per i membri e per guidare gli investimenti che migliorano le condizioni economiche, sanitarie e sociali dei membri e della comunità [90].

---

[85] M.A. STEFANELLI, *La nuova Strategia europea per le PMI. Innovazioni giuridiche digitali: la Piattaforma europea "Fit for the future" e i "Digital Innovation Hub"*, cit., p. 6.

[86] COMMISSIONE EUROPEA, *Sulla revisione intermedia della Strategia per il mercato unico digitale. Un mercato unico digitale connesso per tutti*, p. 10.

[87] COMMISSIONE EUROPEA, *Una nuova strategia industriale per l'Europa*, Brussels, 10 marzo 2020, COM (2020) 102 *final*, p. 4 (*Industria europea: oggi e domani*).

[88] H. BAARS-A. TANK-P. WEBER-H. G. KEMPER-H. LASI-B. PEDELL, *Cooperative Approaches to Data Sharing and Analysis for Industrial Internet of Things Ecosystems*, cit., p. 2.

[89] *Considerando* n. 53 del Regolamento (UE) 2022/868 del Parlamento e del Consiglio, del 30 maggio 2022 *relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (Regolamento sulla governance dei dati)*.

[90] A PENTLAND-T. HARDJONO, *Data cooperatives*, in *Building the New Economy*, cit., p. 10.

«Il grado di resilienza e di capacità di adattamento che il modello cooperativo ha dimostrato di avere al verificarsi delle crisi che hanno accompagnato, via via nel tempo, i processi della logica di mercato di tipo capitalistico ed il sorprendente emergere e consolidarsi di logiche imprenditoriali alternative (…) che trovano lemmi e motivazioni, cioè il loro *genus* fondativo, proprio nell'*ethos* delle cooperative mutualistiche» [91] sembrano fondare la decisione del legislatore europeo di introdurre le cooperative di dati, quale struttura maggiormente adatta al nuovo ruolo, in ragione anche del loro essere «imprese altere cioè diverse per finalismo, modelli di governo e livello e stili di comunicazione e, per questo, (…), altere, nell'uso letterario del termine, perché fiere delle proprie diversità» [92].

Diversità che si fonda sullo stesso carattere mutualistico della forma cooperativa che, «nel perseguimento della mutualità verso i soci (mutualità interna), contestualmente, (…) svolge una funzione correttiva della distribuzione della ricchezza attraverso l'elargizione di un servizio e quindi attraverso la soddisfazione di bisogni piuttosto che a mezzo di elargizione di utili» e, «coerentemente con i propri intenti finalistici – produce quelle che la teoria economica tradizionale chiama esternalità positive» [93], confermando le recenti tesi di quello che, non a torto, è stato definito come un neo mutualismo digitale [94] volto ad ampliare «l'insediarsi di nuove forme di imprenditorialità» [95], valorizzando l'economia della condivisione, sempre garantendo «un'equa ripartizione tra i soci dei vantaggi generati dall'utilizzo dei dati» [96].

Infine, tanto l'intero Digital Data Act quanto, nello specifico, l'istituto delle cooperative di dati rientrano tra le iniziative che intendono sfruttare l'impulso che la pandemia da Covid-19 ha impresso nella duplice direzione di accelerare lo svi-

---

[91] A. MATACENA, *Le cooperative imprese "altere"*, Milano, 2017, p. 9.

[92] A. MATACENA, *Le cooperative imprese "altere"*, cit., p. 9.

[93] A. MATACENA, *Le cooperative imprese "altere"*, cit., p. 24.

[94] In tema, si rimanda a P. VENTURI-F. ZANDONAI, *Neomutualismo. Ridisegnare dal basso competitività e welfare*, Milano, 2022. Sempre in merito al concetto di mutualità, si rinvia anche agli studi di: G. TATARANO, *L'impresa cooperativa*, in A. CICU-F. MESSINEO (a cura di), *Trattato di diritto civile e commerciale*, Milano 2002; G. BONFANTE, *Imprese cooperative*, in F. GALGANO (a cura di), *Commentario al Codice Civile*, Bologna, 1999; V. BUONOCORE, *Diritto della cooperazione*, Bologna, 1997; L.F. PAOLUCCI, *La mutualità delle cooperative*, Milano, 1974. Da ultimo, si ricorda anche la sentenza della Suprema Corte di Cassazione, 8 settembre 1999, n. 9513 ove si afferma come «Lo scopo mutualistico proprio delle cooperative può avere gradazioni diverse, che vanno dalla cosiddetta mutualità pura, caratterizzata dall'assenza di qualsiasi scopo di lucro, alla cosiddetta mutualità spuria, che, attenuandosi il fine mutualistico, consente una maggiore dinamicità operativa anche nei confronti dei terzi non soci, conciliando così il fine mutualistico con un'attività commerciale e con la conseguente possibilità per la cooperativa di cedere beni o servizi a terzi a fini di lucro».

[95] LEGACOOP-FONDAZIONE PICO, *Manifesto* «*Le cooperative e la sfida dell'innovazione digitale: il neo mutualismo in 10 tesi*», Tesi numero 10, disponibile al link https://site.unibo.it/cooperative-didati/it/attivita-di-ricerca/pubblicazioni.

[96] LEGACOOP-FONDAZIONE PICO, *Manifesto* «*Le cooperative e la sfida dell'innovazione digitale: il neo mutualismo in 10 tesi*», Tesi numero 8.

luppo della digitalizzazione ma anche di riflettere sul ruolo delle imprese all'interno della società [97], inducendo sempre più verso la concezione di una industria *sustainable, humancentric and resilient*, in coerenza con i valori e i diritti fondamentali europei nel convincimento «che l'essere umano sia e debba rimanere l'elemento centrale» [98].

Si tratta di una visione umanocentrica che si inserisce tanto nella già citata Strategia europea dei dati, quanto negli studi relativi alla Quinta rivoluzione industriale, Industria 5.0 [99], per certi aspetti già in corso, in cui le tecnologie della digitalizzazione avanzata, dei Big Data e dell'intelligenza artificiale conservano un metodo «*human centric and socio centric*» nella consapevolezza di come «*in the industrial context, there is still place for progress regarding the human-centric approach. In order to ensure that both companies and workers benefit from the digital transition, rethinking and redesigning business models is necessary*» [100].

---

[97] B. BERTARINI, *Misure di sostegno a favore delle micro, piccole e medie imprese nel contesto della pandemia Covid-19*, in *AmbienteDiritto*, n. 4/2020. In merito all'impatto economico causato dalla pandemia alle PMI, la World Trade Organization (WTO), nel report *Helping MSMEs navigate the Covid-19 Crisis*, del 3 giugno 2020, ha evidenziato come «*MSMEs are disproportionately af fected by the COVID-19 pandemic because of their prevalence in the economic sectors most affected by demand shocks caused by the pandemic. These sectors include accommodation and food services, cultural and creative sectors, and wholesale and retail services (OECD, Coronavirus (COVID-19) and cultural and creative sectors: impact, innovations and planning for post-crisis, 2020). Data for OECD and some non-OECD economies show that MSMEs export more than large f irms in these sectors. Partial or full quarantine measures, as well as disruptions to international means of transport, will clearly lead to a dramatic loss of demand and revenue in these areas for both domestic and trade activities*». F. EGGERS, *Masters of disasters? Challenges and opportunities for SMEs in times of crisis*, in *Journal of Business Research*, vol. 116, 12 maggio 2020, p. 199, invece, evidenzia come alcuni tratti caratteristici delle MPMI potrebbero, al contrario, essere dirimenti per superare la crisi in quanto «*given their smaller size, they tend to be rather f lexible when opportunities or threats arise in their environment. Further, the smaller the organization, the closer the decision-makers are to their customers and other stakeholders. This in turn can provide them with valuable market information that can be helpful when reacting to crises*».

[98] COMMISSIONE EUROPEA, *Una strategia europea per i dati*, cit., p. 5.

[99] In tema di Industry 5.0 si rimanda a:A. MARTIN, *Industria 5.0*, Milano, 2022; Y. ZENGIN-S. NAKTIYOK-E. KAYGIN-O. KAVAK-E. TOPÇUO, *An Investigation upon Industry 4.0 and Society 5.0 within the Context of Sustainable Development Goals*, in *Sustainability*, n. 1/2021; B. AQUILANI-M. PICCAROZZI-T. ABBATE-A. CODINI, *The Role of Open Innovation and Value Co-creation in the Challenging Transition from Industry 4.0 to Society 5.0: Toward a Theoretical Framework*, in *Sustainability*, n. 1/2020; F. ASLAM-W. AIMIN-M. LI-K. UR REHMAN, *Innovation in the Era of IoT and Industry 5.0: Absolute Innovation Management*, in *Information*, n. 1/2020; K.A. DEMIR-G. DÖVEN-B. SEZEN, *Industry 5.0 and Human-Robot Co-working*, in *Procedia Computer*, n. 2/2019; S. NAHAVANDI, *Industry 5.0 – A Human-Centric Solution*, in *Sustainability*, n. 11/2019; V. ÖZDEMIR-N. HEKIM, *Birth of Industry 5.0: Making Sense of Big Data with Artificial Intelligence, "The Internet of Things" and Next-Generation Technology Policy*, in *Omics*, n. 22/2018.

[100] COMMISSIONE EUROPEA, *Directorate General for Research and Innovation, Industry 5.0. Towards a sustainable, humancentric and resilient European Industry*, Brussels, gennaio 2021, p. 26.

A differenza della Quarta Rivoluzione Industriale, Industria 4.0, concentrata essenzialmente sull'obiettivo di migliorare l'efficienza dei processi al punto di rischiare di non considerare il costo umano derivante dall'automazione spinta degli stessi, Industria 5.0 è la Rivoluzione industriale in cui uomo e macchina non sono contrapposti ma lavorano assieme per migliorare i mezzi e l'efficienza della produzione.

In detto contesto di passaggio da un capitalismo di tipo tradizionale ad uno di tipo digitale [101], le *Small Business*, fondando anche sulla possibilità di divenire socie di cooperative di dati, possono trovare una nuova collocazione, capace di valorizzarne le potenzialità che certamente posseggono tanto da venire identificate come il «gigante nascosto» [102] dell'economia europea [103], mantenendo quella caratterizzazione che vede nell'imprenditore e, in particolare, nel piccolo imprenditore, colui che nel cambiamento vede «qualcosa di normale e positivo (…)e lo sfrutta come opportunità» [104] per realizzare nuove possibilità [105].

[101] In tema di analisi di capitalismo digitale, si rinvia a: S. ZUBOFF, *Il capitalismo della sorveglianza*, Roma, 2019; G. ALPA (a cura di), *Diritto e intelligenza artificiale: profili generali, soggetti, contratti, responsabilità civile, diritto bancario e finanziario, processo civile*, Pisa, 2020; G. FINOCCHIARO, *Diritto di Internet*, Bologna, 2020; J.E. COHEN, *Between truth and power: The Legal Constructions of Informational Capitalism*, Oxford, 2019; C. O'NEAL, *Weapons of math destruction: how big data increases inequality and threatens democracy*, New York, 2017; M. BETANCOURT, *The critique of digital capitalism*, New York, 2015.

[102] E. PICOZZA, *Il diritto pubblico dell'economia nell'integrazione europea*, Roma, 2001, p. 301.

[103] M.A. STEFANELLI, *Small Business in Europa. Regolamentazione giuridica a geometria variabile*, in G. LEMME (a cura di), *Diritto ed economia del mercato*, Milano, 2021, p. 237.

[104] P. DRUCKER, *Innovazione e imprenditorialità*, Sonzogno, 1986, p. 28.

[105] D. ANTISERI, *Prefazione*, allo studio del 1981 di M. NOVAK, *Verso una teologia dell'impresa*, Milano, 2018.

Capitolo XIX

Cooperative di dati e incubatori di *start-up* innovative certificati: un rapporto possibile? Alcuni spunti tassonomici oltre lo schema mutualistico

Riccardo Michele Colangelo

Abstract: This paper aims to deepen the taxonomic framework of data cooperatives in the context of commercial law. Specifically, it is intended to verify whether a data cooperative may be considered at the same time as a «certified innovative start-up incubator» pursuant to the applicable Italian legislation. A preliminary answer is provided in this paper, also considering the specific scenario of the support offered not to natural persons, with regard to the processing of their personal data, but to innovative start-up companies, in relation to datasets outside the scope of applicability of the GDPR.

1. Le cooperative di dati: alcuni profili tassonomici tra DGA e diritto societario.

L'introduzione nel panorama giuridico eurounitario delle «cooperative di dati» o «*data cooperatives*» – che a propria volta prendono spunto da realtà già in parte operative in alcuni contesti extra-UE [1] – è da ricondursi all'art. 2, Regolamento (UE) 2022/868 (*Digital Governance Act*, noto anche con l'acronimo DGA) [2] che definisce più tecnicamente i «servizi di cooperative di dati» come quei «servizi di

[1] Cfr. F. BRAVO, *Le cooperative di dati*, in *Contratto e impresa*, 2023, 3, p. 770 ss.

[2] Tale acronimo sarà utilizzato nel prosieguo del presente contributo, al fine di indicare il Regolamento (UE) 2022/868 del Parlamento Europeo e del Consiglio del 30 maggio 2022 relativo alla *governance* europea dei dati e che modifica il regolamento (UE) 2018/1724 (Regolamento sulla *governance* dei dati).

intermediazione dei dati offerti da una struttura organizzativa costituita da interessati, imprese individuali o da PMI, che sono membri di tale struttura, avente come obiettivi principali quelli di aiutare i propri membri nell'esercizio dei loro diritti in relazione a determinati dati, anche per quanto riguarda il compiere scelte informate prima di acconsentire al trattamento dei dati, di procedere a uno scambio di opinioni sulle finalità e sulle condizioni del trattamento dei dati che rappresenterebbero al meglio gli interessi dei propri membri in relazione ai loro dati, o di negoziare i termini e le condizioni per il trattamento dei dati per conto dei membri prima di concedere l'autorizzazione al trattamento dei dati non personali o prima che essi diano il loro consenso al trattamento dei dati personali»[3].

Esse, pertanto, risultano annoverate nel più ampio *genus* dei servizi di intermediazione dei dati, ai sensi dell'art. 10, par. 1, lett. *c*), DGA e, in quanto tali, soggette alla specifica procedura di notifica all'autorità competente per i servizi di intermediazione dei dati, come disciplinata nel medesimo Regolamento[4].

Prescindendo da quanto sancito a livello di alcuni *considerando*[5], terminano qui gli sfumati confini della definizione eurounitaria, che, a tutt'oggi, continua a costituire un unicum all'interno del diritto vigente ed applicabile nel nostro ordinamento.

Sulla base di tale scarna ed essenziale disciplina, per quanto interessa direttamente in questa sede, risulta comunque possibile esplicitare ed approfondire un aspetto tassonomico di peculiare rilevanza, già rilevato dalla dottrina italiana[6], analizzandone le principali implicazioni anche sotto profili eminentemente afferenti al diritto societario.

Si tratta, nello specifico, dello schema mutualistico[7]: nonostante il tenore letterale dei termini utilizzati dal legislatore europeo[8], nel contesto dell'istituto in commento non emerge la necessità di attingere al tipo societario della società cooperativa[9], pur permanendo – e, di norma, prevalendo – tale possibilità.

---

[3] Così l'art. 2, par. 1, n. 15, DGA.

[4] Cfr. art. 11, DGA.

[5] Cfr. cons. 31 e 32 DGA.

[6] Si veda in particolare F. BRAVO, *Le cooperative di dati*, cit., pp. 760 e 762.

[7] In dottrina, per tutti, si rimanda a G. BONFANTE, *La società cooperativa*, in *Le Società,* 2023, 1, p. 102 ss. e A. BASSI, *Scopo mutualistico*, in V. DONATIVI (a cura di), *Trattato delle società*, Tomo IV, Milano, 2022, p. 1357 ss.

Si noti, peraltro, come non manchino casi, di natura eccezionale, di società cooperative caratterizzate dall'assenza dello scopo mutualistico: cfr. G. MARASÀ, *Le società: profili sistematici e funzione*, in V. DONATIVI (a cura di), *Trattato delle società*, Tomo I, Milano, 2022, pp. 103-104.

[8] Anche nella versione in lingua inglese del testo del DGA, il riferimento va alle *data cooperatives*.

[9] In argomento, a rigore, risulta maggiormente opportuno il riferimento a «tipi cooperativi», considerata l'ampiezza del relativo paniere, peraltro tratteggiata in dottrina come «polimorfismo cooperativo»: cfr. G. BONFANTE, *Profili tipologici e causali*, in V. DONATIVI (a cura di), *Trattato delle società*, Tomo IV, Milano, 2022, p. 1352 ss.

La stessa nozione di polimorfismo cooperativo sinora elaborata si presta ad essere arricchita da riferimenti alla cooperativa di dati ed alle relative specificità.

Questa evidenza apre ad una interessante serie di considerazioni ulteriori relativamente ai casi in cui la cooperativa di dati fornisca taluni dei servizi previsti dal legislatore eurounitario non a persone fisiche, né a imprese individuali, bensì a società anche di modeste dimensioni, che possono quindi integrare i requisiti propri delle PMI [10]. Tra esse, in questa sede verranno sinteticamente esposte alcune prime note, con particolare riguardo ai casi in cui siano le *start-up* innovative – che pur potrebbero superare le soglie previste per le micro, piccole e medie imprese – a risultare potenziali beneficiari dei servizi propri delle cooperative di dati.

Alla luce di siffatte premesse, talune attività peculiari delle *data cooperatives* mal si addicono al caso in analisi: a titolo esemplificativo, tutto quanto concerne il supporto alla prestazione di un consenso libero ed informato al trattamento dei dati personali può rilevare solamente per i soggetti interessati, per tali intendendosi le persone fisiche – e non giuridiche – a cui, indirettamente o indirettamente, si riferiscono le informazioni [11].

Diversamente, ben potrebbero essere fruibili le attività di intermediazione relative alla negoziazione di termini e condizioni per il trattamento dei dati (anche non personali), annoverate *ex* art. 2 DGA tra le prerogative delle *data cooperatives*.

2. Gli incubatori certificati di start-up innovative.

I confini sfumati dell'ampia formula definitoria adoperata dal legislatore europeo, in particolare, stimolano l'interprete a verificare gli eventuali profili di compatibilità e, in un certo qual modo, di sovrapponibilità tra l'istituto della cooperativa di dati e quello dell'incubatore di start-up innovative certificato [12].

Quest'ultimo, introdotto nel nostro ordinamento giuridico ad opera del d.l. 18 ottobre 2012, n. 179, recante «Ulteriori misure urgenti per la crescita del Paese» e convertito con modificazioni dalla l. 17 dicembre 2012, n. 221, è definito come «una società di capitali, costituita anche in forma cooperativa, di diritto italiano ovvero una Societas Europaea, residente in Italia (…), che offre servizi per sostenere la nascita e lo sviluppo di *start-up* innovative» [13].

Al fine dell'assunzione della qualifica di incubatore certificato [14], è lo stesso art.

---

[10] Il riferimento va *in primis* ai limiti quantitativi di cui alla Raccomandazione della Commissione Europea 2003/361 del 6 maggio 2003.

[11] Arg. *ex* art. 4, par. 1, n. 1, Regolamento (UE) 2016/679 (GDPR).

[12] In relazione a quest'ultimo istituto, in dottrina, si rimanda, *ex multis*, a O. CAGNASSO, E. FREGONARA, *Le società innovative (I parte) – società innovative oggi e domani*, in *Giurisprudenza Italiana*, 2021, 8-9, p. 2006 ss.

[13] Così l'art. 25, co. 5, d.l. 18 ottobre 2012, n. 179.

[14] E quindi della fruizione della disciplina speciale di cui agli artt. 26 e 27, d.l. n. 179/2012 ed in particolare dei benefici fiscali riassunti in G. MOLINARO, *Incentivi fiscali per le start-up innovative*, in *Corriere Tributario*, 2017, 15, p. 1162 ss.

25, co. 5, d.l. n. 179/2012 a prevedere una serie di cinque requisiti, tra i quali, in via riassuntiva, si annoverano: strutture «anche immobiliari» che siano «adeguate ad accogliere *start-up* innovative»; attrezzature, anche informatiche, adeguate all'attività di queste ultime; essere «amministrato o diretto da persone di riconosciuta competenza in materia di impresa e innovazione», nonché dotato di «una struttura tecnica e di consulenza manageriale permanente»; avere «regolari rapporti di collaborazione con università, centri di ricerca, istituzioni pubbliche e partner finanziari che svolgono attività e progetti collegati a *start-up* innovative»; avere «adeguata e comprovata esperienza nell'attività di sostegno a *start-up* innovative» [15].

Sarà il legale rappresentante della società, all'atto della iscrizione nella sezione speciale del registro delle imprese di cui all'art. 25, comma 8, d.l. n. 179/2012 [16], ad autocertificare il possesso di siffatti requisiti, «sulla base di indicatori e relativi valori minimi che sono stabiliti con decreto del Ministero dello sviluppo economico» [17], come previsto dal precedente co. 6 del medesimo articolo.

Diversamente, il co. 7, per quanto attiene all'esperienza pregressa della società che aspira a divenire incubatore certificato, specifica espressamente alcuni indicatori, rimandando anch'esso al decreto attuativo la mera individuazione delle relative soglie minime. Tra gli otto indicatori indicati *expressis verbis* dal legislatore, sono annoverati: il «numero di candidature di progetti di costituzione e/o incubazione di *start-up* innovative ricevute e valutate nel corso dell'anno»; il «numero di *start-up* innovative avviate e ospitate nell'anno», così come di quelle uscite nel medesimo lasso temporale; il «numero complessivo di collaboratori e personale ospitato»; la «percentuale di variazione del numero complessivo degli occupati rispetto all'anno, precedente»; il «tasso di crescita media del valore della produzione delle *start-up* innovative incubate»; i «capitali di rischio ovvero finanziamenti, messi a disposizione dall'Unione europea, dallo Stato e dalle regioni, raccolti a favore delle *start-up* innovative incubate»; il «numero di brevetti registrati dalle *start-up* innovative incubate», da parametrarsi al «relativo settore merceologico» [18].

Alcune di tali informazioni, unitamente a quanto pertiene alla costituzione della

---

[15] *Ibidem*.

[16] Ove si dispone che «per le *start-up* innovative di cui ai commi 2 e 3 e per gli incubatori certificati di cui al comma 5, le Camere di commercio, industria, artigianato e agricoltura istituiscono una apposita sezione speciale del registro delle imprese di cui all'articolo 2188 del codice civile, a cui la *start-up* innovativa e l'incubatore certificato devono essere iscritti al fine di poter beneficiare della disciplina della presente sezione». Il successivo comma 10 precisa le informazioni condivise mediante tale sezione speciale del registro delle imprese. Con particolare riguardo ai soli incubatori certificati si tratta di quanto pertiene «all'anagrafica, all'attività svolta, al bilancio, così come ai requisiti previsti al comma 5».

[17] Si tratta del decreto del Ministro dello Sviluppo Economico del 22 dicembre 2016, recante «Revisione del decreto 22 febbraio 2013 relativo ai requisiti per l'identificazione degli incubatori certificati di *startup* innovative».

[18] Art. 25, co. 7, lett. *a*)-*h*), d.l. n. 179/2012.

società, alle sedi ed all'oggetto sociale [19], debbono essere «rese disponibili, assicurando la massima trasparenza e accessibilità, per via telematica o su supporto informatico in formato tabellare gestibile da motori di ricerca, con possibilità di elaborazione e ripubblicazione gratuita da parte di soggetti terzi». Risulta inoltre essere prevista la pubblicazione delle medesime, similmente a quanto avviene per le *start-up* innovative, con collegamento ipertestuale visibile a partire dalla homepage del sito Internet del singolo incubatore certificato, a norma del co. 11. Le informazioni così pubblicate, inoltre, sono soggette ad un aggiornamento quantomeno annuale [20].

Ciò posto, siamo in presenza di un'attività d'impresa marcatamente orientata alla fornitura di servizi a *start-up* innovative. In argomento, in assenza di specifici vincoli a livello normativo per quanto riguarda l'oggetto sociale, risulta peraltro significativo notare come nulla vieti espressamente che l'oggetto sociale risulti più ampio rispetto a quanto direttamente e strettamente funzionale alla sola prestazione di servizi a *start-up* innovative, rilevanti ai fini dell'applicabilità della disciplina sinora tratteggiata.

3. Il caso dei dati non personali e dei servizi prestati alle imprese.

L'operazione ermeneutica tesa a verificare la possibilità di ascrivere gli incubatori certificati all'interno della nozione di cooperative di dati – e, quindi, la sussumibilità di un istituto proprio dell'ordinamento giuridico nazionale all'interno di un altro, di matrice eurounitaria – risulta ancora più rilevante se si considera uno specifico scenario, che vede, quale oggetto dei servizi offerti, *dataset* al di fuori dell'ambito di applicabilità del GDPR.

In questo caso, i profili di affinità tra cooperativa di dati e incubatore certificato sembrano trovare interessanti punti d'incontro, sostanziandosi l'attività di supporto e di consulenza manageriale su questioni rilevanti ai sensi del DGA, ma escludendo, tra queste ultime, quanto riguarda quelle più marcatamente rivolte alle persone fisiche, in particolare per finalità di supporto alla manifestazione di un consenso effettivamente libero ed informato.

Nell'attuale contesto di una *data driven economy*, caratterizzata da profili di crescente digitalizzazione [21], occorre prendere in considerazione un Regolamento non

---

[19] Più specificamente, si tratta delle informazioni enumerate all'art. 25, co. 13, d.l. n. 179/2012: «a) data e luogo di costituzione, nome e indirizzo del notaio; b) sede principale ed eventuali sedi periferiche; c) oggetto sociale; d) breve descrizione dell'attività svolta; e) elenco delle strutture e attrezzature disponibili per lo svolgimento della propria attività; f) indicazione delle esperienze professionali del personale che amministra e dirige l'incubatore certificato, esclusi eventuali dati sensibili; g) indicazione dell'esistenza di collaborazioni con università e centri di ricerca, istituzioni pubbliche e *partner* finanziari; h) indicazione dell'esperienza acquisita nell'attività di sostegno a *start-up* innovative».

[20] Cfr. art. 25, co. 17-*bis*, d.l. n. 179/2012.

[21] Proprio in questo ambito risultano particolarmente evidenti e rilevanti quelle «nuove sfide» che

particolarmente noto. Si tratta del Reg. 2018/1807, relativo al trattamento dei dati non personali e la cui disciplina risulta caratterizzata da una significativa complementarietà con quella di cui al GDPR.

Queste sintetiche premesse già evidenziano come possa essere necessario, anche per società particolarmente attente all'innovazione tecnologica, uno specifico supporto nella fase di avvio dell'attività d'impresa. Ciò risulta ancor più rilevante se si considera la genesi dei dati anonimi, ai quali sono ascrivibili non solo dati non personali *ab initio*, ma anche informazioni relative a una persona fisica identificata o identificabile, raccolte e più in generale trattate come dati personali e rese anonime solo in un secondo momento.

Sul punto, il GDPR non pare fornire significativi elementi all'interprete, né contribuire a delineare standard condivisi finalizzati a precludere o prevenire la reidentificazione degli interessati, limitandosi ad operare, al *considerando* n. 26, un puntiforme riferimento alla nozione di sufficientemente anonimizzazione di dati personali. Quest'ultima, pertanto, viene maggiormente delineata evidenziando *in primis* i confini con la nozione di pseudonimizzazione, peraltro al centro di alcune significative pronunce giurisprudenziali a livello eurounitario, tra le quali spicca la sentenza del Tribunale UE, pronunciata in data 26 aprile 2023, nella causa T-557/20 [22].

Inoltre, in tali casi occorre tenere in debita considerazione anche il parere del Gruppo di lavoro articolo 29 n. 5/2014 sulle tecniche di anonimizzazione (WP216) [23], ove vengono illustrate alcune di quest'ultime, ascrivibili in ultima analisi ad una delle due macrocategorie di riferimento (randomizzazione e generalizzazione).

Pur trattandosi di un parere, invero non recentissimo, formulato in un contesto normativo differente rispetto all'attuale ed ancora non caratterizzato dalla vigenza e della piena applicabilità del GDPR, le considerazioni ivi formulate non cessano di essere rilevanti, anche nell'ambito dell'esercizio dell'attività di impresa.

In particolare, prescindendo dalle peculiarità delle singole tecniche di anonimizzazione, i riferimenti alla valutazione del rischio di reidentificazione degli interessati contenuti in tale parere meritano di essere sempre più conosciuti ed implementati, anche con la precipua finalità di supportare le società che intendono utilizzare dati anonimi, in modo tale da far sì che i propri modelli di business coinvolti, così come, eventualmente, la stessa incipiente attività d'impresa svolta da start-up innovative, possa iniziare o proseguire senza incorrere in alcuna violazione, pur non voluta, della normativa vigente in materia di *data protection* e non solo.

Ed è proprio l'approccio basato sulla valutazione del rischio a caratterizzare, in modo ancora più marcato, anche la norma tecnica ISO/IEC 27559:2022 (*Information security, cybersecurity and privacy protection – Privacy enhancing data de-*

– come efficacemente rimarca il *considerando* n. 6 del GDPR – derivano dalla «rapidità dell'evoluzione tecnologica e [dal]la globalizzazione».

[22] Il testo integrale della sentenza è consultabile al seguente URL: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:62020TA0557.

[23] ART. 29 WORKING PARTY, *Opinion 05/2014 on Anonymisation Techniques*, 10 April 2014.

identification framework), della quale merita di essere sottolineato il rilievo, in modo particolare considerato che in essa si evidenzia quello che potrebbe essere definito come una sorta di relativismo della nozione di anonimizzazione, risultando l'interprete stimolato a svolgere effettive valutazioni, caso per caso, dei vari fattori rilevanti, individuati *ex ante*.

Nel contesto sinora illustrato, tanto le cooperative di dati quanto gli incubatori di *start-up* innovative certificati potrebbero – possedendo in concreto il *know-how* necessario a tal fine – sostenere e indirizzare le attività di *data preparation* prodromiche alla anonimizzazione dei dati personali e finalizzate all'effettivo mantenimento della medesima nel comunicare o diffondere i *dataset* in questione, così come, più in generale, la circolazione stessa dei dati non personali anche per finalità eminentemente commerciali, garantendone una corretta valutazione, anche economica [24].

Similmente, pare poter essere considerata caratteristica non aliena né alle cooperative di dati né agli incubatori di *start-up* innovative certificati la potenziale agevolazione anche di una effettiva tutela della proprietà intellettuale relativamente ai medesimi *dataset*.

4. Considerazioni conclusive.

A completamento delle considerazioni sinora esposte, fisiologicamente prive di pretese di esaustività, *a fortiori* riferendosi ad un atto normativo di recentissima applicabilità, è anzitutto doveroso affermare che meritano un adeguato approfondimento anche ulteriori specifici scenari che, con riguardo alle *start-up* innovative, possono essere utili nell'arricchire questo stimolante mosaico.

Ciò posto, risulta possibile affermare come, adottando un approccio caso per caso e con riguardo agli specifici servizi forniti ed alle peculiarità delle società destinatarie dei medesimi, un incubatore di *start-up* innovative certificato possa al contempo essere qualificato come cooperativa di dati.

Ad oggi, sul punto, non constano preclusioni correlate al tipo societario, laddove un incubatore di *start-up* innovative certificato può costituito secondo uno dei tipi propri delle società di capitali, così come può essere una società cooperativa, secondo quanto espressamente previsto *ex* art. 25, co. 5, d.l. n. 179/2012.

L'adozione dello schema mutualistico, pertanto, non risulta sempre e comunque necessaria per gli incubatori certificati, riscontrandosi sul punto una significativa vicinanza con la disciplina delle cooperative di dati.

Similmente, non paiono emergere questioni dirimenti nemmeno in merito alla iscrizione in apposita sezione speciale del registro delle imprese. Il registro europeo

---

[24] In argomento, si rimanda agli approfondimenti interdisciplinari riportati in G. CERRINA FERONI (a cura di), *Commerciabilità dei dati personali. Profili economici, giuridici, etici della monetizzazione*, Bologna, 2024.

dei servizi di intermediazione dei dati, infatti, non pare escludere in alcun modo la prestazione dei servizi in concreto compatibili alle sole start-up innovative.

D'altra parte, l'iscrizione nel registro europeo non pare essere *ex se* sufficiente al fine di relazionarsi con *start-up* innovative quale incubatore certificato. Per quest'ultimo, infatti, è lecito considerare la sussistenza delle condizioni previste dal d.l. n. 179/2012 e l'iscrizione nella sezione dedicata del registro delle imprese quali requisiti necessari.

In base a tali prime considerazioni, non è dato escludere che, *de facto*, una cooperativa di dati possa fungere da volano ai fini dell'avvio di singole start-up innovative, anche senza qualificarsi come incubatore certificato ai sensi della vigente normativa italiana; in tal caso, tuttavia, verrebbero a mancare i presupposti necessari al fine di fruire delle agevolazioni *ex lege* previste per gli incubatori e, di riflesso, a quelle società che a questi ultimi possono affidarsi.

Capitolo XX

Le cooperative di dati come forma di tutela collettiva degli interessati: un'opportunità per l'ambito sanitario?

Veronica Palladini-Simone Scagliarini[*]

Abstract: Although European legislators have been largely inactive on the matter, collective protection for data subjects would be crucial in today's data-driven society. This is particularly true for consent, a legal basis that is widely used but not able to ensure the informational self-determination of individuals. Data cooperatives could therefore be a collective body to make up for this lack. The paper analyses the use case of health research, where the model could be largely diffused, especially in consideration of legislation that currently still focuses on consent. Furthermore, not even the very recent amendments to the Privacy Code and the future, desirable approval of the regulation on the European Health Data Space would make this role less important.

1. La necessità di una tutela collettiva per gli interessati.

Benché, a otto anni dalla sua entrata in vigore e sei dalla sua piena applicabilità, il GDPR sia un atto normativo ormai pienamente integrato nel diritto vivente e sistematicamente inserito nel *corpus* delle fonti europee in tema di *governance* dell'economia digitale *data-driven*, c'è un aspetto interessante su cui l'attenzione della dottrina – e ancor più del legislatore – non ci pare sia stata del tutto adegua-

[*] Pur nell'unitaria concezione dello scritto, Simone Scagliarini ha materialmente redatto i paragrafi 1 e 4, Veronica Palladini i restanti 2 e 3.

ta [1]: il tema dei mezzi di tutela collettivi per la protezione dei dati.

Il Regolamento UE n. 679/2016, al riguardo, dimostra, invero, un certo *favor* per siffatti strumenti, specialmente laddove prevede, all'art. 80, che «l'interessato abbia il diritto di dare mandato a un organismo, un'organizzazione o un'associazione senza scopo di lucro, che siano debitamente costituiti secondo il diritto di uno Stato membro, i cui obiettivi statutari siano di pubblico interesse e che siano attivi nel settore della protezione dei diritti e delle libertà degli interessati con riguardo alla protezione dei dati personali, di proporre il reclamo per suo conto e di esercitare per suo conto» i rimedi amministrativi e giurisdizionali sia nei confronti dell'Autorità di controllo che del titolare o del responsabile, oltre che di agire in via risarcitoria ove previsto dall'ordinamento.

Ora, a noi pare che si tratti di una previsione importante, che ben può essere annoverata tra le novità più significative del GDPR [2], la quale offre uno strumento in più di cui avvalersi per dare maggiore effettività di tutela alle plurime situazioni soggettive che il Regolamento stesso intende garantire. Non è certo raro, a ben vedere, il caso in cui il singolo interessato si trovi in una difficoltà di fatto ad esercitare i propri diritti, vuoi per ignoranza degli stessi, vuoi per incapacità di fare ricorso ai mezzi di tutela all'uopo predisposti, vuoi ancora per il carattere bagatellare (a livello del singolo rapporto, ma verosimilmente non a livello aggregato) degli interessi in gioco. In tutte queste ipotesi, l'affidamento dell'esercizio dei diritti ad un soggetto, privo di scopo lucrativo, può dare sostanza ad interessi altrimenti lasciati privi di una tutela effettiva. E, se è vero che sulla base del dettato normativo ciò è già possibile, è pur vero, a nostro avviso, che si renderebbe opportuno un intervento normativo integrativo, almeno a livello nazionale, che sostenesse e fornisse un quadro regolatorio più preciso a questi enti collettivi [3], prevedendo al contempo tanto azioni volte a favorirne l'istituzione ed a sostenerne lo svolgimento delle funzioni (non necessariamente con misure di carattere finanziario), quanto ad introdurre controlli finalizzati ad evitare che si creino «sindacati gialli», atti a canalizzare le pretese degli interessati verso forme più lasche di rivendicazione. D'altro canto, da

---

[1] Con alcune eccezioni, tra cui quella, come sempre formulata con lungimiranza, di S. RODOTÀ, *Tecnopolitica*, Roma-Bari, 2004, spec. p. 156 ss., ove l'A. intuiva già molto tempo addietro, con riferimento ad azioni collettive ed al possibile intervento di associazioni di consumatori o di utenti, che «le strategie di tutela della *privacy* (…)esigono molteplici strumenti, tra loro non incompatibili, e che, almeno in talune situazioni, possono operare congiuntamente».

[2] Come sostengono G. M. RICCIO-G. SCORZA-E. BELISARIO, *GDPR e normativa privacy*, Milano, 2022, p. 713, sottolineando al contempo come, per l'appunto, a ciò non abbia fatto seguito un'adeguata implementazione a livello nazionale.

[3] Tra le (assai poche) indicazioni che possono trarsi in via interpretativa dal Regolamento, secondo A. CANDINI, *Gli strumenti di tutela*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, p. 590, vi è quella per cui, non essendo richiesta la protezione dei dati come finalità esclusiva dell'ente, anche enti con finalità più ampie – e tra queste, come argomenteremo nel paragrafo successivo, a nostro avviso *in primis* anche le Cooperative di dati – potrebbero rientrare nel novero di essi.

tempo è stato rilevato come sia andato maturando, in generale, un modello costituzionale di promozione attiva dell'associazionismo proprio in correlazione ad interessi diffusi emergenti in campo sociale contro il potere privato dei grandi gruppi di interesse [4]: modello che, *optimo jure*, meriterebbe di trovare espansione anche con riferimento alla tutela della *privacy*.

Se poi guardiamo alle analoghe branche dell'ordinamento in cui, attraverso enti collettivi di rappresentanza, si cerca di rimediare allo squilibrio tra un singolo individuo e soggetti, di norma imprenditoriali, di dimensioni e forza (anche contrattuale) incommensurabili, quali il diritto del lavoro ed il diritto dei consumatori, si potrebbe forse ipotizzare l'introduzione di previsioni ancor più incisive. Ad esempio, la consultazione delle parti interessate ai fini della redazione della valutazione di impatto, ovvero uno dei documenti nei quali si sostanzia l'*accountability* del titolare, il quale deve provvedervi «quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie (…) può presentare un rischio elevato per i diritti e le libertà delle persone fisiche» [5] potrebbe essere introdotta, almeno per alcuni casi in cui le situazioni soggettive al nostro esame siano in pericolo, come obbligatoria e magari delegabile (anche) a soggetti collettivi di rappresentanza.

Allo stesso modo, la consultazione degli *stakeholders* per l'adozione dei codici di condotta da parte di organismi rappresentanti le categorie degli interessati, suggerita dal *considerando* n. 99, potrebbe essere prevista come necessaria misura procedimentale, coinvolgendo anche le rappresentanze collettive.

Più ancora, questi soggetti potrebbero avere un ruolo rilevante sul tema del consenso, il quale, se, nelle intenzioni del legislatore, rappresenta uno strumento, quando non il principale, di realizzazione dell'autodeterminazione informativa dell'interessato, si presta nella realtà ad essere utilizzato (anche) come la chiave di volta per eludere diverse tutele previste dal Regolamento [6]. Non è certo, infatti, un mistero che, nella pratica concreta dei rapporti quotidiani, l'idea che l'interessato possa autorizzare un trattamento solo con piena consapevolezza, come pure vorrebbero assicurare le disposizioni del Regolamento che lo disciplinano [7], si scontra con una

---

[4] Cfr. G. GEMMA, *Costituzione ed associazioni: dalla libertà alla promozione*, Milano, 1993, spec. p. 190 ss.

[5] Testualmente, art. 35, par. 1, GDPR. Il corsivo è nostro.

[6] Ci riferiamo, per esempio, al divieto di trattamento delle categorie particolari di dati, al divieto di decisioni automatizzate e finanche a quello di trasferimento di dati al di fuori dell'Unione europea: divieti, tutti, che possono essere facilmente superati ove consti il consenso dell'interessato, sebbene si tratti di profili che pure sono ritenuti particolarmente rischiosi nella valutazione del legislatore.

[7] Sulla disciplina del consenso nel GDPR, anche in confronto alla previgente normativa, v. L. CALIFANO, *Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dei dati*, in L. CALIFANO-C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona*, Napoli, 2017, p. 47 ss., ove l'A. esplicita anche alcune ragioni che rendono parziale la tutela offerta dall'istituto in parola, pur leggendo (seppure a nostro avviso, con eccessivo ottimismo) nelle disposizioni sulla responsabilizzazione del titolare il meccanismo compensativo per completare questa (inevitabile) lacuna. Con riferimento ai limiti in concreto che il consenso scon-

realtà che lo rende di fatto impossibile per le più svariate ragioni. Tra esse, si può pensare quanto meno alla tempistica dei rapporti non compatibile con un'adeguata istruttoria dei profili connessi alla protezione dei dati, alla difficoltà per l'interessato di comprendere effettivamente, sia sotto il profilo giuridico che soprattutto tecnico-informatico, il significato dell'informativa [8] fino alla sostanziale infungibilità (almeno putativa) del servizio in relazione al quale il consenso al trattamento è richiesto [9].

Se dunque il consenso si dimostra in grado di approntare una protezione puramente formale dell'interessato [10], che si risolve in una tutela destinata a rimanere sulla carta, quando addirittura non si ritorce a suo danno, ove questi sia convinto, attraverso la propria manifestazione di volontà, di avere eliminato ogni possibilità di lesione della propria sfera giuridica [11], si potrebbe a nostro avviso ragionare, li-

---

ta come mezzo di garanzia dell'autodeterminazione informativa, si vedano, tra gli altri, i rilievi di C. COLAPIETRO-A. IANNUZZI, *I principi generali del trattamento dei dati personali e i diritti dell'interessato*, in L. CALIFANO-C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona*, cit., p. 115 ss.; e F. BRAVO, *Il consenso e le altre condizioni di liceità*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, cit., spec. p. 157 ss.

[8] La necessità di una funzione informativa complementare da parte dei pubblici poteri per superare i limiti del consenso connessi alla difficoltà di questo istituto di realizzare, in concreto, una reale autodeterminazione informativa, è posta in evidenza da C. COLAPIETRO-A. IANNUZZI, *I principi generali del trattamento dei dati personali e i diritti dell'interessato*, cit., p. 120.

[9] Ancor più netta la posizione di G. DE MINICO, *Big Data e la debole resistenza delle categorie giuridiche. Privacy e lex mercatoria*, in *Diritto pubblico*, 2019, p. 92, la quale afferma che «l'antica tutela della privacy, *consent based*, assistita dalle garanzie dell'autonomia e della consapevolezza, non è più utilmente invocabile. Entrambi questi attributi si sono sbriciolati dinanzi ad assensi estorti con la coercizione psicologica di negare il servizio digitale a chi si fosse rifiutato di cedere i dati o li avesse ceduti senza cognizione di causa nell'ignoranza piena delle finalità del loro impiego».

[10] Analogamente, scrive G. FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, in EAD. (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, cit., p. 3, che «certamente non può soddisfare un sistema basato su un consenso che spesso è vuoto di effettivo significato» di modo che «si tratta di un modello sotto il profilo teorico centrato sull'autodeterminazione, che tuttavia spesso manca dei presupposti sui quali dovrebbe basarsi». Sulla stessa falsariga F. BRAVO, *Il consenso e le altre condizioni di liceità*, cit., spec. p. 138 ss., il quale sottolinea come questa impostazione non sia casuale, ma risponda al preciso disegno, già evidenziato, di fare della protezione dei dati solo uno degli interessi in gioco, al pari, tuttavia, della libera circolazione degli stessi, di modo che si crea «un sistema di selezione degli interessi volto a garantire le nuove esigenze socio-economiche, dettate dall'evoluzione tecnologica […], nel quale l'esigenza di tutela del diritto fondamentale alla protezione dei dati personali finisce per perdere, nella sostanza (anche se non ancora nella forma), quella centralità che dovrebbe consegnargli l'applicazione del principio personalista».

[11] Così L. GATT-R. MONTANARI-A. CAGGIANO, *Consenso al trattamento dei dati personali e analisi giuridico-comportamentale. Spunti di riflessione sull'effettività della tutela dei dati personali*, in *Politica del diritto*, 2017, p. 376, secondo i quali vanno rilevati oggettivi «limiti del *consenso* preventivo sia perché reso inconsapevolmente sia perché – anche quando è reso consapevolmente – non si traduce in un effettivo impedimento alla dannosità del trattamento per la persona dell'utente, dannosi-

mitatamente ai casi più delicati, di un consenso validamente espresso solo "in sede protetta" [12], per mutare una terminologia del diritto sindacale, ovvero esclusivamente con una qualche forma di assistenza, compatibile con lo sviluppo dell'economia digitale, da parte di uno di questi enti collettivi, anche solo incanalando l'acquisizione dello stesso in una procedura concordata, magari nel contesto di un codice di condotta [13], con enti di rappresentanza degli interessi…degli interessati.

Peraltro, l'analogia con altri settori ordinamentali non si arresta qui, se si considera che il secondo paragrafo della medesima disposizione del GDPR prima riportata già prevede altresì la facoltà per gli Stati membri di stabilire un'autonoma legittimazione degli stessi enti ad agire a difesa di interessi collettivi.

Si tratta, in questo caso, di una opzione di cui il legislatore italiano non ha ritenuto di avvalersi [14], benché non manchino certo nell'ordinamento attuale ipotesi di tal fatta, ad esempio in materia ambientale o consumeristica [15]. Epperò, a nostro

---

tà che continua a potersi verificare. Al contrario, la prestazione del consenso potrebbe avere un effetto distorsivo perché esso viene prestato senza che l'utente abbia cognizione degli strumenti di tutela *ex post* ed anzi sulla base della convinzione che la sola concessione del consenso elimini *a priori* la possibilità stessa di una lesione» (corsivi testuali).

[12] In analogia a quanto dispone l'art. 2113 Codice civile. Sul punto, per tutti, v. P. ALBI, *La dismissione dei diritti del lavoratore: art. 2113*, in D. BUSNELLI (diretto da), *Il Codice civile. Commentario*, Milano, 2016.

[13] Per i quali, del resto, il Considerando n. 99 già prevede che gli organismi di rappresentanza dei titolari e dei rappresentanti dovrebbero consultare le parti interessate nella fase di elaborazione.

[14] Come sottolinea anche F. CASAROSA, *La tutela aggregata dei dati personali nel Regol. Ue 2016/679: una base per l'introduzione di rimedi collettivi?*, in A. MANTELERO-D. POLETTI (a cura di), *Regolare la tecnologia: il reg. Ue 2016/679 e la protezione dei dati personali*. *Un dialogo fra Italia e Spagna*, Pisa, 2018, p. 235 e ss., il legislatore italiano – nell'introdurre all'art. 142 del d.lgs. n. 196/2003 ("Codice *privacy*") la possibilità per l'interessato, di conferire mandato per il Reclamo al Garante ad un ente del terzo settore attivo nell'ambito della tutela dei diritti e delle libertà degli interessati, con riguardo alla protezione dei dati personali – ha legittimato soltanto un'azione collettiva a base *opt-in*, in cui gli interessati hanno il diritto di incaricare un ente in possesso delle caratteristiche richieste dalla legge di presentare un reclamo a loro nome, cosicché le decisioni potranno avere effetto giuridico nei confronti dei soli interessati mandatari e non ha, invece, ammesso un'azione collettiva a base *opt-out*, in cui le entità autorizzate possono agire per conto degli interessati senza aver ottenuto un previo mandato; in tema anche D. POLETTI, *Gli intermediari dei dati*, in *European Journal of Privacy Law & Technologies*, 2022, 1, p. 55. Invero, il Legislatore nazionale non ha agito certo in modo isolato, giacché nella stessa direzione si orientata la maggior parte dei Paesi UE, come constatato, non senza rammarico, dal Parlamento europeo nella *Risoluzione del 25 marzo 2021 sulla relazione di valutazione della Commissione concernente l'attuazione del regolamento generale sulla protezione dei dati due anni dopo la sua applicazione (2020/2717(RSP))*, al cui punto 18 si sollecitano gli Stati membri ad avvalersi dell'opzione offerta dal GDPR.

[15] Sul punto v. A. MANTELERO, *La* privacy *all'epoca dei* Big Data, in V. CUFFARO-R. D'ORAZIO-V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, p. 1202 ss., ove l'A. sottolinea come, per un verso, l'analogia sia più forte con l'ambito consumeristico di quanto non lo sia con quello lavoristico, stante l'indeterminatezza del gruppo costituito dagli interessati, non immediatamente identificabile *a priori*, sebbene, per altro verso, nel contesto della protezione dei dati azioni collettive

avviso è stata persa l'occasione per offrire uno strumento di difesa che potrebbe rivelarsi estremamente utile [16], specialmente laddove dovessero crearsi *network* europei, analoghi a quello delle Autorità di controllo, anche tra questi organismi di rappresentanza, la cui forza collettiva potrebbe tentare di esercitare pressioni e proporre azioni anche verso colossi della società digitale. In tal senso, occorrerebbe sul punto sia un'azione a livello europeo di sostegno alla creazione di reti tra enti di rappresentanza collettiva, sia un intervento normativo a livello nazionale per creare il rimedio giudiziale necessario al fine di mettere in grado, anche nel nostro Paese, questi soggetti di procedere nel senso auspicato [17].

2. Le cooperative di dati come possibile strumento di mutua assistenza.

Il crescente impiego di nuove tecnologie in tutti i campi del vivere e la massiccia disponibilità di dati in capo ad un numero ridotto di attori operanti nel mercato hanno determinato una crescita esponenziale dei rischi sopra evidenziati connessi ai trattamenti dei dati di singoli interessati, spesso inconsapevoli della sorte occulta delle proprie informazioni. Lo sviluppo di capacità algoritmiche predittive e di analisi ha accresciuto la possibilità di chi detiene tali conoscenze di anticipare le scelte ed influenzare le decisioni dei cittadini tanto nell'informazione [18] e nel dibattito po-

---

rischierebbero di incontrare un limite nella difficoltà di reazioni tempestive, per la difficoltà stessa degli interessati di venire a conoscenza della lesione che stanno subendo.

[16] Analogamente G. DE MINICO, *Big Data e la debole resistenza delle categorie giuridiche. Privacy e lex mercatoria*, cit., p. 98, che invero critica il legislatore europeo per non avere introdotto una «*class action*, la cui spersonalizzazione del legittimato all'azione processuale ben si combina col concetto di danno diffuso».

[17] Per l'ammissibilità di una *class action* in materia di privacy, in analogia a quella presente in ambito consumeristico, v. G.M. RICCIO-G. SCORZA-E. BELISARIO, *GDPR e normativa privacy*, cit., pp. 715 ss., i quali (contrariamente a A. CANDINI, *Gli strumenti di tutela*, cit., p. 589) ritengono che a ciò non osti il fatto che l'art. 80 sembri alludere ad azioni per la tutela di interessi pur sempre individuali, giacché il Considerando n. 142, cui esso fa rinvio, curiosamente utilizza una diversa formulazione in cui viene utilizzato il plurale. Sul punto, interessanti anche le riflessioni di F. CASAROSA, *La tutela aggregata dei dati personali nel Regol. Ue 2016/679: una base per l'introduzione di rimedi collettivi?*, cit., p. 235 ss., che evidenzia come il legislatore europeo non ha scelto di delineare un'azione collettiva di matrice europea, quanto piuttosto di definire un diritto europeo all'azione collettiva.

[18] Ne è un esempio la diffusione sempre più significativa di contenuti volutamente disinformativi che hanno assunto nei mesi più recenti un ruolo particolarmente pervasivo nei conflitti bellici in corso. Sul tema *ex plurimis*, e senza alcuna pretesa di esaustività, rinviamo agli articoli pubblicati in *Medialaws*, 2017, 1, e in particolare quelli di O. POLLICINO, *Fake news, Internet and Metaphors (to be handled carefully)*, p. 23 ss., che pone bene in luce l'incidenza della disinformazione sulle scelte politiche dei cittadini; C. PINELLI, *"Postverità", verità e libertà di manifestazione del pensiero*, p. 41 ss., che analizza accuratamente sia gli effetti della creazione di informazioni false presentate come vere che della manipolazione informativa, accezione con cui si fa riferimento all'uso di notizie vere presentate con alterazioni e omissioni per indurre il destinatario a trarre implicazioni fuorvianti; M. CU-

litico [19] quanto in relazione ai comportamenti individuali. Ragione per cui nella dimensione *onlife* [20] diviene fondamentale cercare di garantire la possibilità dei cittadini di conservare un controllo su aspetti quali il contenuto delle informazioni che diffondono e le modalità con cui queste sono impiegate e riutilizzate dai grandi attori del mercato digitale, quale garanzia di libertà personale nella sua accezione di diritto all'autodeterminazione.

Di ciò si è dimostrata ben consapevole anche l'Unione europea che negli ultimi anni ha dato prova di aver maturato una cultura giuridica volta a garantire con più forza la tutela delle libertà costituzionali comuni alla tradizione europea nel mercato digitale e assicurare, in modo più efficace, l'esigenza di autodeterminazione per il tramite di strumenti complementari al GDPR, atto normativo che, sul punto, segna il passo di fronte all'evoluzione degli ultimi anni e sconta un processo genetico rivolto più al passato che al futuro.

In questa direzione, a partire dal febbraio 2020, come noto, la Commissione europea con la comunicazione *Una strategia europea per i dati* [21] ha inaugurato una nuova stagione giuridico-normativa confluita, poi, nell'adozione di numerosi atti per lo più di natura regolamentare che disegnano nel loro complesso un *corpus* normativo, il quale, in una con il *Regolamento generale sulla protezione dei dati*, dovrebbe offrire un quadro sistematico e coerente di regolazione della nuova dimensione digitale nella quale siamo immersi. Tra i più recenti e significativi di

---

NIBERTI, *Il contrasto alla disinformazione in rete e (vecchie e nuove) velleità di controllo*, p. 26 ss., il quale evidenzia «le pesanti responsabilità che gli stessi media c.d. *mainstream* hanno avuto, nel recente passato e sino ad oggi, nella costruzione di gigantesche operazioni di disinformazione di massa»; e F. PIZZETTI, *Fake news e allarme sociale: responsabilità, non censura*, pp. 48 ss. In tema v. anche G. PITRUZZELLA-O. POLLICINO-S. QUINTARELLI, *Parole e potere. Libertà d'espressione, hate speech e fake news*, Milano, 2017.

[19] Anche sul punto la dottrina è ormai sterminata. *Ex plurimis*, e a mero scopo esemplificativo, si vedano P. CIARLO, *Democrazia, partecipazione popolare e populismo al tempo della rete*, in *Rivista AIC*, 2018, 2; M. BETZU-G. DEMURO, *I big data e i rischi per la democrazia rappresentativa*, in *Medialaws*, 2020, spec. p. 221, ove gli AA. sottolineano come «la principale funzione dei big data è quella di costituire il presupposto per attività di *microtargeting* politico, consistenti nell'influenzare specifici gruppi di elettori tramite l'invio di messaggi mirati, basati sulle preferenze e sulle caratteristiche personali. In questo modo si possono raggiungere numerosi risultati, primo fra tutti quello di plasmare l'immagine del candidato in funzione delle aspettative – *day by day* – dell'elettorato di riferimento»; B. CARAVITA DI TORITTO, *Social network, formazione del consenso, istituzioni politiche: quale regolamentazione possibile*, in *Federalismi.it*, 2019, 2, spec. p. 3, ove l'A. evidenzia come «la possibilità di far circolare gratuitamente informazioni senza la mediazione dei tradizionali operatori della comunicazione ha totalmente cambiato le carte in tavola nel dibattito politico»; nonché L. SCAFFARDI, *Internet fra auto-limitazione e controllo pubblico*, in *Rivista AIC*, 2023, p. 4.

[20] Richiamando la felice espressione di L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, 2014, spec. p. 47 ss.

[21] COMMISSIONE EUROPEA, *Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni Una strategia europea per i dati*, Bruxelles, 19 febbraio 2020, COMM(2020)66 final.

questi atti, ai fini del nostro discorso, è doveroso ricordare in particolare il *Regolamento sulla governance dei dati* [22] diretto a incoraggiare la nascita di un sentimento filantropico di altruismo dei dati, ossia una maggior disponibilità di informazioni volta sia a favore del settore pubblico che privato, come frutto di scelte libere e consapevoli.

La necessità di garantire una tutela collettiva agli interessati – di cui abbiamo trattato nel paragrafo precedente – e di riconoscere una funzione sociale alla protezione dei dati, a cui faceva già (un blando) riferimento pure il GDPR [23], ha, così, trovato ampia e specifica applicazione nella nuova disciplina della *governance* dei dati, la quale richiama con urgenza la necessità di assistenza, da parte di enti collettivi, dell'interessato nelle fasi cruciali legate alla gestione dei propri dati personali e non.

Come già evidenziato in dottrina [24], il DGA si articola in tre direzioni principali: (I) la disciplina del riuso dei dati gestiti dalla pubblica amministrazione, al fine di incrementare il loro impiego per finalità ulteriori rispetto a quelli di iniziale raccolta, per scopi commerciali o non commerciali, da parte di soggetti terzi; (II) la disciplina dei servizi di intermediazione dei dati, personali e non personali, tramite l'attività dei "fornitori di servizi di intermediazione dei dati", ovvero soggetti che senza possibilità di monetizzare la loro attività, si offrono di instaurare rapporti commerciali a fini di condivisione dei dati tra i cd. *data holders* e i cd. *data users*, persone fisiche o giuridiche; (III) la disciplina dell'altruismo dei dati per finalità solidaristiche ed altruistiche favorita tramite l'introduzione delle "organizzazioni per l'altruismo dei dati". La *ratio* che sottende, nel suo complesso, il DGA è dunque chiaramente quella di favorire il riuso dei dati, per un verso in un'ottica di una comune solidarietà [25], per l'altro in una prospettiva di maggior consapevolezza degli interessati che acconsentono a tale *secondary (and public) use*.

Nel cercare di raggiungere l'obiettivo da ultimo citato, ancora una volta le Istituzioni hanno deciso di lasciare spazio all'autonomia privata tramite la via del consenso. Se, tuttavia, il *Regolamento sulla governance dei dati* è indiscutibilmente

---

[22] Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo alla governance europea dei dati e che modifica il Regolamento (UE) 2018/1724 (Regolamento sulla governance dei dati). Nel seguito ci riferiremo a tale atto normativo anche come *Data Governance Act*, o, più sinteticamente, con l'acronimo DGA.

[23] Oltre all'art. 80 che fa esplicito riferimento alla "Rappresentanza degli interessati" il GDPR richiama la necessità di garantire una lettura non individualistica della protezione dei dati anche al *considerando* n. 4, il quale ne ricorda, per l'appunto, la sua funzione sociale. In tema, A. RICCI, *Sulla «funzione sociale» del diritto alla protezione dei dati personali,* in *Contratto e impresa*, 2017, 2, p. 586 ss.; F. BRAVO, *Il principio di solidarietà in materia di protezione dei dati personali nelle decisioni del Garante e della Corte di Cassazione*, in *Contratto e impresa*, 2023, 2, p. 407 e p. 412 ss.; ID, *Il principio di solidarietà*, in F. BRAVO (a cura di), *Dati personali. Protezione, libera circolazione e governance – Vol. 1. Principi*, Pisa, 2023, p. 541 ss.; e ID., *Il principio di solidarietà tra data protection e data governance*, in *Il diritto dell'informazione e dell'informatica*, 2023, 3, p. 481 ss.

[24] Da F. BRAVO, *Le cooperative di dati*, in *Contratto e impresa*, 2023, 3, p. 757 ss.

[25] In questo senso, F. BRAVO, *Il principio di solidarietà*, cit., p. 550.

"consenso-centrico" in quanto attribuisce all'interessato il potere di decidere di destinare le proprie informazioni ad un secondo utilizzo, esso, a differenza dei precedenti atti normativi, lascia trasparire per la prima volta la consapevolezza del legislatore europeo circa la fragilità di tale istituto. Proprio per questo motivo, sono state introdotte le nuove figure a cui abbiamo fatto cenno poc'anzi, che possono affiancare l'interessato nelle fasi più delicate della formazione della propria autodeterminazione: i servizi di intermediazione dei dati, per quanto riguarda l'instaurazione dei rapporti commerciali [26]; i servizi di altruismo dei dati per quanto riguarda i trattamenti concernenti la messa a disposizione dei dati per obiettivi di interesse generale senza la richiesta o la ricezione di un compenso [27]; gli organismi competenti, per quanto riguarda il riuso dei dati detenuti dagli enti pubblici [28]. Con la comparsa di questi soggetti possiamo affermare senza alcun dubbio che il *Data Governance Act* mira ad un rafforzamento della posizione degli interessati facendo leva proprio sull'azione di soggetti intermediari che possano assicurare maggiore effettività di tutela.

Per quanto riguarda più specificamente l'altruismo dei dati, al fine di garantire che la solidarietà sia espressione di una compiuta autodeterminazione basata sul consenso ai sensi degli artt. 6 e 9 GDPR, l'art. 22 del DGA richiede che la Commissione europea tramite atti delegati stabilisca, tra l'altro, i requisiti da rispettare in materia di informazione, affinché gli interessati ricevano, prima di rilasciare il consenso, informazioni sufficientemente dettagliate, chiare e trasparenti sull'utilizzo dei dati nonché sugli strumenti per fornirlo e revocarlo [29]: la trasparenza informativa, in coerenza con i principi generali che regolano la materia e che troviamo enunciati nell'art. 5 GDPR, diviene così baluardo del nuovo paradigma normativo.

Se, come detto, l'elemento caratterizzante le organizzazioni per l'altruismo dei dati è l'assenza di scopo di lucro, bilanciato tuttavia dalla possibilità di trattare o controllare i dati acquisiti, per gli intermediari dei dati vale il principio della necessaria neutralità [30], in quanto essi non possono sfruttarli a propri fini ma soltanto, nell'esercizio delle proprie attività, essere mossi da una vocazione commerciale che si realizza nella messa a disposizione dei dati per gli utenti.

A tal proposito, l'art. 10, co. 1, del DGA chiarisce più nel dettaglio che questi enti possono offrire: (a) servizi di intermediazione tra i titolari dei dati e i potenziali

---

[26] Art. 2, n. 11, del DGA.

[27] Art. 2, n. 16, del DGA.

[28] L'art. 7 del DGA afferma che gli Stati membri possono istituire uno o più organismi competenti nuovi o avvalersi di enti pubblici esistenti o di servizi interni di enti pubblici che soddisfano le condizioni stabilite dal Regolamento stesso.

[29] Lo ricorda ancora F. BRAVO, *Il principio di solidarietà*, cit., p. 550 ss.

[30] L'art. 12, lettera a) del DGA chiarisce, infatti, che il fornitore di servizi di intermediazione dei dati non utilizza le informazioni per le quali fornisce servizi di intermediazione per scopi diversi dalla messa a disposizione agli utenti, salvo che i dati stessi vengano utilizzati per migliorare il servizio fornito.

utenti dei dati; (b) servizi di intermediazione tra interessati che intendono mettere a disposizione i propri dati personali o persone fisiche che intendono mettere a disposizione dati non personali da un lato e potenziali utenti dei dati dall'altro, al fine, in particolare, di favorire l'esercizio dei diritti degli interessati di cui al Reg. (UE) 2016/679; (c) servizi di cooperative di dati.

Ecco, a proposito del tema cui dedichiamo le presenti note, comparire tra i servizi di intermediazione per l'appunto le cooperative di dati che, più specificamente, l'art. 2, par. 1, n. 15, DGA, definisce come servizi di intermediazione «offerti da una struttura organizzativa costituita da interessati, imprese individuali o da PMI, che sono membri di tale struttura, avente come obiettivi principali quelli di aiutare i propri membri nell'esercizio dei loro diritti in relazione a determinati dati, anche per quanto riguarda il *compiere scelte informate prima di acconsentire al trattamento dei dati*, di procedere a uno scambio di opinioni sulle finalità e sulle condizioni del trattamento dei dati che rappresenterebbero al meglio gli interessi dei propri membri in relazione ai loro dati, o di negoziare i termini e le condizioni per il trattamento dei dati per conto dei membri» (corsivo nostro). Pare evidente che la nozione adottata dall'Unione abbia carattere generale potendo essere ricompresa al suo interno qualsiasi organizzazione a prescindere dalla forma societaria, seppure, come già rilevato in dottrina [31], il modello cooperativo di cui al titolo VI del libro V del Codice civile possa essere ritenuto quello più idoneo a rivestire il ruolo di cooperativa di dati. Riagganciandoci alle considerazioni svolte nel primo paragrafo, crediamo dunque si possa affermare che, tramite l'istituzione dei servizi di intermediazione dei dati, ed in particolare delle cooperative di dati, il legislatore europeo sembra aver colto l'esigenza di affiancare al singolo interessato enti collettivi capaci non solo di assisterlo, come potrebbe fare anche un soggetto terzo, ma anche di permettergli di farsi parte attiva dell'organizzazione e del funzionamento dell'ente, contribuendo ad una forma di rappresentanza e tutela mutualistica di un interesse comune ad altri soggetti cui i dati intermediati si riferiscono.

Per quanto, infatti, la scelta del DGA di attribuire la funzione di intermediari soltanto a dei soggetti "neutrali", perimetri fortemente il loro ruolo alla consulenza che precede la manifestazione del consenso, facendo sorgere dubbi persino sulla possibilità di delegare tale atto a terzi [32], riteniamo si debba aderire alla ricostruzione dottrinale secondo cui la natura personale del consenso potrebbe in tale caso essere superata sì da riconoscere (anche) la possibile rappresentanza nell'espressione di esso [33]. Tale soluzione, invero, non pare nuova, giacché anche lo stesso Reg. (UE)

---

[31] L. PETRONE, *Il mercato digitale europeo e le cooperative di dati*, in *Contratto e impresa*, 3, 2023, p. 810 ss.

[32] *Ivi*, p. 813.

[33] Così G. RESTA, *La regolazione digitale nell'Unione europea – pubblico, privato, collettivo nel sistema europeo di governo dei dati*, in *Rivista trimestrale di diritto pubblico*, 2022, 4, p. 971, le cui considerazioni sono riprese da L. PETRONE, *Il mercato digitale europeo e le cooperative di dati*, cit., p. 815.

2016/679, contempla – per quanto isolate – ipotesi di rappresentanza nella manifestazione del consenso, come nell'art. 80 su cui ci siamo già in precedenza soffermati. Di modo che, ci sembra condivisibile l'assunto di chi, seppur cautamente, afferma che il mero silenzio in merito alla possibilità di fare utilizzo dell'istituto della c.d. rappresentanza volontaria non potrebbe essere inteso come un divieto assoluto [34]. Tanto più che, nel modello cooperativo, il principio della "porta aperta", che consente in ogni momento al singolo di recedere dal rapporto societario, nonché quello della parità di trattamento tra i soci e la democraticità interna che contraddistingue questi enti sono istituti in grado di garantire pienamente la permanenza di un controllo diretto dell'interessato sui propri dati, ciò che altri modelli non sembrano assicurare con la stessa efficacia.

La possibilità di attribuire poteri di rappresentanza alle società cooperative di dati consentirebbe dunque, in buona sostanza, di strutturare enti con poteri analoghi a quelli di un'associazione con funzioni di "rappresentanza sindacale" collettiva [35], laddove la maggior equità, che caratterizza le forme societarie cooperative, non può che favorire e valorizzare l'autodeterminazione e, dunque, la formazione di un consenso più libero. Il "conferimento" dei dati a favore di siffatti soggetti potrebbe, infatti, permettere all'interessato, in quanto socio, di comprendere appieno le informazioni relative al trattamento e quindi decidere pienamente e liberamente la destinazione dei propri dati, scongiurando così il vizio latente della carenza informativa ed assicurando il superamento delle zone d'ombra che non di rado permangono in relazione al trattamento.

A tal fine, si potrebbe pensare anche allo sviluppo di strutture europee che superino i confini nazionali, specularmente a quanto avviene per la tecnologia che non conosce limiti territoriali, di modo che, se questi soggetti fossero effettivamente rappresentativi di una larga parte degli interessi dei soci/interessati – ma per questo dobbiamo riconoscere loro il potere di rappresentanza e non solo di mediazione – potremmo disporre di uno strumento finalmente capace di (provare a) controbilanciare il potere delle *Big tech* offrendo una protezione sul mercato che, a ben vedere, ad oggi ancora non esiste. In tal senso, infatti, si può ipotizzare che i poteri di queste grandi società, che difficilmente possono essere ridimensionati dai governi nazionali, potrebbero essere più efficacemente compensati dalla forza di organizzazioni collettive degli interessati.

Peraltro, a nostro avviso, la forma societaria di cui trattiamo, oltre che assumere il ruolo di soggetto intermediario ai sensi delle norme citate, potrebbe anche costituire un modello organizzativo utilizzabile dagli enti per l'altruismo dei dati, tutte le volte in cui questi agiscano per uno scopo mutualistico, statutariamente imposto come esclusivo, e pertanto senza finalità di lucro, ma svolgendo quella funzione sociale che, come ci ricorda l'art. 45 Cost., è iscritta nello stesso DNA della catego-

[34] Cfr. ancora L. PETRONE, *Il mercato digitale europeo e le cooperative di dati*, loc. cit.

[35] In questa direzione propende L. PETRONE, *Il mercato digitale europeo e le cooperative di dati*, cit., p. 811.

ria di enti di cui andiamo trattando. Del resto, i requisiti per richiedere la registrazione nel registro pubblico nazionale delle organizzazioni per l'altruismo fissati dall'art. 18 DGA non sembrano precludere questa possibilità. La norma citata, infatti, prevede soltanto che questi enti debbano: *a)* svolgere attività di altruismo dei dati; *b)* essere una persona giuridica costituita a norma del diritto nazionale per conseguire obiettivi di interesse generale, stabiliti nel diritto nazionale, ove applicabile; *c)* operare senza scopo di lucro ed essere giuridicamente indipendente da qualsiasi entità che operi a scopo di lucro; *d)* svolgere le proprie attività di altruismo dei dati mediante una struttura funzionalmente separata dalle sue altre attività; *e)* rispettare il codice di cui all'art. 22, par. 1, al più tardi entro 18 mesi dopo la data di entrata in vigore degli atti delegati di cui all'art. 18.

In buona sostanza, che si tratti di altruismo dei dati o di intermediazione a fini commerciali dei medesimi, a nostro avviso le cooperative potrebbero rappresentare uno strumento di rafforzamento del controllo dei singoli individui in merito ai dati che li riguardano supportando i soci/interessati nella concessione e nella revoca del consenso, rappresentandone gli interessi, non per forza economici, e le aspettative.

3. La (inadeguata) protezione dell'interessato in ambito sanitario: una nuova opportunità dalle cooperative di dati?

3.1. Il ricorso all'altruismo e all'intermediazione dei dati nella ricerca medica.

Il settore sanitario – e in particolare quello della ricerca scientifica in ambito medico – è, a nostro avviso, un interessante caso di studio in cui provare ad applicare questa nuova opportunità offerta dalle cooperative di dati.

In primo luogo, infatti, non si può negare che la solidarietà del *data altruism* e la maggiore disponibilità di dati sia destinata a massimizzare i suoi risultati in termini di utilità sociale proprio nel settore dell'assistenza sanitaria [36] sia per la capacità di offrire informazioni funzionali al miglioramento della qualità dei servizi forniti agli utenti, sia per l'utilità dei dati nella elaborazione delle politiche pubbliche, sia soprattutto, per quanto ci interessa in relazione alle presenti note, a fini di ricerca.

In secondo luogo, e non certo per ordine di importanza, va rimarcato come il paziente sia un interessato che, per definizione, versa in una situazione di vulnerabilità, a causa della quale necessita di una particolare assistenza affinché venga garantita la formazione di un consenso effettivamente libero e le sue scelte rispondano ad una reale autodeterminazione allorché aderisca a protocolli di sperimentazione [37].

---

[36] Così si esprime F. BRAVO, *Il principio di solidarietà*, cit., p. 551.

[37] Come è stato correttamente osservato al riguardo, non è raro che accada «che i pazienti destinati all'arruolamento in uno studio clinico versino in cattive condizioni di salute o appartengano a un grup-

Prima di entrare nel merito della questione, occorre tuttavia svolgere una precisazione preliminare circa la possibilità di riferire il nostro discorso sia alle cooperative di dati, costituite come enti di intermediazione ai sensi del Capo III del DGA, sia alle cooperative che svolgono attività nell'ambito della ricerca con finalità altruistiche alle condizioni indicate nel paragrafo precedente.

Infatti, il Regolamento di cui trattiamo riferisce al settore *de quo*, di norma, soltanto le previsioni sul riutilizzo di determinate categorie di dati protetti detenuti da enti pubblici e sull'altruismo dei dati, apparentemente escludendo l'intermediazione (e le cooperative di dati tra i soggetti abilitati a svolgere tale funzione). In realtà, però, l'art. 15 del DGA, nel chiarire che le disposizioni dedicate ai servizi di intermediazione non si applicano alle organizzazioni per l'altruismo dei dati riconosciute o ad altre entità senza scopo di lucro, contempla una deroga a tale preclusione allorché tali enti realizzino pur sempre finalità (e intendano instaurare relazioni) commerciali [38].

Pertanto, se il campo della ricerca scientifica, e in special modo medica, risulta essere sicuramente terreno d'elezione dei servizi di altruismo dei dati da parte di società cooperative che fanno dello scopo mutualistico il loro obiettivo esclusivo, nondimeno esso può altresì rappresentare lo sfondo per lo sviluppo di vere e proprie cooperative di dati, ai sensi del Capo III del DGA, nelle vesti di fornitori di servizi di intermediazione, ogniqualvolta esse agiscano con l'obiettivo di creare relazioni commerciali, giacché è del tutto evidente che la ricerca medica (per esempio si pensi alla sperimentazione di farmaci) ben può sottendere anche rapporti di natura commerciale. In questi casi, allora, le società *de quibus*, come afferma il *considerando* n. 27 DGA, potrebbero garantire un accesso non discriminatorio ai dati per le imprese del settore, come per esempio una *start-up* del settore chimico-

---

po economicamente o socialmente svantaggiato o si trovino in una situazione di dipendenza istituzionale o gerarchica potenzialmente in grado di influire in maniera non appropriata sulla decisione di acconsentire o meno al trattamento dei dati per scopi di ricerca. Il consenso, infatti, potrebbe mancare del necessario requisito di libertà anche a causa di un marcato squilibrio tra l'interessato e il titolare del trattamento (*Parere 3/2019 del Comitato europeo per la protezione dei dati relativo alle domande e risposte sull'interazione tra il regolamento sulla sperimentazione clinica e il regolamento generale sulla protezione dei dati*, 23 gennaio 2019). In tal caso, occorre ed è anzi opportuno, che il titolare valuti la possibilità di fondare il trattamento dei dati personali sensibili dei pazienti arruolati su differenti basi giuridiche, fermo restando, se del caso, che la volontarietà dell'adesione alla ricerca debba comunque essere assicurata»: così G.M. RICCIO-G. SCORZA-E. BELISARIO, *GDPR e normativa privacy*, cit., 2022, p. 881 ss.

[38] Chiarisce, in questo senso, anche il *considerando* n. 29 che «le organizzazioni per l'altruismo dei dati di cui al presente regolamento non dovrebbero essere considerate offrire servizi di intermediazione dei dati a condizione che tali servizi non creino un rapporto commerciale tra potenziali utenti dei dati, da un lato, e interessati e titolari dei dati che mettono a disposizione i dati per motivi altruistici, dall'altro. Altri servizi non finalizzati a instaurare rapporti commerciali, come i *repository* volti a consentire il riutilizzo dei dati della ricerca scientifica conformemente ai principi dell'accesso aperto, non dovrebbero essere considerati servizi di intermediazione dei dati ai sensi del presente regolamento».

farmaceutico non ancora fagocitata da una multinazionale del settore, che volesse introdurre sul mercato un proprio prodotto.

Fatta questa doverosa premessa, che dimostra come le cooperative di dati ben possano rivelarsi utili anche in questo frangente, è ora opportuno soffermarsi dapprima a ricostruire, per quanto brevemente, la disciplina in materia di riuso dei dati a fini di ricerca in ambito sanitario, per poi indicare più nello specifico quale ruolo possono assumere, in tale contesto, le cooperative.

3.2. Il riuso dei dati per finalità di ricerca in sanità nel diritto eurounitario …

Occorre anzitutto rilevare come, in generale e a prescindere dalla finalità (commerciale o di interesse generale) che si voglia raggiungere con la messa a disposizione delle informazioni per un uso secondario, il DGA, coerentemente con il suo approccio consenso-centrico, individua questa come base giuridica legittimante il riutilizzo, ai sensi degli artt. 6, co. 1, lett. *a)* e 9, co. 2, lett. *a)* del GDPR. Ciò è vero pure per quanto concerne il *secondary use* dei dati per ricerca scientifica, che non prescinde mai dall'acquisizione di un consenso dell'interessato reso ai sensi del GDPR. Questo, infatti, è richiesto: (i) per il riuso dei dati personali detenuti da enti pubblici, laddove non sia stato possibile anonimizzarli (art. 5, par. 6 del DGA), circostanza non rara a verificarsi non essendo infrequente nel settore *de quo* che, affinché un dato mantenga una certa utilità ai fini di ricerca, difficilmente lo si possa anonimizzare [39]; (ii) per il trattamento caratterizzato da finalità altruistiche (art. 21, par. 3, del DGA); (iii) per il riuso a fini commerciali la cui acquisizione è favorita dai servizi di intermediazione dei dati (art. 12, lett. *m)* ed *n)* del DGA).

Ebbene nonostante il nobile intento del legislatore eurounitario nel tentativo di valorizzare l'autodeterminazione nel riuso dei dati, non si può non notare come proprio la previsione di una necessaria e inderogabile acquisizione del consenso possa talvolta inficiare il *secondary use* nel settore della ricerca medica, con l'effetto di frapporre un ostacolo al progresso scientifico. E ciò perché, per un verso, in questo ambito, i soggetti interessati, in quanto pazienti, sono naturalmente "affetti" da una vulnerabilità che in molti casi può rendere difficile garantire la formazione di una volontà libera, mentre, per altro verso, non è raro che le esigenze di utilizzo dei dati a fini di ricerca si manifestino in tempi ben lontani da quelli in

[39] Nella prassi, come ricorda F. Di Tano, *Protezione dei dati personali e ricerca scientifica: un rapporto controverso ma necessario*, in *Biolaw Journal*, 2022, 1, p. 82, i dati personali riutilizzati nella ricerca solitamente sono qualificati come dati pseudonimi ai fini della normativa europea in materia di dati personali, ovvero, ai sensi dell'art. 4, n. 5 del GDPR, non più attribuibili a un interessato specifico senza l'utilizzo di informazioni aggiuntive, ma comunque a tutti gli effetti, in quanto dati personali, ricadenti nell'ambito di applicazione della normativa in materia il cui riutilizzo deve poggiare su una adeguata base giuridica.

cui essi sono stati raccolti, ragion per cui si rivela materialmente impossibile acquisire un consenso che possa dirsi davvero specifico.

Di tale strutturale criticità sembrano, a dire il vero, essersi rese conto le stesse Istituzioni europee, se si considera che, invero, non manca qualche eccezione. Già l'art. 5, par. 1, GDPR, infatti, mostra l'intenzione di introdurre una deroga alle disposizioni generali sul consenso proprio in ragione del principio di solidarietà [40], laddove afferma che «un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di *ricerca scientifica* […] non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali» (corsivo nostro), senza contare che l'art. 9, par. 2, lett. *j)* del GDPR, proprio in relazione ai dati particolari, prevede la possibilità di un loro trattamento, a prescindere dal consenso, allorché questo sia «necessario a fini (…)di ricerca scientifica (…)sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato».

3.3. … e in quello nazionale.

Assai meno flessibile del legislatore europeo è parso quello italiano, che, approfittando dello spazio discrezionale riconosciuto dal *considerando* n. 10 [41] e dall'art. 9, par. 4, del GDPR [42], ha introdotto nel campo della ricerca medica, biomedica ed epidemiologica un farraginoso sistema [43] che trova la propria disciplina all'art. 110 del Codice *privacy* [44].

Tale disposizione riconosce, infatti, la possibilità di operare in assenza di consenso dell'interessato al trattamento per fini di ricerca soltanto qualora essa, alter-

---

[40] In questo senso, F. BRAVO, *Il principio di solidarietà*, cit., p. 568.

[41] Il quale attribuisce un certo margine di manovra agli Stati membri, laddove riconosce la possibilità che, per quanto riguarda il trattamento dei dati personali per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, i singoli Paesi rimangano liberi di mantenere o introdurre norme nazionali al fine di specificare ulteriormente l'applicazione delle norme del GDPR anche con riguardo al trattamento di categorie particolari di dati personali, consentendo di stabilire le condizioni per specifiche situazioni di trattamento e determinando con maggiore precisione quelle alle quali il trattamento di dati personali è lecito.

[42] Ai sensi del quale «gli Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute».

[43] Netto il giudizio di F. DI TANO, *Protezione dei dati personali e ricerca scientifica: un rapporto controverso ma necessario*, cit., p. 83, il quale rileva che, rispetto agli altri Paesi europei, l'ordinamento italiano prevede norme, anche contenute in provvedimenti del Garante per la protezione dei dati personali più rigide di quelle contemplate dal GDPR.

[44] Nello scritto, per esigenze di economia della trattazione, ci riferiamo esclusivamente e direttamente al testo vigente della norma; per la precedente disciplina e le evoluzioni di questa disposizione si veda l'ampia ricostruzione di G. TADDEI ELMI, *Art. 110*, in R. SCIAUDONE-E. CARAVÀ (a cura di), *Il Codice della privacy*, Pisa, 2019, p. 446 ss.

nativamente: (i) sia effettuata in forza di disposizioni di legge o di regolamento o del diritto dell'Unione europea in conformità al già ricordato art. 9, par. 2, lett. *j)*, del Regolamento; (ii) rientri in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'art. 12-*bis* del d.lgs. 30 dicembre 1992, n. 502 [45], purché sia resa pubblica una valutazione d'impatto ai sensi degli artt. 35 e 36 del Regolamento; (iii) avvenga, come accade nella maggioranza dei casi, in circostanze tali per cui, a causa di particolari ragioni, informare gli interessati risulti impossibile o implichi uno sforzo sproporzionato, oppure rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca [46].

In quest'ultimo caso, la deroga all'acquisizione del consenso può essere legittimata solo se, cumulativamente: *a)* il titolare del trattamento adotti misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato (ad esempio, ai sensi dell'art. 89 del GDPR, ponga in essere misure tecniche e organizzative, in particolare al fine di garantire il rispetto del principio della minimizzazione dei dati: tali misure possono includere la pseudonimizzazione, purché le finalità in questione possano essere conseguite in tal modo o, meglio ancora, laddove possibile, l'anonimizzazione); *b)* il programma di ricerca sia oggetto di motivato parere favorevole del competente Comitato etico a livello territoriale; e (fino a poco tempo fa, ma sul punto torneremo più ampiamente nel prosieguo, perché la disposizione è stata oggetto di un recentissimo intervento legislativo); *c)* il programma di ricerca sia stato sottoposto a preventiva consultazione del Garante per la protezione dei dati personali [47] ai sensi dell'art. 36, par. 5, del Regolamento.

Rispetto a quest'ultimo requisito, ovvero alla consultazione (*rectius* autorizzazione) preventiva del Garante, occorre rilevare che, dall'analisi di alcuni dei provvedimenti, emerge che l'Autorità di controllo è stata solita autorizzare tali trattamenti in presenza di particolari condizioni spesso di assai difficile dimostrazione o, in ogni caso, la cui *probatio* (diabolica) richiedeva un investimento rilevante di tempo ed energie, come, ad esempio, il coinvolgimento di un numero significativo di pazienti da arruolare nello studio; l'incidenza di mortalità della patologia oggetto dello studio; la difficoltà oggettiva e provabile di contattare i pazienti, ecc. [48].

---

[45] Ovvero la disposizione che contempla l'adozione di un Programma Nazionale per la Ricerca Sanitaria, di validità triennale, che deve essere elaborato tenendo conto degli obiettivi previsti nel Programma Nazionale per la Ricerca, di cui al d.lgs. 5 giugno 1998, n. 204.

[46] Sul consenso come requisito di base per il trattamento dei dati nell'ambito della ricerca medica v. P. GUARDA, *Art. 110*, in R. D'ORAZIO-G. FINOCCHIARO-O. POLLICINO-G. RESTA (a cura di), *Codice della privacy e data protection*, Milano, 2021, spec. p. 1374 ss.

[47] D'ora in avanti anche solo Garante o Autorità di controllo.

[48] A scopo meramente esemplificativo può essere citato il Provvedimento 26 ottobre 2023 *doc. web* 9960973, in cui il Garante concedeva parere favorevole ai sensi dell'art. 110 del Codice privacy e dell'art. 36 del Regolamento, soltanto per i trattamenti riferiti ai pazienti deceduti o non contattabili arruolati, a condizione che, tra gli altri aspetti, l'impossibilità di acquisire il consenso degli interessati venisse attestata all'esito dei ragionevoli sforzi consistenti in tre tentativi di contatto non andati a

La disciplina poc'anzi descritta viene poi completata dall'art. 110-*bis* del Codice *privacy*, introdotto con la l. 20 novembre 2017, n. 167[49], che prevede la facoltà del Garante di autorizzare[50] il trattamento ulteriore di dati personali a fini di ricerca scientifica da parte di soggetti terzi che svolgono principalmente tali attività quando, a causa di particolari ragioni, informare gli interessati risulti impossibile o implichi uno sforzo sproporzionato, oppure rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca, a condizione – anche in questo caso – che siano adottate misure per la tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato, ai sensi dell'art. 89 del GDPR[51].

In dottrina, rispetto alla non facile interpretazione di quest'ultima norma[52], è stata avanzata l'ipotesi che essa sarebbe volta a disciplinare il caso di comunicazioni di dati per scopi di ricerca ovvero a consentire «il trattamento ulteriore di dati» quando vi siano oggettivi impedimenti alla possibilità di informare gli interessati e di acquisirne il consenso, in modo da realizzare il migliore bilanciamento tra l'esigenza di progresso scientifico e la protezione della riservatezza dei soggetti coinvolti[53]. Se-

---

buon fine e registrati nella cartella clinica dei pazienti. Analogamente, nel successivo Provvedimento 21 dicembre 2023, *doc. web* 9979453 il Garante, nel concedere parere favorevole al trattamento e prescrivendo il rispetto di determinate condizioni, ha tenuto in considerazione, tra gli altri e numerosi aspetti, l'impossibilità di riuscire ad informare gli interessati e acquisirne un valido consenso determinato dal significativo numero di malati da analizzare (circa 14.000 gestiti nei circa 9-10 anni di attività cardiochirurgica dell'Azienda); l'elevata probabilità che essi fossero deceduti in ragione dell'età media (circa il 50% avevano un'età superiore a 70 anni e il 20% a 80 anni oppure versavano in situazioni di fragilità cognitiva). Degno di interesse anche il Provvedimento del 24 gennaio 2024 *doc. web* 9988614, in cui Garante, nel concedere parere favorevole al trattamento, ha valutato che per lo studio in questione il 46,67% dei pazienti era deceduto, il 23,33% dei pazienti avrebbe dovuto essere escluso in quanto non elegibile e il 30% di pazienti era ancora in vita, ma erano state rappresentate difficoltà oggettive in ordine al reperimento dei recapiti di contatto. Peraltro, l'Autorità ha comunque richiesto che il promotore dello studio svolgesse almeno tre tentativi prima di attestare la non contattabilità dei pazienti e ne tenesse traccia nella documentazione dello studio.

[49] Le critiche piovute sul legislatore per la frettolosità di un intervento sul Codice privacy al di fuori del più generale contesto dell'adeguamento al GDPR, per il quale era già all'epoca pendente una delega al Governo, sono ricostruite da P. GUARDA, *Art. 110-bis*, in R. D'ORAZIO-G. FINOCCHIARO-O. POLLICINO-G. RESTA (a cura di), *Codice della privacy e data protection*, cit., p. 1377 ss.

[50] Secondo il modello dell'Autorizzazione generale n. 9/2016 al trattamento dei dati personali effettuato per scopi di ricerca scientifica e successive modificazioni, oggi trasfuso nel Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, del 5 giugno 2019 (*doc. web* n. 9124510).

[51] Per un commento alla disposizione si veda S. MELCHIONNA-F. CECAMORE, *Le nuove frontiere della sanità e della ricerca scientifica*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato: commentario al regolamento UE n. 2016/679 (GDPR) e al novellato Codice privacy: scritti in memoria di Stefano Rodotà*, Milano, 2019, p. 579 ss.

[52] Su tali difficoltà interpretative della norma v. ancora S. MELCHIONNA, F. CECAMORE, *Le nuove frontiere della sanità e della ricerca scientifica*, cit., p. 591.

[53] È di questa opinione P. GUARDA, *Art. 110-bis*, cit., p. 1379.

condo tale orientamento, la disposizione – che sembrerebbe fare riferimento a comunicazioni di dati per scopi di ricerca – «potrebbe risultare critica nella misura in cui sembrerebbe anticipare delle conclusioni sul trattamento ulteriore dei dati per scopi di ricerca scientifica (C50 e art. 5, par. 1, lett. b, GDPR) […] invero, limitatamente alle ipotesi in cui il trattamento di dati personali (tanto sensibili quanto comuni) debba essere svolto da un soggetto differente da quello che li detiene. La disposizione concerne, infatti, il trattamento da parte di "soggetti terzi", con l'uso di una definizione forse impropria, giacché a mente del Regolamento tale categoria non dovrebbe includere i titolari del trattamento (cfr. art. 4, n. 10, GDPR)»[54]. L'art. 110-*bis* parrebbe, infatti, andare oltre quanto disposto dal Considerando n. 50 e dall'art. 5 GDPR, che, come visto, mostrano un certo *favor* per l'ulteriore trattamento ai fini di ricerca, introducendo invero, per la comunicazione dei dati e per il conseguente ri-utilizzo, un sistema autorizzativo alternativo all'acquisizione del consenso che richiederebbe nei confronti del ri-utilizzatore «soggetto terzo che svolge principalmente tali attività» la capacità di dimostrare l'impossibilità o l'estrema difficoltà di acquisire il consenso o che la sua acquisizione renda impossibile o pregiudichi gravemente il conseguimento delle finalità della ricerca, oltre all'adozione delle misure appropriate a tutela dei diritti, delle libertà e dei legittimi interessi degli interessati ai sensi dell'art. 89 GDPR.

Non riteniamo invece di poter aderire alle considerazioni secondo cui la disposizione non possa riguardare la ricerca medica, biomedica ed epidemiologica, poiché essa troverebbe nel Codice una regolamentazione specifica nell'art. 110[55], che si porrebbe perciò come *lex specialis*. Se infatti consideriamo che, come vedremo tra poco, l'ultimo comma dell'art 110-*bis*, nell'introdurre un'esenzione per gli Istituti di ricovero e cura a carattere scientifico (IRCCS), va a regolare proprio un'ipotesi precisa in questo campo, non vi è ragione per circoscrivere la sfera di applicazione della norma alle sole ricerche non afferenti all'ambito sanitario.

A nostro avviso, pertanto, il rapporto tra le due norme va inteso nel senso che, se l'art. 110 del Codice trova applicazione all'uso primario e secondario (per studi prospettici e retrospettivi) di dati per finalità di ricerca medica, biomedica ed epidemiologica ogniqualvolta il soggetto che li ha raccolti coincida con il ri-utilizzatore, l'art. 110-*bis* rinviene, per contro, applicazione nei confronti della comunicazione di dati afferenti alla ricerca scientifica nel caso in cui il *secondary use* sia attuato da parte di soggetti terzi, ovvero diversi da chi ha originariamente acquisito i dati[56].

Interessante, tra l'altro, notare come l'art. 110-*bis* del Codice privacy stabilisca che tale procedimento autorizzativo possa avvenire anche tramite autorizzazioni generali, ma con la previsione che, in assenza di queste, il Garante comunichi la

---

[54] Testualmente, G. M. RICCIO-G. SCORZA-E. BELISARIO, *GDPR e normativa privacy*, cit., p. 894.

[55] Cfr. ancora G. M. RICCIO-G. SCORZA-E. BELISARIO, *GDPR e normativa privacy*, cit. p. 895.

[56] Per questa lettura v. già. S. MELCHIONNA, *Art. 110*-bis, in R. SCIAUDONE-E. CARAVÀ (a cura di), *Il Codice della privacy*, cit., p. 467.

decisione adottata entro quarantacinque giorni, decorsi i quali la mancata pronuncia equivale a rigetto. Laddove, al contrario, l'assenza di qualsiasi forma di silenzio significativo all'interno dell'art. 110 del Codice privacy, che non a caso non fa riferimento ad una «autorizzazione» bensì alla «preventiva consultazione del Garante» resa ai sensi dell'articolo 36 del Regolamento, faceva sì, fino alla recentissima modifica di cui diremo a breve, che i promotori degli studi non rientranti nella nozione di soggetti terzi, qualora intendessero procedere in assenza di consenso ai sensi del paragrafo 1 secondo periodo della disposizione, si trovassero costretti ad attendere i tempi di risposta del Garante con potenziali effetti impattanti sull'avvio dello studio [57]. Nonostante, infatti, gli sforzi dell'Autorità di controllo nazionale, non si può negare che un termine anche soltanto, nella migliore ipotesi, di alcuni mesi di attesa possa essere significativo per la ricerca che evolve con inarrestabile rapidità [58]. A questo si aggiunge il fatto, come già evidenziato, che solitamente con lo stesso provvedimento "autorizzativo", l'Autorità di controllo, anche nel fornire parere favorevole, è solita imporre il rispetto di condizioni a cui non è sempre agevole adeguarsi, così che spesso si assiste ad un ulteriore prolungamento dei tempi di attesa per l'attivazione della ricerca.

Infine, come anticipato, l'ultimo comma dell'art. 110-*bis* del Codice *Privacy* introduce una deroga per il riuso a fini di ricerca dei dati personali raccolti per l'attività clinica da parte degli IRCCS, pubblici e privati, in ragione del carattere strumentale della loro attività di assistenza sanitaria rispetto alla ricerca [59]. Anche la formulazione di questa disposizione ha dato adito a perplessità [60], tanto che il Ga-

---

[57] Al riguardo, se non bastasse ricordare che, in generale, la legge n. 241/1990, all'art. 20, stabilisce che il silenzio assenso non opera nei casi in cui la normativa euro-unitaria impone l'adozione di provvedimenti amministrativi formali, ricordiamo anche che, con norma speciale, lo stesso Garante nella Deliberazione del 4 aprile 2019 – Regolamento n. 2/2019, concernente l'individuazione dei termini e delle unità organizzative responsabili dei procedimenti amministrativi, doc. *web* 9107640, chiarisce, all'interno della Tabella n. 2 riepilogativa dei termini previsti nel codice in materia di protezione dei dati personali (d.lgs. 39 giugno 2003, n. 196), che il Parere reso a seguito di consultazione ai sensi dell'art. 110, co. 1, del Codice *privacy* viene reso nei tempi previsto dall'art. 36 GDPR, ovvero otto settimane dalla ricezione della richiesta, prorogabile di ulteriori sei settimane, senza tralasciare che la decorrenza dei termini può essere sospesa fino all'ottenimento da parte dell'autorità di controllo delle informazioni richieste ai fini della consultazione.

[58] Sul preventivo esame del Garante come fattore di «ostacolo, quanto meno temporale, alla circolazione dei dati per finalità scientifica» v. G. FINOCCHIARO, *Digitalizzazione della sanità e protezione dei dati personali*, in G. CERRINA FERONI (a cura di), *Il ruolo del Garante per la protezione dei dati personali*, Bologna, 2023, p. 121, che sollecita il legislatore ad universalizzare quanto previsto per gli IRCCS.

[59] Ampiamente sul tema G. FINOCCHIARO-L. GRECO, *Trattamento di dati sanitari per la ricerca scientifica: nuove prospettive*, in *Diritto, Mercato, Tecnologia*, 22 febbraio 2024, p. 11 ss.

[60] Tanto che, per le difficoltà interpretative che la caratterizzano, la norma non risulta essere mai sia stata concretamente applicata, come rilevano G. M. RICCIO-G. SCORZA-E. BELISARIO, *GDPR e normativa privacy*, cit., p. 894, i quali aggiungono che «la disposizione, per le sue caratteristiche, impone al-

rante con un recente intervento [61] ha sentito l'esigenza di chiarire la portata derogatoria della disciplina specificando che gli IRCCS possono fondare i trattamenti su (i) il consenso degli interessati, ai sensi degli artt. 6, par. 1, lett. *a)* e 9, par. 2, lett. *a)* del Regolamento o, in alternativa, su (ii) l'art. 110-*bis*, co. 4, del Codice. Detta disposizione, che trova applicazione in relazione ad ogni tipo di ricerca medica, biomedica, epidemiologica, prospettiva e retrospettiva, promossa da tali Istituti, costituisce proprio una di quelle disposizioni di legge, che si inseriscono nello spazio di normazione lasciato agli Stati membri, ai sensi dell'art. 9, par. 2, lett. *j)*, del Regolamento, alle quali fa riferimento l'art. 11 (co. 1, primo periodo) del Codice.

3.4. Il possibile ruolo delle cooperative a servizio della ricerca in medicina.

In questo, piuttosto intricato, quadro normativo, peraltro, come diremo a breve, destinato ad arricchirsi per via di alcuni recentissimi e altri imminenti interventi del legislatore, crediamo che possano rivestire un ruolo rilevante tanto organizzazioni per l'altruismo dei dati, strutturate secondo il modello cooperativo, ove siano in ballo esclusivamente obiettivi di interesse generale, quanto le cooperative di dati in senso proprio, per come introdotte dal DGA, quali soggetti fornitori di servizi di intermediazione, laddove attraverso la ricerca si persegua (anche) uno scopo commerciale.

Occorre, tuttavia, precisare che, se esempi di cooperative di dati nel campo della salute già si conoscono [62], la costituzione di società di questo tipo richiede il rispetto di oneri e condizioni ulteriori e maggiormente restrittivi, qualora esse intendano operare nelle due forme testé richiamate.

Per quanto riguarda i fornitori di servizi di intermediazione, infatti, il Regolamento sulla *governance* dei dati prevede che essi debbano rispettare, tra gli altri requisiti, anche quello di agire nell'interesse superiore degli interessati ovvero di fa-

---

l'esegeta un'interpretazione *a contrario* per la deduzione, seppur con talune difficoltà, delle fattispecie da essa potenzialmente regolate». Una conferma sembra provenire dal Garante, che nell'esentare gli IRCCS dalla richiesta di consenso per il trattamento dei dati personali – anche relativi alla salute – nell'ambito delle ricerche mediche relative al Covid-19, ha di recente chiarito che questi Istituti, allorché trattano dati personali nell'ambito delle ricerche mediche finanziate dal Ministero, non devono sottostare agli adempimenti previsti dall'art. 110 del Codice, quando risultano beneficiari dei fondi (banditi dal ministero), nell'ambito delle ricerche finalizzate al contrasto della pandemia, in quanto ineriscono alle funzioni di rilevante interesse pubblico attribuite, senza tuttavia fare alcun riferimento alla deroga di cui al comma 4 dell'art. 110-*bis* del Codice privacy (così le FAQ sul Coronavirus dedicate al trattamento dei dati nel contesto delle sperimentazioni cliniche, pubblicate sul sito web dell'Authority).

[61] GPDP, *Presupposti giuridici e principali adempimenti per il trattamento da parte degli IRCCS dei dati personali raccolti a fini di cura della salute per ulteriori scopi di ricerca*, in https://www.garanteprivacy.it/temi/sanita-e-ricerca-scientifica/irccs.

[62] Ne sono un esempio, tra le altre, Savvy Cooperative (https://www.savvy.coop/about–us); Cooperativa MIDATA (https://www.midata.coop/it/homepage/); Salus Coop (https://www.salus.coop/); PolyPoly.Health (https://polypolyhealth.com/).

cilitare l'esercizio dei loro diritti, in particolare informandoli e, se opportuno, fornendo loro consulenza in maniera concisa, trasparente, intelligibile e facilmente accessibile sugli utilizzi dei dati previsti da parte degli utenti nonché sui termini e le condizioni standard cui sono subordinati tali utilizzi, prima che gli interessati forniscano il loro consenso. Inoltre, tali servizi sono sottoposti ad un obbligo di notifica ai sensi dell'art. 11 DGA all'Autorità competente per i servizi di intermediazione dei dati, cui spettano, ai sensi dell'art. 14 DGA, compiti di monitoraggio, controllo e verifica circa il rispetto dei requisiti prescritti dal regolamento.

Analogamente, anche le organizzazioni per l'altruismo dei dati che, tra le altre cose, devono offrire strumenti per ottenere o revocare il consenso degli interessati, occorre siano registrate presso l'Autorità competente, cui spettano funzioni di vigilanza.

In entrambi i casi, perciò, l'acquisizione dei dati tramite tali enti potrebbe essere garanzia di maggior protezione dell'interessato, anche grazie ad una vigilanza che, per gli enti costituiti in forma cooperativa, andrebbe ad aggiungersi alla revisione biennale o annuale svolta dalle centrali cooperative o dal Ministero delle Imprese e del *made in Italy*, nonché alle eventuali ispezioni straordinarie spettanti a quest'ultimo, ai sensi del d.lgs. n. 220/2002, ulteriormente volte a garantire il rispetto dei requisiti mutualistici.

Non solo, ma, per quanto riguarda gli organismi di altruismo, essi potranno avvalersi del *modulo europeo di consenso all'altruismo dei dati* che – consentendo la personalizzazione in funzione di settori specifici e finalità diverse e garantendo che gli interessati possano dare e revocare il proprio consenso a una specifica operazione di trattamento dei dati conformemente alle prescrizioni di cui al Reg. (UE) 2016/679 – potrà rappresentare uno strumento di grande utilità per facilitare gli obiettivi della ricerca. Tali enti potrebbero, dunque, essere determinanti nel favorire da un lato l'acquisizione di un consenso maggiormente libero in quanto più informato e dall'altro nel garantire una base giuridica al trattamento che, anche attraverso il ricorso a modelli europei, potrà essere acquisita in tempi più celeri.

Sotto altro ma correlato profilo, poi, a nostro avviso, le cooperative potrebbero fornire un prezioso contributo. Si tratta dell'acquisizione del consenso nelle ipotesi prese in esame dal *considerando* n. 33 del GDPR [63], che, facendo riferimento ai casi in cui gli obiettivi della ricerca non siano già chiari e predeterminabili dall'inizio, caso non infrequente se si pon mente alla circostanza che assai spesso oggi sono i dati a guidare questa attività e non viceversa [64], stabilisce che «dovrebbe essere con-

[63] Ai sensi del quale «in molti casi non è possibile individuare pienamente la finalità del trattamento dei dati personali a fini di ricerca scientifica al momento della raccolta dei dati. Pertanto, dovrebbe essere consentito agli interessati di prestare il proprio consenso a taluni settori della ricerca scientifica laddove vi sia rispetto delle norme deontologiche riconosciute per la ricerca scientifica. Gli interessati dovrebbero avere la possibilità di prestare il proprio consenso soltanto a determinati settori di ricerca o parti di progetti di ricerca nella misura consentita dalla finalità prevista».

[64] Lo rilevano G. FINOCCHIARO-L. GRECO, *Trattamento di dati sanitari per la ricerca scientifica: nuove prospettive*, loc. cit.

sentito agli interessati di prestare il proprio consenso a taluni settori della ricerca scientifica laddove vi sia rispetto delle norme deontologiche riconosciute per la ricerca scientifica. Gli interessati dovrebbero avere la possibilità di prestare il proprio consenso soltanto a determinati settori di ricerca o parti di progetti di ricerca nella misura consentita dalla finalità prevista». Laddove, come ha precisato l'EDPB nel *Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research adopted on 2 February 2021*, quando non è possibile specificare appieno le finalità della ricerca, il titolare del trattamento deve cercare altri modi per garantire il rispetto dell'essenza dei requisiti del consenso, ad esempio permettendo agli interessati di acconsentire a una finalità di ricerca in termini più generali e a fasi specifiche di un progetto di ricerca che si sa già sin dall'inizio avranno luogo. Mano a mano che la ricerca avanza, sarà quindi possibile ottenere il consenso per le fasi successive del progetto prima dell'inizio della fase corrispondente in quanto la mancanza di specificazione della finalità può essere compensata dalla fornitura periodica, da parte del titolare del trattamento, di informazioni sullo sviluppo della finalità durante l'avanzamento del progetto di ricerca, in maniera tale che, nel tempo, il consenso sia il più specifico possibile [65]. Ma se è vero che questa procedura rende assai difficile la gestione dell'attività e tende a scoraggiare chi intenda intraprenderla [66], l'esistenza di un soggetto collettivo, che si ponga come unico interlocutore dei ricercatori e che possa avere un continuo contatto, grazie al rapporto mutualistico, con l'interessato per renderlo gradualmente edotto dei progressi della sperimentazione, potrebbe rivelarsi un elemento di semplificazione assai utile.

In conclusione, dunque, per tutte quelle situazioni in cui il consenso rappresenta la base giuridica del trattamento per il riuso dei dati per fini di ricerca, le cooperative, sia come enti con vocazione commerciale sia come enti a finalità di interesse generale con esclusivo interesse mutualistico – e ancor di più se, alla luce delle considerazioni svolte nel secondo paragrafo di questo scritto, dotate di potere di rappresentanza dei propri membri – potranno essere i luoghi di eccellenza per la formazione del consenso dell'interessato. Così che, riprendendo quando detto all'inizio delle presenti note, esse potrebbero rappresentare proprio per i casi più delicati come quelli che coinvolgono interessati particolarmente vulnerabili, quali i pazienti che collaborano ad una ricerca in ambito medico, le sedi per esprimere un consenso (più informato e pertanto) protetto, in quanto luoghi privilegiati per la piena formazione della volontà (negoziata) dell'interessato da esse rappresentato.

---

[65] In questo senso si esprime il documento citato nel testo, par. 25 ss.

[66] Secondo quanto affermano G. FINOCCHIARO-L. GRECO, *Trattamento di dati sanitari per la ricerca scientifica: nuove prospettive*, cit., p. 6.

4. Verso nuovi scenari.

Il tema del trattamento dei dati per finalità di ricerca medica è oggetto proprio in questo momento storico di modifiche normative, potenzialmente rivoluzionarie, in quanto in grado di aprire scenari completamente diversi, nei quali, comunque, a nostro avviso rimane sempre importante, seppure evidentemente soggetto ad una parallela evoluzione, il ruolo delle cooperative.

Analizziamo distintamente le due principali novità, la prima delle quali già approvata, assai di recente, a livello nazionale e la seconda in corso di approvazione nel contesto unionale.

(A) Il legislatore nazionale, in tempi a noi prossimi, ha percepito l'esigenza di un intervento volto a eliminare le barriere alla ricerca che esso stesso ha contribuito a creare, sulle quali ci siamo trattenuti in precedenza, così che, con la legge di conversione del decreto-legge 2 marzo 2024, n. 19, recante ulteriori disposizioni urgenti per l'attuazione del Piano nazionale di ripresa e resilienza (PNRR), si è introdotta una modifica dell'art. 110 del Codice *privacy*, prescrivendo che, nei casi in cui è ammesso il trattamento di dati personali relativi alla salute a fini di ricerca scientifica in campo medico, biomedico o epidemiologico senza il consenso dell'interessato, in luogo della sottoposizione del programma di ricerca alla preventiva consultazione del Garante, si possa procedere osservando le garanzie che la stessa Autorità individua.

A ben vedere, però, con tale intervento, che indubbiamente ha una portata semplificatrice, il legislatore non ha modificato la base giuridica legittimante il trattamento, che rimarrebbe di norma il consenso, ma ha solo previsto che, nel caso di cui ci si possa avvalere della deroga di cui al secondo periodo del primo comma [67], il titolare del trattamento, fermi restando gli obblighi di adottare misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato e di acquisire il motivato parere favorevole del Comitato etico, non debba più attendere la preventiva "autorizzazione" del Garante ai sensi dell'art. 36 del Regolamento, con gli oneri che, secondo quanto abbiamo già evidenziato, ciò comportava, ma possa procedere nell'osservanza delle garanzie *de quibus*. Senza, in ogni caso, che venga meno l'onere del titolare di dimostrare l'impossibilità o l'oggettiva difficoltà o il pregiudizio per la ricerca all'acquisizione del consenso.

Proprio sulla scia di quest'ultima considerazione, il Garante è tempestivamente intervenuto con il provvedimento rubricato *Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica ai sensi degli artt. 2-quater e 106 del Codice* del 9 maggio 2024 [68]. Con esso, l'Autorità, da un lato, ha individuato le prime garanzie da adottare per il trattamento dei dati personali a scopo di ricerca medica, bio-

[67] Ovvero, come abbiamo visto, quando, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca.

[68] Doc. *web* n. 10016146.

medica ed epidemiologica, mentre, dall'altro, ha promosso l'adozione di nuove Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica, ai sensi degli artt. 2-*quater* e 106 del Codice *privacy*.

Ora, rispetto al primo dei due punti di cui sopra, che ha evidenti ricadute dirette sul tema di cui ci andiamo occupando, vale la pena sottolineare come il Garante abbia individuato una serie di assai rigide garanzie da adottare per il trattamento dei dati personali riferiti a pazienti deceduti o non contattabili, che si traducono nella verifica della sussistenza di specifici motivi di carattere etico od organizzativo. In particolare, se nei primi rientrano quelli riconducibili alla circostanza che l'interessato ignora la propria condizione, tra i secondi troviamo quelli rinvenibili nel caso in cui la mancata raccolta dei dati riferiti al numero di interessati che non è possibile contattare, rispetto al numero complessivo dei soggetti che si intende arruolare nella ricerca, produrrebbe conseguenze significative in termini di qualità dei risultati della ricerca stessa in ragione dei criteri di inclusione previsti dallo studio, delle modalità di arruolamento, della numerosità statistica del campione prescelto, del periodo di tempo trascorso dal momento in cui i dati sono stati raccolti.

Più nel dettaglio, sulla base delle indicazioni fornite dal Garante, i motivi di impossibilità organizzativa concernono sia quelli derivanti dalla circostanza, da considerarsi ad avviso dell'Autorità di controllo del tutto residuale, che contattare gli interessati implicherebbe uno sforzo sproporzionato per la elevata numerosità del campione, sia quelli derivanti dalla circostanza, alternativa alla precedente, che all'esito di ogni ragionevole sforzo compiuto per contattarli [69], ciò si riveli impossibile. In tali casi, il titolare del trattamento deve comunque accuratamente motivare e documentare, nel progetto di ricerca, la sussistenza delle ragioni etiche od organizzative per le quali informare gli interessati – e quindi acquisire il consenso – non risulta possibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca, eventualmente documentando altresì gli sforzi profusi per tentare di contattarli.

In ogni caso, il provvedimento prescrive altresì che i titolari del trattamento di dati riferiti a soggetti deceduti o non contattabili devono svolgere e pubblicare la valutazione di impatto, ai sensi dell'art. 35 del Regolamento, dandone comunicazione al Garante.

In sintesi, dunque: *a)* la circostanza per cui contattare gli interessati implicherebbe uno sforzo sproporzionato viene qualificata come residuale; *b)* la mancata acquisizione del consenso è sottoposta ad un severo onere motivazionale; *c)* l'impossibilità di contattare gli interessati deve essere documentata indicando gli sforzi ragionevolmente compiuti a tal fine; *d)* l'assenza del consenso come base giuridica conduce automaticamente all'obbligo di redazione e pubblicizzazione della valutazione di impatto.

---

[69] Peraltro, al riguardo, l'Autorità si premura anche di introdurre alcuni concreti esempi di appropriati tentativi di contatto, come la verifica dello stato di esistenza in vita, la consultazione dei dati riportati nella documentazione clinica, l'impiego dei recapiti telefonici eventualmente a suo tempo forniti nonché l'acquisizione di dati di contatto pubblicamente accessibili.

Sennonché, cumulando tutte queste garanzie che l'Autorità ha ritenuto di introdurre con l'atto *de quo*, ci sembra si debba concludere che vengono di fatto vanificati gli obiettivi della riforma, di modo che l'intervento del legislatore, per quanto apprezzabile, non appare ancora risolutivo del problema più volte emerso nel corso della nostra indagine. Infatti, sebbene la nuova previsione permetta di ridurre i tempi di attesa per l'avvio della sperimentazione, l'intervento del Garante sembra averne paralizzato la portata più innovativa, senza contare che, con la stessa novella, non si è proceduto, come sarebbe stato invece auspicabile, a rivedere alla radice il sistema consenso-centrico e individuare, per le attività di ricerca medica di interesse generale, una differente base giuridica, facendo ricorso a soluzioni alternative, come per esempio, in aderenza al *considerando* n. 50 del GDPR, quella di riconoscere per via legislativa nella ricerca medica un compito di interesse pubblico, la cui esecuzione potrebbe rendere possibile l'ulteriore trattamento (ovvero il *secondary use*), con la precisazione da parte del diritto nazionale delle finalità e i compiti per i quali esso è considerato lecito e compatibile [70].

(B) Proprio la formulazione dell'art. 110 del Codice *privacy*, su cui ci siamo intrattenuti e che, pure nella nuova versione, non sembra risolutiva, induce a rimarcare come il quadro normativo nazionale sopra descritto contribuisca anche a delineare una disomogeneità di attuazione e interpretazione, *in parte qua*, del GDPR da parte degli Stati membri [71], che crea notevoli incertezze giuridiche e conseguenti ostacoli all'uso secondario dei dati sanitari, come del resto sembrano ammettere le stesse Istituzioni europee. Lo si evince chiaramente dal quadro emerso nella *Valutazione delle norme degli Stati membri dell'UE sui dati sanitari alla luce dell'RGPD* [72], in cui si rileva una disarmonica applicazione della disciplina europea relativa ai dati sanitari, partendo proprio dalla constatazione che l'uso di disposizioni di specificazione facoltative ai sensi del GDPR a livello nazionale ha creato frammentazione

[70] La necessità di una riforma normativa è stata sostenuta con forza anche da G. FINOCCHIARO, *Digitalizzazione della sanità e protezione dei dati personali*, cit., p. 122 ss., che ipotizza altre possibili alternative quali un'informazione di carattere generale con possibilità di *opt-out* per l'interessato, laddove il trattamento di dati pseudonimizzati avvenga seguendo standard condivisi in sede scientifica, ovvero la previsione di un consenso di carattere generale sulla falsariga di quanto previsto nel *considerando* n. 33.

[71] Interessante sul punto l'analisi di F. DI TANO, *Protezione dei dati personali e ricerca scientifica: un rapporto controverso ma necessario*, cit., p. 89, in cui l'A. evidenzia come Spagna, Germania e Danimarca siano diversamente intervenute in materia. Talvolta considerando lecito il riuso dei dati personali per scopi di ricerca quando, ottenuto il consenso per una determinata finalità i dati siano utilizzati per finalità o ambiti di ricerca attinenti all'area di quella originaria (Spagna); talaltra riconoscendo lecito il trattamento di categorie particolari di dati personali per finalità di ricerca anche senza consenso, se il trattamento è necessario per tali finalità e gli interessi del titolare al trattamento prevalgono sostanzialmente rispetto a quelli dell'interessato (Germania); talaltra ancora ammettendo il trattamento dei dati personali per finalità di ricerca senza il consenso dell'interessato (Danimarca).

[72] COMMISSIONE EUROPEA, *Assessment of the EU Member States' rules on health data in the light of the GDPR*, Bruxelles, 12 febbraio 2021.

e difficoltà nell'accesso ai dati sanitari elettronici con ripercussioni sulla possibilità per ricercatori, responsabili delle politiche e regolatori di eseguire i loro compiti e le loro attività.

Per tale motivo, in sede unionale è stata presentata una proposta di *Regolamento sullo spazio europeo dei dati sanitari* [73], che si pone l'obiettivo di integrare il DGA al fine di fornire norme più specifiche per questo settore e di armonizzare le legislazioni nazionali. Onde raggiungere tale obiettivo, il *considerando* n. 37 del testo approvato dal Parlamento europeo in prima lettura il 24 aprile 2024, inibisce agli Stati membri la possibilità di mantenere o adottare forme di legislazione speciali e differenziate ai sensi dell'art. 9, par. 4, del GDPR con riguardo al trattamento di dati genetici, biometrici o relativi alla salute, salvo nelle ipotesi previste dall'art. 33, par. 5, del medesimo atto, che fa riferimento ai dati genetici, epigenomici e genomici umani, agli altri dati molecolari umani quali quelli proteomici, trascrittomici, metabolomici, lipidomici e altri dati omici, ai dati provenienti da applicazioni per il benessere nonché ai dati sanitari provenienti da biobanche e banche dati associate.

Nel merito della disciplina uniforme che l'EHDS introdurrebbe, troviamo anche la revisione della base giuridica del trattamento dei dati sanitari elettronici personali [74]. In un'ottica di miglior contemperamento degli interessi in gioco, infatti, l'atto normativo si autoqualifica, ai sensi del già richiamato art. 9, par. 2, lett. *j)* del GDPR, quale previsione di diritto dell'Unione in grado di fungere da base giuridica legittimante il trattamento per finalità di ricerca. In tal modo, i dati *de quibus* potrebbero essere riutilizzati per finalità specifiche e determinate dal testo normativo senza la necessità di passare per il consenso dell'interessato (ovvero in assenza di una forma di *opt-in*), bensì riconoscendo eventualmente una forma di opposizione al trattamento tramite un successivo *opt-out*. Sul punto, infatti, il testo ad oggi disponibile modifica la proposta originaria della Commissione introducendo, tra le altre cose, non un consenso preventivo ma appunto il diritto di opposizione, che prevede la possibilità degli Stati membri di consentire ai pazienti di rinunciare all'uso dei loro dati sanitari elettronici sia da parte di un professionista sanitario per uso primario che per un ulteriore uso secondario, salvo che per scopi di interesse pubblico, elaborazione delle politiche, statistiche e scopi di ricerca nell'interesse pubblico. La svolta sarebbe radicale, giacché quest'ultima direzione intrapresa dal legislatore eurounitario permetterebbe di superare, almeno nell'ambito della ricerca medica, la prospettiva consenso-centrica, facendo pendere l'ago della bilancia più

[73] Nel seguito indicato anche semplicemente con l'acronimo inglese EHDS. Per la versione adottata in prima lettura si veda PARLAMENTO EUROPEO, *Risoluzione legislativa del Parlamento europeo del 24 aprile 2024 sulla proposta di regolamento del Parlamento europeo e del Consiglio sullo spazio europeo dei dati sanitari*, Bruxelles, 24 aprile 2024, COD(2022)0140.

[74] Definiti dall'art. 2, par. 2, lett. *a)* della proposta della Commissione come «i dati relativi alla salute e i dati genetici quali definiti nel regolamento (UE) 2016/679, nonché i dati relativi a determinanti della salute o i dati trattati nell'ambito della prestazione di servizi di assistenza sanitaria, che sono trattati in formato elettronico».

nella direzione del riuso dei dati che in quella dell'autodeterminazione e imponendo anche al legislatore nazionale una profonda revisione degli artt. 110 e 110-*bis* del Codice più volte richiamati.

Nemmeno questi scenari in divenire, ad ogni modo, comporterebbero il venir meno dell'importanza che le cooperative potrebbero avere nel contesto che stiamo analizzando, di modo che il discorso sin qui svolto mantiene, a nostro avviso, tutta la propria validità. Non solo, infatti, permangono non irrilevanti eccezioni in cui il consenso continua a rappresentare la base giuridica del trattamento *rebus sic stantibus*, ma esse non verrebbero meno neppure successivamente all'eventuale adozione dell'EHDS (nonché al necessario intervento nazionale di coordinamento), ipotizzando che il testo finale non si discosti da quello in discussione.

Per quanto riguarda la prima ipotesi, il problema del consenso – e quindi l'utilità delle cooperative a tal fine – pure dopo l'ultima novella cui si è fatto cenno continua a riguardare: *a)* i trattamenti realizzati ai sensi dell'art. 110 da strutture anche pubbliche che non trovano il loro fondamento nella legge ai sensi dell'art. 9, par. 2, lett. *j)*, del GDPR, o ai sensi dell'art. 12-*bis* del d.lgs. 30 dicembre 1992, n. 502 ed i trattamenti di dati personali per finalità di ricerca medica realizzati da enti privati per finalità commerciali e che, quindi, non sono soggetti alla deroga prevista dall'art. 110; *b)* i trattamenti relativi a studi prospettici e quindi non retrospettivi e tutti i trattamenti per cui non sarà possibile dimostrare – ai sensi dell'art. 110, co. 1, secondo periodo – l'impossibilità di acquisire il consenso; *c)* i trattamenti ulteriori realizzati ai sensi dell'art. 110-*bis* da parte di soggetti terzi qualora non sia possibile rientrare nelle esenzioni previste dalla disposizione.

Nella seconda ipotesi prospettata, ovvero l'adozione dell'EHDS, il consenso rimarrebbe – e nuovamente, con esso, l'importanza del ruolo degli enti di cui abbiamo trattato – quanto meno per i trattamenti dei dati sanitari *non elettronici* nonché per i trattamenti per cui lo stesso Regolamento prevede la possibilità degli Stati membri di introdurre misure aggiuntive, nei casi sopra elencati. I quali – è bene evidenziarlo – non sono certo irrilevanti, vuoi, sotto il profilo qualitativo, per la delicatezza della tipologia di dati in questione (come quelli genetici), vuoi, sotto il profilo quantitativo, per il ricorrere della fattispecie (si pensi ai dati provenienti dalle applicazioni per il benessere).

In conclusione, crediamo dunque si possa confermare che il caso della ricerca in ambito sanitario costituisca oggi, così come continuerà a farlo in futuro, un esempio paradigmatico di come si possa (e si debba, se si vuole prendere sul serio il diritto alla protezione dei dati personali) introdurre un meccanismo di tutela collettiva per l'interessato in grado di non far evaporare l'autodeterminazione informativa in una società sempre più basata sulla circolazione e condivisione dei dati.

Capitolo XXI

Cooperative di dati per la tutela della salute

Maura Tampieri

Abstract: The paper presents an analysis of Data Governance Act, as recently outlined by the European legislator in the Data Governance Act (EU Reg. 868/2022), with a particular focus on the applications of new technologies in the various areas of health care. It also points out the need for an anthropocentric governance and an ethical approach of new technologies applied to medical science. In this framework, the paper highlights the role played by data cooperatives with a particular regard to Salus.Coop.

1. La nuova visione del *Data Governance Act.*

Il *Data Governance Act* (DGA) [1] contiene iniziative di potenziamento del mercato digitale, nell'ottica della massima valorizzazione dei dati personali e non personali.

Come è stato condivisibilmente affermato, «il diritto alla protezione dei dati personali viene sempre più invocato di fronte alle innumerevoli "servitù volontarie" cui rischiamo di consegnare noi stessi, in cambio di utilità e servizi che paghiamo al prezzo di porzioni piccole o grandi della nostra libertà. Emerge così un nuovo sottoproletariato del digitale, un "Quinto Stato" formato da quanti siano disposti a cedere, con i propri dati, la libertà, in cambio dei servizi offerti in rete solo apparentemente "a prezzo zero"» [2]. Dunque, ogni innovazione – comprese le nuove

[1] Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio, 30 maggio 2022, *relativo alla* governance *europea dei dati e che modifica il regolamento (UE) 2018/1724* (*Regolamento sulla* governance *dei dati*) (*Data Governance Act*).

[2] A. Soro, *L'universo dei dati e la libertà della persona, Discorso del Presidente del Garante per la protezione dei dati personali 2018*, 7 maggio 2019, doc. *web* 9109075, p. 7.

norme introdotte dal DGA, volte ad incoraggiare la circolazione dei dati, personali e non personali, e ad aumentare la fiducia nell'affidabilità dei servizi di intermediazione dei dati [3] – deve pur sempre essere valutata nella prospettiva della piena tutela della persona e dei suoi diritti fondamentali, con particolare riferimento al diritto alla protezione dei dati personali. Questo aspetto risulta particolarmente rilevante quando le operazioni di trattamento riguardano i dati relativi alla salute.

Come è noto, ai sensi dell'art. 8 della Carta dei diritti fondamentali UE, la protezione dei dati personali si colloca ai vertici della gerarchia delle fonti, tuttavia «non è forse azzardato prevedere che tale primazia sia destinata gradualmente ad incrinarsi sino a cedere il passo (…) a un modello multipolare, nel quale le istanze di protezione dei dati coesisteranno con pari dignità con quelle di libero accesso e riuso dei dati medesimi» [4]. Del resto, il Regolamento (UE) 2016/679 (GDPR) sin dall'art. 1 impone, come necessaria, l'esigenza di un bilanciamento tra il diritto alla protezione dei dati personali e la loro libera circolazione nell'Unione europea. Inoltre, il considerando n. 4 del GDPR afferma che il menzionato diritto alla protezione dei dati personali debba essere proporzionalmente contemperato con gli altri diritti fondamentali, alla luce della sua funzione sociale.

Il DGA intende delineare un sistema di regole concernenti la circolazione e la promozione dell'utilizzo dei dati, nonché un'ampia condivisione degli stessi con particolare riguardo ai fini di ricerca scientifica.

L'art. 2, par. 1, del DGA, definisce i dati come: «qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi raccolta di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva», prendendo così in considerazione sia i dati personali sia i dati non personali.

L'art. 10 del DGA contempla tre diverse tipologie di servizi di intermediazione, soggetti a una procedura di notifica obbligatoria [5]: la prima è quella incentrata sulla condivisione dei dati tra attori di mercato, precisamente «tra i titolari dei dati e i potenziali utenti dei dati, compresa la messa a disposizione di mezzi tecnici o di altro tipo per consentire tali servizi»; la seconda riguarda i «servizi di intermediazione tra interessati che intendono mettere a disposizione i propri dati personali o persone fisiche che intendono mettere a disposizione dati non personali e potenziali utenti dei dati, compresa la messa a disposizione di mezzi tecnici o di altro tipo per consentire tali servizi, permettendo in particolare l'esercizio dei diritti degli inte-

---

[3] F. BRAVO, *Intermediazione di dati personali e servizi di* data sharing *dal* GDPR *al* Data Governance Act, in *Contr. e impr. Europa*, 2021, 1, p. 199 ss.; D. POLETTI, *Gli intermediari dei dati*, in *European J. of Privacy Law & Tech*., 2022, 1, p. 46 ss.; ID., *Gli intermediari dei dati*, in A. MORACE PINELLI (a cura di), *La circolazione dei dati personali. Persona, contratto e mercato*, Pisa, 2023, p. 105 ss.

[4] G. RESTA, *La dimensione collettiva dei dati personali*, in *Parole chiave*, 2023, 1, pp. 90-91.

[5] Giusta l'art. 11, par. 1 la notifica va presentata all'autorità competente per i servizi di intermediazione dei dati, (i cui compiti sono previsti all'art. 13 del DGA) che inoltre prevede l'uso di un logo comune, riconoscibile in tutta l'Unione, per i fornitori di servizi di intermediazione dei dati. Le specifiche *Condizioni per la fornitura di servizi di intermediazione dei dati* sono regolate dall'art. 12 del DGA.

ressati di cui al regolamento (UE) 2016/679»; infine, la terza tipologia è costituita dai «servizi di cooperative di dati» [6]. Questi ultimi servizi di intermediazione dei dati sono a loro volta definiti *ex* art. 2, n. 15, del DGA come servizi «offerti da una struttura organizzativa costituita da interessati, imprese individuali o da PMI, che sono membri di tale struttura, avente come obiettivi principali quelli di aiutare i propri membri nell'esercizio dei loro diritti in relazione a determinati dati, anche per quanto riguarda il compiere scelte informate prima di acconsentire al trattamento dei dati, di procedere a uno scambio di opinioni sulle finalità e sulle condizioni del trattamento dei dati che rappresenterebbero al meglio gli interessi dei propri membri in relazione ai loro dati, o di negoziare i termini e le condizioni per il trattamento dei dati per conto dei membri prima di concedere l'autorizzazione al trattamento dei dati non personali o prima che essi diano il loro consenso al trattamento dei dati personali».

Con il *Data Governance Act*, il modello societario cooperativo [7] – con lo scopo mutualistico che lo contraddistingue (e che, come tale, trascende l'interesse dei singoli soci), costituzionalmente riconosciuto giusta l'art. 45 – riceve un primo riconoscimento nel settore dell'economia digitale e pare garantire un efficace controllo sui dati. Il DGA assegna dunque uno specifico ruolo ai servizi di cooperative di dati, *rectius*, a organizzazioni il cui scopo mutualistico è connaturato alla loro essenza, che svolgeranno un ruolo di rilievo nell'economia e nella società digitale.

Nella cooperativa, in realtà, si possono rinvenire i presupposti essenziali che sono alla base della nuova concezione di cooperativa di dati che può dunque operare, come cooperativa di servizi, sul mercato per la gestione condivisa dei dati forniti dai soci della stessa cooperativa, siano essi persone fisiche o persone giuridiche, o dalle cooperative tra di loro. Un utilizzo consapevole e un'equa condivisione del capitale digitale (rappresentato dal valore, non solo monetario, dei dati conferiti) si

---

[6] G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, in G. RESTA-V. ZENO-ZENCOVICH (a cura di), *Governance of/through big data*, vol. II, Roma, 2023, pp. 625 e 626 osserva che «il testo finale del DGA segna un progresso significativo rispetto all'originaria Proposta della Commissione. Difatti, il Cons. 24 della Proposta, specificamente concernente le cooperative, affermava: "è importante riconoscere che i diritti a norma del regolamento (UE) 2016/679 possono essere esercitati soltanto a titolo individuale e non possono essere conferiti o delegati a una cooperativa di dati". Il riferimento al "conferimento" e alla "delega" è scomparso dal testo finale del Regolamento».

[7] Al considerando 31 del DGA si legge: «le cooperative di dati mirano a raggiungere una serie di obiettivi, in particolare a rafforzare la posizione dei singoli individui, affinché compiano scelte informate prima di acconsentire all'utilizzo dei dati, influenzando i termini e le condizioni, stabiliti dalle organizzazioni di utenti dei dati, cui è subordinato l'utilizzo dei dati, in modo da offrire scelte migliori ai singoli membri del gruppo, o trovando possibili soluzioni alle posizioni contrastanti dei singoli membri di un gruppo in merito alle modalità di utilizzo dei dati laddove tali dati riguardino più interessati all'interno di tale gruppo. In tale contesto è importante riconoscere che i diritti a norma del regolamento (UE) 2016/679 sono diritti personali dell'interessato e che quest'ultimo non può rinunciarvi. Le cooperative di dati potrebbero altresì rappresentare uno strumento utile per imprese individuali e PMI che, in termini di conoscenze in materia di condivisione dei dati, sono spesso equiparabili ai singoli individui».

pone in una logica di cooperazione e di "neomutualismo" digitale [8].

Il Regolamento non definisce *ex se* le cooperative di dati lasciando quindi aperta la strada alla possibilità di utilizzare diverse forme soggettive per la fornitura di tali servizi. Il dato che, comunque, le accomuna, nella prospettiva del (neo)mutualismo digitale, è il miglioramento della qualità della vita, lavorativa e non lavorativa, ivi compreso il benessere psico-fisico dei membri della cooperativa nell'ottica di uno sviluppo solidale [9], sostenibile e democratico, che pone al centro la persona. Tutto questo va oltre la logica del profitto del modello capitalistico proprio delle società che svolgono attività d'impresa, nelle quali le analisi dei dati relativi alla fornitura del servizio sono dirette a vantaggio della stessa società. In altri termini, i soci della cooperativa di dati possono confrontarsi e decidere al meglio sulle scelte di utilizzo e riutilizzo dei dati, mantenendo una piena *governance* dei dati (che la cooperativa è in grado di aggregare) provenienti dagli stessi soci che, oltre alla veste di *data subjects* possono assumere anche quella di *data holders* (titolari di dati) [10].

---

[8] P. VENTURI-F. ZANDONAI, *Neomutualismo. Ridisegnare dal basso competitività e* welfare, Milano, 2022; per una lettura del neomutaualismo nella sua moderna declinazione di neomutualismo digitale cfr. F. BRAVO, *Le cooperative di dati*, in *Contr. e impr*., 2023, 3, p. 764.

[9] F. BRAVO, *Il principio di solidarietà in materia di protezione dei dati personali nelle decisioni del Garante e della Corte di Cassazione*, in *Contr. e impr*., 2023, 2, pp. 407 e 412 ss.; sul tema della solidarietà cfr. P. RESCIGNO, *Solidarietà e diritto*, Napoli, 2006; M.C. BLAIS, *La solidarité. Histoire d'une idée*, Parigi, 2007; RODOTÀ, *Solidarietà. Un'utopia necessaria*, Roma-Bari, 2014; P. PERLINGIERI, *Mercato, solidarietà e diritti umani*, in *Rass. dir. civ*., 1995, p. 84 ss.; M. PARADISO, *La solidarietà giuridica tra pubblico e privato: leggendo il volume omonimo di Roberto Cippitani*, in *Dir. fam. pers.*, 2012, 1, p. 368 ss.; F.D. BUSNELLI, *Può la solidarietà sopravvivere al mercato? Riflessioni a margine de "la compravendita" di Angelo Luminoso nel giorno della solenne consegna del* "liber amicorum", in *Riv. giur. sarda*, 2013, II, p. 89 ss.; ID., *Il principio di solidarietà e "l'attesa della povera gente", oggi*, in *Riv. trim. dir. proc. civ*., 2013, 2, p. 426 ss.; ID., *Solidarietà: aspetti di diritto privato*, in *Iustitia*, 1999, 4, p. 437 ss.; G. RESTA, *Gratuità e solidarietà: fondamenti emotivi e "irrazionali",* in *Riv. crit. dir. priv*, 2014, 1, p. 26 ss.; M. TAMPIERI, *La riscoperta del principio di solidarietà*, in *Jus civile*, 2020, 3, p. 612 ss.

[10] L'art. 2, par. 1, n. 8, del DGA, così definisce il titolare dei dati (*data holder*): «una persona giuridica, compresi gli enti pubblici e le organizzazioni internazionali, o una persona fisica che non è l'interessato rispetto agli specifici dati in questione e che, conformemente al diritto dell'Unione o nazionale applicabile, ha il diritto di concedere l'accesso a determinati dati personali o dati non personali o di condividerli»; per la stessa disposizione, al n. 9, l'utente dei dati (*data user*) è «una persona fisica o giuridica che ha accesso legittimo a determinati dati personali o non personali e che ha diritto, anche a norma del regolamento (UE) 2016/679 in caso di dati personali, a utilizzare tali dati a fini commerciali o non commerciali». In dottrina, F. BRAVO, *Intermediazione di dati personali e servizi di* data sharing *dal GDPR al* Data Governance Act, cit., p. 203 osserva che «mai prima d'ora s'è voluto riferire il concetto di "titolarità" direttamente al dato (e non al trattamento) e ciò denota un cambio di paradigma che rischia di essere un preludio all'introduzione, per via normativa, di una reificazione dei dati personali, quali entità giuridicamente rilevanti *ex sé* più che quali attribuiti della persona»; ID., *Le cooperative di dati*, cit., p. 757 ss., spec. a pp. 785-786 l'Autore afferma che il DGA introduce «modelli di *governance "duale"*, aggiungendo cioè alla (debole e sbiadita) *governance "individuale"* del *data subject* una *governance* ulteriore, che assume talora le vesti di una *governance "collettiva"*, esercitata nel contesto della cooperativa di dati, che il *data subject* concorre a costituire e a formare, e talaltra le vesti di una *governance*

La forma di società cooperativa (di dati) è particolarmente indicata per la gestione di un'attività di intermediazione partecipata, condivisa e altruistica che può concorrere alla democratizzazione dell'economia digitale, stimolando la ricerca (anche) al fine di tutelare al meglio la salute delle persone con cure adeguate. La possibilità di condividere e scambiare dati di qualità (ad esempio immagini) consente, infatti, di individuare tempestivamente importanti patologie con gli evidenti vantaggi che si riflettono sul sistema sanitario e che saranno oggetto delle presenti riflessioni.

Nella prassi troviamo, tra gli altri, l'esempio della cooperativa di dati Salus.Coop.

2. I dati per il benessere psico-fisico della persona (anche) quando si fa paziente.

Se, da un lato, «nella definizione e nell'attuazione di tutte le politiche ed attività dell'Unione è garantito un livello elevato di protezione della salute umana» (art. 168 TFUE), dall'altro, i dati relativi alla salute costituiscono una «categoria particolare di dati personali», ai sensi dell'art. 9 del Regolamento (UE) 2016/679, che riconosce alla categoria una protezione speciale relativa al trattamento.

Al fine di garantire un'efficace tutela del diritto alla salute [11], occorre pertanto concepire l'utilizzo delle nuove tecnologie – che conosce un'evoluzione costante e inarrestabile collegata allo sviluppo e alla diffusione dell'intelligenza artificiale che si afferma con forza – da parte dei sistemi sanitari, come diretto alla prevenzione delle malattie e alla promozione della salute, e non limitato esclusivamente alla cura delle patologie.

La digitalizzazione della sanità è sicuramente un'occasione di sviluppo e innovazione per l'efficienza delle cure, per l'esattezza delle diagnosi e per una migliore programmazione della spesa sanitaria [12].

"aggregata", esercitata dall'intermediario (anche diverso dalla *data cooperative*), che raccoglie dati da soggetti diversi e ne *negozia* l'utilizzo nei confronti di soggetti terzi (agendo al contempo per conto degli interessati e, in caso di delega, anche a loro nome, pure ai fini dell'esercizio dei diritti che l'ordinamento riconosce loro) (…). Il *Data Governance Act* punta ad un rafforzamento della posizione degli interessati, facendo leva sull'azione svolta dagli intermediari che, veicolando i dati di più *data subjects*, possono porsi quale strumento di tutela sostanziale, grazie al *data subject empowerment* realizzabile tramite il controllo "intermediato"»; per una visione critica del concetto di proprietà, con riferimento ai dati personali, cfr. G. ALPA, *La "proprietà" dei dati personali*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, 2019, p. 11 ss.

[11] L'OMS, nel suo statuto, definì la salute come uno stato di completo benessere fisico, mentale e sociale. Più di recente, nel 2011, considera la salute come «la capacità di adattamento e di auto gestirsi di fronte alla sfide sociali, fisiche ed emotive». Si tratta di una definizione evolutiva che pone l'accento sulla capacità della persona di convivere (anche) con la patologia.

[12] M. TAMPIERI, *L'intelligenza artificiale e le sue evoluzioni. Prospettive civilistiche*, Milano, 2022, p. 193 ss.; ID., *Il ruolo delle nuove tecnologie nel contesto della sanità*, in *Responsabilità medica. Diritto e pratica clinica*, 2023, 4, pp. 363-364: «l'impiego di nuove tecnologie, proprio in ambito

A parere di chi scrive, nel settore della sanità, risulta sempre utile applicare le note quattro P della medicina: prevenzione, predizione, personalizzazione e partecipazione, che esprimono il passaggio culturale dalla "cura delle malattie" alla gestione del benessere psico-fisico dei pazienti. In questo senso, i sistemi di intelligenza artificiale, sempre più utilizzati nei diversi settori della medicina, rappresentano un valido strumento al servizio del medico, ma non possono prescindere dall'interazione e dal controllo in capo a quest'ultimo che con scienza e coscienza persegue il fine della cura della persona che si fa paziente.

In altri termini, è pur sempre necessario un approccio *human in command*, inteso come controllo e supervisione dell'uomo per la *governance* del sistema intelligente, in particolare con riferimento alle decisioni della macchina il cui margine di rischio è assai ridotto, ma non completamente eliminabile: si pensi, ad esempio, all'errata progettazione dei sistemi, dovuta (anche) all'assenza di dati di qualità. Si palesa, pertanto, la necessità di un governo antropocentrico dei sistemi di IA, diretto al servizio dell'uomo.

Dunque, il progresso delle nuove tecnologie va accompagnato da un impegno etico dei singoli e delle istituzioni al fine di realizzare un artefatto tecnologico che sia in grado di cambiare in *melius* la vita delle persone [13]. Così al consenso libero, specifico, informato e inequivocabile (*ex* art. 4, par. 1, n. 11 del GDPR), nella specie relativo alla condivisione dei dati sanitari – atto di autodeterminazione riferito a un trattamento chiaramente individuato, ma pur sempre revocabile –, dovrà accompagnarsi un utilizzo etico dei dati da parte dei sistemi sanitari. Pertanto, non è conforme all'etica informare un paziente attraverso un canale elettronico in merito alla diagnosi di una sua malattia incurabile, senza una preventiva comunicazione ad opera del medico nell'ambito di un auspicabile colloquio che dovrebbe rientrare nel pur sempre importante rapporto personale tra medico e paziente.

Dunque, l'utilizzo dei dati relativi alla salute [14], conferiti nelle cooperative di da-

---

sanitario, trova già un ampio spazio applicativo: hanno infatti un ruolo primario nella maggior parte dei progetti elaborati in medicina, incentrati in particolare sulla robotica e sulla telemedicina, e un'importanza crescente nei più diversi settori quali: il settore clinico, chirurgico, riabilitativo e assistenziale ove l'uso dei dati sanitari è un elemento chiave per la trasformazione digitale. Tutto ciò permette di migliorare la qualità della vita e la salute dei pazienti, come pure il lavoro del medico rendendo più efficace l'erogazione dei servizi».

[13] Secondo L. FLORIDI *et al*., *AI 4 People– An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations*, in *Minds and Machines*, 2018, 28, p. 689, l'IA è una *powerful force* che sta rimodellando le nostre vite e le nostre interazioni; sul tema v. G. FINOCCHIARO, *Intelligenza artificiale. Quali regole?*, Bologna, 2024; G. ALPA, *L'intelligenza artificiale. Il contesto giuridico*, Modena, 2021.

[14] Sul tema la Risoluzione del Parlamento europeo, del 3 maggio 2022, *sull'intelligenza artificiale in un'era digitale*, 2020/2266 (INI), punto 21, «rileva che l'analisi metodologica di grandi quantità di dati, anche con l'intelligenza artificiale, può consentire di trovare nuove soluzioni o migliorare le tecniche esistenti nel settore sanitario che potrebbero accelerare considerevolmente la ricerca scientifica, salvare vite umane e migliorare l'assistenza dei pazienti, offrendo trattamenti innovativi e diagnosi migliori e promuovendo contesti favorevoli per stili di vita sani».

ti del settore, deve essere in linea con le condizioni di liceità del trattamento, tra le quali il consenso *ex* art. 9, par. 2, lett. *a*), del GDPR, con il rispetto dei diritti fondamentali della persona e con il sistema di *governance* cooperativo [15].

Nell'*e-Health*, le tecnologie informatiche ed i sistemi di telecomunicazione, in particolare le *Information and Communication Technologies* (ICT), sono utilizzate per il monitoraggio della salute, ma anche per permettere ai professionisti sanitari lo scambio di pareri con riferimento ai dati sanitari del paziente – sulla cui protezione i fattori chiave sono l'interoperabilità e la portabilità – contenuti nella cartella clinica elettronica (una fonte importante per i *Big Data*). Si aggiunga che il medico, per finalità di prevenzione, diagnosi, cura e riabilitazione, consulterà in particolare il fascicolo sanitario elettronico che presenta la storia clinica del paziente e costituisce un aspetto importante della vita più intima dell'interessato che ogni medico dovrà proteggere e rispettare.

Sul tema, giova richiamare la proposta di Regolamento per l'istituzione di uno spazio europeo dei dati sanitari: *European Health Data Space* (EHDS) che ha lo scopo di incentivare l'accesso e lo scambio di dati sanitari elettronici. Tra tali dati rivestono particolare importanza le cartelle cliniche elettroniche (che solitamente contengono l'anamnesi di una persona fisica, diagnosi e cure, medicinali, allergie, immagini radiologiche e risultati di laboratorio), al fine di migliorare l'assistenza sanitaria e di promuovere la ricerca scientifica in campo sanitario, l'innovazione, la sicurezza dei pazienti, come pure la definizione delle politiche sanitarie [16].

---

[15] In argomento si richiama la Cass., 1° giugno 2022, n. 17911, tra le altre in *Giust. civ. Mass*., 2022, che ha affermato il seguente principio: «in tema di dati personali, la legittimità del trattamento presuppone un consenso validamente prestato in modo espresso, libero e specifico, in riferimento a un trattamento chiaramente individuato; tale principio, di portata generale, rileva e prevale in ogni rapporto, e osta a ritenere che un trattamento possa considerarsi giustificato da un consenso funzionalmente diverso come quello espresso nel contesto di maggioranze necessarie ad approvare deliberati assembleari, ed in ispecie il deliberato assembleare di una società cooperativa, della quale il soggetto, del cui dato personale si tratti, sia socio lavoratore». Secondo F. BRAVO, *Le cooperative di dati*, cit., p. 798 si aprono scenari complessi anche riguardo «al tema del rapporto tra formazione della volontà dell'ente e consenso del socio, a quello della libertà del consenso del socio-lavoratore ed al problema in ordine alla determinazione delle condizioni per utilizzo dei propri dati personali anche nei rapporti con i terzi, ma anche ad altre delicate questioni, quali ad esempio quelle concernenti il "conferimento" dei dati da parte dei soci alla cooperativa di dati, sia nel caso in cui siamo di fronte a dati personali del socio persona fisica (*data subject*), sia nel caso in cui il socio della cooperativa non sia un "interessato" in senso tecnico, ma sia "titolare dei dati" (*data holder*) ai sensi del *Data Governance Act*: si pensi al caso in cui tale socio sia un'impresa individuale o una PMI ed intenda conferire in cooperativa i dati di interessati terzi, raccolti e trattati nell'ambito della propria attività d'impresa, per poi riversarli nella cooperativa di dati di cui è socio».

[16] Più precisamente, secondo la proposta di Regolamento del Parlamento europeo e del Consiglio, *sullo spazio europeo dei dati sanitari*, 3 maggio 2022, COM(2022)197 final, in particolare per il considerando 1, «il presente regolamento ha lo scopo di istituire lo spazio europeo dei dati sanitari (*European Health Data Space*, EHDS) al fine di migliorare l'accesso delle persone fisiche ai loro dati sanitari elettronici personali e il loro controllo su tali dati nel contesto dell'assistenza sanitaria (uso primario dei dati sanitari elettronici), e per altre finalità di cui beneficerebbe la società quali la ricerca,

Il legislatore europeo ha inoltre evidenziato l'opportunità per gli Stati membri di tutelare la salute pubblica in uno spirito di solidarietà europea, laddove la salute è un investimento sul quale incentrare il programma proposto [17].

L'intelligenza artificiale, grazie alla sua versatilità, ha dato un notevole contributo all'analisi dei dati mondiali finalizzata alla previsione (e al contenimento) della diffusione geografica della pandemia da Covid-19, fino allo sviluppo dei primi vaccini e di terapie adeguate.

L'utilizzo dei dati e il loro riutilizzo, oggi promosso dal DGA, risultano importanti anche per tutelare il fondamentale diritto alla salute [18], per migliorare i sistemi di assistenza sanitaria, con particolare riguardo alla loro accessibilità, efficacia e sostenibilità nonché per ridurne i costi. Più precisamente, l'utilizzo e il riutilizzo dei dati a fini di ricerca scientifica si mostra oggi come obiettivo d'interesse generale.

A tal fine, un codice di condotta per il trattamento dei dati personali nel settore

---

l'innovazione, la definizione delle politiche, la sicurezza dei pazienti, la medicina personalizzata, le statistiche ufficiali o le attività normative (uso secondario dei dati sanitari elettronici). Il suo obiettivo è inoltre di migliorare il funzionamento del mercato interno istituendo un quadro giuridico uniforme in particolare per quanto riguarda lo sviluppo, la commercializzazione e l'uso di sistemi di cartelle cliniche elettroniche in conformità ai valori dell'Unione»; più precisamente per l'art. 1, par. 1 «il presente regolamento istituisce lo spazio europeo dei dati sanitari (*European Health Data Space*, EHDS) prevedendo disposizioni, norme e prassi comuni, infrastrutture e un quadro di *governance* per l'uso primario e secondario dei dati sanitari elettronici». Esso, in sintesi, si applica ai fabbricanti e ai fornitori di sistemi di cartelle cliniche elettroniche, ai titolari del trattamento e ai responsabili del trattamento stabiliti nella UE o in un Paese terzo, agli utenti dei dati sanitari elettronici (art 1, par. 3). Nel contesto dell'uso primario dei propri dati sanitari elettronici, *ex* art. 3, par. 1 «le persone fisiche hanno il diritto di accedere immediatamente, gratuitamente e in un formato facilmente leggibile, consolidato e accessibile». Si aggiunga che per agevolare la cooperazione e lo scambio di informazioni tra gli Stati membri è prevista l'istituzione di un comitato dello spazio europeo dei dati sanitari (comitato EHDS), ai sensi dell'art. 64 della proposta di Regolamento.

[17] Cfr. il Regolamento (UE) 2021/522 del Parlamento europeo e del Consiglio, 24 marzo 2021, *che istituisce un programma d'azione dell'Unione in materia di salute per il periodo 2021-2027 («programma UE per la salute»)* (EU4Health) *e che abroga il regolamento (UE) n. 282/2014*, in particolare al considerando 6: «sebbene siano responsabili delle loro politiche sanitarie, è opportuno che gli Stati membri tutelino la salute pubblica in uno spirito di solidarietà europea (...). L'esperienza maturata con l'attuale crisi COVID-19 ha dimostrato la necessità di un'ulteriore azione risoluta da parte dell'Unione, volta a sostenere la cooperazione e il coordinamento tra gli Stati membri. Tale cooperazione dovrebbe migliorare la preparazione, la prevenzione e il controllo della diffusione di gravi infezioni e malattie umane oltre le frontiere al fine di lottare contro altre gravi minacce per la salute a carattere transfrontaliero e salvaguardare e migliorare la salute e il benessere di tutti i cittadini nell'Unione. La preparazione è fondamentale per migliorare la resilienza alle future minacce».

[18] In argomento, nella Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, 19 febbraio 2020, *Una strategia europea per i dati*, COM(2020)66 final – che sostiene la creazione, tra gli altri, di uno spazio comune europeo di dati sanitari – al punto 2 si legge: «la medicina personalizzata risponderà meglio alle esigenze dei pazienti permettendo ai medici di prendere decisioni basate sui dati, in modo tale da adeguare la strategia terapeutica giusta alle esigenze della persona giusta al momento giusto, e/o da determinare la predisposizione alla malattia e/o da attuare una prevenzione mirata e tempestiva».

sanitario, come già indicato dall'art. 40 del GDPR, pare di ausilio alla prevenzione, alla diagnosi e al trattamento delle patologie, e si pone in linea con la ricerca scientifica e l'innovazione.

3. Una cooperativa di dati operante nel settore della salute: Salus.Coop.

Nel novero delle cooperative di dati operanti nel settore della salute, un caso emblematico è rappresentato da Salus.Coop. Si tratta di una cooperativa finalizzata alla ricerca scientifica in campo sanitario che viene qui intesa come veicolo di trasformazione sociale.

La Salus.Coop, attraverso l'approccio di stampo mutualistico proprio della cooperativa, si propone di connettere le persone a progetti di ricerca con un positivo impatto sociale. Nella specie, siamo di fronte ad una sorta di *crowdfunding* ove il ruolo del "finanziatore" non è ricoperto da colui che mette a disposizione i propri risparmi, ma da colui che autorizza l'accesso e il trattamento dei propri dati che saranno così utilizzati per realizzare uno o più specifici progetti di ricerca (in particolare biomedica). Sul punto, può essere lo stesso interessato al trattamento a proporre uno specifico progetto di ricerca di suo particolare interesse.

Inoltre, è prevista l'utilizzazione di un'apposita *app* che permette un collegamento sicuro tra "donatori" di dati – sul punto si rileva l'uso improprio del lemma donatori – e ricercatori, nonché l'uso della *blockchain*: un nuovo paradigma di archiviazione e gestione dei dati le cui potenzialità applicative si rivelano di grande utilità anche nella medicina [19].

Nella specie, i ricercatori scaricano i dati dei donatori – considerati il nuovo patrimonio personale e sociale – dopo averli anonimizzati e vi possono accedere e utilizzarli solo per lo specifico progetto per il quale i dati sono stati conferiti. Il rapporto tra ricercatore e donatore può svolgersi attraverso questionari, ma sempre con l'esplicito consenso del *data subject* che riceverà informazioni personalizzate e comprensibili, potrà monitorare lo sviluppo del progetto di ricerca e avrà accesso al rapporto finale redatto dai ricercatori grazie alla valorizzazione dei dati raccolti.

---

[19] La Risoluzione del Parlamento europeo, 13 dicembre 2018, *sulla* blockchain: *una politica commerciale lungimirante*, 2018/2085 (INI), al considerando A, precisa che per *blockchain* «s'intende, salvo diversamente indicato, una tecnologia di registro distribuito (DLT) privata e soggetta ad autorizzazione, che comprende una base di dati costituita da blocchi sequenziali di dati che vengono aggiunti con il consenso degli operatori di rete»; si aggiunga che la stessa Risoluzione, al punto 25, «osserva con preoccupazione che, nei casi in cui la *blockchain* contiene dati personali, la proliferazione delle copie di dati in una *blockchain* è probabilmente incompatibile con il principio della minimizzazione dei dati di cui all'articolo 5 del GDPR». In dottrina cfr. A. CONTALDO-F. CAMPARA, Blockchain, *criptovalute*, Smart Contract, *industria 4.0. Registri digitali, accordi giuridici e nuove tecnologie*, Pisa, 2019.

Capitolo XXII

Le cooperative di dati sanitari tra codice civile e *Data Governance Act*

Stefano Faillace

Abstract: This paper analyzes the eu-derived legislation that has introduced a new type of company into our legal system: the data cooperative. In particular, the study of a subtype of it, the health data cooperative, is deepened through the investigation of some already existing international cooperatives. The compatibility of the health data cooperative with our national legal system is then assessed, also in the light of the most recent doctrine and jurisprudence.

1. L'ingresso della cooperativa di dati nel nostro sistema giuridico.

Il Regolamento UE 2022/868, denominato *Data Governance Act* ("Regolamento sulla governance europea dei dati"), nato dall'esigenza di condividere a livello europeo una quantità maggiore di dati e contrastare lo strapotere delle multinazionali d'oltreoceano che ormai gestiscono quasi indisturbate i cosiddetti *Big data*, ha introdotto un modello già censito nella prassi, basato sul ruolo dell'intermediario di dati che, nel fornire un servizio di *data sharing*, agisce come una sorta di *broker* tra "titolare dei dati" e "interessato" da un lato e "utente dei dati" dall'altro [1].

[1] Pongono l'accento sul fatto che, attraverso il *Data Governance Act*, l'UE abbia inteso perseguire l'obiettivo di incentivare la creazione di un mercato digitale unico europeo basato sull'uso e sul riuso di dati, rafforzando il ruolo delle imprese europee, F. BRAVO, *Intermediazione di dati personali e servizi di*

Tra le tipologie di intermediari descritti dalla suddetta normativa spicca la figura nuova, almeno per la nostra esperienza giuridica, della cooperativa di dati, che, in prima approssimazione, può definirsi come uno strumento atto a rafforzare l'influenza effettiva di un gruppo di persone sui propri dati personali nei confronti di terzi ("sovranità dei dati") e, allo stesso tempo, ad assoggettare tale risorsa a regole comuni di utilizzo, in vista di un obiettivo collettivo [2].

La società cooperativa è un modello d'impresa nato in funzione della realizzazione dei bisogni dei suoi promotori e partecipanti e del miglioramento delle loro condizioni sociali ed economiche [3]. Le dinamiche mutualistiche tipiche del modello cooperativo mirano, infatti, a consentire a categorie svantaggiate di soggetti – quali consumatori, utenti, lavoratori, risparmiatori – di accedere a beni, servizi od occasioni di lavoro a condizioni più convenienti rispetto a quelle offerte dal mercato [4].

---

data sharing *dal GDPR al* Data Governance Act, in *Contratto e impresa Europa*, 2021, 1, p. 199 ss.; D. POLETTI, *Gli intermediari dei dati*, in *European Journal of Privacy Law & Technologies*, 2022, 1, p. 46 ss.

[2] Il numero di cooperative di dati istituite a livello europeo è stato finora esiguo. Resta quindi da vedere se e in che misura le cooperative di dati si svilupperanno sul mercato. Cfr., in tal senso, pure A. PASCHKE-D RÜCKER, *Data governance act, Kommentar*, München, 2024, sub art. 10, p. 180.

[3] Si tratta di un modello le cui origini vengono tradizionalmente rinvenute nell'Inghilterra della metà del diciannovesimo secolo e ricondotte all'iniziativa dei cosiddetti "*probi pionieri di Rochdale*", che costituirono la *Rochdale Pioneers Equitable Society*. Sulle origini e sull'evoluzione della disciplina delle società cooperative, si vedano, tra i tanti contributi, G. BONFANTE, *La legislazione cooperativa. Evoluzione e problemi*, Milano, 1984, p. 9 ss.; A. BASSI, *Delle imprese cooperative e delle mutue assicuratrici (artt. 2511-2548)*, in *Il codice civile comm.*, diretto da Schlesinger, Milano, 1988, p. 1 ss.; V. BUONOCORE, *Diritto della cooperazione*, Bologna, 1997, 35 ss. Sulla storia del movimento cooperativo in Italia, cfr. M. FORNASARI-V. ZAMAGNI, *Il movimento cooperativo in Italia. Un profilo storico-economico (1854-1992)*, Firenze, 1997; R. ZANGHERI-G. GALASSO-V. CASTRONOVO, *Storia del movimento cooperativo in Italia. La Lega Nazionale delle Cooperative e Mutue (1886-1986)*, Torino, 1987; S. ZAMAGNI-V. ZAMAGNI, *La cooperazione*, Bologna, 2008.

[4] Tale impronta della cooperazione, d'altra parte, si coglie in tutta evidenza nella "Dichiarazione di identità cooperativa approvata dal XXXI Congresso dell'Alleanza Cooperativa Interstatale", tenutosi a Manchester nel settembre del 1995, ove si legge: «*A cooperative is an autonomous association of persons united voluntarily to meet their common economic, social, and cultural needs and aspirations through a jointly-owned and democratically-controlled enterprise*». In particolare, nella definizione di cooperativa, quale si ricava dalla «Dichiarazione di identità cooperativa», si sottolinea la sua natura di impresa posseduta e controllata da un insieme di persone, che si associano su base volontaria fra loro per soddisfare i propri comuni bisogni e le aspirazioni economiche, sociali e culturali. Il perseguimento di tali obiettivi passa attraverso il rispetto di sette principi di fondo, contenuti nella sopra ricordata Dichiarazione, che, così come sono oggi formulati, sono l'esito di un continuo lavoro di aggiornamento che ha avuto nei congressi di Parigi del 1937, di Vienna del 1966 e di Manchester nel 1995 le sue espressioni principali. Attualmente i sette principi sono i seguenti: 1) carattere aperto e volontario dell'adesione; 2) controllo democratico dei soci; 3) partecipazione economica del socio; 4) autonomia e indipendenza; 5) educazione e formazione del socio; 6) collaborazione fra cooperative; 7) partecipazione allo sviluppo della comunità locale. Cfr., in argomento, P. VERRUCOLI, *I principi dell'Alleanza cooperativa Internazionale e la loro applicazione nella legislazione italiana*, in *Riv. coop*., 1980, n. 5, p. 136 ss., G. SAPELLI, *L'A.C.I. e lo sviluppo dell'economia cooperativa*, in *Riv. coop*., 1997, I, p. 147.

La cooperazione, quindi, si è storicamente proposta e affermata come una forma organizzativa dell'attività d'impresa capace di dare impulso, attraverso metodologie produttive incentrate sulla gestione di servizio ai soci, e non ispirate da logiche speculative, all'elevazione economica e sociale delle categorie interessate; promuove e favorisce, inoltre, processi di crescita complessiva delle collettività destinatarie della sua azione. Proprio tale attitudine dell'impresa cooperativa ha condotto al riconoscimento, nell'art. 45 della Costituzione italiana, della «funzione sociale della cooperazione a carattere di mutualità e senza fini di speculazione privata» [5]. Storicamente, le cooperative sono state create per affrontare i cambiamenti sociali strutturali attraverso innovazioni economiche dirompenti. Peraltro, assecondando e metabolizzando i processi evolutivi che, negli anni, hanno attraversato la società, il fenomeno cooperativo ha vissuto sensibili mutamenti, indotti dall'esigenza di affrontare, nei diversi settori in cui esso ha trovato esplicazione, sfide nuove e sempre più impegnative e di acquisire competitività, rispetto all'impresa per così dire "lucrativa", nel quadro di mercati sempre più dinamici e sensibili alle emergenti istanze economiche e sociali e sempre più improntati alle logiche della globalizzazione [6].

D'altra parte, la proiezione dell'attività economica verso fini d'interesse generale costituisce una vocazione la cui compatibilità con i modelli organizzativi tradizionali dell'impresa, se pure non mutualistica, rappresenta un dato oggi acquisito anche in ottica normativa, se solo si considera – aldilà della disciplina speciale in tema di cooperative sociali [7] – la regolamentazione dell'impresa sociale (d.lgs. 3 luglio 2017, n. 112), che, come è noto, tale qualifica riconosce a «tutti gli enti privati, inclusi quelli costituiti nelle forme di cui al libro V del codice civile, che [...] esercitano in via stabile e principale un'attività d'impresa di interesse generale, senza scopo di lucro e per finalità civiche, solidaristiche e di utilità sociale, adot-

[5] Per una compiuta ricostruzione del dibattito sulla dimensione costituzionale del fenomeno cooperativo, cfr. A. NIGRO, *Art. 45*, in G. BRANCA (a cura di) *Commentario della costituzione italiana*, III, Bologna-Roma, 1980, p. 4 ss.; G. DE FERRA, *Principi costituzionali in materia di cooperazione a carattere di mutualità*, in *Riv. soc*., 1964, p. 776, R. ROMBOLI, *Problemi costituzionali della cooperazione*, in *Riv. trim. dir. pubbl.*, 1977, p. 105; F. GALGANO, *La cooperazione nel sistema costituzionale*, in *Nuovo dir. agr*., 1977, p. 412, B. CARBONI, *Struttura cooperativa e funzione mutualistica*, Teramo, 1977, p. 11 ss., S.M. CESQUI, *La funzione sociale della cooperazione nel progetto costituzionale*, in *Riv. soc*., 1995, p. 1153.

[6] Cfr., in tal senso, G. CAPO, *Le cooperative di comunità*, in *Giur. comm.*, 2021, 4, p. 616. In argomento, vedi da ultimo anche G. BONFANTE, *La società cooperativa*, in *Società*, 2023, 1, p. 102 ss. In questo contesto, si spiega il motivo per il quale il nostro legislatore abbia optato per scelte normative poco incisive sul piano dell'identificazione dei caratteri distintivi della cooperativa, accontentandosi di statuire essenzialmente la variabilità del capitale sociale e il voto per testa, e demandando alla legislazione speciale, ispirata dall'attribuzione alla cooperativa di specifiche funzioni, una più articolata e specifica normativa.

[7] In tale modello di cooperativa, lo scopo mutualistico è integrato dal riferimento legale allo «scopo di perseguire l'interesse generale della comunità alla promozione umana e all'integrazione sociale dei cittadini». In questo modo, la cooperativa sociale tende non solo ad assicurare il servizio mutualistico ai soci, ma anche a produrre vantaggi per la collettività (mutualità esterna).

tando modalità di gestione responsabili e trasparenti e favorendo il più ampio coinvolgimento dei lavoratori, degli utenti e di altri soggetti interessati alle loro attività» (art. 1, co. 1) [8].

Il fenomeno cooperativo, caratterizzato da un polimorfismo strutturale, fermi restando i principi generali enunciati a livello europeo, presenti nel Reg. CE n. 1453/2003 del 22 luglio 2003 sulla società cooperativa europea (SCE), trasfusi anche nel codice civile, è stato regolamentato nel nostro ordinamento, a livello extracodicistico, da norme speciali di settore la cui casistica è estremamente ampia. Si pensi alle cooperative di abitazione (cfr. r.d. 28 aprile 1938, n. 1165), le cooperative sociali (cfr. l. n. 381/91), le cooperative di credito (cfr. artt. 28 ss., d.lgs. n. 385/93) le cooperative di garanzia o confidi (cfr. art. 13, d.l. n. 269/2003) i consorzi agrari (cfr. 1. 28 ottobre 1999, n. 410).

Nonostante un'evidente inclinazione del legislatore europeo verso una torrenziale e quasi sfrenata normazione sulla *governance* dei dati, nulla è stato invece ancora concepito sulle cooperative di dati, e neppure a tale istituto si è dedicato alcun legislatore domestico nell'ambito dell'Unione. Non si può però negare che tale tipo di cooperativa, sia per la funzione sociale che dovrebbe ricoprire per riequilibrare la posizione di "sottomissione" o "dipendenza" che ha il cittadino nei confronti dei grandi operatori che bramano di ottenere dati personali, che per le peculiarità che la medesima ricopre rispetto agli altri tipi di cooperativa esistenti nel nostro ordinamento, necessiterebbe di una disciplina *ad hoc* che ne regolasse le intrinseche sue tipicità.

Allo stato, quindi, l'attività delle cooperative di dati non potrà che rimanere all'interno dei vincoli, come si è accennato, non poi così limitanti, della normativa attualmente in vigore.

2. L'incerta disciplina afferente le cooperative di dati dettata dal *Data Governance Act*.

Pur in assenza di una vera legislazione *ad hoc*, ma solo sulla base delle poche e non certo esaustive disposizioni presenti nel *Data Governance Act*, è possibile tentare di ricostruire la funzione della cooperativa di dati, che si sostanzia nel consentire agli interessati/titolari di dati personali di avere un maggiore controllo sulle

[8] Cfr., in argomento, A. FICI, *Tipo e status nella nuova disciplina dell'impresa sociale*, in *Contratto e impresa*, 2023, p. 112 ss. Non si può che concordare con chi (C. CAMARDI, *Enti collettivi e formazioni sociali, dal Libro I al Libro V attraverso il Terzo settore*, in *Contratto e impresa*, 2023, p. 470 ss.) ha rilevato come la situazione odierna esibisca uno scenario che sembra aver sostituito il paradigma dell'autonomia relativa (e della pacifica coesistenza) dei singoli sottosistemi giuridico-sociali con quello dell'*ibrido*, cioè con un paradigma che destruttura il precedente tentativo di bilanciamento istituito tra ciascuna funzione e le corrispondenti figure organizzative di riferimento. Ciò – indipendentemente dall'intenzione del legislatore – viene non solo semanticamente rappresentato dalle espressioni identificative delle discipline dei nuovi enti: "terzo settore", "impresa sociale", "società *benefit*".

proprie informazioni, di esercitare i propri diritti, di compiere scelte informate sul trattamento dei dati personali e di orientarne l'uso in base alle loro motivazioni e preferenze. Il tutto, previa raccolta o recupero collaborativo dei dati dei propri membri, ad esempio nella propria infrastruttura *cloud*, aiutando a ridurli e gestirli in un formato utile a livello di interoperabilità. Si veda infatti l'art. 12, par. 1, lett. *e*) del *Data Governance Act*, nel quale si stabilisce che i servizi di intermediazione, incluso quello di cooperative di dati, «possono comprendere l'offerta di strumenti e servizi supplementari specifici ai titolari dei dati o agli interessati allo scopo specifico di facilitare lo scambio dei dati, come la conservazione temporanea, la cura, la conversione, l'anonimizzazione e la pseudonimizzazione, fermo restando che tali strumenti e servizi sono utilizzati solo su richiesta o approvazione esplicita del titolare dei dati o dell'interessato e gli strumenti di terzi offerti in tale contesto non utilizzano i dati per altri scopi».

Le cooperative di dati mirano, quindi, a creare alternative più eque, sostenibili e socialmente responsabili rispetto alle piattaforme digitali tradizionali [9]. Sembra pertanto affacciarsi con questo nuovo strumento l'archetipo di quello che è stato definito il "*neomutualismo digitale*", come modello di crescita dell'economia, delle imprese, delle persone e della comunità, con l'obiettivo di agevolare una redistri-

---

[9] Cfr., per la dottrina italiana sulle cooperative di dati, F. BRAVO, *Cooperative di dati*, in *Contratto e impresa*, 2023, p. 757 ss.; L. PETRONE, *Il mercato digitale europeo e* le *cooperative di dati*, in *Contratto e impresa*, 2023, p. 800 ss. Per approfondimenti di dottrina straniera di taglio perlopiù economico sulle cooperative di dati, cfr. K. MILLER, 2021 *Radical proposal: data cooperatives could give us more power over our data*, consultabile in https://hai.stanford.edu/news/radical-proposal-data-cooperatives-could-give-us-more-power-over-our-data; J. KNAPP-J. KOBLER-F. RICHTER, *Data cooperatives-collective action as an opportunity for the european data economy and a european data private Law*, in *InTeR* 1/23; M. MICHELI-E. FARELL-B. CARBALLA-SMICHOWSKI-M. POSADA-SÁNCHEZ- S. SIGNORELLI- M. VESPE, *Mapping the landscape of data intermediaries: Emerging models for more inclusive data governance*, 2023 [Report], Publications Office of the European Union, in https://data.europa.eu/doi/10.2760/8943; R. GADONI CANAAN, *Data cooperatives in Brazil: applicability and property rights*, in *Revista de Direito e as Novas Tecnologias*, n. 11, 2021; I. NAEEM-A. NURUL-M. VASKA-S. GOOPY-R. RASHID-A. KASSAN-F. AGHAJAFARI-I. FERRER-A. KAZI-I. SADI-M. O'BIERNE-C. LEDUC-T.C. TURIN, *Community-based health data cooperatives towards improving the immigrant community health: a scoping review to inform policy and practice*, 2020, in https://ijpds.org/article/view/1158/3214; P. KENKEL, *Economic justification for a cooperative*, 2020, in https://cooperatives.extension.org/economic-justification-for-a-cooperative/; T. HARDJONO, T. PENTLAND, *Data Cooperatives: towards a foundation for decentralized personal data management*, in arXiv.org; F. GILLE-E. VAYENA, *How private individuals maintain privacy and govern their own health data cooperative: MIDATA in Switzerland*, in *Governing privacy in knowledge Commons*, Cambridge, 2021; pp. 53-69; A. BLASIMME-E. VAYENA-E. HAFEN, *Democratizing health research through data cooperatives*, in *Philosophy and technology*, 2018, 31(3): pp. 473-79, in https://doi.org/10.1007/s13347-018-0320-8; M. DAWANDE-S. MEHTA-L. MU, *Robin Hood to the rescue: sustainable revenue-allocation schemes for data cooperatives*, in *Production and operation management*, 2022, vol. 32, p. 8; A.S. TANWAR-N. EVANGELATOS-G.VENNE-L. OGILVIE-K. SATYAMOORTHY-A. BRAND, *Global Open Health Data Cooperatives Cloud in an Era of COVID-19 and Planetary Health*, in *OMICS: A Journal of Integrative Biology*, 2021, in https://doi.org/10.1089/omi.2020.01.

buzione equa del valore aggiunto prodotto e l'affermarsi di un'economia del riuso sostenibile e dalla circolarità comunitaria [10].

In linea di principio, le cooperative promuovono un "approccio comunitario alla condivisione dei dati", inteso come un "modello decentralizzato" in cui l'intera comunità partecipa al processo decisionale, ad esempio quando i dati sono gestiti come beni comuni. Viene, quindi, sostenuta la *governance* dal basso verso l'alto, con l'obiettivo di ridurre le asimmetrie di potere e i monopoli per la raccolta e l'utilizzo dei dati [11]. La comunità di una cooperativa di dati dovrebbe essere in grado di decidere su diverse questioni, quali le regole, le norme e i principi per l'uso dei dati; la raccolta dei dati; le finalità di utilizzo dei dati; le modalità di accesso ai dati, ecc. Attraverso tale strumento, gli interessati possono mantenere un maggiore controllo sui propri dati rispetto a quanto accade nella maggior parte degli altri regimi di *governance* ed eventualmente ricevere un'equa quota dei benefici prodotti dall'uso dei dati [12]. Il prerequisito che viene in gioco è quindi una competenza giu-

---

[10] Lo evoca F. BRAVO, *Cooperative di dati*, cit., p. 764 ss., il quale a sua volta fa esplicito riferimento agli scritti di P. VENTURI-F. ZANDONAI, *Neomutualismo. Ridisegnare dal basso competitività e* welfare, Milano, 2022. In questa direzione vanno anche le riflessioni del comitato scientifico della Fondazione PICO, che nel 2023 ha pubblicato il Manifesto del neomutualismo digitale, precisando che il medesimo potenzia le forme per affermare una corretta pratica dell'identità cooperativa, grazie alla condivisione di dati e informazioni, allo sviluppo di modalità di *governance* aperte, trasparenti e partecipate, alla circolarità di servizi e prestazioni, allo scambio di energie e tempo, allo sviluppo dei percorsi di conoscenza, alla nascita di innovativi modelli compensativi, alla definizione di nuove alleanze tra consumatori, soci e imprese, alla riduzione dei rischi sociali generati dai processi di automazione. Sempre secondo questo manifesto, il mutualismo digitale agevola una redistribuzione equa del valore aggiunto prodotto e l'affermarsi di un'economia del riuso sostenibile e dalla circolarità comunitaria. Il mutualismo digitale garantirebbe la redistribuzione dei vantaggi dell'automazione e della robotizzazione, dell'uso dei dati e dell'efficientamento produttivo, senza lasciare l'innovazione solo a beneficio del profitto. Il tema della gestione dei dati è centrale nel neomutualismo e nella distintività delle imprese cooperative rispetto a quelle capitalistiche. Per le imprese cooperative potrebbe significare il garantire un'equa redistribuzione del valore aggiunto prodotto dall'uso dei dati. Un processo che può avere implicazioni sia sulle forme di garanzia, trasparenza, tutela e gestione dei dati di proprietà del singolo individuo o della singola impresa, sia sulla facilitazione delle forme di scambio e condivisione dei dati tra le imprese e gli individui, al fine di dare valore collettivo ai dati. La realizzazione e lo sviluppo di cooperative per la gestione dei dati è, in questo ambito, lo strumento volontario che può consentire ai titolari dei dati di costruire un soggetto reticolare, di loro proprietà e con una *governance* diffusa democratica e partecipata, in grado di tutelare la proprietà dei dati dei soci, l'uso collettivo e la condivisione dei dati, nonché l'equa ripartizione dei benefici.

[11] Cfr. K. MILLER, *Radical proposal: data cooperatives could give us more power over our data*, Stanford HAI, 2021, consultabile in https://hai.stanford.edu/news/radical-proposal-data-cooperatives-could-give-us-more-power-over-our-data. Sulla distinzione tra fiduciari di dati e cooperative di dati, si veda L. SPECHT-RIEMENSCHNEIDER-A. BLANKERTZ-P. SIEREK-R. SCHNEIDER-J. KNAPP-T. HENNE, *Die Datentreuhand*, in *MMR-Beil*, 2021, p 25.

[12] Cfr., in tal senso, S. BORKIN, *Platform co-operatives – solving the capital conundrum*, 2019, consultabile in https://platform.coop/blog/nesta-foundation-proposes-gbp-1-million-investment-fund-for-platform-co-ops/; S. DELACROIX-N.D. LAWRENCE, *International Data Privacy Law*, Volume 9, 4, November 2019, pp. 236-252.

ridica ed etica della cooperativa di dati, che consenta la valutazione dei fatti e la successiva consulenza ai soci, anche attraverso organi di revisione interni o esterni e comitati etici. In questo contesto, il servizio di supporto può includere anche meccanismi di risoluzione dei conflitti dei soci nell'ambito di una procedura regolamentata [13].

La cooperativa di dati è stata definita in maniera pervero ambigua dall'art. 2, n. 16, del *Data Governance Act*, come «(...) una *struttura organizzativa* costituita da *interessati*, *imprese individuali o* da *PMI*, che sono *membri di tale struttura*». La lettera della norma non esplicita chiaramente la forma societaria, ma essa sembra potersi concretizzare anche in una «struttura organizzativa» «costituita» nella forma del gruppo cooperativo (con una cooperativa in posizione di *holding*), nella declinazione delle sue tipologie, quali il gruppo-consorzio, la cooperativa holding, il gruppo cooperativo paritetico [14]. Né può aiutare a livello ermeneutico il Reg. CE n. 1453/2003 del 22 luglio 2003 sulla società cooperativa europea (SCE), che però, lo si ricorda, esprime una sostanziale identità con la normativa italiana [15].

---

[13] Cfr., in argomento, L. SPECHT-M. HENNEMANN, *Data governance act*, Baden-Baden, 2023, p. 103 ss.; vedi pure, a riguardo, A. PASCHKE-D. *RÜCKER, Data governance act. Kommentar*, cit., p. 179 ss.

[14] In questo caso, potrebbe richiamarsi il concetto di mutualità mediata, che ha avuto il suo battesimo legislativo con il regolamento (CE) n. 1435/2003 sulla società cooperativa europea, il quale precisa che i soci possono essere anche persone giuridiche, a condizione che i membri di queste ultime siano utilizzatori dei servizi della cooperativa. Peraltro, già negli anni Sessanta, in una fase di uscita dalla marginalità economica della cooperativa, specie nel settore del consumo, abbondavano le prese di posizione della giurisprudenza sulla conciliabilità dello scopo mutualistico con lo scopo di lucro, prendendo così forma una maggiore disponibilità in ordine alla partecipazione alla cooperativa di società ordinarie (cfr. Cass., 13 dicembre 1967, n. 2943, in *Dir. fall*., 1968, II, p. 564, Cass., 24 febbraio 1968, n.632, in *Giust. civ*., 1968, I, p. 1475). Non si può negare che in molti casi le stessi leggi speciali e la prassi consentano altresì la partecipazione di enti o società, anche di capitali, in una logica di strumentalità rispetto all'attività della cooperativa. La piena legittimità di una siffatta fattispecie resta incontrovertibilmente confermata dal 1° comma dell'art. 2527 c.c., che, vietando l'accesso alla cooperativa ai soggetti che esercitano in proprio un'attività imprenditoriale in concorrenza con quella della cooperativa, legittima il fatto che possano far parte della compagine sociale imprenditori con diversi campi di attività. Con la L. n. 127 del 1971, poi, il consorzio fra cooperative ha avuto un suo adeguato riconoscimento a livello generale e nel 1983 con la c.d. Visentini-*bis* ha avuto diritto di cittadinanza la c.d. *holding* cooperativa controllante una o più società capitalistiche. Il legislatore ha introdotto poi il gruppo paritetico cooperativo con la riforma del 2003, e sono nate altre forme di collaborazione quali i c.d. contratti di rete. Su queste tipologie di cooperative, vedi F. VELLA-R. GENCO-P. MORARA, *Diritto delle società cooperative*, Bologna, 2018, p. 235 ss. Suggerisce l'ipotesi che possano essere coinvolte associazioni temporanee di imprese (ATI) o dei raggruppamenti temporanei di impresa (RTI) o, ancora, delle "reti di imprese", che svolgano "servizi di intermediazione di dati" mediante logiche di "cooperazione" a beneficio dei propri membri, F. BRAVO, *Cooperative di dati*, cit., p. 760 ss.

[15] Cfr., riguardo alla legge sulla società cooperativa europea, *ex multis*, R. DABORMIDA, *La cooperativa europea finalmente in porto*, in *Riv. Coop*., 2003, p. 123, A. CECCHERINI, *La società cooperativa europea (Regolamento CE, n. 1435/03 del Consiglio)*, in *Le nuove leggi civili commentate*, 2003, p. 1295; E. MARRA*, La società cooperativa europea*, in *Notariato*, 2005, p. 108; P. MARANO, *La società cooperativa europea e le politiche comunitarie per reti e gruppi di imprese*, in *Riv. Coop*., 2006, p. 9.

Gli obiettivi individuati dalla definizione di servizi di cooperativa di dati di cui all'art. 2, n. 16 del *Data Governance Act* sono menzionati in via alternativa. Si richiede che la predetta «struttura organizzativa» agisca con il fine principale di: aiutare i propri "membri" nel far valere le facoltà che l'ordinamento giuridico riconosce loro, favorendo l'acquisizione delle informazioni per l'esercizio dei diritti sui propri dati, in particolare qualora si tratti di dati personali; facilitare un confronto interno tra i propri "membri", basato sullo «scambio di opinioni sulle finalità e sulle condizioni del trattamento dei dati», per rappresentare «al meglio gli interessi dei propri membri in relazione ai loro dati»; «(...) negoziare i termini e le condizioni per il trattamento dei dati per conto dei membri (...)», ossia concordare con soggetti terzi, che utilizzeranno i dati, quali siano le condizioni giuridiche ed economiche volte a regolare i rapporti aventi ad oggetto l'uso di dati, personali e non personali, dei propri membri, persone fisiche o giuridiche. L'attività di negoziazione, aggiunge la definizione del servizio in questione, va svolta in un momento antecedente rispetto all'autorizzazione o al consenso al trattamento dei dati da parte dei «membri» della «struttura organizzativa» fornitrice del servizio.

Il *considerando* n. 31 precisa che «Le cooperative di dati mirano a raggiungere una serie di obiettivi, in particolare a rafforzare la posizione dei singoli individui, affinché compiano scelte informate prima di acconsentire all'utilizzo dei dati, influenzando i termini e le condizioni, stabiliti dalle organizzazioni di utenti dei dati, cui è subordinato l'utilizzo dei dati, in modo da offrire scelte migliori ai singoli membri del *gruppo*, o trovando possibili soluzioni alle posizioni contrastanti dei singoli membri di un *gruppo* in merito alle modalità di utilizzo dei dati, laddove tali dati riguardino più interessati all'interno di tale *gruppo*. In tale contesto, è importante riconoscere che i diritti a norma del Reg. (UE) 2016/679 sono diritti personali dell'interessato e che quest'ultimo non può rinunciarvi» [16].

---

[16] In sede di commento al testo della Proposta di Regolamento sulla *governance* dei dati, l'EDPB e l'EDPS hanno reso il Parere congiunto n. 3/2021, vers. 1.1 del 9 giugno 2021, ove sono state sollevate alcune critiche al *servizio di cooperative di dati*, ad iniziare dal concetto poco chiaro di tale servizio, in particolare con riferimento alla sua natura (EDPB-EDPS, *Parere congiunto sulla proposta di regolamento del Parlamento europeo e del Consiglio relativo alla governance europea dei dati (Atto sulla governance dei dati) n. 3/2021*, par. 3.4.2, p. 35, consultabile in https://www.edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032021-proposal_it). Veniva denunciata altresì l'assenza di chiarezza, in realtà, anche nella stessa definizione di tali intermediari di dati e della disciplina applicabile, con riguardo soprattutto agli obblighi a loro carico, con conseguenti rischi di incertezza giuridica nella fornitura di tali servizi. Si tratta, come visto, di problemi non risolti neanche nel testo definitivo del Regolamento. In tale parere, l'EDPB e l'EDPS affermano poi «che la posizione dei singoli individui nel compiere scelte informate e la soluzione di potenziali controversie sulle modalità di utilizzo dei dati non siano da considerarsi condizioni *negoziabili*, ma piuttosto obblighi dei titolari del trattamento a norma del regolamento (UE) 2016/679. Ancora, l'EDPB e l'EDPS hanno rinvenuto una contraddizione tra il *Considerando* n. 24 della Proposta di regolamento sulla *governance* dei dati (ora Considerando 31), in cui si trovava affermato espressamente che «i diritti a norma del regolamento (UE) 016/679 possono essere esercitati soltanto a titolo individuale e non possono essere conferiti o delegati a una cooperativa di dati» e il potere di nego-

Come visto, la definizione basata sui compiti suggerita dal *Data Governance Act* comprende le cooperative che aiutano i membri a compiere scelte informate prima di acconsentire all'uso dei dati e a negoziare termini e condizioni con gli utenti dei dati prima di dare il consenso individuale. La cooperativa di dati, insomma, dovrebbe avere la capacità di fornire agli individui e alle comunità le risorse e le conoscenze per valutare i termini del consenso. I membri della cooperativa, dopo essersi giovati della consulenza dalla struttura saranno più propensi ad accettare condizioni favorevoli e, dopo il consenso, potranno avvalersi delle competenze della cooperativa per valutare il trattamento dei dati da parte di terzi. Ciò può avvenire attraverso valutazioni etiche espresse anche da dipartimenti interni per monitorare il trattamento dei dati personali. Le cooperative di dati dovrebbero avere anche la possibilità di avviare unilateralmente negoziati contrattuali con le organizzazioni di utenti dei dati nell'interesse dei loro membri e di adoperarsi per ottenere condizioni contrattuali che meglio si adattino ai loro interessi.

Le cooperative di dati dovrebbero poi valutare le conseguenze sociali prodotte dall'implementazione di sistemi di IA da parte di terzi o aiutare a distribuire i dati in *pool* per fornire valore ai dati dei propri membri, eseguendo algoritmi in modo autonomo [17]. In taluni casi, la cooperativa potrà intervenire in proprio, quale soggetto au-

---

ziazione di cui godrebbe la cooperativa medesima su termini e condizioni da ottenere a beneficio dei soci persone fisiche, prima che questi forniscano il consenso al trattamento dei propri dati personali. Nella prospettiva dell'EDPB e dell'EDPS, «i "termini e le condizioni" per il trattamento di dati personali di fatto sono quelli contenuti nel GDPR e pertanto non possono essere modificati, né sostituiti, in virtù di un contratto o di un altro tipo di accordo privato». Cfr. però F. BRAVO, *Cooperative di dati*, cit., p. 787 ss., che evidenzia efficacemente che «i termini e le condizioni a cui fa riferimento la nuova disciplina europea sulla *data governance* – rimessi alla negoziazione delle *data cooperatives* – sono ben altra cosa rispetto alle condizioni di liceità del trattamento individuate nel GDPR quale base giuridica del trattamento. Una volta che sia stato rimosso il vincolo giuridico che impedisce lo svolgimento delle attività di trattamento a protezione dei diritti e delle libertà dell'interessato e sia operante il presupposto giuridico che consente al titolare di svolgere attività di trattamento sui dati personali – qual è, *in primis*, il consenso dell'interessato, che è atto autorizzatorio unilaterale volto a rimuovere il vincolo giuridico che l'ordinamento europeo ha previsto al fine di rimettere all'interessato le decisioni in ordine al bilanciamento degli interessati in gioco nella fattispecie di trattamento, nella prospettiva dell'autodeterminazione informativa –, l'*utilizzo* del dato personale (e non il "*dato personale*" in sé) può essere oggetto di negoziazione e di contrattualizzazione, attraverso un accordo che si raggiunge mediante un consenso di natura contrattuale (non autorizzatorio), vertente sulle condizioni economiche e contrattuali (*terms and conditions*) stabilite tra le parti [Per tale ricostruzione cfr., F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, in FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia*, Bologna, 2019, p. 140 ss.; F. BRAVO, *Lo "scambio di dati personali" nella fornitura di servizi digitali ed il consenso dell'interessato tra autorizzazione e contratto*, in *Contratto e impresa*, 2019, 1, p. 34 ss., con considerazioni rese anche a commento di due importanti *leading case* della S.C., e, segnatamente, Cass. n. 1748 del 29 gennaio 2016, caso *Segafredo Zanetti*, e Cass. n. 17278 del 2 luglio 2018, caso *AdSpray* (…) [, in cui] la Cassazione apre (…) ad una manifestazione congiunta delle due componenti, autorizzatoria e contrattuale, che rimangono tuttavia ontologicamente distinte, in quanto una incidente sul regime giuridico dei diritti della personalità, l'altra sul regime giuridico del diritto dei contratti (…)]».

[17] Cfr. F. BRAVO, *Cooperative di dati*, cit., p 785 ss., secondo cui si viene a realizzare una "*gover-*

tonomo e distinto dai propri soci; in altri casi, potrebbe intervenire come soggetto che agisce in nome e per conto dei soci; in altri casi ancora come facilitatore o mediatore per la formazione di accordi o, più in generale, di atti giuridici (anche unilaterali, come il consenso in materia di protezione dei dati personali) che verranno posti in essere direttamente dal socio o dal socio per il tramite della cooperativa, mediante il meccanismo della delega [18].

Ovviamente, l'apporto del socio-interessato alla formazione della volontà della cooperativa non può tradursi nell'automatico trasferimento alla cooperativa del potere di autodeterminazione facente capo all'interessato medesimo [19]. È ribadito il principio di irrinunciabilità dei diritti dell'interessato, incluso il diritto di revoca del consenso al trattamento dei dati personali, che non può ritenersi abdicato neanche qualora l'esercizio dei diritti fosse delegato alla cooperativa di dati. Ciò spinge a ritenere che i diritti sui dati non possano essere mai oggetto di trasferimento e, al contempo, sono da escludere operazioni volte a configurare l'apporto dei soci, che forniscono dati alle cooperative, come una sorta di conferimento "reale". I dati personali hanno tutt'altra natura e, al più, ciò che può essere conferito riguarderà il di-

---

nance" *duale*, in base alla quale le scelte strategiche ed operative delineate a livello di cooperativa di dati (tramite la "*governance* collettiva") non precludono l'esercizio della "*governance* individuale", quantomeno qualora si tratti di dati personali facenti capo a singoli membri qualificabili come interessati al trattamento ai sensi del Reg. UE n. 679/2016.

[18] Secondo L. PETRONE, *Mercato digitale europeo e le cooperative di dati*, cit., p. 800 ss., l'impostazione data al *Data Governance Act* appare limitativa per una cooperativa di dati, la quale, per conseguire efficacemente i propri scopi sociali e per contendere il primato del modello imprenditoriale lucrativo, necessiterebbe di un più ampio margine di azione. È per questa ragione che la natura personale del consenso, «(...) che pure costituisce un baluardo dell'autodeterminazione nell'ambito dei rapporti di mercato, trasposto alla sfera dei rapporti fiduciari e ai sistemi di imprenditoria sociale, meriterebbe forse di essere superato (...) sì da riconoscere la possibilità di rappresentanza nell'espressione del consenso al trattamento dei dati, con il solo limite della soggezione della procura ai requisiti fissati dall'art. 7, GDPR, e in particolare a quello della specificità».

[19] Come ricorda F. BRAVO, *Cooperative di dati*, cit., p. 789 ss., «il principio è stato già espresso dalla S.C. nella sent. n. 17911 del 1° giugno 2022 (su cui v. S. THOBANI, *Consenso al trattamento e delibere assembleari*, in *Giur. it.*, 2022, 12, p. 2599 ss.), in un caso di trattamento illecito posto in essere da una cooperativa nei confronti di un socio lavoratore, in una fattispecie in cui veniva contestato il difetto del consenso al trattamento da parte di quest'ultimo, senza che potesse supplire, in tal senso, la volontà formatasi in seno all'adozione della delibera assembleare di funzionamento della cooperativa (la fattispecie riguardava la pubblicazione in bacheca di dati relativi a contestazioni disciplinari e le valutazioni effettuate dalla cooperativa sull'attività svolta dai soci lavoratori, mediante uso di "faccine" accostate alle foto di questi ultimi, nell'ambito di un "concorso" interno). La Cassazione, nella citata sentenza, ha infatti chiarito che è priva di rilievo la circostanza che "il trattamento sarebbe stato comunque, nella specie, giustificato dal consenso espresso in seno al rapporto associativo venutosi a costituire liberamente tra i soci e la cooperativa (e tra i soci stessi). La circostanza che il rapporto abbia natura associativa (o anche organizzativa), sì che alla gestione e alla formazione della volontà dell'ente contribuiscano gli stessi soci nelle forme assembleari previste, non comporta affatto che ogni trattamento di dati divenga per ciò solo consentito dai singoli secondo le forme stabilite in assemblea"».

ritto all'utilizzo dei dati, sempre revocabile ad opera dell'interessato, ma non i dati in sé, su cui gli interessati continuano a mantenere inalterato il controllo [20]. Sembra ragionevole ritenere, però, che, mentre il divieto della rinunzia, quale tipico atto abdicativo, implichi l'impossibilità del conferimento in società (atto con efficacia reale), esso non precluda la stipula di un contratto di mandato (con rappresentanza), in quanto atto con mera efficacia obbligatoria. In questo modo, la cooperativa opererebbe per la tutela esterna dei diritti degli interessati in qualità di rappresentante dei suoi membri [21]. Che il consenso al trattamento dei dati personali non sia atto personalissimo, ma manifestabile anche tramite un rappresentante, emerge, peraltro, con evidenza nell'art. 8 GDPR, relativo al consenso dei minori, ove si trova stabilito che, nei casi in cui questi non possano esercitarlo personalmente, potrà essere esercitato, in loro rappresentanza, da chi esercita la responsabilità genitoriale [22].

Le cooperative di dati rientrano nell'ambito di applicazione del terzo capitolo del *Data Governance Act*, in quanto servizi di intermediazione di dati (art. 10 lett. c). Si differenziano, però, in maniera significativa rispetto ai servizi di intermediazione di dati di cui all'art. 10, lett. *a*) e *b*) [23].

---

[20] Lo sottolinea F. BRAVO, *Cooperative di dati*, cit., p. 757 ss.

[21] Così G. RESTA, *Pubblico, privato e collettivo nel sistema europeo di governo dei dati*, in *Riv. trim. dir. pubbl.*, 2022, 4, pp. 971-995, e, *ivi*, par. 5, e F. BRAVO, *Cooperative di dati*, cit., p 793 ss.

[22] Del resto, nessuna norma prevede espressamente il contrario. Anche in tempi più recenti, viene più volte confermata la conformità all'ordinamento giuridico della delega per l'esercizio dei diritti dell'interessato. Così, ad esempio, il Garante ha precisato che «la disciplina in materia di protezione dei dati personali prevede –in ambito sanitario – che le informazioni sullo stato di salute devono essere comunicate all'interessato e possono essere comunicate a terzi solo sulla base di un idoneo presupposto giuridico o su indicazione dell'interessato stesso previa *delega* scritta di quest'ultimo» (GPDP, provv. 29 aprile 2021, n. 174, doc. *web* n. 9676143). L'art. 80, par. 1, del GDPR prevede, poi, espressamente che l'interessato abbia «il diritto di dare mandato a un organismo, un'organizzazione o un'associazione senza scopo di lucro, che siano debitamente costituiti secondo il diritto di uno Stato membro, i cui obiettivi statutari siano di pubblico interesse e che siano attivi nel settore della protezione dei dati personali, di proporre il reclamo per suo conto e di esercitare per suo conto i diritti di cui agli artt. 77, 78 e 79 nonché, se previsto dal diritto degli Stati membri, il diritto di ottenere il risarcimento di cui all'articolo 82».

[23] La disciplina sulla fornitura del servizio di cooperativa di dati, come per gli altri servizi di intermediazione dei dati, è delineata all'art. 12 del *Data Governance Act*, contenente le «condizioni» applicabili alla fornitura del servizio. La prima "condizione" riguarda sia l'*esclusività dello scopo* relativo all'utilizzo dei dati per i quali il fornitore si appresta ad erogare il servizio, sia il *criterio di separazione,* sotto il profilo soggettivo, tra fornitore e utilizzatore dei dati intermediati. Segnatamente, l'art. 10, par. 1, lett. *a*), *Data Governance Act*, precisa che «il fornitore di servizi di intermediazione dei dati [e dunque anche il fornitore del servizio di cooperativa di dati] non utilizza i dati per i quali fornisce servizi di intermediazione dei dati per scopi diversi dalla messa a disposizione di tali dati agli utenti dei dati e fornisce servizi di intermediazione dei dati attraverso una persona giuridica distinta» Secondo F. BRAVO, *Cooperative di dati*, cit., p. 757 ss., «La norma, per come è formulata, si presta a facili elusioni, in quanto si può ben prevedere un aggiramento, nell'ambito di gruppi societari o di collegamenti tra imprese, in cui una di esse esercita il ruolo di intermediario, un'altra quello di utilizzatore dei dati». Il medesimo Autore suggerisce che «da un lato si potrebbe intervenire a livello inter-

Se i *broker* di dati hanno lo scopo di ridurre i costi di transazione attraverso la loro funzione di *match-making* e di supporto nell'esecuzione tecnica e legale delle transazioni di dati, le cooperative di dati perseguono primariamente l'obiettivo di rafforzare la formazione e l'applicazione degli interessi dei loro membri e quindi aumentare il loro controllo dei dati[24]. Queste ultime si distinguono pure per la struttura di gestione, considerando che sono composte da soci, che partecipano in una certa misura al processo decisionale e organizzativo dell'ente.

Va pure considerato il fatto che l'articolo 2 del *Data Governance Act* definisce il servizio di intermediazione dei dati come qualsiasi servizio il cui scopo sia quello di stabilire relazioni commerciali per lo scambio di dati tra un numero indeterminato di interessati e di titolari, da un lato, e gli utenti dei dati, dall'altro. Tale definizione non sembra calzante rispetto alla condizione dei soci di cooperativa, che paiono soggetti "interessati" determinati o determinabili a priori. Tutt'al più potrebbe esserlo rispetto ai titolari di *account* della piattaforma informatica della cooperativa che gestisce i dati personali, che non abbiano la posizione di socio, su cui ci si soffermerà brevemente nell'ambito dell'analisi delle cooperative di dati sanitari già operative.

Inoltre, per le stesse peculiarità strutturali della cooperativa di dati, salvo quelle che abbiano società o imprese come membri, non dovrebbero essere previsti conflitti di interesse tra chi fornisce servizi di intermediazione dei dati e l'utente dei dati, contrariamente a quanto può avvenire per gli altri intermediari di dati. Ci si chiede, quindi, per quale motivo, il legislatore abbia deciso di includere le cooperative di dati nell'ambito di applicazione del *Data Governance Act*[25]. Detto per inci-

---

pretativo, applicando in maniera non rigida la "condizione" concernente l'obbligo di separazione soggettiva tra (fornitore del servizio di) *cooperativa* di dati e *utilizzatore* di dati, volta a sterilizzarne l'applicazione in considerazione della natura mutualistica della cooperativa, al fine di far salve le norme tipiche della società cooperativa, che devono essere coordinate a livello di sistema con quelle frettolosamente inserite, sul punto, nel *Data Governance Act*. La natura stessa della cooperativa potrebbe consentire cioè un'interpretazione volta a valorizzare la funzione della "cooperativa di dati" anche in ragione di un utilizzo dei dati medesimi a favore di quest'ultima e, dunque, anche a beneficio dei soci che la vanno a costituire» (*Ibidem*). Dall'altro lato, l'Autore propone di «intervenire (…) in via normativa – in sede europea o in sede nazionale, a livello di coordinamento della disciplina domestica con quella unionale –, chiarendo in maniera più dettagliata le peculiarità della disciplina della *data governance* con riguardo al caso specifico delle "*cooperative di dati*", facendo salva l'utilizzabilità dei dati da parte di quest'ultima, nello spirito mutualistico che la contraddistingue e la contrappone al modello più tipicamente capitalistico» (*Ibidem*).

[24] Ciò che distingue le cooperative di dati da altri tipi di intermediari di dati è che esse promuovono un approccio di *governance* più democratico perché le finalità e le condizioni in base alle quali i dati vengono condivisi, elaborati e utilizzati si basano su accordi tra i membri (cfr. A. BLASIMME-E. VAYENA-E. HAFEN, *Democratizing health research through data cooperatives, in Philosophy and technology*, 2018, 31, 3, p. 473-479, DOI: 10.1007/s13347-018-0320-8).

[25] Si pone questo interrogativo pure L. VON DITFURTH, *Datenmärkte, Datenintermediäre Und Der Data Governance Act: Eine Analyse Der Europäischen Regulierung Von B2b-datenvermittlungsdiensten*, Berlin, 2023, p. 265 ss.

so, peraltro, tali differenze di struttura e funzioni tra intermediari non può che riverberarsi sull'eventuale natura della responsabilità civilistica degli uni e degli altri, in caso di illegittimo trattamento dei dati personali degli interessati, rispondendo gli intermediari di cui alla lettera a) e b) di cui all'art. 10, DGA, come soggetti autonomi, sulla base di una responsabilità precontrattuale o contrattuale a seconda dell'inquadramento del rapporto preesistente, in linea con la discussa posizione degli intermediari finanziari, e le cooperative di dati, invece, sulla base del rapporto societario, salvo per quanto si preciserà nel prosieguo, in ordine all'esistenza di contratti di servizi conclusi tra socio e cooperativa [26].

La fiducia che l'interessato deve riporre nell'intermediario è uno degli obiettivi del *Data Governance Act*, e, nel caso delle cooperative, dovrebbe essere accentuata o quantomeno preservata, oltre che dalla presenza dei controlli propri della normativa a tutela della *privacy*, anche da quelli previsti dalle norme sulle cooperative *tout court*. Accanto al controllo dei dati da parte dell'individuo, con il sistema ormai consolidato del consenso dell'interessato e ora dell'autorizzazione del titolare dei dati, a cui si aggiunge la funzione di sorveglianza dell'autorità di settore, è stato affiancato un meccanismo incentrato: sulla notifica preventiva all'autorità competente in tema di intermediazione dei dati (l'Agenzia per l'Italia digitale, AgID, ai sensi del d.lgs. 7 ottobre 2024 n. 144), accompagnata dall'istituzione del registro pubblico degli intermediari di dati tenuto dalla Commissione europea; sulla previsione di una serie articolata di condizioni di fornitura del servizio; sul monitoraggio delle conformità ad esse da parte della medesima autorità. È stato poi introdotto un sistema di esercizio "*rafforzato*" dei diritti dell'interessato, tramite l'azione esercitata dall'intermediario dei dati per conto dell'interessato, che si prospetta di maggior efficacia quando l'intermediario è una cooperativa di dati. Ma, come appena accennato, non ci si può dimenticare che la società cooperativa è sottoposta già ad

---

[26] Sulla disciplina degli intermediari finanziari, vedi *La Mifid II. Rapporti con la clientela – regole di governance – mercati*, a cura di V. TROIANO-R. MOTRONI, Milano, 2016. Per una rassegna giurisprudenziale sull'argomento, vedi G. FAPPIANO, *Gli obblighi informativi degli intermediari finanziari al vaglio della giurisprudenza*, in *Contratti*, 2019, 4, p. 424 ss. Ci si consenta, inoltre, un rinvio in argomento a S. FAILLACE, *La controversa categoria delle obbligazioni ex lege*, Milano, 2023, p. 161 ss.

Viene suggerita l'istituzione di un quadro normativo che chiarisca le questioni di responsabilità degli intermediari di cui al *Data Governance Act* nel documento dell'associazione federale dell'organizzazione dei consumatori intitolato *Verbraucherzentrale Bundesverband, 'Neue Datenintermediäre'* (*VZBV*, 15 September 2020), consultabile in: https://www.vzbv.de/sites/default/files/downloads/2020/09/17/20-09-15_vzbv-positionspapier_datenintermediaere.pdf. In senso dubitativo a riguardo, ritenendo che sia sufficiente un maggiore controllo da parte delle istituzioni di vigilanza, e che il mercato sia così immaturo che le norme esistenti lascerebbero un margine di manovra e incentivi sufficienti per sviluppare tali servizi di intermediazione, J. KÜHLING-F. SACKMANN-H. SCHNEIDER, *'Datenschutzrechtliche Dimension Datentreuhänder: Kurzexpertise' (Bundesministerium für Arbeit und Soziales, 2020)*, p. 20, in https://nbn-resolving.org/urn:nbn:de:0168-ssoar-70086-9. In argomento, vedi pure H. RICHTER, *Looking at the Data Governance Act and Beyond: How to Better Integrate Data Intermediaries in the Market Order for Data Sharing*, in *GRUR International*, 72, 5, May 2023, pp. 458-470, consultabile in https://doi.org/10.1093/grurint/ikad014.

una serie di ulteriori controlli esterni sulla gestione di natura amministrativa che si aggiungono a quello dei sindaci, delle società di revisione e dello stesso tribunale *ex* art. 2409 c.c., controlli che mirano anche a preservare il rispetto delle finalità mutualistiche in ogni espressione cooperativa ed hanno indirettamente una funzione di tutela degli interessi dei soci e dei terzi [27].

3. L'esperienza delle cooperative di dati sanitari d'oltralpe e l'ipotetica sussunzione di tali modelli nel nostro sistema giuridico.

3.1 Le sfide delle cooperative di dati sanitari tra difficile sostenibilità economica e potenziali benefici collettivi. I casi Midata e Salus.coop.

Tra le cooperative di dati, rivestono particolare importanza e saranno oggetto di analisi in questa sede quelle attinenti il settore sanitario, le quali, oltre a fornire un modello di *governance* equo per gli ecosistemi dei dati di tale tipologia, possono aspirare a garantire il miglioramento della qualità dell'assistenza sanitaria ed i progressi nella diagnostica e nella terapia, attraverso la ricerca scientifica, correggendo così l'asimmetria di potere tra interessati o titolari del trattamento dei dati e utenti dei dati, in particolare quelli del settore privato [28]. A fronte di questi potenziali benefici individuali e collettivi, le cooperative di dati sanitari devono però affrontare una sfida irta di ostacoli: il non poter disporre di un chiaro flusso di entrate.

Infatti, i dati provenienti dalle cooperative possono generare benefici non economici per i membri della comunità che hanno interessi condivisi, e che sono dediti alla raccolta e alla gestione dei dati sanitari per far progredire la ricerca sulle malattie rare o il miglioramento della salute, obiettivi che non possono essere perseguiti individualmente. Però questo tipo di incentivo è solitamente specifico per una comunità ristretta di individui. Per raggiungere la sostenibilità finanziaria, le coopera-

---

[27] La fonte giuridica dei controlli sulle cooperative citati nel testo si trova nel d.lgs. n. 220/2002, parzialmente emendato dalla l. n. 99/2009 e dall'art. 23 del d.l. 18 ottobre 2012, n. 179, ove viene statuito come questa funzione sia affidata al Ministero dello sviluppo economico, salvo per le banche popolari (Banca d'Italia), le cooperative di assicurazione (ISVAP), i consorzi agrari, le cooperative edilizie a contributo erariale, le cooperative con sede nelle regioni a statuto speciale per le quali la vigilanza spetta a soggetti diversi. L'altro soggetto protagonista nell'attività di vigilanza nel nostro ordinamento è rappresentato dalle organizzazioni di rappresentanza. Sul tema, vedi S. PATANÈ, *La revisione cooperativa*, in E. CUSA (a cura di), *La cooperativa s.r.l. fra legge e autonomia statutaria*, Padova, 2008, p. 489; C. TEDESCHI, *I controlli*, in G. MARASÀ (a cura di), *Le cooperative prima e dopo la riforma societaria*, Padova, 2004, p. 717, P. MORARA, *Il sistema dei controlli*, in R. GENCO (a cura di), *La riforma delle società cooperative*, Milano, 2003, p. 211, M. IENGO, sub art. 2545-*quaterdecies*, in G. BONFANTE-D. CORAPI- G. MARZIALE-R. RORDORF-V. SALAFIA (a cura di), *Codice delle società commentato*, Milano, 2011, p. 1851, E. CUSA, *La vigilanza sulla gestione delle cooperative nella legge n. 142 del 2001*, in *Riv. coop*., 2002, p. 33.

[28] Cfr. J. WILBANKS-E. TOPOL, *Stop the privatization of health data*, in *Nature*, 2016, 535, p. 345 ss.

tive di dati dovrebbero condividere i dati a fronte di un corrispettivo economico di terze parti e utilizzare una parte del valore generato per sostenersi. Tuttavia, nel caso il progetto sia di nicchia e manchi di *input* continui da parte degli interessati, il reddito ottenuto rischia di essere molto limitato e non sufficiente a garantire la sostenibilità dell'ente [29]. Anche se la cooperativa di dati avesse una base di utenti sufficientemente ampia, gli incentivi che guidano il loro coinvolgimento dovrebbero essere sostenuti nel tempo. Se, ad esempio, la ricompensa non economica che gli interessati ottengono è *una tantum*, ma la loro dedizione è necessaria in modo continuativo, c'è il rischio di un disimpegno a breve o a medio termine.

Nelle cooperative di dati sanitari, come vedremo, gli individui caricano e condividono dati, allo scopo di sostenere la ricerca scientifica, mantenendo al contempo un controllo granulare sui propri dati personali (conservando la possibilità di limitare o revocare l'accesso). Pertanto, dopo il consenso alla raccolta, i dati non scompaiono in banche dati inaccessibili, ma è consentito agli utenti di modificare le autorizzazioni di accesso in qualsiasi momento e di conoscere per quale scopo vengono utilizzati i propri dati. Ciò è reso possibile da sistemi tecnici, che includono l'archiviazione *cloud*, l'infrastruttura informatica, la gestione del consenso, le applicazioni *front-end* e *back-end* per l'accesso, la manipolazione e l'analisi dei dati e le considerazioni sulla sicurezza.

L'organizzazione collettiva e la messa in comune delle risorse nelle cooperative avranno peraltro lo scopo di attribuire ai membri un potere di contrattazione collettiva attraverso il quale possono negoziare con centri di potere esterni, quali, ad esempio, le aziende farmaceutiche. A tal proposito, le cooperative di dati potrebbero concedere un beneficio anche economico nel fornire un *surplus* ai propri membri, utilizzando dati aggregati elaborati per ottenere un valore aggiunto. Tuttavia, le cooperative che cercano di mettere in comune ed elaborare dati aggregati sembrano non rientrare nelle funzioni consentite dal *Data Governance Act* (cfr. Considerando

[29] Le cooperative di dati hanno un alto rischio di fallimento, in quanto affrontano problemi di sostenibilità a causa del fatto che il loro modello di *business* sottende iniziative altruistiche, volontarie e condotte da privati. Si pensi al caso della cooperativa europea, con sede a Berlino, denominata Polypoly, che si è brevemente affacciata in questo panorama, con il fine dichiarato di aiutare i suoi soci a rivendicare la sovranità sui propri dati. Ogni membro della cooperativa poteva scaricare un'applicazione che memorizzava i dati dell'utente sul dispositivo personale. Questa applicazione aveva pure la funzione di raccogliere e ordinare i dati presenti *online* dell'interessato. I soci della cooperativa potevano scegliere come rendere disponibili i propri dati, in forma di donazione o a pagamento e se inoltrarli o meno in *database* di terze parti. In caso di scambio di denaro, la cooperativa riceveva una piccola percentuale da distribuire poi a tutti i soci della cooperativa. Purtroppo, a quanto risulta, l'avventura di questa società è già volta al termine, essendo attualmente in liquidazione. Anche LunaDNA, cooperativa di dati con sede a San Diego, California, che, offrendo un compenso, intendeva sollecitare le persone a condividere i propri dati personali, ha in realtà avuto vita breve (risulta essere stata cancellata in data 31 gennaio 2024). Destino diverso pare avere, invece, Savvy Cooperative, con sede a New York, che propone uno schema diverso, offrendo un *database* per i propri membri e promettendo ai medesimi un corrispettivo economico variabile a seconda del contributo proposto durante l'anno ai progetti di ricerca considerati dalla cooperativa degni di essere sviluppati.

n. 28). Inoltre, la possibilità che l'interessato ottenga un corrispettivo economico per condividere i propri dati sanitari è stata ampiamente criticata da chi ritiene che in tal modo si amplifichino le disuguaglianze, con riduzione dell'altruismo, suggerendo, a contrasto, l'idea del dato sanitario come una proprietà collettiva [30].

Lo stato di fatto, anche precedente all'emanazione ed entrata in vigore del *Data Governance Act*, ci ha presentato tipologie di cooperative di dati che hanno funzioni e svolgono compiti diversi. Alcune cooperative cercano di isolarsi dal mercato adottando uno *status* senza scopo di lucro: ciò consente all'ente di godere di determinate forme di sgravio fiscale e rende ammissibili in suo favore sovvenzioni, finanziamenti governativi, ecc. Tuttavia, è probabile che questa forma di finanziamento sia, da sola, insufficiente per i costi considerevoli che comporta, ad esempio, lo sviluppo e l'utilizzo del *software* dedicato di cui necessita l'ente per i servizi per la gestione dei dati. Altre cooperative operano come entità commerciali, il che apre la possibilità di ricevere finanziamenti da una gamma più ampia di operatori del mercato, quali investitori esterni, come categoria di membri particolari all'interno della cooperativa che detengano una classe distinta di azioni o valutando l'emissione di obbligazioni cooperative, titoli di partecipazione e certificati senza diritto di voto. Il fatto che possano coesistere motivazioni economiche senza scopo di lucro, imprenditoriali e altre motivazioni economiche ibride conferma più in generale l'ambivalenza delle cooperative, cui non possono far eccezione le cooperative di dati.

Le cooperative di dati sanitari che, nel prosieguo, saranno oggetto di analisi si configurano come cooperative dichiaratamente senza scopo di lucro. All'esito di tale studio, valuteremo se, in quanto tali, siano o meno destinatarie della disciplina di cui agli artt. 10-14 del *Data Governance Act* e segnatamente delle condizioni per la fornitura di servizi di intermediazione dei dati (art. 12).

La cooperativa di dati Midata, fondata nel 2015 da un gruppo di ricercatori dell'ETH Zurigo e dell'Università di Scienze Applicate di Berna, è un'istituzione senza scopo di lucro [31], con una motivazione altruistica che va oltre la stessa comunità dei suoi membri e tesa a creare beneficio per l'intera società, come proclamato dall'art. 2 del suo statuto [32]. Tale cooperativa gestisce una piattaforma informatica definita "sicura" per l'archiviazione, la gestione e la condivisione di dati personali di qualsiasi tipo, in particolare dati sanitari e relativi all'istruzione, e per fornire i pertinenti servizi. Da un lato, afferma di «promuovere l'autodeterminazione digitale della popolazione consentendo ai titolari di conti di utilizzare i propri dati personali

---

[30] Cfr., in tal senso, B. PRAINSACK-N. FORGÓ, *Why paying individual people for their data is a bad idea*, in *Nature Medicine*, 2022, 28, p. 1989 ss.

[31] In base alla legge delle obbligazioni svizzera, all'art. 828, "la società cooperativa è l'unione di un numero variabile di persone o di società commerciali, organizzata corporativamente, la quale si propone in modo principale l'incremento o la salvaguardia, mediante un'azione comune, di interessi economici dei suoi membri o persegue uno scopo di utilità pubblica".

[32] Lo statuto è consultabile al seguente indirizzo: https://midata.coop/docs/MIDATA_Statuten_20170905.pdf.

secondo i propri desideri, in particolare per sostenere scopi di ricerca»; dall'altro «promuove gli interessi collettivi dei titolari dei conti, consentendo l'utilizzo dei loro dati personali come risorsa comune». Adotta un approccio di *governance* chiamato "supervisione sistemica" che si basa sui principi di adattabilità, flessibilità, monitoraggio, reattività, riflessività e inclusività, per affrontare le preoccupazioni relative alla *privacy*, contribuendo attivamente alla ricerca medica e agli studi clinici, garantendo ai propri membri un accesso selettivo ai propri dati personali [33].

Chiunque può aprire un conto sulla piattaforma Midata o diventare socio della cooperativa (conferendo un contributo), il che ha il potenziale per rafforzare tale ente, aumentando il volume di dati e quindi il valore per la ricerca, e facilita la democratizzazione dell'economia dei dati. Il titolare di un *account* deposita copia dei propri dati (che usualmente sono stati raccolti e archiviati altrove), e poi sceglie di renderli accessibili ai ricercatori, sulla base di progetti di ricerca. Tale cooperativa, peraltro, rimborsa le strutture sanitarie che forniscono dati in formato *standard*, partendo dal presupposto che tali dati possano generare entrate da reinvestire nella cooperativa stessa. I dati memorizzati da Midata sui *server* situati in Svizzera sono crittografati e accessibili solo dal titolare dell'*account*, a meno che il medesimo non li rilasci per uno scopo specifico. Il titolare di *account* può richiedere la cancellazione dei propri dati in qualsiasi momento, ma può anche condividere i propri dati personali (o specifici sottogruppi dei propri dati personali) con altri titolari di conto, con la cooperativa o con terzi. L'accesso da parte della cooperativa e da parte di terzi ai dati personali di un titolare di *account* richiede ovviamente il consenso espresso e informato di quest'ultimo, sia che i dati personali siano in forma originale, sia che siano in forma criptata (collegata attraverso una chiave ad una persona determinata) o anonima. Il consenso, peraltro, è gestito elettronicamente direttamente tramite la cooperativa. I titolari del conto hanno il potere decisionale esclusivo su quali dati devono essere memorizzati all'interno della cooperativa e quali dati rilasciare in vista di un progetto di ricerca.

---

[33] In argomento, vedi F. GILLE-E. VAYENA, *How private individuals maintain privacy and govern their own health data cooperative – MIDATA in Switzerland*, in M. SANFILIPPO-K. STRANDBURG-B. FRISCHMANN, *Governing Privacy as Knowledge Commons*, Cambridge, 2021; S. GIRISH-M. AVERY, *Data Cooperative: Enabling Meaningful Collective Negotiation of Data Rights for Communities,* 2022, consultabile in https://ssrn.com/abstract=4414473; A. BLASIMME-E. VAYENA-E. HAFEN, *Democratizing Health Research Through Data Cooperatives*, Philos. Technol., 2018, 31, p. 473 ss., consultabile in https://doi.org/10.1007/s13347-018-0320-8; J. RODON MÒDOL, *Citizens Cooperation in the Reuse of Their Personal Data: The Case of Data Cooperatives in Healthcare*, in K. RIEMER-S. SCHELLHAMMER-M. MEINERT, *Collaboration in the Digital Age: how technology enables individuals, teams and businesses*, in *Progress in IS*, Berlin, 2018, p. 159 ss., consultabile in https://doi.org/10.1007/978-3-319-94487-6_8; I. VAN ROESSEL-M. REUMANN-A. BRAND, *Potentials and Challenges of the Health Data Cooperative Model*, in *Public health genomics* 20, n. 6 (2018), pp. 321-331, consultabile in https://doi.org/10.1159/000489994; *CNIL (Commission Nationale de l'Informatique et des Libertés) and Analysis of Big Data Projects in the Health Sector*, consultabile al link: https://link.springer.com/chapter/10.1007/978-3-030-32161-1_29.

La cooperativa si serve di un revisore indipendente e gli utenti dei dati devono presentare una proposta per l'utilizzo dei dati dei soci che deve essere esaminata dal comitato etico. Questo organo valuta gli strumenti a garanzia della *privacy* offerti dall'utente dei dati-richiedente e poi relaziona all'assemblea generale. Se tale proposta viene valutata positivamente dal comitato etico, il titolare dell'*account* può acconsentire a rilasciare i propri dati per il progetto specifico. Infatti, i meccanismi di supervisione all'interno della cooperativa garantiscono una valutazione scientifica ed etica delle richieste di accesso ai dati in entrata, ma gli interessati mantengono il controllo sull'opportunità di concedere tale accesso.

Inoltre, gli interessati possono diventare soci della cooperativa, ed in tal caso esercitano un controllo sulla medesima in occasione dell'assemblea generale, cui possono partecipare. I soci partecipano inoltre alla *governance* della piattaforma, direttamente o indirettamente (ad esempio, eleggendo i membri dei comitati di sorveglianza) ed esercitano un controllo collettivo sull'intero *set* di dati, decidono come reinvestire i ricavi ed elaborano politiche per attività o questioni specifiche.

La cooperativa non fornisce alcun servizio che consenta ai titolari di *account* di vendere l'accesso ai propri dati personali a fronte di un corrispettivo individuale. Si evita in tal modo la creazione di incentivi finanziari personali in grado di creare problemi di tipo etico. Se l'uso secondario dei propri dati personali è richiesto da parte di terzi, il titolare di *account* può però chiedere in cambio una remunerazione economica da devolversi alla cooperativa. Ciò fermo restando il fatto che la cooperativa non distribuisce dividendi e non garantisce ai propri membri e ai titolari di *account* alcun indennizzo. Per finanziarsi, inoltre, la cooperativa può svolgere attività di investimento finanziario, detenere partecipazioni in altre società in Svizzera e all'estero, acquistare, detenere e vendere beni immobili. L'utile di bilancio deve però essere utilizzato per il miglioramento dei servizi offerti con e tramite la piattaforma Midata da un punto di vista qualitativo-quantitativo, per assicurare la sostenibilità finanziaria e perseguire gli scopi di utilità pubblica che si prefigge la cooperativa. Ciò dovrebbe garantire al contempo elevati *standard* di sicurezza e tutela dei dati. Tale cooperativa può, inoltre, sostenere la costituzione di cooperative di pari utilità in Svizzera e all'estero e costituire insieme ad esse una federazione di cooperative. Similare all'esperienza di Midata, è quella di Salus.coop, una cooperativa di dati, pure senza scopo di lucro, con sede in Barcellona, fondata nel 2017, che mira a facilitare la condivisione sicura dei dati sanitari, consentendo ai cittadini di controllare le proprie cartelle cliniche, e incentivando al contempo l'innovazione della ricerca sanitaria. È definita come una società cooperativa di consumatori e utenti, soggetta ai principi e alle disposizioni della Legge sulle cooperative della Catalogna [34]. Ai sensi dell'art. 115 della suddetta legge, «obiettivo primario delle

[34] La l. n. 12/2005 delle cooperative catalane si basa sui principi generali storici dell'Alleanza cooperativa internazionale (ICA) e, in particolare, afferma che la cooperativa è un'associazione autonoma di persone unite volontariamente per soddisfare i propri bisogni e le proprie aspirazioni economiche, sociali e culturali comuni attraverso un'impresa di proprietà comune e controllata democraticamente.

cooperative di consumatori e utenti è la consegna di beni o la prestazione di servizi per il consumo diretto dei soci e delle loro famiglie, e lo sviluppo delle attività necessarie a promuovere l'informazione, la formazione e la difesa dei diritti dei consumatori e degli utenti» [35]. Ai sensi dell'art. 2 dello statuto della cooperativa Salus, lo scopo di tale ente è: *a*) operare attraverso una piattaforma informatica sicura per la conservazione, la gestione e lo scambio di dati personali di ogni genere, ed in particolare dati sanitari e scolastici per fornire i relativi servizi; *b*) mettere a disposizione delle persone fisiche la piattaforma informatica per l'utilizzo da parte dei titolari di *account* di dati personali; *c*) sviluppare le attività necessarie per l'incremento dell'informazione, della formazione e della difesa dei diritti dei consumatori e degli utenti. La cooperativa può svolgere il proprio oggetto sociale direttamente o indirettamente, anche attraverso la partecipazione in altre società. Ai sensi dell'art. 5 dello statuto, in maniera generica, si stabilisce che può essere socio chiunque desideri ottenere beni e/o servizi, per il proprio consumo e uso e quello delle proprie famiglie nelle migliori condizioni di qualità, opportunità, informazioni e prezzi. Ai sensi dell'art. 6 dello Statuto, per l'ammissione di una persona come membro, occorre sottoscrivere il contributo minimo obbligatorio al capitale sociale.

Salus.coop fornisce consulenza ai propri soci in ordine all'utilizzo dei propri dati ed effettua controlli di *due diligence* sugli utenti dei dati, crea, inoltre, un modello di *governance* collaborativa per la gestione dei dati sanitari, che consente ai membri di decidere quale ricerca sostenere. Le persone che intendono "donare" i propri dati sanitari possono essere informate e assistite dalla cooperativa, che fornisce loro le informazioni necessarie per decidere con consapevolezza. Le persone che ripongono fiducia nella cooperativa possono delegare le decisioni ad essa.

Al socio viene chiesta una quota associativa in denaro. Una parte di questo contributo sarà collocata nel fondo cooperativo e il resto sarà fornito all'individuo sotto forma di SalusCoin nel suo portafoglio personale. SalusCoin è la moneta interna

[35] È noto che il modello di cooperazione di consumo sia tra quelli più diffusi anche in Italia e si articola in diversi settori dell'economia. Tra le manifestazioni più risalenti di tale tipologia di cooperativa può citarsi la cooperazione di abitazione, di credito o di assicurazione, ma stanno emergendo già da alcuni anni altre tipologie di cooperative tra consumatori, quali – a titolo di esempio – quelle per l'acquisto di energia. Il legislatore italiano non ha avvertito la necessità di dedicare a questa categoria di cooperazione una disciplina speciale. La normativa riferita al modello delle cooperative di consumo è quindi quella generale presente nel codice civile, né vi è una nozione di cooperativa di consumo e/o del suo scopo mutualistico. Quest'ultimo è stato ricostruito dalla dottrina o da circolari dei Ministeri competenti: i soci consumatori conseguono il vantaggio mutualistico attraverso un risparmio di spesa nell'ambito di rapporti di scambio originati da autonomi contratti intercorsi tra i soci stessi e la cooperativa. Il primo riferimento alla cooperazione di consumo nel codice civile è previsto dall'art. 2512 c.c., il quale afferma, tra l'altro, che sono società cooperative a mutualità prevalente quelle che «svolgono la loro attività prevalentemente in favore dei soci, consumatori o utenti di beni o servizi». L'art. 2513 c.c. precisa poi che le cooperative di consumo acquisiscono il requisito della prevalenza mutualistica qualora dimostrino di avere ricavi dalle vendite dei beni e dalle prestazioni di servizi verso i soci superiori al cinquanta per cento del totale dei ricavi delle vendite e delle prestazioni, ai sensi dell'art. 2425, co. 1, punto A 1, c.c.

sviluppata dalla cooperativa, che dà valore ai dati e alla partecipazione dei soci della cooperativa. I membri della cooperativa non ricevono incentivi monetari personali, per questo motivo è stata proposta la creazione di tale moneta interna, che permette alla cooperativa di premiare il contributo di tutti i soggetti coinvolti nel rendere possibile il modello. Più dati corrispondono a più SalusCoin. I cittadini possono utilizzare SalusCoin per acquisire servizi da fornitori accreditati o per finanziare progetti di ricerca promossi dalla cooperativa.

È prevista poi la creazione di un fondo di proprietà della cooperativa atto a concedere finanziamenti a specifici progetti di ricerca. Salus.coop si propone di offrire condizioni migliori ai progetti di ricerca più in linea con i valori delle cooperative e addebitare un prezzo più alto per i progetti considerati meno pertinenti dai membri della cooperativa (ad esempio, ricerca malattie rare vs. ricerca su chirurgia estetica). Pertanto, grazie a questo fondo, la cooperativa è in grado di contribuire ai campi di ricerca ritenuti più importanti, non solo con i dati, ma anche con le risorse finanziarie.

Come è possibile notare, nello svolgersi della vita societaria di entrambe le cooperative di dati sanitari analizzate, i rapporti tra le parti sono vincolati da una serie di accordi contrattuali che delineano il comportamento etico, lo scambio di valori, gli standard tecnologici, i termini di utilizzo dei dati, ecc., che le parti devono accettare. Tali accordi richiedono la gestione degli interessi divergenti delle parti, affrontando questioni quali le licenze, la proprietà intellettuale e la protezione dei dati. Un ruolo importante della cooperativa è quello di garantire il rispetto di questi accordi. Il contenuto specifico di tali accordi proviene da una decisione collettiva dei membri del gruppo. Innanzitutto, viene in rilievo l'accordo sul trasferimento dei dati tra gli interessati e la cooperativa. L'accordo stabilisce il diritto dei primi di essere "ricompensati" con dati meglio strutturati rispetto ai dati iniziali forniti. In altre parole, i dati saranno restituiti dopo essere stati ordinati e trattati in forma anonima e sicura. Vi è poi un contratto tra le società fornitrici di servizi e la cooperativa, nonché tra le prime e gli utenti dei dati o i membri della cooperativa. Per poter concludere tali contratti, le aziende esterne devono ricevere l'accreditamento rilasciato dalla cooperativa. Vi è infine un accordo di sfruttamento, destinato agli utenti dei dati che effettuano richieste di accesso ai dati dei membri. Il nucleo di questo accordo regola l'utilizzo consentito dei dati, le condizioni in base alle quali i dati vengono messi a disposizione e gli obblighi a cui gli utenti dei dati devono attenersi. Copre anche i criteri che governano il flusso economico tra le parti. Stabilendo il tipo di utilizzo dei dati consentito, questo accordo è finalizzato all'obiettivo precipuo di accelerare la ricerca e generare benefici collettivi. L'accordo riguarda anche la titolarità della proprietà intellettuale, le condizioni di licenza e di pubblicazione per i servizi sviluppati utilizzando l'insieme di dati cooperativo. A tale riguardo, un obiettivo importante dell'accordo è la promozione di licenze che garantiscano il prezzo più basso possibile dei farmaci (ad esempio *royalty free*, non esclusivo), riservatezza limitata e condivisione aperta delle conoscenze (ad esempio *Creative Commons*, pubblicazioni ad accesso aperto).

3.2. L'ambito di applicazione soggettivo della disciplina concernente gli intermediari dei dati nel *Data Governance Act* e la sottile linea di confine tra concetto di "*no profit*" e "altruismo dei dati". I contratti di servizi tra soci e società cooperativa di dati sanitari e il relativo vantaggio mutualistico.

Come già rilevato, le due cooperative di dati sanitari analizzate dichiarano di non avere scopo di lucro, e, in tal senso, per come sono attualmente strutturate, non sembrerebbero loro applicabili, a prima vista, gli artt. 10 ss. del *Data Governance Act*, ma la disciplina dedicata agli enti per l'altruismo dei dati di cui agli artt. 16 ss. della medesima norma. Del resto, le organizzazioni per l'altruismo dei dati riconosciute nell'Unione e i servizi di intermediazione di dati, nell'ambito di tale regolamento europeo, sono soggetti che hanno punti di contatto fra loro e, in alcuni casi, i loro modelli sembrano sovrapporsi.

Occorre, quindi, un breve approfondimento a riguardo, visto che tali cooperative di dati si inseriscono in un dibattito già incandescente sul concetto di *no profit* nell'interpretazione vigente in sede unionale e nel nostro ordinamento [36]. Di recente la Corte di Giustizia dell'Unione Europea ha tracciato un chiaro confine tra organizzazioni lucrative e organizzazioni non lucrative, confine che è certamente vincolante per chi è chiamato a interpretare il diritto dell'Unione europea (e pertanto anche il conseguente diritto italiano di attuazione) in materia di contratti pubblici, ma allo stesso tempo utilizzabile al fine di fissare il perimetro dell'economia sociale e distinguere le diverse forme di enti, anche con limitati scopi lucrativi. Secondo la Corte di Giustizia le "organizzazioni e associazioni senza scopo di lucro" (di cui all'art. 10, lett. *h)*, Dir. 2014/24/UE) sono quelle che "hanno l'obiettivo di svolgere funzioni sociali", "non hanno finalità commerciali" e "reinvestono eventuali utili al fine di raggiungere l'obiettivo della stessa organizzazione o associazione". Non sono, invece, sussumibili tra gli enti *no profit*, secondo tale orientamento, quelli il cui statuto consenta la distribuzione degli utili tra i soci, anche solo a titolo di ristor-

[36] In generale, sull'argomento, vedi da ultima C. CAMARDI, *Enti collettivi e formazioni sociali, dal Libro I al Libro V attraverso il Terzo settore*, in *Contratto e impresa*, 2023, p. 470, ss. secondo cui vi è un affievolimento della dicotomia concettuale tra scopo lucrativo e non lucrativo, da tempo avvertito da autorevoli studiosi, attraverso il riferimento sia al tramonto dello scopo lucrativo nelle società, con riferimento ad alcuni tipi sociali, sia – correlativamente – alla funzionalità della figura fondazione all'esercizio di un'impresa. Cfr., ad esempio, Cass. civ., sez. I, 27 ottobre 2023, n. 29801, in *Fallimento*, 2023, 12, p. 1492, che ricorda che le imprese sociali disciplinate dal d.lgs. n. 112/2017, a differenza degli enti del terzo settore (di cui al parallelo d.lgs. n. 117 del 2017), possono assumere tanto la forma organizzativa societaria (del Libro V del c.c.), che quella *lato sensu* associativa o fondazionale (del Libro I c.c.). Le imprese sociali, conservando l'assenza di scopo di lucro e le finalità civiche solidaristiche o di utilità sociale e secondo criteri di gestione e partecipazione solidaristica, possono dunque assumere la veste giuridica di società, cooperative comuni, cooperative sociali o loro consorzi. La possibilità di limitate forme di remunerazione del capitale o le regole sui ristorni hanno poi attenuato il distanziamento in termini assoluti tra *non profit* e scopo di lucro (in argomento, vedi pure MARASÀ, *Imprese sociali, altri enti del terzo settore, società* benefit, Torino, 2019).

no [37]. Ebbene, negli statuti delle sopra analizzate cooperative di dati sanitari non sono contemplati ristorni. Inoltre, tali cooperative non forniscono alcun servizio che consenta ai titolari di *account* di cedere la possibilità di utilizzare i propri dati personali a fronte di un corrispettivo individuale. Tali cooperative, poi, non distribuiscono dividendi e non garantiscono ai propri membri e ai titolari di *account* alcun indennizzo. Dunque, anche secondo l'interpretazione della Corte di Giustizia europea, tali enti dovrebbero correttamente essere inseriti tra quelli che non perseguono un fine di lucro. Peraltro, i titolari di *account* o i soci di tali cooperative possono dare un esplicito consenso informato per l'uso secondario dei propri dati personali da parte di terzi, in cambio di una remunerazione economica da devolversi alla cooperativa per il raggiungimento dei fini propri di essa. E ciò confligge con l'art. 2, punto 16, del *Data Governance Act*, secondo cui le organizzazioni riconosciute per l'altruismo dei dati non dovrebbero «chiedere o ricevere una ricompensa che vada al di là del compenso relativo ai costi sostenuti quando mettono a disposizione i loro dati per obiettivi di interesse generale» [38]. Ci troviamo, quindi, di fronte a cooperative senza scopo di lucro che svolgono attività commerciale solo al fine di perseguire il proprio sostentamento, ma che non possono, per ciò solo, essere inserite tra gli enti per l'"altruismo dei dati" e rispettare la relativa disciplina.

Per giungere ad inquadrare la disciplina corretta cui possono essere assoggettate tali cooperative di dati sanitari, corre in soccorso, dunque, quanto stabilito dall'art. 15 del *Data Governance Act*, il quale traccia le condizioni di applicabilità della normativa di cui agli artt. 10 ss., nei seguenti termini: «Il presente capo non si applica alle organizzazioni per l'altruismo dei dati riconosciute o ad altre entità senza scopo di lucro nella misura in cui le loro attività consistono nel cercare di raccogliere, per obiettivi di interesse generale, dati messi a disposizione da persone fisiche o giuridiche sulla base dell'altruismo dei dati, a meno che tali organizzazioni e entità non puntino a stabilire relazioni commerciali tra un numero indeterminato di interessati e titolari dei dati, da un lato, e utenti dei dati, dall'altro». E tra le organizzazioni senza fini di lucro che puntano, per sostenersi, a stabilire relazioni com-

---

[37] Cfr. Corte Giustizia Unione Europea, Sez. VIII, 7 luglio 2022 n. 213/21, in *Società*, 2023, p. 21, con nota di E. CUSA, *La nozione unionale di organizzazione non lucrativa tra contratti pubblici, terzo settore e trasporti sanitari di urgenza*, che afferma che i ristorni sono da considerarsi una quota dell'utile di esercizio, quand'anche fossero regolati dalla cooperativa come costi derivanti da appositi negozi parziari (nel medesimo senso, anche Cons. Stato, 3 maggio 2022, n. 3460 e Cass. civ., 30 agosto 2022, n. 25495, entrambe in *Dejure*).

[38] È stato il *Data Governance Act* a definire per la prima volta giuridicamente il termine "altruismo dei dati". È interessante notare che tale Regolamento europeo non usa il termine "donazione" e il richiamo a tale istituto pare sia stato deliberatamente evitato dal legislatore, in quanto implica il trasferimento di proprietà, mentre il diritto fondamentale alla protezione dei dati personali non può essere ceduto. Il concetto di altruismo dei dati sottende un consenso volontario e proattivo degli interessati all'uso dei loro dati per obiettivi di interesse generale, come la ricerca scientifica o il miglioramento dei servizi pubblici. In argomento, si rimanda a F. BRAVO, *Il principio di solidarietà tra data protection e data governance*, in *Dir. inf.*, 2023, p. 481 ss.

merciali tra un numero indeterminato di interessati (se non i soci, che paiono soggetti determinabili *a priori*, i titolari di *account* delle piattaforme della cooperativa, che invece non lo sono) e titolari dei dati, da un lato, e utenti dei dati, dall'altro, paiono annoverarsi società cooperative quali Midata e Salus.coop, che quindi ben potrebbero essere prese a modello per la costituzione di future cooperative di dati ai sensi dell'art. 10 lett. *c)* del *Data Governance Act*. Tali cooperative, infatti, da statuto, prima che i propri membri diano il loro consenso al trattamento dei dati personali, aiutano i medesimi nell'esercizio dei loro diritti, consentendo loro di operare scelte informate ed eventualmente anche negoziando i termini e le condizioni per il trattamento dei dati (in linea con quanto stabilito all'art. 2, n. 15 del *Data Governance Act*). Dovranno, altresì, sottostare alle condizioni per la fornitura dei servizi di cui all'art. 12, oltre che ai controlli e monitoraggi da parte delle autorità competenti per il servizio di intermediazione dei dati disciplinati dagli artt. 13 e 14 del *Data Governance Act*.

Ma è legittimo porsi ancora una domanda. È possibile nell'ordinamento cooperativo italiano attuale escludere con apposita clausola statutaria, come sembrerebbe avvenire per le due cooperative di dati sopradescritte, la ripartizione dei ristorni, una delle forme attraverso cui il socio può partecipare ai vantaggi cooperativistici, vantaggi che possono avere contenuto diverso a seconda del tipo di cooperativa? Per un'impostazione dottrinale, in assenza di una norma del nostro ordinamento che riconosca esplicitamente o implicitamente un diritto al vantaggio mutualistico e che riconosca più in particolare un diritto al ristorno, tale tipo di clausola sarebbe legittimo [39]. Ma l'interpretazione contraria ha solide basi normative nell'art. 2521, n. 8, c.c., il quale pretende che lo statuto indichi i criteri di ripartizione dei ristorni, e nell'art. 2545 *sexies* c.c., che precisa che il ristorno remunera il servizio mutualistico in ragione della qualità e quantità degli scambi mutualistici [40]. Si prefigura,

[39] Cfr. E. CUSA, *I ristorni nelle società cooperative*, Milano, 2000, p. 163. Ritiene che una clausola siffatta andrebbe nel senso del rafforzamento della struttura patrimoniale della società, senza che quest'ultima perda di per sé quel tasso di mutualità che può essere goduto dal socio all'atto stesso dello scambio, R. GENCO, *La struttura finanziaria*, in GENCO (a cura di) *La riforma delle società cooperative*, Milano, 2003, p. 92. Sul punto, vedi Trib. Milano 10 dicembre 2014, con nota di R. DABORMIDA, *Mutualità e ristorni nei consorzi con attività esterna*, in *Società*, 2015, p. 670.

[40] Cfr., in tal senso, anche G. BONFANTE, *sub* art. 2545 *sexies*, in G. COTTINO-G. BONFANTE, O. CAGNASSO-P. MONTALENTI, *Il nuovo diritto societario*, *Commentario*, Bologna, 2004, 2626, che ritiene che il ristorno sia la misura dell'efficacia mutualistica della cooperativa. Nell'attuale contesto normativo, secondo una dottrina (così G. FALCONE, *Commento* sub *art. 2545*-sexies, in M. SANDULLI-V. SANTORO (a cura di), *Le riforma delle società. Società cooperative. Artt. 2511-2548 cod. civ.*, Torino, 2003, 179-180), il ristorno sarebbe divenuto una vera e propria categoria normativa. Si tratterebbe di una prescrizione obbligatoria, anche se poi la legge lascia una notevole, ma non assoluta, autonomia statutaria di fissazione dei criteri di attribuzione del ristorno, i quali devono rispettare comunque la parità di trattamento di cui all'art. 2516 c.c. Ossia a parità di condizioni quantitative e qualitative non è permessa una discriminazione fra i soci nel trattamento dello scambio mutualistico. Viene fatto salvo il caso in cui la mancata attribuzione del ristorno non sia giustificata dalla dimostrazione nella relazione *ex* art. 2545 c.c. di aver già conferito la prestazione mutualistica

quindi, un problema interpretativo rilevante per chi volesse sussumere nel nostro ordinamento tale tipo di cooperative, che non prevedono ristorni a livello statutario. Peraltro, il nostro legislatore, anche con la riforma societaria di cui al d.gs. 17 gennaio 2003, n. 6, così come già il codice civile, evita di definire espressamente lo scopo mutualistico, alimentando il dibattito a riguardo, ancorché sussista una certa prevalenza a riconoscere tale scopo nei termini della c.d. gestione di servizio al socio [41]. Quindi, il vantaggio mutualistico per il socio deve esistere e nelle cooperative nelle quali il socio chiede, e poi retribuisce, la prestazione della società (come nella cooperativa di consumo), viene conseguito attraverso un risparmio di spesa, mentre in quelle in cui è la società che chiede, e poi retribuisce, la prestazione del socio, il vantaggio viene conseguito attraverso un aumento del corrispettivo per l'attività prestata o per le forniture effettuate [42].

Dunque, da dove deriva il vantaggio mutualistico per i soci della cooperativa di dati sanitari senza fine di lucro? Pare derivare, anche in assenza di un ristorno in senso tecnico, dai servizi forniti dalla cooperativa senza un corrispettivo e collegati al trasferimento dei dati tra gli interessati e la cooperativa. La cooperativa, infatti, rafforza la posizione dei singoli individui, affinché compiano scelte informate prima di acconsentire all'utilizzo dei dati, influenzando i termini e le condizioni cui è subordinato l'utilizzo dei dati, in modo da offrire scelte migliori ai singoli membri

---

al costo o comunque anticipatamente o per contingenti necessità di investire nel patrimonio sociale tutte le eccedenze mutualistiche.

[41] Sulla circostanza che il legislatore dell'ultima riforma societaria del 2003 abbia fatto una precisa scelta di campo a favore della mutualità come gestione di servizio al socio, vi è una sostanziale concordia di opinioni nella maggioranza degli studiosi. Si veda a riguardo A. BASSI, sub *art. 2511 c.c.*, in G. PRESTI (a cura di), *Le società cooperative*, Milano, 2007, p. 3 ss.; F. CASALE, *Scambio e mutualità nella società cooperativa*, Milano, 2005, p. 86; G. MARASÀ, *Problemi attuali della società cooperativa e soluzioni della riforma*, in *La riforma di società, cooperative, associazioni e fondazioni*, Padova, 2005, p. 156.

[42] In molti casi, il vantaggio cooperativistico viene realizzato anche praticando un prezzo o corrispondendo un salario identici a quelli di mercato, e versando ai soci, a scadenze periodiche, e tenuto conto delle operazioni fatte, somme di denaro corrispondenti alla differenza, o fra i prezzi praticati e i costi (nella cooperazione di consumo), o fra i ricavi netti e i salari, o, comunque, i corrispettivi, già versati dalla cooperativa al socio. È quest'ultima soluzione quella che viene definita come pratica del ristorno, tipico compenso nel rapporto mutualistico che, pur avendo con gli utili la comune caratteristica di essere rappresentato da somme di danaro periodicamente ripartite fra i soci, ne differisce proprio per il fatto che viene corrisposto in proporzione ai rapporti mutualistici intrattenuti dal socio con la società e non (come gli utili) in proporzione alla quota di capitale conferita (cfr. L.F. PAOLUCCI, *I ristorni nelle cooperative*, in *Società*, 2000, p. 43). La concreta attribuzione del vantaggio mutualistico, quindi, può aver luogo in forza di due tecniche fra loro diverse, quella del vantaggio immediato e quella del vantaggio differito (cfr., però, F. GALGANO, *Mutualità e scambio nelle società cooperative*, in *Riv. dir. civ.,* 1985, 1031, che parla di vantaggio immediato e mediato). Sulla differenza tra utili e ristorni si è espressa, con una nota sentenza, la Suprema Corte (Cass. 22 maggio 2015 n. 10641, in *Società*, 2015, p. 1034) affermando che: «La sola caratteristica che i ristorni hanno in comune con gli utili è la aleatorietà, in quanto la società potrà distribuirli soltanto se la gestione mutualistica dell'impresa si è chiusa con un'eccedenza dei ricavi rispetto ai costi».

del gruppo, o trovando possibili soluzioni alle posizioni contrastanti dei singoli membri di un gruppo in merito alle modalità di utilizzo dei dati. Si può quindi enucleare da tali rapporti tra cooperativa e socio un rapporto contrattuale ulteriore di consulenza ed eventualmente di mandato. L'accordo, poi, stabilisce il diritto degli interessati-soci ad ottenere dati meglio strutturati rispetto ai dati iniziali forniti, eventualmente anonimizzandoli e/o rendendoli più sicuri. Del resto, appare ormai pacifico, dopo la riforma del 2003, ed il dato testuale degli artt. 2512, 2516, 2544, co. 1, c.c., che lo scopo mutualistico delle cooperative si realizzi con la stipula di contratti di scambio separati e distinti rispetto al contratto sociale, con un evidente collegamento contrattuale, potendosi piuttosto discutere se, a seconda dei tipi cooperativi, si sia in presenza di contratti tipici o atipici[43]. È stata superata, quindi,

[43] Sul punto è la stessa Relazione all'art. 2516 c.c. a definire lo scambio mutualistico come "rapporto contrattuale distinto da quello societario". In dottrina, vedi V. BUONOCORE, *Rapporto mutualistico e parità di trattamento*, in *Il nuovo diritto delle società, Liber amicorum Gianfranco Campobasso*, diretto da P. ABBADESSA-G.B. PORTALE, 4, Torino, 2007, p. 579 ss., che, nel commentare la riforma del 2003, ha osservato come essa abbia definitivamente legittimato lo scambio mutualistico come contratto distinto dal contratto sociale. Cfr., in senso analogo G. BONFANTE, *La società cooperativa, Itinerari di giurisprudenza*, in *Società*, 2023, p. 102 ss.; E. TONELLI, *Scambio mutualistico e rapporto sociale: interferenze e connessioni*, in M. SANDULLI-P. VALENSISE (a cura di), *Le cooperative dopo la riforma del diritto societario*, Milano, 2005, p. 29; E. ROCCHI, sub *artt. 2512-2514 c.c.*, in PRESTI (a cura di), *Società cooperative*, Milano, 2006, p. 28 ss.; G. RACUGNO, *La società cooperativa*, in *Tratt. dir. comm.*, diretto da Buonocore, IV, 9, 2006, p. 15 ss.; G. TATARANO, *La nuova impresa cooperativa*, Milano, 2011, p. 91 ss.; A. PIRAS, *Profili mutualistici della* governance *delle società cooperative*, in M. CAMPOBASSO-V. CARIELLO-V. DI CATALDO-F. GUERRERA-A. SCIARRONE ALIBRANDI, *Società, banche e crisi di impresa, Liber amicorum Pietro Abbadessa*, Torino, 2, 2014, p. 2023 ss. In giurisprudenza, fra le altre, vedi Cass. civ. 28 marzo 2007, n. 7646, in *Contratti*, 2007, p. 673; Cass. civ. 12 dicembre 2014, n. 26222, in *Società*, 2015, p. 941, con nota di M. CAVANNA; Cass. civ. 31 luglio 2014, n. 17465, in *Mass. Giur. it.*, 2014; Cass. civ. 26 gennaio 2015, n. 1343, in *Società*, 2015, p. 1328, con commento di G. BONFANTE; Cass. civ. 13 maggio 2021, n. 12949, in *Mass. Giur. it.*, 2021, nonché Cass. civ. 2 agosto 2023, n. 23606, con nota di C. GARILLI, in *Le società*, 2024, 2, p. 167 ss.

Nelle cooperative edilizie, la giurisprudenza da tempo ha avuto occasione di affermare che un rapporto economico-giuridico distinto da quello sociale s'instaura tra la società e il socio prenotatario nella fase della successiva attribuzione dell'unità immobiliare costruita, che si configura come vero e proprio atto traslativo della proprietà a titolo oneroso. In tale fase, dunque, riprendono vigore i rimedi generali volti a mantenere o ristabilire l'equilibrio sinallagmatico tra la prestazione traslativa e la controprestazione economica. Vedi per tutte Cass. civ., 18 gennaio 2001, n. 694, in *Società*, 2001, p. 945 ss., con nota di L.F. PAOLUCCI. Pur individuandosi distinti rapporti di scambio con i soci caratterizzati dalla corrispettività delle reciproche prestazioni, il contenuto dei medesimi potrebbe essere interamente o parzialmente predeterminato nello statuto, che finisce così con l'assumere le vesti di un contratto preliminare o di un contratto normativo, a seconda delle diverse configurazioni concrete e delle differenti interpretazioni datane dalla dottrina (vedi soprattutto F. CASALE, *Scambio e mutualità nella società cooperativa*, Milano, 2005, pp. 48 ss. e 140 ss., che propende per la tesi del contratto normativo). Anche per la disciplina della Società cooperativa europea, lo scopo mutualistico è inteso come «soddisfacimento dei bisogni e/o promozione delle attività economiche e sociali» dei soci e promozione della loro partecipazione ad attività economiche, e si realizza attraverso rapporti di scambio mutualistico, che la norma definisce come «accordi per la fornitura di beni o di servizi o l'esecuzione di

l'idea che tendeva ad escludere che siffatto atto di scambio avesse natura contrattuale per la mancanza di una contrapposizione di interessi fra le parti [44]. Rispetto a tali rapporti tra cooperativa di dati e soci, allora, saranno applicabili tutti i rimedi generali volti a mantenere o ristabilire l'equilibrio sinallagmatico tra le prestazioni, come l'art. 1460 c.c., nonché le regole generali in materia di responsabilità contrattuale (art. 1218 c.c.). Dovrà essere pure valutata la relazione tra un eventuale recesso del socio della cooperativa ed i rapporti mutualistici in corso, visto il collegamento contrattuale tra contratto di società e contratto di scambio, fermo restando che, anche nel caso in cui non esista alcuna disciplina nello statuto o nel regolamento a riguardo, il recesso dal contratto di società dovrebbe determinare l'estinzione dei rapporti mutualistici [45]. Non altrettanto, invece, sembra potersi dire nel caso inverso in cui il socio intenda recedere dai contratti di servizi collegati al trasferimento dei dati, non sembrando, nella fattispecie, possa considerarsi automatico anche uno scioglimento del rapporto del socio con la società.

---

lavori». In senso contrario, ma con decisione recentissima e, allo stato isolata, vedi però Cass. civ., 9 agosto 2023, n. 24242, in *Società*, 2024, p. 22, con commento di G. BONFANTE, *La "morte" del contratto di scambio nelle cooperative secondo una sentenza del Supremo Collegio*, in *Società*, 2024, p. 24 ss., secondo cui l'obbligo di conferimento del prodotto che grava sui soci di una cooperativa agricola di trasformazione, obbligo essenziale per il funzionamento della società, è riconducibile a un contratto di durata ad esecuzione periodica, contratto che però non avrebbe una sua autonomia risultando essere parte integrante del contratto sociale. Conseguentemente la consegna da parte del socio del prodotto non determinerebbe l'operatività del principio di corrispettività, ma una mera aspettativa alla remunerazione del conferimento. In particolare, non essendo la remunerazione un "prezzo" in senso tecnico, ma soltanto l'attribuzione al socio/imprenditore *pro quota* del profitto generato dalla vendita dei prodotti trasformati, non sarebbe configurabile in capo al socio un diritto di credito al percepimento di un corrispettivo. E questa conclusione troverebbe conferma, nel caso di specie, secondo la Corte, anche dal regolamento approvato dalla cooperativa in cui si afferma che il valore definitivo dei conferimenti deve essere stabilito in base ai risultati di gestione desumibili alla chiusura dell'esercizio sociale. Dunque, secondo la Suprema Corte il socio verrebbe remunerato dei suoi conferimenti attraverso il profitto della cooperativa, mancando il quale non avrebbe diritto ad alcun corrispettivo in quanto socio/imprenditore.

[44] Cfr., per questa risalente impostazione, Cass. civ., 23 aprile 1957, n. 1382, in *Foro pad.*, 1957, I, p. 649, secondo cui la distribuzione di merce ai soci non è assimilabile a una vendita (vedi ulteriori riferimenti in R. GENCO, *Scopo mutualistico e gestione dell'impresa*, in G. SCHIANO DI PEPE (a cura di), *Cooperative, consorzi, raggruppamenti*, Milano, 1996, p. 30). Si è anche sostenuto che tali negozi, pur autonomi e distinti rispetto al contratto sociale, subissero una sorta di curvatura causale in ragione degli scopi mutualistici della cooperativa (cfr. P. VERRUCOLI, voce *Cooperative (Imprese)*, in *Enc. dir.*, Milano, 1962, p. 568).

[45] Cfr., in tal senso, A. BASSI, *Delle imprese cooperative e delle mutue assicuratrici*, in *Il codice civile. Commentario* diretto da P. SCHLESINGER, Milano, 1988, p. 606; ID., *Le società cooperative*, Torino, 1995, p. 192. Vedi poi, in argomento, E. BONAVERA, *Recesso parziale del socio di cooperativa tra rapporto societario e rapporto mutualistico*, in *Società*, 2022, p. 549 ss.

Capitolo XXIII

Cooperative di dati, Spazio europeo dei dati sanitari e *Data Act* nel dedalo normativo

Giuseppe Proietti

Abstract: The paper aims to explore the role of data cooperatives within the European health data space that is being shaped by the proposed "European Health Data Space" regulation (EHDS). It is intended to highlight the complex coordination between the various and recent European legislation that will have to be carried out. The topic of this paper concerns the implementation of the system for the circulation and sharing of health data, leaving aside the cybersecurity issue, that sees the coordination between the General Data Protection Regulation, the Data Governance Act, the Data Act and the national rules.

1. Premessa.

È molto probabile che una delle qualità che il giurista dovrà necessariamente possedere negli anni a venire sarà legata al senso dell'orientamento nel nuovo e complesso quadro normativo europeo che si va componendo e che delineerà il c.d. diritto digitale [1]. Nel corso degli ultimi anni, infatti, in questo settore il legi-

[1] Si può dire che negli ultimi anni si va delineando un settore come il «diritto digitale», che va a costituire una *materia culturale*, la quale si differenzia dalle materie istituzionali; dicotomia, questa, che si ritrova in merito al diritto industriale in P. SPADA, *Diritto industriale*, 2ª ed., Torino, 2005, p. 4. Nel diritto digitale in composizione si può includere, *inter alia*, il trattamento e la circolazione dei dati

slatore europeo si è dimostrato particolarmente produttivo.

Gli interventi legislativi, avvenuti per lo più con lo strumento del regolamento europeo, sono copiosi e necessitano di una proficua e complessa attività di attuazione e coordinamento, fondamentale per evitare un "effetto sabbie mobili" nei vari ambiti.

Il presente contributo si inserisce nel Progetto di Terza Missione sulle «Cooperative di dati» promosso dall'Università di Bologna e l'obiettivo è quello di partecipare alla cennata opera di coordinamento, focalizzandosi sul ruolo che le cooperative di dati possono ricoprire nel settore della sanità, anche con uno sguardo rivolto all'*IoT* (*Internet of Things*).

In particolare, perché ciò possa compiersi, sarà necessario mettere ordine alle diverse normative, tra cui il *Data governance Act* (Reg. UE 2022/868), il regolamento europeo sullo spazio europeo dei dati sanitari (EHDS) in fase di approvazione, il *Data Act* (Reg. UE 2023/2854) e, va da sé, il *General Data Protection Regulation* (GDPR – Reg. UE 2016/679).

L'intero quadro dovrebbe poi essere integrato con un'ulteriore normativa – che non può essere analizzata nel presente contributo – ossia la legislazione in materia di cybersicurezza, come la recente direttiva NIS-2 (Dir. UE 2022/2555) e il nuovo *Cyber Resilience Act*.

2. Il *Data Governance Act* (DGA) e il significativo cambio di paradigma nell'approccio legislativo.

2.1. La disciplina del *Data Governance Act.*

Per inquadrare le cooperative di dati è necessario prendere le mosse dal regolamento sulla *governance* europea dei dati (*Data Governance Act* – DGA), il quale è entrato in vigore nel giugno del 2022 ed è applicabile dal 24 settembre del 2023. Questo regolamento si inserisce nel complesso quadro della «strategia europea per i dati» con cui si persegue l'obiettivo della creazione di uno spazio comune europeo di dati nel quale questi possono essere condivisi e utilizzati, indipendentemente dal luogo di conservazione nell'UE [2]. Si realizza così il passaggio da una disciplina

personali, il settore dei mercati e dei servizi digitali, incluso l'ambito delle piattaforme e i servizi di intermediazione online, oltreché l'intelligenza artificiale e la *cybersecurity*.

[2] A.M. PINELLI, *La circolazione dei dati personali tra tutela della persona, contratto e mercato*, in *Nuova giur. civ. comm.*, 2022, 6, p. 1322. In senso anche critico si veda F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in *Contratto e impresa Europa*, 2021, 1, p. 199, spec. p. 256, secondo il quale con «il *Data Governance Act* l'UE intraprende una strada interessante, che cela però il rischio di svilimento dei diritti fondamentali della persona qualora la direzione intrapresa, registrata sin dai significativi mutamenti del lessico, porti ad un irreversibile processo di reificazione dei dati prima e del soggetto poi, sul quale occorre far rimanere sempre desta l'attenzione, facendo sì che in Europa rimanga viva (…) la convinzione che l'essere umano sia e debba rimanere l'elemento centrale».

puramente fondata sulla salvaguardia di determinati beni incorporali, dovuta al potenziale di conoscenza che possono rivelare in merito a una persona, a una disciplina che favorisce la circolazione e l'uso di dati «in relazione alla loro strutturazione formale (…), indipendentemente dal tipo di significati che questi siano atti a veicolare» [3].

L'obiettivo del legislatore è di dar vita a un'economia dei dati che consenta alle imprese di progredire garantendo allo stesso tempo la neutralità dell'accesso, la portabilità e l'interoperabilità dei dati, evitando effetti di dipendenza (*lock-in*).

In questo quadro, si intende stimolare una circolazione dei dati libera e sicura, non solo all'interno dei confini europei, ma finanche con paesi terzi; per questo, la visione del legislatore è quella di creare spazi comuni europei di dati specifici per settore (come sanità, manifattura, clima, energia e altri). La *ratio legis*, peraltro, si focalizza sul ruolo "neutrale" degli intermediari rispetto ai dati scambiati tra gli utenti, realizzando una separazione anche strutturale del modello organizzativo dell'attività d'impresa [4].

Sostanzialmente, la nuova normativa ha segnato un cambio di paradigma strutturale. Si è passati da una logica primariamente difensiva e protezionistica del GDPR a una logica «in cui la circolazione medesima ed i meccanismi di controllo sono ripensati profondamente» [5].

Il DGA, peraltro, si inserisce nell'ambito di una situazione di intrinseca debolezza dell'interessato il quale, spesso, non è consapevole o non è in grado di esercitare appieno i propri diritti. Come già segnalato in dottrina, quindi, il legislatore ha introdotto modelli di *governance* "duale", unendo alla *governance* "individuale" del *data subject* una *governance* ulteriore che, in alcuni casi, assume le vesti di una *governance* "collettiva", esercitata nel caso della cooperativa di dati. In altri casi, invece, può assumere le vesti di una *governance* "aggregata", esercitata dall'intermediario, il quale raccoglie dati da soggetti diversi e negozia il loro utilizzo con soggetti terzi [6].

Il contenuto normativo del DGA può essere compendiato nella parte dedicata al riutilizzo di determinate categorie di dati protetti e detenuti da enti pubblici (capo II), dal capo dedicato ai servizi di intermediazione dei dati (capo III) e dal capo dedicato all'altruismo dei dati (capo IV).

Il capo VII, poi, è dedicato all'accesso internazionale e al trasferimento dei dati.

---

[3] G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, in *Riv. trim. dir. pubblico*, 2022, 4, p. 971, spec. p. 976. Secondo l'A. è intervenuto il passaggio da una normativa essenzialmente limitativa ad una di stampo promozionale sull'uso dei dati e sottolinea come in Europa circa l'85% dei dati raccolti non viene riutilizzato.

[4] D. POLETTI, *Gli intermediari dei dati*, in *European Journal of Privacy Law & Technologies*, 2022, 1, p. 45, spec. p. 51.

[5] F. BRAVO, *Le cooperative di dati*, in *Contratto e impresa*, 2023, 3, p. 757, spec. p. 781.

[6] *Ivi*, p. 785.

Il legislatore precisa che (art. 1, par. 2, co. 2, DGA) non sono pregiudicate ulteriori e concorrenti normative europee o nazionali settoriali che impongano a enti pubblici, fornitori di servizi di intermediazione o organizzazioni per l'altruismo, un ulteriore regime di certificazione o autorizzazione. In caso di conflitto tra le norme del DGA e le norme del GDPR (Reg. UE 2016/679), o le norme nazionali adottate in conformità di quest'ultimo, prevale «il pertinente diritto dell'Unione o nazionale in materia di protezione dei dati personali» (art. 1, par. 3, DGA). Il coordinamento tra la disciplina contenuta nel DGA con altre normative, nazionali o europee, costituisce un elemento cruciale e delicato.

Il capo II del DGA, come già accennato, prevede la facoltà, per gli enti pubblici, di consentire il riutilizzo di una o più categorie di dati previste all'art. 3 DGA [7], intendendosi con «riutilizzo» un diverso e secondario uso per scopi diversi rispetto a quello originario. Affinché ciò possa essere concesso, è necessario che i dati siano anonimizzati (se si tratta di dati personali) e modificati, aggregati o trattati con qualsiasi altro metodo di controllo della divulgazione, in caso di informazioni commerciali riservate. Il tutto nel quadro di un ambiente di trattamento sicuro.

I riutilizzatori sono tenuti ad adottare tutte le tecniche volte a impedire la reidentificazione degli interessati a cui quei dati personali fanno riferimento e sono tenuti a osservare un obbligo di riservatezza che impedisce loro di divulgare quei dati per i quali sono stati autorizzati.

Il capo III, dedicato all'intermediazione dei dati, prevede invece un servizio volto a instaurare rapporti commerciali per finalità di condivisione dei dati tra un numero indeterminato di interessati e di titolari di dati, da un lato, e di utenti dall'altro. Con «condivisione dei dati» si intende proprio la fornitura di dati da un interessato o da un titolare dei dati a un utente ai fini del loro utilizzo.

L'art. 2, n. 11, del DGA fornisce la definizione di «servizio di intermediazione dei dati» descrivendolo come un servizio che ha l'obiettivo di instaurare, mediante strumenti tecnici, giuridici o di altro tipo, «rapporti commerciali ai fini della condivisione dei dati tra un numero indeterminato di interessati e di titolari dei dati, da un lato, e gli utenti dei dati, dall'altro, anche al fine dell'esercizio dei diritti degli interessati in relazione ai dati personali». La definizione normativa, poi, prosegue annoverando alcune esclusioni come: «a) servizi che ottengono dati dai titolari dei dati e li aggregano, arricchiscono o trasformano al fine di aggiungervi un valore sostanziale e concedono licenze per l'utilizzo dei dati risultanti agli utenti dei dati, senza instaurare un rapporto commerciale tra i titolari dei dati e gli utenti dei dati; b) servizi il cui obiettivo principale è l'intermediazione di contenuti protetti da diritto d'autore; c) servizi utilizzati esclusivamente da un titolare dei dati per consentire l'utilizzo dei dati detenuti da tale titolare dei dati, oppure utilizzati da varie persone giuridiche all'interno di un gruppo chiuso, anche nel quadro di rapporti con i

[7] La normativa del DGA va a completare la disciplina dettata dalla direttiva UE 2019/1024 relativa all'apertura dei dati e al riutilizzo dell'informazione nel settore pubblico, recepita con il D.lgs. n. 200/2021. In tal senso, D. POLETTI, *Gli intermediari dei dati*, cit., p. 49.

fornitori o i clienti o di collaborazioni contrattualmente stabilite, in particolare quelli aventi come obiettivo principale quello di garantire la funzionalità di oggetti o dispositivi connessi all'internet delle cose; d) servizi di condivisione dei dati offerti da enti pubblici che non mirano a instaurare rapporti commerciali».

Proseguendo con l'impianto definitorio offerto dalla normativa, con «titolare dei dati» il legislatore fa riferimento a quel soggetto che ha il diritto di concedere l'accesso a determinati dati personali o non personali, o di condividerli. Con «utente dei dati» si allude a quella persona che ha il legittimo accesso a determinati dati e che ha diritto a utilizzarli per finalità commerciali o non commerciali.

Il cambio di paradigma normativo che si è verificato con il DGA, già segnalato nel precedente paragrafo, è avvenuto anche a livello lessicale, là dove per la prima volta si menziona una "titolarità dei dati". È una differenza che, si è sottolineato, potrebbe costituire il preludio all'introduzione, per via normativa, di «una reificazione dei dati personali, quali entità giuridicamente rilevanti ex sé più che quali attribuiti della persona» [8].

L'intermediazione dei dati può avvenire tra titolari dei dati e potenziali utenti dei dati e può includere servizi come scambi di dati bilaterali o multilaterali o la creazione di piattaforme o banche dati che consentono lo scambio o l'utilizzo congiunto dei dati (art. 10, lett. *a*, DGA); può consistere in servizi di intermediazione tra interessati che intendono mettere a disposizione i propri dati e potenziali utenti dei dati, consentendo così l'esercizio dei diritti degli interessati di cui al GDPR (art. 10, lett. *b*, DGA); oppure, si può trattare di cooperative di dati (art. 10, lett. *c*, DGA) [9], considerate positivamente da più parti [10].

Il fulcro della disciplina che interessa il servizio di intermediazione dei dati è l'art. 12 del DGA che prescrive una serie di condizioni affinché si possa fornire il servizio il cui esercizio è subordinato a una prodromica procedura di notificazione prevista all'art. 11 DGA.

Il capo IV del regolamento è invece dedicato all'altruismo dei dati. Si tratta di un meccanismo, già "avvalorato" in precedenza dall'EDPB, attraverso cui un soggetto interessato può spontaneamente offrirsi di mettere a disposizione determinati dati per finalità di riutilizzo. Perciò, il DGA prevede una serie di condizioni e prescrizioni affinché questo meccanismo possa essere attuato per il tramite di apposite organizzazioni per l'altruismo dei dati riconosciute, le quali a loro volta sono sottoposte ad una serie di obblighi.

Ai fini del presente contributo, però, l'attenzione si focalizza sui servizi di intermediazione dei dati e, in particolare, sul servizio svolto per il tramite di cooperative di dati.

---

[8] F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, cit., p. 203.

[9] Per queste ultime si veda F. BRAVO, *Le cooperative di dati*, cit., p. 757 e ss.; nonché L. PETRONE, *Il mercato digitale europeo e le cooperative di dati*, in *Contratto e impresa*, 2023, 3, p. 800.

[10] G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit., p. 986.

2.2. Le cooperative di dati.

Sono state citate più volte e si è visto che tra i servizi di intermediazione dei dati il DGA annovera anche le cooperative di dati (art 10, lett. *c*, DGA).

Con tali organizzazioni si possono perseguire una serie di obiettivi. In particolare, esse possono essere finalizzate a rafforzare la posizione dei singoli individui, affinché questi siano in grado di compiere scelte informate prima di prestare il consenso all'utilizzo dei dati, «influenzando i termini e le condizioni, stabiliti dalle organizzazioni di utenti dei dati, cui è subordinato l'utilizzo dei dati, in modo da offrire scelte migliori ai singoli membri del gruppo, o trovando possibili soluzioni alle posizioni contrastanti dei singoli membri di un gruppo in merito alle modalità di utilizzo dei dati laddove tali dati riguardino più interessati all'interno di tale gruppo» [11].

Con una scelta legislativa singolare, però, nel DGA non viene fornita una definizione di cooperativa di dati, bensì di «servizi di cooperative di dati». Si può ricavare questa definizione al n. 15 dell'art. 2 DGA in cui si fa riferimento a servizi di intermediazione offerti da una struttura organizzativa costituita da interessati, imprese individuali o da PMI, che può «principalmente» essere finalizzata ad aiutare i propri membri nell'esercizio dei loro diritti in relazione a determinati dati, anche per il compimento di «scelte informate prima di acconsentire al trattamento dei dati, di procedere a uno scambio di opinioni sulle finalità e sulle condizioni del trattamento dei dati che rappresenterebbero al meglio gli interessi dei propri membri in relazione ai loro dati», oppure, in via alternativa, «di negoziare i termini e le condizioni per il trattamento dei dati per conto dei membri prima di concedere l'autorizzazione al trattamento dei dati non personali o prima che essi diano il loro consenso al trattamento dei dati personali».

Il perimetro dei servizi che possono offrire le cooperative di dati, però, non può e non deve considerarsi limitato a quelli contemplati nella loro definizione che fa riferimento a «obiettivi principali». L'oggetto dei servizi deve essere integrato nell'alveo dei tipici servizi dell'intermediazione dei dati così come consentita nell'ambito del *Data Governance Act*.

In letteratura si è posto l'accento sulle due caratteristiche strutturali inerenti alle cooperative di dati che possono ricavarsi dalle condizioni per la fornitura di servizi di intermediazione di dati previste dall'art. 12 del DGA.

La prima, concerne l'esclusività dello scopo dell'utilizzo dei dati e, la seconda, il criterio di separazione soggettiva tra fornitore e utilizzatore dei dati intermediati [12]. Vale a dire, la cooperativa non può utilizzare i dati per i quali fornisce il servizio di intermediazione.

L'elemento della separazione è già stato oggetto di critica dal momento che essa può essere confacente per quelle società di intermediazione di dati non mutualistiche, ma sembrerebbe fuori luogo «per le cooperative di dati, per le quali sarebbe

[11] In questo senso il *considerando* n. 31 del DGA.

[12] F. BRAVO, *Le cooperative di dati*, cit., p. 774.

stato utile mantenere invece, in maniera chiara, la possibilità di utilizzo dei dati conferiti dai soci, connaturata proprio con le esigenze di svolgimento dell'attività cooperativa» [13].

Le altre peculiarità, tipiche delle cooperative di dati, sarebbero la permanenza del potere di controllo sui dati in capo ai singoli membri e la loro utilizzazione da parte dell'organizzazione che, tuttavia, fa permanere in capo ai singoli la *governance* individuale. A ciò si affianca una *governance* collettiva sui dati conferiti dai singoli membri, la quale viene esercitata dall'organizzazione e viene definita dai singoli membri che la compongono [14]. Si verrebbe, quindi, a generare una *governance* duale in forza della quale le scelte strategiche e operative tracciate a livello di organizzazione non impediscono l'esercizio di una *governance* individuale, «quantomeno qualora si tratti di dati personali facenti capo ai singoli membri qualificabili come interessati al trattamento ai sensi del Reg. UE 679/2016» [15]. Infine, un'ulteriore peculiarità risiede nel perseguimento dell'interesse dei membri della cooperativa [16].

Da un punto di vista operativo, infine, è necessario riepilogare i diversi modelli all'interno dei quali le cooperative possono estrinsecarsi [17].

Un primo modello è quello che riguarda i dati conferiti dai membri della cooperativa e che vengono condivisi solo internamente all'organizzazione (*Member-to-Cooperative*).

Un altro modello prevede una condivisione dei dati tra i singoli membri della cooperativa, con quest'ultima che facilita lo scambio di dati, ossia che funge da "intermediario" tra i singoli "membri" o soci. È un modello attraverso il quale un socio può accedere a certi dati per lui utili per il riuso, oppure ai fini della composizione di un *benchmark* finalizzato a valutare una determinata attività (*Member-to-Member*).

Un terzo modello prevede la condivisione dei dati tra differenti organizzazioni con finalità analoghe (*Federated*). Infine, altri modelli possono prevedere la condivi-

---

[13] *Ivi*, p. 775. L'A., quindi, da un lato propone una soluzione interpretativa «applicando in maniera non rigida la "condizione" concernente l'obbligo di separazione soggettiva tra (fornitore del servizio di) cooperativa di dati e utilizzatore di dati, volta a sterilizzarne l'applicazione in considerazione della natura mutualistica della cooperativa, al fine di far salve le norme tipiche della società cooperativa, che devono essere coordinate a livello di sistema con quelle frettolosamente inserite, sul punto, nel *Data Governance Act*», dall'altro, invece viene suggerito l'intervento normativo «in sede europea o in sede nazionale, a livello di coordinamento della disciplina domestica con quella unionale –, chiarendo in maniera più dettagliata le peculiarità della disciplina della data governance con riguardo al caso di specifico delle "cooperative di dati", facendo salva l'utilizzabilità dei dati da parte di quest'ultima, nello spirito mutualistico che la contraddistingue e la contrappone al modello più tipicamente capitalistico».

[14] *Ivi*, p. 762.

[15] *Ibidem*.

[16] *Ivi*, p. 763.

[17] Anche per la descrizione dei cinque modelli operativi si seguirà la classificazione operata da F. BRAVO, *Le cooperative di dati*, cit., pp. 769-770.

sione dei dati con altre organizzazioni, diverse rispetto alle cooperative (*Third Party*), oppure una messa a disposizione dei dati liberamente accessibili a tutti (*Open Data*).

Nelle esperienze di altri Stati, gli ambiti all'interno dei quali una cooperativa di dati può operare sono i più disparati e le applicazioni pratiche costituiscono già un fattore consolidato [18]. Ciascuno di questi ambiti ha le proprie peculiarità e deve adattarsi specificatamente agli strumenti e alle misure da adottare alla luce della normativa vigente che non si limita, va da sé, alla legislazione in materia di dati personali [19]. Nel mosaico normativo, infatti, si deve tener conto della regolamentazione in materia di *cybersecurity* e di tutto il frammentato impianto del diritto digitale.

In ogni caso, nella realtà pratica, i settori che più si prestano all'intermediazione di una cooperativa di dati sembrano essere quelli dell'agricoltura [20], della finanza [21], della c.d. *gig economy* [22] e della sanità [23]. Per quest'ultimo importante settore gli intermediari possono fornire un contributo notevole, ma il tema si lega inevitabilmente a un'altra novità legislativa: il Regolamento europeo sullo spazio europeo dei dati sanitari, attualmente ancora in fase di proposta.

3. Il Regolamento europeo sullo spazio europeo dei dati sanitari (EHDS).

Nel mese di marzo del 2024 le istituzioni europee hanno raggiunto un compromesso anche sul testo legislativo del regolamento (UE) sullo spazio europeo dei dati sanitari che si inserisce nel quadro della già accennata strategia europea dei dati [24]. Il

---

[18] Si veda AA.VV., *Harnessing digital federation platforms and data cooperatives to empower SMEs and local small communities, TF-2: our common Digital Future*, 2023, p. 10 ss. in cui vengono riportati una serie di casi studio in differenti settori e Stati. Tra questi Stati, solamente due sono europei.

[19] Sulla infrastruttura tecnica si veda M. DOCKENDORF-R. DANTU-J. LONG, *Graph Algorithms over Homomorphic Encryption for Data Cooperatives*, in SECRYPT 2022, *19th International Conference on Security and Cryptography*, 2022, p. 205 ss.; T. HARDJONO-A. PENTLAND, *Data Cooperatives: Towards a Foundation for Decentralized Personal Data Management*, in arXiv:1905.08819v1, 2019, p. 1 ss.

[20] P. BODENHAM, *Datacooperatives in agricolture: An opportunity for farmers?*, in *Nova itinera – Percorsi del diritto nel XXI secolo*, 2023, p. 35, il quale rileva come le cooperative di dati possano essere una soluzione per il problema di data lock-in che riguarda molti operatori nel settore dell'agricoltura.

[21] In questo settore ci sono varie realtà già consolidate a livello globale come la *Kenya's M-Pesa platform* o la *Brazil's Nubank platform*.

[22] Una delle realtà è riportata in F. BRAVO, *Le cooperative di dati*, cit., p. 771, e riguarda la piattaforma *Driver's Seat data co-op* che opera negli U.S.A.

[23] AA.VV., *European Healt Data Space-An opportunity now to grasp the future od Data-Driven healthcare*, in *Healthcare* 2022, pp. 1 e ss.; I. VAN ROESSEL-M. REUMANN-A. BRAND, *Potentials and Challenges of the Health Data Cooperative Model*, in *Public Health Genomics*, 2017, p. 321 ss.

[24] Per un'analisi della proposta presentata dalla Commissione europea nel 2022 si veda S. CORSO, *Lo spazio europeo dei dati sanitari: la Commissione Europea presenta la proposta di regolamento*, in *Federalismi.it*, *Oss. dir. sanitario*, agosto 2022, p. 1.

testo ha ricevuto l'approvazione del Parlamento europeo e si attende quella del Consiglio.

Il regolamento, anch'esso voluminoso, persegue l'obiettivo di istituire uno spazio europeo per la condivisione dei dati sanitari (*European Health Data Space*, EHDS) prevedendo un "uso primario" e un "uso secondario".

Con il primo si intende favorire l'accesso degli interessati ai propri dati sanitari elettronici personali, garantendo allo stesso tempo il loro controllo nel contesto dell'assistenza sanitaria; con il secondo, si intende conseguire ulteriori finalità nel settore a beneficio della società come la ricerca, l'innovazione, la definizione delle politiche, la preparazione e la risposta alle minacce sanitarie, la sicurezza dei pazienti, la medicina personalizzata e le statistiche ufficiali.

Lo scopo dell'iniziativa legislativa è anche quello di ottimizzare il funzionamento del mercato interno con la realizzazione di un quadro giuridico e tecnico uniforme, con particolare riguardo allo sviluppo, alla commercializzazione e all'uso di sistemi di cartelle cliniche elettroniche in conformità ai valori propri dell'UE.

L'uso secondario dei dati sanitari costituisce probabilmente la parte del regolamento più promettente, il quale può rappresentare terreno fertile per l'innovazione, anche con l'ausilio degli intermediari dei dati che possono favorire la loro condivisione.

L'EHDS prevede che con «titolari dei dati sanitari», nell'ambito dell'uso secondario, bisogna considerare quei soggetti fornitori di servizi sanitari o di assistenza o che svolgono attività di ricerca nel settore sanitario o dell'assistenza o che sviluppano prodotti o servizi destinati al settore sanitario o dell'assistenza [25].

Il riferimento, perciò, è agli enti pubblici, no profit o privati, facendo rientrare anche le case di cura, gli enti che forniscono servizi alle persone con disabilità, le attività commerciali e tecnologiche legate all'assistenza, come l'ortopedia, e le aziende che forniscono servizi di assistenza.

Stando al considerando n. 40, anche le persone giuridiche che sviluppano applicazioni per il benessere dovrebbero essere considerati titolari di dati sanitari. Al pari di queste, sarebbero titolari di dati sanitari anche le istituzioni, gli organismi, gli uffici o le agenzie dell'UE che trattano le categorie di dati sanitari e di assistenza sanitaria di cui sopra, nonché i registri di mortalità.

Viene poi specificato che, salvo diverse scelte legislative nazionali, per evitare un onere sproporzionato, le persone fisiche e le microimprese dovrebbero essere esentate dagli obblighi di titolari di dati sanitari previsti nell'EHDS [26].

---

[25] In tal senso il considerando n. 40 del EHDS.

[26] Secondo il *considerando* n. 53 gli Stati membri possono designare titolari di dati di fiducia per i quali è prevista una procedura di autorizzazione semplificata. Ciò al fine di alleggerire l'onere amministrativo che gli organismi di accesso ai dati sanitari devono sostenere per gestire le richieste relative ai dati da essi trattati. I titolari di dati di fiducia dovrebbero essere in grado di valutare le richieste di accesso ai dati presentate nell'ambito di questa procedura semplificata, tenendo conto della loro esperienza nel trattare il tipo di dati sanitari che trattano. L'organismo di accesso ai dati sanitari dovrebbe rimanere responsabile del rilascio dell'autorizzazione finale e non dovrebbe essere vincolato dalla

I dati sanitari raccolti e trattati da questi titolari devono essere resi disponibili agli «organismi di accesso ai dati sanitari» per massimizzare l'impatto dell'investimento pubblico e sostenere la ricerca, l'innovazione, la sicurezza dei pazienti o la definizione delle politiche, il tutto a beneficio della società.

Questi organismi sono cruciali per il funzionamento dell'intero sistema e sono quegli enti designati dai singoli Stati membri che hanno il compito di decidere sulle domande di accesso ai dati, di autorizzare e rilasciare i permessi di accesso ai dati per il loro uso secondario. Inoltre, siffatti organismi svolgono specifiche funzioni come l'adozione di tutte quelle misure necessarie volte a preservare la riservatezza dei diritti di proprietà intellettuale, nonché la tutela dei segreti commerciali; collaborano con i titolari dei dati; mantengono un sistema di gestione per registrare ed elaborare le domande di accesso ai dati; cooperano a livello europeo e nazionale per la definizione di norme comuni, dei requisiti tecnici e delle misure appropriate per l'accesso ai dati sanitari elettronici in un ambiente di trattamento sicuro e per le tecniche e le migliori pratiche per l'uso secondario e la gestione dei dati sanitari elettronici; facilitano l'accesso transfrontaliero ai dati sanitari elettronici per uso secondario ospitati in altri Stati membri attraverso il HealthData@EU e cooperano strettamente tra loro e con la Commissione UE.

Il regolamento EHDS prescrive che gli organismi di accesso ai dati sanitari concedono a un utente l'accesso per un uso secondario ai dati sanitari elettronici solo se tale riutilizzo è diretto a una delle finalità ammesse dal regolamento stesso. Tra queste viene menzionato l'interesse pubblico nel settore della salute pubblica e professionale, come le attività di protezione contro gravi minacce transfrontaliere per la salute e la sorveglianza della salute pubblica o le attività che garantiscono elevati livelli di qualità e sicurezza dell'assistenza sanitaria, compresa la sicurezza dei pazienti, e dei medicinali o dispositivi medici. Vengono specificati gli scopi come quelli statistici o le attività di istruzione nei settori sanitari o assistenziali.

Un'altra finalità è quella della ricerca scientifica per i settori della salute o dell'assistenza che contribuisce alla salute pubblica o alla valutazione delle tecnologie sanitarie, o che garantisce elevati livelli di qualità e sicurezza dell'assistenza sanitaria, dei medicinali o dei dispositivi medici, con l'obiettivo di favorire gli utenti finali, come i pazienti, gli operatori sanitari e gli amministratori della sanità, tra cui: (i) l'attività di sviluppo e l'innovazione di prodotti o servizi; (ii) la formazione, la sperimentazione e la valutazione di algoritmi, anche in dispositivi medici, dispositivi medici diagnostici in vitro [27], sistemi di intelligenza artificiale e applicazioni sanitarie digitali.

---

raccomandazione fornita dal titolare dei dati di fiducia. Gli enti di intermediazione dei dati sanitari, prosegue il considerando, non dovrebbero essere designati come titolari fiduciari di dati sanitari.

[27] Occorre precisare che nel caso in cui si fosse al cospetto di un sistema di intelligenza artificiale (IA), rientrante nella definizione offerta nell'emanando *Artificial Intelligence Act*, che funga da componente di sicurezza o sia il prodotto stesso di un dispositivo medico diagnostico in vitro, troverebbe altresì applicazione la disciplina ivi prevista per i sistemi di IA ad alto rischio.

Per alcune finalità, come l'interesse pubblico o gli scopi statistici, l'accesso è circoscritto e limitato agli enti pubblici anche nel caso in cui il trattamento dei dati per l'esecuzione di questi compiti venga effettuato da terzi per conto dell'organismo del settore pubblico.

L'EHDS prevede specifici obblighi, non solo in capo ai titolari dei dati, ma anche in capo agli utenti dei dati sanitari. Questi possono accedere ai dati sanitari elettronici per l'uso secondario e possono trattarli solo al cospetto dell'autorizzazione ai dati rilasciata dall'organismo responsabile dell'accesso ai dati sanitari. Non possono reidentificare o cercare di reidentificare le persone fisiche cui appartengono i dati sanitari elettronici ottenuti sulla base dell'autorizzazione. Sono tenuti a rendere pubblici i risultati o gli esiti dell'uso secondario dei dati sanitari elettronici, comprese le informazioni pertinenti per la prestazione di assistenza sanitaria. I risultati o gli esiti non possono contenere riferimenti ai dati personali.

Con uno sguardo rivolto anche alla normativa nazionale italiana, occorre specificare come nell'ambito del vigente Codice *Privacy* italiano (d.lgs. n. 196/2003), gli artt. 110 e 110-*bis* prescrivono che il trattamento dei dati relativi alla salute per finalità di ricerca scientifica in campo medico, biomedico o epidemiologico senza consenso sia ammissibile solo se consentito da specifiche disposizioni di legge, in conformità con l'articolo 9, comma 2, lett. *j)*, GDPR, oppure, al sussistere di determinate condizioni, previa consultazione del Garante per la Protezione dei Dati Personali (GPDP)[28]. Con una recentissima modifica normativa è stata rimossa la preventiva consultazione del GPDP prevedendo che quest'ultimo sia tenuto a individuare le garanzie da osservare.

Pertanto, il Regolamento EHDS costituisce, al sussistere di specifici presupposti, una base normativa necessaria che consente l'utilizzazione dei dati sanitari senza il consenso dell'interessato[29].

È utile precisare, infatti, che il consenso dell'interessato ai sensi dell'EHDS si presume prestato di *default*, ossia è previsto il meccanismo dell'*opt-out* per l'uso primario e secondario dei dati sanitari. In altri termini, in base a questo meccanismo, il consenso dell'interessato si presume prestato, ma quest'ultimo conserva in ogni momento il diritto di negarlo o revocarlo. Perciò, mentre nel caso dell'*opt-in* è necessario che vi sia una condotta attiva dell'interessato per la prestazione del consenso, nel caso dell'*opt-out* non sarebbe necessario.

---

[28] Sul tema, A. BERNES, *La protezione dei dati personali nell'attività di ricerca scientifica*, in *NLCC*, 2020, 1, p. 175. In materia, si veda anche GPDP, *compendio sul trattamento dei dati personali effettuato attraverso piattaforme volte a mettere in contatto i pazienti con i professionisti sanitari accessibili via web e app*, vers. marzo 2024.

[29] Il Regolamento EHDS potrebbe costituire la base giuridica richiesta dall'art. 9, par. 2, lett. *j)*, GDPR, eccezione al divieto generale di trattamento delle categorie particolari di dati personali in caso di «trattamento necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, par. 1, sulla base del diritto dell'Unione o nazionale (…)».

4. La sinergia tra *Data Governance Act* e l'*European Health Data Space*.

Le cooperative di dati possono rappresentare un importante strumento attuativo per realizzare concretamente lo spazio europeo dei dati sanitari, facilitando la loro condivisione in modo sicuro e controllato tra i diversi attori del settore sanitario.

Tuttavia, è importante analizzare ulteriori aspetti della disciplina normativa dell'EHDS. Esso, per l'uso secondario dei dati sanitari, prescrive alcuni obblighi gravanti sui titolari dei dati, i quali sono tenuti a mettere a disposizione i dati pertinenti ad esito di una richiesta dell'organismo di accesso che segue una apposita autorizzazione.

Il titolare è tenuto a mettere a disposizione dell'organismo di accesso i dati richiesti entro un termine ragionevole, e non oltre tre mesi dal ricevimento della richiesta. È tenuto poi all'adempimento degli obblighi nei confronti delle persone fisiche prescritti dal regolamento stesso e a comunicare all'organismo di accesso una descrizione dell'insieme di dati in suo possesso. Se questa serie di dati è corredata di un marchio di qualità e di utilità dei dati, il titolare dei dati sanitari fornisce all'organismo responsabile dell'accesso una documentazione sufficiente affinché quest'ultimo possa confermare la correttezza del marchio.

I detentori di dati sanitari elettronici non personali devono garantire l'accesso ai dati attraverso banche dati aperte per assicurare un accesso illimitato a tutti gli utenti e l'archiviazione e conservazione dei dati.

È ulteriormente importante evidenziare che l'EHDS prevede la facoltà per gli Stati membri di consentire, per alcune categorie di titolari di dati, che i loro obblighi siano assolti da entità di intermediazione di dati per ridurre l'onere amministrativo su di loro incombenti. Tali intermediari, come specificato nel considerando n. 40, possono essere persone giuridiche in grado di elaborare e rendere disponibili, per un uso secondario, i dati sanitari elettronici forniti dai titolari dei dati. Viene specificato che con «entità di intermediazione di dati sanitari» si deve intendere una persona giuridica in grado di mettere a disposizione, anche per la registrazione, la fornitura, il trattamento, la limitazione dell'accesso o lo scambio di dati sanitari elettronici forniti dai titolari dei dati per uso secondario. Lo stesso considerando precisa, però, che tali entità di intermediazione di dati sanitari svolgono compiti diversi dai servizi di intermediazione di dati previsti all'art. 10 del DGA.

Dunque, saranno necessari chiarimenti in ordine al riferimento che l'EHDS fa ad «alcune categorie di titolari di dati» che si possono avvalere di intermediari che, però, svolgono compiti diversi rispetto a quelli di cui al DGA.

Il tenore del regolamento in questione non consente di chiarire quali siano tali categorie di titolari di dati e rende difficile definire un perimetro chiaro entro cui un intermediario di dati disciplinato dal DGA (e quindi anche una cooperativa di dati) possa agire coadiuvando le attività di titolari di dati nell'adempimento dei propri obblighi prescritti dal regolamento. In ogni caso, il considerando succitato prevede che gli intermediari in questione svolgono «compiti diversi» rispetto agli intermediari di cui al DGA, ma ciò non esclude che quegli stessi intermediari previsti nel regolamento sulla *governance* dei dati possano agire coadiuvando i titolari dei dati sanitari. La

previsione normativa dell'EHDS che stabilisce la possibilità per gli intermediari di assolvere gli obblighi dei titolari per ridurre il loro onere amministrativo dovrebbe essere intesa come una ulteriore forma di intermediazione che si aggiunge ai servizi di cui all'art. 10 DGA, ma che non esclude l'applicabilità di tale ultimo regolamento europeo. Perciò, si potrebbe finanche ritenere ammissibile la costituzione di cooperative di dati composte da titolari di dati sanitari di cui all'EHDS.

Nel quadro del regolamento EHDS, per l'uso secondario, i soggetti coinvolti sono: gli interessati (i pazienti a cui i dati sanitari, benché da anonimizzare, si riferiscono); i titolari di dati (struttura ospedaliera, clinica o altro ente che opera nel settore sanitario); l'organismo pubblico di accesso (autorità nazionale designata ai sensi dell'EHDS) e gli utenti (centri di ricerca o aziende nel settore dell'innovazione).

È quindi possibile immaginare un intermediario, anche sotto forma di cooperativa di dati, che operi per far sì che gli interessati compiano scelte informate in un ambito così delicato, anche sotto forma di una struttura che predisponga strumenti digitali utili per il mantenimento del controllo sui dati sanitari. Il discorso non rimane circoscritto al solo uso secondario, ma potrebbe essere esteso anche all'uso primario.

Gli intermediari, anche in questo caso sotto forma di cooperativa di dati, potrebbero svolgere ugualmente un ruolo cruciale a favore dei titolari di dati sanitari. Tuttavia, come si è visto, in questo caso è necessario chiarire il perimetro normativo entro il quale si può ipotizzare che una cooperativa disciplinata dal DGA possa operare a favore di titolari di dati personali consentendo una condivisione di dati, anche per la loro anonimizzazione, più fluida e trasparente, ma la possibilità di costituire una cooperativa di dati composta da titolari di dati personali dovrebbe ritenersi ammissibile.

Non sembra possa ipotizzarsi – almeno focalizzandosi sul quadro offerto dal DGA – una cooperativa di dati per gli organismi di accesso designati, trattandosi di autorità pubbliche, così come non sembra possibile ipotizzare una simile organizzazione composta da "utenti", poiché esse operano a tutela dei membri per i propri dati personali, e non per i dati di altri soggetti interessati o detentori.

Sull'ammissibilità di un servizio di intermediazione di dati è inoltre necessario accertare che ciò sia volto a instaurare un rapporto commerciale ai fini della condivisione dei dati tra un numero indeterminato di interessati e di titolari da un lato e di utenti dall'altro (v. art. 2, n. 11, DGA) [30].

Un margine di operatività da parte di intermediari nell'ambito dell'EHDS sembra ipotizzabile anche là dove previsto da una normativa nazionale. Infatti, all'art. 1, il regolamento sui dati sanitari prevede che rimangono impregiudicate le norme europee o nazionali in materia di trattamento elettronico dei dati sanitari a fini di rendicontazione, di ottemperanza alle richieste di accesso alle informazioni o di dimostrazione o verifica del rispetto degli obblighi di legge o quelle in materia di concessione dell'accesso e di divulgazione dei documenti ufficiali.

[30] Benché non sia esplicitata la ragione circa la necessità dell'instaurazione di un "rapporto commerciale", e non semplicemente di un "rapporto giuridico", alcune specificazioni su quale possa essere inteso un tale rapporto è contenuta nel considerando n. 28 e n. 29 del DGA.

Rimangono altresì impregiudicate quelle norme sull'accesso ai dati sanitari elettronici per uso secondario concordato nel quadro di accordi contrattuali o amministrativi tra soggetti pubblici o privati. Dunque, su una base negoziale e di coordinamento con la normativa nazionale, si potrebbe ipotizzare anche un diverso e più esteso perimetro per gli intermediari di dati, soprattutto a supporto dei titolari dei dati e degli organismi di accesso.

L'intero quadro della condivisione dei dati nel settore sanitario, però, deve considerare che oggi molti di questi dati vengono rilevati, talvolta generati, o comunque trattati, mediante prodotti connessi, anche da remoto. Ciò rende doverosa l'analisi e il coordinamento con la normativa del *Data Act*.

5. Il *Data Act* (Reg. UE 2023/2854).

La nuova normativa delineata dal *Data Act* stabilisce una serie di regole con cui si intende, *inter alia*, individuare i soggetti legittimati all'accesso e all'utilizzo dei dati generati dai prodotti connessi e dai servizi correlati (ci si trova nel settore del c.d. *Internet of Things*)[31]. Il regolamento è stato pubblicato nella G.U. europea il 22 dicembre 2023 ed è vigente a partire dal 11 gennaio 2024. La sua applicazione è prevista a cadenze differenti a seconda dei relativi capi [32]. In caso di contrasto tra GDPR e *Data Act*, prevale il primo.

---

[31] D. POLETTI, *Il controllo dell'interessato e la strategia europea sui dati*, in *Osservatorio sulle fonti*, 2023, 2, p. 367, spec. p. 373.

Il *considerando* n. 15 del *Data Act* precisa a quali dati si fa riferimento nel regolamento legittimando l'accesso e la loro circolazione. Si specifica che i dati generati dall'uso di un prodotto connesso o di un servizio correlato devono essere intesi come dati registrati intenzionalmente o dati che derivano indirettamente da un'azione dell'utente, ad esempio i dati relativi all'ambiente o alle interazioni del prodotto connesso. «Ciò dovrebbe comprendere i dati sull'uso di un prodotto connesso generati da un'interfaccia utente o tramite un servizio correlato e non dovrebbe limitarsi all'informazione relativa al fatto che tale uso è avvenuto, ma dovrebbe comprendere tutti i dati generati dal prodotto connesso a seguito di tale uso, ad esempio i dati generati automaticamente da sensori e i dati registrati da applicazioni incorporate, incluse le applicazioni indicanti lo stato dell'hardware e i malfunzionamenti. Dovrebbe altresì comprendere i dati generati dal prodotto connesso o dal servizio correlato durante i periodi di inattività dell'utente, ad esempio quando quest'ultimo sceglie di non utilizzare un prodotto connesso per un determinato periodo di tempo ma di tenerlo in modalità stand-by o addirittura spento, in quanto lo stato di un prodotto connesso o dei suoi componenti, ad esempio le batterie, può variare quando il prodotto connesso è in modalità stand-by o spento. I dati che non sono modificati in modo sostanziale, ossia i dati in forma grezza, noti anche come dati fonte o dati primari che si riferiscono a punti di dati generati automaticamente senza alcuna ulteriore forma di trattamento, e i dati che sono stati pretrattati al fine di renderli comprensibili e utilizzabili prima di ulteriori operazioni di trattamento e analisi rientrano nell'ambito di applicazione del presente regolamento».

[32] L'art. 50 del *Data Act* prevede la sua applicazione dal 12 settembre 2025. L'obbligo derivante dall'art. 3, paragrafo 1, si applica ai prodotti connessi e ai servizi correlati immessi sul mercato dopo il 12 settembre 2026. Il capo III si applica solo in relazione agli obblighi di messa a disposizione dei

Anche nel *Data Act*, al pari di quanto avviene nel DGA, si assiste a un cambio di paradigma, anche lessicale, visti i riferimenti alla "titolarità dei dati".

Infatti, ai sensi del regolamento in questione, con «titolare dei dati» deve intendersi quella persona che ha il diritto o l'obbligo di utilizzare e mettere a disposizione i dati, inclusi quei dati del prodotto o di un servizio correlato, se previsto contrattualmente. Con «utente» si intende quella persona che possiede un prodotto connesso o una persona a cui, temporaneamente, sono stati concessi i diritti di utilizzo in relazione a tale prodotto.

Con «destinatario dei dati» si intende quella persona alla quale vengono messi a disposizione i dati da parte del titolare.

Con «servizio correlato» deve intendersi quel servizio digitale (diverso rispetto a un servizio di comunicazione elettronica), connesso con il prodotto al momento dell'acquisto o noleggio. Infine, con il termine «prodotto connesso» il legislatore intende quel bene che ottiene, genera o raccoglie dati relativi al suo utilizzo o al suo ambiente. Tale prodotto è in grado di comunicare dati tramite un servizio di comunicazione elettronica, una connessione fisica o l'accesso su dispositivo, e la sua funzione primaria non riguarda l'archiviazione, il trattamento o la trasmissione dei dati per conto di una parte diversa dall'utente.

6. Funzione, struttura e disciplina del *Data Act* in sinergia con il GDPR e l'EHDS.

Il *Data Act*, in una prospettiva complementare al DGA, intende favorire la circolazione dei dati e ampliare la platea dei soggetti che possono avere accesso alle informazioni, consentendo, ad esempio, ai proprietari di dispositivi connessi, di accedere ai dati da essi generati, autorizzandone poi la condivisione con terze parti nella fornitura di servizi post-vendita.

In un altro capo del regolamento sono poi previste nuove prerogative di accesso ai dati da parte degli enti pubblici in presenza di «necessità eccezionali» [33].

Si tratta, perciò, di un regolamento complesso che regola differenti sfaccettature e ambiti inerenti all'accesso ai dati.

A partire dall'art. 3 del *Data Act*, vengono stabilite una serie di regole volte a determinare le modalità di esercizio del diritto di accesso ai dati generati dal prodotto connesso o dal servizio correlato da parte dell'utente. L'art. 5, peraltro, pre-

---

dati a norma del diritto dell'Unione o della legislazione nazionale adottata in conformità del diritto dell'Unione, che entrano in vigore dopo il 12 settembre 2025. Il capo IV si applica ai contratti conclusi dopo il 12 settembre 2025. Il capo IV si applica a decorrere dal 12 settembre 2027 ai contratti conclusi il o anteriormente al 12 settembre 2025, a condizione che: a) siano a tempo indeterminato; o b) scadano almeno 10 anni dopo l'11 gennaio 2024.

[33] G. BUTTARELLI, *La regolazione delle piattaforme digitali: il ruolo delle istituzioni pubbliche*, in *Giornale dir. amministrativo*, 2023, 1, p. 116, spec. p. 120.

vede un diritto dell'utente di condividere i dati con terzi, prontamente messi a loro disposizione dal titolare dei dati, oltre ai relativi metadati necessari a interpretare e utilizzare i dati in questione. Tuttavia, è da notare come dalla nozione di «terzo», a cui possono essere messi a disposizione i dati, il par. 3 dell'art. 5 esclude espressamente quei soggetti che sono *gatekeeper* ai sensi del *Digital Markets Act* (DMA).

Se l'utente intende condividere – per i tramite del titolare – dati con terzi, qualora essi riguardino dati personali anche di altri soggetti, diversi dall'utente, possono essere messi a disposizione del terzo solo al cospetto di un'idonea base giuridica prevista dall'articolo 6 GDPR e, se necessario, nel rispetto dell'art. 9 GDPR inerente ai dati personali particolari e all'art. 5, par. 3, dir. (UE) 2022/58.

Ma in generale, come specificato nel considerando n. 7, il *Data Act* non costituisce una base giuridica per la raccolta o la generazione di dati personali da parte del titolare dei dati. La normativa impone ai titolari dei dati, dietro richiesta di un utente, di mettere i dati personali a disposizione degli utenti o di terzi scelti dall'utente, ma l'accesso deve essere fornito ai dati personali trattati dal titolare dei dati in forza di una delle basi giuridiche del GDPR. Se l'utente non coincide con l'interessato, il *Data Act* non costituisce una base giuridica per consentire l'accesso ai dati personali o per mettere i dati personali a disposizione di terzi e non dovrebbe essere inteso nel senso che conferisce al titolare dei dati un nuovo diritto di utilizzare i dati personali generati dall'uso di un prodotto connesso o di un servizio correlato. In tali casi potrebbe essere nell'interesse dell'utente facilitare il rispetto dei requisiti di cui all'art. 6 del GDPR. Visto che il *Data Act* non dovrebbe ledere i diritti alla protezione dei dati degli interessati, in questi casi il titolare dei dati può dar seguito alle richieste, tra l'altro, anonimizzando i dati personali o, nel caso in cui i dati prontamente disponibili contengano dati personali di più interessati, trasmettendo solo i dati personali relativi all'utente.

In una chiave di lettura combinata tra GDPR (artt. 6 e 9), *Data Act* (art. 5 e ss.) e il regolamento EHDS, quest'ultimo potrebbe costituire quella norma europea che prescrive quelle misure appropriate e specifiche per la tutela dei diritti e delle libertà dell'interessato per finalità di ricerca scientifica (art. 9, par. 2, lett. *j*), GDPR) e per motivi di interesse pubblico nel settore della sanità pubblica (art. 9, par. 2, lett. *i)*, GDPR). Ciò potrebbe costituire la base giuridica necessariamente richiesta dal *Data Act* affinché possa essere attivato il meccanismo di condivisione dei dati sanitari anche mediante prodotti connessi e per il tramite del *opt-out* sancito nell'EHDS per l'uso secondario.

Il Capo III del *Data Act* prosegue stabilendo gli obblighi gravanti sul titolare di mettere a disposizione i dati ai destinatari sulla base delle condizioni concordate con questi ultimi (art. 8). Gli accordi tra questi due soggetti non devono contenere clausole abusive disciplinate nel successivo art. 13 del *Data Act*.

Inoltre, l'attività prevista a carico del titolare dei dati può prevedere un congruo compenso che, nello schema di combinazione con l'EHDS potrebbe essere corrisposto dall'*utente dei dati* secondo la concezione di quest'ultimo regolamento il quale, a sua volta, lo potrebbe ricevere dall'*utente finale* come l'ente di ricerca o l'impresa.

L'utente dovrebbe essere libero di utilizzare i dati per qualsiasi finalità legittima, inclusa la fornitura dei dati che egli ha ricevuto nell'esercizio dei suoi diritti a un terzo che offre un servizio post-vendita e che può essere in concorrenza con un servizio fornito da un titolare dei dati.

I titolari dei dati devono perciò garantire che i dati messi a disposizione del terzo siano tanto accurati, completi, affidabili, pertinenti e aggiornati quanto i dati ai quali il titolare stesso può essere in grado o avere il diritto di accedere in virtù dell'uso del prodotto connesso o del servizio correlato [34].

Secondo il *considerando* n. 33, nella messa a disposizione dei dati a un terzo, il titolare dei dati non deve abusare della sua posizione per ottenere un vantaggio competitivo in mercati in cui il titolare dei dati e il terzo possono trovarsi in concorrenza diretta. Quindi, il «titolare dei dati» non deve utilizzare dati prontamente disponibili al fine di ottenere informazioni sulla situazione economica, sulle risorse o sui metodi di produzione del terzo o sul loro utilizzo da parte di quest'ultimo in un modo tale da compromettere la posizione commerciale del terzo sui mercati in cui quest'ultimo è attivo.

Ma lo stesso *considerando* n. 33 prevede espressamente che «gli intermediari di dati tra impresa e impresa e i sistemi di gestione delle informazioni personali, denominati servizi di intermediazione dei dati nel Reg. (UE) 2022/868, possono aiutare gli utenti o i terzi a stabilire relazioni commerciali con un numero indeterminato di potenziali controparti per qualsiasi finalità legittima rientrante nell'ambito di applicazione del presente regolamento. Essi potrebbero svolgere un ruolo determinante nell'aggregare l'accesso ai dati in modo da facilitare le analisi dei *big data* o l'apprendimento automatico, purché gli utenti mantengano il pieno controllo sulla facoltà di fornire o meno i propri dati a tale aggregazione e sulle condizioni commerciali alle quali i loro dati devono essere utilizzati». Ecco, quindi, che ancora una volta la figura dell'intermediario può ricoprire un ruolo centrale.

7. Osservazioni conclusive sulla nuova geometria dei rapporti giuridici delineati dalla normativa europea.

Si è messo in risalto, già dal titolo del presente contributo, che il tema della condivisione dei dati (in questo caso sanitari) deve fare i conti con un dedalo normativo che costituisce un campanello di allarme per la certezza del diritto.

Più precisamente, se occorre procedere con la sola attuazione dell'EHDS, il suo contenuto, benché voluminoso e articolato, non presenta profili problematici. Questi ultimi emergono nel caso in cui si intenda integrare il meccanismo ivi delineato con la partecipazione di intermediari di dati come le cooperative di dati, le quali possono favorire il suo funzionamento, oppure, nel caso in cui la condivisione dei

[34] In questo senso il *considerando* n. 30 del EHDS.

dati sanitari avvenga per mezzo di prodotti connessi che portano all'applicazione del *Data Act*. L'intero quadro deve essere in ogni caso armonizzato con il GDPR, con la normativa in materia di *cybersecurity* e con il Codice della privacy italiano.

Le cooperative di dati possono essere, quali intermediari, attori centrali nell'attuazione di un ecosistema di condivisione dei dati sanitari che dovranno essere valorizzati affinché esso possa essere attuato in modo efficace, favorendo i titolari dei dati e gli interessati.

Tra l'altro occorre considerare la necessità di un equilibrato coordinamento tra le varie discipline citate anche in un'ottica definitoria. Infatti, in tutte quelle situazioni in cui la condivisione dei dati avviene con il tramite di prodotti connessi, i titolari dei dati secondo il DGA e l'EHDS, come si è visto, sarebbero quegli enti, ospedalieri o di assistenza sanitaria, che possono (o devono) concedere l'accesso ai dati sanitari.

Sul punto, occorre notare che, secondo il DGA, i "titolari dei dati" hanno il *diritto* di accedere o di condividere i dati; ma, in una lettura combinata con l'emanando EHDS, si dovrebbe considerare che su tali soggetti può incombere anche l'*obbligo* di condivisione. Ai sensi del *Data Act*, invece, i titolari dei dati sarebbero quei soggetti aventi il *diritto* o l'*obbligo* di mettere a disposizione i dati generati dal prodotto connesso e, quindi, i fornitori di quegli strumenti dal quale vengono estratti o generati i dati sanitari. Sempre ai sensi del *Data Act*, l'utente sarebbe colui che ha il possesso/detenzione del prodotto o il soggetto che ha il diritto di utilizzo del prodotto connesso; quindi, nella struttura sinergica tra DGA e EHDS, sarebbero le strutture ospedaliere, o gli altri operatori del settore rientranti nella nozione, oppure, direttamente il soggetto interessato. Il destinatario dei dati previsto dal *Data Act*, al quale vengono messi a disposizione i dati, può essere identificato, a seconda dei casi, anche con l'utente dei dati previsto nel DGA e con l'organismo di accesso ai dati sanitari previsto dal EHDS, il quale, concederà poi la condivisione all'utente dei dati qualificato come tale dallo stesso EHDS, quindi all'ente di ricerca o all'impresa che produce sistemi innovativi. Infine, dovrà essere ricomposta la trama dei ruoli definiti dal GDPR come la titolarità del trattamento, che potrà essere evidentemente condivisa tra più soggetti, oltre alla figura del responsabile del trattamento.

In tale articolato schema normativo, le cooperative di dati rappresentano una opportunità a beneficio degli interessati e dei titolari dei dati. Perciò, le opportunità di creare un sistema di condivisione dei dati sanitari in un ambiente europeo sicuro sono tante e lo sforzo necessario in termini di attuazione sarà una sfida che dovrà essere necessariamente vinta.

Capitolo XXIV

Data Governance Act e cooperative di dati: una "possibile" nuova frontiera per la ricerca in sanità

Luigi Rufo

Abstract: The essay scrutinizes the opportunity of circulating data concerning health, for the purpose of clinical research, through the creation of a data cooperative. Just to better understand the phenomenon, some existing practical cases of data cooperatives active in the field of health are reviewed, lastly, the data protection legislation and the limits it places on the Data Governance act in the processing of data concerning health are examined.

1. Premessa, il dato relativo alla salute come bene comune.

La sanità elettronica, il crescente e sempre "nuovo" rapporto uomo-tecnologia, il periodo della pandemia da Covid 19 sono tutti fattori che in ambito sanitario stanno spingendo verso il ritenere il dato relativo alla salute del cittadino un elemento sempre più importante nel completamento del concetto di «salute come bene comune» [1], così non facendo più solo corrispondere alla "salute" la semplice assenza di malattie o complessiva efficienza psicofisica [2], ma configurandola an-

[1] Sul punto: T. SEPPILLI, *Salute e sanità come beni comuni. Per un nuovo sistema sanitario*, in *Educazione Sanitaria e Promozione della Salute*, Perugia, vol. 33, n. 4, 2010; S. RODOTÀ, *Il diritto di avere diritti*, Roma-Bari, 2013.

[2] L'Organizzazione Mondiale della Sanità (OMS) ha definito il concetto di salute come «Una

che come un ecosistema di elementi e di soluzioni atta a garantirla.

In questo quadro, la quotidiana generazione di dati nei percorsi diagnostico-terapeutici assistenziali (c.d. PDTA) conduce verso una migliore condivisione dei processi decisionali tra gli operatori sanitari e a una più efficace erogazione delle prestazioni di diagnosi, trattamento e cura per i pazienti che si trovano sia in regime di ricovero ospedaliero che di assistenza domiciliare.

È doveroso però evidenziare come il dato sia un elemento grezzo che solamente inserito in uno specifico contesto assume un proprio patrimonio informativo collegato e/o collegabile ad un interessato, rappresentando così l'elemento tecnico-giuridico attraverso il quale vengono tutelati i diritti collegati all'identità personale, alla riservatezza e al diritto della protezione dei dati personali di un soggetto [3].

Se vogliamo provare a dare una definizione di dato, nella sua eccezione di elemento grezzo, è sicuramente di aiuto il *Data Governance Act* che all'art. 2, n. 1, afferma che sono «"dati": qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi raccolta di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva».

Passando però ad una descrizione più precisa, il Regolamento Europeo per la protezione dei dati personali n. 679 del 2016 (c.d. GDPR), all'art. 4, n. 1, prevede che «"dato personale": qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale».

In questo contesto, tuttavia, particolarmente importante è la classificazione e la tassonomia delle varie tipologie di dati personali che a seconda della loro peculiarità sono trattati con cautele e regole giuridiche diverse.

Una delle *species* più delicate di dati personali è quella relativa ai dati rientranti in categorie particolari: si tratta dei dati c.d. "*sensibili*", cioè quelli che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politi-

---

condizione di completo benessere fisico, mentale e sociale e non esclusivamente l'assenza di malattia o infermità». Si rimanda a tal riguardo al Preambolo alla costituzione dell'organizzazione Mondiale della Sanità come adottato dalla Conferenza Internazionale della Sanità, New York, 19-22 giugno 1946 e sottoscritto il 22 luglio 1946 dai rappresentanti di 61 stati (Official Records of the World Health Organization, no. 2, p. 100), entrato in vigore il 7 aprile 1948.

[3] Il diritto alla protezione dei dati personali, alla luce dell'art. 2 del Codice *privacy*, ha rappresentato nell'ordinamento italiano un'importante innovazione rispetto alla legge n. 675 del 1996. Infatti, nel 2003 per la prima volta non si è fatto più solo riferimento alla tutela delle persone fisiche o delle persone giuridiche ma indistintamente si è iniziato a parlare di interessato, in questo modo si è aperta la possibilità di riconoscere come titolari di tali diritti una pluralità di soggetti, oltre ad aprire alla possibilità di tutelare diritti fondamentali già riconosciuti dalla giurisprudenza della Corte di Cassazione, come il diritto alla riservatezza riconosciuto per la prima volta nel 1975.

che, l'appartenenza sindacale, nonché i dati genetici, i dati biometrici, i dati relativi alla salute o alla vita sessuale.

Proprio con l'evoluzione delle nuove tecnologie e della sanità elettronica, i dati relativi alla salute hanno assunto un ruolo significativo e trovato per la prima volta all'art. 4, n. 15, del GDPR una propria definizione che afferma: «"dati relativi alla salute"»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute».

Possiamo così dividere il dato personale (più nello specifico quello relativo alla salute) in quattro elementi fondamentali, e precisamente:

a) «qualsiasi informazione»,

b) «riguardante» [4] (l'interessato a cui si riferiscono i dati),

c) «persona fisica» (riferito all'interessato),

d) «identificata o identificabile» (riferito all'informazione).

Ne deriva che il dato personale è un concetto dinamico ed ampio che include tutte le informazioni [5] (comprese quelle sanitarie) riferibili direttamente e indirettamente alla persona fisica e la vera chiave imprescindibile di congiunzione tra i vari elementi diventa il collegamento funzionale che deve esistere tra il "frammento di informazione" e la persona fisica. Così, andando bene ad analizzare la nozione di dato relativo alla salute si devono pertanto ritenere comprese nella sua definizione le informazioni derivanti da test e/o esami che riguardano la malattia, l'eventuale stato di disabilità, la storia clinica passata e presente, l'incidenza del rischio di una malattia ereditaria, le mappature genetiche familiari, ecc., indipendentemente che siano state generate da risultanze di un professionista sanitario o da un dispositivo medico da un esame di laboratorio [6].

Tutto questo patrimonio informativo (*id est*: il dato) relativo alla salute dei cittadini derivante da cartelle cliniche, da sperimentazioni cliniche, da registri sanitari, da spese rendicontate della sanità pubblica e privata, può rappresentare sicuramente un bene comune nell'evoluzione futura della ricerca scientifica in ambito sanitario. Il personale della ricerca, infatti, potrà avere accesso ed analizzare dati più completi e maggiormente attinenti al fenomeno di interesse, incrociandoli anche attraverso un riutilizzo di dati storici, su larga scala.

Così, anche muovendoci sul solco di volere valorizzazione i dati relativi alla salute, ritenuti come bene comune e patrimonio prezioso per lo sviluppo del benessere psico-fisico dei cittadini, può diventare strategico l'applicazione del *Data Go-*

---

[4] Si noi come nella Direttiva 95/46/CE, abrogata dal GDPR, era utilizzato il termine "concernente".

[5] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, pareri: n. 162 del 30 marzo 2017 (doc. web. n. 6393422); n. 246 del 24 maggio 2017 (doc. web. n. 6495600); n. 366 del 7 settembre 2017 (doc. web n. 7155171); n. 433 del 26 ottobre 2017 (doc. web n. 7156158).

[6] Sul punto P. GUARDA, *i dati sanitari*, in V. CUFFARO-R. D'ORAZIO-V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019.

vernance Act – DGA (Regolamento UE 2022/868) [7], pilastro della strategia europea per i dati che, con un forte e concreto cambio di passo rispetto alla *Direttiva Open Data* (Direttiva UE 2019/1024) [8], mira a creare un mercato interno dei dati incentivando la condivisione di dati personali e non, tenendo conto di non pregiudicare le esigenze di tutela che le varie tipologie di dati (come quelli relativi alla salute) richiedono.

2. L'applicazione del *Data Governance Act* nella ricerca sanitaria.

2.1. Circolazione dei dati relativi alla salute per fini altruistici.

Come accennato in precedenza il *Data Governance Act* mirando a rafforzare la fiducia nella condivisione volontaria dei dati a beneficio della collettività rappresenta, grazie alla lettura unitaria dei suoi tre elementi strutturali, una "possibile" nuova frontiera per la ricerca sanitaria.

Ebbene, la capacità di raccogliere, organizzare, elaborare, analizzare, accedere e condividere i dati relativi alla salute si conferma come fattore indispensabile per garantire una mirata assistenza sanitaria e sociale. Scenario questo appena descritto già sperimentato durante la prima fase della pandemia da Covid-19, ed infatti a posteriori è stato possibile constatare che solo le realtà territoriali strutturalmente più organizzate hanno tratto beneficio proprio dalla possibilità di disporre di dati organizzati e interoperabili provenienti da *datasets* afferenti a organismi, pubblici e privati, differenti.

A questo punto è doveroso richiamare i tre elementi strutturali [9] del *Data Governance Act* che sono di sicuro collettore per la sua applicazione in ambito di ricerca sanitaria.

Un primo elemento strutturale importante dà richiamare è la circolazione dei dati per fini altruistici [10].

Il *Data Governance Act*, all'art. 2, n. 16, da una chiara definizione di altruismo di dati: «"Altruismo dei dati": la condivisione volontaria di dati sulla base del consenso accordato dagli interessati al trattamento dei dati personali che li riguardano, o sulle autorizzazioni di altri titolari dei dati volte a consentire l'uso dei loro dati non

---

[7] Per un maggior approfondimento sul tema: F. BRAVO, *Intermediazione di dati personali e servizi di* data sharing *dal GDPR al* Data Governance Act, in *Contratto e impresa Europa*, 2021, 1, pp. 199-256.

[8] Direttiva recepita in Italia con il d.lgs. n. 200 del 2021.

[9] Per un maggior approfondimento sul punto: G. RESTA, *Pubblico, privato e collettivo nel sistema europeo di governo dei dati*, in *Riv. trim. dir. pubbl.*, 2022, 4, pp. 971-995.

[10] Il capo IV della proposta è finalizzato proprio ad agevolare l'altruismo dei dati, fenomeno sino ad oggi piuttosto trascurato, eppure di grande interesse per gli studiosi, perché introduce, nella circolazione dei dati, una logica sostanzialmente donativa, si rimanda sul punto a: D. POLETTI, *Gli intermediari dei dati*, in *European Journal of Privacy Law & Technologies*, 2022, 1, p. 46 ss.

personali, senza la richiesta o la ricezione di un compenso che vada oltre la compensazione dei costi sostenuti per mettere a disposizione i propri dati, per obiettivi di interesse generale, stabiliti nel diritto nazionale, ove applicabile, quali l'assistenza sanitaria, la lotta ai cambiamenti climatici, il miglioramento della mobilità, l'agevolazione dell'elaborazione, della produzione e della divulgazione di statistiche ufficiali, il miglioramento della fornitura dei servizi pubblici, l'elaborazione delle politiche pubbliche o la ricerca scientifica nell'interesse generale».

Si tratta, in altri termini, di dati personali messi a disposizione dagli interessati su base volontaria (e comunque previo il rilascio del consenso al trattamento) oppure di dati non personali messi a disposizione dai titolari dei dati che li hanno legittimamente acquisiti nel rispetto delle finalità istituzionali.

Senza dubbio il campo della ricerca in ambito sanitario rappresenta il miglior terreno su cui testare la condivisione e circolazione dei dati per fini altruistici con lo scopo di soddisfare un interesse generale. Infatti, se andiamo a individuare una definizione di ricerca clinica, dobbiamo intendere un qualsiasi studio condotto su esseri umani con il fine di aiutare la comunità a determinare l'uso di una nuova medicina, dispositivo medico o trattamento sanitario.

Tutti gli studi clinici hanno come obiettivo il progresso della medicina al fine di garantire una migliore assistenza ai cittadini/pazienti, anche in termini di prevenzione.

A tutela degli interessati e con l'intento di aumentare la loro fiducia nel mettere a disposizione i propri dati, il *Data Governance Act* prevede, all'art. 17, che le organizzazioni per l'altruismo dei dati siano censite in «un registro pubblico nazionale delle organizzazioni per l'altruismo dei dati riconosciute» periodicamente aggiornato. Ed al fine di essere ammissibile alla registrazione, ai sensi del successivo art. 18, un ente deve: «*a)* volgere attività di altruismo dei dati; *b)* essere una persona giuridica costituita a norma del diritto nazionale per conseguire obiettivi di interesse generale, stabiliti nel diritto nazionale, ove applicabile; *c)* operare senza scopo di lucro ed essere giuridicamente indipendente da qualsiasi entità che operi a scopo di lucro; *d)* svolgere le proprie attività di altruismo dei dati mediante una struttura funzionalmente separata dalle sue altre attività» [11].

Il controllo sull'attività delle organizzazioni per l'altruismo dei dati è garantito da un sistema di registrazione amministrativa, ai sensi dell'art. 19, e dall'obbligo di trasparenza ai sensi all'art. 20 che prevede che ogni organizzazione per l'altruismo dei dati debba redigere una relazione annuale di attività annotando tra le varie cose «una descrizione delle modalità con cui, nel corso dell'esercizio finanziario in questione, sono stati promossi gli obiettivi di interesse generale per le quali sono stati raccolti i dati» e «una sintesi dei risultati dei trattamenti dei dati autorizzati».

[11] Con il d.lgs.7 ottobre 2024, n. 144, all'art. 2 l'AgID è stata designata autorità competente alla registrazione di organizzazioni per l'altruismo dei dati.

2.2. Riutilizzo dei dati relativi alla salute delle strutture pubbliche e/o privati convenzionati.

Un secondo elemento strutturale del *Data Governance Act*, che si può ritenere strettamente legato all'altruismo dei dati (sopra richiamato), interessante da analizzare – in ottica di adattabilità alla ricerca clinica – è il possibile riutilizzo dei dati in mano pubblica.

Previsione, nella sua portata generale, espressamente richiamata nel *considerando* n. 6 del testo normativo, che prevede: «(…) i dati generati o raccolti da enti pubblici o altre entità a carico dei bilanci pubblici debbano apportare benefici alla società è da tempo parte integrante delle politiche dell'Unione. La direttiva (UE) 2019/1024 e la normativa settoriale dell'Unione garantiscono che gli enti pubblici rendano facilmente disponibile per l'utilizzo e il riutilizzo una quota maggiore dei dati che producono».

Questo segnerebbe una rilevante prospettiva futura per la ricerca sanitaria, infatti l'accesso ai *datasets* della pubblica amministrazione e dei privati, in regime di convenzionamento con il SSN, porterebbe i ricercatori a poter sfruttare un patrimonio informativo granulare e continuamente aggiornato. Si potrebbe così ipotizzare un *Data Lake* [12] nazionale (o anche europeo) di dati relativi alla salute utilizzali per la ricerca sanitaria, e ad oggi basterebbe solo convogliare i dati sanitari dei tanti strumenti già esistenti come il Fasciolo Sanitario Elettronico (FSE).

Ipotesi questa del riutilizzo conosciuta già nel nostro sistema normativo, prevista nell'ambito del codice dell'amministrazione digitale, quando si parla di acquisizione e riuso del *software* della pubblica amministrazione [13]. In modo particolare grazie a delle linee guida dell'Agenzia per l'Italia digitale, si è nel tempo promosso un importante cambio culturale che ha condotto verso un più ampio utilizzo del *software* di tipo aperto facendo sì che qualsiasi investimento di una P.A. sia messo a fattor comune delle altre amministrazioni e della collettività e consentendo di semplificare le scelte di acquisto e gli investimenti in tema di servizi digitali.

Naturalmente ogni soggetto pubblico è libero di decidere se consentire o negare l'accesso e/o la condivisione per il riutilizzo, ma in caso di scelta positiva anche in questa circostanza sono previste delle condizioni specifiche regolate ai sensi dell'art. 5.

Le condizioni ovviamente sono «proporzionate e oggettivamente giustificate in relazione alle categorie di dati e alle finalità del riutilizzo e alla natura dei dati per i quali è consentito il riutilizzo» e ad esempio, se si tratta di dati personali, questi devono essere resi in forma anonima; se invece il riuso ha ad oggetto informazioni

---

[12] Un *Data Lake* è un *repository* centralizzato che permette di archiviare tutti i dati strutturati e non su qualsiasi scala. È possibile archiviare dati grezzi, senza doverli preliminarmente strutturare, ed eseguire diversi tipi di analisi, dall'elaborazione classica di Big Data all'analisi dei dati in tempo reale sfruttando il *machine learning*.

[13] L'acquisizione e il riuso del *software* PA è previsto all'art. 68 del d.lgs. 7 marzo 2005, n. 82 (Codice dell'Amministrazione Digitale).

commerciali riservate «compresi i segreti commerciali o i contenuti protetti da diritti di proprietà intellettuale», queste devono essere aggregate per salvaguardarne la confidenzialità.

2.3. Intermediazione: le cooperative di dati.

Il servizio di intermediazione dei dati è definito all'interno del *Data Governance Act* all'art. 2, n. 11, come «un servizio che mira a instaurare, attraverso strumenti tecnici, giuridici o di altro tipo, rapporti commerciali a fini di condivisione dei dati tra un numero indeterminato di interessati e di titolari di dati, da un lato, e gli utenti dei dati dall'altro, anche al fine dell'esercizio dei diritti degli interessati in relazione ai dati personali».

Al fine di comprendere la portata dei servizi di intermediazione è doveroso e sin da subito precisare i ruoli dei soggetti coinvolti. In particolare:

– l'interessato è da intendersi, come richiamato nel GDPR (art. 4, n. 1), la persona fisica identificata, direttamente o indirettamente, al quale i dati si riferiscono;

– il titolare dei dati (c.d. *data holder*) è definito come la persona giuridica, comprese le pubbliche amministrazioni, o un terzo persona fisica (che non è l'interessato) che ha il diritto di concedere l'accesso a determinati dati o di condividerli;

– gli utenti di dati (c.d. *data users*) sono invece persone fisiche o giuridiche che hanno l'accesso legittimo a determinati dati personali e non personali e che hanno diritto, ai sensi del GDPR, di utilizzarli per fini commerciali o non commerciali.

Chiariti i ruoli è ora opportuno comprendere quale sia il miglior servizio di intermediazione per la condivisione e il riuso dei dati relativi alla salute da utilizzare nella ricerca clinica.

Leggendo il testo normativo, ai sensi dell'art. 10 sono previste tre tipologie di servizi di intermediazione:

a) la prima tipologia di servizio di intermediazione è incentrata sulla condivisione dei dati tra titolari e utenti dei dati, al fine di instaurare rapporti commerciali – bilaterali o multilaterali – di scambio di dati (c.d. scambio B2B). L'azione dell'intermediario è svolta per il mezzo della creazione di piattaforme o banche dati *ovvero* attraverso la creazione di una infrastruttura d'interconnessione diretta tra titolari e utenti dei dati;

b) una seconda tipologia di servizio di intermediazione è invece incentrata nel mettere in contatto direttamente gli interessati che hanno volontà nel rendere accessibili i propri dati (personali e non) con potenziali utenti di dati, agevolando l'esercizio dei diritti riconosciuti dal GDPR.

In tale circostanza il servizio di intermediazione è volto a tutelare e a rafforzare la posizione dell'interessato, assicurandogli un maggior controllo dei dati che lo riguardano. L'intermediario, infatti eroga il servizio di assistenza all'interessato non solo nel supportarlo ad esercitare i diritti a norma del GDPR, quali, ad esempio, la revoca del consenso al trattamento dei dati, la cancellazione, il diritto all'oblio o alla

portabilità, ma anche ad assicurargli che l'utente non tratti i suoi dati per scopi diversi o illeciti;

c) un'ultima tipologia di servizio di intermediazione è incentrata sui servizi di cooperative di dati.

I servizi di cooperative di dati sono definiti ai sensi dell'art. 2, n. 15, DGA come: «"servizi di cooperative di dati": servizi di intermediazione dei dati offerti da una struttura organizzativa costituita da interessati, imprese individuali o da PMI, che sono membri di tale struttura, avente come obiettivi principali quelli di aiutare i propri membri nell'esercizio dei loro diritti in relazione a determinati dati, anche per quanto riguarda il compiere scelte informate prima di acconsentire al trattamento dei dati, di procedere a uno scambio di opinioni sulle finalità e sulle condizioni del trattamento dei dati che rappresenterebbero al meglio gli interessi dei propri membri in relazione ai loro dati, o di negoziare i termini e le condizioni per il trattamento dei dati per conto dei membri prima di concedere l'autorizzazione al trattamento dei dati non personali o prima che essi diano il loro consenso al trattamento dei dati personali».

Anche in questo caso l'intermediario ha un importante obiettivo, quello di assistere l'interessato, le imprese individuali o le PMI che sono membri della stessa struttura organizzativa ad effettuare una scelta consapevole sull'utilizzo dei propri dati, trovando anche soluzioni comuni sulle modalità di impiego laddove vi siano posizioni contrastanti all'interno di uno stesso gruppo.

Senza dubbio il *Data Governance Act* delinea una figura di intermediario neutrale rispetto ai soggetti coinvolti e ha infatti un ruolo di mero facilitatore della condivisione dei dati, ma alla luce della distinzione sopra riportata si ritiene che tra le tipologie di servizio d'intermediazione analizzate la più idonea a valorizzare la condivisione e il riuso dei dati relativi alla salute nel mondo della ricerca sanitaria sia proprio l'organizzazione in cooperative di dati.

La prevalenza, in questo caso particolare, della finalità mutualistica, in base all'assunto per cui creando una struttura collettiva e di coordinamento volta a socializzare il valore dei dati, i singoli membri di essa ne ricaverebbero un guadagno non soltanto in termini monetari, ma anche e soprattutto sul piano del controllo sulle modalità di trattamento e utilizzo secondario dei dati, la fa preferire agli altri modelli [14]. Si ritornerebbe così all'assunto iniziale [15] che i dati relativi alla salute potrebbero essere utilizzati come bene comune per assicurare la salute pubblica alla collettività.

[14] Cfr. G. RESTA, *Pubblico, privato e collettivo nel sistema europeo di governo dei dati*, cit., p. 619.

[15] Cfr. *supra*, par. 1.

3. Cooperative di dati sanitari: primi casi di studio.

3.1. Il caso Savvy Cooperative.

Con stretto riferimento alle cooperative di dati applicate al comparto della salute, sono già emerse nella prassi dei casi di studio.

Savvy Cooperative è un portale di informazione per pazienti attraverso il racconto di altri pazienti. La piattaforma è nata dalla volontà di voler restituire centralità al paziente permettendogli di connettersi con professionisti del settore sanitario, in modo che possano collaborare per creare e implementare soluzioni orientate ad altri pazienti.

Se pur ci troviamo davanti ad un progetto molto innovativo si deve però constatare come questo non sia propriamente collegabile al *Data Governance Act* e al servizio cooperative di dati. Analizzando il sito web manca proprio quello che è lo spirito mutualistico dell'attività svolta prevalentemente a favore degli interessati (c.d. soci), trovandosi l'interessato davanti ad uno sfruttamento economico dei suoi dati senza così poter esercitare forme di controllo su di essi [16].

Infatti, come si può apprendere nella pagina di registrazione della piattaforma, l'interessato dopo essersi registrato e aver fornito alcune informazioni di base sul suo stato di salute, viene inviato a consultare la pagina dei questionari e/o dei *focus group* organizzati da aziende farmaceutiche e/o ricercatori che ad attività conclusa gli faranno avere 100 dollari e questo al fine di incentivare i propri membri esistenti a diffondere l'esperienza su Savvy e così a portare nuovi membri che possono fornire un'ulteriore esperienza unica e diversificata.

Questa esperienza progettuale si potrebbe classificare più come un'evoluzione, nel mondo del *web* 2.0, del già conosciuto forum a pagamento, se pur in questa circostanza regolato e alimentato da pazienti con i propri dati sanitari.

3.2. Il caso MIDATA Cooperativa.

MIDATA è una cooperativa di utilità pubblica (non profit) costituita ai sensi del Codice delle obbligazioni svizzero.

Al fine di meglio comprenderne se collegabile alla *mission* del *Data Governan-*

---

[16] Cfr. Lettera del Presidente del Garante per la protezione dei dati personali al Presidente dell'*European Data Protection Board* (EDPB), avente ad oggetto «Richiesta di parere in tema di commercializzazione dei dati personali e diritto alla portabilità», Garante per la protezione dei dati personali (doc web n. 9126725). Per un'analisi delle questioni giuridiche sulla commercializzazione dei dati personali: V. RICCIUTO*, La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in V. CUFFARO-R. D'ORAZIO-V. RICCIUTO (a cura di), *I dati personali nel diritto europe*o, Torino, 2019; F. BRAVO, *Il commercio elettronico dei dati personali,* in T. PASQUINO-A. RIZZO-M. TESCARO (a cura di), *Questioni attuali in tema di commercio elettronico*, Napoli, 2020, pp. 83-130.

ce Act è doveroso un approfondimento del punto n. 2 dello Statuto, rubricato "scopo". Più specificatamente si dice che la cooperativa mira, secondo un principio di utilità pubblica a:

«*a)* gestire una piattaforma IT sicura ("piattaforma MIDATA") atta alla memorizzazione, la gestione e la condivisione di dati personali di qualsiasi tipo, segnatamente dati sanitari e relativi alla formazione, nonché la fornitura di servizi ad essi correlati;

b) a mettere la piattaforma MIDATA a disposizione delle persone fisiche (membri e terzi) che partecipano alla piattaforma in qualità di titolari di un account dati ("titolare di account");

c) promuovere un'ampia partecipazione alla cooperativa da parte dei titolari di account e renderla loro possibile in qualità di membri della cooperativa, a tutelare gli interessi comuni;

d) promuovere l'autodeterminazione digitale della popolazione consentendo ai titolari di account di utilizzare i propri dati personali secondo le proprie esigenze in qualità di agenti autodeterminati, segnatamente per scopi di ricerca;

e) tutelare gli interessi comuni dei titolari di account utilizzando i loro dati personali, previo loro consenso, come risorsa comune. Ciò avviene permettendo ai titolari di account di accettare le richieste da parte di terzi di analisi dei loro dati personali e dando il loro consenso espresso ed informato a terzi per l'utilizzo secondario dei loro dati personali; ciò risulta in un ritorno economico per la cooperativa;

f) chiedere, con la piattaforma MIDATA, la creazione di un ecosistema innovativo nel quale i terzi possano offrire ai titolari di account servizi basati sui dati;

g) chiedere la realizzazione di progetti di ricerca in campo medico e ulteriori progetti per una società digitale equa e per l'autodeterminazione digitale della popolazione;

h) utilizzare i risultati scientifici ottenuti attraverso i dati personali da utilizzo secondario e le entrate risultanti nel quadro degli scopi summenzionati».

Ebbene, dalla lettura punto per punto si può ritenere che MIDATA sia a tutti gli effetti un servizio di cooperativa di dati come definito all'art. 2, n. 15, del Regolamento. È, infatti, una cooperativa non profit che gestisce in qualità di amministratrice una piattaforma per la raccolta e condivisione di dati, garantendo all'interessato la piena sovranità sui suoi dati e supportandolo ove richiesto da terzi nella condivisione.

Un aspetto molto interessante è che MIDATA si focalizza principalmente su dati relativi alla salute e con una particolare attenzione verso il consentire ai cittadini di condividerli liberamente nell'ambito di progetti di ricerca, in modo che possano giocare un ruolo attivo come "*Citizen scientists*" nella ricerca clinica.

Più nel dettaglio, la piattaforma è divisa in due macro-funzionalità: la parte legata alla registrazione dati, amministrazione dell'accesso e dell'autorizzazione, e la parte dall'impiego dei dati (applicazioni mobili), dando così origine a un ecosistema aperto prontato all'innovazione.

Gli utenti avranno a disposizione diversi servizi relativi alla gestione dei dati e potranno decidere a quali progetti di ricerca partecipare [17].

3.3. Il caso SALUS.COOP.

SALUS.COOP è una cooperativa di donatori di dati che ha come *mission* la ricerca come bene comune. Infatti, come sua filosofia ritiene che la ricerca consenta di generare informazioni che, una volta condivise e analizzate, diventano un elemento di valore per il processo decisionale e veicolo di trasformazione sociale.

Sul sito del progetto gli ideatori definiscono l'App che utilizzano per alimentare la *community*, una sorta di *crowdfunding* dove invece di dare soldi, si danno attraverso esplicito consenso i propri dati relativi alla salute. Dati utilizzati per supportare progetti di ricerca.

Un punto molto importante è che lo scambio dei dati, appartenendo alla categoria dei dati relativi alla salute e quindi con un grado di tutela relativa alla protezione dei dati personali rafforzato, avviene in modo sicuro: il donatore (c.d. interessato) ha il controllo, i suoi dati sono resi anonimi [18] e il ricercatore accede solo a quanto indicato nell'accordo di condivisione.

Dalle informazioni reperite sul sito del progetto anche SALUS.COOP, se pur una realtà sociale molto bene organizzata ed in grado di restituire valore sociale, non è classificabile come un servizio di cooperative di dati ma quanto piuttosto un servizio di intermediazione tra interessati che intendono mettere a disposizione gratuitamente i propri dati personali.

Infatti, la piattaforma è programmata per condividere dati relativi alla salute con gruppi di ricerca, in maniera anonima e nel rispetto di un'apposita licenza di condivisione dati nata nell'interazione con la cittadinanza attiva [19].

3.4. Il caso LunaDNA.

Tra i casi di studi è interessante accennare brevemente anche a LunaDNA, progetto focalizzato nel mediare la condivisione di dati genomici e relativi alla salute attraverso l'uso della *blockchain* e le criptovalute.

Nello specifico, LunaDNA è una piattaforma di proprietà per la ricerca sanitaria, attraverso la quale chiunque può condividere i dati sanitari e ricevere una quota di proprietà in criptovaluta. I ricercatori pagano per condurre ricerche utilizzando dati aggregati dalla piattaforma e tutti i profitti generati da questa ricerca vengono ridistribuiti agli azionisti che hanno condiviso i loro dati.

---

[17] Per lo schema dettaglio del *workflow* si veda: https://www.midata.coop/it/ricerca-partner/.

[18] Per lo schema dettaglio del processo di condivisione e di anonimizzazione si veda: https://www.salus.coop/app-de-salus-coop/#pseudoanonimat/.

[19] Per un approfondimento: https://www.salus.coop/wp-content/uploads/2023/03/CAT-Llicencia-CG.pdf.

Anche questo progetto più che rientrare nei servizi di cooperative di dati, rientra nell'intermediazione tra interessati e utenti, con la particolarità proprio dello sfruttamento economico della condivisione dei dati.

LunaDNA ha però chiuso la sua operatività il 31 gennaio 2024, dopo aver dichiarato che non aveva più liquidità economica per portare avanti il progetto.

4. I dati relativi alla salute e il *Data Governance Act*: un richiamo al GDPR.

I dati personali e più nello specifico i dati relativi alla salute sono divenuti negli ultimi anni, anche per via della pandemia da Covid-19, oggetto di una crescente attenzione da parte di operatori sanitari, ricercatori e società del mondo farmaceutico (c.d. *Big Farm*).

Tutto questo interesse ha portato le Autorità Garanti di tutti gli Stati membri ad alzare l'asticella dei controlli. Ma già da una lettura attenta del GDPR si può notare come questo, in riferimento ai dati relativi alla salute, stabilisca un generale divieto di trattamento, impedimento che non si applica però se i dati vengono utilizzati esclusivamente per: *a*) finalità connesse alla salute (finalità di cura); *b*) per motivi di interesse pubblico o finalità di governo; *c*) per la ricerca nel pubblico interesse (se effettuata in base a norme di legge o regolamento e previa valutazione di impatto). In tutti gli altri casi il trattamento di questa tipologia di dati necessita di una base giuridica forte, che spesso viene individuata nel consenso.

Proprio su questo aspetto potrebbe sorgere della tensione tra GDPR e il *Data Governance Act*. Infatti, si auspica che in caso di condivisione volontaria dei dati per finalità di ricerca sanitaria il *Data Governance Act* possa costituire una valida base giuridica per il trattamento dei dati, dal momento che l'altruismo degli interessati di donare i dati per finalità dell'interesse pubblico sia di per sé base giuridica espressa ed inequivocabile. Tuttavia, mancando nel testo della norma un'indicazione di natura sostanziale atta a circoscrivere la specificità del consenso esiste il forte timore che sia la condivisione che il riuso dei dati per finalità di ricerca debba ripassare da uno specifico consenso dell'interessato, trasformando l'altruismo dei dati in elemento privo di significato.

Un ulteriore elemento di tensione con il GDPR è l'opportunità data dal *Data Governance Act* agli intermediari di assicurare l'esercizio dei diritti degli interessati, ma questi per poter adempiere efficacemente ai compiti loro assegnati dovrebbero poter sostituirsi all'interessato. Purtroppo, il *considerando* n. 30 del DGA, dopo aver premesso che il ricorso a servizi di intermediazione potrebbe permettere di «rafforzare la capacità di agire degli interessati e, in particolare, il controllo dei singoli individui in merito ai dati che li riguardano», prospetta un mero ruolo di assistenza dando l'idea (nella vaghezza della terminologia giuridica) dell'assenza di autonomo potere decisionale in capo al fiduciario.

5. Conclusioni.

L'enorme flusso di dati relativi alla salute che quotidianamente le strutture sanitarie, pubbliche e private, producono sta trasformando e sempre più trasformerà il modo di accedere e condividere i dati sanitari. Questo sta accadendo anche alla luce dei continui impulsi del Legislatore europeo nel sostenere la creazione di spazi europei dei dati, da non ultimo con lo Spazio europeo dei dati sanitari [20] (c.d. *Health Data Space*).

Nel quadro di un continuo sviluppo la digitalizzazione e la condivisione dei dati sanitari permetterebbero proprio un approccio *data-driven* [21] da parte degli operatori sanitari e ricercatori, creando così non solo percorsi diagnostici e terapeutici più aderenti alle necessità dei pazienti – soprattutto per quelli cronici – ma anche conducendo nel minor tempo alla conclusione di progetti connessi allo studio delle patologie nonché alla ricerca e allo sviluppo di nuove cure farmacologiche.

In questo solco evolutivo e di valorizzazione sociale dei dati relativi alla salute non possiamo escludere il *Data Governance Act* che attraverso il suo quadro normativo e i suoi elementi strutturali può, a sua volta, spingere verso un riuso strutturato e consapevole tra più soggetti (persone fisiche e/o giuridiche) portatori d'interessi diffusi.

Ci si auspica però che in questo quadro complesso e stratificato di discipline che devono fare anche i conti con il sistema normativo delineato dal GDPR non ci siano letture anacronistiche, rappresentative di una visione superata, che pongano nel delicato campo della ricerca sanitaria forti ostacoli alla libera circolazione dei dati.

---

[20] COMMISSIONE EUROPEA, *Proposta di regolamento per istituire lo spazio europeo dei dati sanitari*, 3 maggio 2022, COM (2022) 197/2.

[21] Z. HOU-Z. WANG, *From model-based control to data-driven control: Survey, classification and perspective,* in *Information Sciences*, 2013, pp. 3-35; S.L. BRUNTON-J.N. KUTZ, *Data-Driven Science and Engineering: Machine Learning, Dynamical Systems, and Control*, Cambridge, 2017, pp. 414-416; V. BRESCHI-A. CHIUSO-S. FORMENTIN, *The role of regularization in data-driven predictive control*, in *arXiv preprint*, 2022.

Capitolo XXV

I servizi di cooperazione di dati nella ricerca clinica farmaceutica: analisi e prospettive

Alessandro De Vico

Abstract: In clinical pharmacological research, data is a fundamental richness; it generally expresses a health condition and the effects of a medicinal treatment on a pathology. Clearly, that data refers to a natural person, but its elaboration is such that it loses its original nature and becomes a scientific data, or rather a "research data". However, it is essential that the individual to whom that data element initially relates can be informed and, above all, not to be in the position of having to accept merely because the provision of the data is a condition for accessing to a clinical trial. Data intermediation services and services of data cooperatives fit precisely and primarily into this context, in which patients could find forms of mutualistic aggregation, even to be able to negotiate conditions or modalities of such conferral, this also in the perspective of a secondary use of the data itself. Associationism, as a phenomenon of particular interest to patients, could find in cooperatives a new participatory mode, finding convenience and greater protection against *big data*. Networks of researchers or research institutions, as defined by the Regulations (EU) No 536/2014 and Ethics Committees, could also find in cooperation a legitimate and qualified negotiating counterpart with which to interact.

1. Premessa.

Il Regolamento (UE) 2022/868 del 30 maggio 2022, relativo alla governance europea dei dati e che modifica il Regolamento (UE) 2018/1724 (di seguito chia-

mato *Data Governance Act*) si inserisce in una prospettiva di valorizzazione dei dati personali, o meglio dei dati in generale, e ciò trova anche una precisa collocazione nell'ambito delle attività di ricerca e sviluppo.

In particolare, il settore farmaceutico, soprattutto nell'ultimo decennio, ha visto l'intensificarsi delle relazioni tra industria farmaceutica, organizzazioni di ricerca e sviluppo e associazionismo.

I "servizi di cooperative di dati" e l'"altruismo dei dati", così come definiti e previsti nel *Data Governance Act*, potrebbero trovare un proprio ruolo applicativo proprio nel contesto delle complesse relazioni che riguardano gli stakeholders sopra menzionati.

In questa direzione, l'aspetto mutualistico, così come definito nel *Data Governance Act*, potrebbe indurre una trasformazione nel mondo della ricerca scientifica farmaceutica valorizzando l'associazionismo, o alcune forme di esso, verso la transizione nella cooperazione, in alcuni casi dando una maggior qualificazione e rappresentatività a fenomeni che cominciano solo appena ad affacciarsi.

Inoltre, i percorsi offerti dal *Data Governance Act*, potrebbero risolvere alcune problematiche ancora aperte e relative ai rapporti tra le organizzazioni che svolgono attività di ricerca ed i pazienti in merito all'utilizzo dei dati di quest'ultimi, anche molto dopo la conclusione di uno specifico programma di ricerca.

In particolare, le misure di semplificazione che mirano a rendere più agili le condizioni e le modalità di trattamento dei dati dei pazienti, potrebbero incontrare nel *mutualismo* e nella *cooperazione* proprio quell'elemento di equilibrio per fare in modo che determinate scelte da parte dei pazienti siano prese con maggior consapevolezza.

2. L'interesse verso il dato, il dato personale ed il dato di cura.

Il Codice in materia di protezione dei dati personali, così come modificato dal d.lgs. del 10 agosto 2018, n. 101, in adeguamento al Regolamento UE 2016/679/UE (di seguito chiamati rispettivamente "decreto legislativo" e "GDPR"), non contiene più alcun riferimento alla locuzione "identità personale" e la circostanza non è irrilevante o di poco conto. È stato già rilevato come intorno al concetto giuridico di identità personale si sia sviluppata importante giurisprudenza e dottrina che aveva condotto tale nozione ad inquadrarsi nel contesto dei diritti e delle libertà fondamentali [1]. Non vi è motivo di ritenere che, con il GDPR tale approdo sia stato smentito, anzi il fatto stesso che la regolamentazione si sia focalizzata sul dato, e non principalmente sulla identità, sta a significare che i due aspetti possono essere considerati distinti sebbene intrinsecamente connessi [2].

---

[1] G. FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo*, in G. FINOCCHIARO (a cura di) *Il nuovo regolamento europeo sul la privacy e sulla protezione dei dati personali*, Bologna, 2017.

[2] Sull'argomento si legga anche F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Milano, 2018, nel quale si evidenzia come il legislatore europeo abbia voluto favorire le istanze volte alla libertà di circolazione dei dati e l'integrazione del mercato.

Potremmo considerarli distinti in quanto singolarmente definibili, nei contorni e negli elementi che li caratterizzano, e intrinsecamente connessi in quanto il dato è pur sempre riferito a qualcosa o a qualcuno, ancorché questo qualcosa o qualcuno siano indentificati o identificabili, o il dato stesso non permetta la identificazione. Il percorso di ricostruzione del rapporto tra dato e persona, nell'ultimo ventennio si è sviluppato seguendo il processo di informatizzazione della società, sia sotto il profilo strettamente tecnologico, sia sotto il profilo economico [3]. Si è partiti con un approccio fenomenologico che, osservando il passaggio dalla identità personale alla identità digitale [4], ha concepito la identità personale come la sommatoria di singoli elementi informativi, tuttavia suscettibili di una diversa o, addirittura, autonoma (ri)composizione [5]; motivo per il quale è stato rilevato come la norma si limitasse a proteggere il frammento e non l'insieme [6].

Tuttavia, è proprio l'aspetto della scomposizione e ricomposizione del dato (o dei dati), secondo lo stato delle tecnologie a disposizione, ad aprire verso nuove considerazioni nel rapporto tra dato e identità personale.

Il dato di per sé non incontra l'interesse se non nella prospettiva di poter essere utilizzato per esprimere qualcosa. Se quindi il dato è diverso dall'informazione, quest'ultima diventa d'interesse nel momento in cui è in grado di conferire nella sua natura semantica, o meglio ancora nelle molteplici manifestazioni in cui quella stessa informazione può essere processata e/o apparire in maniera tale da significare qualcosa secondo l'uso che se ne vuole dare [7].

Le moderne tecnologie, da ultimo le varie forme di intelligenza artificiale, hanno assunto la capacità di analizzare ed elaborare il dato con un livello di combinazione e velocità tali che dati apparentemente insignificanti o "inutili" vengono messi in connessione tra loro per acquisire significati. Si tratta di attività solo astrattamente immaginabili dalla mente umana, che tuttavia sovrintende al disegno originario della elaborazione concettuale, che possono avere una notevole importanza secondo la finalità e l'uso che se ne vuole conferire [8].

Se da un lato il livello di complessità della tecnologia diventa determinante ai fini della elaborazione del dato per poterne trarne effetti significativi, dall'altro ap-

---

[3] G. RESTA, *Identità personale e identità digitale*, in *Dir. inf.*, 2007, p. 516 ss.

[4] G. MARINI, *La giuridificazione della persona idee e tecniche nei diritti della personalità*, in *Riv. dir. civ.*, 2006, p. 359 ss., a p. 387.

[5] Sul tema si veda C. IRTI, *Dato personale, dato anonimo e crisi del modello normativo dell'identità*, in *Jus civile*, 2020 ed in particolare la nota n. 19 laddove fa riferimento allo studio "*What are personal data*" dell'Università di Sheffield, lo studio è reperibile al seguente link: https://www.frareg.com/cms/wp-content/uploads/personal_data.pdf.

[6] G. FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo*, cit., nota 1.

[7] L. FLORIDI, *Philosophical Conceptions of Information*, in G. SOMMARUGA (ed. by), *Formal Theories of Information: From Shannon to Semantic Information Theory and General Concepts of Information*, Springer, 2009.

[8] *Ibidem*.

pare ugualmente importante il contesto nel quale tale elaborazione avviene per poter definire se il dato è in grado di comporre una realtà attribuibile ad una persona.

Si tratta di un aspetto già abbastanza approfondito in dottrina ed in giurisprudenza, con una tendenza da parte di quest'ultima ad interpretare in maniera estensiva il concetto di "identificabilità" laddove vi fossero elementi sufficienti a ricomporre il dato-informazione fino a delineare contorni idonei a identificare una persona[9]. Il processo è stato da sempre esaminato disattendendo ogni elemento utile a comprenderne l'aspetto intenzionale per cui, il semplice fatto – spesso teorico – che un processo potesse essere ripercorso a ritroso andando a scandagliare pezzi di informazione per (re)identificare un soggetto, persona fisica, ha decisamente orientato l'interprete verso la applicazione di misure a tutela dell'interessato.

Anche per tale motivo, tante fattispecie scaturenti da nuove analisi, spesso indotte dalla attività di monitoraggio o investigativa delle autorità preposte alla tutela dei dati personali, continuano a mantenere alto il rischio di non conformità per ogni attività imprenditoriale o istituzionale, nonostante gli sforzi compiuti per mantenere vivo e dimostrato il principio di *accountability*[10].

A tale quadro si somma il progresso costante delle potenze di calcolo che combinano e ricostituiscono dati fino a prima inidonei a qualsiasi caratterizzazione, andando ad aggiornare e rivoluzionare costantemente le tecniche e le forme di anonimizzazione o pseudoanonimizzazione.

C'è tuttavia un fenomeno, che spesso sfugge alle medesime autorità che sovrintendono alla tutela dei soggetti, probabilmente per una ancora inadeguato inquadramento positivo, e cioè la distinzione che si va realizzando tra il "*dato personale*" quale dato direttamente o indirettamente attribuibile alla identificazione della persona, anche nella sua natura strutturale (il cd. *dato particolare*) ed il "*dato astrattamente personale*" per il quale, pur sussistendo in linea teorica una qualche possibilità di attribuzione ad una persona fisica, tale possibilità non è mai nella direzione della identificabilità (della persona) in quanto il *dato astrattamente personale* è tale se ha perso la sua funzionalità originaria e ne ha acquisito una altra. In alcune situazioni, addirittura, quello che definiamo essere il dato "*astrattamente personale*" diventa tale solo nel momento in cui acquista una sua funzionalità, che non va verso la identificazione ma piuttosto verso una differente finalità.

---

[9] Si veda ad esempio l'evoluzione giurisprudenziale che ha caratterizzato l'idoneità di un indirizzo IP dinamico ad identificare una persona: Corte di Giustizia UE, II, causa C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland*, 19 ottobre 2016; Corte di Giustizia UE, causa C-70/10 *Scarlet Extended SA v. Société Belge des Auteurs, Compositeurs et Editeurs SCRL* (SABAM), 24 novembre 2011. Si legga anche: R. DUCATO, *La crisi della definizione di dato personale nell'era del web 3.0*, in F. CORTESE-M. TOSASI (a cura di), *Le definizioni nel diritto*, Torino, 2016, p. 165 ss., nonché A.M. GAMBINO-R. PETTI, Privacy *e proprietà intellettuale*, in E. TOSI (a cura di), Privacy *digitale*, Torino, 2019, p. 229 ss.

[10] Tale principio, infatti, nella sua novità concettuale richiede al titolare del trattamento di andare oltre il rispetto della norma, attraverso un approccio proattivo, sistematico e documentato per fare in modo che siano garantite tutte le misure praticabili il caso concreto.

Si tratta di una distinzione apparentemente solo astratta ma che trova ad esempio concreta applicazione, nel settore della ricerca clinica farmacologica, nella differenza tra "*dato di cura*" e "*dato di ricerca*" [11].

Il "*dato di ricerca*" è originariamente un "*dato di cura*" che ha perso la sua capacità diretta di identificazione della persona fisica, in quanto ha subito un processo di anonimizzazione, ma a differenza di un dato meramente anonimizzato, ha assunto una funzione propria che è quella di essere oggetto di ricerca fino ad acquisire una propria identità ontologica [12].

L'indipendenza del "*dato di ricerca*" è garantita da almeno tre elementi fondamentali: 1) ha una unica esclusiva finalità propria che è quella della ricerca scientifica, 2) la chiave di cifratura è in possesso di un unico soggetto (il medico curante) che può utilizzarlo solo per specifiche esigenze di cura del paziente (finalità diversa), 3) ha degli elementi informativi caratteristici, di natura prettamente medico scientifica, che lo rendono usabile solo a fini di ricerca.

La distinzione tra "*dato di cura*" e "*dato di ricerca*" rappresenta un dettaglio utile per definire le modalità di individuazione di possibili diverse basi giuridiche, idonee a legittimare l'uso ulteriore dei dati della ricerca scientifica, un aspetto molto attuale per una semplificazione delle procedure autorizzative ed una riduzione dei costi associati alla ricerca e sviluppo in ambito farmaceutico.

Ma è molto utile anche per approfondire la natura dei dati che entrano nel gioco valutativo della ricerca e, per dimostrare che forse è più importante concentrare gli sforzi interpretativi e tecnologici verso forme di elaborazione del dato, inizialmente personale, per fare in modo che diventi qualcosa di diverso ed utile per la stessa ricerca scientifica.

Ma, secondo il funzionamento dell'*input/output*, è nel processo di elaborazione anche concettuale e sociale, oltre che tecnologico, che si misura la sfida futura.

---

[11] Un accenno a tale distinzione è anche in: A. MIGONE DE AMICIS, *Scienza, Ricerca Clinica e Privacy: Rinnovate riflessioni*, in F. FRATTINI-F. MASSIMINO (a cura di), *I Dati il Futuro della Sanità*, EDRA e Fondazione Roche, 2022, sebbene non si spinga a teorizzare una funzione indipendente e propria del dato di cura.

[12] La anonimizzazione del dato è un processo ampiamente utilizzato nella ricerca clinica, e non solo per una maggiore *compliance* alla Data Privacy, in generale, ma soprattutto perché quello che interessa alla ricerca scientifica sono le informazioni utili alla ricerca stessa, ovviamente riferite ad una persona, intesa come soggetto umano, risultando del tutto indifferente o non rilevante chi effettivamente sia questa persona. Sul tema della anonimizzazione appare utile menzionare il fatto che le più recenti posizioni assunte dal Garante sul tema, qual è quella relativa il caso THIN (Provvedimento 1 giugno 2023, n. 226) non convincono molto, in quanto spostano l'elemento valutativo non già sulla verifica se il soggetto che riceve il dato disponga o meno dai dati necessari alla identificazione, quanto le vicende contrattuali che legano il soggetto deputato ad eseguire la procedura di anonimizzazione e quello che riceve i dati anonimizzati. Cosicché una eccessiva focalizzazione su quelle che potrebbero essere tutte le ipotetiche vicende afferenti al rapporto contrattuale, ivi compresa una eventuale interferenza proprio in occasione del contratto di committenza alla base del rapporto, finiscono per condizionare il percorso interpretativo.

Le forme di intermediazione e di cooperazione si pongono proprio nel centro di questo processo per fare in modo che, se l'informazione che "entra" è riferibile ad una persona fisica (non potrebbe essere diversamente) cosa ne "esce" è una informazione diversa, più utile dal punto di vista della ricerca scientifica, e – soprattutto – mirano a fare in modo che il processo elaborativo si svolga con la partecipazione attiva e sorvegliata proprio di coloro che si pongono come soggetti interessati.

3. Gli studi clinici sui medicinali e il GDPR: come i servizi di cooperazione potrebbero incrementare le garanzie dei soggetti interessati pur mantenendo il *favor* per la ricerca scientifica.

Per una analisi di quali sono le implicazioni della normativa sul trattamento dei dati personali in ambito farmaceutico non si può prescindere da una illustrazione, seppur sommaria, della regolamentazione di settore, peraltro principalmente di derivazione europea.

Il trattamento dei dati, anche personali, nel settore farmaceutico comprende tutte le attività e le fasi che concernono la ricerca, lo sviluppo, la commercializzazione, l'acquisto, la somministrazione e la farmacovigilanza di medicinali. Ognuna di queste attività e fasi ha una normativa di legge, regolamentare e deontologica propria e, a livello dogmatico, risponde ai principi della tutela della salute, della ricerca scientifica e dello sviluppo imprenditoriale, ivi inclusa la libera concorrenza tra imprese commerciali.

Con un'eccessiva schematizzazione possiamo affermare che le due principali attività, prima e dopo l'autorizzazione all'immissione in commercio di un medicinale, sono regolamentate rispettivamente da due norme di riferimento, il Regolamento (UE) n. 536/2014 del 16 aprile 2014 (di seguito chiamato "Regolamento CT") sulle sperimentazioni cliniche di medicinali ad uso umano e la Direttiva 2001/83 [13] riguardante i processi di autorizzazione, distribuzione, commercializzazione e farmacovigilanza.

Sebbene, appunto, tali normative non esauriscano la regolamentazione in materia, che è notevolmente complessa e variegata, è essenziale avere come riferimento criteri e principi in esse contenuti ai fini della individuazione delle possibili connessioni ed implicazioni con il GDPR ed *Data Governance Act*.

Nella fase precedente la autorizzazione all'immissione in commercio, possiamo suddividere la attività di studio sui medicinali ad uso umano in due macro ambiti:

[13] Vale la pena ricordare che, nel contesto italiano, il primo approfondimento sul tema del trattamento dei dati personali nelle sperimentazioni cliniche si è avuto con l'emanazione delle Linee Guida per i trattamenti di dati personali nell'ambito delle sperimentazioni cliniche di medicinali, emanate dal Garante il 24 luglio 2008. Dopo quel provvedimento non vi sono stati sostanziali aggiornamenti, ma decisioni ed orientamenti sono stati emanati nel corso degli anni senza un fondamentale scostamento dai principi contenuti nelle già menzionate Linee Guida.

la sperimentazione clinica, intesa quindi come studio interventistico, e lo studio clinico non interventistico [14]. La differenza tra le due tipologie sta nel fatto che la sperimentazione clinica, ossia lo studio clinico interventistico, deve soddisfare una delle seguenti condizioni: *a*) l'assegnazione del soggetto allo studio è decisa anticipatamente e non rientra nella normale pratica clinica; *b*) la decisione di prescrivere il medicinale sperimentale e la decisione di includere il soggetto nello studio clinico sono prese nello stesso momento, o sono applicate al soggetto procedure diagnostiche o di monitoraggio aggiuntive rispetto alla pratica clinica. Se l'indagine clinica non soddisfa i criteri sopra menzionati, si tratterà di uno studio clinico, quindi non interventistico in quanto si presume, ed è questo il requisito essenziale, che il medicinale sia studiato nella indicazione terapeutica autorizzata dall'autorità regolatoria europea o nazionale [15].

Oltre all'aspetto oggettivo, gli studi clinici sono caratterizzati dalla presenza di alcuni soggetti che svolgono a vario titolo molteplici attività, oltre chiaramente al soggetto che partecipa allo studio clinico, e segnatamente: il promotore e lo sperimentatore.

Il promotore è una persona, società, istituzione oppure organismo che si assume la responsabilità di avviare e gestire la sperimentazione clinica, curandone altresì il relativo finanziamento, lo sperimentatore è una persona responsabile della conduzione della sperimentazione clinica presso un sito di sperimentazione clinica. Queste due figure rappresentano i punti cardine sui cui già le Linee Guida del Garante del 2008 avevano individuato le responsabilità nella definizione di tutti gli aspetti relativi al trattamento dei dati personali, fino ad enucleare che, sotto la responsabilità del promotore, agiscono i soggetti preposti ad eseguire le cd. attività di monitoraggio del contesto dello studio clinico.

I processi che sottendono gli studi clinici sono quindi caratterizzati dalla elaborazione di una notevole quantità e qualità di dati personali e particolari, in quanto attinenti allo stato di salute, ed in questo ambito si colloca anche la pseudoanonimizzazione del dato, sia come misura essenziale di sicurezza, sia come processo che di fatto giustifica un interesse precipuo del titolare che è prettamente finalizzato al compimento dello studio clinico [16-17].

---

[14] Lo studio clinico non interventistico è possibile anche successivamente all'immissione in commercio di un medicinale, quando si vuole osservare l'uso del medicinale nella pratica clinica (es. gli studi di farmacovigilanza e gli studi di Fase IV).

[15] Per una descrizione più precisa ed esaustiva si legga l'art. 2 del Reg. UE n. 536 del 16 aprile 2014.

[16] Il processo di pseudoanonimizzazione del dato del paziente si realizza in particolare nel momento della raccolta ed elaborazione della c.d. *Case Report Form* (par 1.11 delle *Good Clinical Practice*) e nel momento del caricamento dei dati nel Portale UE di cui all'art. 81 del Regolamento n. 536/2014, nonché ancora nelle segnalazioni di farmacovigilanza, sebbene in quest'ultimo caso è anche possibile sostenere che non si tratti in senso proprio di pseudoanonimizzazione in quanto i dati contenuti in chiari potrebbero essere di per sé idonei alla identificazione del soggetto.

[17] Cfr. anche art. 56 del Reg. n. 536/2014 per il quale: «1. Tutte le informazioni sulla sperimenta-

Sebbene gli aspetti relativi alle attribuzioni di responsabilità, nonché alla idoneità delle tecniche di pseudoanonimizzazione siano state ampiamente discusse fino a seguire prassi abbastanza consolidate, nell'ultimo periodo si sono aperte ampie discussioni attorno al tema della utilizzabilità o ri-utilizzabilità dei dati raccolti nell'ambito degli studi clinici.

La questione non è nuova dal punto di vista dell'inquadramento giuridico e non emerge da un punto irrisolto, in quanto il GDPR è molto chiaro nel definire quelle che sono, sia le finalità lecite del trattamento sia le basi giuridiche affinché un trattamento lecito possa realizzarsi.

Nell'ambito degli studi clinici è stato rilevato che, sebbene i trattamenti correlati ad uno specifico protocollo di ricerca vadano intesi come un uso primario dei dati, non tutti i trattamenti relativi a tale "uso primario" dei dati di sperimentazione clinica perseguono gli stessi scopi e rientrano nella stessa base giuridica [18].

Posto che non deve essere fatta alcuna confusione tra il consenso informato alla partecipazione alla ricerca clinica ed il consenso quale base giuridica al trattamento dei dati personali e di salute, non può trascurarsi il fatto che nell'ambito della complessiva manifestazione di volontà del soggetto, come espressione della autodeterminazione libera ed incondizionata alla scelta, le due tipologie di consenso sono accomunate da una chiara situazione di squilibrio di potere tra il partecipante ed il promotore/sperimentatore.

Motivo per il quale incombe sul titolare del trattamento un onere valutativo particolarmente approfondito per valutare tutte le circostanze rilevanti, e non, prima di ricorrere al consenso dell'interessato; ma d'altra parte è noto che il consenso, quale base giuridica, è forse la modalità di elezione per consentire al soggetto di esprimersi in maniera compiuta, se preceduto da una adeguata informativa.

Tuttavia, nel processo di formazione a manifestazione della volontà, non può disconoscersi il fatto che tra le due tipologie di consenso sussiste una intrinseca connessione per la quale: *a*) non possono ammettersi distonie interpretative in sede informativa, *b*) è sempre presente il rischio di un condizionamento in capo al soggetto di acconsentire al consenso al trattamento dei dati quale logica conseguenza del consenso alla sperimentazione clinica. Ed in effetti il trattamento dei dati si configura come necessaria conseguenza della volontà di sottoporsi alla sperimentazione clinica.

---

zione clinica sono registrate, elaborate, gestite e conservate dal promotore o dallo sperimentatore, a seconda dei casi, in modo tale da poter essere comunicate, interpretate e verificate in modo preciso, tutelando al tempo stesso la riservatezza dei dati e i dati personali dei soggetti in conformità del diritto applicabile in materia di protezione dei dati personali. 2. Sono attuate idonee misure tecniche e organizzative per tutelare le informazioni e i dati personali trattati da rivelazione, diffusione, modifica non autorizzati o illeciti, o dalla distruzione o perdita accidentale, in particolare quando il trattamento comporta la trasmissione attraverso una rete telematica».

[18] Cfr. Parere n. 3/2019 relativo alle domande e risposte sull'interazione tra il regolamento sulla sperimentazione clinica e il regolamento generale sulla protezione dei dati (art. 70, par. 1, lett. *b*)) del 23 gennaio 2019.

L'ordinamento in materia, peraltro, prevede alcuni casi in cui, in deroga alle norme sul consenso informato alla sperimentazione clinica, è possibile acquisire la (conferma) della volontà del soggetto successivamente alla decisione di includere il soggetto nella sperimentazione clinica, purché siano soddisfatti tutti i determinati criteri elencati nell'art. 35 del Regolamento CT. Sebbene non espressamente indicato nel Regolamento sulle sperimentazioni cliniche, tale espressione *ex post* di volontà partecipativa, può essere esercitata anche per il consenso al trattamento dei dati personali e di salute, nei casi contemplati dal citato art. 35.

La questione del differimento del consenso pone tuttavia alcune problematiche, spesso di difficile risoluzione, per quanto concerne gli aspetti relativi al trattamento sanitario relativo alla sperimentazione clinica, ma anche con riferimento al trattamento dei dati sanitari. Sebbene si tratti di un aspetto particolare, limitato a casi specifici, indubbiamente si pone una questione, ad esempio, relativa alla utilizzabilità dei dati di salute nel caso in cui il soggetto, una volta in grado, revochi il consenso o, addirittura, in caso di decesso prima ancora che si possa esprimere.

Una recentissima modifica all'art. 110 del d.lgs. n. 196/2003 ha sostituito le parole «e deve essere sottoposto a preventiva consultazione del Garante ai sensi dell'articolo 36 del Regolamento» con le seguenti: «Nei casi di cui al presente comma, il Garante individua le garanzie da osservare ai sensi dell'articolo 106, comma 2, lettera d), del presente codice» [19]. È stata quindi, apparentemente, risolta la annosa questione per la quale se la acquisizione del consenso non fosse stata impossibile, per particolari ragioni, o avesse comportato uno sforzo sproporzionato o il rischio di un pregiudizio grave alla ricerca scientifica occorreva la preventiva consultazione del Garante[20]. Si tratta di una semplificazione nella direzione del principio di *accountability*, tuttavia, occorrerà osservarne la pratica realizzazione per capire se questa modifica comporterà un reale vantaggio alla ricerca scientifica pur mantenendo le garanzie per i pazienti (soggetti interessati).

La modifica normativa tuttavia, è indubbio, che si inserisce proprio in uno degli aspetti fondamentali sul rapporto tra due pilastri dommatici, e nel quale dovrebbe trovarsi il punto di equilibrio tra esigenze della ricerca scientifica e tutela dei dati personali degli interessati.

Il principio di *accountability* è tipico del Titolare, nel senso che è un'attribuzione che compete solo ad esso al fine di dimostrare di aver adottato ogni comportamento proattivo di concreta adozione di misure finalizzate ad assicurare l'applicazione del GDPR. Tuttavia, l'attuazione di tale principio non può prescindere da

---

[19] L. 29 aprile 2024, n. 56 (G.U. n. 100 del 30 aprile 2024) di conversione del d.l. 2 marzo 2024, n. 19, recante ulteriori disposizioni urenti per l'attuazione del Piano Nazionale di ripresa e resilienza (PNRR).

[20] A tal proposito si veda la Delibera 9 maggio 2024 del Garante, pubblicata sulla Gazzetta Ufficiale n. 130 del 5 giugno 2024 dal titolo «Regole deontologiche per trattamenti di dati personali a fini statistici e di ricerca scientifica, ai sensi degli articoli 2-*quater* e 106 del Codice (Provvedimento n. 298)».

una presa in considerazione della posizione dell'interessato al trattamento, esso involve tutto il processo di valutazione ed implementazione del trattamento. Ciò che prima era rappresentato, come strumento di garanzia, dalla consultazione col Garante ed ora è sostituito dalla osservanza di regole deontologiche [21], apre alla possibilità di una partecipazione più attiva dei soggetti il cui trattamento è maggiormente esposto alla pedissequa applicazione del principio di *accountability*, concretizzato nel rispetto appunto delle suddette regole deontologiche e di ogni altra misura valutativa che il Titolare vorrà espletare.

Il punto di equilibrio identificato da questa modifica normativa, sebbene semplifichi nella prospettiva di una maggior *favor* verso la ricerca scientifica, dall'altro dimentica e non preclude che nella contrapposta prospettiva del "soggetto interessato" possano trovarsi forme partecipative, che potremmo definire "a priori", per le quali l'insieme dei "soggetti interessati" possano trovare forme di cooperazione che andrebbero a rafforzare lo stesso punto equilibrio, realizzando forme nuove di una compartecipazione responsabilizzata.

La soluzione offerta dalla nuova formulazione della norma, che per certi versi potrebbe apparire *tranchant*, sembra voler dimenticare qualsiasi elemento essenziale dalla parte del soggetto interessato che possa essere suscettibile di una qualche diversa qualificazione. Nelle locuzioni «*particolari ragioni ... risulta impossibile ... sforzo sproporzionato .... rendere impossibile ... pregiudicare gravemente*» si celano realtà difficilmente definibili, ma prevedibili "a priori" se inquadrate in contesti aventi contorni predeterminati.

Si tratta di ipotesi di non identificabilità del soggetto interessato, per diverse ragioni, ma dall'altra parte non si può automaticamente escludere da ogni forma partecipativa il gruppo o l'organizzazione che astrattamente coincidono con quella categoria di soggetti non personalmente identificabile nel caso specifico.

In questo contesto, infatti, potrebbero inserirsi forme di partecipazione che, sotto forma della organizzazione mutualistica, andrebbero ad esercitare un ruolo suppletivo laddove le circostanze non danno luogo alla possibilità di una acquisizione del consenso da parte degli interessati, per diverse ragioni. In tal modo si andrebbe ad attuare proprio quella parte della *governance* definita *governance collettiva* sui dati conferiti dai singoli membri ed esercitata dalla struttura organizzata [22].

I primi due commi dell'art. 106 del d.lgs. n. 196/2003 diventano quindi determinanti e nella loro funzione sostanzialmente suppletiva, tipica della regolamentazione deontologica, rappresentano l'ambito nel quale diversi *stakeholders* possono aprire interlocuzioni, proponendosi come centro di interesse qualificati.

Le possibili problematiche sottese, ivi comprese le incertezze sostanziali, ad esempio sulla effettiva impossibilità a contattare i soggetti interessati, potrebbero

---

[21] Anche attraverso lo svolgimento di un *Data Protection Impact Assessment*, ai sensi dell'art. 35 del GDPR.

[22] F. BRAVO, *Le Cooperative di dati*, in *Contratto e impresa*, 2023, 3, p. 757 ss. e sul sito del Progetto di Terza Missione sulle Cooperative di dati, *Project Version*, p. 6.

essere superate attraverso il ricorso a servizi di intermediazione dei dati, ovvero ai servizi di cooperative di dati.

Se la nuova formulazione dell'art. 110 semplifica e favorisce la ricerca scientifica, rimane immodificata la formulazione del successivo art. 110-*bis* che concerne sempre il trattamento di dati personali a fini di ricerca scientifica o a fini statistici, ma con finalità ulteriore rispetto ad una precedentemente svolta legittimamente. Il trattamento ulteriore, o secondario, laddove per le medesime ragioni di cui all'art. 110 non fosse possibile chiedere il consenso dell'interessato è soggetto ad autorizzazione del Garante ed a condizione che *siano adottate misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, in conformità all'articolo 89 del Regolamento, comprese forme preventive di minimizzazione e di anonimizzazione dei dati*.

La portata dei due articoli, nonostante i tentativi interpretativi, appare ancora di dubbio inquadramento; sembrerebbe che l'art. 110-*bis* faccia più generico riferimento alla "*ricerca scientifica*" anziché alla "*ricerca medica, biomedica ed epidemiologica*" ma a questo punto, stando il rapporto di *genus* a *species* non si comprenderebbe la numerazione consequenziale degli articoli, che avrebbe dovuto essere invertita.

Il trattamento ulteriore, o secondario, secondo la *ratio* del GDPR è comunque un nuovo trattamento se non già coperto dal precedente, ma avrebbe una sua logica invece dal punto di vista della ricerca scientifica, in tutte le sue branche e declinazioni, essendo essa caratterizzata da una alea di imprevedibilità nei risultati e nei percorsi.

La conferma che l'art. 110-*bis* riguardi la ricerca scientifica nella sua totalità sembra confermata dal co. 4 del medesimo articolo ove si afferma che «non costituisce trattamento ulteriore da parte di terzi il trattamento dei dati personali raccolti per l'attività clinica, a fini di ricerca, da parte degli Istituti di ricovero e cura a carattere scientifico, pubblici e privati, in ragione del carattere strumentale dell'attività di assistenza sanitaria svolta dai predetti istituti rispetto alla ricerca, nell'osservanza di quanto previsto dall'articolo 89 del Regolamento».

Ma se da un lato il legislatore conferma una certa preferenza per la ricerca scientifica condotta da enti che abbiano una rilevanza pubblica, dall'altra per le ricerche condotte e/o finanziate da enti privati, sarà molto più verosimile ricadere nella fattispecie di cui all'art. 110 anziché nell'art. 110-*bis*[23].

---

[23] Si veda ad esempio il Parere del Garante n. 140 del 20 giugno 2019 dal titolo «*Parere in ordine al trattamento dei dati personali, anche inerenti a particolari categorie di dati, per finalità di ricerca medica, biomedica e epidemiologica, riferiti alla coorte di pazienti arruolati nello studio "MATTERHORN" – 20 giugno 2019* [9123447]» nonché il Parere del Garante n. 95 del 22 febbraio 2024 sullo studio clinico dal titolo «*Analisi retrospettiva di pazienti con carcinoma a cellule renali metastatico trattati con CABOzantinib: una firma GENomica per descrivere la risposta di lunga durata (CABOGEN)*». Si è trattato di casi sostanzialmente simili in quanto trattavasi di studi clinici osservazionali retrospettivi su campioni di tessuto di pazienti affetti da determinate patologie, alcuni dei quali deceduti, conservati presso strutture sanitarie pubbliche e private.

In fattispecie simili non v'è dubbio che l'aspetto mutualistico, così come emerge nella definizione di «*servizi di cooperazione di dati*» nonché di «altruismo *dei dati*» possano trovare uno spazio applicativo in modalità diversa a seconda delle situazioni e degli obiettivi.

Uno degli ambiti applicativi possibili e forse anche più aderenti alle necessità specifiche è il modello cooperativo *Third Party*[24] che, facendo leva su una struttura funzionale tradizionale, prevede che i dati collazionati all'interno della cooperativa, in base alla autorizzazione o al consenso rilasciato dai singoli soci ai cui i dati sono riferibili, attribuiscono alla cooperativa il compito di definire condizioni e modalità di un riuso dei dati; tutto questo nell'ambito di una attività ancora più complessa che prevede una analisi strutturata dei trattamenti interessati dalla attività con specifico riferimento alla patologia trattata, la disponibilità di cura ed i possibili sviluppi terapeutici futuri.

Appare importante, inoltre, ricordare che sussiste una sostanziale interconnessione tra il consenso alla sperimentazione clinica ed il consenso al trattamento dei dati, soprattutto nel caso in cui l'adesione al trattamento clinico sperimentale è una vitale opportunità terapeutica per il paziente. In questi casi, come già delineato, c'è il rischio evidente che la manifestazione di volontà del soggetto con riferimento al trattamento dei dati di salute assuma una posizione di subordine rispetto alla primaria esigenza di tutelare la propria salute[25]. Certamente poi non si dovrebbe sconfinare nella condizione per la quale, *condicio sine qua non* per la partecipazione alla sperimentazione clinica, sia il conferimento del consenso al trattamento dei dati di salute, ciò – ovviamente – nelle parti della informativa e consenso in cui il trattamento dei dati è essenziale ai fini della sperimentazione clinica.

Sul punto, l'art. 7, par. 4, del GDPR è molto chiaro nell'affermare che giammai la esecuzione di un contratto e la prestazione di un servizio può condizionare la libera espressione del consenso al trattamento dei dati[26].

Un ulteriore aspetto che dovrebbe essere considerato nell'esaminare quelli che sono i tratti caratteristici del trattamento dei dati personali nella sperimentazione clinica è che, i rapporti sottesi, non possono spiegarsi mediante il solo ricorso allo schema tipico dei rapporti obbligatori, o meglio la struttura obbligatorio-contrat-

---

[24] Secondo lo schema indicato in F. BRAVO, *Le cooperative di dati*, cit., p. 12.

[25] Siamo comunque in contesto di liceità del trattamento e la situazione dimostra emblematicamente che la liceità non basta ma è importante la manifestazione del consenso.

[26] Peraltro il *considerando* n. 43 del GDPR afferma che «per assicurare la libertà di espressione del consenso, è opportuno che il consenso non costituisca un valido presupposto per il trattamento dei dati personali in un caso specifico, qualora esista un evidente squilibrio tra l'interessato e il titolare del trattamento, specie quando il titolare del trattamento è un'autorità pubblica e ciò rende pertanto improbabile che il consenso sia stato espresso liberamente in tutte le circostanze di tale situazione specifica. Si presume che il consenso non sia stato liberamente espresso se non è possibile esprimere un consenso separato a distinti trattamenti di dati personali, nonostante sia appropriato nel singolo caso, o se l'esecuzione di un contratto, compresa la prestazione di un servizio, è subordinata al consenso sebbene esso non sia necessario per tale esecuzione».

tuale che lega lo sponsor allo sperimentatore (o alla istituzione a cui appartiene lo sperimentatore) non esaurisce ogni aspetto della sperimentazione clinica. Questo perché tale attività si inserisce nel contesto personalissimo della tutela della salute, con la declinazione essenziale che tale tutela si attua attraverso il sottoporsi a trattamenti terapeutici che, in quanto sperimentali, non possono dare garanzie di successo o assenza di rischi per la salute; molto spesso poi tali trattamenti si inseriscono nel contesto di un regime di ricovero e cura più ampio erogato dai servizi sanitari in un regime di assistenza pubblica.

Gli aspetti intorno ai quali potrebbe senz'altro concretizzarsi l'aspetto mutualistico e di soccorso ai soci della cooperativa sono pertanto diversi, e tra questi non possono tralasciarsi le vicende che interessano il consenso alla sperimentazione ed il consenso al trattamento dei dati personali durante tutto il periodo nel quale il soggetto interessato rimane nel trattamento terapeutico sperimentale. Tra questi l'istituto della revoca del consenso, quale ipotesi che si pone in diretta connessione col diritto alla libera autodeterminazione del soggetto, e per il quale sia il Regolamento CT sia il GDPR dedicano una specifica disciplina. Il tema concerne la sorte dei dati (scientifici) raccolti dopo la revoca del consenso, in maniera tale che si contemperi la tutela del soggetto e dei suoi dati con le necessità della ricerca scientifica. Già l'EDPB, nel *Parere n. 3 relativo alle domande e risposte sull'interazione tra il Regolamento sulla sperimentazione clinica e il regolamento generale sulla protezione dei dati (articolo 70, paragrafo 1, lettera b)) del 23 gennaio 2019*, limitava la possibilità di un uso dei dati di salute, successivamente alla revoca del consenso, solo ai trattamenti che si fondano su altre basi giuridiche e, segnatamente gli obblighi a cui il promotore e lo sperimentatore sono sottoposti per via di disposizioni di legge, quali quelle in materia di sicurezza. Con la conseguenza che i soli dati utilizzabili sono quelli connessi alla farmacovigilanza mentre rimarrebbe incerto se per "materia di sicurezza" possano intendersi anche quelli utili per tutelare la salute del soggetto, a distanza di tempo.

Se da un lato quindi, una adeguata e quanto più possibile stratificazione e granularità descrittiva nella Informativa e Consenso consentirebbe al soggetto di scegliere con maggior consapevolezza ed ampiezza, dall'altro l'utilizzabilità dei dati per finalità di ricerca, in caso di recesso dal consenso, verrebbe inficiata per dare spazio, appunto, alla tutela del dato personale.

In questo ambito senz'altro si inserisce la riforma dell'art. 110 del Decreto Legislativo ed in questo ambito potrebbero trovare spazio forme di cooperazione finalizzata anche all'altruismo dei dati così come definite nel *Data Governance Act*.

4. Una diversa prospettiva: dall'associazionismo alla cooperazione.

Il livello di partecipazione attiva da parte dei cittadini alla vita sociale, intesa nella sua accezione più generale, è senz'altro aumentato. Le moderne tecnologie informatiche e comunicative hanno ampliato la possibilità comunicativa ed espres-

siva, ridotto o addirittura abbattuto ogni barriera geografica e dotato i cittadini di strumenti partecipativi, fino ad assumere un ruolo in prima persona nelle problematiche indotte dalle sfide del nostro tempo. Le complessità della società post-moderna, per certi versi amplificate proprio dalle medesime tecnologie informatiche e comunicative, hanno fatto emergere una impossibilità delle istituzioni classiche a far fronte ai bisogni dei cittadini, spesso anche solo per motivi di scarsità di risorse economiche, nonché una sostanziale inadeguatezza ad anticipare le necessità, ciò anche per motivi strutturali e culturali.

Nell'ambito della tutela della salute, sebbene si tratti di un principio e compito di primaria importanza e funzionalità sotto il profilo pubblico, sono emerse le figure del *caregiver* [27] e del *paziente esperto* [28], quale risposta "istituzionale" a ruoli che di fatto esprimono la necessità del cittadino, nelle sue diverse condizioni di condizioni di vita e di salute, a farsi carico delle lacune e delle incompetenze delle istituzioni pubbliche.

La sensibilità del legislatore si è spinta fino ad approvare il cd. "Codice del Terzo Settore" [29] che, prevedendo proprio le imprese sociali, incluse le cooperative sociali, come enti che possono dotarsi di finalità dirette «a perseguire il bene comune, ad elevare i livelli di cittadinanza attiva, di coesione e protezione sociale, favorendo la partecipazione, l'inclusione e il pieno sviluppo della persona, a valorizzare il potenziale di crescita e di occupazione lavorativa», stabilisce che queste possono svolgere attività aventi ad oggetto la «ricerca scientifica di particolare interesse sociale».

L'approfondimento che si è sviluppato attorno al concetto di «particolare interesse sociale» sembra essere, ancora una volta, ancorato alla classica contrapposizione dialogica tra generale e particolare, a cui si continua a far corrispondere l'opposizione tra pubblico e privato. In altri termini il concetto di interesse sociale rimarrebbe, legittimamente, perseguibile solo attraverso l'esercizio di pubblici poteri.

Il fatto è che nell'ambito della ricerca scientifica farmacologica, la distinzione tra

---

[27] Ai sensi dell'art. 1, co. 255, delle l. 27 dicembre 2017, n. 205 «si definisce caregiver familiare la persona che assiste e si prende cura del coniuge, dell'altra parte dell'unione civile tra persone dello stesso sesso o del convivente di fatto ai sensi della legge 20 maggio 2016, n. 76, di un familiare o di un affine entro il secondo grado, ovvero, nei soli casi indicati dall'articolo 33, comma 3, della legge 5 febbraio 1992, n. 104, di un familiare entro il terzo grado che, a causa di malattia, infermità o disabilità, anche croniche o degenerative, non sia autosufficiente e in grado di prendersi cura di sé, sia riconosciuto invalido in quanto bisognoso di assistenza globale e continua di lunga durata ai sensi dell'articolo 3, comma 3, della legge 5 febbraio 1992, n. 104, o sia titolare di indennità di accompagnamento ai sensi della legge 11 febbraio 1980, n. 18».

[28] Sebbene non esista ancora una definizione giuridica di «*paziente esperto*» è possibile adottare la nozione che ne dà il Codice Deontologico di Farmindustria, ossia il paziente «che, oltre ad avere conoscenza diretta della patologia, sono dotati di specifica competenza ed esperienza in aspetti connessi alla ricerca e sviluppo dei farmaci, alle attività regolatorie o in attività di advocacy intesa quale capacità di promuovere e supportare le cause e le necessità di una pluralità di pazienti»; si veda sul punto anche la associazione Accademia del Paziente Esperto, EUPATI.

[29] D.lgs. 3 luglio 2017, n. 117.

una attività che abbia una finalità sociale, ossia generale, ed una che abbia finalità particolare, o privata, non sempre appare riflettere la realtà degli obiettivi e dei bisogni a cui la stessa ricerca scientifica e farmacologica vorrebbe dare una risposta.

Per quanto concerne il concetto di ricerca scientifica di particolare interesse sociale è stato fatto riferimento al d.p.r. n. 135/2003 riferito alle ONLUS per cui sono state elencate tutta una serie di attività, tra le quali la più generale «prevenzione diagnosi e cura di tutte le patologie dell'essere umano» purché (ed è questo l'elemento sostanziale) si tratti di attività non commerciali. Precisando inoltre, con ciò confermando, il requisito della finalità non commerciale, che deve «intendersi riferita allo sviluppo più che alla produzione di farmaci ad uso umano o veterinario» [30]. Appare evidente che una simile considerazione parte dal presupposto che la fase di sviluppo possa idealmente attribuirsi ad una finalità sociale, di ricerca e sviluppo e tutela della salute, piuttosto che ad un obiettivo commerciale mentre, al contrario, la produzione viene intesa come attività diretta alla commercializzazione e quindi soggetta alle logiche dei ricavi e dei profitti.

Si tratta di un presupposto che convince poco e, probabilmente, rischia di non riflettere una realtà dinamica e complessa che vede lo stanziamento di notevoli risorse economiche per sostenere gli sforzi della ricerca, ed inoltre la necessità, ovvero opportunità, di instaurare accordi e collaborazioni tra diversi stakeholders (imprese, università, centri di ricerca, strutture sanitarie, medici e scienziati, etc.) per poter avanzare e raggiungere risultati apprezzabili ed utili per la collettività.

In questo contesto il *Data Governance Act* sembra aprire alla possibilità per gli enti pubblici di concedere a terzi una serie di dati, così come indentificati all'art. 3, par. 1, stabilendo le condizioni e modalità anche per un loro riutilizzo da parte di soggetti terzi. Indubbiamente, nelle categorie di dati sopra definiti, rientrano anche quelli derivanti sia dalla pratica della assistenza sanitaria (si pensi ad esempio ai dati contenuti nei Registri per patologia), utili per la ricerca scientifica, sia quelli derivanti dalla ricerca scientifica da essi svolta.

Se da un lato si qualifica la posizione delle strutture sanitarie pubbliche nel catalogare ed elaborare dati molto utili ai fini di ricerca scientifica, prevedendone la possibilità di una condivisione ampia con soggetti terzi, dall'altra appare ancora più importante che il soggetto interessato riceva dal titolare primo, una adeguata informazione sulle modalità e finalità del trattamento, ciò a prescindere dalla base giuridica identificata.

In questo ambito potrebbero giocare un ruolo importante proprio i servizi di cooperative di dati, rappresentando la modalità organizzativa funzionalizzata a dare supporto alle posizioni giuridiche dei soggetti coinvolti nei trattamenti dei dati, sottesi ai processi della ricerca scientifica, costituendo inoltre un elemento di (ri)equilibrio nella dialettica dei rapporti tra figure contemplate nel GDPR e nella normativa di settore.

---

[30] Parere sui concetti di interesse sociale e di particolare interesse sociale di cui all'art. 5 del d.lgs. n. 117/2017 (Testo approvato dal Consiglio nazionale del Terzo settore nella seduta del 5 luglio 2022), Ministero del Lavoro e delle Politiche Sociali.

Le cooperative di dati sembrerebbero avere un primo obiettivo che è quello di rafforzare la posizione dei singoli individui nel maturare scelte informate. Ciò potrebbe concretizzarsi anche attraverso una modalità per certi versi "invertita", ossia influenzando i termini e le condizioni a cui l'uso dei dati sarebbe subordinato. La tutela dell'interesse dei singoli soci della cooperativa, avendo riguardo proprio a ciascuna posizione individuale del soggetto, vedrebbe la propria, maggior tutela proprio nella determinazione a priori delle condizioni alle quali un consenso potrebbe essere esercitato.

In effetti la cooperazione viene inquadrata nell'ambito del servizio di condivisione dei dati come strumento di ausilio alle persone fisiche, imprese individuali, microimprese o piccole e medie imprese, interessate nella fase di negoziazione dei termini e delle condizioni per il trattamento dei dati.

In sostanza quello che emerge è una propensione da parte del legislatore ad incentivare l'aspetto mutualistico sotteso alla cooperazione, più che dare precise indicazioni in merito ad una, eventuale, struttura societaria da adottare, per consentire ad un insieme di soggetti o imprese, di fare leva sulla rappresentatività ai fini di una migliore definizione di strumenti negoziali, quale appunto le condizioni contenute nel consenso al trattamento dei dati.

Tanto è vero che il *Data Governance Act* fa riferimento a «*servizi di cooperazione di dati*», come se dal punto di vista oggettivo fosse necessaria la presenza di una messa in condivisione (dei dati), quale elemento costitutivo della cooperazione, per poterne ricevere poi il vantaggio di un maggior o particolare potere negoziale nel trattamento dei dati.

L'aspetto non è di poca rilevanza dal punto di vista fenomenico, in quanto si andrebbe ad inserire, quale punto di forza, in alcuni contesti nei quali i trattamenti dei dati sono di fatto indirizzati da politiche dettate da *Big Data*, ponendosi quindi nella direzione di poter ottenere una posizione di auspicato equilibrio. Il principio è semplicemente applicabile anche al settore farmaceutico, un ambito nel quale i dati stanno assumendo una notevole importanza, anche per la studio e lo sviluppo di terapie geniche e della medicina personalizzata.

Si pensi, ad esempio, proprio a casi di studi osservazionali diretti a verificare l'espressione genetica su tessuti umani, conservati presso strutture di ricerca e precedentemente prelevati per scopi di cura, comunque diversi da quello della verifica genetica; si tratta di studi *ex post* che si avviano non appena le condizioni del progresso scientifico si verificano.

Ecco quindi che, se da un lato un numero ridotto di imprese tecnologiche detiene buona parte dei dati disponibili a livello mondiale, gruppi di pazienti potrebbero raccogliere e conservare dati relativi alla patologia e diventare essi stessi centri di elaborazione, proponendosi attivamente nel contesto delle dinamiche che contraddistinguono lo scambio di dati.

Si pensi, ancora, ad esempio alle cd. malattie rare, per le quali l'incidenza a livello sociale è bassissima ed il bisogno di cure o nuovi approcci terapeutici è altissimo, ovvero ad alcune forme di neoplasie per le quali l'espressione genetica è un

fattore di rischio notevole, o ancora a malattie per le quali, al momento, non esistono delle cure.

Ma, con tutti i *caveat* derivanti dal rischio, non irrilevante, di una sorta di *dual governance* [31], per la quale alla governance collettiva si andrebbe ad accompagnare quella individuale, in quanto il singolo soggetto sarebbe comunque "*interessato al trattamento*", la messa a disposizione di dati e la definizione di politiche comuni e condivise per il loro utilizzo, andrebbe di fatto a rafforzare notevolmente posizioni giuridiche soggettive che altrimenti non si riuscirebbero ad esercitare. Da un lato, quindi, il rafforzamento negoziale delle posizioni giuridiche soggettive, dall'altro una maggior attività informativa interna alla organizzazione; ciò in quanto, l'organizzazione potrebbe capitalizzare al suo interno, conoscenze che altrimenti sarebbero difficili da collettare a livello di singolo soggetto, proponendosi inoltre come momento di approfondimento e proposizione di forme nuove ed innovative di collaborazione.

I servizi di intermediazione di dati possono essere svolti anche da una cooperativa di dati intesa come struttura organizzata, costituita da soggetti interessati, che abbia come obiettivo principale quello di aiutare i propri membri nell'esercizio dei propri diritti in relazione a determinati dati. L'esercizio dei propri diritti si attua mediante scelte informate, precedute da chiara ed esaustiva spiegazione delle implicazioni legate alle diverse scelte, forza negoziale nei termini e nelle condizioni per il trattamento dei dati dei propri membri.

Il fenomeno dell'associazionismo dei cittadini aventi un comune interesse su una o un gruppo di patologie è abbastanza vasto e variegato, esse mirano perlopiù a favorire la consapevolezza e la capacità di autodeterminazione del paziente, punto di forza indispensabile per le malattie rare; offrono un bagaglio di conoscenza diverso e complementare a quello medico e/o istituzionale, stimolando ricerche, azioni ed interventi socio-sanitari [32].

Il loro coinvolgimento a livello istituzionale è ormai inquadrato, sebbene in una forma meramente partecipativa, peraltro già contemplata in linea programmatica dalla c.d. Riforma Bis della Sanità, laddove all'art. 14 del d.lgs. n. 502/1992 poi meglio dall'art. 12 del d.lgs. 19 giugno 1999, n. 229, prevede che le Regioni promuovano «consultazioni con i cittadini e le loro organizzazioni anche sindacali ed in particolare con gli organismi di volontariato e di tutela dei diritti al fine di fornire e raccogliere informazioni sull'organizzazione dei servizi».

Una forma partecipativa che si è andata rafforzando nel tempo, soprattutto nell'ambito di alcuni settori di cura particolarmente delicati e bisognosi di assistenza compartecipativa, qual è quello dell'oncologia.

Quello che emerge nel Documento tecnico di indirizzo per ridurre il carico di

---

[31] Si veda a proposito, F. BRAVO, *Le cooperative di dati*, cit., p. 6.

[32] T. PETRANGOLINI-F. MORANDI-L. DELLE MONACHE-M. MORO-E. DI BRINO-A. CICCHETTI (a cura di), *La storia delle associazioni dei pazienti e dei cittadini impegnate in sanità in Italia: conquiste, ostacoli e trasformazioni*, marzo 2021, ALTEMS Università Cattolica del Sacro Cuore.

malattia del Cancro per il 2023-2027 (cosiddetto Piano Oncologico Nazionale), adottato con Intesa in Conferenza Stato-Regioni del 17 aprile 2019, è che deve essere rafforzato il ruolo del volontariato e dell'associazionismo in campo oncologico, componenti formalmente riconosciute, prevedendone la partecipazione ai livelli rappresentativi e direzionali, così come alle funzioni di integrazione e/o completamento dell'offerta istituzionale.

In questa direzione anche alcune recenti esperienze regionali quali la Deliberazione della Giunta Regionale del Lazio del 15 ottobre 2019, n. 736 (c.d. Participation Act), che ha approvato il documento dal titolo «Ruolo e strumenti di partecipazione delle organizzazioni dei cittadini nella programmazione e valutazione dei servizi sanitari regionali».

Con tale deliberazione la Regione intende attuare il coinvolgimento delle organizzazioni di tutela dei pazienti e dei loro familiari nella definizione, nel monitoraggio e nel miglioramento delle politiche regionali in materia sanitaria [33]. Una certa rilevanza, nel documento sviluppato dalla Regione, è il requisito che deve avere una associazione/organizzazione di pazienti affinché possa accedere ed esercitare la propria rappresentatività, ossia il fatto che l'organo assembleare debba essere partecipato in maggioranza da pazienti e *caregiver*, risultando del tutto ininfluente ai fini della qualificazione il fatto che, invece, l'organo direttivo sia composto, anche nella sua totalità, da soggetti che non abbiano alcuna esperienza diretta della malattia.

Il fenomeno consistente nella attività sociale dei cittadini, nelle loro diverse situazioni (professionali, geografiche, espressione di pensiero, condizioni sociali e di salute, etc.) è abbastanza variegato, e questa disomogenea manifestazione fenomenologica comporta non facili tentativi di classificare ed inquadrare queste situazioni.

La questione si complica nel momento in cui queste organizzazioni, che nella maggior parte dei casi assumono la veste giuridica delle Associazioni (di rado anche quella di Fondazioni), non si limitano solo a svolgere attività di supporto ai propri associati, anche e soprattutto attraverso forme di volontariato, ma esercitano attività di sensibilizzazione sociale molto attiva, a tal punto che esse stesse si pongono come centri di imputazione di interessi particolari (in quanto finalizzati ad una specifica patologia o area terapeutica). Non è un caso che per la complessità e vastità di relazione che svolgono, esercitano attività di *lobbying*, ponendosi come canale di contatto tra gli associati, le istituzioni e gli altri *stakeholders* di riferimento.

---

[33] In particolare, si tratta di una convocazione, almeno una volta all'anno, di un'assemblea delle Organizzazioni, che costituisce la sede per un confronto con le organizzazioni stesse. Il modello di partecipazione prevede inoltre l'istituzione da parte della Direzione regionale Salute e Integrazione Sociosanitaria di una Cabina di Regia per i rapporti con le Organizzazioni di tutela dei pazienti e dei loro familiari, presieduta dall'Assessore regionale alla Sanità o da un suo delegato, che svolge una funzione di ascolto, di interlocuzione e promozione di proposte e consultazione attiva, definendo i criteri di priorità per l'esame delle richieste formulate dalle Organizzazioni e le modalità per dare attuazione alla richieste accolte e assicura il monitoraggio dell'attuazione delle decisioni assunte.

Se, in generale, la legislazione del Terzo Settore si basa sul pluralismo identitario, dall'altro diventa essenziale che i soggetti che appartengono ad una medesima organizzazione, si sentano accomunati da una fondamentale identità di appartenenza. Tuttavia, l'appartenenza non è mai «mera appartenenza», nel senso che anche le associazioni devono avere uno scopo, ma ciò che accomuna gli associati è solo il fatto di avere una comunanza di interessi, spesso – appunto – dettata da una condizione comune (i.e. di vita, professionale, di salute).

Ma, quando il fattor comune dell'agire degli associati si ferma ai soli mezzi, si rimane nell'ambito della concertazione, del coordinamento, del confronto e del discutere, ma quando tale fattore si sposta in avanti verso i fini, ossia lo scopo dell'essere comune, ecco che la questione diventa come realizzare la cooperazione [34]. In questa situazione, ciascun soggetto che partecipa alla organizzazione assume come rilevante la posizione dell'altro, facendo affidamento su una situazione di reciprocità, in questo ambito si parla appunto di *mutual responsiveness* [35].

5. Le reti di ricercatori, gli studi clinici di medicinali senza scopo di lucro e gli ambiti di applicazione dei «servizi di cooperazione di dati».

Il Regolamento CT ha introdotto il concetto di «reti di ricercatori»; si tratta di un fenomeno già preesistente alla entrata in vigore del Regolamento stesso, ma che ha trovato una precisa collocazione normativa nell'ambito della fattispecie «cosponsorizzazione» prevista nell'art. 72 del citato Regolamento.

Ciò accade, soprattutto ma non in via esclusiva, nei programmi di ricerca avviati e condotti da enti non privati, che hanno per oggetto esclusivo la ricerca scientifica, a volte sotto la guida di un ente capofila.

Il Regolamento le chiama anche «*reti aperte e informali*» ed indica un percorso preferenziale che prevede la co-responsabilità, o responsabilità condivisa nello svolgimento della sperimentazione clinica, attraverso la assunzione del ruolo di copromotore. Un aspetto interessante è che la collaborazione nell'ambito delle reti di ricercatori può coinvolgere sia soggetti che per loro natura svolgono attività di ricerca in via esclusiva, sia soggetti privati o società che invece l'attività di ricerca la svolgono ai fini della successiva e possibile commercializzazione di risultati della stessa. Appare evidente che ai fini dell'utilizzo, sia dei dati della ricerca sia dei dati di salute, che intervengono ed emergono nelle attività di ricerca, gli interessi e le finalità possono essere diverse a seconda del soggetto che conduce, o conduce congiuntamente, l'attività di ricerca.

Ciò si riflette su tutti gli aspetti di elaborazione dell'informativa e del consenso

---

[34] A. BASSI-R. VILLANI (a cura di), *I forum deliberativi. La rappresentanza per il Terzo Settore*, di Stefano Zamagni, Università di Bologna in *Rappresentanza: modelli e prospettive per il Terzo Settore*, p. 23 – AICCON, Forlì.

[35] *Ibidem.*

e più in particolare attraverso una stratificazione del consenso, che individui e chiarisca tutte le finalità ancillari rispetto alla tematica principale dello studio clinico.

Un esempio di reti di ricercatori sono gli Istituti di Ricoveri e Cura a Carattere Scientifico (IRCCS) [36], la cui connessione tra loro, o per mezzo di loro, in reti collaborative è stata promossa proprio dal Ministero della Salute [37].

Gli IRCCS sono istituti pubblici o privati ai quali con Decreto del Ministero della salute viene riconosciuto il carattere scientifico in una specifica area tematica [38].

Appare difficile che, stante la loro natura, privatistica o pubblicistica, ma comunque esclusivamente indirizzata alla attività scientifica e di cura, tali Istituti possano rivestire un ruolo nell'ambito dei servizi di cooperazione di dati. Tuttavia, andrebbero a porsi come controparte negoziale qualora, ad esempio, una cooperativa di pazienti dovesse negoziare condizioni e modalità per il trattamento dei loro dati di salute; o ancora, nell'ambito di una maggiore collaborazione potrebbero essi stessi, gli Istituti, farsi facilitatori e promotori di forme di cooperazione.

Il settore della ricerca scientifica farmacologica, come si è già avuto modo di accennare *supra*, è caratterizzato, oltre che dalla preponderante natura specifica del dato personale trattato, anche dalla asimmetria informativa che viene a crearsi tra il soggetto che svolge ricerca e il soggetto che partecipa alla ricerca. Tale aspetto trova una maggiore qualificazione qualora l'oggetto della ricerca riguardi patologie che coinvolgono la capacità di vita quotidiana e professionale della persona, le sue relazioni sociali e, ancora, le conseguenze e le connessioni nel suo ambito familiare a causa, ad esempio, delle anomalie cromosomiche e genetiche.

Non è solo la persona, soggetto che partecipa allo studio clinico o i cui dati afferiscono ad uno studio clinico, ad essere coinvolta, ma anche la sua sfera di relazioni amicali e familiari.

La già citata modifica dell'art. 110 del Decreto Legislativo è senz'altro nella direzione di una semplificazione e di un maggior *favor* verso il progresso e la ricerca scientifica, ma di fatto affievolisce la maggior tutela che era stata accordata al soggetto interessato attraverso la previsione di una valutazione diretta da parte del Garante, contenuta nella precedente formulazione.

Il ricorso a fenomeni aggregativi con l'obiettivo di meglio analizzare e valutare il contesto nel quale il trattamento dei dati viene effettuato, al fine di aiutare il sog-

---

[36] Già il d.lgs. n. 288 del 16 ottobre 2003 recante norme sul «Riordino della disciplina degli Istituti di ricovero e cura a carattere scientifico, a norma dell'art. 42, co. 1, della l. 16 gennaio 2003, n. 3» all'art. 10 riserva, nella ripartizione dei fondi di cui agli artt. 12 e 12-*bis* del d.lgs. 30 dicembre 1992, n. 502, apposite quote, annualmente stabilite dal Ministro della salute, per il finanziamento di progetti gestiti mediante organizzazioni in rete.

[37] https://www.salute.gov.it/portale/ricercaSanitaria/dettaglioContenutiRicercaSanitaria.jsp?lingua=italiano&id=5533&area=Ricerca%20sanitaria&menu=reti.

[38] Cfr. d.lgs. 16 ottobre 2003, n. 288 come modificato dal d.lgs. 23 dicembre 2022, n. 200 concernente «*Riordino della disciplina degli Istituti di ricovero e cura a carattere scientifico, a norma dell'art. 42, comma 1, della legge 16 gennaio 2003, n. 3*».

getto, collocato in una posizione di debolezza nel rapporto che si instaura con il conferimento dei propri dati di salute, potrebbe riportare il rapporto stesso in una situazione di miglior equilibrio.

I servizi di cooperative di dati, alle quali i soggetti partecipanti allo studio clinico, potrebbero di volta in volta aderire o anche solo per ricevere quell'aiuto a meglio comprendere tutte le circostanze del trattamento, ivi inclusi i possibili usi ulteriori e futuri dei dati e le loro modalità di utilizzo, si andrebbero ad inserire proprio in questo contesto.

Un punto di snodo importante per quanto concerne tutti i possibili usi ulteriori e futuri dei dati personali, una volta conferiti nell'ambito della partecipazione a studi clinici, è contenuto nella regolamentazione riguardante i cd. studi clinici di medicinali senza scopo di lucro.

Si tratta di studi clinici secondo il Decreto Ministero Salute del 30 novembre 2021 dal titolo «Misure volte a facilitare e sostenere la realizzazione degli studi clinici di medicinali senza scopo di lucro e degli studi osservazionali e a disciplinare la cessione di dati e risultati di sperimentazioni senza scopo di lucro a fini registrativi, ai sensi dell'art. 1, comma 1, lettera c), del decreto legislativo 14 maggio 2019, n. 52» (GU n.42 del 19-2-2022) [39].

Il Decreto è stato adottato anche ai sensi del considerando n. 81 del citato regolamento (UE) n. 536/2014 per il quale «fine di sfruttare al massimo il prezioso contributo dei promotori non commerciali e incentivare ulteriormente le loro ricerche, senza tuttavia compromettere la qualità delle sperimentazioni cliniche, gli Stati membri dovrebbero adottare apposite misure per incentivare le sperimentazioni cliniche condotte da tali promotori non commerciali».

Ed in effetti la contrapposizione tra ricerca clinica a scopo commerciale e non, nasce proprio dalla regolamentazione europea sulla base di un presupposto a proposito del quale molto poco si è discusso negli ultimi decenni, ossia il fatto che la ricerca clinica commerciale sia la normalità o meglio la via standard per lo sviluppo di medicinali.

Il regime che caratterizza la commercializzazione dei medicinali ad uso umano è basato su un aspetto autorizzatorio con procedure di analisi e valutazione, europee e nazionali, molto analitiche, ma alla fine quello che ne risulta è la possibilità di commercializzare, quindi fare profitto e, possibilmente, reinvestire i proventi nella ricerca e sviluppo di altri nuovi medicinali.

L'aspetto autorizzatorio che peraltro permea tutte le fasi anche molto anteriori alla autorizzazione alla immissione in commercio, è il primo atto nel quale le istituzioni pubbliche danno seguito al principio di tutela della salute umana, gli atti successivi si concretizzano con la, eventuale, negoziazione del prezzo e ammissione al rimborso del medicinale e le relative condizioni.

---

[39] Il Decreto sostituisce la precedente e desueta regolamentazione, ossia il D.M. 17 dicembre 2004, introducendo proprio una specifica previsione in caso di cessione di dati ai fini della commercializzazione.

La fase di sviluppo clinico del medicinale è quindi solo indirettamente caratterizzata dalla partecipazione diretta di istituzioni pubbliche e, le organizzazioni che sviluppano medicinali, sono imprese commerciali, alle quali risulta piuttosto difficile applicare la finalità di «ricerca scientifica» così come espressa nel Regolamento all'art. 9 paragrafo 2 lettera j) in quanto svolta sulla base del diritto dell'Unione [40]; ciò in quanto le imprese commerciali non operano a causa di una disposizione normativa ma per poter commercializzare e quindi tranne vantaggio economico dalla attività di ricerca.

Tuttavia, gli elementi di contatti tra le ricerche scientifiche condotte secondo le due differenti finalità sono numerosi, e la osmosi caratterizzata dalla intensa collaborazione tra il modo delle imprese e quella della ricerca scientifica istituzionale, come anche le agenzie regolatorie, è molto forte.

L'art. 3 del D.M. del 30 novembre 2021, rubricato «cessione dei dati e risultati di sperimentazioni senza scopo di lucro a fini registrativi» al comma 5 afferma che «per effetto della cessione, il cessionario subentra a tutti gli effetti nella titolarità del trattamento dei dati personali».

La norma è di difficile interpretazione perché si pone come anello di congiunzione tra ricerche cliniche che potrebbero avere effettuato trattamenti di dati particolari (di salute) su basi legali differenti e che, nel caso di subentro, potrebbero dover comportare un diverso *assesment* in merito, prima della utilizzabilità dei dati stessi. In realtà più che una apertura verso una visione «consenso – centrica» del trattamento dei dati nella ricerca clinica, la norma sembra aver, forse distrattamente, minimizzato le problematiche sottese ad un passaggio di titolarità che, anche sulla base della legislazione europea, avrebbe invece richiesto maggiore attenzione.

In effetti, le moderne circostanze della ricerca clinica, richiedono che, in generale, il trattamento dei dati personali avvenga in maniera molto diversa dal passato. Una osservazione sulla possibile inadeguatezza del consenso quale base giuridica per il trattamento dei dati negli studi clinici è stata espressa anche dal Centro di Coordinamento Nazionale dei Comitati Etici nella Nota «Ricerca osservazionale: un pilastro nel processo di produzione di conoscenza», emessa il 26 luglio 2022 proprio nel contesto del Decreto Ministeriale novembre 2021. In tale documento il CCNCE suggerisce «la massima semplificazione degli adempimenti relativi, rimuovendo o limitando il più possibile gli ostacoli formali che un'interpretazione della normativa, improntata ad un approccio prevalentemente 'interventistico' e 'monouso', tuttora frappone all'utilizzo e riutilizzo dei dati di ricerca. In quanto 'fonte' di conoscenze significative per la comunità scientifica, tali dati debbono poter circolare il più liberamente possibile all'interno di essa» [41].

La questione si pone, secondo quanto rileva il CCNCE, in particolare agli studi osservazionali per i quali risulta difficile ed a volte impossibile dover riaprire la

[40] Ovvero: «in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea» come afferma l'art. 110, co. 1, del d.lgs. n. 196/2003.

[41] Documento disponibile al seguente link: https://www.aifa.gov.it/en/centro-coordinamento-comitati-etici.

consultazione attraverso il consenso dell'interessato ogniqualvolta vi fosse la necessità di avviare una nuova ricerca su dati già disponibili o proseguire secondo un diverso filone di ricerca.

Per tale motivo il CCNCE suggerisce di indagare se il legittimo interesse possa costituire una possibile base giuridica di trattamento in maniera da giovare alla promozione della ricerca osservazionale, tenendo conto che la pratica della pseudoanonimizzazione/cifratura della identità del paziente e già ampiamente adottata nel contesto degli studi.

Ebbene, anche alla luce della recente modifica dell'art. 110 del Decreto Legislativo, occorre chiedersi se nell'ambito delle previsioni di cui all'art. 106, ed in particolare nel co. 2, lett. *b)* e *d)*, possano trovare spazio forme di cooperazione tra soggetti interessati che legittimamente operino nell'individuare concrete forme attuative riguardo: *a)* durata della conservazione dei dati, *b)* redazione di idonee informative, *c)* criteri selettivi da osservare per il trattamento dei dati identificativi, *d)* idonee e specifiche misure di sicurezza, *e)* ambito e condizioni per un uso ulteriore dei dati ivi inclusa l'ipotesi di un subentro nella titolarità di un soggetto terzo.

La risposta sarebbe affermativa soprattutto alla luce della disposizione di cui all'art. 35, par. 9, del GDPR per il quale «se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti».

Peraltro, proprio la presenza di organizzazioni rappresentative di soggetti interessati (pazienti), sotto forma di servizi di cooperazione di dati, darebbe concreta attuazione ad una disposizione che il GDPR prevedeva meramente eventuale; in altri termini il titolare del trattamento sarebbe comunque tenuto ad interloquire con le organizzazioni cooperative ai fini della predisposizione della valutazione di impatto. Ed ancora, pur in presenza di una valutazione di impatto, le organizzazioni cooperative potrebbero svolgere un ruolo di sorveglianza di eventuali termini e condizioni negoziate così come potrebbero emergere dalla medesima valutazione di impatto.

6. I comitati etici e le possibili interazioni con i servizi di cooperazione di dati.

Il Regolamento CT definisce il comitato etico come «un organismo indipendente istituito in uno Stato membro a norma del diritto di tale Stato membro e incaricato di fornire pareri ai fini del presente regolamento che tenga conto della prospettiva dei non addetti ai lavori, in particolare i pazienti o le loro organizzazioni»; ed in effetti è l'unico ente in grado di poter garantire il rispetto delle norme tutte applicabili allo studio clinico, con un approccio di riguardo verso i pazienti. L'eticità, che sembra essere prerogativa funzionale di tali organizzazioni, dovrebbe quindi realizzarsi attraverso una tutela dei soggetti meno esperti e forse anche più deboli, quali

sono i pazienti, per fare in modo che l'intero studio clinico non presenti elementi pregiudizievoli a loro carico.

Su base della legge delega dell'11 gennaio 2018 n. 3 sono stati emanati due decreti ministeriali, ossia il Decreto Ministero della salute del 1° febbraio 2022 dal titolo «Individuazione dei comitati etici a valenza nazionale» (GU Serie Generale n.63 del 16 marzo 2022) ed il Decreto Ministero dalla Salute 30 gennaio 2023 dal titolo «Definizione dei criteri per la composizione e il funzionamento dei comitati etici territoriali» (GU Serie Generale n. 31 del 7 febbraio 2023).

La regolamentazione prevede quindi tre comitati etici nazionali [42] ed i comitati etici territoriali, questi ultimi hanno competenza esclusiva sulla valutazione delle sperimentazioni cliniche di fase I, II, III e IV, sulla valutazione di indagini cliniche sui dispostivi medici e valutazione di studi osservazionali farmacologici.

Ad integrazione delle norme europee, la regolamentazione italiana è molto più specifica nell'individuare le competenze dei Comitati Etici, essi hanno «la responsabilità di garantire la tutela dei diritti, della sicurezza e del benessere delle persone in sperimentazione e di fornire pubblica garanzia di tale tutela» [43]. Tra i membri devono essere presenti, obbligatoriamente, anche «un rappresentante delle associazioni di pazienti o di cittadini impegnati sui temi della salute» [44].

Sebbene la normativa sopra citata non contenga alcun preciso e specifico riferimento ad eventuali competenze valutative in materia di trattamento dei dati personali è verosimile far rientrare, nel più generale compito di garantire la tutela dei diritti dei partecipanti allo studio clinico, anche compiti in materia di *Data Privacy*. Del resto, sia gli interventi storici del Garante [45], sia gli interventi del Centro di Coordinamento Nazionale dei Comitati Etici [46] sui temi relativi all'interazione tra la disciplina del GDPR e la ricerca clinica, confermano che non sarebbero sottratte alle valutazioni del Comitato Etico anche gli aspetti relativi alla *Data Privacy*.

Nel contesto così sommariamente delineato il Comitato Etico, in particolare quello territoriale, sembra essere l'unico organo in grado di porsi in una posizione mediana di garanzia tra lo sponsor/sperimentatore ed il soggetto che si sottopone alla sperimentazione, con ciò potendo legittimamente esercitare tutte quelle valutazioni ed azioni di tutela previste dall'ordinamento. Peraltro, stante la sua natura ter-

---

[42] Si tratta del Comitato etico per le sperimentazioni cliniche in ambito pediatrico, del Comitato etico per le sperimentazioni cliniche relative a terapie avanzate e del Comitato etico per le sperimentazioni cliniche degli enti pubblici di ricerca e altri enti pubblici a carattere nazionale.

[43] Art. 1 del Decreto Ministeriale 30 gennaio 2023.

[44] *Ibidem*, art. 3, co. 4.

[45] Linee Guida per i trattamenti di dati personali nell'ambito delle sperimentazioni cliniche dei medicinali del 24 luglio 2008.

[46] Cfr. documento del Centro di Coordinamento Nazionale dei Comitati Etici dal titolo «Criticità etiche e normative nel trattamento dei dati personali sanitari nella ricerca osservazionale» del 6 aprile 2023.

ritoriale ed il fatto di essere incardinato all'interno della struttura sanitaria, il Comitato Etico è anche il centro di rifermento unico che può conoscere le specificità territoriali, nelle varie declinazioni culturali, economiche ed epidemiologiche, oltre che conservare una storia di tutte le attività di ricerca clinica svolte nel proprio territorio di competenza [47].

Una opportunità funzionale che, se pienamente esercitata farebbe anche uscire i Comitati Etici da meri supervisori di un iter procedurale regolatorio, fino a diventare un centro di riferimento per molteplici aspetti, ivi compresa una corretta e compiuta gestione di tutte le vicende che riguardano il trattamento dei dati personali.

La regolamentazione già prevede la rappresentanza delle organizzazioni di pazienti all'interno del Comitato Etico, ma tale ruolo potrebbe risultare limitato essendo l'universo delle patologie e degli ambiti della ricerca clinica molto vasti e per certi versi imprevedibili. Mentre, ciò che potrebbe apparire fondamentale è invece la possibilità che i Comitati Etici abbiano un interlocutore qualificato che sintetizzi le istanze dei pazienti, nel momento in cui diventano soggetti interessati dal trattamento dei dati.

In questa direzione potrebbero costituirsi dei servizi di cooperazione, anche sotto forma di cooperative, a livello locale che catalizzino le istanze dei pazienti (soggetti interessati), intervenendo attraverso tutto il processo e con le molteplici modalità previste dal *Data Governance Act*.

Così, ad esempio, le cooperative potrebbero costituire un *hub* nel quale i pazienti, oltre che conferire i propri dati in vista di una successiva condivisione con lo sperimentatore/sponsor, possono ricevere una consulenza o, anche senza conferimento di dati, aderendo ad essa, essere parte negoziale nel definire condizioni, termini e modalità del trattamento, usufruendo di questi servizi.

In tale contesto il Comitato Etico avrebbe un interlocutore qualificato con cui definire anche a priori una serie di elementi per cui, lo sponsor e lo sperimentatore, una volta aderito alle condizioni già predefinite, seguirebbero un iter agevolato ed agile con un evidente beneficio anche per le attività di ricerca clinica.

In ogni caso, il posto di rappresentanza all'interno del Comitato Etico verrebbe comunque garantito in quanto spettante per legge e, qualora tale ruolo venisse rivestito da un rappresentante della o delle cooperative, avrebbe modo di intervenire e contribuire direttamente alla formazione della volontà del medesimo Comitato Etico.

Nulla vieta, ancora, che qualora fossero presenti più organizzazioni create sotto forma cooperativa, insieme possano eleggere un unico rappresentante, dando così indirettamente vita ad una rete di cooperative; tale fattispecie potrebbe verosimilmente attuarsi nel momento in cui ogni cooperativa fosse espressione di una specifica esigenza legata ad esperienza di patologia.

---

[47] Si legga a tal fine anche A. MIGONE DE AMICIS, *Scienza, Ricerca Clinica e Privacy: Rinnovate riflessioni*, cit.

7. Conclusioni, un approccio etico.

Una delle novità contenute nel *Data Governance Act*, è l'introduzione di una nuova figura: il «titolare dei dati»; si tratta di una persona, fisica o giuridica, che ha il diritto di concedere l'accesso a determinati dati personali o dati non personali o di condividerli.

Ebbene, se da un lato l'intenzione di creare un mercato interno dei dati avrebbe comunque comportato l'elaborazione di una figura ulteriore rispetto al dualismo «titolare del trattamento» e «soggetto interessato», dall'altro questa figura del titolare dei dati sembra aprire a due ordini di considerazioni, sulle quali potrebbe svilupparsi un futuro approfondimento.

Da un lato, infatti, le due figure tradizionali (del titolare del trattamento e del soggetto interessato) dovranno ripensare i propri ruoli e responsabilità operative laddove si apre alla possibilità di una circolazione del dato, al di fuori dello schema classico del trattamento; e su questo già il *Data Governance Act* offre precise indicazioni sul sistema della governance, che troveranno nel disegno esecutivo un importante sostegno dalle *best practice* in ambito informatico, di sicurezza e responsabilità organizzativa all'interno degli enti.

Conseguentemente, dall'altro lato è verosimile immaginare che si aprano temi legati all'etica, laddove il *Data Governance Act* non sembra progredire moltissimo rispetto ai principi preesistenti nella legislazione. In altri termini, il novello «titolare dei dati», essendo investito di un ruolo per certi versi trasversale (toccando tutti gli aspetti del Trattamento) e potendo esercitare diritti che prima erano prerogativa del solo interessato, pur non essendo un interessato, si potrebbe trovare nella opportunità di sviluppare un apparato etico a guida del proprio operato; con ciò andando a colmare o raffinare elementi già presenti nella normativa.

In questo contesto, la forma cooperativa, che appunto per sua natura non può prescindere dal rapporto mutualistico, che di per sé ricompone, nello schema dell'impresa, un elemento soggettivo del socio-persona, appare un luogo di elezione per sviluppare anche una componente etica-deontologica dell'agire.

Capitolo XXVI

Le cooperative di dati e l'amministrazione condivisa

Simone Franca

Abstract: The present contribution focuses on data cooperatives, aiming to highlight their potential within the theoretical and practical framework of shared administration. To this end, the contribution is divided into three parts. The first part reconstructs the legal regime of data cooperatives as inferred from the DGA. In the second part, an attempt is made to assess the extent to which data cooperatives can be relevant in their relationship with public administration, with particular reference to the shared administration model. Finally, in the third part, the potential of data cooperatives regarding shared administration practices is highlighted, also concluding with the persistent areas of criticism stemming from the uncertain legal regime of data cooperatives.

1. Introduzione.

«La Commissione è convinta che le imprese e il settore pubblico dell'UE possano, tramite l'uso dei dati, disporre degli strumenti per adottare decisioni migliori» [1].

Con queste parole la Commissione europea sintetizza la visione posta al fondo della Strategia sui dati del 2020.

La Strategia, a ben vedere, rappresenta un punto di snodo da due punti di vista.

Dal punto di vista diacronico, la strategia rappresenta l'ultimo tassello di un percorso tracciato già nel 2014 con la Comunicazione della Commissione intitolata

[1] COMMISSIONE EUROPEA, *Una strategia europea per i dati*, Brussels, 19 febbraio 2020, COM(2020)66 final, p. 1.

«Verso una florida economia basata sui dati» [2] e nella Strategia per il mercato unico digitale in Europa del 2015 [3], ma, al tempo stesso, il primo di una nuova stagione di valorizzazione dell'economia dei dati.

Dal punto di vista sincronico, la strategia si colloca al centro di un'azione più generale nel vasto ambito del digitale, comprensivo anche della Comunicazione della Commissione «Plasmare il futuro digitale dell'Europa» [4] e a un libro bianco sull'intelligenza artificiale [5]. L'obiettivo è chiaro: favorire un posizionamento privilegiato nel contesto globale dell'economia dei dati, generando valore tramite questi ultimi e favorendone la circolazione [6].

Per raggiungere tale obiettivo, tuttavia, l'Unione Europea individua un modello differente da quello di altri attori sullo scenario globale. Differentemente dalle strategie statunitense e cinese [7], quella eurounitaria si fonda sulla valorizzazione della circolazione dei dati e sulla contestuale considerazione del principio personalistico [8]. L'opzione eurounitaria, dunque, si inserisce nella tradizione, inaugurata già dalla direttiva madre e proseguita con il GDPR, che contempera esigenze di prote-

---

[2] COMMISSIONE EUROPEA, *Verso una florida economia basata sui dati*, Brussels, 2 luglio 2014, COM(2014)442 final. Qui si avanzava un orientamento delle istituzioni europee teso a cogliere le opportunità date dalla circolazione dei dati e, contestualmente, a individuare adeguate tecniche di protezione delle persone fisiche.

[3] COMMISSIONE EUROPEA, *Strategia per il mercato unico digitale in Europa*, Brussels, 6 maggio 2015, COM(2015)192 final si evince l'esigenza di un bilanciamento dalla definizione di mercato unico digitale come «un mercato in cui è garantita la libera circolazione delle merci, delle persone, dei servizi e dei capitali e in cui (…) persone e imprese non incontrano ostacoli all'accesso e all'esercizio delle attività online in condizioni di concorrenza leale e potendo contare su un livello elevato di protezione dei consumatori e dei dati personali». Ancora, nell'art. 1 GDPR si chiarisce come la protezione delle persone fisiche non possa ostacolare la circolazione dei dati personali.

[4] COMMISSIONE EUROPEA, *Plasmare il futuro digitale dell'Europa*, Brussels, 19 febbraio 2020, COM(2020)67 final.

[5] COMMISSIONE EUROPEA, *Libro Bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia*, Brussels, 19 febbraio 2020, COM(2020)65 final.

[6] In questo senso rispetto agli obiettivi della Strategia, cfr. D. POLETTI, *Gli intermediari dei dati* – data intermediaries, in *Eur. Journal of Privacy Law and Technology*, 2022, 1, p. 48.

[7] Il modello statunitense si caratterizza, in particolare, per la scelta di fare riferimento ad un modello regolatorio in cui il controllo sull'economia dei dati e l'organizzazione dei relativi spazi è affidato ai cd. poteri privati, ossia alle *big tech*. Il modello cinese, invece, si fonda su un controllo più stretto del Governo, non orientato comunque in una prospettiva garantista. Su questi modelli e sul loro confronto col modello eurounitario cfr. F. BRAVO, *Le cooperative di dati*, in *Contr. Impr*, 2023, 3, p. 765. Indirizzi in parte simili si evincono rispetto alla posizione di USA, UE e Cina con riguardo alla disciplina dell'*e-commerce*. In tema cfr. in part. F. ANTONELLI, *The international regulatory framework for e-commerce; the approach of the US, China and the EU*, in G. FINOCCHIARO (a cura di), *Major legal trends in the digital economy: the approach of the EU, the US, and China*, Bologna, 2022.

[8] Cfr. sul punto F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al* Data Governance Act, in *Contr. Impr.*, 2021, 1, p. 202.

zione e di circolazione [9]: con la Strategia, tuttavia, l'enfasi è posta maggiormente sulla circolazione [10]. A questo scopo la Strategia ipotizza il ricorso a «strumenti per la gestione del consenso, app per la gestione delle informazioni personali, comprese soluzioni completamente decentrate basate sulla blockchain, come pure cooperative o *trust* per i dati personali, che agiscono da intermediari neutrali di nuova concezione nell'economia dei dati personali» [11].

Tale indirizzo è stato attuato attraverso il *Data governance act* [12] (d'ora in avanti, DGA), il quale disciplina i servizi di intermediazione dei dati [13], fra cui figurano i servizi di cooperative di dati.

Questi ultimi sono intesi come servizi «offerti da una struttura organizzativa costituita da interessati, imprese individuali o da PMI, che sono membri di tale struttura» [14]; tali servizi sono funzionali a diversi obiettivi, fra cui quello di «rafforzare la posizione dei singoli individui, affinché compiano scelte informate prima di acconsentire all'utilizzo dei dati» [15].

Così, la cooperativa di dati si pone come strumento utile a valorizzare la posizione di autodeterminazione informativa [16] del singolo, ma, a ben vedere, permette altresì di favorire nuove forme di circolazione dei dati. In questa prospettiva, uno spazio particolarmente interessante appare quello relativo alla circolazione dei dati funzionale al perseguimento dell'interesse pubblico. Le cooperative di dati, infatti,

---

[9] Rispetto alla portata di tale dialettica nella disciplina eurounitaria in tema di protezione di dati personali sia consentito rinviare a S. FRANCA, *I dati personali nell'amministrazione pubblica. Attività di trattamento e tutela del privato*, Napoli, 2023.

[10] È stato rilevato, rispetto agli sviluppi della disciplina eurounitaria concernente i dati, che «[a]fianco a un *Datenschutzrecht* sembra emergere e acquistare giuridica consistenza un *Datenwirtschaftsrecht*» (G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, in *Riv. trim. dir. pubbl.*, 2022, 4, p. 975).

[11] COMMISSIONE EUROPEA, *Una strategia europea per i dati*, cit., p. 12.

[12] Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (Regolamento sulla governance dei dati).

[13] Ai sensi dell'art. 2, par. 1, n. 11, DGA è tale «un servizio che mira a instaurare, attraverso strumenti tecnici, giuridici o di altro tipo, rapporti commerciali ai fini della condivisione dei dati tra un numero indeterminato di interessati e di titolari dei dati, da un lato, e gli utenti dei dati, dall'altro, anche al fine dell'esercizio dei diritti degli interessati in relazione ai dati personali», salvo alcune esclusioni specifiche previste nella stessa disposizione.

[14] Così la prima parte della definizione di servizi di cooperative di dati evincibile dall'art. 2, par. 1, n. 15, DGA. Su tale definizione si tornerà più approfonditamente *infra*.

[15] Così il *considerando* n. 31 DGA.

[16] Sul rilievo dell'autodeterminazione informativa il richiamo non può che andare a Si tratta della lettura che in Italia è stata sostenuta originariamente e con particolare nitore in S. RODOTÀ, *La privacy tra individuo e collettività*, in *Pol. dir.*, 1975, p. 547 (successivamente anche in ID., *Tecnologia dell'informazione e frontiere del sistema socio-politico*, in *Pol. dir.*, 1982, p. 25 ss.; ID., *Repertorio di fine secolo*, Roma, 1999, p. 205 ss.).

possono fungere da vettore per nuovi utilizzi di dati nell'ambito di *partnership* pubblico-private.

Alla luce di questo contesto, il presente contributo intende approfondire il ruolo delle cooperative di dati nell'ambito di un peculiare modello di collaborazione tra pubblico e privato, quello dell'amministrazione condivisa.

A tale scopo il contributo sarà suddiviso in tre parti.

Nella prima parte si ricostruirà lo statuto giuridico delle cooperative di dati evincibile dal DGA.

Nella seconda parte, alla luce della ricostruzione svolta, si tenterà di verificare in che misura le cooperative di dati possono rivelarsi rilevanti nel rapporto con l'amministrazione pubblica, con particolare riferimento al modello dell'amministrazione condivisa.

Infine, nella terza parte, si evidenzieranno le possibili potenzialità delle cooperative di dati rispetto alle prassi di amministrazione condivisa, evidenziando anche, in sede conclusiva, gli ancora persistenti margini di criticità dati dall'incerto regime giuridico delle *data cooperatives*.

2. Le cooperative di dati: uno strumento collaborativo nell'economia digitale.

La cooperativa di dati è una forma di *business* già presente nella prassi prima dell'emanazione del DGA e attiva nella fornitura di servizi di intermediazione dei dati.

In effetti, se si consulta la letteratura relativa ai servizi di intermediazione dei dati, si può evincere da tempo la presenza di operatori del mercato che offrono simili servizi e, fra di essi, di alcuni soggetti che operano come cooperative [17].

[17] Per approfondimenti anche in chiave empirica sulle cooperative di dati cfr. in part. E. BIETTI, A. ETXBERRIA-M. MANNAN-J. WONG, *Data Cooperatives in Europe: A Legal and Empirical Investigation*, White Paper created as part of The New School's Platform Cooperativism Consortium and Harvard University's Berkman Klein Center for Internet & Society, Research Sprint, December 2021, in https://cyber.harvard.edu/sites/default/files/2022-02/Data_Cooperatives_Europe-group2.pdf; M.M. BÜHLER-I. CALZADA-I. CANE-T. JELINEK-A. KAPOOR-M. MANNAN-S. MEHTA-V. MOOKERJE-K. NÜBEL-A. PENTLAND-T. SCHOLZ-D. SIDDARTH-J. TAIT-B. VAITLA-J. ZHU, *Unlocking the Power of Digital Commons: Data Cooperatives as a Pathway for Data Sovereign, Innovative and Equitable Digital Communities*, in *Digital*, 2023, 3, p. 146 ss.; M.M. BÜHLER-K. NÜBEL-T. JELINEK-D. RIECHERT-T. BAUER-T. SCHMID-M. SCHNEIDER, *Data cooperatives as a Catalyst for Collaboration, Data Sharing and the Digital Transformation of the Construction Sector*, in *Buildings*, 2023, 13, p. 1 ss.; M. DAWANDE-S. MEHTA-L. MU, *Robin Hood to the Rescue: Sustainable Revenue-Allocation Schemes for Data Cooperatives*, in *Production and Operation Management*, 2023, Vol. 32, n. 8, p. 2560 ss.; E. HAFEN, *Personal Data Cooperatives – A New Data Governance Framework for Data Donations and Precision Health*, in J. KRUTZINNA-L FLORIDI (eds.), *The Ethics of Medical Data Donation*, Cham, 2019, p. 141 ss.; M. MICHELI-E. FARRELL-B. CARBALLA-SMICHOWSKI-M. POSADA-SÁNCHEZ-S. SI-

Gli esempi sono abbastanza numerosi e coinvolgono società cooperative in settori variegati, dalle costruzioni alla telemedicina [18].

Rispetto ai casi ricavabili dalla prassi è possibile, in ogni caso, tracciare una tassonomia al fine di isolare diversi "modelli" di cooperative di dati.

In particolare, tenendo conto di come si struttura la circolazione dei dati, sicché possono aversi casi in cui i dati vengono condivisi nella cooperativa per uso interno da parte della cooperativa (*Member-to-Cooperative*) o dei membri stessi (*Member-to-Member*); possono aversi anche casi in cui i dati vengono trasferiti ad altre cooperative di dati che svolgono simili attività (*Federated*), a soggetti terzi (*Third Party*) o diffusi, rendendoli pubblici alla collettività (*Open Data*) [19].

Ciò che è rilevante, in ogni caso, è che le cooperative si caratterizzano per la capacità di strutturare architetture di trattamento in una visione eminentemente mutualistica [20].

Se questo è quanto è evincibile dalla prassi, il DGA fornisce alcune coordinate per inquadrare il fenomeno con la definizione di "servizi di cooperative di dati", da un lato, e le regole relative all'intermediazione dei dati, dall'altro lato.

Sul primo fronte giova rilevare che la definizione di servizi di cooperative di dati è scomponibile in due parti. La prima parte, richiamata già *supra*, riguarda i profili strutturali e definisce tali servizi come «servizi di intermediazione dei dati offerti da una struttura organizzativa costituita da interessati, imprese individuali o da PMI, che sono membri di tale struttura» [21]. In base a tale definizione (incentrata sul servizio e non sulla cooperativa in sé), una cooperativa di dati si presenta come una struttura organizzativa composta da interessati (cioè soggetti cui sono riferibili dei dati) e da imprese, membri della struttura. Si tratta, dunque, di un'organizzazione privatistica non necessariamente coincidente con la società cooperativa, benché trovi in quest'ultima, molto probabilmente, la sua più coerente estrinsecazione [22].

GNORELLI-M. VESPE, *Mapping the landscape of data intermediaries. Emerging models for more inclusive data governance*, Luxembourg, 2023, spec. p. 47 ss.; J. TAIT, *The Case for Data Cooperatives*, Whitepaper Series, Open Data Manchester, 6th September 2021, disponibile al seguente link: https://thedataeconomylab.com/2021/09/06/the-case-for-data-cooperatives/.

[18] Esempi significativi sono, ad esempio, *GemeinWerk,* nel campo delle costruzioni, *Salus coop* nel campo della telemedicina, *Driver's Seat* nel campo dei trasporti. Su alcuni di questi esempi si tornerà più approfonditamente *infra*.

[19] Cfr. la classificazione di J. TAIT, *The Case for Data Cooperatives*, cit., ripresa anche in F. BRAVO, *Le cooperative di dati*, cit., pp. 769-770.

[20] Sul rilievo della finalità mutualistica nelle cooperative di dati cfr. F. BRAVO, *Le cooperative di dati*, cit., p. 764 ss. ove si trovano riferimenti interessanti anche al modello del neo-mutualismo; G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit., pp. 985-986, il quale enfatizza come la struttura delle *data cooperatives* non garantisce un ricavo in termini meramente economici, ma anche sul piano del controllo sui propri dati.

[21] Art. 2, par. 1, n. 15, DGA.

[22] Come rileva F. BRAVO, *Le cooperative di dati*, cit., p. 760, la definizione «lascia intuire che la fornitura di "servizi di cooperative di dati" possa essere svolta, eventualmente, anche in forme diverse

Accanto ai profili strutturali, la definizione reca alcuni profili rilevanti sul piano teleologico. Essa stabilisce diversi possibili obiettivi. Le cooperative di dati, infatti, hanno «come obiettivi principali quelli di aiutare i propri membri nell'esercizio dei loro diritti in relazione a determinati dati, anche per quanto riguarda il compiere scelte informate prima di acconsentire al trattamento dei dati, di procedere a uno scambio di opinioni sulle finalità e sulle condizioni del trattamento dei dati che rappresenterebbero al meglio gli interessi dei propri membri in relazione ai loro dati, o di negoziare i termini e le condizioni per il trattamento dei dati per conto dei membri prima di concedere l'autorizzazione al trattamento dei dati non personali o prima che essi diano il loro consenso al trattamento dei dati personali» [23].

Dunque, ciascuna cooperativa di dati deve perseguire almeno uno dei predetti obiettivi principali [24] – peraltro, tutti orientati a rafforzare la posizione dell'individuo rispetto alla gestione dei propri dati [25] –, ossia agevolare gli interessati nell'esercizio dei propri diritti, di fornire possibilità di scambio di opinioni tra i membri su come gestire i loro dati o di negoziare per conto dei membri le condizioni per il trattamento dei loro dati.

A questa disciplina si aggiunge quella ricavabile dalle regole sull'intermediazione dei dati.

Sul punto rileva in particolare l'art. 12 DGA che pone le condizioni per l'intermediazione dei dati. In base a tale norma, la cooperativa di dati è tenuta a seguire determinate regole rispetto alla gestione dei dati, ivi incluse l'adozione di adeguate misure di sicurezza e la tenuta di un registro in cui annotare i servizi offerti. Particolarmente rilevante è la regola che prevede una separazione strutturale tra l'intermediazione e l'utilizzo dei dati, ossia di neutralità del fornitore di servizi di intermediazione dei dati (*considerando* n. 33 DGA). È previsto, infatti, che quest'ultimo non possa utilizzare i dati che riceve per scopi diversi dalla messa a disposizione di tali dati a soggetti terzi abilitati a trattarli (c.d. utenti dei dati) e possa fornire servizi di intermediazione dei dati solo «attraverso una persona giuridica distinta». Sembrerebbe dunque che sia precluso anche alla cooperativa di dati utilizzare i dati dei propri consociati pur per le proprie finalità mutualistiche. Si tratta di un problema invero facilmente eludibile, dato che potrebbe prospettarsi una colla-

---

da quella societaria, benché la "società cooperativa" (…) sia il soggetto fisiologicamente chiamato a ricoprire il ruolo di "cooperativa di dati"».

[23] Art. 2, par. 1, n. 15, DGA.

[24] Cfr. F. BRAVO, *Le cooperative di dati*, cit., p. 760, che rileva che le finalità possono essere alternative, tenendo conto del tenore letterale della disposizione. Si noti che il riferimento ad una serie di obiettivi qualificati come principali nella definizione di «servizi di cooperative di dati» di cui all'art. 2, par. 1, n. 15, DGA lascia supporre che possano essere perseguiti obiettivi ulteriori (e differenti), purché non in via principale. Tale circostanza potrebbe indurre a ritenere che il principio di neutralità degli intermediari (su cui v. *infra*) abbia una portata più limitata rispetto alle cooperative di dati.

[25] D. POLETTI, *Gli intermediari dei dati*, cit., p. 51; L. PETRONE, *Il mercato digitale europeo e le cooperative di dati*, in *Contr. Impr.*, 2023, 3, p. 811.

borazione tra persone giuridiche separate e autonome, nella specie enti che operano come intermediari ed enti che operano come utenti dei dati, così da aggirare il limite posto dalla regola di neutralità, qualora ritenuta applicabile alle cooperative [26]. In ogni caso, come è stato puntualmente osservato, non pare che tale limitazione sia particolarmente in linea con le finalità mutualistiche, attestate anche dalla prassi, delle società cooperative e, per questo, si è prospettato di superare l'ostacolo sul piano interpretativo, auspicando comunque, *de iure condendo*, un intervento chiarificatore del legislatore nazionale in sede di adattamento interno alla disciplina eurounitaria [27].

Pare dunque di poter affermare che la cooperativa di dati fornisce senz'altro un ponte tra chi è titolare dei dati e chi invece è interessato ad utilizzarli, fornendo una "piattaforma" entro cui favorire l'autodeterminazione informativa e, conseguentemente, alimentando la fiducia nell'economia dei dati.

Rispetto al modello del GDPR, quello cooperativo si segnala così per il maggiore accento sulla circolazione dei dati. In questo schema, tuttavia, va anche evidenziato il maggiore realismo nelle dinamiche protettive rispetto al GDPR. Se infatti quest'ultimo fonda principalmente la tutela del singolo su una sua supposta capacità di autodeterminarsi sul piano informativo, le previsioni di intermediari di dati e, in particolare, di cooperative di dati si muove in una prospettiva diametralmente opposta, ma più coerente con la realtà. Posto che l'autodeterminazione informativa è difficilmente raggiungibile dal singolo senza un supporto, il ruolo dell'intermediario è quello di fornire un ausilio al singolo. Nel caso della cooperativa, infine, questo ausilio passa attraverso uno strumento mutualistico che si colloca, dunque, in una dimensione essenzialmente collaborativa.

3. Le cooperative di dati e la pubblica amministrazione. La convergenza tra cooperative e amministrazione condivisa.

Così come ricostruite le cooperative di dati si rivelano uno strumento che conferisce una piattaforma "intermedia" tra i soggetti cui i dati si riferiscono e gli utilizzatori dei dati stessi.

Questa capacità di intermediazione, come anticipato, è proficua in linea generale nel rapporto con gli operatori del mercato, ma può avere un ruolo significativo anche nel rapporto tra cittadini e pubblica amministrazione.

La pubblica amministrazione, infatti, può trarre dai dati messi a disposizione dai

---

[26] F. BRAVO, *Le cooperative di dati*, cit., p. 775.

[27] *Ibidem*. Con d.lgs. del 7 ottobre 2024, n. 144 è stato adottato un pacchetto di norme di adeguamento della normativa nazionale alle disposizioni del DGA. Tuttavia, non è stata colta l'occasione per disciplinare questi aspetti, concentrandosi l'attenzione del legislatore delegato sulla designazione di AgID come autorità competente ai sensi degli articoli 13, 23 e 26 DGA.

cittadini una base conoscitiva [28] assai ampia sia per migliorare servizi già erogati sia per implementare nuove tipologie di servizio. È sempre più evidente, d'altronde, come l'efficienza e l'efficacia dell'azione amministrativa passi attraverso l'acquisizione di nuovi dati o la valorizzazione dei dati a disposizione.

L'acquisizione di dati dei cittadini, tuttavia, non è sempre semplice. Occorre considerare che i cittadini spesso nutrono una certa diffidenza rispetto alla gestione dei dati che li riguardano ad opera di soggetti pubblici.

Si pensi al caso dell'applicazione "Immuni", nell'ambito dell'emergenza pandemica. Si può constatare come tale app non solo sia stata scarsamente utilizzata [29], ma abbia suscitato un dibattito piuttosto acceso in ordine alla protezione dei dati personali [30], anche se i timori rispetto all'uso dell'app apparivano, almeno ad alcuni studiosi e almeno in parte, infondati [31].

---

[28] Cfr. B. PONTI, *Il patrimonio informativo pubblico come risorsa. I limiti del regime italiano di riutilizzo dei dati delle pubbliche amministrazioni*, in *Dir. pubbl.*, 2007, 3, p. 996; più recentemente, si v. anche M. FALCONE, *Ripensare il potere conoscitivo pubblico tra algoritmi e Big Data*, Napoli, 2023, p. 92 ss.

[29] Le ragioni dello scarso utilizzo vengono individuate, anzitutto, nella scarsa alfabetizzazione digitale della popolazione italiana (in questo senso, cfr. G. DELLA MORTE, *Quanto Immuni? Luci, ombre e penombre dell'app selezionata dal Governo italiano*, in *Dir. umani e dir. internazionale*, 2020, 2, pp. 328-329). Sulla base dei dati sull'utilizzo dei *social network*, tuttavia, sembrerebbe che una fascia consistente della popolazione, per così dire, digitalmente alfabetizzata non abbia comunque optato per utilizzare l'app. In questo senso, cfr. G. RESCE, *Perché immuni non piace*, in *Lavoce.info*, 2020. Si consideri, altresì, che non pare ci siano stati gli stessi scrupoli rispetto al destino dei propri dati rispetto all'app IO, che prevedeva un *cashback* di Stato: l'app è stata scaricata da molti più utenti. Sul punto cfr. S. SCAGLIARINI, *La tutela della privacy e dell'identità digitale nell'evoluzione tecnologica*, in *Consultaonline.it*, 2021, 2, p. 583.

[30] Per una preziosa sintesi dei punti nodali del dibattito si v. G. TROPEA, *Biopolitica e diritto amministrativo del tempo pandemico*, Napoli, 2023, p. 95 ss., ma si vedano pure M.B. ARMIENTO, *Amministrazione digitale e tutela della salute: il caso Immuni tra fallimenti e nuove prospettive*, in *Munus*, 2021, 1, p. 265 ss.; C. COLAPIETRO-A. IANNUZZI, *App di contact tracing e trattamento dei dati con algoritmi: la falsa alternativa fra tutela del diritto alla salute e protezione dei dati personali*, in *Dirittifondamentali.it*, 2020, 2, p. 772 ss. G. DELLA MORTE, *Quanto Immuni?*, cit., p. 303 ss.; M. PLUTINO, *"Immuni". Un'*exposure notification *app alla prova del bilanciamento tra tutela dei diritti e degli interessi pubblici*, in *Dirittifondamentali.it*, 2020, 2, p. 553 ss.; S. SCAGLIARINI, *La tutela della privacy e dell'identità digitale nell'evoluzione tecnologica*, cit., p. 590 ss.; L. TRUCCO, *App Immuni: una storia stran(ier)a e incompiuta*, in *Giustiziainsieme.it*, 2020; V. ZENO-ZENCOVICH, *I limiti delle discussioni sulle "app" di tracciamento anti-Covid e il futuro della medicina digitale*, in *MediaLaws*, 26 maggio 2020.

[31] Parte della dottrina ha puntualmente criticato i timori relativi alla *privacy*, specie operando un paragone su trattamenti di tenore analogo ad opera di soggetti privati. In tal senso, cfr. S. SCAGLIARINI, *La tutela della privacy e dell'identità digitale nell'evoluzione tecnologica*, cit., p. 590 ss. che rileva come le garanzie previste per Immuni siano state, oltretutto, il frutto di un bilanciamento eccessivamente favorevole alla *privacy*; V. ZENO-ZENCOVICH, *I limiti delle discussioni sulle "app" di tracciamento anti-Covid*, cit. Per una prospettiva che, rispetto alle app di tracciamento, si mostra favorevole ad un approccio più equilibrato in relazione ai rischi per la *privacy* cfr. E. CARLONI, "*Fisime per la privacy"? Protezione dei dati personali e interesse pubblico nella pandemia*, in *Ridiam.it*, 2020.

La presenza di cooperative di dati, dunque, può essere utile proprio ad evitare che timori infondati possano ostacolare la circolazione dei dati, quando tale circolazione possa beneficiare la pubblica amministrazione, sempreché i dati siano trattati in modo lecito e corretto.

In questa prospettiva, la cooperativa di dati si pone come diaframma tra cittadini e p.a. favorendo una comunicazione di dati maggiormente consapevole per i primi. Si tratta di una circostanza di non poco momento, posto che l'intermediazione può innescare anche un duplice stimolo, per le amministrazioni ad agire correttamente nei trattamenti e per i cittadini a condividere i dati che li riguardano.

Ciò premesso, le potenzialità sinora descritte delle cooperative dei dati sono evidenti, in particolare, nell'ambito di un rapporto essenzialmente bipolare tra cittadino e pubblica amministrazione, fondato sulla separazione e sulla reciproca diffidenza, in luogo di un rapporto multipolare dove cittadini e p.a. compartecipano alla gestione di attività di interesse generale [32].

Vale la pena però considerare che, nel corso del tempo, il rapporto dei cittadini, singoli e associati, con la p.a. ha assunto anche forme differenti, non solo nella prospettiva dell'amministrazione tradizionale o anche consensuale [33], ma, in particolare, dell'amministrazione condivisa.

Con tale locuzione si allude al modello amministrativo «fondato sulla collaborazione fra amministrazione e cittadini» in grado di «consentire una soluzione dei problemi di interesse generale migliore dei modelli attualmente operanti, basati sulla separazione più o meno netta fra amministrazione e amministrati» [34]. Si tratta di un modello che si basa sull'attuazione del principio di sussidiarietà orizzontale (art. 118, co. 4, Cost.), il quale, a sua volta, dispone che la Repubblica ha il compito di

---

[32] Sulle criticità del modello bipolare e sulla necessità di considerare una logica multipolare cfr. in part. G. ARENA, *Un nuovo modo di amministrare*, in *Riv. it. di com. pubbl.*, 2004, 19, p. 23 ss.; M. BOMBARDELLI, *Democrazia partecipativa e assetto policentrico dell'organizzazione amministrativa*, in G. ARENA-F. CORTESE (a cura di), *Per governare insieme: il federalismo come metodo: verso nuove forme della democrazia*, Padova, 2011, p. 28 ss.; S. CASSESE, *L'arena pubblica. Nuovi paradigmi per lo Stato*, in *Riv. trim. dir. pubbl.*, 2001, 3, p. 601 ss., spec. pp. 649-650 (più recentemente, anche in ID., *Mezzo secolo di trasformazioni nel diritto amministrativo*, in AA.VV., *Diritto amministrativo e società civile. Volume I – Studi introduttivi*, Bologna, 2018, p. 7), ove si rileva che la logica bipolare fa spazio a rapporti multipolari che superano anche la dicotomia oppositiva pubblico-privato.

[33] Per un confronto tra diversi modelli amministrativi, comprensivo anche dell'amministrazione condivisa, si v. V. CERULLI IRELLI, *L'amministrazione condivisa nel sistema del diritto amministrativo*, in G. ARENA-M. BOMBARDELLI (a cura di), *L'amministrazione condivisa*, Napoli, 2022, p. 21 ss.

[34] Così in G. ARENA, *Introduzione all'amministrazione condivisa*, in *Studi parlamentari e di politica costituzionale*, 1997, 117-118, p. 29, che rappresenta la prima teorizzazione dell'amministrazione condivisa. L'impostazione teorica si ricollega alla tradizione di studi di Feliciano Benvenuti, specie rispetto al concetto di demarchia illustrato in F. BENVENUTI, *Il nuovo cittadino. Tra libertà garantita e libertà attiva,* Venezia, 1994. Sul punto cfr. V. CERULLI IRELLI, *L'amministrazione condivisa nel sistema del diritto amministrativo*, cit., p. 21; S.S. SCOCA, *L'amministrazione condivisa nei servizi sociali: una complessa strada ancora da percorrere*, in *Dir. econ.*, 2021, 3, pp. 83-86.

promuovere e sostenere l'autonoma iniziativa dei cittadini rispetto ad attività di interesse generale [35]. Da modello inizialmente solo teorico l'amministrazione condivisa è diventata ben presto «una pratica viva delle istituzioni e della società civile» [36], facendosi strada «alla stregua dell'ordinamento positivo» [37] tanto che persino la Corte costituzionale, nel 2020 [38], con riguardo all'art. 55 del Codice del Terzo settore ha rilevato che esso instaura «un canale di amministrazione condivisa, alternativo a quello del profitto e del mercato», attraverso strumenti come la co-programmazione e la co-progettazione che «si configurano come fasi di un procedimento complesso espressione di un diverso rapporto tra il pubblico ed il privato sociale, non fondato semplicemente su un rapporto sinallagmatico» [39].

A ben vedere, vi sono molteplici elementi comuni tra amministrazione condivisa e cooperative dei dati.

In primo luogo, entrambi i modelli ambiscono a superare la dicotomia tra pubblico e privato intesa in senso rigido, recuperando una dimensione essenzialmente comunitaria [40].

---

[35] Rispetto alla portata di tale principio come fonte di un simile dovere in capo ai soggetti pubblici si vedano, *ex multis*, G. ARENA, *Il principio di sussidiarietà orizzontale nell'art. 118 u.c. della Costituzione*, in *Studi in onore di Giorgio Berti*, I, Napoli, 2005, pp. 182; V. CERULLI IRELLI, voce *Sussidiarietà (dir. amm.)*, in *Enc. giur.*, XII, Roma, 2004, p. 5; D. DE PRETIS, *Principi costituzionali e amministrazione condivisa*, in G. ARENA-M. BOMBARDELLI (a cura di), *L'amministrazione condivisa*, cit., pp. 35-36; D. D'ALESSANDRO, *Sussidiarietà solidarietà e azione amministrativa*, Milano, 2004, p. 68; G.U. RESCIGNO, *Principio di sussidiarietà orizzontale e diritti sociali*, in *Dir. pubbl.*, 2002, 1, pp. 29-32. Da notare che il principio di sussidiarietà orizzontale è stato oggetto anche di letture differenti e pertanto censurato in dottrina, come grimaldello per una riduzione della sfera pubblica a favore di logiche di mercato. Per una critica a tali impostazioni si v. in part. L. VIOLINI, *Teorie e tecniche della sussidiarietà*, in EAD. (a cura di), *L'attuazione della sussidiarietà orizzontale in Lombardia*, Milano, 2004, pp. 16-17.

[36] F. CORTESE, *Amministrazione condivisa e biografia giuridica della Nazione*, in G. ARENA-M. BOMBARDELLI (a cura di), *L'amministrazione condivisa*, cit., p. 15.

[37] V. CERULLI IRELLI, *L'amministrazione condivisa nel sistema del diritto amministrativo*, cit., p. 24. Per un'aggiornata analisi con metodo multidisciplinare dei diversi modelli normativi e operativi si v. i diversi contributi in B.L. BOSCHETTI (a cura di), *Per un laboratorio dell'amministrazione condivisa. Primi risultati di una ricerca multidisciplinare*, Napoli, 2024 e, in particolare, B.L. BOSCHETTI, *Conclusioni*, *ivi*, p. 236 ss. per interessanti considerazioni sulla normatività del modello dell'amministrazione condivisa.

[38] Si allude alla sentenza Corte cost., 26 giugno 2020, n. 131, sulla cui portata si v. G. ARENA, *L'amministrazione condivisa ed i suoi sviluppi nel rapporto con cittadini ed enti del terzo settore*, in *Giur. cost.*, 2020, 3, p. 1449 ss.; F. CIARLARIELLO, *Un conflitto di competenza sul terreno della sussidiarietà: quale rapporto tra pubblica amministrazione ed enti del terzo settore?*, in *Diritti regionali*, 2022, 1, p. 262 ss.; E. ROSSI, *Il fondamento del Terzo settore è nella Costituzione. Prime osservazioni sulla sent. n. 131 del 2020 della Corte costituzionale*, in *Le Regioni*, 2020, 5, p. 1184 ss.; nonché i diversi contributi contenuti in S. PELLIZZARI-C. BORZAGA (a cura di), *Terzo settore e pubblica amministrazione. La svolta della Corte costituzionale*, Trento, 2020.

[39] Così, Corte cost., 26 giugno 2020, n. 131, p.to 2.1.

[40] Per quanto riguarda l'amministrazione condivisa, la dimensione comunitaria è particolarmente evidente rispetto al modello dell'amministrazione condivisa dei beni comuni, proprio perché caratteri-

In secondo luogo, i due modelli si caratterizzano per essere espressione del "paradigma fiduciario" del diritto [41]. Entrambi pongono l'esigenza di favorire un clima di fiducia strumentale a specifiche finalità, nella specie al perseguimento dell'interesse generale (nel caso dell'amministrazione condivisa) [42] e alla realizzazione dell'economia digitale (nel caso delle cooperative di dati).

In terzo luogo, entrambi i modelli si fondano su strumenti che si ispirano ad una logica eminentemente collaborativa piuttosto che competitiva o, comunque, basata sul capitalismo estrattivo, ponendo sempre al centro la persona e le sue relazioni [43].

---

stica della nozione stessa di bene comune (in tal senso cfr. in part. M. BOMBARDELLI, *La cura dei beni comuni come via per uscire dalla crisi*, in ID. (a cura di), *Prendersi cura dei beni comuni per uscire dalla crisi*, Napoli, 2016, p. 20 ss.), ma si riscontra altresì rispetto al ruolo degli enti del terzo settore (cfr. in part. A. FICI, *I "presupposti negoziali" dell'"amministrazione condivisa": profili di diritto privato*, in A. FICI-L. GALLO-F. GIGLIONI (a cura di), *I rapporti tra pubbliche amministrazioni ed enti del terzo settore. Dopo la sentenza della Corte Costituzionale n. 131 del 2020*, Napoli, 2020, p. 55; P. IAMICELI, *La tipizzazione funzionale degli enti del terzo settore*, in S. PELLIZZARI-C. BORZAGA (a cura di*), Terzo settore e pubblica amministrazione*, cit., pp. 30-31). Simile logica si riscontra anche nelle scelte del regolatore europeo che con il DGA e, in particolare, con le cooperative di dati mostra di dare particolare risalto ad una dimensione collettiva, collocabile oltre la dicotomia pubblico- privato. In tal senso cfr. F. BRAVO, *Le cooperative di dati*, cit., p. 762 che enfatizza, in particolare, il carattere collettivo della *governance* della cooperativa di dati; G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit., p. 981 ss. che rinviene un rafforzamento della dimensione collettiva nella disciplina degli intermediari dei dati.

[41] Il riferimento va senz'altro a T. GRECO, *La legge della fiducia. Alle radici del diritto*, Bari, 2021. Per una valorizzazione della lettura di Greco rispetto al paradigma dell'amministrazione condivisa cfr. M. SCLAVI, *Amministrazione condivisa come innesco al necessario cambiamento paradigmatico della democrazia*, in G. ARENA-M. BOMBARDELLI (a cura di), *L'amministrazione condivisa*, cit., p. 157 ss.

[42] Il concetto di fiducia torna in più *luoghi* di disciplina dell'amministrazione condivisa. Si consideri, ad esempio, che il prototipo dei regolamenti comunali sulla collaborazione tra cittadini e amministrazioni per la cura, la rigenerazione e la gestione condivisa dei beni comuni urbani elaborato di Labsus contiene all'art. 3 un elenco di principi, fra cui figura quello di "fiducia reciproca". Ancora, si tenga conto che nelle linee guida del Ministero del Lavoro e delle Politiche sociali sul rapporto tra pubbliche amministrazioni ed enti del Terzo settore negli artt. 55-57 del decreto legislativo n. 117/2017 (d.m. 30 marzo 2021, n. 72) si afferma che «La co-programmazione dovrebbe generare un arricchimento della lettura dei bisogni, anche in modo integrato, rispetto ai tradizionali ambiti di competenza amministrativa degli enti, agevolando – in fase attuativa – la continuità del rapporto di collaborazione sussidiaria, come tale produttiva di integrazione di attività, risorse, anche immateriali, qualificazione della spesa e, da ultimo, costruzione di politiche pubbliche condivise e potenzialmente effettive, oltre alla produzione di clima di fiducia reciproco».

Allo stesso modo, la generazione di un clima di fiducia è più volte ribadita nel DGA (cfr. *considerando* nn. 5, 23, 24, 32 DGA), ma era già chiaramente stabilito come obiettivo del GDPR (*considerando* n. 7 GDPR).

[43] Su questo profilo, con riguardo all'amministrazione condivisa, cfr. in part. M. BOMBARDELLI, *L'organizzazione dell'amministrazione condivisa*, cit., p. 141 ss. e F. GIGLIONI, *Forme e strumenti dell'amministrazione condivisa,* spec. p. 75 ss., entrambi in G. ARENA-M. BOMBARDELLI (a cura di), *L'amministrazione condivisa*, cit.; S. PELLIZZARI, *Coprogettazione tra PA ed ETS nel diritto amministrativo*, in S. PELLIZZARI-C. BORZAGA (a cura di*), Terzo settore e pubblica amministrazione*, cit., p.

4. Le cooperative di dati nell'amministrazione condivisa.

Posta questa comunanza tra i due modelli occorre interrogarsi su come le cooperative di dati possano rivelarsi uno strumento utile per rafforzare le attuali prassi di amministrazione condivisa o per avviarne di nuove.

Tale punto richiede, tuttavia, di considerare partitamente i due filoni in cui si articolano le pratiche di amministrazione condivisa [44].

All'amministrazione condivisa, infatti, possono essere ricondotte sia l'esperienza dei regolamenti comunali per la gestione condivisa dei beni comuni sia le forme di collaborazione tra pubblica amministrazione e terzo settore.

In entrambi i casi, come si vedrà, le cooperative di dati possono rappresentare uno strumento efficace per affrontare le sfide che la transizione digitale pone al modello dell'amministrazione condivisa.

4.1. Le cooperative di dati nell'amministrazione condivisa dei beni comuni.

Con riguardo alla gestione condivisa dei beni comuni è opportuno fornire alcune coordinate di fondo [45]. Tale modello si sviluppa attraverso prassi regolate da re-

---

41 ss., mentre, con riferimento alle cooperative di dati, si v. G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit., p. 995. Si consideri, inoltre, S. VILJOEN, *A Relational Theory of Data Governance*, in *Yale Law Journal*, 2021, Vol. 131, n. 2, pp. 573, spec. 607 ss. rispetto al rilievo delle dinamiche relazionali orizzontali che dovrebbero ispirare la *data governance*.

[44] Per l'individuazione di due gruppi di prassi di amministrazione condivisa si v. V. CERULLI IRELLI, *L'amministrazione condivisa nel sistema del diritto amministrativo*, cit., p. 26 ss.

[45] In generale, su tale modello cfr. G. ARENA, *I custodi della bellezza. Prendersi cura dei beni comuni. Un patto per l'Italia fra cittadini e le istituzioni*, Milano, 2020; M. BOMBARDELLI, *La cura dei beni comuni: esperienze e prospettive*, in *Gior. dir. amm*., 2018, 5, p. 559 ss.; E. CHITI, *La rigenerazione di spazi e beni pubblici*, in F. DI LASCIO-F. GIGLIONI (a cura di), *La rigenerazione di beni e spazi urbani. Contributo al diritto delle città*, Bologna, 2017, p. 15 ss.; F. DI LASCIO, *Spazi urbani e processi di rigenerazione condivisa*, *ivi*, p. 65 ss.; R. TUCCILLO, *Rigenerazione dei beni attraverso i patti di collaborazione tra amministrazione e cittadinanza attiva: situazioni giuridiche soggettive e forme di responsabilità*, *ivi*, p. 89 ss.; R. DIPACE, *Le politiche di rigenerazione dei territori tra interventi legislativi e pratiche locali*, in *Ist. Fed*., 2017, 3, pp. 640-641; D. DONATI, *Le città collaborative: forme, garanzie e limiti delle relazioni orizzontali*, in *Ist. Fed.*, 2019, 4, p. 964 ss.; ID., *Dai beni comuni al benessere comunitario. Evidenze, incertezze e limiti di un concetto sotto osservazione*, in ID. (a cura di), *La cura dei beni comuni tra teoria e prassi. Un'analisi interdisciplinar*e, Milano, 2024, p. 21 ss.; E. FIDELBO, *Strumenti giuridici di valorizzazione del rapporto tra patrimonio culturale e territorio: il caso dei patti di collaborazione tra amministrazioni locali e cittadini*, in *Aedon*, 2018, 3, p. 13 ss.; G. FIDONE, *Proprietà pubblica e beni comuni*, Pisa, 2017, p. 41 ss.; F. GIGLIONI, *Forme e strumenti dell'amministrazione condivisa*, cit., p. 85 ss.; C. TUBERTINI, *Sviluppare l'amministrazione condivisa attraverso i principi di sussidiarietà (verticale) e leale collaborazione: riflessioni e proposte*, in *Ist. Fed.*, 2019, 4, p. 971 ss.; C. DE LUCA*, La ri-generazione urbana come laboratorio di cittadinanza attiva*, in M. PASSALACQUA-A. FIORITTO-S. RUSCI, *Ri-conoscere la Rigenerazione. Strumenti giuridici e tecniche urbanistiche*, Sant'Arcangelo di Romagna, 2018, p. 309 ss.; A. GIUSTI, *La rigenerazione urbana. Temi, questioni e approcci nell'urbanistica di nuova generazione* Napoli, 2018, p. 138 ss.; P. MICHIARA, *Tipicità e autonomia nella regolamentazione della cittadinanza attiva*, in P. CHI-

golamenti comunali e patti di collaborazione. I regolamenti forniscono la cornice entro cui possono collocarsi attività di cura dell'interesse generale. Sulla base dei regolamenti, adottati da Comuni, l'amministrazione comunale e i cittadini sono abilitati a sottoscrivere patti di collaborazione per la gestione dei beni comuni. È bene precisare, tuttavia, che i beni comuni urbani oggetto di cura secondo i vari regolamenti possono essere materiali, immateriali e digitali.

La prassi mostra esperienze molto eterogenee di amministrazione dei beni comuni così intesi: si va dal recupero di immobili in disuso alla gestione del verde pubblico, fino anche alla gestione di attività involgenti il riciclo [46].

È piuttosto evidente che simili attività non hanno ad oggetto, in genere, l'uso di dati. Sovente, inoltre, queste pratiche non si sviluppano entro ecosistemi digitali.

Tuttavia, i dati e il modello della cooperativa di dati diventano rilevanti qualora si ipotizzino delle piattaforme che siano in grado di offrire servizi alla collettività locale. Tali piattaforme possono infatti assurgere a beni comuni digitali (o *digital commons*) [47] passibili, dunque, per quanto qui interessa, di essere amministrati in modo condiviso. Non si tratta di casi solo ipotetici, ma, a ben vedere, di esperienze in atto nell'ambito di altri ordinamenti.

Si fa riferimento a piattaforme che offrono servizi a privati e che non hanno sempre un legame diretto con l'interesse generale: si pensi alle piattaforme locali dedicate ai trasporti [48], alla condivisione di dati relativi a impianti agricoli [49] o alla gestione di dati sanitari [50].

RULLI-C. IAIONE (a cura di), *La co-città. Diritto urbano e politiche pubbliche per la rigenerazione urbana l'innovazione sociale l'economia collaborativa e i beni comuni*, Napoli, 2018, p. 135 ss.

Se si vuole, si v. pure S. FRANCA, *Cura dei beni comuni e responsabilità condivisa. Spunti ricostruttivi*, in *Munus*, 2018, 1, p. 54 ss.

[46] Per una panoramica in tal senso è sufficiente consultare la pagina web di Labsus nella sezione dedicata ai patti di collaborazione: https://www.labsus.org/category/beni-comuni-e-amministrazione-condivisa/patti-collaborazione/.

[47] Su tale categoria di *commons* cfr. M.M. BÜHLER-I. CALZADA-I. CANE-T. JELINEK-A. KAPOOR-M. MANNAN-S. MEHTA-V. MOOKERJE-K. NÜBEL-A. PENTLAND-T. SCHOLZ-D. SIDDARTH-J. TAIT-B. VAITLA-J. ZHU, *Unlocking the Power of Digital Commons*, cit., spec. p. 151; A. PRADI, *I beni comuni digitali nell'era della proprietà intellettuale*, in A. PRADI-A. ROSSATO (a cura di), *I beni comuni digitali. Valorizzazione delle informazioni pubbliche in Trentino*, Napoli, 2014, p. 18 ss. Rileva puntualmente G. PETTINARI, *Beni comuni, azioni collettive e amministrazione condivisa: un inquadramento della materia. La prospettiva di una lettura dinamica sull'attività*, in D. DONATI (a cura di), *La cura dei beni comuni tra teoria e prassi*, cit., p. 107 che «lo sviluppo tecnologico cambia le condizioni di contesto, quindi, anche le caratteristiche dei beni, dove gli strumenti digitali ampliano le opportunità democratiche». Rispetto alla configurabilità dei dati, personali e non, come beni comuni cfr. da ultimo E. CREMONA, *Quando i dati diventano beni comuni: modelli di* data sharing *e prospettive di riuso*, in *Riv. it. inf. e dir.*, 2023, 2, p. 124 ss.

[48] Il caso più noto è quello di *Driver's seat*. Si tratta di una cooperativa di dati americana che gestisce servizi di *ride-sharing* e *delivering*. I membri della cooperativa tramite un'app possono verificare i dati che li riguardano e che sono oggetto di trattamento, disponendo altresì se e come condividerli. Per maggiori informazioni su questo caso cfr. F. BRAVO, *Le cooperative di dati*, cit., pp. 771-772; E. BIETTI-A. ETXBERRIA-M. MANNAN-J. WONG, *Data Cooperatives in Europe*, cit., p. 8, p. 18.

[49] Rileva il caso di eKutir, un'impresa sociale sita in India che utilizza tecnologie digitali a favore

Queste piattaforme, solitamente, "amministrano" dati per le proprie finalità, ossia, rispettivamente, per gestire per servizi di *ride-sharing* e *delivering* in modo da rendere più efficiente il servizio, per favorire la condivisione di informazioni tra agricoltori e per organizzare i dati sanitari dei cittadini per la fruizione di specifici servizi.

Tuttavia, questi dati possono avere un'utilità ulteriore nel momento in cui vengono messi a disposizione della pubblica amministrazione che può utilizzarli per organizzare i propri servizi. Si pensi all'utilità che i dati relativi al trasporto possono avere per la gestione del traffico in un contesto locale.

Le cooperative di dati, in questo quadro, possono fungere da canale di comunicazione tra gli utenti delle piattaforme e la pubblica amministrazione, verificando che quest'ultima adotti condizioni di trattamento eque, in ciò restando in una dinamica di rapporto bipolare tra cooperative e amministrazione. Tuttavia, se si inserisce l'infrastruttura della cooperativa dei dati all'interno di una prassi di amministrazione condivisa, si può immaginare che i cittadini attivi possano non solo ottenere utilità diretta dalla monetizzazione della comunicazione dei dati o indiretta dal miglioramento del servizio, ma sfruttare le risorse maturate sul piano informativo per strutturare patti di collaborazione con l'amministrazione pubblica in modo da far fronte a bisogni e istanze locali secondo il modello della *smart city* 2.0 [51], operando così una gestione molto più democratica dei dati di quanto non avvenga tramite piattaforme fornite da terzi senza alcun legame con la comunità di riferimento. Per rimanere all'esempio dei trasporti si pensi a come la condivisione di dati con l'amministrazione possa essere coordinata con azioni in cui i cit-

---

di piccoli agricoltori in una prospettiva di sviluppo sostenibile. Rispetto a questa esperienza si v. in particolare M.M. BÜHLER-I. CALZADA-I. CANE-T. JELINEK-A. KAPOOR-M. MANNAN-S. MEHTA-V. MOOKERJE-K. NÜBEL-A. PENTLAND-T. SCHOLZ-D. SIDDARTH-J. TAIT-B. VAITLA-J. ZHU, *Unlocking the Power of Digital Commons*, cit. p. 146 ss.; J. SRIVARDHINI-K.A. PINSONNEAULT-L. DUBÉ, *The Evolution of an ICT Platform-Enabled Ecosystem for Poverty Alleviation: The Case of eKutir*, in *MIS Quarterly* 40, 2, 2016, p. 431 ss.

[50] Si può considerare il caso *di Pc polypoly coop SCE mbH*, una cooperativa di dati di Berlino che dispone di una struttura decentrata per consentire la conservazione, la gestione e l'uso di dati sanitari di cittadini. Allo stesso modo si può considerare *Salus Coop* una cooperativa di dati spagnola che mira a favorire la cessione di dati a ricerche *non-profit* sulla salute. Su questi e altri casi si v., spec. R. LAUER-S. MERKEL-J. BOSOMPEM-H. LANGER-P. NAEVE-B. HERTEN-A. BURMANN-H.C. VOLLMAR-I. OTTE, *(Data-) Cooperatives in health and social care: a scoping review*, in *Journal of Public Health*, 2024; E. BIETTI-A. ETXBERRIA-M. MANNAN-J. WONG, *Data Cooperatives in Europe*, cit., p. 8 ss.

[51] Con tale espressione si allude ad un paradigma di *smart* city più avanzato in quanto fondato sulla necessità di far fronte a istanze sociali tramite un approccio decentro e incentrato sulla comunità di riferimento. Tale modello può portare numerosi benefici, identificando soluzioni innovative che sarebbero altrimenti difficilmente immaginabili, facendo fronte ai bisogni sociali della collettività locale. In tema cfr. F. CREUTZIG, *From smart city to digital urban commons: Institutional considerations for governing shared mobility data*, in *Environ. Res.: Infrastruct. Sustain*., 2021, 1, spec. p. 3; G. TRENCHER, *Towards the smart city 2.0: Empirical evidence of using smartness as a tool for tackling social challenges*, in *Technological Forecasting & Social Change*, 2019, 142, spec. p. 119.

tadini si attivano per iniziative di mobilità sostenibile [52].

È evidente, peraltro, che il ricorso alla cooperativa di dati, nella misura in cui consente di accrescere la consapevolezza degli utenti, così anche da scongiurare derive negative nell'ambito delle *smart cities*, specie qualora si utilizzi l'intelligenza artificiale, in particolare rispetto all'avvio più o meno cosciente di prassi di *social scoring* [53].

Il successo di queste piattaforme e la loro gestione controllata ad opera delle cooperative può consentire di aumentare il bacino di utenza, generando non solo un incremento del patrimonio informativo della cooperativa, ma anche il diffondersi di *best practices* di amministrazione condivisa, capace di riverberarsi in un miglioramento dei servizi offerti dalla p.a. [54].

4.2. Le cooperative di dati nell'amministrazione condivisa tra p.a. e terzo settore.

Il secondo filone relativo all'amministrazione condivisa è quello che si ricollega al fenomeno della collaborazione tra pubblica amministrazione e terzo settore. Questa collaborazione ha radici ben profonde nel nostro ordinamento e ha ricevuto nel tempo riconoscimenti nell'ambito di una legislazione frammentaria [55] sino all'emana-

---

[52] Peraltro, un esempio di mobilitazione per questo scopo si ha già con il Patto di collaborazione #Cambiamolastrada sottoscritto dal Comune di Trento con le associazioni FIAB e Acropoli (maggiori informazioni in tema sono disponibili al seguente link: https://www.comune.trento.it/Aree-tematiche/Beni-comuni/Patti-di-collaborazione-e-adesioni/Patto-di-collaborazione-Cambiamolastrada).

[53] Si allude alla prassi che, tramite l'utilizzo dell'intelligenza artificiale, consente di generare valutazioni classificatorie dei cittadini sulla base di dati raccolti. Si tratta di un fenomeno che ha anche sollecitato la preoccupazione del Garante italiano per la protezione dei dati personali (cfr. il comunicato stampa GARANTE PRIVACY, *"Cittadinanza a punti": Garante privacy ha avviato tre istruttorie. Preoccupanti i meccanismi di scoring che premiano i cittadini "virtuosi"*, 8 giugno 2022). In tema si v., ad esempio, E. DI CARPEGNA BRIVIO, *Pari dignità sociale e* Reputation scoring. *Per una lettura costituzionale della società digitale*, Torino, 2024, p. 130 ss.; G. SCIASCIA, *Reputazione e potere: il* social scoring *tra distopia e realtà*, in *Giorn. dir. amm.*, 2021, 3, p. 317 ss.; A. VIGORITO, *Sul crinale tra data altruism e social scoring: esperienze applicative della sequenza dati-algoritmi nel nuovo contesto regolatorio europeo*, in *MediaLaws*, 2023, 1, p. 104 ss.

[54] Il miglioramento, peraltro, può passare anche attraverso l'elaborazione di atti di *soft law* di autodisciplina in cui si individuano regole per offrire maggiori garanzie nel trattamento dei dati personali. Si tratta, d'altronde, di forme di regolazione *soft* che sono diffuse in diverse realtà locali, ad esempio, in Francia con le *chartes éthiques des données*. Su tali esperienze e sul loro rilievo cfr. U. VERDI, *L'éthique des données dans les chartes éthiques des collectivités territoriales*, in *Communication & Organisation*, 2023, 64, p. 51 ss.

[55] Un primo momento in cui si è superata la frammentarietà della legislazione sui servizi sociali in favore di un sistema integrato è l'emanazione della l. quadro 8 novembre 2000, n. 328. Sulla portata di questa svolta si v. *ex multis* E. FERRARI, *I servizi sociali*, in S. CASSESE, (a cura di), *Trattato di diritto amministrativo. Diritto amministrativo speciale. – Vol. I*, Milano, 2003, p. 891 ss.; S.A. FREGO

zione del codice del terzo settore dove, peraltro, hanno trovato spazio strumenti innovativi come la co-progettazione e la co-programmazione [56]: si tratta di strumenti che permettono agli enti del terzo settore assieme alle pubbliche amministrazioni di definire specifici interventi o anche intere politiche nel campo socio-assistenziale.

Anche in quest'ambito, invero, si possono individuare le potenzialità delle cooperative di dati.

Al terzo settore, infatti, è riconosciuto un ruolo peculiare in base al relativo codice, tanto da permettergli di co-programmare e co-progettare interventi sul piano sociale, in virtù della propria *expertise*. L'esperienza mostra, tuttavia, che la capacità del terzo settore di porsi come interlocutore della pubblica amministrazione, specie rispetto all'attivazione di co-programmazioni, si basa sulla disponibilità di informazioni [57].

Proprio con riguardo alle co-programmazioni, infatti, è importante disporre del *set* informativo che consente di leggere i bisogni della collettività locale. Ovviamente, la disponibilità di dati diviene rilevante anche per la co-progettazione. Benché quest'ultima riguardi solo singoli interventi, a fronte della scarsità delle risorse di cui dispone l'amministrazione è importante che esse siano investite in interventi per cui sussista un effettivo bisogno. Dopotutto, il fatto che l'ente del terzo settore disponga di un quadro informativo sui bisogni più completo, in quanto ente più vicino ai problemi sociali, è ciò che lo legittima maggiormente alla co-progettazione [58].

Le cooperative di dati potrebbero così fornire supporto agli enti del terzo settore rispetto alla raccolta e alla gestione di dati sui bisogni.

In tal modo, i dati raccolti possono poi essere utilizzati nell'ambito di co-progettazioni e co-programmazioni con la pubblica amministrazione.

LUPPI, *Servizi sociali e diritti della persona*, Milano, 2004, p. 85 ss.; A. GUALDANI, *Diritto dei servizi sociali*, Torino, 2018, p. 65 ss.

[56] Su tali istituti cfr. in part. E. FREDIANI, *La co-progettazione dei servizi sociali. Un itinerario di diritto amministrativo*, Torino, 2021, p. 185 ss.; L. GALLI, *La coprogrammazione e la coprogettazione dei servizi di integrazione dei migranti. Paradigmi di coinvolgimento della società civile nei percorsi di inclusione sociale*, Torino, 2022, p. 89 ss.; S. PELLIZZARI, *La coprogettazione come forma di collaborazione tra PA e enti del terzo settore*, in *Munus*, 2019, 2, p. 545 ss.

[57] Rispetto alle co-programmazioni più strutturate è stato rilevato come esse implichino «la conoscenza dei dati e delle buone prassi nazionali e internazionali, la capacità di tracciare, a partire da un adeguato supporto scientifico, gli scenari evolutivi e dunque di immaginare un nuovo assetto del sistema di risposte ai bisogni» (G. MAROCCHI, *Perché la coprogrammazione arranca?*, in *Welforum.it*, 29 febbraio 2024). È evidente che molti dati hanno anche carattere personale e seguono, pertanto, il regime multilivello dettato da GDPR e Codice privacy; in tema cfr. F. MIDIRI, *Protezione dei dati personali e servizi sociali*, in E. CODINI-A. FOSSATI-S.A. FREGO LUPPI (a cura di), *Manuale di diritto dei servizi sociali*, Torino, 2019, p. 402 ss.

[58] Sull'importanza per la co-progettazione del ruolo del terzo settore in quanto soggetto più vicino ai bisogni sociali cfr. L. FAZZI, *Sussidiarietà e coprogettazione: un legame implicito o ancora da costruire?*, in *Impresa Sociale*, 2022, 4, p. 69 ss.; E. FREDIANI, *La co-progettazione dei servizi sociali*, cit., p. 196 ss., che valorizza la funzione informativa del terzo settore; L. GALLI, *La coprogrammazione e la coprogettazione dei servizi di integrazione dei migranti*, cit., p. 26.

Il vantaggio del modello cooperativo, peraltro, sarebbe quello di non considerare i destinatari degli interventi sociali come soggetti passivi, ma come membri della cooperativa di dati, con il riconoscimento e la valorizzazione della loro esigenza di autodeterminazione. In questo modo, potrebbe profilarsi una nuova stagione di collaborazione tra terzo settore e pubbliche amministrazioni nel solco di una maggiore partecipazione anche dei destinatari degli interventi socio-assistenziali. Questi ultimi, grazie all'intermediazione delle cooperative sociali, sarebbero così in grado di "capitalizzare" i propri dati, incidendo sugli interventi e sulle politiche in ambito sociale.

In questo quadro, inoltre, gli enti del terzo settore attraverso la fornitura di servizi di cooperative di dati potrebbero farsi latori delle istanze di innovazione dei servizi sociali offrendo piattaforme decentrate e di rilevanza locale per l'amministrazione dei dati relativi a tali servizi [59], con ciò rafforzando il loro ruolo di interlocutori della p.a. e, in prospettiva, generando un effetto *spillover* rispetto alla diffusione di co-programmazioni e co-progettazioni.

5. Conclusioni.

Come si è cercato di dimostrare, la cooperativa di dati rappresenta uno strumento innovativo che ha numerose potenzialità dal punto di vista dell'amministrazione condivisa.

Già nella prospettiva del rapporto più tradizionale tra amministrazione e amministrati la cooperativa di dati si caratterizza per la capacità di innescare la diffusione di nuovi flussi informativi tra cittadini e soggetti pubblici, in modo funzionale alla gestione delle attività di pubblico interesse e senza passare per l'intermediazione di poteri privati digitali.

Tuttavia, il nuovo istituto pare avere una funzione ancor più rilevante, come fattore di promozione dell'autonoma iniziativa dei cittadini a fronte delle nuove sfide della transizione digitale. La cooperativa di dati, infatti, può rappresentare l'infrastruttura per la gestione dei *digital commons*, in modo da garantire alle collettività locali di mantenere il controllo su piattaforme che producono utilità a livello locale, pure rispetto al perseguimento dell'interesse generale. Anche nell'ambito del rapporto tra amministrazione e terzo settore la cooperativa di dati può rivelarsi particolarmente funzionale a gestire in modo più efficiente il patrimonio informativo degli

[59] Recentemente, sulla rilevanza e sui vantaggi del modello della cooperativa di dati nell'ambito del *nonprofit* cfr. A. FINK, *The Potential of Data Cooperatives in the Nonprofit and Social Service Sectors*, in *Platform Cooperativism Consortium. Blog*, 30 maggio 2024. Sul rilievo della collaborazione tra attori pubblici e privati come elemento che fa emergere la dimensione ecosistemica della transizione digitale si v. B.L. BOSCHETTI, *La transizione della pubblica amministrazione verso il modello Government* as a platform, in A. LALLI (a cura di), *L'amministrazione pubblica nell'era digitale*, Torino, 2022, p. 20 ss.

enti del terzo settore e anche per attivare una nuova stagione collaborativa, che rende più partecipi i soggetti a favore dei quali è svolta l'attività di cura.

Ciò fa emergere, peraltro, la capacità della cooperativa di dati di farsi veicolo delle istanze di solidarietà proprie del tessuto costituzionale italiano [60] e, peraltro, inverate dal DGA anche con riguardo al cd. altruismo dei dati [61]. Anzi, pare proprio che l'importazione della cooperativa di dati nelle prassi dell'amministrazione condivisa possa saldarsi anche a forme di *data altruism*, posto che altruismo dei dati e amministrazione condivisa sono accomunati dal rifuggire una logica meramente sinallagmatica, per favorire iniziative nell'interesse generale [62].

C'è un dato ulteriore da mettere in evidenza e che pare particolarmente importante. Tipicamente, anche se non esclusivamente, il paradigma dell'amministrazione condivisa è stato impiegato per curare nell'interesse generale beni pubblici o privati in stato di abbandono o per cui non si avevano risorse. Le cooperative di dati si mostrano, invece, come strumento utile a raggiungere un obiettivo ancora più ambizioso, ossia quello di portare nell'ambito dell'interesse generale risorse che, tipicamente, sono sfruttate da poteri privati digitali, ma non per finalità di interesse generale, se non indirettamente e comunque in via non principale.

A fronte di questo quadro dai tratti essenzialmente ottimistici, sussistono, nondimeno, una serie di criticità che vanno necessariamente considerate. Se ne individuano almeno tre in questa sede.

In primo luogo, un problema significativo in parte già sollevato *supra* concerne l'incerto regime delle cooperative di dati. Il DGA, infatti, si occupa unicamente di alcune definizioni di massima con riguardo alle cooperative di dati, ma sembrerebbe appiattire queste ultime sul regime generale dei servizi di intermediazione dei dati. In questo modo, l'applicazione del principio di neutralità comporterebbe, come già specificato, un sostanziale depotenziamento rispetto alla cooperativa di dati che non pare ammissibile.

---

[60] In tema cfr. in part. A. PIOGGIA, *La cura nella Costituzione. Prospettive per un'amministrazione della cura*, in G. ARENA-M. BOMBARDELLI (a cura di), *L'amministrazione condivisa*, cit., p. 52 ss.

[61] Sul punto cfr. in part. F. BRAVO, *Il principio di solidarietà tra* data protection *e* data governance, in *Dir. inf.*, 2023, 3, spec. p. 494 ss. Cfr. anche A. ALEMANNO, *Data for Good. Unlocking Privately – Held Data to the Benefit of the Many*, in *European Journal of Risk Regulation*, 2018, 2, spec. p. 190, ove evidenzia il rilievo del *data sharing* rispetto al miglioramento del *welfare*.

[62] Rispetto all'assenza di una logica sinallagmatica nelle prassi di amministrazione condivisa si veda quanto già rilevato *supra* (§ 3). Con riguardo alla logica non sinallagmatica del *data altruism* è sufficiente considerare la definizione ricavabile dall'art. 2, par. 1, n. 16 del DGA ove esso è definito come «la condivisione volontaria di dati sulla base del consenso accordato dagli interessati al trattamento dei dati personali che li riguardano, o sulle autorizzazioni di altri titolari dei dati volte a consentire l'uso dei loro dati non personali, senza la richiesta o la ricezione di un compenso che vada oltre la compensazione dei costi sostenuti per mettere a disposizione i propri dati, per obiettivi di interesse generale, stabiliti nel diritto nazionale, ove applicabile, quali l'assistenza sanitaria, la lotta ai cambiamenti climatici, il miglioramento della mobilità, l'agevolazione dell'elaborazione, della produzione e della divulgazione di statistiche ufficiali, il miglioramento della fornitura dei servizi pubblici, l'elaborazione delle politiche pubbliche o la ricerca scientifica nell'interesse generale».

In secondo luogo, un problema che si profila concerne il coordinamento della disciplina del DGA con quella del GDPR. In effetti, i Garanti europei hanno sollevato dubbi rispetto all'approccio del DGA, anche con riguardo alle cooperative di dati, specie con riferimento alla negoziabilità di certe scelte relative a dati personali [63]. Anche al di là di questo, il DGA non determina il sorgere di basi giuridiche [64], il che rende necessario considerare che ogni flusso di dati personali tramite servizi di cooperative dovrebbe avere una propria base giuridica [65].

Infine, un fattore da considerare, e collegato a quello appena esaminato, concerne il problema della sicurezza dei dati. Si tratta di un tema che, se non affrontato opportunamente, pare suscettibile di minare la svolta legata alle cooperative di dati. Se infatti queste cooperative non sono dotate delle necessarie infrastrutture di sicurezza, il rischio è che il modello della cooperativa di dati diventi progressivamente recessivo. Non è un caso che il DGA richieda che i servizi di intermediazione siano offerti assicurando un livello adeguato di sicurezza (art. 12, par. 1, lett. l), DGA). Se però si pensa ai costi per un fornitore rispetto alla garanzia di un livello di sicurezza adeguato, si intuisce che tale aspetto può rivelarsi problematico per soggetti come le cooperative, ossia organizzazioni che tendono a collegarsi a specifiche comunità e, conseguentemente, ad avere una dimensione tutto sommato ridotta.

In conclusione, il modello delle cooperative di dati rappresenta un ulteriore tassello della via europea all'economia digitale che porta con sé molte potenzialità. Sarà fondamentale, pertanto, far fronte alle diverse sfide che tale innovativo modello pone agli interpreti.

---

[63] Cfr. EDPB-EDPS, *Parere congiunto 03/2021 sulla proposta di regolamento del Parlamento europeo e del Consiglio relativo alla governance europea dei dati* (Atto sulla governance dei dati), vers. 1.1, 9 giugno 2021, p. 8, p. 35.

[64] Cfr. in part. G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit., p. 990, il quale ritiene che questa scelta – unita alla prevalenza in caso di contrasto del GDPR sul DGA – depotenzi fortemente le potenzialità di quest'ultimo.

[65] Con particolare riguardo al caso del consenso e alle criticità che tale base giuridica può comportare a fronte anche della *governance* collettiva della cooperativa cfr. F. BRAVO, *Le cooperative di dati*, cit., spec. p. 789 ss.

Capitolo XXVII

Le cooperative di dati nella pubblica amministrazione italiana: alcune riflessioni in punto di valorizzazione dei dati alla luce del *Data Governance Act* e dell'*AI Act*

Maddalena Ippolito

Abstract: The paper emphasises the centrality of AI and data cooperatives in Italian public administration in the imperative need to facilitate a process of digitalisation and traceability of data, as the result of a transformation oriented at greater verifiability and contestability of the administration's decisions. The observations move in line with numerous European and national initiatives aimed at framing a range of mutations that aim to orient the whole system of administrative automation to implement data cooperatives and digital platforms to ensure the timeliness, security and efficiency of (and in) the processes and services of public administrations. In particular, we see the centrality of data. From this point of view, the use of sophisticated database implies an inevitable balancing act between public interests and the individual's in terms of guarantees of transparency of algorithms, accountability, privacy, security and intellectual property.

1. Premessa.

La centralità dei dati, cui consegue una conoscenza dell'effettiva situazione esistente, ben si concilia con un possibile ripensamento del potere conoscitivo pubbli-

co nell'imperante esigenza di favorire un'amministrazione pubblica digitale e, conseguentemente, l'implementazione dell'intelligenza artificiale nel procedimento amministrativo [1]. Questa tendenza, alla conoscenza di fatti e fenomeni, rappresenta il presupposto per utilizzare il potere pubblico e i dati, «formati, raccolti, conservati, resi disponibili e accessibili con l'uso delle tecnologie dell'informazione e della comunicazione» *ex* art. 50 CAD, consentono la tracciabilità dell'intera vicenda procedimentale garantendone la correttezza e l'esattezza.

Ciò premesso, i dati, intesi come nuovi strumenti dell'amministrazione pubblica digitale, permettono una accorta valutazione della concreta situazione di fatto e il metodo algoritmico, in base alle sue caratteristiche strutturali, in uno con l'implementazione di servizi di intermediazione dei dati (cooperative di dati *ex* art. 2, par. 1, n. 15 del *Data Governance Act*), si prestano ad attingere e a combinare ingenti volumi di dati e di informazioni, di diversa provenienza, ampliando, largamente, le possibilità umane di utilizzo. In tale contesto la capacità *valutazionale* dell'algoritmo, capace di classificare decine di migliaia di casi, che fungono da precedenti applicativi di un enunciato normativo, si dimostra compatibile con l'attività cognitiva, acquisitiva e di giudizio dell'istruttoria affidata ad un funzionario persona fisica, sia nei procedimenti standardizzati sia nei procedimenti a carattere discrezionale, fermo restando un margine di *riserva di umanità*.

Ma è proprio la latitudine del concetto di condivisione dei dati a sancire il perimetro di applicabilità dei "servizi di cooperativa di dati": ora, se la raccolta, la gestione e l'utilizzo dei dati, personali e non personali, tramite la cooperativa di dati estende le possibilità di condivisione e riutilizzo degli stessi, la prospettiva della democrazia partecipata (non mediata), in uno con l'applicazione delle tecnologie emergenti, disegna i confini di applicabilità di siffatti sistemi e ambisce a neutralizzare le problematiche connesse con la protezione dei dati attraverso il coinvolgimento degli interessati e degli intermediari nel controllo dei dati [2].

Nel nostro tempo, nel trattare di questo fenomeno, è necessario volgere uno sguardo al quadro normativo e giurisprudenziale, nazionale e sovranazionale, prodromico all'approvazione del Regolamento Europeo sull'intelligenza artificiale (e al DDL sull'intelligenza artificiale di recente approvazione da parte del Governo italiano) e del *Data Governance Act*, col fine precipuo di coniugare l'innovazione digitale, derivante da un'attività cognitiva più informata e interconnessa, e i servizi di intermediazione dei dati con la tutela della *privacy* sulla scorta delle previsioni del Reg. UE n. 679/2016 (GDPR).

---

[1] Tracce del possibile ripensamento del potere conoscitivo pubblico possono rinvenirsi già nelle acute riflessioni di F. LEVI, *L'attività conoscitiva della pubblica amministrazione*, Torino, 1967, *passim*.

[2] Più in generale, per lucidi rilievi sulla c.d. "cittadinanza attiva", cfr. F. BENVENUTI, *Il nuovo cittadino. Tra libertà garantita e libertà attiva*, Venezia, 1994, *passim*. L'A. discorre della libertà quale libertà attiva della persona in permanente confronto con il potere.

2. Analisi del contesto sotteso alla complessiva presa di posizione dell'Unione Europea in punto di apertura ai dati e al riutilizzo dell'informazione nel settore pubblico attraverso le cooperative di dati e in punto di implementazione dell'AI nell'amministrazione pubblica.

Uno dei fattori che ha contribuito alla crescita delle riforme amministrative, nel nostro Paese, è, senza dubbio, l'internazionalizzazione «che impone, da un lato, di aggiustare i sistemi nazionali a quelli degli altri paesi; dall'altro, di coordinare gli uni con gli altri. Ogni amministrazione nazionale deve adattarsi agli sviluppi delle altre amministrazioni, pena condizioni di svantaggio per i suoi utenti»[3].

In seno alle istituzioni comunitarie, infatti, negli ultimi anni, sono emerse le inarrestabili potenzialità derivanti sia dall'apertura ai dati e al riutilizzo dell'informazione nel settore pubblico (sulla scorta dell'ottavo *considerando* della Direttiva 2019/1024/UE) che dall'implementazione dell'Intelligenza Artificiale (AI)[4] per applicazioni pratiche che migliorino l'operato delle amministrazioni pubbliche, combinando dati di diversa provenienza e garantendone la correttezza e la riutilizzabilità (l'uso delle procedure automatizzate – tecnologie di registro distribuito e intelligenza artificiale – nell'attività amministrativa e l'intermediazione offerta dalle cooperative di dati[5])[6].

In un'ottica di apertura al riutilizzo delle informazioni del (e nel) settore pubblico,

---

[3] Cfr., in tal senso, S. CASSESE, *La semplificazione amministrativa e l'orologio di Taylor*, in *Riv. trim. dir. pubbl.*, 1998, p. 84.

[4] L'intelligenza artificiale fu ampiamente studiata a partire dagli anni '50 del secolo scorso, tant'è che la sua nascita si fa risalire alla Conferenza di Dartmouth del 1956: cfr., per il testo della proposta, J. MCCARTHY-M.L. MINSKY-N. ROCHESTER-C. SHANNON, *A proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, 31 agosto 1955, in *AI Magazine*, 27, 4, 2006, p. 12 ss. Cfr., per un'analisi dei *new risks* per le pubbliche amministrazioni nell'uso dell'AI, A. BARONE, *Amministrazione del rischio e intelligenza artificiale*, in *European Review of Digital Administration & Law – Erdal*, 2020, Vol. 1, Issue 1-2, p. 63 ss.; cfr., altresì, in dottrina M. BASSINI-G. DE GREGORIO-M. MACCHIA-A. PAJNO, *AI: profili giuridici. Intelligenza Artificiale: criticità emergenti e sfide per il giurista*, in *BioLaw Journal – Riv. BioDiritto*, 3, 2019, p. 205 ss.; R. BICHI, *Intelligenza Artificiale tra "calcolabilità" del diritto e tutela dei diritti*, in *Giur. it*., 7, 2019, p. 17 ss.; J. VALERO TORRIJOS, *The legal guarantees of Artificial Intelligence in Administrative Activity: reflections and contributions from the viewpoint of Spanish administrative law and good administration requirements*, in *European Review of Digital Administrative Law – Erdal*, 2020, Vol. 1, Issue 1-2, p. 55 ss.; V. NERI, *Diritto amministrativo e intelligenza artificiale: un amore possibile*, in *Urb. e app.*, 2021, 5, p. 581 ss.

[5] In argomento, in dottrina, cfr. F. BRAVO, *Le cooperative di dati*, in *Contr. e impr.*, 3, 2023, p. 757 ss.; ID., *Intermediazione di dati personali e servizi di* data sharing *dal GDPR al* Data Governance Act, in *Contratto e impresa*, n. 1, 2021, pp. 199-256; L. PETRONE, *Il mercato digitale europeo e le cooperative di dati*, in *Contr. e impr.*, 3, 2023, p. 800 ss.

[6] Per un'analisi delle soluzioni offerte dall'Unione Europea, cfr. AA.VV., *La via europea per l'intelligenza artificiale. Atti del Convegno del Progetto Dottorale di Alta Formazione in Scienze Giuridiche Ca' Foscari Venezia, 25-26 novembre 2021*, a cura di C. Camardi, Milano, 2022.

l'UE adotta, dapprima, la *Public Service Information Directive* (Direttiva 2003/98/CE del 17 novembre 2003) [7] e, successivamente, la Direttiva 2013/37/UE, nell'ambito della quale evidenzia la necessità di aumentare la disponibilità dei dati pubblici "tramite formati aperti e leggibili meccanicamente" che garantiscano l'interoperabilità [8]. A questa linea di tendenza si affiancano alcune previsioni volte a contemperare la trasparenza, derivante dall'accessibilità, dalla riutilizzabilità e dalla fruibilità dei dati [9], con le misure adottate per tutelare la riservatezza degli stessi, in conformità al principio "il più aperto possibile, chiuso il tanto necessario" [10].

Da qui, più di recente, l'intento dell'Unione europea, col fine precipuo di migliorare l'elaborazione di politiche basate sull'ostensione dei dati (*open data oriented*) e aumentare l'efficienza nelle p.a., nonché di rimarcare la necessità di creare un ecosistema tecnologico, sicuro, per la condivisione dei dati tra gli Stati membri: in un primo momento viene adottata la Direttiva UE 2019/1024 che disciplina, in parti-

---

[7] Cfr., in proposito, le osservazioni di B. PONTI, *Il riutilizzo di documenti del settore pubblico*, in *Giorn. dir. amm.*, 2006, 8, p. 817 ss.; S. GIACCHETTI, *Una nuova frontiera del diritto d'accesso: il «riutilizzo dell'informazione del settore pubblico» (direttiva 2003/98/CE)*, in *Cons. Stato*, 2004, 5-6, p. 1245 ss.; C. ALBERTI, E-society *e riutilizzo dell'informazione nel settore pubblico. Disciplina comunitaria e riflessi nazionali*, in *Riv. ital. dir. pubbl. comunit.*, 2005, p. 1237; A. CERRILLO-I. MARTINEZ, *The reuse of Public Sector Information in Europe and its impact on transparency*, in *European Law Journal*, 2012, p. 770 ss.

[8] Così il *considerando* n. 20 della Direttiva 2013/37/UE del Parlamento europeo e del Consiglio, del 26 giugno 2013, che modifica la direttiva 2003/98/CE, relativa al riutilizzo dell'informazione del settore pubblico.

[9] Sulla fruibilità dei dati, cfr. G. CARULLO, *Gestione, fruizione e diffusione dei dati dell'amministrazione digitale e funzione amministrativa*, Torino, 2017, *passim* e, *amplius*, M. FALCONE, *Ripensare il potere conoscitivo pubblico tra algoritmi e big data*, Napoli, 2023, p. 90 s. L'A. precisa che «la generale fruibilità dei dati pubblici pone due necessità (…) la prima è quella di evitare la frammentazione informativa che può scaturire dall'autonomia organizzativa delle amministrazioni ai diversi livelli di governo. I nodi e gli strumenti di gestione dei dati pubblici rientrano pienamente nell'autonomia organizzativa delle amministrazioni, in particolare degli enti territoriali. La seconda necessità è quella di garantire la congruità dei dati e delle informazioni raccolte ai diversi livelli di governo e dalle diverse amministrazioni, sia per l'esercizio di alcuni fondamentali compiti "di sistema" (…) sia per basare la relazione tra i diversi livelli di governo su elementi di razionalità che costituiscono il presupposto indispensabile della leale collaborazione. Tali necessità hanno trovato una considerazione esplicita a livello costituzionale nel riconoscimento in capo al legislatore statale della competenza esclusiva in materia di "coordinamento informativo statistico e informativo dei dati dell'amministrazione statale, regionale e locale"».

[10] L'art. 10 della Direttiva 2019/1024/UE così recita: «gli Stati membri promuovono la disponibilità dei dati della ricerca adottando politiche nazionali e azioni pertinenti per rendere ('politiche di accesso aperto') secondo il principio dell'apertura per impostazione predefinita e compatibili con i principi FAIR. In tale contesto, occorre prendere in considerazione le preoccupazioni in materia di diritti di proprietà intellettuale, protezione dei dati personali e riservatezza, sicurezza e legittimi interessi commerciali, in conformità del principio «il più aperto possibile, chiuso il tanto necessario». Tali politiche di accesso aperto sono indirizzate alle organizzazioni che svolgono attività di ricerca e alle organizzazioni che finanziano la ricerca».

colar modo, gli *open data* intesi come la "pratica di pubblicare dati (grezzi) in modo che siano accessibili, riutilizzabili, leggibili con dispositivi elettronici e concessi in licenza liberamente" e che "possono essere generati da un'ampia gamma di soggetti, tra cui le pubbliche autorità, settore parastatale, imprese e pubblico"; in un secondo momento viene approvato il *Data Governance Act* – DGA (Reg. 2022/868/UE) – entrato in vigore il 24 settembre 2023 – finalizzato a stabilire le condizioni per il riutilizzo dei dati detenuti dagli enti pubblici, nonché volto a creare una base giuridica per gli operatori digitali per la condivisione e lo scambio degli stessi [11].

Il *Data Governance Act* presuppone: una condivisione volontaria dei dati, un uso altruistico finalizzato al perseguimento di obiettivi di interesse generale, cui si affianca la previsione di condizioni «non discriminatorie, proporzionate e oggettivamente giustificate in relazione alle categorie di dati, alle finalità del riutilizzo e alla natura dei dati per i quali è consentito il riutilizzo» (*ex* art. 5, par. 1) [12]; nonché ser-

[11] Cfr., sulla condivisione dei dati, sostenuta dal DGA, per favorire lo sviluppo economico europeo ed il perseguimento di finalità sociali, nel rispetto dei valori della persona, A. MORACE PINNELLI, *Dalla* Data Protection *alla* Data Governance*: il Regolamento UE 2022/868*, in *Nuova giur. civ.*, 2024, 2, p. 486 ss. L'A. precisa che «il DGA è figlio della dialettica tra tutela della persona e libera circolazione dei dati. Benché la parola d'ordine divenga *data sharing*, ad indicare l'esigenza di riutilizzo delle informazioni e della loro condivisione, in vista della creazione di un mercato unico europeo, basato sullo scambio massivo dei dati, personali e di altra natura, le ragioni dell'economia non sbiadiscono la tutela della persona. Il legislatore europeo ha, infatti, chiaramente stabilito la prevalenza del GDPR sul DGA, in caso di conflitto, e ribadito la centralità del rispetto dei diritti fondamentali; d'altro canto lo spazio unico europeo dei dati è immaginato anche nell'ottica della protezione dei soggetti economici deboli e della valorizzazione delle finalità solidaristiche che mirati trattamenti dei dati possono realizzare, nell'interesse generale. Autorevolmente è stata posta in luce l'opportunità di dare vita ad "un sistema di governo dei dati capace di promuovere tanto l'innovazione e l'iniziativa economica, quanto l'interesse generale cui è funzionale l'altruismo dei dati, nel rispetto sempre dei diritti della persona", e come quest'ultimo istituto scardini "un'idea meramente dominicale della protezione dei dati", inducendo l'interprete a valorizzarne la funzione sociale». Sul DGA, cfr., altresì, F. BRAVO, *Data Governance Act and Re-Use of data in the Public Sector*, in *European Review of Digital Administration & Law - Erdal*, 2022, vol. 3, Issue 2, pp. 13-33. L'A. si propone di fornire un'analisi critica del quadro giuridico per il riutilizzo dei dati detenuti dagli enti pubblici, alla luce sia della Comunicazione della Commissione Europea sulla Strategia Europea sui Dati che della nuova Legge Europea sulla *Governance* dei Dati.

[12] In argomento, in dottrina, cfr. S. TRANQUILLI, *Il nuovo citoyen européen nell'epoca del Data governance act*, in *Rivista di digital politics*, 2022, 1-2, p. 179 ss., spec. p. 181. L'A. precisa che «capita molto spesso che i dati in possesso dei soggetti pubblici non riescano poi ad essere condivisi con altre amministrazioni e riutilizzati da quest'ultime per altri fini di interesse generale, quali ad esempio la ricerca scientifica o il miglioramento dei servizi pubblici. Sono invece numerosi i soggetti terzi che (gratuitamente o dietro corrispettivo) nutrono e manifestano un forte interesse a riutilizzare tali dati in modo fruttuoso e potenzialmente innovativo. È agevole quindi comprendere che la spinta del legislatore europeo a creare un quadro regolatorio integrato e uniforme per la gestione del mercato dei dati in possesso dell'amministrazione – specialmente rispetto alle categorie di dati finora esclusi dal "riutilizzo", ossia quelli oggetto di diritto dei terzi – è generata, principalmente, dall'esigenza di rafforzare la sicurezza dei relativi scambi. Il DGA evidenzia, infatti, che, in molti casi, l'utilizzo e il riutilizzo dei dati è possibile solo in un ambiente di trattamento sicuro, predisposto e controllato dalle autorità pubbliche».

vizi di intermediazione dei dati, i c.d. *servizi di cooperative di dati* intesi come «(...) una struttura organizzativa costituita da interessati, imprese individuali o da PMI, che sono membri di tale struttura, avente come obiettivi principali quelli di aiutare i propri membri nell'esercizio dei loro diritti in relazione a determinati dati, anche per quanto riguarda il compiere scelte informate prima di acconsentire al trattamento dei dati, di procedere a uno scambio di opinioni sulle finalità e sulle condizioni del trattamento dei dati che rappresenterebbero al meglio gli interessi dei propri membri in relazione ai loro dati, o di negoziare i termini e le condizioni per il trattamento dei dati per conto dei membri prima di concedere l'autorizzazione al trattamento dei dati non personali o prima che essi diano il loro consenso al trattamento dei dati personali» (*ex* art. 2, par. 1, n. 15 del Reg. 2022/868/UE) [13].

È proprio qui che si innestano alcune riflessioni nell'intento di «plasmare il futuro digitale dell'Europa» [14]: il DGA perviene all'inquadramento delle cooperative di dati quale strumento finalizzato a rafforzare la posizione dei cittadini affinché prendano decisioni consapevoli circa l'utilizzo dei dati. Così come sottolineato dal *considerando* n. 5 del Reg. n. 868/2022, «l'azione a livello dell'Unione è necessaria per aumentare la fiducia nella condivisione dei dati istituendo adeguati meccanismi che garantiscano il controllo da parte degli interessati e dei titolari dei dati sui dati» [15]. Non può non convenirsi che, in un contesto siffatto, l'uso delle coope-

---

[13] Acutamente, su questo profilo, F. BRAVO, *Le cooperative di dati*, cit., p. 757 ss. L'A. sottolinea le peculiarità delle cooperative di dati nel *Data Governance Act* (Reg. UE n. 868/2022) quale «strumento utile per imprese individuali e PMI (…)in grado di orientare l'economia verso una pluralità di mercati, con riduzione dei rischi di monopolizzazione, creando al contempo "pratiche di sostenibilità economica, ambientale e sociale" attraverso il conferimento, alle persone che ne fanno parte, della possibilità di scegliere le azioni da intraprendere in base a valori solidaristici, che spingono l'impresa verso "una modalità generativa e non solo estrattiva dell'economia". (…)le cooperative di dati (…) si pongono come uno strumento perfettamente in grado di dare risposta ad esigenze di "sostenibilità" sul piano economico, sociale e giuridico, attraverso un modello di impresa caratterizzato da solidarietà mutualistica e democraticità, capace però di travalicare la mera riferibilità interna, nella prospettiva di una valorizzazione dei dati che, di necessità, porta a sviluppare la funzione *sociale* dei trattamenti. (…) l'utilizzo dei dati conferiti nelle cooperative di dati, ovviamente, va sempre effettuato nel rispetto delle condizioni di liceità del trattamento previste *ex lege* e dei diritti fondamentali della persona, da conciliare con il sistema di *governance* cooperativo in tale specifico settore».

[14] Cfr., diffusamente, la Comunicazione quadro Plasmare il futuro digitale dell'Europa COM(2020)67, in *www.commission.europa.eu*, 2020.

[15] Il *considerando* prosegue precisando che «un quadro di *governance* a livello dell'Unione dovrebbe avere l'obiettivo di creare fiducia tra gli individui e le imprese per quanto riguarda l'accesso ai dati, la loro condivisione e il loro controllo, utilizzo e riutilizzo, in particolare stabilendo adeguati meccanismi per gli interessati affinché conoscano ed esercitino fattivamente i propri diritti nonché per quanto riguarda il riutilizzo di alcune tipologie di dati detenuti dagli enti pubblici, la fornitura di servizi da parte dei fornitori di servizi di intermediazione dei dati agli interessati, ai titolari e agli utenti dei dati, nonché la raccolta e il trattamento dei dati messi a disposizione a fini altruistici da persone fisiche e giuridiche. In particolare, una maggiore trasparenza per quanto riguarda la finalità dell'utilizzo dei dati e le condizioni in cui i dati sono conservati dalle imprese può contribuire ad aumentare la fiducia».

rative di dati consenta agli individui di compiere scelte informate, prima di acconsentire all'uso/riuso dei dati, in un contesto indirizzato alla trasparenza [16] e all'altruismo dei dati.

Il *Data Governance Act* incide, infatti, proprio in punto di *altruismo dei dati* mediante un primo, sensibile, incremento delle finalità di interesse generale che legittimano l'interesse delle pubbliche amministrazioni alla condivisione dei dati. Divengono rilevanti, ai fini della condivisione, obiettivi quali la ricerca scientifica, l'assistenza sanitaria, la lotta ai cambiamenti climatici e il miglioramento della mobilità. Da ciò non può non inferirsi che il potenziale delle nuove tecnologie, nel contesto del mutualismo digitale, promuove, altresì, una rilettura del concetto stesso di *privacy* in favore di una conoscibilità maggiore dei dati.

Prima di procedere ad una ricognizione delle peculiari (e possibili) modifiche derivanti dal Regolamento di recente conio, appare alquanto impellente l'anticipazione di una valutazione inerente alla natura e alla portata complessiva del medesimo testo normativo. Difatti il Regolamento pare porsi, inesorabilmente, in linea, di sostanziale continuità, rispetto ad ormai sempre più dilaganti tendenze all'accessibilità, pressoché totale, ai dati, veicolate da un linguaggio giuridico contrassegnato dall'ambizione di facilitare e accelerare la circolazione dei dati mediante meccanismi uniformi (mercato unico europeo dei dati) e assicurare che il riuso avvenga in ambiti protetti.

In un simile contesto, nell'ambito dell'ampio programma di riforme delineato dall'incessante processo di digitalizzazione e dal continuo mutamento degli scenari di raccolta e archiviazione dei dati personali, l'Unione europea ha attentamente osservato l'applicabilità delle tecnologie di registro distribuito e, segnatamente, della tecnologia *Blockchain* quale importante guida nel processo di semplificazione/digitalizzazione amministrativa [17] e quale infrastruttura per la fornitura di servizi (nuo-

---

[16] Su questo profilo, cfr. A.G. OROFINO, *L'attuazione del principio di trasparenza nello svolgimento dell'amministrazione elettronica*, in *Judicium*, 2020; ID., *Openness of public data and transparency of administrative action*, in *European Review of Digital Administration & Law – Erdal*, 2022, vol. 3, Issue 2, pp. 51-54.

[17] Per una ricostruzione tecnica della tecnologia *Blockchain*, L. PAROLA, Blockchain *e contratti intelligenti: uno sguardo al mercato dell'energia*, in E. BRUTI LIBERATI-M. DE FOCATIIS-A. TRAVI (a cura di), *Il teleriscaldamento, la* Blockchain *e i contratti intelligenti*, Padova, 2019, p. 93 ss.; F. FAINI, *Il diritto nella tecnica: tecnologie emergenti e nuove forme di regolazione*, in *www.federalismi.it*, 27 maggio 2020, p. 93 ss.; F. SARZANA DI S. IPPOLITO-M. NICOTRA, *Diritto della* Blockchain*, intelligenza artificiale e IOT*, Milano, 2018, p. 23 ss. e M. FAIOLI-E. PETRILLI-D. FAIOLI, Blockchain*, contratti e lavoro. La ri-rivoluzione del digitale nel mondo produttivo e nella PA*, in *Economia e lav.*, 2016, p. 143 ss. Cfr., altresì, O. LASMOLES, *La difficile appréhension des blockchains par le droit*, in *Revue internationale de droit économique*, 2018, 4, p. 453 ss. e B. BARRAUD, *Les blockchains et le droit*, in *Revue Lamy droit de l'immatériel*, 2018, 147, p. 48 ss., ad avviso del quale una *Blockchain* può rievocare (usando una metafora) l'idea di un grande libro contabile aperto e non falsificabile, a libera consultazione e nel quale è possibile scrivere sotto il controllo di tutti, nella consapevolezza di quanto già scritto e che quanto scritto è immodificabile. Una pagina di un libro corrisponderebbe ad un blocco, mentre la sua rilegatura costituirebbe la catena.

vi) secondo i più alti *standards* di sicurezza e *privacy* (nonostante i seppur legittimi dubbi in punto di anonimizzazione dei dati e diritto all'oblio). In questa accezione si inserisce la Risoluzione del Parlamento Europeo del 3 ottobre 2018 sulle tecnologie di registro distribuito e *Blockchain* (2017/2772(RSP)), la quale riconosce che «le potenzialità delle DLT e di *Blockchain* possono costituire uno strumento che rafforza l'autonomia dei cittadini, dando loro l'opportunità di controllare i propri dati e decidere quali condividere nel registro, nonché la capacità di scegliere chi possa vedere tali dati» e sottolinea che le predette tecnologie, in linea con una tendenza alla protezione dei dati, fin dalla fase di progettazione della piattaforma, possono modificare alcuni paradigmi esistenti nel procedimento amministrativo, incentivando la disintermediazione e la decentralizzazione di alcune attività e di alcuni settori al fine di favorire sia la semplificazione dei procedimenti (in particolar modo snellendo la fase istruttoria), sia la partecipazione democratica dei cittadini [18] anche attraverso forme di intermediazione assolte per il tramite di cooperative di dati.

È un approccio, particolarmente innovativo, che si inserisce nel percorso tracciato dalle politiche comunitarie rivolte a riconoscere al *dato* [19] il ruolo di promotore di un "nuovo" rapporto, tra cittadino e pubblica amministrazione, orientato ad una sensibile riduzione dell'asimmetria informativa [20].

Al netto delle – seppur brevi – considerazioni suesposte può riconoscersi che l'importante coinvolgimento europeo, al processo di digitalizzazione delle pubbliche amministrazioni e all'ostensione e al riutilizzo delle informazioni nel settore pubblico, è improntato ad una maggiore trasparenza dei dati (scongiurandone l'uso improprio), con conseguente facilitazione nella condivisione e nello scambio degli

---

[18] Sull'uso delle tecnologie ICT, a supporto dell'attività amministrativa, e sulla necessità di aggiornare gli istituti del procedimento amministrativo, cfr., lucidamente, D.U. GALETTA, *Digitalizzazione e diritto ad una buona amministrazione*, in R. CAVALLO PERIN-D.U. GALETTA (a cura di), *Il diritto dell'amministrazione pubblica digitale*, Torino, 2020, p. 85 ss.

[19] Sulla nozione di dato, cfr. le lucide riflessioni di A. MASUCCI, *Il documento informatico. Profili ricostruttivi della nozione e della disciplina*, in *Riv. dir. civ.*, 2004, 5, p. 749 ss., ad avviso del quale il dato, seppur considerato come sinonimo di informazione è l'elemento di partenza su cui viene elaborata l'informazione; cfr., altresì, G. CARULLO, *Dati, banche dati, blockchain e interoperabilità dei sistemi informativi*, in *Il diritto dell'amministrazione pubblica digitale*, cit., p. 192 s. L'A. precisa che «il termine *dato* può essere definito quale rappresentazione reinterpretabile di informazioni in modo formalizzato, idoneo alla loro comunicazione, interpretazione od elaborazione. Possiamo perciò affermare che il concetto di dato è distinto da quello di informazione, essendo quest'ultima il frutto della reinterpretazione di ciò che è rappresentato dal dato. In altri termini, i dati diventeranno informazioni o conoscenza solo quando sono interpretati da essere umani o, in alcuni casi, da sistemi di intelligenza artificiale. (…) [Q]uando parliamo di dati delle pubbliche amministrazioni ci riferiamo ad un elemento digitale, e quindi immateriale, che permette la memorizzazione e lo scambio di informazioni di qualsiasi tipo».

[20] Cfr., sul ruolo della pubblica amministrazione come intermediario e facilitatore nella circolazione dei dati personali, F. BRAVO-J.V. TORRIJOS, *Data in the public sector and data valorisation*, in *European Review of Digital Administration & Law – Erdal*, 2022, Vol. 3, Issue 2, pp. 5-8.

stessi (previo consenso)[21], e a una maggiore efficacia, a livello procedimentale, perseguibile proprio con il ricorso all'automazione e con l'applicabilità delle cooperative di dati come fonte di approvvigionamento qualificato dei dati da parte delle pubbliche amministrazioni.

3. L'intelligenza artificiale e le cooperative di dati per la pubblica amministrazione italiana: dal quadro normativo e giurisprudenziale di riferimento …

Nel solco delle predette iniziative e in piena sintonia con la tendenza eurounitaria, la normativa italiana e la giurisprudenza amministrativa hanno sviluppato un'attenzione ai dati (*open data*[22], dati pubblici e *big data*[23]), nonché una propensione verso la digitalizzazione dell'attività amministrativa[24] e circa la validità dell'impiego degli

---

[21] Sull'autonomia del consenso, cfr. F. BRAVO, *Le cooperative di dati*, cit., p. 789 ss. Cfr., altresì, ID., *Data Governance Act and Re-Use of data in the Public Sector*, cit., p. 32. L'A. precisa che il responsabile del trattamento, a cui l'interessato ha fornito il consenso al trattamento dei suoi dati personali, non ha il diritto di "scambiare" o "commerciare" i dati personali in un modo che risulterebbe non conforme ai principi e alle norme applicabili in materia di protezione dei dati personali. Una previsione siffatta ben può applicarsi, analogicamente, alle cooperative di dati nella prospettiva qui ricostruita.

[22] Nel nostro ordinamento la definizione giuridica di *open data* è desumibile dall'art. 68, comma 3, D.Lgs. n. 82/2005. Cfr., in dottrina, sugli *open data* come forma di trasparenza proattiva D. MARONGIU, *I dati aperti come strumento di partecipazione*, in D. SORACE-L. FERRARA-S. CIVITARESE MATTEUCCI-L. TORCHIA, (a cura di), *A 150 anni dall'unificazione amministrativa italiana. La tecnificazione*, vol. IV, Firenze, 2017, p. 77 ss.; G.A. CAVALIERE, *Open Data*, in M. IASELLI (a cura di), *La nuova Pubblica Amministrazione. I principi dell'agenda digitale*, Roma, 2014, p. 30 ss.; B. COCCAGNA-G. ZICCARDI, Open data*, trasparenza elettronica e codice aperto*, in M. DURANTE-U. PAGALLO (a cura di), *Manuale di informatica giuridica e diritto delle nuove tecnologie*, Torino, 2012, p. 395 ss.; B. COCCAGNA, *Libero accesso nelle politiche di* open data*: trasparenza, apertura e auto-organizzazione nel riutilizzo delle informazioni del settore pubblico*, in *Ciberspazio e diritto*, 2011, p. 129 ss.; M.C. DE VIVO-A. POLZONETTI-P. TAPANELLI, Open data*, Business intelligence e Governance nella Pubblica amministrazione*, in *Informatica e Diritto*, 2011, p. 239 ss.; F. MARZANO, *La trasparenza nella Pubblica Amministrazione passa dall'*Open Data *o l'*Open Data *passa dalla trasparenza?*, in *Informatica e diritto*, 2011, p. 287 ss.; F. DI MASCIO, *Gli* Open Data *in Italia: Quantità senza Qualità*, in A. NATALINI-G. VESPERINI (a cura di), *Il Big Bang della Trasparenza*, , Napoli, 2015, p. 275 ss.

[23] Cfr., sul punto, *ex plurimis*, G. CARULLO, *"Big data" e pubblica amministrazione nell'era delle banche dati interconnesse*, in *Conc. merc*., 2016, p. 181 ss.; F. COSTANTINO, *Lampi. Nuove frontiere delle decisioni amministrative tra* open *e* big data, in *Dir. amm*., 2017, 4, p. 799 ss.; ID., *Rischi e opportunità del ricorso delle amministrazioni alle predizioni dei "big data"*, in *Dir. pubbl*., 2019, 1, p. 43 ss.; S. FARO-N. LETTIERI, Big Data*: una lettura informatico-giuridica*, in L. LOMBARDI VALLAURI (a cura di), *Scritti per Luigi Lombardi Vallauri*, I, Padova, 2016, p. 503 ss.; A. GIANNACCARI, *La storia dei* Big Data *tra riflessioni teoriche e primi casi applicativi*, in *Conc. merc.*, 2017, p. 307 ss.

[24] Cfr. le autorevoli riflessioni di I.M. DELGADO, *La riforma dell'amministrazione digitale: un'opportunità per ripensare la pubblica amministrazione*, in D. SORACE-L. FERRARA-S. CIVITARESE MAT-

algoritmi informatici [25], nell'ambito dei procedimenti amministrativi, nella consapevolezza di dover bilanciare il diritto all'innovazione tecnologica con un diritto costituzionalmente garantito quale quello alla riservatezza dei dati personali.

Si possono distinguere tre diversi momenti nel rapporto p.a.-nuove tecnologie. Un primo momento in cui si assiste al passaggio dal cartaceo al digitale e alla necessità di conferire una nuova dimensione ai dati; un secondo momento in cui emerge l'esigenza di raccogliere e conservare i dati pubblici in sistemi interoperabili, capaci "di dialogare in forma automatica, scambiando informazioni e condividendo risorse" e in cui si avverte la necessità di porre in evidenza il rapporto tra piena conoscibilità e democrazia attiva (in ossequio al principio di sussidiarietà orizzontale *ex* art. 118, co. 4, Cost.); un terzo momento dove la libera circolazione dei dati pubblici e il progresso cognitivo dell'intelligenza artificiale sembrano dominare (almeno in parte) sull'esistente pur nella consapevolezza di dover coordinare la conoscenza algoritmica e le strategie di comunicazione digitale con la riserva di umanità [26]. Siffatti sistemi rivestendo una pluralità di ruoli differenti, nel ciclo di vita dell'attività amministrativa, si prestano a un possibile utilizzo, in un ecosiste-

---

TEUCCI-L. TORCHIA, cit., p. 133; di G. DUNI, *Amministrazione digitale*, in *Enc. dir.*, Milano, Annali I, 2007, p. 13 ss. e di C. LEONE, *Il ruolo del diritto europeo nella costruzione dell'amministrazione digitale*, in *Riv. it. dir. pubbl. comunit.*, 2014, 3-4, p. 867 ss. Sul processo di transizione digitale della p.a. e sulla relazione innovazione, diritti e nuove disuguaglianze, cfr. P. PIRAS, *L'amministrazione digitale tra divari e doveri. "Non camminare davanti a me, ma al mio fianco"*, in *P.A. Persona e amministrazione*, 2022, 2, p. 417 ss.

[25] Cfr., su questo profilo, A.G. OROFINO-G. GALLONE, *L'intelligenza artificiale al servizio delle funzioni amministrative: profili problematici e spunti di riflessione*, in *Giur. it.*, 2020, 7, p. 1738 ss. e M.C. CAVALLARO-G. SMORTO, *Decisione pubblica e responsabilità dell'amministrazione nella società dell'algoritmo*, in *www.federalismi.it*, 2019, 16, p. 2 ss.

[26] In argomento, prezioso il richiamo a G. GALLONE, *Riserva di umanità e funzioni amministrative. Indagine sui limiti dell'automazione decisionale tra procedimento e processo*, Milano, 2023, *passim*; ID., *Digitalizzazione, amministrazione e persona: per una "riserva di umanità" tra spunti codicistici di teoria giuridica dell'automazione*, in *P.A. Persona e amministrazione*, 2023, 1, p. 329 ss. e, su questi temi, B. MARCHETTI, *La garanzia dello* human in the loop *alla prova della decisione algoritmica amministrativa*, in *BioLaw Journal*, 2021, 2, p. 367 ss. e M. CHIRIATTI, *Incoscienza artificiale*, Milano, 2021, *passim*, che ci ricorda che anche le macchine più intelligenti non possono prendere decisioni che sostituiscono interamente quelle dell'uomo e ne assorbono la capacità di scelta. Cfr., altresì, la Convenzione quadro del Consiglio d'Europa sull'intelligenza artificiale e i diritti umani, la democrazia e lo Stato di diritto. La Convenzione è stata approvata dalla Commissione CAI – *Committee on artificial intelligence* – istituita presso il Consiglio d'Europa in materia di intelligenza artificiale e all'art. 7 e all'art. 15 dispone sulla c.d. riserva di umanità. L'art. 7, rubricato «*Human dignity and individual autonomy*», chiarisce che «*each Party shall adopt or maintain measures to respect human dignity and individual autonomy related to activities within the lifecycle of artificial intelligence systems*»; l'art. 15, rubricato «*Procedural safeguards*», precisa che «*each Party shall ensure that, where an artificial intelligence system significantly impacts upon the enjoyment of human rights, effective procedural guarantees, safeguards and rights, in accordance with the applicable international and domestic law, are available to persons affected thereby. Each Party shall seek to ensure that, as appropriate for the context, persons interacting with artificial intelligence systems are notified that they are interacting with such systems rather than with a human*».

ma digitale, (anche) delle cooperative di dati per la fornitura di un servizio di intermediazione – quale strumento di riduzione, ove necessario, del divario digitale tra p.a. e cittadini – nella produzione di materiali e nella condivisione di contenuti tra gli interessati e le pubbliche amministrazioni che, per il tramite dell'intermediazione della cooperativa, diventano destinatarie dei dati così raccolti per procedere alla loro conservazione e riutilizzo.

In un primo momento, il legislatore nazionale introduce, con il Codice dell'amministrazione Digitale (d.lgs. 7 marzo 2005, n. 82), la nozione di *open data*, *ex* art. 1, co. 1, lett. 1-*ter*, e il principio di fruibilità dei dati che assicura di accedere, direttamente e gratuitamente, alle banche dati di cui sono titolari le p.a., attraverso la predisposizione di accordi quadro (art. 50, co. 2-*ter*, CAD), nel rispetto delle specifiche regole tecniche e infrastrutturali finalizzate a salvaguardare le esigenze di interoperabilità, di coordinamento informativo e di tutela dei dati personali (art. 73, co. 1, CAD). Si inseriscono, in questo stesso contesto, le previsioni dell'atto di recepimento della Direttiva 2003/98/CE, il d.lgs. n. 36/2006, finalizzate alla riutilizzabilità delle informazioni in possesso degli enti pubblici e gli obblighi di trasparenza per le amministrazioni pubbliche, confluiti nel d.lgs. 14 marzo 2013, n. 33. Siffatti istituti vengono interpretati, al pari dell'istituto dell'accesso civico, quali espressione di un *mutamento genetico della pelle dell'amministrazione*[27] volto a favorire una "cultura" della condivisione quale «"punto di confluenza" dei principi giuridici, costituzionalmente posti, dell'azione amministrativa (dal buon andamento all'imparzialità, al rispetto del c.d. "principio di legalità sostanziale", al metodo di partecipazione democratica), dal quale derivano istituti giuridici di tipo trasversale, che possono essere considerati come volti a realizzare la trasparenza»[28].

---

[27] Cfr., in questo senso, F. CARINGELLA, *Profili generali del diritto di accesso*, in F. CARINGELLA-R. GAROFOLI-M.T. SEMPREVIVA (a cura di), *L'accesso ai documenti amministrativi. Profili sostanziali e processuali*, Milano, 2003, p. 4 ss., ad avviso del quale «ben prima del varo della legge 241, il legislatore non ha disdegnato sortite sintomatiche della percezione, pur viziata da settorialità, della necessità di imboccare la strada della pubblicità dell'azione e dell'apparato della pubblica amministrazione. Interventi, non da ultimo, sollecitati da poderose spinte comunitarie verso l'adeguamento delle legislazioni nazionali al principio di ostensibilità dell'*agere* dei pubblici soggetti, nonché dal ritardo cronico del Parlamento nostrano rispetto alle iniziative di Paesi vicini. (…)il salto di qualità è stato finalmente sancito dall'approdo della legge 7 agosto 1990, n. 241 che, nel dare vita ad una rinnovata visione del rapporto tra cittadini e P.A. (…)non ha potuto fare a meno di universalizzare la voglia di accesso dettando una regolamentazione del diritto di informazione amministrativa applicabile indistintamente a tutti i procedimenti amministrativi. Lo strumento dell'accesso, calato nella riscrittura delle regole che presiedono al dipanarsi dell'*iter* procedimentale, diventa un capitolo centrale del più ampio diritto all'informazione amministrativa. Diritto quest'ultimo, maturato sulla scorta della diffusa esigenza di estendere in generale al procedimento amministrativo garanzie proprie del processo giurisdizionale, che vede nell'informazione un ingrediente necessario per rendere operativo nell'*iter* amministrativo lo strumento del contraddittorio, secondo lo schema del *due process of law*, sulla falsariga del principio dell'*audi et altera partem* degli ordinamenti di *natural justice*».

[28] In questi termini cfr., Cons. St., Sez. consultiva atti normativi, 24 febbraio 2016, n. 515. Sulla trasparenza amministrativa la bibliografia è molto ampia: cfr., *ex plurimis*, G. ARENA, *Trasparenza*

In un secondo momento, il costante processo di digitalizzazione procedimentale ha condotto il legislatore, prima, e la giurisprudenza amministrativa, poi, ad impostazioni favorevoli alla definitiva trasformazione della fruibilità dei dati pubblici e alla predilezione della legittimità del ricorso ad algoritmi informatizzati [29]. Nell'intento di valorizzare il principio del *digital first* – quale strumento di promozione verso la transizione al digitale, cui conseguono, indubitabilmente, nuove forme di uso e riuso dei dati e potenziali rischi, nella cura dei contenuti, operata dalle piattaforme digitali – il legislatore nazionale disciplina, con l'art. 8-*ter* del d.l. 14 dicembre 2018, n. 135, convertito in l. 11 febbraio 2019, n. 12, le "tecnologie basate su registri distribuiti" (tra le quali rientra la *Blockchain*) e gli *smart contracts* [30].

L'idea di fondo che attraversa la nuova legge è congeniale all'abbandono del modello tradizionale di amministrazione – con uno sforzo di revisione e di ri-concettualizzazione – propugnando un intervento riformatore, nell'ottica della valorizzazione della disintermediazione, asservito al principio del *trust by computation* [31].

---

amministrativa, in *Diz. dir. pubbl.*, a cura di S. Cassese, VI, Milano, 2006, p. 5945 ss.; F. MANGANARO, *L'evoluzione del principio di trasparenza amministrativa*, in *www.astrid-online.it*, 2009; M. CLARICH, *Trasparenza e protezione dei dati personali nell'azione amministrativa*, in *Foro amm.-TAR*, 2004, 12, p. 3885 ss.; R. VILLATA, *La trasparenza dell'azione amministrativa*, in *Dir. proc. amm.*, 1987, p. 528 ss.; E. CARLONI, *La "casa di vetro" e le riforme. Modelli e paradossi della trasparenza amministrativa*, in *Dir. pubbl.*, 2009, p. 3 ss.; M.R. SPASIANO, *Trasparenza e qualità dell'azione amministrativa*, in *Nuove Autonomie*, 2005, p. 945; V. FANTI, *La pubblicità e la trasparenza amministrativa in funzione del contrasto alla corruzione: una breve riflessione in attesa del legislatore delegato*, in *www.giustamm.it*, 2016, 3; B. PONTI, *La trasparenza ed i suoi strumenti: dalla pubblicità all'accesso generalizzato*, in *La libertà di accesso alle informazioni. Commento sistematico al nuovo decreto 33*, Rimini, 2016, *passim*; V.M. BOMBARDELLI, *Fra sospetto e partecipazione: la duplice declinazione del principio di trasparenza*, in *Ist. federalismo*, 2015, 3-4, p. 657 ss.; M. SAVINO, *Il FOIA italiano. La fine della trasparenza di Bertoldo*, in *Giorn. dir. amm.*, 2016, 5, p. 593 ss.; D.U. GALETTA, *La trasparenza, per un nuovo rapporto tra cittadino e pubblica amministrazione: un'analisi storico-evolutiva, in una prospettiva di diritto comparato ed europeo*, in *Riv. it. dir. pubbl. comunit.*, 2016, 5, p. 1019 ss.; M. RENNA-S. VACCARI, *Dalla "vecchia" trasparenza amministrativa al c.d.* open government, in *www.giustamm.it*, 2019; S. FOÀ, *La trasparenza amministrativa*, in *Dir. amm.*, 2017, 1, p. 65 ss. e, da ultimo, T. ALTI-C. BARBIERI, *La trasparenza amministrativa come strumento di potere e di democrazia*, in *Riv. trim. dir. pubbl.*, 2023, 2, p. 809 ss.

[29] Cfr., in proposito, l'accurata ricostruzione giurisprudenziale operata da M.C. CAVALLARO-G. SMORTO, *Decisione pubblica e responsabilità dell'amministrazione nella società dell'algoritmo*, cit., p. 11 ss. e, sulla questione della discrezionalità come limite all'algoritmo, cfr. E. CARLONI, *I principi della legalità algoritmica. Le decisioni automatizzate di fronte al giudice amministrativo*, in *Dir. amm.*, 2020, 2, pp. 271 ss. spec. 283.

[30] Sul fenomeno *smart contracts*, cfr. *amplius* C. ROBUSTELLA-C.E. PAPADIMITRIU, *Spunti ricostruttivi in tema di* smart contracts, *tra innovazione tecnologica e regola giuridica*, in *P.A. Persona e amministrazione*, 2022, 1, p. 963 ss.

[31] «La scienza della computazione si è sviluppata in modo straordinariamente veloce e l'elaborazione dei *big data* viene fatta mediante la programmazione di un risultato, individuato e raggiunto secondo il grado di certezza proprio dei numeri, palesando una desertificazione della parola che, destrutturata, mette in crisi la sua polisemia, con ricadute rilevanti sul concetto di interpretazione che,

Antecedentemente all'entrata in vigore della predetta legge, il quadro normativo nazionale pareva ignorare – pressoché integralmente – il fenomeno dell'automazione contrattuale e le potenzialità dell'uso degli algoritmi ai fini di una automatizzazione delle attività delle p.a. Diversamente, l'opzione normativa di cui all'art. 8-*ter*, involge l'intero "sistema" di automazione amministrativa, orientandolo all'implementazione di piattaforme tecnologiche. Tali piattaforme offrono una funzione di monitoraggio dell'azione amministrativa, in grado di assicurare maggiore efficienza e celerità nella digitalizzazione dei processi e dei servizi delle pubbliche amministrazioni e maggiore trasparenza dei dati, che rappresentano anche interessi dei cittadini, derivante dalla conoscibilità e riutilizzabilità dei dati inseriti nei registri distribuiti (e ivi condivisi) [32]. Come vedremo, l'approccio seguito dal legislatore, nella disposizione in commento, condivide il complessivo impianto argomentativo posto alla base della Strategia digitale dell'UE e della Strategia europea per i dati 2019-2024, in punto di *data activism* e altruismo dei dati (così come denominata dal *Data Governance Act*) per favorire un miglioramento dei servizi pubblici, sia per soggetti pubblici che privati, e un riutilizzo dei dati, in un sistema sicuro, avvalendosi di tecniche di condivisione e scambio innovative ed efficaci [33].

Vediamo, più nel dettaglio, come l'ordinamento italiano ha sviluppato la trama

---

diventando progressivamente monosemica, afferma un'ermeneutica funzionale univoca. Una volta ideati, gli algoritmi operano con il potere della riduzione computazionale di elementi centrali dell'esistenza e della coesistenza. (…)per l'algoritmo, l'interezza degli elementi elaborati è calcolabile, quantificabile, misurabile secondo un linguaggio numerico. Ma quel che interessa maggiormente è la trasformazione della libertà umana, gli elementi empatici, in quantità calcolabili, trattati dalle procedure algoritmiche, che incidono sulla realtà delle persone destinate ad una produzione di dati serializzati, attraverso una profilazione di massa non immediatamente percepibile, che condiziona e sagoma le azioni della soggettività»: in questi termini L. AVITABILE, *Presentazione*, in B. ROMANO (a cura di), *Algoritmi al potere. Calcolo giudizio-pensiero*, Torino, 2018, p. XIII s. Cfr., altresì, in dottrina M. DURANTE, *Potere computazionale. L'impatto delle ICT su diritto, società e sapere*, Sesto San Giovanni (MI), 2019, *passim*.

[32] Sul punto risulta, di primaria importanza, il Piano triennale per l'informatica nella Pubblica Amministrazione 2020-2022, in *www.agid.gov.it*, 2020, p. 23, che, «coerentemente con quanto previsto dal Modello strategico di riferimento, riprende il concetto di piattaforme della Pubblica Amministrazione: piattaforme tecnologiche che offrono funzionalità fondamentali, trasversali, abilitanti e riusabili nella digitalizzazione dei processi e dei servizi della P.A. (…)Si tratta quindi di piattaforme tecnologiche che nascono per supportare la razionalizzazione dei processi di *back-office* della PA, al fine di migliorare l'efficienza e generare risparmi economici, per favorire la semplificazione e la riduzione degli oneri amministrativi a carico di imprese, professionisti e cittadini, nonché per stimolare la creazione di nuovi servizi digitali. Le piattaforme favoriscono la realizzazione di processi distribuiti e la standardizzazione dei flussi di dati tra amministrazioni». Cfr., in dottrina, G. CARULLO, *L'amministrazione quale piattaforma di servizi digitali*, Napoli, 2022, *passim*, il quale evidenzia che fornire avanzati servizi digitali «pone in capo alle amministrazioni il compito di dotarsi di sistemi informatici in grado sia di informatizzare le fasi interne dell'attività amministrativa, sia di consentire l'interazione a distanza dell'amministrato con l'ente erogatore di una data prestazione».

[33] Nella dottrina giuspubblicistica, cfr., da ultimo, S. TRANQUILLI, *Il nuovo citoyen européen nell'epoca del Data governance act*, cit., p. 180 ss.

argomentativa dell'art. 8-*ter* nella legislazione successiva. Emblematico, sotto il profilo della valorizzazione delle tecnologie basate su registri distribuiti, è l'art. 26 del d.l. n. 76/2020 (Misure urgenti per la semplificazione e l'innovazione digitale), convertito con modificazioni in l. n. 120/2020, il quale, nel disciplinare la piattaforma per le notifiche digitali di atti, provvedimenti, avvisi e comunicazioni della Pubblica Amministrazione [34], dispone che ciascuna amministrazione, nel rispetto delle Linee guida, possa ricorrere alle tecnologie basate su registri distribuiti, tra le quali rientra la *Blockchain*, onde assicurare «l'autenticità, l'integrità, l'immodificabilità, la leggibilità e la reperibilità dei documenti informatici resi disponibili dalle amministrazioni» [35].

In tale direzione, più di recente, l'attenzione rivolta allo sviluppo e alla diffusione delle tecnologie emergenti dell'intelligenza artificiale, dell'internet delle cose (IoT) e della *Blockchain* trova spazio nel d.l. 1° marzo 2021, n. 22, convertito dalla l. 22 aprile 2021, n. 55, che istituisce il Comitato interministeriale della transizione digitale deputato al coordinamento e al monitoraggio dell'attuazione delle iniziative di innovazione tecnologica e transizione digitale delle p.a., e nell'art. 30 del d. lgs. 31 marzo 2023, n. 36 che, al fine di migliorare l'efficienza, statuisce che «le stazioni appaltanti e gli enti concedenti provvedono ove possibile ad automatizzare le proprie attività ricorrendo a soluzioni tecnologiche, ivi incluse l'intelligenza artificiale e le tecnologie di registri distribuiti».

Previsioni siffatte, corollario dell'art. 3-*bis* della l. n. 241/1990 (così come, da ultimo, modificato dal Decreto Semplificazioni), costituiscono operazioni (anche *pro-futuro*) finalizzate a consentire un uso delle DLT per ridurre frodi relative alla procedura e alla documentazione prodotta, accelerando le procedure e riducendo il contenzioso, perlomeno quello che si fonda sulla violazione delle procedure e sulla non autenticità dei documenti [36].

Nel mettere in evidenza le ragioni che consentono di disporre dei dati, a fini altruistici, e di procedere ad un'attività di intermediazione degli stessi, anche attraverso le cooperative di dati e l'interoperabilità offerta da una tecnologia *Blockchain*, pur ammettendo eccezioni alla sua operatività, la struttura argomentativa proposta fa interagire i diritti fondamentali (tra cui spicca il diritto alla riservatezza dei dati), il diritto all'innovazione tecnologica e i servizi di condivisione dei dati, le c.d. cooperative di dati.

---

[34] Cfr., circa il funzionamento della piattaforma, P. CLARIZIA, *La digitalizzazione della pubblica amministrazione*, in *Giorn. dir. amm.*, 2020, 6, p. 775 ss.

[35] Cfr., in dottrina, P. CLARIZIA, *Il decreto n. 76/2020 per la semplificazione e l'innovazione digitale: la pandemia riuscirà dove tutti hanno fallito?*, in *www.irpa.eu*, 8 dicembre 2020.

[36] In argomento, cfr., *ex multis*, A. CORRADO, *I nuovi contratti pubblici, intelligenza artificiale e* blockchain: *le sfide del prossimo futuro*, in *www.federalismi.it*, 2023, 19; G. CARULLO, *Piattaforme digitali e interconnessione informativa nel nuovo Codice dei contratti pubblici*, in *www.federalismi.it*, 2023, 19; P. CLARIZIA, *La digitalizzazione*, in *Giorn. dir. amm*., 2023, 3, p. 302 ss. e G.R. CONFORTI, *Digitalizzazione nel nuovo codice dei contratti pubblici*, in *Diritto di Internet*, 2023, 2, p. 399 ss.

Al contempo, l'indirizzo della giurisprudenza amministrativa – sostenuto dal Consiglio di Stato [37] – procede attribuendo al metodo algoritmico l'indubbio merito di realizzare nuove forme di trasparenza informatica ed enfatizza i vantaggi correlati all'impiego degli algoritmi nei procedimenti amministrativi, a carattere discrezionale, in termini di riduzione della disparità di trattamento, di ampliamento della partecipazione dei soggetti interessati (con conseguente riduzione dell'asimmetria informativa) e di certezza nell'applicazione del diritto.

Con lo scopo precipuo di colmare la lacuna relativa all'impiego dell'intelligenza artificiale nei procedimenti amministrativi discrezionali, il giudice amministrativo individua alcuni elementi di minima garanzia per ogni ipotesi di utilizzo degli algoritmi in sede decisoria pubblica: a) la piena conoscibilità, a monte, del modulo utilizzato e dei criteri applicati che si completa con la comprensibilità e, cioè, con la possibilità di ricevere *informazioni significative sulla logica utilizzata* dall'algoritmo; b) l'imputabilità della decisione dell'organo titolare del potere, il quale deve poter svolgere la necessaria verifica di logicità e legittimità della scelta e degli esiti affidati all'algoritmo [38] e la non esclusività della decisione algoritmica per cui deve, comunque, esistere, nel processo decisionale, un contributo umano capace di controllare, validare ovvero smentire la decisione automatica. In ambito matematico ed informatico, il modello viene definito come HITL (*human in the loop*), in cui, per

---

[37] Cfr. Cons. Stato, Sez. VI, 8 aprile 2019, n. 2270, in *Foro it.*, 2019, 11, p. 606 ss. e in *Giorn. dir. amm.*, 2019, 6, p. 781 ss. con nota di V. CANALINI, *L'algoritmo come "atto amministrativo informatico" e il sindacato del giudice*. In senso conforme, Cons. Stato, Sez. VI, 13 dicembre 2019, n. 8472, in *Giorn. dir. amm.*, 2020, 3, p. 366 ss. con nota di A. MASCOLO, *Gli algoritmi amministrativi: la sfida della comprensibilità*; in *Giur. it.*, 2020, p. 1190 ss. con nota di M. TIMO, *Il procedimento di assunzione del personale scolastico al vaglio del Consiglio di Stato*; in *www.giustamm.it*, con nota di A. SOLA, *La giurisprudenza e la sfida dell'utilizzo di algoritmi nel procedimento amministrativo* e in *Nuova giur. civ.*, 4, 2020, p. 809 ss. con nota di R. MATTERA, *Decisioni algoritmiche. Il Consiglio di Stato fissa i limiti*. Le sentenze citate rappresentano una linea guida per un utilizzo consapevole dell'algoritmo, rispondente ai principi garantistici del procedimento amministrativo. L'organo giudicante, rilevando le potenzialità della rivoluzione digitale, ha evidenziato che «da un lato c'è l'ansia dell'uomo di perdere la propria primazia ontologica a cui è stato sempre abituato, la quale si veste di argomenti razionali (a titolo esemplificativo: la macchina conduce all'oblio dell'essere) (…) dall'altro c'è invece chi intravede nel robot una via d'uscita dalla complessità caratterizzante la società odierna, in grado di trattenerne l'incertezza. E così il robot è visto come uno strumento in grado di correggere le imperfezioni che caratterizzano i processi cognitivi propri della mente umana, di ridurre al minimo i tempi della giustizia, di ridurre il contenzioso pregresso, di rendere le decisioni prevedibili, di svolgere una funzione dissuasiva nei confronti dell'abuso del processo». Cfr., in senso conforme, Cons. Stato, Sez. VI, 4 febbraio 2020, n. 881, in *Giur. it.*, 2020, 7, p. 1738 ss. con nota di A.G. OROFINO-G. GALLONE, *L'intelligenza artificiale al servizio delle funzioni amministrative: profili problematici e spunti di riflessione*.

[38] Cfr., per un quadro sinottico del criterio di imputazione dell'atto amministrativo, M.C. CAVALLARO, *Imputazione e responsabilità delle decisioni automatizzate*, in *European Review of Digital Administration & Law – Erdal*, 2020, Vol. 1, Issue 1-2, p. 71 ss.; A.G. OROFINO-G. GALLONE, *L'intelligenza artificiale al servizio delle funzioni amministrative: profili problematici e spunti di riflessione*, cit., M.C. CAVALLARO-G. SMORTO, *Decisione pubblica e responsabilità dell'amministrazione nella società dell'algoritmo*, cit.

produrre il risultato, è necessario che la macchina interagisca con l'essere umano [39]; e c) la non discriminazione algoritmica, finalizzata a garantire che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori al fine di garantire la sicurezza dei dati personali.

Risulta lampante l'enfasi posta sulla sicurezza dei dati che riceve una forte accentazione proprio nel contesto del *Data Governance Act* in cui il nuovo sistema di *governance* dei dati si confronta con le effettive possibilità di riutilizzo degli stessi, anche presso le pubbliche amministrazioni, e l'attività di intermediazione dei dati è chiamata a convivere con le peculiari caratteristiche strutturali delle piattaforme interoperabili.

Ciò premesso, l'implementazione di detti sistemi procede prendendo atto dell'esigenza di contribuire a indirizzare l'attività amministrativa al principio di legalità [40], ai criteri di efficienza, economicità ed efficacia e a promuovere nuove forme di trasparenza amministrativa tenendo conto dei profondi cambiamenti tecnologici e sociali derivanti dall'utilizzo (e riutilizzo) dei dati.

È proprio il percorso tracciato, nell'esperienza italiana, in punto di dilatazione della portata del riutilizzo/fruibilità dei dati pubblici, che favorisce l'armonizzazione della normativa nazionale alle politiche europee e, segnatamente, al Regolamento n. 679 del 2016 (GDPR) e alla COM(2017) 9 final volta a "Costruire un'economia dei dati europei", secondo la quale i *dati aperti* rafforzano la trasparenza e la responsabilità dei governi e stimolano l'offerta di servizi *online*, innovativi ed efficienti, da parte degli operatori privati [41]. Colpisce, in questo contesto, l'impronta comunitaria, anche nell'opzione normativa assunta, all'art. 50-*ter* del d. lgs. 13 dicembre 2017, n. 217, che ha istituito la Piattaforma Nazionale Digitale Dati (d'ora in poi PDND [42]): la piattaforma è intesa quale «infrastruttura tecnologica che rende possibile l'interoperabilità dei sistemi informativi e delle basi di dati delle pubbliche amministrazioni e dei gestori di servizi pubblici» [43]. Tale modello appli-

---

[39] Così Cons. Stato, Sez. VI, 4 febbraio 2020, n. 881.

[40] Sul punto cfr., *amplius*, F. CARDARELLI, *Amministrazione digitale, trasparenza e principio di legalità*, in *Dir. inf.*, 2015, 2, p. 227 ss.

[41] Sul valore polisemico dei dati (personali e non), cfr., ampiamente, F. BRAVO-J.V. TORRIJOS, *Data in the public sector and data valorisation*, cit., p. 7.

[42] Per una ricostruzione dell'assetto normativo relativo alle infrastrutture digitali nazionali strategiche e sul caso della Piattaforma digitale nazionale dati (PDND), cfr. A. SANDULLI, *Lo "Stato digitale" pubblico e privato nelle infrastrutture strategiche*, in *Riv. trim. dir. pubbl.*, 2021, 2, p. 513 ss. Cfr., altresì, in argomento P. FALLETTA, *Lo "Stato digitale". La trasparenza amministrativa in rete: le nuove piattaforme digitali per la diffusione di contenuti informativi*, in *Riv. trim. dir. pubbl.*, 2021, 2, p. 559 ss.; ID., *La riforma delle amministrazioni pubbliche, tra piattaforme interoperabili e atti amministrativi digitali*, in *www.federalismi.it*, 2023, 31; G. STRAZZA, *I dati aperti in Italia: un focus sull'*openness *digitale dei Comuni*, in *www.federalismi.it*, 2022, 34.

[43] Cfr., in proposito, l'accurata ricostruzione operata da M. FALCONE, *Ripensare il potere conoscitivo pubblico tra algoritmi e big data*, cit., p. 251 ss., ad avviso del quale «il primo grande effetto di sistema che queste riforme hanno avuto è stata la definitiva trasformazione della declinazione tradi-

cativo, favorendo l'analisi dei *big data*, prodotti dalle amministrazioni, per l'elaborazione di politiche *data-driven*, comporta non solo una sensibile riduzione dei tempi di gestione dei processi delle pubbliche amministrazioni quanto, soprattutto, apprezzabili esiti in punto di condivisione generalizzata dei dati e di miglioramento dei servizi ai cittadini attraverso l'implementazione di un sistema informativo unitario pubblico.

La previsione di un siffatto sistema di condivisione dei dati pubblici – emerso nel Codice dell'amministrazione digitale (così come integrato, anche, con il d. lgs. 13 dicembre 2017, n. 217) e nel d. lgs. 24 gennaio 2006, n. 36 sul riutilizzo dell'informazione pubblica – incoraggia lo sviluppo e la diffusione di sistemi di intelligenza artificiale e di piattaforme interoperabili che consentano, tra le altre, una sorta di conservazione digitale, (de)centralizzata e interconnessa, dei dati con un ampliamento esponenziale della base conoscitiva di cui le pubbliche amministrazioni possono avvalersi nelle diverse fasi procedimentali.

Nel mettere in evidenza le ragioni che consentono l'utilizzo di sistemi automatizzati è possibile, a partire dal *Data Governance Act*, sviluppare una struttura argomentativa che favorisce l'interazione tra le tecnologie di registro distribuito e le cooperative di dati, prestando particolare attenzione alla tutela della riservatezza dei dati personali.

Sintetizzo i passaggi principali.

Sotto il profilo del possibile uso delle tecnologie di registro distribuito e delle cooperative di dati, strumentale alla creazione di una forma di collaborazione/interazione, rientrante nelle maglie della sussidiarietà orizzontale *ex* art. 118, co. 4, Cost., merita di essere rilevato che le recenti innovazioni (succitate) potrebbero manifestarsi quale sede privilegiata per il definitivo superamento dell'annosa sovraordinazione dell'attività amministrativa sui cittadini. L'utilizzo delle tecnologie di registro distribuito rappresenta, in uno con l'intermediazione offerta dalle cooperative di dati, un modello strategico per «migliorare l'efficienza e generare risparmi economici, per favorire la semplificazione e la riduzione degli oneri amministrativi a carico di imprese, professionisti e cittadini, nonché per stimolare la creazione di

zionale del principio di fruibilità dei dati pubblici. Questo è avvenuto a livello nazionale con il d.l. 31 maggio 2021, n. 77, che ha modificato l'art. 50-*ter* del Codice dell'amministrazione digitale e ha reso la Piattaforma Digitale Nazionale Dati (PDND) lo strumento principale di accesso, di condivisione e di utilizzo dei dati pubblici detenuti dalle amministrazioni. La PDND è attualmente il luogo principale, centralizzato e controllato dalla Presidenza del Consiglio dei ministri, all'interno del quale progressivamente dovranno essere accessibili i dati pubblici la cui condivisione è ritenuta determinante per il corretto svolgimento delle funzioni amministrative a partire dai dati contenuti nelle basi di dati di interesse nazionale. Per accedere a questi dati, le amministrazioni dovranno accreditarsi alla piattaforma, sviluppare le interfacce di programmazione delle applicazioni (API) – attraverso le quali accedere e operare all'interno della Piattaforma – e rendere disponibili le proprie basi dati, in modo tale che tutte le altre amministrazioni possano accedervi facilmente. Una condivisione che deve avvenire nel rispetto delle regole tecniche e infrastrutturali del Sistema pubblico di connettività e cooperazione, volte a salvaguardare le esigenze di interoperabilità, di coordinamento informatico e di tutela dei dati personali».

nuovi servizi digitali»[44], favorendo la condivisione di flussi di dati tra amministrazioni, tra amministrazioni e cooperative di dati e tra cooperative di dati e cittadini.

Nel percorso di transizione digitale, per la conservazione dei dati – introdotti direttamente dai cittadini o, previo consenso, dalle cooperative di dati, per ridurre i problemi di validità del consenso acquisito dall'ente pubblico che detiene i dati – si auspica, pertanto, l'introduzione della tecnologia *Blockchain*, quale *database* distribuito (uno strumento di disintermediazione) validamente inserito nell'ambito della gestione e della classificazione dei dati e delle informazioni nella disponibilità delle amministrazioni[45].

Quest'intervento riformatore assicurerebbe un adeguato livello di sicurezza informatica, in linea con le *best practices* nazionali e internazionali, e si inserirebbe nella prospettiva di catalogare e indicizzare i dati secondo i presupposti, le logiche e le modalità sperimentate nel sistema pubblico. E viepiù! Una scelta siffatta, imponendo il ricorso a modelli partecipativi comuni e standardizzati, coinvolgerebbe tutti gli attori – i nodi della catena – in una sorta di cogestione dei dati.

I "nodi della catena", pubbliche amministrazioni, cooperative di dati e cittadini, si impegnano a condividere tutti i dati in loro possesso, la validazione capillare, c.d. *timestamp*, dei dati consente un controllo incrociato e decentralizzato delle operazioni effettuate e l'immutabilità dei dati, inseriti nel registro distribuito, unitamente all'uso della crittografia asimmetrica, rende particolarmente difficoltosa ogni indebita alterazione successiva o violazioni ai requisiti del consenso.

In un contesto siffatto, l'inserimento delle recenti innovazioni tecnologiche potrebbe progredire simultaneamente alle nuove forme di interconnessione/interoperabilità tra cittadini e pubblica amministrazione, nonché ai servizi offerti dalle cooperative di dati, offrendo un alto grado di trasparenza nelle interazioni reciproche e una disintermediazione dei processi in ossequio (e in attuazione) al principio, costituzionalmente garantito, di sussidiarietà orizzontale *ex* art. 118, co. 4.

Parimenti rilevanti sono le esigenze connesse con l'integrazione del *know-how* del personale, in forza presso gli uffici pubblici, e con l'effettiva disponibilità dei dati predetti, derivante dal superamento delle carenze di infrastrutture digitali negli uffici dell'amministrazione[46]. È indubbio che il c.d. *digital divide* è accentuato dai

---

[44] In questi termini il Piano triennale per l'informatica nella Pubblica Amministrazione 2020-2022, in *www.agid.gov.it*, 2020, p. 23.

[45] Cfr. M. Macchia, *Blockchain e pubblica amministrazione*, in *www.federalismi.it*, 2021, 2, p. 117, ad avviso del quale «tra *blockchain* e pubblica amministrazione non può mancare il reciproco interesse. La prima consente di ripensare i sistemi di informazione, promuovere fiducia degli utenti e creare nuove opportunità prestazionali. La seconda è sempre affetta da una perenne ansia semplificatoria, di snellimento e di facilità dei rapporti con i cittadini. Se ci si fermasse a questo dato, il matrimonio tra i due non potrebbe ritenersi che a portata di mano».

[46] Cfr., in questo senso, B. Ponti, *Tre scenari di digitalizzazione amministrativa "complessa": dalla interoperabilità predicata alla standardizzazione praticata*, in *Ist. federalismo*, 2023, 3, p. 599 ss., secondo il quale «affinché la capacità conoscitiva connessa e potenzialmente abilitata dalla disponibilità di dati in formato digitale possa portare frutti (…) occorre non solo disporre del *know-how*

predetti fattori, cui si sopperisce destinando le risorse (effettivamente disponibili) non solo all'acquisto di macchinari all'avanguardia e all'infrastrutturazione posta a servizio/supporto delle piattaforme interoperabili, ma anche attraverso la previsione di percorsi informativi e di aggiornamento del personale da cui derivi, altresì, la consapevolezza dei rischi discendenti da un uso improprio della tecnica informatica (capacità organizzative dell'amministrazione e responsabilità/imputabilità delle decisioni automatizzate) [47].

4. … all'algoritmizzazione del procedimento amministrativo e alla conservazione digitale dei dati su piattaforme interoperabili.

Più di recente, l'attenzione si è rivolta – come già anticipato nel paragrafo precedente – a strutturare un avvicinamento all'AI e alle tecnologie di registro distribuito – per le pubbliche amministrazioni e per i cittadini – con una particolare attenzione alla necessaria *reingegnerizzazione* e digitalizzazione dei procedimenti amministrativi e delle procedure di catalogazione, conservazione e condivisione dei dati. Tra le novità più rilevanti si inseriscono, da ultimo, anche i servizi di cooperative di dati quale possibile sistema virtuoso di approvvigionamento dei dati per le pubbliche amministrazioni.

Ora, ferma restando la possibilità di prescrivere taluni accorgimenti circa l'utilizzo delle nuove risorse tecnologiche da parte della p.a. [48], pare evidente che il perimetro di applicabilità delle procedure informatizzate, e con esso degli strumenti per la conservazione digitale dei dati (p.e. l'uso della tecnologia *Blockchain*) e dei servizi di intermediazione di dati, coincida con un regime di pubblicità dei dati orientato alla conoscenza (anche algoritmica).

Fissati sinteticamente tali presupposti diviene indispensabile concentrarsi sugli obiettivi e gli impegni del Piano Nazionale di Ripresa e Resilienza (PNRR) e del Piano Triennale per l'informatica nella Pubblica Amministrazione (2021-2023, prima, e 2024-2026, poi), che trova, tra le sue peculiarità più rilevanti, la previsione di misure per il rafforzamento delle strutture amministrative e di accelerazione e snellimento delle procedure amministrative.

---

relativo al come utilizzare i dati in questo senso, ma occorre, prima ancora (…) disporre effettivamente dei dati, ossia raccogliere e integrare basi di dati».

[47] La Commissione europea, nel suo piano d'azione per l'istruzione digitale 2021-2027, definisce «le competenze digitali come l'insieme di conoscenze, abilità e atteggiamenti per vivere, lavorare, apprendere e prosperare in un mondo sempre più mediato dalle tecnologie digitali (…) l'alfabetizzazione e le competenze digitali sono essenziali e non dovrebbero più essere ignorate. Tali competenze dovrebbero essere costantemente sviluppate di pari passo con l'infrastruttura digitale. Solo in questo modo gli investimenti nella tecnologia si riveleranno efficaci».

[48] Cfr. D.U. GALETTA, Human-stupidity-in-the-loop*? Riflessioni (di un giurista) sulle potenzialità e i rischi dell'Intelligenza Artificiale*, in *www.federalismi.it*, 2023, 5.

L'idea di fondo che attraversa il PNRR [49] è congeniale ad accelerare la digitalizzazione dei servizi pubblici e a semplificare i rapporti tra cittadini e pubblica amministrazione, anche nell'ottica di diffusione della cultura dell'innovazione e superamento del *digital divide*. A ciò non può non aggiungersi che la Missione 1 del Piano, offrendo ampi spazi agli sviluppi dell'intelligenza artificiale, pur non occupandosi del riutilizzo dei dati, si impone di provvedere a un ripensamento delle politiche e delle azioni comuni, in punto di "Digitalizzazione, innovazione, competitività, cultura e turismo": *in primis* offre l'opportunità di intervenire sulla c.d. *democrazia dei dati* nell'ambito della quale la trasformazione digitale si pone come articolata e generale sfida di innovazione del sistema produttivo con conseguente partecipazione (attiva) della società civile; e, *in secundis*, interviene con una necessaria reingegnerizzazione dei procedimenti prevista, tra l'altro, come riforma abilitante nella Parte II del Piano. Alla Missione 1 si affianca la Missione 6 del Piano, che riguarda la Salute, la quale, fornendo una risposta coordinata e senza precedenti dell'Unione alla pandemia da Covid-19, presuppone l'utilizzo di strumenti quali la *Blockchain* e gli *smart contracts* per il futuro dell'*e-health* [50].

Per quanto riguarda il Piano Triennale per l'informatica nella pubblica amministrazione, dai principi guida è possibile cogliere quanto emerge dalla società nella sua dimensione plurale. Il Piano ripensa – tra le altre cose – all'accessibilità ai servizi che devono essere resi accessibili, in via esclusiva, per il tramite dei sistemi di identità digitale (principio del *digital & mobile first*); dispone che le pubbliche amministrazioni devono rendere disponibili a livello transfrontaliero i servizi pubblici digitali rilevanti (principio del transfrontaliero *by design*) e devono evitare di chiedere ai cittadini e alle imprese informazioni già fornite (principio dell'*once only*); e, infine, consacra il patrimonio informativo della pubblica amministrazione quale bene fondamentale per lo sviluppo del Paese, da valorizzare e rendere disponibile ai cittadini e alle imprese, in formato aperto e interoperabile.

L'enfasi posta su una rinnovata forma di conservazione e condivisione digitale dei dati riceve una forte accentazione in recenti progetti dedicati, non a caso, all'uso dei servizi di intermediazione dei dati, le c.d. cooperative di dati, nel contesto della sanità digitale. Non può sottacersi, infatti, il ruolo decisivo giocato dalle cooperative di dati nella raccolta, analisi e condivisione dei dati sanitari, alla ricerca di nuove forme di salvaguardia dei dati personali e di nuove modalità di gestione degli stessi.

In primo luogo, si evidenziano le peculiarità del progetto cooperativa MIDATA che ha previsto la creazione di una piattaforma nell'ambito della quale i titolari

---

[49] Sulla natura del PNRR, M. CLARICH, *Il PNRR tra diritto europeo e nazionale: un tentativo di inquadramento giuridico*, in *www.astridonline.it*, luglio 2021 e in *Corr. giur.*, 2021, 8-9, p. 1025 ss. Cfr., altresì, I. MACRÌ, *Il PNRR italiano per la digitalizzazione e l'innovazione della pubblica amministrazione*, in *Azienditalia*, 2022, 1, p. 38 ss.

[50] In argomento, prezioso è il richiamo a F. CIMBALI, *La* governance *della sanità digitale*, Milano, 2023, *passim*.

dell'*account* contribuiscono, attivamente, alla ricerca medica e agli studi clinici, fornendo un accesso selettivo ai propri dati personali. Allo scopo di salvaguardare i dati personali (sanitari), insiti nelle informazioni condivise, la piattaforma attenziona i soli dati che possono essere utilizzati per scopi comuni assicurando, parallelamente, la protezione degli stessi [51].

Quale "nuova frontiera" per la condivisione e la valorizzazione dei dati sanitari si segnalano, altresì, i meriti del progetto Salus Coop pensato quale sistema di autovalutazione della propria saluta fisica e mentale. Siffatto progetto cooperativo persegue l'obiettivo di legittimare, simultaneamente, il diritto dei cittadini a controllare e condividere i dati sanitari per efficientare la ricerca e innovare il settore (e, conseguentemente, il sistema) sanitario [52].

Come emerge chiaramente, la tesi centrale è che la valorizzazione dei dati sanitari andrebbe intesa in maniera composita, cioè sia in un'ottica di valorizzazione/condivisione del dato sia quale diritto dei cittadini al controllo dei dati personali condivisi, e che esso costituirebbe massima espressione di una rinnovata e proficua forma di cittadinanza attiva. In un approccio siffatto, le cooperative di dati fungono da intermediario, nell'accessibilità e utilizzabilità del dato, nell'ambito di un mercato unico dei dati orientato all'altruismo degli stessi, in ossequio alle previsioni del *Data Governance Act* [53].

Ciò premesso, non pochi sono, inoltre, i possibili vantaggi legati all'approccio sistematico derivante dall'automazione dei processi decisionali attraverso l'implementazione di sistemi interoperabili [54]. Si pensi, nello specifico, allo scambio di dati e di informazioni tra amministrazioni pubbliche, tra amministrazioni pubbliche e cooperative di dati e tra amministrazioni pubbliche e cittadini che, seguendo predefiniti moduli procedimentali e ricorrendo ad asettici calcoli razionali basati esclusivamente sui dati, consentono di velocizzare e semplificare le procedure conferendo una corretta rappresentazione della realtà amministrata. L'implementazione di sistemi informatici comuni, a livello nazionale (e non solo), offre un enorme potenziale analitico volto a riprodurre, in pochi secondi, il processo intellettivo della mente umana: massimizzando l'efficienza e l'efficacia dell'azione amministrativa,

---

[51] Cfr., *amplius*, Salus Coop, in *www.salus.coop*.

[52] Cfr., in argomento, MIDATA, in *www.midata.coop.it*.

[53] Sul principio di solidarietà, come "orizzonte" secondo logiche inclusive di condivisione e altruistiche, nel GDPR e nel Data Governance Act (Reg. UE n. 868/2022), cfr. F. BRAVO, *Il principio di solidarietà tra* data protection *e* data governance, in *Dir. inf.*, 2023, 3, p. 481 ss.

[54] Cfr., in punto di interoperabilità, l'art. 12 CAD, che la identifica come principio dell'amministrazione digitale; l'art. 13-*bis* CAD, introdotto dall'art. 32, co. 4, d.l. n. 76/2020, ove si identifica l'interoperabilità come principio di condotta tecnologica per l'amministrazione digitale; l'art. 54 del Testo Unico sul pubblico impiego, così come integrato dall'art. 4, d.l. n. 36/2022, che introduce l'obbligo per il Codice di condotta di una sezione dedicata al corretto utilizzo delle tecnologie informatiche e dei mezzi di informazione e *social media* da parte dei dipendenti pubblici, anche al fine di tutelare l'immagine della pubblica amministrazione.

le piattaforme interoperabili, in uno con l'intermediazione offerta dalle cooperative di dati, offrono una dinamicità del (e nel) canale di raccolta e conservazione dei dati che, consentendo di estrarre direttamente dal *database* i dati utili, favorisce la fruizione degli stessi per le diverse fasi procedimentali (specialmente per lo svolgimento dell'istruttoria procedimentale). A ciò non può non aggiungersi che l'acquisizione e la memorizzazione dei dati, nonché l'accesso e la capacità di analisi degli stessi, costituiscono gli elementi essenziali per poter offrire un quadro di regole, certe e trasparenti, all'interno delle quali gli operatori e la pubblica amministrazione sono in grado di svolgere le loro funzioni efficacemente.

Proprio muovendo da tali considerazioni, può rilevarsi particolarmente utile tale modello applicativo, fondato sull'accessibilità (pressoché) totale ai dati: siffatto sistema riduce gli atteggiamenti arbitrari, oscuri e irragionevoli attraverso decisioni automatizzate, su situazioni future, basate sulla prevedibilità della risposta amministrativa. Vero è che dal superamento delle sopraccennate variabili, si indirizza il rapporto intercorrente tra tecnologia e diritto al principio di legalità e, conseguentemente, si conferisce un indubbio contributo alla trasformazione digitale, rimarcandosi, altresì, la rilevanza della funzione predittiva dell'intelligenza artificiale, quale strumento idoneo a perseguire la modernizzazione dell'attività e dell'apparato amministrativo.

Per tali ragioni, in un percorso organico di rivisitazione del sistema [55], si potrebbe proseguire con la "ascesa" della transizione digitale [56], il cui processo evolutivo include sia la valorizzazione del principio dell'*once only*, con conseguente sviluppo di reti digitali che consentano una «solida cultura del dato, o meglio una cultura amministrativa che sappia effettivamente amministrare attraverso i dati in possesso delle amministrazioni» [57], sia la valorizzazione di piattaforme interoperabili e di servizi di intermediazione dei dati in grado di procedere alla conservazione (con conseguente diffusione e condivisione controllata) digitale dei dati [58].

---

[55] Cfr., sulle implicazioni dello sviluppo impetuoso dell'A.I. nell'ambito del diritto amministrativo italiano, E. PICOZZA, *Politica, diritto amministrativo* and Artificial intelligence, in *Giur. it.*, 2019, p. 1761 ss.

[56] Per una accorta indagine circa l'impatto delle nuove tecnologie sulla c.d. rivoluzione digitale, cfr. B. BOSCHETTI, *La transizione della pubblica amministrazione verso il modello* Government as a platform, in A. LALLI (a cura di), *L'amministrazione pubblica nell'era digitale*, Torino, 2022, p. 1 ss., la quale osserva che la transizione digitale comporta «una sfida di design non solo tecnologico, ma eticopolitico-normativo fondamentale, di rilievo costitutivo e costituzionale, attraverso cui il sistema giuridico-istituzionale può/deve farsi carico degli effetti di rottura che la rivoluzione digitale ha sin qui prodotto e via via produrrà, anche, e soprattutto, sul piano dell'esperienza umana e delle istituzioni cui questa ha dato vita».

[57] In questi termini, M. FALCONE, *Ripensare il potere conoscitivo pubblico tra algoritmi e big data*, cit., p. 265.

[58] Sul collegamento tra *once only* e interoperabilità, D.U. GALETTA, *Public Administration in the Era of Database and Information Exchange Networks: Empowering Administrative Power or Just Better Serving the Citizens?*, in *European Public Law*, Vol. 25(2), 2019, p. 175 ss. Cfr., nel quadro

5. La valorizzazione dei dati nel Regolamento Europeo sull'intelligenza artificiale e nel DDL sull'AI.

Rispetto allo scenario considerato, il Regolamento europeo sull'intelligenza artificiale si qualifica per la sua capacità di aver ripensato alla rilevanza dei dati per un corretto funzionamento degli strumenti AI a livello comunitario.

L'*AI Act*, il primo Regolamento sull'intelligenza artificiale, viene approvato dal Parlamento europeo il 13 marzo 2024[59]: con tale atto l'Unione europea si impegna, in un progetto di armonizzazione avviato nel 2021 (COM(2021) 206 final del 21 aprile 2021), a disciplinare l'uso dell'intelligenza artificiale, nel rispetto dei diritti fondamentali e della dignità umana, tracciando un percorso, fondato sulla cooperazione internazionale, volto allo sviluppo e alla diffusione di strumenti siffatti.

Occorre, preliminarmente, precisare che il Regolamento definisce, all'art. 3 – *Definizioni* – lett. 1, secondo una nozione ampia, cosa si intenda per sistema di intelligenza artificiale. Trattasi di un «*software* sviluppato con una o più (…) tecniche e approcci (…) che può, per una determinata serie di obiettivi definiti dall'uomo, generare *output* quali contenuti, previsioni, raccomandazioni o decisioni che influenzano gli ambienti con cui interagiscono». Come meglio precisato nel *considerando* n. 6

---

sovranazionale di riferimento, l'*Interoperable Europe Act* entrato in vigore l'11 aprile 2024. L'interoperabilità è intesa come una delle caratteristiche fondamentali del mercato unico digitale, pertanto, nell'ambito del programma di riforme rientrante nel c.d. decennio digitale, si punta ad un'attuazione più efficace delle caratteristiche digitali delle politiche pubbliche, dalla giustizia alla sanità e ai trasporti.

[59] Sul dibattito che ha preceduto l'approvazione dell'*AI Act*, cfr. B. MARCHETTI-L. PARONA, *La regolazione dell'intelligenza artificiale: Stati Uniti e Unione europea alla ricerca di un possibile equilibrio*, in *DPCE online*, 2022, 1, p. 232 ss.; G. FINOCCHIARO, *La regolazione dell'intelligenza artificiale*, in *Riv. trim. dir. pubbl.*, 2022, 4, p. 1090 ss.; D. CHIAPPINI, *Intelligenza Artificiale e responsabilità civile: nuovi orizzonti di regolamentazione alla luce dell'Artificial Intelligence Act dell'Unione europea*, in *Riv. it. di informatica e diritto*, 2022, 2, p. 100 ss.; G. SCHNEIDER, *La proposta di Regolamento europeo sull'intelligenza artificiale alla prova dei mercati finanziari: limiti e prospettive (di vigilanza)*, in *Resp. civ. e prev.*, 2023, 3, p. 1014 ss.; G. RESTA, *Cosa c'è di "europeo" nella Proposta di Regolamento UE sull'intelligenza artificiale?*, in *Dir. inf.*, 2022, 2, p. 323 ss.; E. CARLONI, *Il sentiero si fa camminando: la strategia statunitense per intelligenze artificiali*, in *Giorn. dir. amm.*, 2024, 1, p. 135 ss.; A. AMIDEI, *La governance dell'Intelligenza Artificiale: profili e prospettive di diritto dell'Unione Europea*, in U. RUFFOLO (a cura di), *Intelligenza artificiale – Il diritto, i diritti, l'etica*, Milano, 2020, p. 571 ss.; O. POLLICINO-G. DE GREGORIO-F. PAOLUCCI-F. BAVETTA, *Regolamento AI, la "terza via" lascia troppi nodi irrisolti: ecco quali*, in *www.agendadigitale.eu*, 21 maggio 2021; L. EDWARDS, *Regulating AI in Europe: four problems and four solutions*, in *www.adalovelaceinstitute.org*, 31 marzo 2022; D. MESSINA, *La proposta di regolamento europeo in materia di Intelligenza Artificiale: verso una "discutibile" tutela individuale di tipo consumer-centric nella società dominata dal "pensiero artificiale"*, in *Rivista di diritto dei media*, 2022, 2, p. 196 ss.; C. CASONATO-B. MARCHETTI, *Prime osservazioni sulla proposta di regolamento dell'Unione europea in materia di intelligenza artificiale*, in *BioLaw Journal*, 2021, 3, p. 415 ss.; A. MORESCHINI, *La proposta di Regolamento sull'intelligenza artificiale nel contesto globale*, in *L'amministrazione pubblica nell'era digitale*, cit., p. 145 ss.

del Regolamento «la definizione di sistema di IA dovrebbe essere completata da un elenco di tecniche e approcci specifici utilizzati per il suo sviluppo, che dovrebbe essere tenuto aggiornato alla luce degli sviluppi di mercato e tecnologici mediante l'adozione da parte della Commissione di atti delegati volti a modificare tale elenco».

Tale forma di regolamentazione orizzontale dell'AI, così come meglio chiarito nella Relazione di accompagnamento, persegue obiettivi specifici quali «assicurare che i sistemi di IA immessi sul mercato dell'Unione e utilizzati siano sicuri e rispettino la normativa vigente in materia di diritti fondamentali e i valori dell'Unione; assicurare la certezza del diritto per facilitare gli investimenti e l'innovazione nell'intelligenza artificiale; migliorare la *governance* e l'applicazione effettiva della normativa esistente in materia di diritti fondamentali e requisiti di sicurezza applicabili ai sistemi di IA; facilitare lo sviluppo di un mercato unico per applicazioni di IA lecite, sicure e affidabili nonché prevenire la frammentazione del mercato».

A fronte delle predette precisazioni è opportuno chiarire che il quadro giuridico proposto per l'intelligenza artificiale si contraddistingue per la predeterminazione dei livelli di rischio derivanti dall'implementazione, prima, e dal concreto utilizzo, poi, di sistemi di AI. Conservando un approccio *risk-oriented*[60], (al crescere del rischio consegue un maggior rigore delle regole), con una particolare attenzione nei confronti dei sistemi ad alto rischio, il Regolamento inquadra, nel novero dei predetti sistemi, quelli rientranti tra le componenti di sicurezza di prodotti (o che sono esse stesse prodotti) normalmente soggetti a valutazione della conformità *ex ante* da parte di terzi, nonché quelli che presentano implicazioni in relazione ai diritti fondamentali[61]; al di fuori di queste macroaree, le categorie di rischio vengono qualificate come aventi un rischio minimo, limitato o inaccettabile (manipolazione dei comportamenti delle persone o di gruppi vulnerabili)[62].

---

[60] Cfr. sulla proposta di Regolamento europeo sull'intelligenza artificiale A. INGRAO, Hic sunt leones! *La piramide del rischio costruita dalla proposta di Regolamento sulla intelligenza artificiale (emendata)*, in *Lavoro e prev. Oggi*, 2023, 11-12, p. 778 ss.; G. FINOCCHIARO, *La proposta di regolamento sull'intelligenza artificiale: il modello europeo basato sulla gestione del rischio*, in *Dir. inf.*, 2022, 2, p. 303 ss.

[61] I sistemi di AI ad alto rischio possono essere ricompresi in uno dei seguenti settori: identificazione e categorizzazione biometrica delle persone fisiche; gestione e funzionamento delle infrastrutture critiche; istruzione e formazione professionale; accesso a prestazioni e servizi pubblici e a servizi privati essenziali e fruizione degli stessi; occupazione, gestione dei lavoratori e accesso al lavoro autonomo; gestione della migrazione, dell'asilo e del controllo delle frontiere; amministrazione della giustizia e processi democratici. Cfr., in tal senso, All. 3, Sistemi di IA ad alto rischio di cui all'art. 6, par. 2Allegati della proposta di Regolamento, del Parlamento europeo e del Consiglio, che stabilisce regole armonizzate sull'intelligenza artificiale (Legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione, COM (2021) 206 final, Bruxelles, 21 aprile 2021, in *www.eur-lex.europa.eu*.

[62] «La valutazione del rischio è il cuore dei doveri del titolare. Ciò che va tutelato, insomma, è il rischio che i trattamenti possono comportare per i dati. La stessa valutazione di rischio, tuttavia, non può essere limitata al dato o ai suoi trattamenti. Il rischio va sempre commisurato ai diritti e alle liber-

Con riferimento alle regole di classificazione dei sistemi di AI, di sicuro rilievo, al fine di garantire la stabilità e l'elasticità della disciplina in commento, è il riconoscimento di specifici presupposti che consentono di "spostare" dall'elenco dei sistemi ad alto rischio quelli che, dopo l'immissione e la messa in commercio, non presentano più caratteristiche tali da incidere negativamente sui diritti fondamentali dei cittadini/consumatori dell'Unione. In sostanza, deve essere sempre possibile dimostrare che il sistema di AI non pone più rischi significativi e che la scelta di espungerlo dalla classificazione "ad alto rischio" non comporta la riduzione del livello generale di protezione della salute, della sicurezza e dei diritti fondamentali, a norma del diritto dell'Unione, quanto, piuttosto, la consapevolezza dell'inattualità delle condizioni che legittimavano l'inquadramento nella categoria *High-Risk AI Systems*.

La scelta operata dal Legislatore merita una chiara approvazione nell'ottica della promozione di un utilizzo responsabile dell'AI conforme alle priorità dettate dall'agenda politica europea e nazionale e al ritmo dello sviluppo tecnologico.

Passando al problema dell'efficacia dei sistemi di AI è opportuno sottolineare che l'efficacia dei sistemi di AI è strettamente correlata con la qualità e la quantità dei dati raccolti, condivisi e riutilizzabili e che il già citato approccio *risk oriented* costituisce la base per un insieme proporzionato ed efficace di regole vincolanti.

In una prospettiva armonizzata, ma allo stesso tempo innovatrice, i dati (e la loro fruibilità) non possono prescindere dall'interoperabilità semantica e tecnica con diversi tipi di dati (*ex considerando* n. 81 dell'*AI Act*) "conservati" nei *database* e dall'idea di promuovere un mercato comune europeo dei dati che privilegia sistemi di AI con *data center* unici che garantiscono livelli di sicurezza e protezione dei dati personali all'interno dell'intero spazio economico europeo.

Da ciò si possono trarre alcune riflessioni significative.

La disponibilità di grandi quantità di dati (pur prescindendo dalla qualità degli stessi) può consentire l'addestramento di algoritmi di apprendimento – AI avanzate – da applicare al processo di "ottimizzazione" della pubblica amministrazione, con

---

tà fondamentali delle persone fisiche la cui tutela, per quanto riguarda i loro dati, è l'obiettivo fondamentale del GDPR, anche al fine di garantire lo svilupparsi della fiducia della persona nella società digitale. Sarà sempre meno possibile, infatti, individuare con certezza quando, e per quali finalità, i dati di una persona fisica diventeranno anche oggetto in concreto di un trattamento. Allo stesso modo, sarà sempre più difficile stabilire con sicurezza quando i dati relativi a una persona fisica saranno "oggetto" di un trattamento, e quando invece ne saranno il "prodotto". (…)è il Regolamento stesso che offre la chiave di lettura adatta ad interpretare e attuare le sue norme in modo da proteggere non solo gli "interessati" (cioè coloro a cui si riferiscono dati oggetto di trattamenti per finalità individuate) ma anche e soprattutto le "persone fisiche come tali": tutti coloro, cioè che potranno diventare interessati, ma ancora non lo sono, e coloro i cui dati personali non sono l'oggetto, ma caso mai il prodotto di trattamenti posti in atto. Ed è ancora il Regolamento che, inserendo la valutazione di rischio come parametro fondamentale per la legittimità di ogni trattamento, introduce una visione "dinamica" della tutela, strettamente legata ai rischi che possono correre i diritti e le libertà delle persone»: queste le acute riflessioni di F. PIZZETTI, *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, p. 41 s.

conseguenti positive ripercussioni in punto di neutralità e obiettività del giudizio e garanzia di imparzialità del processo decisionale amministrativo. Le capacità computazionali di siffatte tecnologie consentono, in un sistema *data oriented*, dal punto di vista pratico, la valorizzazione di uno strumento interoperabile e funzionale all'agevole e rapido scambio di dati e informazioni che si muove su un piano armonico rispetto alla sicurezza degli stessi.

Completano il quadro le cooperative di dati. Rispetto alle riflessioni innanzi proposte, non può sottacersi che un dialogo fruttuoso tra *data holder* (il titolare del dato: il cittadino) e *data user* (l'utilizzatore dei dati: le pubbliche amministrazioni) richiede una forte cooperazione basata sul controllo reciproco delle posizioni in conflitto e sullo scambio delle informazioni per l'esercizio dei loro compiti assicurando la coerenza delle decisioni adottate [63]. Entro questo contesto, i servizi di intermediazione tra i titolari dei dati e i potenziali utenti dei dati possono agevolare gli scambi di dati, bilaterali o multilaterali, così come la creazione di piattaforme o banche dati (delle *blockchain*) che consentono lo scambio o l'utilizzo congiunto dei dati.

La strada additata dal *Data Governance Act*, alla luce delle forti accelerazioni tecnologiche degli ultimi anni, e dell'*AI Ac*t, si colloca fra un limite invalicabile di protezione dei dati personali e lo spazio aperto all'uso/riutilizzo dei dati quali/quantitativamente incrementati anche dalle conoscenze offerte dagli intermediari dei dati. Nell'ipotesi configurata, è ravvisabile la possibilità di consentire l'accesso a grandi quantitativi di dati da parte delle cooperative di dati, seppur con le opportune cautele volte ad evitare il rischio di elisione dei principi generali in materia di protezione dei dati personali, che, promuovendo una innovativa forma di *governance* partecipata e condivisa, possono facilitare il processo di disintermediazione e l'implementazione effettiva delle tecnologie di registro distribuito.

Dato questo nucleo minimo, è opportuno sottolineare che l'ultimo atto progettuale, lo Schema di Disegno di Legge recante disposizioni e delega al Governo in materia di intelligenza artificiale, pur ribadendo l'indispensabilità di un utilizzo *antropo-controllato* delle tecnologie emergenti, ne promuove un «utilizzo corretto, trasparente e responsabile, volto a coglierne le opportunità». Le potenzialità dell'in-

---

[63] In argomento, prezioso il richiamo a F. BRAVO, *Intermediazione di dati personali e servizi di* data sharing *dal GDPR al* Data Governance Act, cit., p. 202 ss. L'A., nel delineare il cambio di paradigma nelle strategie dell'Unione, riconosce un innegabile mutamento del linguaggio «fino ad ora l'UE aveva sempre rifiutato di introdurre il concetto di "titolarità" direttamente riferito ai dati: non era considerato «titolare dei dati» né il soggetto a cui si riferisce il dato personale, indicato come «interessato al trattamento di dati personali» – o «*data subject*», nella versione inglese –, né il soggetto che predispone il trattamento dei dati personali per finalità legittime dal medesimo stabilite, indicato come «titolare del trattamento dei dati personali» – o «data controller», nella versione inglese. Mai prima d'ora s'è voluto riferire il concetto di "titolarità" direttamente al dato (e non al trattamento) e ciò denota un cambio di paradigma che rischia di essere un preludio all'introduzione, per via normativa, di una reificazione dei dati personali, quali entità giuridicamente rilevanti *ex se* più che quali attributi della persona. (…)Il mutamento del registro linguistico è un chiaro segno dell'apertura verso un mutamento di paradigma nelle logiche di circolazione dei dati personali».

telligenza artificiale e delle piattaforme interoperabili al servizio delle funzioni amministrative, in punto di efficienza, integrità e innovazione, sono desumibili dalle previsioni dell'art. 13 del DDL AI da cui si fanno discendere anche alcuni profili problematici, derivanti dall'utilizzo di sistemi di AI, quali la necessità di rendere conoscibile il funzionamento dei suddetti sistemi e la possibilità di tracciamento delle decisioni da parte degli interessati. Ciò premesso, sotto il profilo della valorizzazione dei dati, l'art. 8 dispone che i dati, anche personali, trattati «da soggetti pubblici e privati senza scopo di lucro per la ricerca e la sperimentazione scientifica (…) sono dichiarati di rilevante interesse pubblico in attuazione dell'articolo 32 della Costituzione e nel rispetto di quanto previsto nell'articolo 9 del Regolamento UE n. 679/2016». Una precisazione siffatta consente di implementare un modello applicativo fondato sull'accessibilità (quasi) totale ai dati in una prospettiva altruistica volta ad adempiere ad una accorta rendicontazione degli stessi, che, alla luce dei potenziali rischi di compromissione dei dati personali, possono legittimare l'intervento delle cooperative di dati.

6. *AI Act* e GDPR: due regolamenti in costante coordinamento.

L'esigenza di dare piena attuazione all'armonizzazione delle regole sull'intelligenza artificiale e sulla possibile operatività, in contesti siffatti, delle cooperative di dati non preclude alcuni chiarimenti in punto di trattamento dei dati personali, con contestuale ulteriore valorizzazione del dato quale strumento di alimentazione dei sistemi AI (seppur il Regolamento non sia inteso a fornire la base giuridica per il trattamento dei dati predetti).

Il GDPR deriva dalla necessità di creare le condizioni ottimali per lo sviluppo economico degli ambienti digitali nell'ottica della realizzazione del mercato unico europeo in un'Europa fondata sui diritti fondamentali (come previsto dalla Carta UE e dalla CEDU) [64] con una particolare attenzione per i «diritti dei cittadini nella società dell'informazione».

L'infrastruttura dei sistemi di AI, come congegnata a livello comunitario, è addestrata a processare dati di elevata quantità per produrre risultati sulla base di processi di apprendimento propri; l'accuratezza, l'affidabilità e la trasparenza del sistema contribuisce a creare "fiducia" e a garantire eventuali misure a rimedio nella denegata ipotesi di un uso discriminatorio o errato delle informazioni (*id est* dati personali) confluite nel sistema.

Tale ecosistema digitale, pur riconoscendo il trattamento dei dati personali funzionale a processi decisionali automatizzati, sancisce il diritto alla conoscibilità/comprensibilità della decisione automatizzata, il diritto alla revisione umana e

[64] In argomento, cfr. le preziose riflessioni di L. TORCHIA, *Lo Stato digitale. Una introduzione*, Bologna, 2023, 49 s.

il divieto di discriminazione quali elementi minimi di garanzia, sia per confermare la maggior circolazione possibile delle tecnologie e dei dati ivi raccolti, sia per tutelare il diritto fondamentale alla protezione dei dati personali riconosciuto ai residenti nel territorio dell'Unione dalla Carta di Nizza (prima) e dal Trattato di Lisbona (poi).

Secondo questa interpretazione, è di tutta evidenza che lo scopo primario del raffronto tra *AI Act* e GDPR è tracciare una "linea di confine" tra l'uso e la condivisione dei dati, nei sistemi di intelligenza artificiale, e il grado di rischio per i diritti fondamentali (valutando l'uniformità delle disposizioni confluite nell'*AI Act* rispetto ai parametri fissati dal GDPR). In un approccio *risk-based* (l'approccio dell'*AI Act*), il *deployer* (le p.a.), prima di utilizzare un sistema di AI, valuta l'impatto sui diritti fondamentali che l'uso di tale sistema e l'utilizzo dei dati condivisi possa produrre (art. 27, par. 1, *AI Act*).

La condivisione (in uno con la libera circolazione dei dati), il riutilizzo dei dati (auspicata dall'*AI Act*) e l'altruismo dei dati (consacrato nel DGA) si muovono sotto un aspetto parzialmente divaricato, ma inevitabilmente inglobante le prospettive concernenti la protezione dei dati personali nella ricerca (costante) di un equilibrio tra l'AI e la libera circolazione dei dati in armonia con i diritti e le libertà fondamentali [65]. Sotto questo profilo l'impiego di sofisticati canali di raccolta di dati e informazioni implica un inevitabile bilanciamento tra gli interessi pubblici e quelli dell'individuo, in punto di garanzie di specificità del consenso, trasparenza degli algoritmi, *accountability*, *privacy*, sicurezza informatica e proprietà intellettuale. Il presente sistema regolatorio avverte l'esigenza di contemperare la rivoluzione digitale in atto (*big data*, *data analysis*, *machine learning*) con la condizione della persona fisica interessata alla tutela dei propri dati, in qualunque momento, indipendentemente dal fatto che i dati siano o meno oggetto di un trattamento in atto.

Ciò che qui, più in particolare, rileva è quanto, meglio, esplicitato al *considerando* n. 69 dell'*AI Act* secondo il quale «il diritto alla vita privata e alla protezione dei dati personali deve essere garantito durante l'intero ciclo di vita del sistema di IA. A tale riguardo, i principi della minimizzazione dei dati e della protezione dei dati fin dalla progettazione (…)sono applicabili nel trattamento dei dati personali. Le misure adottate dai fornitori per garantire il rispetto di tali principi possono includere non solo l'anonimizzazione e la cifratura, ma anche l'uso di tecnologie che consentano di inserire algoritmi nei dati e di addestrare i sistemi di IA senza trasmissione tra le parti o copia degli stessi dati grezzi o strutturati (…)». Nell'addestrare sistemi di in-

---

[65] Cfr., in dottrina, S. EL SABI, *La tutela della privacy nel trattamento dei dati biometrici e genetici per scopi di pubblica sicurezza. Spunti di diritto comparato*, in *Dir. inf.*, 2023, 4, p. 789 ss.; E. BATTELLI, *Necessità di un umanesimo tecnologico: sistemi di intelligenza artificiale e diritti della persona*, in *Dir. di fam. e delle persone*, 2022, 3, p. 1096 ss.; L. MEGALE, *Il garante della privacy contro Chatgpt: quale ruolo per le autorità pubbliche nel bilanciare sostegno all'innovazione e tutela dei diritti?*, in *Giorn. dir. amm.*, 2023, 3, p. 403 ss.; G. FINOCCHIARO, *Intelligenza Artificiale e protezione dei dati*, in *Giur. it.*, 2019, 7, p. 1657 ss.

telligenza artificiale, conformemente alle previsioni del GDPR, deve, quindi, tenersi conto dei diritti degli interessati, quali il diritto di accesso e il diritto all'oblio [66], nonché fornire informazioni chiare sull'elaborazione dei propri dati nei sistemi di AI.

Dalle riflessioni fin qui condotte, pur rilevando, in questa sede, le indubitabili potenzialità dei sistemi di Intelligenza Artificiale e la, possibile, funzione di intermediazione svolta dalle cooperative di dati, al fine ultimo di elidere i confini della sovraordinazione della p.a., non può sottacersi che la diffusione dei sistemi di intelligenza artificiale avanzata non presuppone la scomparsa degli attori pubblici o l'accantonamento dei poteri unilaterali di matrice autoritativa dell'amministrazione. Per assicurare la coerenza dei sistemi di intelligenza artificiale rispetto alle previsioni normative confluite nel GDPR si applica, inderogabilmente, l'art. 22, comma 1, secondo il quale «l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona» e, sulla medesima falsariga, il *considerando* n. 71 – del medesimo Regolamento – afferma che «l'interessato dovrebbe avere il diritto di non essere sottoposto a una decisione, che possa includere una misura, che valuti aspetti personali che lo riguardano, che sia basata unicamente su un trattamento automatizzato e che produca effetti giuridici che lo riguardano o incida in modo analogo significativamente sulla sua persona».

Per quanto inerisce, invece, la fattispecie che più da vicino impegna le presenti riflessioni, deve rimarcarsi che le cooperative di dati «gestiscono per conto degli interessati del trattamento tutti i diritti degli interessati che il GDPR accorda loro, incluso il diritto al consenso e il diritto alla portabilità dei dati (…) sorgono dunque problemi legati alla tutela dell'interessato contro i rischi di abuso da parte degli *infomediari*» [67].

Tale prospettazione arricchisce gli spazi di operatività delle tecnologie di registro distribuito che procedendo, parallelamente, alla condivisione/riutilizzo e alla crittografia dei dati, immessi nel *database* distribuito, segnano una rigorosa delimitazione dei predetti rischi di abuso.

La trasposizione di tali assunti alle cooperative di dati conduce ad esiti peculiari: le cooperative di dati discendono dall'esigenza di rendere i dati accessibili, per un riutilizzo innovativo finalizzato allo sviluppo dell'intelligenza artificiale, e si pongono quale idoneo punto di riferimento per i cittadini per una tutela più efficace dei loro interessi; l'intelligenza artificiale e le tecnologie di registro distribuito, a loro volta, rappresentano una risposta proattiva alle sfide poste dagli sviluppi tec-

---

[66] Su tale aspetto basti il rinvio a G. BEVIVINO, *Il diritto all'oblio nella società digitale*, in *Il Diritto nell'era digitale. Persona, mercato, amministrazione, giustizia*, Milano, 2022, 37 ss.

[67] Cfr. F. BRAVO, *Intermediazione di dati personali e servizi di* data sharing *dal GDPR al* Data Governance Act, cit., p. 244 s.

nologici e all'aumento quali/quantitativo dei dati condivisi; pertanto, esclusa, a priori, la condivisione di taluni dati intesi come fonte di possibili tensioni tra la protezione dei dati personali e le tecnologie emergenti, gli intermediari e le p.a., accomunati dall'imprescindibile riferibilità dei dati, in loro possesso, ad un ampio novero di destinatari, possono creare una rete decentralizzata nell'ambito della quale consentire l'archiviazione e la condivisione dei dati in modo trasparente e sicuro.

Una scelta siffatta risulta, tra l'altro, coerente rispetto agli *adversarial attacks* o ai possibili attacchi di *data poisoning*: l'*AI Act* e il GDPR operano, congiuntamente, a supporto della tutela della *privacy* in un contesto tecnologico avanzato in cui l'integrazione delle banche dati e l'elaborazione massiva dei dati pongono concreti rischi (in alcune ipotesi rischi sistemici) legati all'applicazione di sistemi di AI mitigabili con *la tutela e la promozione della persona umana* intesa quale *misura e fine dello sviluppo tecnologico* che consente di escludere *in radice che la macchina possa assumere un rilievo diverso da quello di mero* instrumentum *al servizio dell'uomo* dalla quale deriva *la necessità di enucleare, nei diversi campi, una sfera di azione inderogabilmente sottratta all'automazione e riservata all'uomo* [68].

In linea con tale approccio, si chiarisce, altresì, che la sicurezza e la fiducia nel riuso dei dati pubblici è garantita dall'immutabilità dei dati, inseriti nel registro distribuito, che, unitamente all'uso della crittografia asimmetrica, scongiura fenomeni di indebita ingerenza della cooperativa nei dati la cui condivisione, nell'ecosistema tecnologico, è stata acconsentita preliminarmente dal *data holder*. È evidente che l'alterazione retroattiva, ad opera dell'*infomediario*, di un singolo dato, spezzerebbe la catena di blocchi, causando l'inevitabile mutamento dei dati susseguenti cui conseguirebbe l'evidente contrasto con le copie presenti nei restanti "nodi".

Ciò posto si può affermare – sulla scorta delle diverse possibilità di accesso al *database* e del grado di distribuzione dello stesso – l'applicabilità di una *blockchain* ibrida o consortile poiché dotata di un parziale decentramento: i dati possono essere accessibili ad un determinato numero di partecipanti alla catena (i titolari dei dati condivisi e, previo consenso, la collettività), il meccanismo di consenso è, invece, subordinato a una previa identificazione, fondato su un meccanismo basato sull'autorità, sull'identità e la capacità dei singoli "nodi" e controllato da un insieme di nodi preselezionati ovvero le pubbliche amministrazioni e le cooperative di dati.

7. Alcune riflessioni (non) conclusive.

Le riflessioni sin qui condotte assumono particolare pregnanza proprio con riguardo all'incessante processo di implementazione dei sistemi di intelligenza artificiale, nelle pubbliche amministrazioni, per la creazione di una rete nazionale inte-

[68] Quanto riportato in corsivo richiama le condivisibili argomentazioni di G. GALLONE, *Riserva di umanità e funzioni amministrative. Indagine sui limiti dell'automazione decisionale tra procedimento e processo*, cit., p. 35 ss.

roperabile, e sulla incessante valorizzazione dei dati che rappresentano la "bussola" della rivoluzione digitale in atto. La ricognizione delle diverse normative, nazionali e sovranazionali in materia, ripercorre un percorso riformatore culminato con le recenti pagine scritte dal Regolamento sull'AI e dalla Bussola Digitale 2030, a mezzo della quale la Commissione europea ha chiarito che il cambio di paradigma riguarda il «modo in cui i cittadini, le pubbliche amministrazioni e le istituzioni democratiche interagiscono garantendo l'interoperabilità a tutti i livelli di governo e tra i servizi pubblici». Una formulazione che riecheggia la necessità di orientare l'intero sistema di automazione amministrativa all'implementazione di piattaforme digitali che assicurino la tempestività, la sicurezza e l'efficienza dei (e nei) processi e servizi delle pubbliche amministrazioni in «uno spazio sicuro e controllato per la sperimentazione, garantendo nel contempo un'innovazione responsabile e l'integrazione di tutele adeguate e di misure di attenuazione dei rischi»[69].

Dalla sintetica e, a tratti, rapsodica cornice ricostruttiva proposta emergono molteplici spunti di riflessione attinenti all'orizzonte *digitale* che si dischiude dinanzi alle potenzialità dell'intelligenza artificiale. L'idea di fondo dell'amministrazione pubblica digitale è sintetizzabile in questa frase: «*an ecosystem comprised of government actors, non-governmental organisations, business, citizens' associations and individuals which support the production of and access to data, services and content through interactions with the government*» [70].

Ciò posto, le tendenze normative descritte rappresentano, in uno con gli utilizzi concreti delle tecnologie emergenti, le imprescindibili fondamenta dell'analisi che ne è seguita orientata alla valorizzazione del dato, dei sistemi di AI e delle tecnologie di registro distribuito e dell'intermediazione svolta dalle cooperative di dati. Il necessario punto di partenza, di tale sintetica ricostruzione, dell'opzione normativa assunta, poi, dal *Data Governance Act*, è l'altruismo di grandi quantità di dati che ci consente di focalizzare l'attenzione sugli aspetti maggiormente rilevanti ai fini di tale percorso argomentativo.

Il dato, nella ricostruzione operata, «diviene il mezzo attraverso il quale l'amministrazione acquisisce le informazioni necessarie per l'espletamento delle proprie funzioni, così che lo stesso assurge a componente fondamentale dell'azione amministrativa, quale strumento di conoscenza e interpretazione della realtà. Il che significa che il patrimonio di dati delle pubbliche amministrazioni può essere considerato come un'immensa miniera informativa dalla quale i soggetti pubblici possono attingere quanto necessitano per avere una corretta rappresentazione della realtà amministrativa» [71].

---

[69] Così il *considerando* n. 138 dell'*AI Act*.

[70] Così OCSE, *Recommendation of the Council on Digital Government Strategies Digital Government Policy Framework*.

[71] Così, limpidamente, G. CARULLO, *Dati, banche dati, blockchain e interoperabilità dei sistemi informativi*, cit., p. 191 ss.

Risultano evidenti, da quanto sopra osservato, le potenzialità e i notevoli benefici connessi all'impiego e alla crescente diffusione dei sistemi di intelligenza artificiale e le indubitabili potenzialità dell'applicazione della piattaforma *Blockchain* in termini di trasparenza, gestione e conservazione digitale dei dati. Quale canale privilegiato per la raccolta, gestione e utilizzo dei dati, la *blockchain* può rappresentare la sede privilegiata del confronto tra pubbliche amministrazioni e cooperative di dati, per una condivisione e un riuso dei dati, nell'ambito della quale la p.a. dismette la propria sovraordinazione in favore di un più efficace flusso e valorizzazione dei dati.

Le argomentazioni suesposte possono trovare un adeguato riscontro pratico nella creazione di un sistema di gestione-conservazione dei dati, strutturato in un registro distribuito, in cui si sostanzia un rinnovato "patto" tra cittadino e pubblica amministrazione. Un "patto" emancipato rispetto al modello originario di amministrazione centralizzata e inserito in una rinnovata forma di cooperazione, intermediata anche dalle cooperative di dati, basata sulla comparazione tra i molteplici interessi coinvolti dall'azione amministrativa, da cui derivano risultati, improntati all'interconnessione e all'accessibilità ai dati, all'esito di una collaborazione uomo-macchina con conseguenti vantaggi in termini di sviluppo sostenibile e benessere della collettività.

Capitolo XXVIII

Cooperative di dati e gemelli digitali urbani

Ilaria Speziale-Carlo Basunti[*]

Abstract: This paper analyzes the possible interactions between services of data cooperatives, as recently outlined by the European legislator in the Data Governance Act, and urban digital twins created and implemented by public authorities. The analysis, starting from the legal framework, explores the concrete applications that have already emerged in practice, in order to examine the cooperative model as an in-progress tool, aimed at collective well-being through public action.

1. Premessa: la valorizzazione dei dati nel settore pubblico promossa dalla Strategia europea per i dati.

La Commissione europea, nella Comunicazione del 19 febbraio 2020 «*A European Strategy for Data*» [1], ha avviato un percorso di più marcata valorizzazione dei dati, personali e non personali, senza per questo trascurare la tutela della persona umana e, dunque, la centralità del principio personalistico.

---

[*] Pur essendo lo scritto, nel suo complesso, frutto di riflessioni comuni, sono da attribuire a Ilaria Speziale i parr. 1, 2, 3.1. e 4.2.; e a Carlo Basunti i parr. 3.2., 4.1 e 5.

[1] COMMISSIONE EUROPEA, Comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Una strategia europea per i dati*, Bruxelles, 19 febbraio 2020, COM (2020) 66 *final*.

I dati sono oggi linfa vitale dello sviluppo economico: essi sono alla base di processi generativi di svariati nuovi prodotti e servizi e, al contempo, accrescono la produttività e l'efficienza delle risorse in tutti i settori economici, consentendo, tra l'altro, strategie politiche finora inedite, volte (anche) al potenziamento dei servizi pubblici.

La *European Strategy for Data* intende porre le basi per assicurare all'Unione europea un ruolo guida nell'economia sempre più *data driven*, rendendola così un vero punto di riferimento per lo sfruttamento dei vantaggi derivanti da un sapiente utilizzo dei dati non solo a livello imprenditoriale, ma anche nel settore pubblico. In tale contesto, assume primaria importanza la *European Data Governance*, scolpita nel *Data Governance Act*, Reg. (UE) n. 868/2022 (DGA) che è entrato in vigore il 3 giugno 2022 e si applica dal 24 settembre 2023.

In particolare, il DGA si snoda lungo tre direzioni principali:

(i) il riuso dei dati personali e non personali, che sono nella disponibilità della pubblica amministrazione, la quale ha la facoltà di coinvolgere soggetti terzi nelle attività di trattamento dei dati per finalità, commerciali o non commerciali, ulteriori rispetto a quelle che hanno giustificato il primo trattamento. Le operazioni di riutilizzo dei dati devono avvenire pur sempre nell'ambito di compiti di servizio pubblico, sul presupposto che i dati gestiti da enti pubblici con fondi pubblici vadano impiegati a beneficio dei cittadini, delle imprese e, in generale, della comunità;

(ii) i servizi di intermediazione dei dati, personali e non personali, offerti dai c.d. fornitori di servizi di intermediazione dei dati che mediano tra gli utenti e le imprese, le quali svolgono operazioni sui dati;

(iii) l'altruismo dei dati, ossia la condivisione volontaria di dati, personali o non personali, che prescinde dalla richiesta o ricezione di un compenso che vada oltre il recupero dei costi di messa a disposizione del dato, per il perseguimento di obiettivi di interesse generale, quali, ad esempio, l'assistenza sanitaria, la lotta ai cambiamenti climatici, il miglioramento della mobilità, la ricerca scientifica.

Nell'ambito dei menzionati servizi di intermediazione dei dati, l'art. 10 DGA prevede: «*a*) servizi di intermediazione tra i titolari dei dati e i potenziali utenti dei dati, compresa la messa a disposizione di mezzi tecnici o di altro tipo per consentire tali servizi; tali servizi possono includere scambi di dati bilaterali o multilaterali o la creazione di piattaforme o banche dati che consentono lo scambio o l'utilizzo congiunto dei dati, nonché l'istituzione di altra infrastruttura specifica per l'interconnessione di titolari dei dati con gli utenti dei dati; *b*) servizi di intermediazione tra interessati che intendono mettere a disposizione i propri dati personali o persone fisiche che intendono mettere a disposizione dati non personali e potenziali utenti dei dati, compresa la messa a disposizione di mezzi tecnici o di altro tipo per consentire tali servizi, permettendo in particolare l'esercizio dei diritti degli interessati di cui al regolamento (UE) 2016/679; *c*) servizi di cooperative di dati».

La *governance* dei dati, promossa a livello europeo, incoraggia, dunque, l'utilizzo e la valorizzazione dei dati, non più solo da parte di imprese private, ma anche e soprattutto da parte di soggetti pubblici che, nell'esercizio dei pubblici poteri di cui dispongono, perseguono il benessere della collettività.

Di particolare interesse è, altresì, il riferimento della Strategia europea per i dati ai gemelli digitali. Questi ultimi sono analizzati con specifico riguardo all'industria manifatturiera e, secondo quanto affermato dalla Commissione europea, «creano una copia virtuale di un prodotto, processo o sistema fisico che può ad esempio prevedere, sulla base dell'analisi dei dati, quando un'apparecchiatura avrà un guasto, consentendo di incrementare la produttività mediante una manutenzione predittiva» [2].

Tali copie virtuali, a ben vedere, possono trovare applicazione nei campi più disparati e, quindi, anche nell'ambito delle *smart cities* rispetto alle quali assumono l'accezione di gemelli digitali urbani (GDU). Un simile modello rappresenta la proiezione digitale di un certo territorio, capace di adattarsi continuamente ai cambiamenti operativi delle città, sulla base di dati forniti in tempo reale che, (anche) con l'ausilio dell'intelligenza artificiale, vengono trattati, tra le altre, con finalità predittive. Così, il GDU consente di calibrare le scelte di pianificazione urbana sui processi di progressiva trasformazione territoriale, determinando notevoli vantaggi.

Il maggiore coinvolgimento di soggetti pubblici nelle logiche di sfruttamento dei dati rappresenta un fenomeno che, a tratti inedito, pone nuove sfide in capo agli interpreti, tenuti a farvi fronte anche attraverso soluzioni esegetiche già consolidate [3]. Del resto, come autorevolmente affermato [4], non è sempre vero che per regolare fenomeni nuovi occorra un diritto nuovo, dal momento che il ricorso ai principi generali del diritto consente di attribuire la giusta rilevanza al quadro di insieme senza la pretesa di soluzioni *ad hoc* – e, quindi, norme *ad hoc* – per ogni problema specifico.

Il presente contributo si inserisce all'interno di tale vivo dibattito e mira a inquadrare i servizi di cooperative di dati ed i gemelli digitali, nonché ad esplorare le possibili interazioni tra di essi e le relative ricadute pratiche, muovendosi nell'ottica di un'efficace azione del settore pubblico sul mercato digitale.

2. Cooperative di dati e gemelli digitali (urbani) a confronto.

Come accennato, nell'ambito dei servizi di intermediazione dei dati, il DGA include i servizi di cooperative di dati [5]. Il legislatore europeo disciplina tale fenome-

---

[2] Così Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Una strategia europea per i dati*, cit., p. 3.

[3] Sul tema v. F. BRAVO-J. VALERO TORRIJOS (eds.), *Data Governance, Open Data and Data Protection in the Public Sector (Monographic Section)*, in *European Review of Digital Administration & Law (ERDAL)*, 2022, 2, p. 5 ss. in cui gli Autori rilevano che i nuovi «*legal issues relating to data in the public sector*» siano, principalmente, «*(i) the new setup of public-private relations, (ii) the new balance between public powers and citizens' rights, (iii) the emergence of new duties for public sector bodies and new rights for individuals and companies, (iv) the new role of public administration in the data-driven society and economy*».

[4] Così G. FINOCCHIARO, *Riflessioni su diritto e tecnica*, in *Dir. inf.*, 2012, 4-5, p. 838.

[5] Cfr. F. BRAVO, *Le cooperative di dati*, in *Contr. e impr.*, 2023, 3, p. 757 ss.

no sotto il profilo oggettivo e non soggettivo, fornendo, per l'appunto, una definizione dei servizi di cooperative di dati e non delle cooperative di dati in sé.

Ai sensi dell'art. 2, par. 1, 15) DGA, i servizi di cooperative di dati sono «servizi di intermediazione dei dati offerti da una struttura organizzativa costituita da interessati, imprese individuali o da PMI, che sono membri di tale struttura, avente come obiettivi principali quelli di aiutare i propri membri nell'esercizio dei loro diritti in relazione a determinati dati, anche per quanto riguarda il compiere scelte informate prima di acconsentire al trattamento dei dati, di procedere a uno scambio di opinioni sulle finalità e sulle condizioni del trattamento dei dati che rappresenterebbero al meglio gli interessi dei propri membri in relazione ai loro dati, o di negoziare i termini e le condizioni per il trattamento dei dati per conto dei membri prima di concedere l'autorizzazione al trattamento dei dati non personali o prima che essi diano il loro consenso al trattamento dei dati personali».

Si tratta, dunque, di una struttura organizzativa, di cui non viene esplicitata la forma (necessariamente) societaria, che supporta i propri membri – interessati, imprese individuali e/o PMI – nel far valere le facoltà che l'ordinamento riconosce loro. Quindi, la nozione di cooperativa di dati è piuttosto ampia e tale da lasciare intuire che i relativi servizi possono essere forniti non solo da società cooperative – le quali paiono, invero, i soggetti fisiologicamente deputati a ricoprire un simile ruolo –, ma anche da enti diversi. Del resto, il legislatore europeo è stato, sul punto, volutamente generico, scegliendo di soffermarsi unicamente sull'elemento oggettivo del concetto – ossia la fornitura del servizio di cooperativa di dati – e non, invece, sulla natura soggettiva del fornitore. Dunque, la struttura organizzativa cui si riferisce il DGA ben potrà essere costituita anche nella forma di associazioni temporanee di imprese (ATI) o di raggruppamenti temporanei di imprese (RTI) o, ancora, di reti di imprese che, comunque, svolgano i servizi di intermediazione dei dati attraverso logiche di cooperazione e, più in generale, nel pieno rispetto delle previsioni di cui al DGA [6].

I singoli membri della cooperativa di dati mantengono la *governance* individuale sui propri dati, ma partecipano anche alla *governance* collettiva esercitata dalla struttura organizzativa e definita in base ad un confronto (democratico) tra i membri stessi. La cooperativa accresce l'*empowerment* dei suoi singoli componenti, i quali diventano così più consapevoli delle potenzialità offerte dai dati di cui dispongono e acquisiscono maggior potere di negoziazione sugli stessi di fronte alle *Big Tech*. Nell'attuale società dell'informazione, infatti, le multinazionali dell'IT (conosciute anche con l'acronimo GAFAM che indica, nel loro insieme, Google, Apple, Facebook, Amazon e Microsoft) detengono un sostanziale oligopolio in forza dell'enorme pletora di dati a loro disposizione (i c.d. *Big Data*).

Proprio sul punto interviene il DGA che, prendendo atto degli squilibri di potere che avvantaggiano in via pressocché esclusiva i *Big Players*, mira a rendere possibile e significativa anche la partecipazione dei singoli, delle PMI e delle *start-up*

[6] V. F. BRAVO, *Le cooperative di dati*, cit., p. 760.

sul mercato digitale. È ampiamente noto, infatti, che i menzionati grandi gruppi societari operano nel mercato erigendo barriere all'ingresso per evitare l'imporsi di ulteriori *competitors*, e ciò in forza delle attività di trattamento di (*big*) *data* e di profilazione degli utenti che permette loro di offrire servizi "gratuitamente" [7] o, comunque, a costi decisamente inferiori a quelli che potrebbe proporre qualsivoglia impresa concorrente che intendesse affacciarsi sul mercato.

Nell'ambito dei processi di scambio, utilizzo e sfruttamento economico dei dati (personali) – e, dunque, del mercato dei dati [8] –, diviene cruciale rafforzare e tutelare la posizione della *weaker party*, sia essa *data subject* (ai sensi del GDPR) o *data holder* (ai sensi del DGA) [9]. Normalmente, infatti, l'interessato ed il titolare dei dati versano in una condizione di debolezza, *in primis* sul lato contrattuale, dal momento che subiscono le condizioni definite da altri, senza la possibilità di rivestire un ruolo attivo nella trattativa precontrattuale. Di più, nell'accedere ai beni e servizi offerti sul mercato digitale, essi spesso si trovano a prestare, in cambio, il proprio consenso al trattamento dei dati, senza essere neppure consapevoli del loro valore (di scambio).

Quindi, l'architettura delineata dal *Data Governance Act* è funzionale a riequilibrare le posizioni degli agenti sul mercato nella direzione di quello che potrebbe definirsi come *digital market reshaping*. In questo senso, i servizi di intermediazione dei dati – tra i quali spiccano i servizi di cooperative di dati – supportano gli interessati e i *data holders* nell'esercizio consapevole dei propri diritti sui dati, assumendo un ruolo guida – di intermediario, appunto – nelle operazioni di trattamento.

Lo squilibrio di potere, che caratterizza ontologicamente l'insieme delle attività relative ai dati, non concerne solamente gli agenti privati del mercato (dei dati), ma può coinvolgere anche soggetti pubblici nei rapporti con le altre pubbliche amministrazioni. Si pensi, ad esempio, alla diversa rilevanza che, nei processi decisionali, hanno i

---

[7] Sul tema, v. per tutti G. RESTA-V. ZENO ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim. dir. e proc. civ*., 2018, 2, p. 411 ss.

[8] Cfr. V. ZENO ZENCOVICH, *Do "Data Markets" Exist?*, in *Media Laws*, 2019, 2, p. 1 ss.; ID., *Do "data markets" exist?*, in G. RESTA-V. ZENO ZENCOVICH (a cura di), *Governance of/through Big Data*, vol. 1, Roma, 2023, p. 415 ss.

[9] Il *Data Governance Act* introduce concetti fino a quel momento inediti con riguardo ai soggetti del trattamento, creando una nuova tassonomia. In particolare, si segnala la previsione della figura del titolare dei dati (*data holder*), definito *ex* art. 2, par. 1, 8) come «una persona giuridica, compresi gli enti pubblici e le organizzazioni internazionali, o una persona fisica che non è l'interessato rispetto agli specifici dati in questione e che, conformemente al diritto dell'Unione o nazionale applicabile, ha il diritto di concedere l'accesso a determinati dati personali o dati non personali o di condividerli». Tale definizione deve essere coordinata con quella di interessato (*data subject*), inteso dall'art. 4, par. 1, 1) come «la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo *online* o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale». Sul punto, v. F. BRAVO, *Intermediazione di dati personali e servizi di* data sharing *dal GDPR al* Data Governance Act, in *Contr. e impr./Europa*, 2021, 1, pp. 202-203.

comuni di piccole dimensioni già solo al cospetto delle città metropolitane. Del resto, al di là di un discorso relativo alle nuove prospettive di utilizzo dei dati, che in questa sede ci interessa, sin dai primi anni Settanta in Italia è prevista la possibilità per i (piccoli) comuni montani e pedemontani di unirsi, formando le Comunità montane [10], con lo scopo di valorizzare il territorio e di esercitare in forma associata le funzioni loro proprie. Chiaramente, un istituto come questo mira, seppur in un altro contesto, all'obbiettivo di dare voce a soggetti che, altrimenti, non ne avrebbero alcuna.

Nella prospettiva di migliorare l'esercizio della funzione pubblica, avvantaggiando così l'intera società – oltre che di accrescere il peso dei singoli enti pubblici, specie se di piccole dimensioni –, le cooperative di dati possono rivestire un ruolo chiave nella creazione e nell'implementazione di gemelli digitali urbani.

Si precisa che la realtà offre diverse fattispecie di gemelli digitali, intesi quali rappresentazioni virtuali (traduzione in dati) di entità analogiche di qualsiasi tipo: fisiche, viventi o non viventi, giuridiche, economiche, e così via. Ai nostri fini occorre, però, soffermarci sulla sola ipotesi del gemello digitale urbano.

Tale ipotesi integra un modello digitale preciso di un determinato territorio, che, alimentato dai dati raccolti anche in tempo reale, si presenta come completo, integrato, dinamico e predittivo. Esso appare completo, perché rappresenta il territorio di riferimento nelle sue infrastrutture fisiche oltre che nei suoi processi e dinamiche economiche, sociali ed organizzative; è integrato, perché riesce a catturare la complessità delle relazioni come delle influenze reciproche tra i vari sistemi urbani esistenti; è dinamico, in quanto evolve insieme al territorio, alimentandosi del costante flusso di dati ivi prodotti; è, infine, predittivo, dal momento che consente a chi lo utilizza di prevedere e anticipare comportamenti e trasformazioni che hanno luogo nella realtà analogica.

Seppur citato in un passaggio della Strategia europea per i dati, il gemello digitale, generalmente inteso, manca di una definizione legislativa sia a livello europeo sia nazionale. Il silenzio del legislatore non ha, comunque, limitato l'emersione del fenomeno nella prassi, dal momento che, nella declinazione urbana, varie città, anche al di fuori dell'Unione europea, si stanno dotando di simili infrastrutture civiche. Si segnalano, a titolo di esempio, i casi di Singapore, Barcellona e Bologna [11].

Si tratta, in sostanza, di una piattaforma tecnologica per la raccolta, l'analisi, l'integrazione, la visualizzazione e la simulazione dei dati di una città e per il supporto ai processi decisionali. Tali gemelli digitali sono, dunque, molto più di una replica digitale di sistemi fisici, persone e ambienti. Essi vanno tenuti distinti da altri approcci di analisi e visualizzazione dei dati, proprio perché sono in grado di integrare dati provenienti da varie fonti in tempo reale e di valutare scenari futuri attraverso simulazioni avanzate.

Applicati in contesti urbani, i gemelli digitali appaiono idonei a rivoluzionare il

---

[10] Il riferimento è alla l. 3 dicembre 1971, n. 1102, poi confluita nel T.U. sugli enti locali, d.lgs. 18 agosto 2000, n. 267 (art. 27).

[11] V. *infra* al par. 3.2.

modo in cui le città affrontano la gestione, il monitoraggio e la pianificazione futura, nella prospettiva di uno sviluppo sostenibile.

Si delinea così un modello di amministrazione massimamente condivisa delle risorse cittadine che consente ai Comuni ed ai cittadini che si inseriscono attivamente in questo disegno di realizzare attività volte alla rigenerazione urbana, alla cura della città, all'implementazione dei servizi cittadini, alla gestione dei beni comuni e così via, su un piano paritetico, improntato ad una solida idea di democrazia. È chiaro che la pubblica amministrazione non agisce qui in via autoritativa e/o imperativa, secondo lo schema classico potere-funzione-procedimento, ma predilige, nella propria azione, logiche di condivisione e di parità secondo le norme di diritto privato, *ex* art. 1, co. 1 *bis*, l. n. 241/1990 [12].

Il gemello digitale urbano integra un'inedita ipotesi applicativa del principio di sussidiarietà [13], consacrato nell'art. 118 Cost., ai sensi del quale «Stato, Regioni, Città metropolitane, Province e Comuni favoriscono l'autonoma iniziativa dei cittadini, singoli e associati, per lo svolgimento di attività di interesse generale, sulla base del principio di sussidiarietà». Tale principio permea di sé l'intero tessuto della Carta costituzionale laddove disciplina i rapporti tra PA e cittadini, delineando nuovi equilibri tra amministratori e amministrati. In questo senso, «il principio di sussidiarietà orizzontale svolge una funzione di emancipazione delle esperienze sociali, attribuendo a esse un valore giuridico che altrimenti stenterebbe a essere riconosciuto se non in termini di mera espressione di autonomia privata del tutto disancorata dagli interessi generali» [14].

Attraverso l'utilizzo di gemelli digitali urbani, il principio di sussidiarietà esplica appieno la sua declinazione sociale. Si può, quindi, parlare di sussidiarietà sociale quale espressione di libertà solidale con la quale i consociati esprimono la propria identità personale secondo un modello di autorganizzazione del vivere associa-

---

[12] Cfr. L. CASALINI, Commons, commoning and community. *I patti di collaborazione*, in *Pers. e merc.*, 2022, 1, p. 36.

[13] *Ex multis*, G.U. RESCIGNO, *Principio di sussidiarietà orizzontale e diritti sociali*, in *Dir. pubbl.*, 2002, 1, p. 4 ss.; A. D'ATENA, *Costituzione e principio di sussidiarietà*, in *Quad. cost.*, 2001, 1, p. 13 ss.; ID., *Il principio di sussidiarietà nella Costituzione italiana*, in *Riv. it. dir. pubbl. com.*, 1997, 3-4, p. 603 ss.; L. COEN-C. MAINARDIS, *Art. 118*, in V. CRISAFULLI-L. PALADIN-S. BARTOLE-R. BIN (a cura di) *Commentario breve alla Costituzione*, II ed., 2008, Padova, p. 1065 ss.; CAMERLENGO, *Art. 118*, in R. BIFULCO-A. CELOTTO-M. OLIVETTI (a cura di), *Commentario alla Costituzione*, vol. III, Torino, 2006, p. 2333 ss.; P. DE PASQUALE, *Il principio di sussidiarietà nella Comunità europea*, Napoli, 2000; I. MASSA PINTO, *Il principio di sussidiarietà. Profili storici e costituzionali*, Napoli, 2003; P. DE CARLI, *Sussidiarietà e governo economico*, Milano, 2002; E. DE MARCO (a cura di), *Problemi attuali della sussidiarietà*, Milano, 2005; D. DE FELICE, *Principio di sussidiarietà e autonomia negoziale*, Napoli, 2008; P. VIPIANA, *Il principio di sussidiarietà "verticale". Attuazioni e prospettive*, Milano, 2002; G. URBANO, *Le "città intelligenti" alla luce del principio di sussidiarietà*, in *Ist. fed.*, 2019, 2, p. 463 ss.; J.M. DE AREILZA CARVAJAL, *El principio de subsidiariedad en la construcción de la Unión Europea*, Madrid, 1996.

[14] Così F. GIGLIONI, *I regolamenti comunali per la gestione dei beni comuni urbani come laboratorio per un nuovo diritto delle città*, in *Munus*, 2016, 2, p. 286.

to che trascende l'interesse del singolo in favore di quello della collettività [15]. Il privato assume così un ruolo attivo fondamentale in una logica di condivisione con la pubblica amministrazione, contribuendo alle scelte decisionali con cui realizzare l'interesse generale (anche) per mezzo della propria libertà e autonomia.

In tale contesto, i gemelli digitali urbani si mostrano quali *trait d'union* tra il menzionato principio di sussidiarietà ed il principio normativo di solidarietà [16] che con il primo ben si coordina. Infatti, nei processi di trasformazione digitale che, allo stato attuale, coinvolgono diritto, economia e società, si può far riferimento al neomutualismo [17], nella sua moderna declinazione di neomutualismo digitale [18], come moderno paradigma di sviluppo sostenibile delle imprese, delle persone e della comunità. Ciò, in definitiva, appare perfettamente in linea con gli obiettivi perseguiti a livello europeo attraverso la Strategia europea per i dati e, in particolare, il *Data Governance Act*.

3. Cooperative di dati e gemelli digitali urbani: casi pratici.

3.1. Le cooperative di dati nel settore di *ride hailing*: il caso Driver's Seat.

Nell'ambito delle cooperative di dati già esistenti sul mercato, quelle che si oc-

---

[15] Sempre attuali sul punto le considerazioni di W. CESARINI SFORZA, *Il diritto dei privati*, Milano, 1929, rist. 1963, p. 21 ss. che ricostruisce l'ordinamento giuridico come un complesso di ordinamenti in cui sia da ricomprendere anche quello dell'autorganizzazione sociale che sfugge al dato normativo del diritto privato e che si nutre solo di capacità autorganizzativa.

[16] Sul principio di solidarietà, inquadrato quale principio normativo, cfr. G. ALPA, *Solidarietà. Un principio normativo*, Bologna, 2022; ID., *I principi generali*, Milano, 2023, p. 256 ss.; v. anche la ricostruzione del principio offerta da S. RODOTÀ, *Solidarietà. Un'utopia necessaria*, Roma-Bari, 2014; P. RESCIGNO, *Solidarietà e diritto*, Napoli, 2006; N. LIPARI, *"Spirito di liberalità" e "spirito di solidarietà"*, in *Riv. trim. dir. e proc. civ*., 1997, 1, p. 1 ss.; F.D. BUSNELLI, *Il principio di solidarietà e "l'attesa della povera gente", oggi*, in *Riv. trim. dir. e proc. civ*., 2013, 2, p. 413 ss.; M. TAMPIERI, *La riscoperta del principio di solidarietà*, in *Jus Civile*, 2020, 3, p. 612 ss.; B. BERTARINI, *Il principio di solidarietà tra diritto ed economia. Un nuovo ruolo dell'impresa per uno sviluppo economico inclusivo e sostenibile*, Torino, 2020; A. APOSTOLI, *La svalutazione del principio di solidarietà: crisi di un valore fondamentale per la democrazia*, Milano, 2012; F. POLACCHINI, *Doveri costituzionali e principio di solidarietà*, Bologna, 2017; sul principio di solidarietà applicato al tema della protezione dei dati personali, cfr. F. BRAVO, *Il principio di solidarietà in materia di protezione dei dati personali nelle decisioni del Garante e della Corte di cassazione*, in *questa rivista*, 2023, 2, p. 405 ss.; ID. (a cura di), *Il principio di solidarietà*, in *Dati personali. Protezione, libera circolazione e* governance – Vol. 1., *Principi*, Pisa, 2023, p. 541 ss.; ID., *Il principio di solidarietà tra* data protection *e* data governance, in *Dir. inf*., 2023, 3, p. 481 ss.

[17] Cfr. P. VENTURI-F. ZANDONAI, *Neomutualismo. Ridisegnare dal basso competitività e* welfare, Milano, 2022.

[18] V. F. BRAVO, *Le cooperative di dati*, cit., p. 764; ID., Ubi societas ibi ius *e fonti del diritto nell'età della globalizzazione*, in *Contr. e impr*., 2016, 6, p. 1344 ss.; T.E. FROSINI, *Il costituzionalismo nella società tecnologica*, in *Dir. inf*., 2020, 3, p. 1 ss.

cupano dell'erogazione di servizi di *ride-hailing* hanno una posizione di particolare rilievo.

Driver's Seat [19] si propone come alternativa al modello capitalistico tracciato dalle *gig platform* di settore che esercitano un controllo penetrante sull'attività di chi opera attraverso le relative piattaforme, per mezzo di algoritmi opachi e fornendo informazioni limitate circa l'organizzazione del lavoro, soprattutto nel rapporto tra tempo e guadagno.

Driver's Seat è una cooperativa di dati creata da *gig workers* per *gig workers*: si includono tutti coloro che trasportano beni o persone ed il cui lavoro è mediato da una *app*. Come erogatore di servizi, essa si propone di offrire servizi di *ride-hailing* e *ride-sharing* (sul modello di Uber e Lyft), nonché di *food-delivering* (sul modello di Glovo, Deliveroo e Uber Eats). Non si presenta come una classica *ride-hailing company*, ma è progettata su misura per gli autisti, al fine di massimizzare le potenzialità dei loro dati, aumentare i loro margini di profitto e promuovere il bene comune.

L'obiettivo centrale non è tanto la monetizzazione dei dati per finalità di guadagno (fine comunque presente, ma che assume qui una portata secondaria), ma piuttosto quello di collazionare i dati e di analizzarli, al fine di condividere conoscenze utili per i propri membri.

In qualità di erogatore di servizi di cooperativa di dati, Driver's Seat opera in diverse città statunitensi. Gli autisti, quali membri della cooperativa, devono scaricare un'apposita *app*, che consente loro di condividere con la cooperativa i dati nella loro disponibilità. In questo senso, Driver's Seat si impegna ad aumentare i margini di guadagno degli autisti, tramite la più ampia condivisione di informazioni sugli orari migliori in cui lavorare, le zone in cui è solitamente presente una maggiore richiesta del servizio, i flussi di traffico. I singoli membri possono monitorare in modo costante e trasparente il proprio lavoro, con particolare riguardo al rapporto tra tempo impiegato, chilometraggio complessivamente percorso e spese sostenute (carburante, pedaggi, riparazioni del veicolo, e così via).

Il motto di Driver's Seat, che racchiude efficacemente il suo operato, è «*Know more. Earn more*» [20]. La maggior conoscenza (*know more*), a parere di chi scrive, merita un breve approfondimento. Essa pare poter essere declinata (almeno) in una

---

[19] Per maggiori informazioni, si rinvia al sito *web* della cooperativa: *https://driversseat.co*. V. anche F. BRAVO, *Le cooperative di dati*, cit., p. 770 ss.; H.A. CHAUDARI-J. BYERS-E. TERZI, *Putting Data in the Driver's Seat: Optimizing Earnings for On-Demand Ride-Hailing*, in *WSDM*, 2018, p. 90 ss.; M.M. BÜLER-AL., *Unlocking the Power of Digital Commons: Data Cooperatives as a Pathway for Data Sovereign, Innovative and Equitable Digital Communities*, in *Digital*, 2023, 3, p. 146 ss.; V. DUBAL, *On Algorithmic Wage Discrimination*, in *Columbia Law Rev*., 2023, 7, spec. p. 1985 ss.; A. FISHER-T. STREINZ, *Confronting Data Inequality*, in *Columbia J. of Trans. Law*., 2022, 3, spec. p. 946; E. BIETTI-A. ETXEBERRIA-M. MANNAN-J. WONG, *Data Cooperatives in Europe: A Legal and Empirical Investigation*, *White Paper created as part of The New School's Platform Cooperativism Consortium and Harvard University's Berkman Klein Center for Internet & Society, Research Sprint*, Dicembre 2021, in *https://cyber.harvard.edu/sites/default/files/2022-02/Data_Cooperatives_Europe-group2.pdf*, p. 8 ss.

[20] Lo *slogan* si rinviene nella pagina di apertura del sito *web* di Driver's Seat.

duplice prospettiva, riferendola a: *i*) la maggior consapevolezza che il singolo autista ha del proprio lavoro, tenuto conto dell'esatto rapporto costi-benefici; *ii*) la maggior consapevolezza che il singolo autista ha dell'operato degli altri colleghi che lavorano per Driver's Seat o per i *competitors*.

La cooperativa, ovviamente, provvede a crittografare i dati e adotta misure di sicurezza amministrative, fisiche e tecnologiche, per difendersi da eventuali *data breaches*. Inoltre, chiunque abbia accesso ai dati presenti nel sistema è soggetto ad obblighi contrattuali e professionali di salvaguardia dei dati stessi, nel rispetto della normativa *privacy* [21].

Driver's Seat sottolinea, altresì, che «*empowerment requires transparency*». È apprezzabile che essa sensibilizzi i membri e chiunque utilizzi i suoi servizi sulla sorte dei dati inseriti in dinamiche circolatorie. Diversamente dalle grandi piattaforme rivali, Driver's Seat provvede a rendere edotti i propri soci dei benefici insiti nella partecipazione mutualistica alla cooperativa. Ma non solo: essa condivide tutte le informazioni relative ai soggetti a cui i dati vengono trasferiti, alle finalità dei vari trattamenti e alla durata degli stessi, così da agevolare un utilizzo sempre più consapevole dei dati da parte degli interessati. La cooperativa offre, dunque, il proprio significativo contributo all'alfabetizzazione circa l'utilizzo dei dati, promuovendo il diritto all'autodeterminazione informativa.

Driver's Seat trasferisce i dati secondo un modello che viene definito di «*shared ownership*».

Sul punto, preme però precisare che una simile qualificazione non è giuridicamente appropriata. La cooperativa non può tecnicamente qualificarsi come comproprietaria dei dati insieme agli interessati e, neppure con riguardo a questi ultimi, appare corretto parlare di diritto di proprietà [22]. I dati vengono condivisi dagli interessati con la cooperativa che può, sulla base ed entro i limiti del consenso [23], utilizzarli per apportare benefici ai suoi membri e ad essa stessa, nel suo complesso.

---

[21] Driver's Seat sottolinea, però, che: «*while we strive to use commercially acceptable means to protect your personal information, no method of transmission over the Internet or form of electronic storage is 100 percent secure. Therefore, we cannot guarantee its absolute security*». In tema di *data breach* cfr. A. MANTELERO, *La gestione del rischio*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, 2019, p. 473 ss.; A. MANTELERO, *Si rafforza la tutela dei dati personali: "*data breach notification*" e limiti alla profilazione mediante* cookies, in *Dir. inf*., 2012, 4-5, p. 781 ss.

[22] V. V. ZENO ZENCOVICH, *Do "Data Markets" Exist?*, cit., spec. p. 25, ove l'Autore, da un punto di vista semantico, afferma: «*"Ownership" is not a notion which is engraved in some sacred tables. It is the result of centuries, millennia of theoretical, religious, political, social, economic evolution*» e aggiunge: «*ownership is a concept quite different from proprieté or from Eigentum*»; v. anche J.S. BERGÉ-S.M. GRUMBACH-V. ZENO ZENCOVICH, *The 'Datasphere', Data Flows beyond Control, and the Challenges for Law and Governance*, in *European J. of Comp. Law and Governance*, 2018, 2, p. 144 ss.

[23] Sul sito *web* di Driver's Seat si riporta, infatti, la possibilità di inviare una richiesta di cancellazione dell'*account* che comporta anche la cancellazione di tutti dati raccolti dall'istante, e quindi anche l'interruzione della possibilità di uno sfruttamento di tali dati.

Ad essere condivisa è la possibilità di utilizzo dei dati e non i dati in sé, secondo vincoli di tipo reale, e quindi la cooperativa non è proprietaria dei dati dei suoi membri, ma è, piuttosto, titolare di una situazione giuridica soggettiva attiva (un diritto) che ne consente l'uso per il tempo stabilito o, comunque, fino alla revoca del consenso da parte dell'interessato.

Nel novero dei destinatari dei dati collazionati da Driver's Seat, figurano anche soggetti pubblici che intendano utilizzare tali dati per finalità di interesse generale, come potrebbe essere la creazione di gemelli digitali urbani. In quest'ottica, le logiche solidaristiche e mutualistiche, proprie della cooperativa di dati, raggiungono il loro apice, potendo esternare un forte impatto non solo per i membri della cooperativa in sé, ma per la società intera.

In definitiva, il modello proposto dalla cooperativa qui in esame appare di sicuro apprezzamento. L'idea è quella di porre al centro la tutela della persona umana, nei suoi diritti fondamentali, primo fra tutti quello all'autodeterminazione informativa. Tale tutela, pur dovendo essere declinata lungo la coordinata del bilanciamento di interessi, non può mai essere irragionevolmente compressa nell'odierna *data driven society*. Solo così la persona verrà davvero a trovarsi, nella gestione dei propri dati, "al posto del guidatore".

3.2. I gemelli digitali urbani di Singapore, Barcellona e Bologna.

Una volta analizzato il caso Driver's Seat, quale esempio paradigmatico di cooperativa di dati operante nel settore dei trasporti, preme soffermarsi ora, sempre con un approccio casistico, sulle applicazioni pratiche in essere ed in divenire dell'altra nozione prima introdotta, ossia quella di gemelli digitali urbani.

Tutti gli esempi offerti dalla prassi sono accomunati dall'obiettivo di costruire una sovranità digitale, ponendo il dato territoriale al centro della sfida urbana. Infatti, il digitale, se applicato ad un'attenta progettazione locale, può favorire il dialogo tra gli utenti del territorio e la pubblica amministrazione in tutte le fasi del vivere urbano.

Tra i primi casi di gemelli digitali urbani, si segnalano quelli delle città di Singapore, Barcellona e Bologna. L'idea condivisa dai tre modelli è quella di costruire una sovranità digitale, ponendo il dato territoriale al centro della sfida urbana. Infatti, il digitale, se applicato ad una attenta progettazione locale, può favorire il dialogo tra gli utenti del territorio e la pubblica amministrazione in tutte le fasi del vivere urbano.

In particolare, l'esempio di Singapore rappresenta un *unicum*, nel panorama internazionale, in quanto si tratta del solo gemello digitale su scala nazionale (riferito, appunto, alla città Stato di Singapore). Le potenziali applicazioni di questo gemello digitale sono molteplici e vanno dalla pianificazione urbana, *lato sensu* intesa, alla risposta alle emergenze e alla gestione delle catastrofi, come la simulazione delle operazioni di evacuazione e dell'impatto della dispersione della folla. Singapore, infatti, quale Paese insulare, è chiamato a fronteggiare declinazioni particolari delle sfide imposte dal *climate change*, come il progressivo e incontrollato innalzamento del livello del mare. In questo senso, il Paese sta sfruttando la sua infra-

struttura digitale, la quale offre una mappatura accurata, affidabile e coerente dell'intero territorio, condividendo i dati raccolti con l'agenzia nazionale per l'acqua, operando così congiuntamente nella gestione delle risorse, nella pianificazione e nella protezione delle aree costiere.

Emerge, dunque, come Singapore, anche e soprattutto attraverso il suo gemello digitale urbano, si impegni attivamente nel rispetto degli obbiettivi previsti dall'Agenda ONU 2030. Nello specifico, la città opera concretamente, valorizzando il potenziale dei dati, nella diffusione delle energie rinnovabili nella prospettiva della transizione energetica. E, infatti, attraverso l'uso dell'infrastruttura di dati, Singapore ha implementato l'energia solare fotovoltaica con l'obiettivo di distribuire due gigawatt picco (GWp) di energia solare entro il 2030.

Preme sottolineare che i gemelli digitali urbani, come quello di Singapore, nel tracciare il territorio, danno un contributo ben diverso da quello che può offrire una mappa tradizionale (analogica), a fronte della loro capacità di aggiornarsi costantemente grazie all'utilizzo di grandi flussi di dati. Tra l'altro, tali infrastrutture di dati non si limitano a rappresentare il solo spazio fisico della città di riferimento, ma anche il suo spazio legale, comprensivo, ad esempio, delle mappe catastali.

Parimenti, la città di Barcellona si è dotata di un gemello digitale urbano che è il risultato della collaborazione tra il Comune ed il *Centro Nacional de Supercomputación* (BSC-CNS). Si tratta, anche in questo caso, di una infrastruttura di dati che, però, nello specifico, è declinata in funzione di ridefinizione degli spazi urbani secondo il modello de «la città dei 15 minuti» elaborato da Carlos Moreno [24]. Tale concetto, fondato sul crono-urbanismo che legge la città in relazione ai tempi di percorrenza pedonale, mira a promuovere un'idea di città c.d. di prossimità che vada nella direzione opposta a quella tradizionalmente percorsa dall'urbanismo moderno. Quest'ultimo, infatti, separava nettamente lo spazio residenziale dal lavoro, dal commercio, dall'industria e dal tempo libero, con evidenti ricadute negative sulla vita quotidiana di ciascun individuo.

Diversamente, la città dei 15 minuti ripensa gli spazi urbani in modo che ogni cittadino sia potenzialmente in grado di soddisfare i propri bisogni umani essenziali spostandosi entro un'area percorribile a piedi o in bicicletta in un tempo massimo di quindici minuti. Simile obiettivo può essere raggiunto, tra l'altro, destinando uno stesso luogo ad usi diversi, scanditi anche in tempi diversi: vengono così a crearsi aree polifunzionali da utilizzare preferibilmente in forma condivisa.

Nel caso di Barcellona, il gemello digitale urbano si ripromette proprio di (ri)modellare la città come città della prossimità. La piattaforma di dati analizza l'accessibilità delle strutture pubbliche già esistenti e consente alla PA di valutare l'impatto di nuovi progetti edilizi, vagliandone la concreta fruibilità da parte del pubblico. Si potrà, in questo modo, identificare le aree che non rientrano nel modello di percorribilità pedonale in quindici minuti e, dunque, stimare il numero di cittadini esclusi dalla fruizione (agile) di quegli stessi spazi e servizi.

---

[24] Cfr. C. MORENO, *La città dei 15 minuti. Per una cultura urbana democratica*, Torino, 2024.

Lo sviluppo del gemello digitale urbano di Barcellona è stato articolato in due fasi: la prima è volta a creare una copia digitale della città che ne offra una fotografia molto dettagliata, seppur statica. La seconda è indirizzata, invece, a creare un modello digitale dinamico – e, dunque, adeso alla realtà – che sia attento ai cambiamenti dei luoghi e alle esigenze socio-lavorative delle persone che vivono quei luoghi, così da far dialogare tra loro diversi sistemi fisici e sociali nel contesto digitale. Questa seconda fase consente, ad esempio, di comprendere appieno l'impatto che le variazioni occupazionali dei cittadini di una certa area urbana hanno, tra l'altro, sui flussi di traffico, come pure sui livelli di inquinamento atmosferico e di immissioni acustiche nella medesima zona ed in aree limitrofe.

Di particolare interesse è il fatto che il progetto catalano sia stato implementato dal menzionato *Centro Nacional de Supercomputación* in *partnership* con il comune di Bologna e, in particolare, con l'apporto tecnologico del Consorzio Interuniversitario, ad intera partecipazione pubblica, CINECA che ha la propria sede centrale a Bologna.

Proprio la città di Bologna offre un ulteriore calzante esempio di gemello digitale urbano.

Recentemente, il Comune ha avviato la creazione della propria infrastruttura civica digitale avvalendosi di un apposito consorzio pubblico che include lo stesso Comune nel ruolo di coordinatore strategico, la Fondazione Bruno Kessler come coordinatore tecnico e *project manager*, la Fondazione Innovazione urbana come *community manager*, e l'*Alma Mater Studiorum* come *manager* scientifico.

Il progetto è indirizzato lungo quattro direttrici: *i*) città della conoscenza; *ii*) missione clima; *iii*) impronta verde; *iv*) piano per l'abitare.

Nello specifico: la città della conoscenza si prefigge di trattare i dati già a disposizione del comune e quelli che, nel corso del tempo, verranno generati, nell'ambito della città al fine di gestirli in modo democratico e con un approccio orientato al benessere della collettività locale. L'idea è quella di condividere le informazioni con una pluralità di *stakeholders* pubblici e privati, quali, ad esempio, centri di ricerca, fondazioni, associazioni civiche e singoli cittadini.

La missione clima mira a raggiungere la neutralità climatica all'interno del perimetro comunale entro il 2030, attraverso investimenti oculati in tema di mobilità, rieducazione cittadina sulle tematiche della sostenibilità ambientale, efficientamento energetico, migliore gestione dei rifiuti e degli spazi versi urbani.

L'impronta verde, sempre nell'ottica di fronteggiare le ineludibili sfide imposte dal *climate change*, punta a migliorare la salute delle persone, la qualità della vita e degli spazi pubblici, attraverso la progettazione digitale e la conseguente costruzione reale di una grande infrastruttura verde che abbracci la città nella sua interezza.

Il piano per l'abitare, infine, si pone l'ambizioso obbiettivo di affrontare e risolvere la tensione abitativa, creando una molteplicità di nuovi alloggi in un periodo di tempo indicativo di dieci anni.

Il gemello digitale urbano di Bologna si mostra particolarmente attento alla dimensione etica come a quella legale, entrambe riferite all'utilizzo, al riutilizzo e al-

la valorizzazione dei dati (personali). Segnatamente, il Comune intende garantire la conformità della propria azione amministrativa, nella creazione del *digital twin*, alla normativa in tema di *data protection*, senza per questo precludersi le opportunità oggi offerte dalla Strategia europea per i dati.

Dunque, un modello cittadino, fondato sulle quattro direttrici di cui si è appena dato conto, rispettoso dei parametri legali e che si muove lungo i binari dell'etica, appare idoneo a tratteggiare un paradigma di amministrazione sostenibile del tessuto urbano.

4. L'ingresso delle pubbliche amministrazioni nelle cooperative di dati.

4.1. I possibili modelli partecipativi degli enti pubblici alle cooperative di dati.

Una volta inquadrati i gemelli digitali urbani e le cooperative di dati, pare opportuno esplorare le possibili interazioni tra loro sussistenti. Il *Data Governance Act*, occupandosi sia delle attività di utilizzo e riutilizzo dei dati da parte delle PA [25] sia delle cooperative di dati, apre la strada a nuove linee di sviluppo del settore pubblico attraverso una più ampia valorizzazione dei dati.

La disciplina dei servizi di cooperative di dati, di cui all'art. 2, par. 1, 15) DGA, prevede che tali strutture organizzative possano essere partecipate da interessati, imprese individuali e PMI. In assenza di una puntuale menzione da parte del legislatore europeo, occorre chiedersi se anche i soggetti pubblici possano divenire membri di una cooperativa di dati. È già *prima facie* evidente che una simile eventualità consentirebbe, auspicabilmente, alle pubbliche amministrazioni di implementare i propri servizi, in primo luogo i gemelli digitali urbani, attraverso i servizi di intermediazione di dati di nuova introduzione.

Riteniamo che il breve elenco dei soggetti ammessi a partecipare alle cooperative di dati ai sensi del DGA non sia tassativo. E ciò sia avendo riguardo alla lettera della norma (art. 2, par. 1, 15) DGA) sia con riferimento all'impostazione sistematica del Regolamento nel suo complesso. Infatti, la menzionata norma non afferma esplicitamente – né lascia intendere – che tale elenco sia esaustivo e, dunque, chiuso. Inoltre, da un punto di vista sistematico, mentre sono certamente da escludere dal novero dei possibili membri di una cooperativa di dati le grandi imprese – si minerebbe altrimenti la *ratio* sottesa al DGA di arginare il sostanziale oligopolio detenuto dalle *Big Tech* sul mercato digitale –, nulla osta alla partecipazione di soggetti pubblici. Questi ultimi, anzi, potrebbero massimizzare gli obbiettivi altruistici e (neo)mutualistici del DGA, per il benessere sociale, nel rispetto dei principi di legalità, buon andamento e imparzialità, propri dell'azione amministrativa, ben

[25] Sul tema, v. F. BRAVO, *Data Governance Act and Re-Use of Data in the Public Sector*, in F. BRAVO-J. VALERO TORRIJOS (eds.), *Data Governance, Open Data and Data Protection in the Public Sector (Monographic Section)*, cit., p. 13 ss.

più di quanto non potrebbero fare i soggetti privati, pur sempre mossi (anche) da logiche di profitto.

Al fine di confermare una simile tesi, chi scrive ha avuto modo di entrare in contatto con il *Senior Advisor* della *Data Space Europe*[26] (Autorità competente per i servizi di intermediazione dei dati in Finlandia, la prima autorità in tal senso costituita conformemente al disposto dell'art. 13 DGA[27]) che, seppur in *layman terms*, si è detto possibilista sulla partecipazione di un ente pubblico ad una cooperativa di dati, citando l'esempio di Fintraffic su cui si tornerà in seguito[28]. Inoltre, è stato interrogato il *Team Leader* della *Unit G1 – Data Policy & Innovation* del *Directorate-General for Communications Networks, Content and Technology*, istituito in seno alla Commissione europea[29], che, in prima battuta, ha ammesso come nei lavori preparatori del DGA non fosse stata presa in considerazione l'opzione di una partecipazione pubblica alle cooperative di dati; ma ha poi dichiarato che nulla parrebbe ostare a detta fattispecie[30].

Ora, anche laddove si volesse escludere la possibilità, per gli enti pubblici, di divenire membri di una cooperativa di dati, essi – a ben vedere – potrebbero comunque avvalersi di PMI interamente partecipate dagli enti stessi, eventualmente costituendole *ad hoc* per partecipare ad una *data cooperative*. Una cooperativa di dati diverrebbe così accessibile, seppur indirettamente e attraverso lo schermo di una PMI partecipata, all'ente pubblico, possibilità che appare senz'altro conforme al dettato normativo e che, anzi, pare proprio avvalorare ulteriormente la lettura estensiva dell'art. 2, par. 1, 15), DGA appena suggerita.

La possibilità per un ente pubblico territoriale di partecipare ad una cooperativa di dati trova altresì conferma nell'art. 3, comma 1 del d.lgs. 19 agosto 2016, n. 175

---

[26] V. il sito *web* di *Data Space Europe*: *https://www.dataspace.fi/en/homepage*.

[27] Per quanto concerne l'ordinamento italiano, il recente d.lgs. 7 ottobre 2024, n. 144, recante *norme di adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio, del 30 maggio 2022, relativo alla* governance *europea dei dati e che modifica il regolamento (UE) 2018/1724*, ai sensi dell'art. 2, comma 1, prevede che sia l'Agenzia per l'Italia digitale (AgID) l'autorità competente per lo svolgimento dei compiti inerenti alla procedura di notifica per i servizi di intermediazione dei dati, nonché l'autorità competente alla registrazione di organizzazioni per l'altruismo dei dati. Essa è altresì chiamata, giusta il comma 2 della norma, a cooperare con l'Agenzia per la cybersicurezza nazionale, con l'Autorità garante della concorrenza e del mercato e con il Garante per la protezione dei dati personali, potendo altresì, a tal fine, stipulare specifici accordi di collaborazione non onerosi.

[28] Precisamente, chi scrive ha chiesto, tramite mail inviata in data 12 aprile 2024, «*if, under the discipline of DGA Regulation, public administrations, institutions and, in general, public entities could become member of a data cooperative*» che ha ricevuto risposta in data 15 aprile 2024.

[29] V. *https://commission.europa.eu/about-european-commission/departments-and-executive-agencies/communications-networks-content-and-technology_en*.

[30] Precisamente, a fronte della domanda presentata da chi scrive, tramite mail inviata in data 9 aprile 2024, in merito alla possibilità per un ente pubblico di partecipare ad una cooperativa di dati, è stata ricevuta la risposta chiarita nel testo in data 15 aprile 2024.

(Testo unico in materia di società a partecipazione pubblica, TUSP). Tale previsione, infatti, dispone che «le amministrazioni pubbliche possono partecipare esclusivamente a società, anche consortili, costituite in forma di società per azioni o di società a responsabilità limitata, *anche in forma cooperativa*»[31]. Si precisa che le pubbliche amministrazioni richiamate dalla norma non sono solo quelle incluse nell'art. 1, comma 2 del d.lgs. 165/2001[32], ma anche i «loro consorzi o associazioni per qualsiasi fine istituiti», «le autorità di sistema portuale», e soprattutto, tutti «gli enti pubblici economici» (che, come tali, sono estranei alla nozione di pubblica amministrazione, di cui al d.lgs. 165/2001). Si stabilisce così, con sufficiente chiarezza, che le pubbliche amministrazioni, intese in questo senso, possono essere socie (o titolari di strumenti finanziari che conferiscano diritti amministrativi) solo di società per azioni e società a responsabilità limitata, le une e le altre eventualmente declinate in forma cooperativa, con l'altrettanto sicura preclusione della possibilità di partecipare a società semplici, società in nome collettivo e società in accomandita semplice. Inoltre, in assenza di una espressa previsione nel testo dell'art. 3, comma 1, TUSP delle società quotate, si desume che, fra i tipi di società in cui è ammessa la partecipazione pubblica, non rientrano le società quotate. Infatti, l'art. 1, comma 5, TUSP stabilisce che «le disposizioni del presente decreto si applicano, solo se espressamente previsto, alle società quotate»[33].

Ecco che il TUSP, nell'introdurre una disciplina organica delle società a partecipazione pubblica, permette alle PA di sfruttare un modello organizzativo meno burocratico che si avvalga della maggiore elasticità prevista per le assunzioni e i rapporti anche temporanei di consulenza e collaborazione nell'ambito dell'impiego privato (con minori garanzie rispetto al pubblico impiego). In altri termini, l'ente opera a condizione che la sua partecipazione nelle forme societarie ammesse sia funzionale al perseguimento delle attività di diritto pubblico che gli sono proprie. È

---

[31] Per un commento, v. M. STELLA RICHTER JR., *Art. 3*, in *Codice delle società a partecipazione pubblica*, a cura di G. Morbidelli, Milano, 2018, p. 154 ss.

[32] Ai sensi della norma, «per amministrazioni pubbliche si intendono tutte le amministrazioni dello Stato, ivi compresi gli istituti e scuole di ogni ordine e grado e le istituzioni educative, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le Regioni, le Province, i Comuni, le Comunità montane, e loro consorzi e associazioni, le istituzioni universitarie, gli Istituti autonomi case popolari, le Camere di commercio, industria, artigianato e agricoltura e loro associazioni, tutti gli enti pubblici non economici nazionali, regionali e locali, le amministrazioni, le aziende e gli enti del Servizio sanitario nazionale l'Agenzia per la rappresentanza negoziale delle pubbliche amministrazioni (ARAN) e le Agenzie di cui al decreto legislativo 30 luglio 1999, n. 300».

[33] Sul punto, M. CALCAGNILE, *La razionalizzazione delle società a partecipazione pubblica*, in *Giorn. dir. amm*., 2017, 4, p. 443 che sottolinea come «la sottoposizione delle società quotate, ancorché a partecipazione pubblica, ai limiti ed agli oneri stabiliti dal D.Lgs. n. 175/2016 comporterebbe l'alterazione dei principi di parità di trattamento tra imprese pubbliche e private e quindi di libera iniziativa economica, perché le società a partecipazione pubblica quotate risulterebbero soggette a sistemi di controllo (ulteriori rispetto a quelli già previsti dal D.Lgs. n. 58/1998) suscettibili di interferire sulla loro ordinaria attività e comunque di generare costi cui non sarebbero tenuti i concorrenti privati».

pur sempre vero che, in varie previsioni del TUSP, emerge la natura pubblica (indisponibile) dell'interesse amministrato, nonché l'agire dell'ente in funzione del benessere della collettività anche quando costituisce o partecipa ad una società [34]. In proposito, basti solo menzionare l'art. 4, comma 1 TUSP che si apre con una delimitazione in negativo, vietando alle amministrazioni pubbliche di svolgere «direttamente o indirettamente, (…) attività di produzione di beni e servizi non strettamente necessarie per il perseguimento delle proprie finalità istituzionali» [35]. Del resto, la partecipazione di pubbliche amministrazioni alle fattispecie societarie previste nel TUSP rende possibile orientare l'attività di impresa in forma collettiva non solo alla realizzazione dell'egoistico interesse alla massimizzazione del profitto, ma anche al perseguimento di benefici collettivi e pubblici [36].

Orbene, le cooperative di dati, qui ipotizzate anche a partecipazione pubblica, e i gemelli digitali urbani possono, ad avviso di chi scrive, coordinarsi fra loro, secondo diversi possibili modelli operativi.

In primo luogo, si può verificare il caso in cui un ente territoriale promotore di un gemello digitale urbano entri direttamente a far parte di una o più cooperative di dati. In questa ipotesi, l'ente pubblico sarebbe sicuramente avvantaggiato dalla possibilità di accedere e utilizzare, su più fronti, le grandi quantità di dati, mutualisticamente condivise dagli altri membri della cooperativa. I dati così raccolti ben potrebbero essere fatti confluire nel gemello digitale urbano, unendosi a quelli già a disposizione dell'ente pubblico e che quest'ultimo abbia già sfruttato (anche) per la creazione del gemello digitale stesso. È, però, chiaro che, in una simile fattispecie, l'ente pubblico dovrebbe contribuire al buon funzionamento della cooperativa di cui è membro, mettendo a propria volta in condivisione i dati che è già nella condizione di poter utilizzare.

A tal fine non è superfluo ricordare la necessità di una base giuridica [37] che giu-

---

[34] Cfr. C.F. GIAMPAOLINO-F. PANETTI, *Le società a partecipazione pubblica*, in *Giur. comm*., 2023, 4, p. 529 ss., spec. p. 530.

[35] Si segnala che, in applicazione di tale previsione, si è espressa Corte cost., 22 aprile 2022, n. 86, tra le altre in *Giur. cost*., 2022, 2, p. 914 ss.

[36] Tali obiettivi convivono anche nella c.d. società *benefit* di cui alla l. 28 dicembre 2015, n. 208, commi 376 ss., così come rilevato da C.L. APPIO-D. DE FILIPPIS, *Sulla fallibilità delle società a partecipazione pubblica*, in *Giur. comm*., 2018, 4, p. 681.

[37] Sulle condizioni di liceità del trattamento, v. F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, cit., p. 110 ss.; D. POLETTI, *Le condizioni di liceità del trattamento dei dati personali*, in *Giur. it*., 2019, 12, p. 2783 ss.; ID., *Art. 6 GDPR. Liceità del trattamento*, in R. D'ORAZIO-G. FINOCCHIARO-O. POLLICINO-G. RESTA (a cura di), *Codice della* privacy *e* data protection, Milano, 2021, p. 191 ss.; M. DELL'UTRI, *Principi generali e condizioni di liceità del trattamento dei dati personali*, in V. CUFFARO-R. D'ORAZIO- V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, p. 179 ss.; con particolare riguardo al consenso al trattamento dei dati, *ex multis*, v. P. GALLO, *Il consenso al trattamento dei dati personali come prestazione*, in *Riv. dir. civ*., 2022, 6, p. 1054 ss.; C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, Torino, 2021; P. MANES, *Il consenso al trattamento dei dati personali*, Padova, 2001; V. BACHELET,

stifichi simili plurimi trattamenti di dati. Infatti, nel caso più semplice, il singolo individuo – interessato al trattamento – è membro di una cooperativa di dati e condivide con essa i dati a sua disposizione. Qui sarà egli stesso a prestare il proprio consenso al trattamento, conformemente a quanto previsto nel GDPR [38]. La questione, però, si complica nel caso in cui ad essere o a divenire membro di una cooperativa di dati sia un *data holder*, come, ad esempio, un'impresa individuale, una PMI o, nella nostra ricostruzione, un ente pubblico. In tale seconda opzione, il *data holder* che abbia già raccolto dati da più persone fisiche o giuridiche e intenda conferirli nella cooperativa, dovrà pur sempre giustificare ciascuna singola operazione in forza di un'idonea condizione di liceità [39].

È essenziale sul punto tenere in debita considerazione il principio di limitazione delle finalità, di cui all'art. 5, par. 1, lett. b), GDPR. Ai sensi di tale previsione, i dati personali devono essere «raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali». Si determina, infatti, un intreccio di consensi-autorizzazioni, l'uno susseguente all'altro, dove il primo deve necessariamente essere in grado di giustificare il secondo, così da renderlo valido.

L'ente pubblico-*data holder*, nel definire *ab initio* le finalità ed i mezzi del trattamento che intende effettuare, è tenuto ad informare adeguatamente gli interessati sul punto. Infatti, nel rispetto del principio di trasparenza, ciascun interessato deve essere messo in condizione di compiere scelte libere, in quanto informate, esercitando così il proprio diritto all'autodeterminazione informativa.

Al contempo, il *data holder* (che agisce qui come titolare del trattamento) è obbligato ad una corretta e ponderata organizzazione delle operazioni di trattamento da effettuarsi, sulla scorta del principio di *accountability*. Inoltre, l'ente pubblico è chiamato ad esprimersi sulla necessità e proporzionalità del trattamento [40], operan-

---

Il consenso oltre il consenso: dati personali, contratto, mercato, Pisa, 2023; E. TOSI, *Circolazione dei dati personali tra contratto e responsabilità: riflessioni sulla fragilità del consenso e sulla patrimonializzazione dei dati personali nella società della sorveglianza digitale*, Milano, 2023; S. THOBANI, *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità*, in *Eur. dir. priv*., 2016, 2, p. 513 ss.; G. COMANDÈ, *Leggibilità algoritmica e consenso al trattamento dei dati personali*, in *Danno e resp.*, 2022, 1, p. 33 ss.; A. VIVARELLI, *Il consenso al trattamento dei dati personali nell'era digitale: sfide tecnologiche e soluzioni giuridiche*, Napoli, 2019; sia poi consentito il rinvio a C. BASUNTI, *La (perduta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali*, in *Contr. e impr.*, 2020, 2, p. 860 ss.

[38] Tale consenso deve essere, infatti, rispettoso delle note caratteristiche espresse dall'art. 4, par. 1, n. 11), GDPR e, dunque, essere libero, specifico, informato e inequivocabile, altrimenti il trattamento non sarà lecito in mancanza di un'altra valida base giuridica *ex* art. 6 GDPR.

[39] Tale problematica viene posta in luce da F. BRAVO, *Le cooperative di dati*, cit., p. 798.

[40] V. EDPS, *Quick-guide to necessity and proportionality*, del 28 gennaio 2020; e EDPS, *Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the*

do, a tal fine, una valutazione "costi-benefici" che consenta il più giusto bilanciamento degli interessi in gioco, così da limitare al massimo la compressione dei diritti degli interessati e, in special modo, del diritto alla protezione dei dati personali.

In definitiva, laddove un ente pubblico intenda autorizzare la cooperativa di cui è membro ad accedere e a trattare i dati raccolti nell'ambito della propria attività, dovrà chiarire in modo adeguato agli interessati la finalità di destinare quegli stessi dati alla cooperativa, di guisa che gli interessati possano decidere consapevolmente in merito.

Potrebbe poi verificarsi il diverso caso in cui l'ente pubblico diventi membro della cooperativa di dati in un momento successivo rispetto alla raccolta del consenso da parte di taluni interessati di cui (già) tratta i dati personali. In tale fattispecie, ove per ovvie ragioni non si è potuto prestare un consenso riferito anche allo sfruttamento dei dati da parte della cooperativa, dovranno essere esaminate le finalità su cui si è fondato il consenso prestato a monte dall'interessato, al fine di vagliarne la compatibilità con quelle sorte successivamente e, segnatamente, con la possibilità di utilizzo dei dati da parte della cooperativa. L'ente pubblico-titolare potrebbe, infatti, in forza del principio di *accountability*, riscontrare tale compatibilità tra le finalità e non richiedere un ulteriore consenso all'interessato, dal momento che il legislatore europeo ha previsto [41] la possibilità di trattamento dei dati personali per finalità ulteriori rispetto a quelle per le quali i dati sono stati inizialmente raccolti, purché compatibili con queste ultime.

Diversamente, l'ente pubblico sarà tenuto a chiedere un ulteriore consenso all'interessato (o trovare una nuova e diversa base giuridica), in modo da ottenere l'ulteriore autorizzazione ad un utilizzo dei dati in questo senso, rendendo lecito il trattamento [42]. Si delinea, pertanto, una sorta di differenziazione delle logiche di utilizzo dei dati raccolti da parte dell'ente pubblico, in cui solo una parte dei dati potrà essere sfruttata (anche) dalla cooperativa in base alle logiche mutualistiche che le sono proprie. In altri termini, dovrà essere effettuato, caso per caso, il c.d. *compatibility assessment* [43]. Ciò, tenendo conto del fatto che la meritevolezza del *cooperative model* e la sua promozione sul mercato digitale non può certo condurre ad un irragionevole restringimento delle tutele offerte al *data subject* ed alla libertà di cui deve godere nell'esercizio del proprio diritto all'autodeterminazione informativa.

---

protection of personal data, del 19 dicembre 2019. Sul tema, si consenta il rinvio a C. BASUNTI, *Il principio di proporzionalità*, in F. BRAVO (a cura di), *Dati personali. Protezione, libera circolazione e* governance – *Vol. 1., Principi*, cit., p. 411 ss.

[41] V., in particolare, gli artt. 5, par. 1, lett. *b)* e 6, par. 4, GDPR, il *considerando* n. 50 GDPR, nonché l'art. 7 della Convenzione 108+ ed il relativo *Explanatory Report*, al punto 49.

[42] La ricostruzione del consenso-condizione di liceità come consenso di tipo autorizzatorio, idoneo a rimuovere un ostacolo posto dall'ordinamento al preesistente potere del titolare, viene efficacemente fornita da F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, cit., p. 140 ss.; ID., *Lo "scambio di dati personali" nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto*, in *Contr. e impr*., 2019, 1, spec. p. 40 ss.

[43] Al riguardo v. GRUPPO DI LAVORO *EX* ART. 29, *Opinion 03/2013 on purpose limitation*, *adopted on 2 April 2013*, spec. p. 20 ss.

Al netto del problema appena esposto, relativo alla circolazione dei dati tra interessati, enti pubblici e cooperative di dati, è bene esaminare ora l'altro possibile modello di cooperazione tra cooperative di dati e gemelli digitali.

Nello specifico, può accadere che la cooperativa di dati decida di condividere i dati collazionati con una *third party* che, nel nostro esempio, sarebbe l'ente pubblico. Quest'ultimo ben potrebbe poi utilizzare i dati ottenuti per creare e implementare un gemello digitale urbano. Potrebbe anche darsi che talune società cooperative vengano convertite, in piena conformità con le *rationes* perseguite dal *Data Governance Act*, in cooperative di dati. Così tali cooperative di dati potrebbero dialogare con il soggetto pubblico fornendo il proprio contributo all'azione amministrativa, qui declinata nello sviluppo di gemelli digitali urbani.

La condivisione dei dati tra una cooperativa di dati ed un ente pubblico deve avvenire sulla base di un accordo interno tra i membri della cooperativa, che deve necessariamente tenersi ben distinto dall'autorizzazione al trattamento dei dati fornito da ogni singolo socio della cooperativa. Il consenso al trattamento dei dati deve, infatti, essere tenuto distinto dal consenso fornito dal membro alla formazione della volontà della società cooperativa. Il consenso espresso nel contesto di maggioranze necessarie all'approvazione di delibere assembleari è funzionalmente diverso dal consenso-condizione di liceità.

In proposito, si è espressa la Corte di Cassazione in un caso di trattamento illecito effettuato da una società cooperativa sui dati di un socio lavoratore [44]. Nel caso vagliato, si è evidenziata la presenza di una asimmetria tra la cooperativa e il lavoratore, stante il timore di quest'ultimo di ripercussioni negative in caso di mancata prestazione del consenso al trattamento dei dati, idoneo a minare la libertà (e, quindi, la validità) del consenso eventualmente prestato. Secondo la S.C., nonostante il rapporto in questione abbia natura associativa e, dunque, siano gli stessi soci a contribuire alla formazione della volontà dell'ente tramite le delibere assembleari, il trattamento dei dati non può considerarsi legittimo quando fondato sulle sole decisioni dell'assemblea e sulla maggioranza emersa in seno ad essa. Il consenso al trattamento dei dati, pertanto, deve essere circondato da idonee garanzie, tali da determinare una adeguata ponderazione e consapevolezza dell'interessato, sicuramente incompatibili con eventuali condizionamenti che possono emergere nei rapporti di lavoro e nelle delibere assembleari. In questo senso, «il consenso è validamente prestato solo se espresso liberamente e specificamente in riferimento a un trattamento chiaramente individuato» [45].

---

[44] Il riferimento è a Cass., 1° giugno 2022, n. 17911, in *Giur. it*., 2022, 12, p. 2597 ss., con nota di S. Thobani. Il caso riguarda la pubblicazione, da parte di una società cooperativa, sulla bacheca aziendale, di dati relativi ai soci in merito a contestazioni disciplinari unitamente alle relative valutazioni effettuate dalla cooperativa stessa, mediante l'uso di "faccine" nell'ambito di un concorso a premi per i soci lavoratori, finalizzato ad incentivare condotte meritevoli tra i soci e la cui partecipazione era per loro obbligatoria.

[45] Così Cass., 1° giugno 2022, n. 17911, cit.; sull'argomento v. anche Cass., 25 maggio 2021, n.

Dunque, anche in questo secondo modello di interazione tra cooperative e gemelli digitali urbani è necessario svolgere un'indagine caso per caso che permetta qui di valutare le effettive circostanze in cui operano i vari consensi, tenendo presente che, all'interno della cooperativa di dati, «i due piani di *governance*, individuale e collettiva, rimangono distinti» [46].

Si aggiunga che la condivisione di dati da parte di una cooperativa di dati a favore di una parte terza deve pur sempre muoversi entro i binari dell'etica. A nostro avviso, se la *third party* è un ente pubblico, come può essere il comune promotore di un gemello digitale urbano, la finalizzazione etica del trattamento può considerarsi (almeno) presunta, tenuto conto del fatto che l'ente pubblico è tenuto a perseguire il bene collettivo attraverso la propria azione pubblica.

4.2. Fintraffic: un caso pratico di partecipazione pubblica nella creazione ed implementazione di un ecosistema di dati sul traffico.

La possibilità per un ente pubblico di partecipare ad una cooperativa di dati apre nuovi scenari di utilizzo dei dati, in modo funzionale al miglior esercizio dell'azione pubblica. Tale possibilità che, a parere di chi scrive, merita di essere valorizzata, ha, come detto, trovato un riscontro positivo da parte del *Senior Advisor* dell'Autorità competente per i servizi di intermediazione dei dati finlandese [47]. Nel citato riscontro, proprio al fine di giustificare la percorribilità di una simile tesi, e muovendosi pur sempre nel contesto territoriale della Finlandia, è stato suggerito l'esempio di Fintraffic [48].

A ben vedere, non si tratta di una cooperativa di dati a partecipazione statale, ma, comunque, di un gruppo societario che opera sotto la guida del Ministero del trasporto e delle comunicazioni locale. Fintraffic, una *Traffic Management Company*, delinea un moderno *Traffic Data Ecosystem*, per fronteggiare le sfide che il mercato digitale impone anche nel settore dei trasporti.

Tale gruppo societario unisce tutti coloro che operano nel contesto della mobilità e che decidano di aderire all'iniziativa, coordinandone le attività, nella prospettiva di un'economia dei dati equa, inclusiva e sostenibile nel mercato del traffico. In forza della cooperazione instaurata dalla società tra oltre duecento soggetti – *shareholder* e *stakeholder* nel nuovo paradigma dell'impresa sostenibile [49] –, essa offre servizi competitivi e scalari per il traffico e la mobilità sia sul territorio finlandese sia esportabili a li-

14381, in *Dir. inform*., 2021, 6, p. 1001 ss.; Cass., 2 luglio 2018, n. 17278, in *Guida al dir*., 2018, 31, p. 20 ss.

[46] Così F. BRAVO, *Le cooperative di dati*, cit., p. 790.

[47] Il riferimento è alla richiesta avanzata, tramite mail inviata in data 12 aprile 2024, che ha ricevuto risposta in data 15 aprile 2024, di cui si è detto in precedenza.

[48] Cfr. il sito *web* di Fintraffic: *https://www.fintraffic.fi/en*.

[49] Sia consentito il rinvio a I. SPEZIALE, *Il nuovo paradigma dell'impresa sostenibile*, in *Contr. e impr*., 2022, 3, p. 752 ss.

vello internazionale. L'obbiettivo è quello di consentire agli utenti di viaggiare in modo sicuro, a basse emissioni di Co2 e utilizzando forme di trasporto multimodale.

Un simile obiettivo, preme sottolinearlo, viene perseguito attraverso una strategia che sembra rispecchiare proprio il modello legislativo delle cooperative di dati.

Infatti, Fintraffic promuove la fiducia e la trasparenza nell'utilizzo dei dati e pone il suo *know-how* e la sua *expertise* a beneficio (anche) della collettività. In questa prospettiva, il gruppo societario favorisce la più ampia interazione con gli *stakeholders*: essi sono chiamati ad implementare il sistema dei dati in tempo reale, principalmente scaricando la *Fintraffic App* sui propri dispositivi mobili [50]. In una apposita sezione di tale applicazione, l'utente è sollecitato ad inviare segnalazioni relative al traffico che possono presentarsi utili in una condivisione collettiva, in vista dello sviluppo congiunto ed aperto del proprio ecosistema di dati. Pur non potendosi parlare qui della partecipazione spiccatamente democratica riferibile alle cooperative di dati, emerge chiaramente l'intento di tratteggiare un *network* degli *stakeholders*, caratterizzato da un *collaborative ecosystem* [51].

Le modalità attuative poste alla base del funzionamento di Fintraffic tendono ad avere valenza generale, senza differenziazioni legate alla singola modalità di trasporto. Fintraffic comunica attivamente le misure concordate, nonché i progressi e i risultati via via ottenuti, in modo tale da facilitare l'interazione tra gli operatori in ciascuna fase del processo. Il gruppo societario si presta così ad essere un punto di riferimento per *start-up* e PMI, agevolandone l'ingresso e l'affermazione nel mercato rilevante. Particolare importanza assume, in ciascuna attività promossa da e attraverso Fintraffic, il rispetto della legislazione vigente, con speciale riguardo alla normativa a tutela del diritto alla protezione dei dati personali.

I benefici che un simile modello offre sono chiari.

Da un lato, chi fornisce i servizi ha agile accesso ai dati sul traffico costantemente aggiornati, così da poter migliorare la propria offerta e formare reti commerciali con altri *competitors*; dall'altro, gli *users* beneficiano di servizi più sicuri, sostenibili e convenienti grazie alla più ampia condivisione dei dati promossa da Fintraffic. Tra i menzionati *users*, spiccano gli operatori logistici che si vedono fornire catene logistiche integrate ed efficienti perché adattate alle varie forme di trasporto multimodale con un importante risparmio di costi, sempre in ragione della condivisione dei dati.

Ma vi è di più.

L'ecosistema dei dati sul traffico tratteggiato dal gruppo societario riconducibile a Fintraffic risponde anche alla logica, che è poi quella più alta e più nobile del diritto, di promuovere un dato modello di sviluppo della società e dell'economia [52]: i dati sul sistema di trasporto, così come raccolti e valorizzati dall'impresa, concor-

---

[50] V. *https://www.fintraffic.fi/en/digitalservices/fintraffic_app*.

[51] V. *https://www.fintraffic.fi/en/news/finnish-businesses-launch-collaboration-exporting-traffic-data-services*.

[52] In argomento, v. N. ZORZI GALGANO, *Il contratto di consumo e la libertà del consumatore*, in F. GALGANO (diretto da), *Tratt. dir. comm. e dir. pubblico dell'econom*., Padova, 2012, p. 77.

rono alla costruzione di una società e un'economia nel segno della sostenibilità.

A vantaggio della collettività, Fintraffic tutela l'ambiente e promuove la ricerca scientifica. In prima battuta, infatti, per suo tramite, viene garantito un utilizzo maggiore di trasporti pubblici e condivisi in alternativa alle auto private, determinando un traffico più pulito. La riduzione dell'impatto ambientale da circolazione stradale viene altresì garantito, grazie all'utilizzo dei dati nella mappatura delle infrastrutture urbane e nel tracciamento dei flussi di traffico, implementando così una circolazione più efficiente. Inoltre, l'enorme quantità di dati che l'impresa è autorizzata a trattare è messa a disposizione dei soggetti che svolgono attività di ricerca scientifica, anche a livello internazionale, volta al progresso dei servizi di trasporto urbano.

Fintraffic intende poi promuovere un più serrato dialogo tra settore pubblico e settore privato che non si limiti al solo contesto territoriale finlandese, ma che, pur utilizzato primariamente in Finlandia, possa trovare ulteriore applicazione in altri Paesi e mercati. Il *Traffic Data Ecosystem* crea, infatti, nuove opportunità di *business* per i soggetti privati e, al contempo, mette a disposizione degli enti territoriali *assets* fondamentali per lo svolgimento dell'attività di buona amministrazione del territorio. Del resto, i dati così utilizzati potrebbero avvantaggiare i privati nelle proprie analisi di *business planning* in misura maggiore rispetto alle tecniche di stampo più tradizionale. Ecco che, ad esempio, i gestori di esercizi commerciali potrebbero pianificare l'eventuale apertura di nuovi punti vendita, ovvero decidere se acquisire o meno aree da destinare al parcheggio delle auto dei clienti, in una realtà urbana che, preme sottolinearlo, appare segnata dal crescente sviluppo dell'*e-commerce* e del *food delivery*.

Sul fronte pubblico, i menzionati dati hanno un'importanza cruciale nel (ri)definire i flussi di traffico in base alle varie fasce orarie, così come nella scelta di implementare determinati servizi di trasporto pubblico. Si pensi, ad esempio, alla valutazione in ordine alla creazione di una linea tramviaria in una zona urbana servita solamente da mezzi di trasporto su strada e che, proprio a seguito della *data analysis*, sia risultata non sufficientemente collegata. Quegli stessi dati potrebbero poi essere utilizzati per una migliore distribuzione delle aree di parcheggio, in base alle concrete esigenze della platea cittadina. E ancora: essi potrebbero servire al singolo ente territoriale per l'attuazione di mirate politiche di sicurezza urbana, grazie, tra l'altro, all'uso di sistemi di videosorveglianza.

5. Osservazioni conclusive.

Da quanto affermato è possibile prospettare un proficuo dialogo tra cooperative di dati e gemelli digitali urbani.

Le indicazioni dettate recentemente dal legislatore europeo sono sporadiche e talvolta creano un vero e proprio corto circuito logico, in relazione sia alle cooperative di dati sia ai gemelli digitali che, nella declinazione di gemelli digitali urbani, non conoscono alcuna previsione normativa. Tuttavia, le applicazioni pratiche di cui si è dato conto, unitamente agli obiettivi generali perseguiti dalla Stra-

tegia europea per i dati, spingono nella direzione appena ipotizzata.

Infatti, la progressiva emersione nella prassi di gemelli digitali urbani, come nei casi analizzati di Singapore, Barcellona e Bologna, richiede un massivo afflusso di dati che possono e devono essere veicolati (anche) da e verso gli enti pubblici che ne sono promotori all'interno di simili innovative realtà. La struttura organizzativa delle cooperative di dati, volte, tra l'altro, alla realizzazione di finalità di interesse generale, si rivela uno strumento particolarmente efficace nella creazione e implementazione di gemelli digitali urbani.

Del resto, i dati collazionati da una cooperativa seguono le logiche del (neo)mutualismo digitale e, in questo senso, sono valorizzati attraverso un utilizzo improntato a solidi valori etici. L'utilizzo dei dati in chiave etica mira ad affrontare e vieppiù a risolvere le sfide che la tutela del benessere collettivo richiede, *in primis*, alle pubbliche amministrazioni. Non a caso, gli esempi di gemelli digitali in essere e in divenire pongono, quali obiettivi centrali della loro azione (pubblica), la lotta ai cambiamenti climatici, il miglioramento della mobilità cittadina e il progresso nella ricerca scientifica.

L'interazione tra soggetti pubblici – che vogliano munirsi di gemelli digitali urbani – e cooperative di dati, nel senso di una partecipazione dei primi alle seconde (anche) sulla base degli schemi operativi ipotizzati nel presente lavoro, non è (stata ancora) contemplata dal formante legislativo europeo.

Non per questo, però, essa appare preclusa.

Le stesse *rationes* sottese alla Strategia europea per i dati e, specialmente, al *Data Governance Act*, sembrano avvalorare l'opportunità di tale interazione. Quest'ultima trova poi conferma nei riscontri che chi scrive ha ricevuto sia dal *Senior Advisor* della *Data Space Europe* finlandese sia dal *Team Leader* della *Unit G1 – Data Policy & Innovation* del *Directorate-General for Communications Networks, Content and Technology*, istituito in seno alla Commissione europea [53]. Proprio in Finlandia spicca l'esempio virtuoso di Fintraffic: il gruppo societario, a partecipazione statale, che agisce nel settore dei trasporti, declinando in chiave di mobilità sostenibile l'utilizzo dei dati, sulla scorta, almeno in parte, di quegli stessi principi che, più tipicamente, ispirano l'agire di un fornitore di servizi di intermediazione dei dati.

La strada da percorrere è sicuramente *in progress* e non può, soprattutto in futuro, prescindere da un maggiore coinvolgimento del legislatore sul tema, a livello europeo come pure nazionale.

Dunque, appaiono di particolare rilevanza le ricostruzioni degli interpreti che devono essere indirizzate a tratteggiare un quadro di massima valorizzazione dei dati, senza che ciò comporti una ingiustificata compressione delle prerogative proprie della persona umana. In questa direzione, si muove il *cooperative model* che, specie nelle sue (possibili) applicazioni nel settore pubblico, prima fra tutte i gemelli digitali urbani, promuove il benessere degli individui *uti singuli* e della società tutta.

---

[53] V. *supra* par. 4.1.

Capitolo XXIX

Cooperative di dati e mondo assicurativo: potenzialità, nuove prospettive e inediti scenari nell'utilizzo dei dati

Giulia Rossi

Abstract: The "extractive" model used so far in the insurance sector has guaranteed the accumulation of significant quantities of digital information in the hands of very few subjects who, by exploiting this competitive advantage, have created real monopolies aimed at only increasing the wealth and profitability of large companies. Like an inverted pyramid, however, we could move on to a data development and management model oriented towards protecting the dignity and freedom of data subjects, which would have as its final result a primary advantage for the data subject himself, then for the insurance company and finally for society as a whole.

1. L'importanza dell'utilizzo dei dati nel settore assicurativo.

Le applicazioni pratiche hanno mostrato come le cooperative dati costituiscano un nuovo sistema di gestione dei dati con carattere imprenditoriale alternativo rispetto agli schemi tradizionali ispirati a visioni di capitalismo estrattivo dei dati stessi [1]. La sfida del futuro è sicuramente quella di porre la condivisione dei dati

[1] Cfr. in questo senso L. PETRONE, *Il mercato digitale europeo e le cooperative di dati*, in *Contratto e impresa*, 2023, n. 3, pp. 880-817, il quale sostiene che il sistema delle cooperative di dati ha ottenuto crescente interesse soprattutto in un'ottica di implementazione delle sempre più diffuse *smart cities*, ovvero città intelligenti, in cui le risorse, anche informatiche e digitali, dovrebbero essere gestite con particolare cura al fine di funzionalizzarle ad un miglioramento della qualità della vita dei cittadini. Del resto, prosegue l'a., il modello di sviluppo e di gestione dei dati da parte delle cooperative di dati sarebbe finalizzato a garantire la dignità e la libertà dei cittadini europei a cui detti dati si riferiscono, valorizzando il capitale umano sotteso ad ogni iniziativa che implica l'utilizzo di dati. In senso più ampio sulla normativa dei dati personali: G. ALPA, *La normativa sui dati personali. Modelli di*

degli utenti al servizio del benessere della collettività: in sostanza, da utente passivo e sfruttato dalle grandi compagnie digitali, l'utente si trasformerebbe, attraverso la cessione consapevole dei propri dati, in artefice del processo di miglioramento dei servizi offerti dalle grandi imprese dei vari settori [2].

Orbene, questo discorso, in ambito assicurativo, si incastra alla perfezione con lo scenario attualmente esistente e con le nuove prospettive che la normativa in materia permette di immaginare: è un settore, del resto, che da sempre è ruotato intorno ai dati [3] e che, nell'ultimo decennio, è stato fortemente condizionato dalla digitalizzazione e dall'evoluzione degli strumenti di analisi dei dati. Ciò è tanto vero che ad oggi le compagnie assicurative riescono ad avere accesso, e processare, un numero incredibilmente ampio di dati, aventi peraltro origine e fonti diverse.

Nella logica del mercato capitalistico di estrazione dei dati, pertanto, le compagnie assicurative hanno un ruolo centrale nel lucrare sulle tracce digitali lasciate dai clienti che si stanno progressivamente spostando sul mercato online per concludere contratti assicurativi o per rinnovare polizze già esistenti. Ci sono addirittura, polizze denominate *usage-based* che sono strutturate proprio per assecondare le abitudini, le inclinazioni, la prassi e la ripetitività di determinate azioni da parte dei clienti [4].

Le compagnie assicurative, in sostanza, hanno oramai imparato a monetizzare i dati per ottenere un vantaggio competitivo sui loro avversari [5]: così, se gli analisti prevedono che il mercato globale della monetizzazione dei dati crescerà dai 2,3 miliardi di dollari del 2020 ai 6,1 miliardi di dollari entro il 2025, l'integrazione di programmi UBI nella mappa applicativa digitale (CRM, Trouble ticket, CDP, etc.),

---

lettura e problemi esegetici, in V. CUFFARO-V. RICCIUTO-V. ZENO ZENCOVICH (a cura di), *Trattamento dei dati e tutela della persona*, Milano, 1998, p. 3 s.

[2] Così V. RINALDI, *Co-app e Big Data: per un paradigma alternativo nella gestione dei dati*, in *Pandora*, 2020, 3.

[3] In un passato ormai remoto, ovvero prima dell'avvento di Internet, gli assicuratori utilizzavano dati storici abbinati ad inferenze sul futuro per valutare il rischio nel modo più accurato possibile e prendere decisioni di sottoscrizione informate: cfr. E. SEVERONI, *Cos'è la data-driven insurance e quali sono le sue potenzialità*, reperibile in *www.doxee.com*.

[4] La *usage-based insurance* (assicurazione basata sull'utilizzo o UBI) è un tipo di assicurazione che utilizza un dispositivo, come uno smartphone o un device telematico, per tracciare e misurare il comportamento di un individuo al fine di determinare il premio assicurativo. Negli ultimi anni, sempre più compagnie assicurative si sono orientate verso polizze *usage-based*, che offrono ai clienti la possibilità di adattare la copertura alle loro esigenze concrete e di pagare esclusivamente per quello di cui hanno bisogno, quando ne hanno bisogno. Investire nelle polizze *usage-based* permette di utilizzare le informazioni ottenute per massimizzare i ricavi elaborando soluzioni in linea con le tendenze e le richieste di ogni utente; implementare più efficaci sistemi di automazione; strutturare comunicazioni mirate per convincere i clienti esistenti a rimanere più a lungo, a rinnovare e ad acquistare nuovi prodotti e servizi aggiuntivi.

[5] V. RICCIUTO, *La patrimonializzazione dei dati personali*, in V. CUFFARO-R. D'ORAZIO-V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, p. 28 ss., già al tempo della direttiva 96/45/CEE aveva rilevato come la stessa non disconosceva la formazione e lo sviluppo di un mercato dei dati, considerati anche nella loro valenza patrimonialistica.

consentirà alle agenzie assicurative di valorizzare l'enorme quantità di dati prodotta e raccolta incrementando i loro introiti di quasi il 40%.

In questo modo le assicurazioni trasformeranno, come già stanno facendo, i dati sul comportamento dei loro clienti in nuovi flussi di entrate.

Questo modello "estrattivo" di utilizzo dei dati, tuttavia, ha un lato oscuro di non poco rilievo: l'accumulo di notevoli quantità di informazioni digitali in mano di pochissimi soggetti che sfruttando il vantaggio competitivo creano veri e propri monopoli.

In questo contesto la grande opportunità di applicare il modello delle cooperative di dati nel settore assicurativo sarebbero indiscutibilmente enorme: si passerebbe dal modello imprenditoriale lucrativo basato sullo sfruttamento dei dati altrui, ad un modello di sviluppo e di gestione dei dati dei cittadini europei orientato alla tutela della dignità e della libertà degli stessi [6]. Tutto questo, peraltro, renderebbe giustizia anche allo sforzo del legislatore eurounitario di creare un mercato unico digitale e offrire ai cittadini un modo per esercitare potere negoziale nell'utilizzo dei propri dati [7]: in altri termini, con il modello cooperativo di controllo dei dati si restituirebbe centralità all'individuo garantendo un controllo diffuso dei dati da parte dei relativi interessati. Del resto, i dati andrebbero considerati come un nuovo tipo di capitale che viene conferito da parte dei soci nella cooperativa per raggiungere, travalicando il tornaconto individuale, un interesse collettivo più ampio sia in termini di benessere della società tutta, sia dell'economia e sia del mercato settoriale in cui la specifica cooperativa opera.

2. Le Cooperative di dati e il mondo assicurativo: quali prospettive?

Nel mondo delle assicurazioni si deve partire dal concetto che le milioni di scatole nere delle auto dei clienti delle assicurazioni monitorano ogni giorno strade, viabilità, conducenti di auto private e abitudini di guida, generando una quantità di dati ed informazioni pertinenti alle vie più percorse, alle più pericolose, alle meno

---

[6] Così come suggerito da L. PETRONE, *Il mercato digitale europeo e le cooperative di dati*, cit., p. 15.

[7] Senza pretese di esaustività basti pensare che accanto alle esigenze di protezione dei dati personali disciplinate attraverso il Reg. UE n. 679/2016, il legislatore europea ha introdotto il Reg. UE 868/2022 contenente norme sulla *Governance* europea dei dati (*Data Governance Act*), in cui è stata fortemente rimarcata l'intenzione di stimolare una maggiore condivisione dei dati aumentando la fiducia dei cittadini europei nella neutralità e nell'affidabilità dei servizi di intermediazione. L'art. 2, par. 1, n. 11 Reg. UE 2022/868, in merito ai servizi di intermediazione, recita: il «servizio mira ad instaurare, attraverso strumenti tecnici, giuridici o di altro tipo, rapporti commerciali ai fini della condivisione dei dati tra un numero indeterminato di interessati e di titolari dei dati, da un lato, e gli utenti dei dati, dall'altro (…)». All'interno poi delle 3 tipologie di servizi di intermediazione si colloca, art. 10, co. 1, del Reg. 2022/868, proprio i servizi di cooperative dati. Su tutto, v. F. BRAVO, *Le cooperative dei dati*, in *Contratto e impresa*, 2023, n. 3, pp. 757-799, nonché L. PETRONE, *Il mercato digitale europeo e le cooperative di dati*, cit., pp. 7-8.

sorvegliate, ai momenti e ai luoghi in cui si formano gli ingorghi, alle cause più diffuse di incidenti, alle fasce orarie più frequenti in cui gli stessi incidenti si verificano e così via. Le compagnie assicurative, inoltre, si avvalgono anche dell'attività di *data sharing*[8], prelevando ulteriori informazioni relative ai propri clienti attraverso la condivisione di dati con fornitori di diversi settori, ed analizzando e incrociando i dati così ottenuti, per raggiungere tre vantaggi fondamentali: il miglioramento della capacità di valutazione del rischio[9]; la capacità di offrire prodotti personalizzati[10]; la possibilità di prevenire le frodi assicurative[11].

Non è un caso che in America sia stata sperimentata, a livello assicurativo, una piattaforma (accessibile anche tramite una app), finalizzata – tra i vari servizi– anche alla condivisione dei dati "lato assicuratori": il principio è che l'analisi è valida tanto quanto i dati su cui viene eseguita, e le previsioni intelligenti richiedono la raccolta di grandi volumi di dati di settore rilevanti. Quando si tratta di modellistica predittiva, più dati significano previsioni migliori: l'osservazione di un gran numero di sinistri può prevedere risultati più accurati. Tuttavia, le osservazioni degli assicuratori sono limitate dal numero di sinistri che essi stessi elaborano e gestiscono. Sebbene un assicuratore possa spesso ottenere buoni risultati solo con i propri dati, tanti più risultati performanti potrebbero essere realizzati con l'utilizzo dei dati relativi ai sinistri dell'intero settore. Ma raccogliere e aggregare tali dati da più assicuratori è difficile.

Ecco perché realizzare un sistema innovativo di "cooperazione" denominato *Guidewire*, ovvero una piattaforma che riunisce, gestisce e analizza dati per migliorare le prestazioni operative e affrontare i punti critici del settore[12]. Quando un membro della *Data Cooperative* accede ai sistemi core di *Guidewire*, contribuisce in modo sicuro all'attività della piattaforma con le proprie richieste di indennizzo e

---

[8] In argomento, per una trattazione più diffusa dei servizi di *data sharing* si rinvia a F. BRAVO, *Intermediazione di dati personali e servizi di* data sharing *dal GDPR al* Data Governance Act, in *Contratto e impresa Europa*, 2021, 1, p. 199.

[9] La condivisione dei dati tra diverse fonti, come i fornitori di servizi sanitari o di trasporto, permette di stimare più accuratamente il rischio associato ad un determinato cliente o ad una specifica polizza. Per esempio, i dati sullo stile di vita, i fattori di rischio medici o le abitudini di guida possono essere utilizzati per valutare il rischio di malattie o incidenti.

[10] Grazie ai dati ottenuti da più fonti si possono creare polizze "su misura" per i clienti che coprono esattamente i rischi a cui sono esposti, evitando il sovrapprezzo o la sottostima di alcune situazioni. Una compagnia assicurativa potrebbe utilizzare i dati sui comportamenti di guida per offrire tariffe personalizzate ai guidatori più prudenti o coperture aggiuntive per i clienti con particolari condizioni di salute.

[11] L'analisi dei dati permette di intercettare con più facilità false denunce, richieste di risarcimento eccessive o altre attività fraudolente ai danni della compagnia assicurativa.

[12] *Guidewire* opera in tutto il mondo: la *Data Cooperative* è ora globale e conta 15 assicuratori membri, con più di 35 membri aggiuntivi in fase di *onboarding*. La cooperativa è attualmente alimentata da 25 milioni di richieste in più settori di attività, tra cui la compensazione personale, commerciale e dei lavoratori. Man mano che il volume dei dati nella cooperativa cresce, le informazioni ricavate diventeranno più potenti.

sottoscrivendo i dati. Questi dati di settore vengono quindi raggruppati, analizzati e valorizzati, in termini monetari e non, ad esclusivo vantaggio di tutti i membri della *Data Cooperative*.

Il modello così realizzato in ambito assicurativo, per alcuni aspetti, è lo schema attualmente in circolazione più simile a quello di una cooperativa di dati come disciplinata e regolamentata dal Reg. UE 868/2022: le compagnie assicurative si aggregano per massimizzare i propri profitti, condividere un obiettivo comune e generare – tramite la piattaforma – ulteriore valore dalla raccolta e messa in condivisione dei dati. Potremmo sostenere – secondo i modelli di operatività che le cooperative dati possono utilizzare per l'erogazione dei propri servizi [13], che lo schema proposto da *Guidewire* rientrerebbe nella tipologia *Member to member* (*intra-cooperative*) secondo cui i dati vengono condivisi tra i singoli membri della cooperativa, mentre quest'ultima assume un ruolo di facilitatore dello scambio di dati, ossia di "intermediario" tra i singoli membri o soci. In tal modo ad un socio (la compagnia assicurativa) verrebbe consentito di accedere a determinati dati, ritenuti utili in sé, per il riuso, oppure ai fini della formazione di un *benchmark* per la valutazione di una determinata attività o di un determinato servizio o per comprendere, appunto, il livello di *performance* di una determinata azione.

Tale schema, sebbene apprezzabile per i risvolti di incremento della produttività, miglioramento dei servizi resi, aumento delle performance aziendali anche a vantaggio della clientela, mantiene in sé, tuttavia, un aspetto insidioso e poco coerente con la nuova visione europea di gestione e utilizzo dei dati: non risponde in alcun modo a logiche solidaristiche e mutualistiche, in quanto non viene introdotto un modello alternativo virtuoso e ad alta sostenibilità sociale di estrazione dei dati, ma si limita a massimizzare il benessere delle imprese assicurative che aderiscono al progetto, per aumentarne i propri profitti e accrescere i loro risultati in termini di *performance*.

Diverso sarebbe, invece, ipotizzare, una cooperativa dati tra i singoli clienti del settore assicurativo, ad oggi non esistente in nessun paese: ipotizziamo quindi uno schema capovolto sia in termini di soggetti che aderiscono, sia in termini di soggetti che conferiscono i dati e che mirano, per tale ragione, al raggiungimento di un determinato obiettivo comune, sia, infine, in termini di vantaggi da massimizzare per i *members*, nell'ottica di una valorizzazione estrema dei dati immessi nella cooperativa.

L'operazione si dovrebbe realizzare mediante la costituzione di una cooperativa nel settore delle assicurazioni i cui membri siano i clienti delle compagnie assicurative, dunque gli interessati: la cooperativa funzionerebbe mediante una app e/o una piattaforma fornendo servizi di consulenza assicurativa e procacciamento della soluzione contrattuale (polizza assicurativa) più adatta alle esigenze del cliente. I *Members*, tramite l'app o la piattaforma gestirebbero e controllerebbero direttamente i propri dati generati nella fornitura del servizio, stabilendo se e quando metterli in

[13] In argomento si veda diffusamente F. BRAVO, *Le cooperative dei dati*, cit., pp. 757-799, ove ulteriori e ampi riferimenti anche stranieri.

condivisione. Detti dati, tuttavia, una volta raccolti ed analizzati dal sistema della *data cooperative* genererebbero un vantaggio, non solo per il singolo, ma per tutti i suoi soci in termini di valorizzazione dei risultati ottenuti: scontistiche, contratti personalizzati, gestione sinistri con tempi ridotti e così via.

L'assicurato, in altri termini, potrebbe giovarsi dei dati analizzati dal sistema per incrementare a proprio vantaggio l'efficienza del servizio assicurativo: individuare le tariffe più basse in base alle compagnie; i migliori centri di assistenza in caso di sinistri; l'assunzione e la valutazione del rischio da parte delle compagnie per scegliere quella più competitiva.

A ciò si aggiunga che tutti i dati immessi nella cooperativa potrebbero anche essere valorizzati in termini monetari qualora la stessa cooperativa avesse mandato per concedere ("intermediare") a terzi, pubblici o privati l'accesso ai dati. Pensiamo all'ipotesi in cui l'app fosse utilizzata anche per la gestione sinistri con la conseguente raccolta di tutti i dati relativi ai luoghi, ai tempi, alle modalità in cui tali sinistri avvengono (una sorta di scatola nera che torna al suo legittimo proprietario, l'assicurato) (*sic*!) [14].

Ebbene, l'attività negoziale con terzi, da parte della cooperativa di dati in ambito assicurativo, permetterebbe di realizzare anche un'utilità sociale di non poco rilievo: pensiamo a come l'aggregazione dei dati assicurativi fornita dai molteplici assicurati, unita alla *data analysis*, aiuterebbe gli enti pubblici a sviluppare politiche di viabilità e/o interventi sul traffico in grado di far scendere statisticamente, ad esempio, il numero dei sinistri cittadini nonché migliorare la stessa sicurezza urbana. Da questo punto di vista, si realizzerebbe davvero il perseguimento di un interesse sovraindividuale di carattere sociale, virtuoso ed altamente funzionale al benessere della collettività tutta e non già dei singoli interessati [15].

Ma non è tutto: una cooperativa di dati così intesa in ambito assicurativo potrebbe portare dei benefici e dei vantaggi anche alle stesse compagnie assicurative. Se esse, infatti, avessero accesso ai predetti dati tramite l'attività di intermediazione della cooperative, esse riuscirebbero a pianificare, ad esempio, l'apertura di nuovi punti vendita in determinate zone ove la richiesta e le esigenze di protezione risultassero, dall'analisi dei dati, più alte; oppure potrebbero destinare maggiori operatori dediti al servizio clienti oppure all'assistenza in caso di sinistri o, infine, potrebbero finanche ipotizzare nuove formule contrattuali (polizze) rispondenti alle specifiche richieste/esigenze emerse dall'analisi dei dati forniti, in modo da performare l'offerta dei propri servizi ad una clientela specifica.

---

[14] In quest'ottica i soci trasferirebbero in cooperativa i dati, personali e non, che li riguardano avendo certezza di mantenere il controllo, tenuto conto delle caratteristiche tipiche di questa forma di impresa collettiva: così, L. PETRONE, *Il mercato digitale europeo e le cooperative di dati*, cit., p. 11.

[15] Le cooperative sono ancorate a una serie di principi concordati a livello globale: adesione aperta e volontaria; controllo democratico dei membri; partecipazione economica dei soci; autonomia e indipendenza; istruzione, formazione e informazione; cooperazione tra cooperative; e, soprattutto, la preoccupazione per la comunità.

In altri termini, uno schema del genere, travalicherebbe i confini di un tornaconto individuale e, comunque limitato ai soli membri della cooperativa, e consentirebbe di adottare decisioni migliori, incrementare il benessere, ottenere migliori condizioni economiche e, persino, ricavare un possibile guadagno economico monetizzando i dati a beneficio di soggetti terzi [16].

Se dunque con l'unico modello ad oggi in circolazione, si mira a generare un vantaggio alle società che svolgono attività di impresa assicurativa, al fine di rendere il processo di fornitura del servizio più competitivo ed efficiente massimizzandone i profitti, con il modello mutualistico l'analisi e la raccolta dei dati avvantaggerebbe tre tipologie di soggetti: in primo luogo, il singolo assicurato, poi la cooperativa medesima e, infine, i soggetti terzi (pubblici o privati che siano) [17].

L'utente si trasformerebbe, attraverso la cessione consapevole dei propri dati, davvero in artefice del processo di miglioramento dei servizi offerti al livello assicurativo [18], con ricadute positive anche dal punto di vista sociale ed ambientale [19].

---

[16] Così F. BRAVO, *Le cooperative dei dati*, cit., pp. 757-799, in merito all'esame di un modello già in circolazione, in America, nel settore dei trasporti: Driver's Seat. In argomento si veda anche G. ALPA, *La proprietà dei dati personali*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, 2019, p. 11 ss.

[17] In argomento si veda G. RESTA, *La regolazione digitale nell'Unione europea – pubblico, privato, collettivo nel sistema europeo di governo dei dati*, in *Riv. trim. dir. pubbl*., 2022, 4, p. 971; nonché le riflessioni di F. BRAVO-J. VALERO TORRIJOS, *Data in the Public Sector and Data Valorisation*, in *European Review of Digital Administration & Law (ERDAL)*, 2022, Vol. 3, n. 2, pp. 5-8.

[18] L. LIONELLO, *La creazione del mercato europeo dei dati: sfide e prospettive*, in *Diritto del Commercio Internazionale*, 2021, 3, p. 675.

[19] Ad oggi abbiamo già casi di cooperative assicurative di utenti finalizzate a massimizzare gli interessi e i vantaggi dei soci, in cui però il *focus* non sono i dati ma i bisogni degli assicurati (ricerca di soluzioni assicurative adeguate ed economicamente più convenienti). Cfr. per un es. Cooperativa Insieme.

Capitolo XXX

Le cooperative di dati nel settore bancario per la valutazione del merito creditizio: un alleato per le banche cooperative e per i clienti?

Margherita Zappatore

Abstract: New technologies, and in particular big data, are at the heart of the «Digital revolution 4.0», which has profoundly innovated not only the world of science and technology but also the banking, insurance and financial sector. Regarding the banking sector, the impact of new technologies has been considered «revolutionary» for its multiple uses as the one for the assessment of the creditworthiness of a customer that allows to obtain, thanks to the immense pool of data analyzed, a more accurate and capillary assessment than the traditional one. The traditional assessment of creditworthiness, in fact, suffers from the difficulty of finding and accessing the information contained in the hard data. The innovative evaluation carried out through big data is capillary thanks to the huge amount of data collected and analyzed. However, the data in question derive mostly from the use of social networks and the internet, which contain the information released by a single user on the web, of a different nature and origin. The data transmitted by the user during the use of social networks, such as Facebook, Twitter and Instagram, are also subject to analysis. These data represent the new «black gold», as it is able to provide information on the propensities and preferences of each individual user, useful not only to modulate the offer of a product but also to predict the behaviors of the same in the world of the market or the finance. Although credit assessment obtained by big data and social data could appear more accurate than the traditional one, conducted with «hard» data, especially when relating to the credit history of a customer who lives in developing countries or in countries characterized by a low income, there are some critical profiles regarding the effectiveness of the results and the accuracy of the credit reference and the risk of a damage caused to the customer who will be granted a credit that will not be able to repay or be refused in a discriminatory way a credit to which it would have been entitled. There are also other critical profiles according to the risk of obtaining a distorted credit reference, from which an erroneous creditworthiness would result, and the existence of distortive and discriminatory effects. On the merits, some foreign cases have ascertained this risk as the Kevin Johnson case against American Express and the case of the Non-Discrimination Ombudsman at the Finnish Non-Discrimination and Equality Tribunal. In recognition of this, data cooperatives could become useful tools, in the credit assessment process, for the collection of customer da-

ta for the benefit of customers and banks, especially cooperatives banks which are closer to the territory and have smaller assets than those of large banking companies. These banks could provide access to a wider range of data from financial sources and not finance, while avoiding the use of big data from social networks. Thus, banks could make a more accurate assessment of credit risk, reducing the risk of consumer overindebtedness and business failure, and improving the overall quality of the credit portfolio. In addition, they could help identify predictive signals that can affect a customer's ability to refund, such as changes in spending patterns, abnormal financial behavior, or changes in demographic data, by anticipating and taking measures to mitigate credit risk. Ultimately, data cooperatives could help cooperative banks in the process of assessing the creditworthiness of their customers without recourse to external services; At the same time, they could lead to greater customer protection by ensuring that social data is not used to determine the amount of funding to be granted. This is an unexplored path – but equally worthy of research and study – as there are no similar experiences in the banking sector, nor, in more general terms, in other sectors in the national context, unlike what has happened, until now, overseas.

1. La *digital economy*: i *big data* come il nuovo «oro nero» (anche) nel settore bancario.

La «Rivoluzione digitale 4.0»[1], di cui i *big data* quale nuovo «oro nero»[2] ne rappresentano il cuore pulsante, sta profondamente innovando non soltanto il mondo della scienza e della tecnica ma anche il mondo del diritto. Dall'avvento della tv

[1] G. OLIVI, Big Data, *metadati e intelligenza artificiale: modelli di business e profili di valutazione*, in *Il dir. ind*., 2018, 5, p. 421.

[2] R.H. WEBER, *Data portability and big data analytics. New competition policy challenges*, in *Conc. e merc.*, 2016, 1, p. 59, il quale afferma che «without any doubt, data is the oil of the information society». I *big data* sono diventati una merce di scambio nell'era digitale capace di fornire informazioni sulle propensioni, sui gusti e sulle preferenze di ogni singolo utente fino ad essere in grado di predirne le scelte e le decisioni.

a internet, dai *social network* agli algoritmi [3], sono molteplici le innovazioni tecnologiche con cui il diritto ha dovuto fare i conti. In questo *mare magnum*, non sono di certo rimasti impermeabili il settore bancario, assicurativo [4] e finanziario interessati da alcuni fenomeni che sono il frutto di questa inesorabile e inarrestabile evoluzione tecnologica.

Con particolare riguardo al mondo bancario e finanziario, infatti, l'impatto delle nuove tecnologie è stato considerato «rivoluzionario» [5] viste le implicazioni derivanti dallo sfruttamento dei *big data* [6] che rilevano non tanto sul piano quantitativo delle

---

[3] L'algoritmo si può definire quale insieme di istruzioni matematiche per manipolare dati o per risolvere un problema che opera solo sulla base dei dati raccolti. *Cfr.* S. SASSI, *Gli algoritmi nelle decisioni pubbliche tra trasparenza e responsabilità*, in *Analisi Giuridica dell'Economia*, 1, 2019, p. 110 ss.

[4] Sul punto, *vd*. E. BATTELLI, Big Data *e algoritmi predittivi nel settore assicurativo: vantaggi e nuovi rischi*, in *Corr. giur*., 2019, 12, p. 1517.

[5] F. MATTASSOGLIO, *Informazione tecnologica e valutazione del merito creditizio dei consumatori. Verso un social* credit system?, Milano, 2018 p. 93.

[6] Caratteristica identificativa dei *big data* è la presenza delle c.d. tre "V", quali volume, velocità e varietà. I *big data* si contraddistinguono, anzitutto, per il volume, ossia per l'enorme quantità di informazioni che sono contenute e collezionate in un singolo dato. Tali informazioni, collezionate e raccolte nei big data, provengono dall'utilizzo dei *social network*, dei *browser* e, in generale, di internet. Basti pensare che il mero utilizzo di un'applicazione istallata su uno smartphone produce una quantità smisurata di dati, concernenti informazioni più disparate. L'enorme quantità di informazioni contenute nei big data è raccolta e memorizzata in un ridotto intervallo di tempo. La velocità rappresenta, di conseguenza, la seconda "V" dei *big data*. La velocità di trasmissione e raccolta dei dati si registra a livello esponenziale. Per fornire una chiara esemplificazione, si pensi a Facebook, dal quale ogni ventiquattro ore sono raccolte circa novecento milioni di foto, per un totale di duecentocinquanta miliardi di foto in un anno. La terza caratteristica dei *big data* è la varietà, *i.e.* la diversità dei *big data*, i quali differiscono per natura e provenienza. Infatti, i *big data* possono essere generati automaticamente da macchine, come avviene per i dati provenienti dai *log* di accesso a un sito web, ovvero provenire dall'utilizzo di piattaforme e siti internet. Inoltre, con il termine di varietà si suole fare riferimento al fenomeno di destrutturazione dei dati. Mentre in passato i dati erano strutturati, e di conseguenza erano organizzati e analizzati in tabelle o database relazionali per gruppi omogenei, attualmente circa l'80% dei dati si caratterizza per essere a bassa strutturazione, non essendo passibili di classificazione mediante le tradizionali tecniche di organizzazione nei *database*. Dati siffatti sono provenienti, ad esempio, dall'utilizzo dei social network, come Facebook, Instagram e Twitter. Si pensi ai dati connessi ad una immagine condivisa su un social network, alla quale sono corredati *hashtag*, *like* e *tracking* di geolocalizzazione e quindi informazioni di diversa origine e qualità. Invero, si possono scorgere altre caratteristiche identificative dei *big data*, essendo questi protagonisti di un processo di evoluzione costante. Da tale evoluzione emerge la possibilità di individuare altre caratteristiche identificative, come la variabilità, la viralità e la veridicità. La variabilità è caratteristica per la quale l'interpretazione del dato varia in funzione del contesto da cui si ricava e da cui vi è l'analisi. La viralità si riferisce, invece, agli effetti virali della circolazione dei big data, alle conseguenze o alle reazioni prodotte dalla circolazione delle informazioni che sono estrapolate da essi, capaci di essere propagate a notevoli distanza e velocità. La veridicità si riferisce all'attendibilità dei dati. I dati non avrebbero, infatti, alcuna utilità se non fossero accurati e qualitativamente veritieri, rispondenti alla realtà da cui provengono e potrebbero essere non veritieri allorquando provengano da programmi che utilizzano un algoritmo di apprendimento automatico non supervisionato. Sul punto, v. E. MC NULTY, *Understanding Big Data: the seven's*, in *Datacomy*, 2014.

informazioni ivi contenute, quanto sul piano qualitativo, poiché dall'analisi delle innumerevoli informazioni raccolte tramite la profilazione [7] si consente di tracciare le caratteristiche degli utenti cui si riferiscono. Si pensi all'uso che ne fanno le banche con specifico riguardo ai contratti relativi a prodotti finanziari, le quali, tramite l'utilizzo dei *big data*, possono ricavare una valutazione accurata sui tipi di rischio ai quali l'investitore è particolarmente avverso o i tipi di condizioni contrattuali che non è disposto ad accettare. Tramite l'analisi dei dati sociali e comportamentali derivanti dai *social media*, si trae un quadro completo del potenziale debitore potendolo inquadrare nel segmento di clientela che rispecchia maggiormente le sue esigenze e caratteristiche specifiche. Con l'analisi dei dati immessi nei *social network* si può anche captare la preferenza del cliente in merito a questo o quello strumento finanziario permettendo alle banche di sviluppare delle offerte *ad hoc* per ogni categoria di cliente [8] o, persino, prevedere l'andamento dei mercati finanziari [9].

L'attendibilità e il grado di accuratezza dei *big data* si fa discendere dal grado di affidabilità della fonte da cui essi hanno origine, nonché al processo di elaborazione dei dati per l'estrapolazione di un set di informazioni. L'attendibilità e la precisione dei dati è un risultato raggiungibile a valle di un processo che mira a individuare e rimuove anomalie, incongruenze e duplicazioni. Il grado di veridicità dei dati discende, inoltre, dal metodo di elaborazione dei dati utilizzato, il quale deve tener conto delle esigenze e delle finalità per cui esso è applicato al fine di ottenere un'informazione pertinente agli obiettivi perseguiti. Analizzare i big data per tramite di un modello corretto di elaborazione garantisce risultati pertinenti e utili ai fini perseguiti. Alle caratteristiche sopraelencate se ne aggiungerebbe, infine, un'altra: la volatilità. Sul punto, vd. C. MCNEILL, *Veracity: The Most Important "V" of Big Data*, 2018, in https://www.gutcheckit.com/. La volatilità contraddistingue solo alcuni dati e consiste nel tasso di variazione e nella durata del singolo dato. Tali caratteristiche permettono ai *big data* di assumere un valore economico. Le imprese recentemente hanno carpito l'importanza strategica dei dati sul mercato e quindi hanno creato proprie piattaforme di dati e investito sulle tecniche di analisi degli stessi.

[7] La profilazione digitale consistente nella creazione di identità ideali alle quali sono attribuite. caratteristiche derivanti dall'analisi dei big data provenienti, ad esempio, da Facebook, Instagram, Twitter, Google e persino Netflix. Tali informazioni possono divenire oggetto di analisi da parte di soggetti terzi ai gestori delle piattaforme social i quali, grazie all'utilizzo di software che connettono e riordinano i dati, sono in grado di tracciare un profilo dell'utente cui si riferiscono e da cui promanano. Le identità astratte così create sono assegnate, tramite l'utilizzo di algoritmi automatici, a un'identità digitale relativa a un individuo reale. Pertanto, a un individuo saranno associate delle caratteristiche, dei gusti, delle preferenze, ergo un profilo completo, dal quale potranno essere tracciate persino previsioni su comportamenti futuri. Ai sensi dell'art. 4 del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati, per «profilazione» s'intende «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica».

[8] Cfr. F. DI PORTO, *La regolazione degli obblighi informativi. Le sfide delle scienze cognitive e dei* big data, coll. *Ricerche giuridiche*, Napoli, 2017, p. 223.

[9] Su questo tema è stato avviato un progetto di ricerca nel 2011 da parte del Laboratorio di Economia Sperimentale GAM Ca' Foscari, il quale ha accertato la funzionalità dell'"Indice Twitter del-

Tra i vari impieghi delle nuove tecnologie nel settore bancario, per quanto qui specificamente interessa, v'è da annoverare l'utilizzo dei *big data* per la valutazione del merito creditizio di un cliente – con sguardo vigile alle prospettive futuribili che possono discendere dall'intelligenza artificiale – in quanto consente di ottenere, grazie all'«immenso bacino» [10] di dati analizzati, una valutazione più accurata e capillare rispetto a quella tradizionalmente condotta. La valutazione tradizionale del merito creditizio, infatti, risente della difficoltà di reperire e accedere alle informazioni contenute negli *hard data*. La valutazione innovativa, condotta tramite *big data*, risulterebbe, invece, capillare grazie alla smisurata mole di dati raccolti e analizzati. I dati in questione derivano perlopiù dall'utilizzo dei *social network* e di internet, i quali contengono le informazioni rilasciate da un singolo utente nel web, di natura e provenienza diversa. Ad esempio, figurano tra questi i dati raccolti per tramite dei *cookies*, i quali permettono di trasmettere al gestore gli indirizzi di Internet Protocol dell'utente, con cui è possibile identificare il codice di avviamento postale del luogo da cui l'utente si è collegato. Sono oggetto di analisi anche i dati trasmessi dall'utente durante l'utilizzo dei *social network*, quali, a titolo di esempio, Facebook, X (ex Twitter), Tiktok e Instagram.

È in questo contesto che assume importanza primaria, per il creditore, la conoscenza e la conoscibilità dei dati attraverso i quali viene condotta la valutazione del

---

l'Incertezza" al fine di prevedere l'andamento dei mercati finanziari. Esso fungerebbe come un "barometro" capace di predire la volatilità dei mercati azionari, cioè la variabilità dei prezzi o dei tassi di rendimento di un titolo negoziato in un mercato ufficiale. L'indice è stato ideato da Moneyfarm in collaborazione con l'Università Milano-Bicocca nel 2016. Esso è il frutto di un'attenta analisi di più di centocinquanta mila articoli sulle testate giornalistiche web e dei messaggi su Twitter su temi economico-finanziari. Dai risultati si è ricavata una «fotografia di come i principali eventi politici, economici e sociali sono trasmessi dai media e vissuti dalla gente comune nel nostro Paese e dell'incertezza e instabilità che questi provocano», come ha affermato Paolo Galvani, presidente di MoneyFarm. In particolare, si sono registrati picchi di incertezza in occasione del referendum greco o del crollo di Monte dei Paschi di Siena. L'indice è composto da due indicatori: l'uno è l'indicatore di incertezza trasmessa, che misura il grado di incertezza che è contenuto negli articoli delle testate web nazionali; l'altro è l'indicatore di incertezza percepita cioè avvertita dalle persone che si può desumere dai cinguettii su Twitter. Infatti, quando l'indicatore di incertezza trasmessa precipita, precipita anche l'indicatore di incertezza percepita a dimostrazione del fatto che il sentimento dei singoli è orientato dal tenore delle informazioni trasmesse. Proseguendo su questa linea, i ricercatori del Laboratorio GAM Ca' Foscari hanno analizzato più di un milione di tweet contenenti la parola inglese «uncertainty» tra aprile e dicembre 2016, un periodo particolarmente turbolento dal punto di vista politico per la Brexit e le elezioni presidenziali americane. Twitter risulterebbe un ottimo campo di ricerca, a detta del Professore Massimo Warglien che ha coordinato gli studi, in quanto permette di tracciare i movimenti delle opinioni e dei sentimenti degli utenti in una ampia «società civile online». Si è dimostrato pertanto che è possibile prevedere in anticipo il segno della volatilità nei mercati azionari partendo dall'analisi dell'umore dei singoli utenti che si rinviene dai tweet, a loro volta condizionati dall'indice di incertezza trasmesso da parte dei media. Inoltre, i big data possono essere impiegati nell'ambito della «fornitura di prodotti e servizi finanziari» e della «intermediazione finanziaria, gestione del rischio finanziario, valute elettroniche», v. R. MORO VISCONTI, *L'intelligenza artificiale, modelli di business e profili di valutazione*, in *Dir. ind*., 2018, 5, p. 421.

[10] *Ibidem*.

proprio merito di credito da parte dell'istituto bancario, anche ai fini della tutela della privacy. Un tale obiettivo potrebbe essere perseguito tramite uno strumento recentemente apparso sulla scena del diritto eurounitario, la cooperativa di dati, al fine di rendere edotto l'interessato dei suoi diritti con riguardo ai dati utilizzati ai fini della valutazione della sua posizione creditoria non solo per la tutela della *privacy* ma anche per la garanzia di un buon funzionamento dell'intero sistema.

2. La valutazione del merito creditizio tramite big data: profili critici.

La valutazione del merito creditizio innovativa condotta tramite l'impiego dei *big data* consentirebbe di ottenere, si diceva, giudizi più accurati rispetto a quella tradizionalmente condotta mediante l'analisi di informazioni bancarie e finanziarie attinte dalla storia creditizia del cliente e dalle banche dati creditizie. E questo vale soprattutto in contesti ove risultino scarse, o del tutto assenti, le *hard information*, relative alla storia creditizia e finanziaria di un cliente. Fenomeni siffatti si registrano, ad esempio, nei Paesi in via di sviluppo [11] o connotati da un basso reddito *pro capite* [12], ovvero con riferimento a piccole e medie imprese di nuova costituzione. Nell'un caso, gli istituti creditizi avvertono la difficoltà di reperire informazioni concernenti il profilo economico-finanziario del proprio cliente, dal momento che vi sono «sistemi bancari e soprattutto di informazione creditizia meno sviluppati e capillari» [13], nonché «ampie fasce di popolazione prive di accesso al credito» [14] che non risultano già affidate ad un sistema bancario. Nell'altro caso, invece, seppur in presenza di sistemi di informazione creditizia avanzati e capillari, gli istituti bancari potrebbero ricorrere alle informazioni di tipo *soft* al fine di superare l'«opacità informativa» [15] che connota le piccole e medie imprese di nuova costituzione, rispetto alle quali manca una storia creditizia e vigono obblighi informativi meno onerosi rispetto alle imprese di grandi dimensioni [16].

Di talché, in tali contesti al fine di espletare l'attività di valutazione del merito

---

[11] F. MATTASSOGLIO, *Informazione tecnologica e valutazione del merito creditizio dei consumatori. Verso un* social credit system?, cit., p. 94.

[12] Y. WEI-P. YILDIRIM-C. VON DEN BULTE-C. DELLORACS, *Credit scoring with social network data*, in *Market Science*, 2014, p. 1, per i quali autori «*in low-income countries, in particular, part of the credit access problem stems from the fact that reliable data on financial history do not exist, are limited, costly to collect or hard to verify. In these countries, lenders tend to be very conservative in accepting borrowers' credit applications*».

[13] F. MATTASSOGLIO, *op. ult. cit.*

[14] *Ibidem*.

[15] G. ALBARETO-M. BENVENUTI-S. MOCETTI-M. PAGNINI-P. ROSSI, *L'organizzazione dell'attività creditizia e l'utilizzo di tecniche di scoring del sistema bancario italiano: risultati di un'indagine campionaria*, in *Questioni di Economia e Finanza*, Roma, Banca d'Italia, 12, p. 5.

[16] *Ibidem*.

creditizio, determinante per ridurre il rischio di credito [17], si è reso necessario il ricorso ai *big data* e, in particolare, ai *social data* [18]. Essi rappresentano, in mancanza di *hard information*, la principale, se non unica, fonte informativa da cui estrapolare, tramite un processo di analisi, le *soft information*, relative ai gusti, alle inclinazioni, alle abitudini del soggetto da cui tali dati promanano [19]. Le informazioni *soft* derivanti dai *social network* sono, infatti, varie e copiose, comprendendo migliaia di variabili [20] di cui risultano manchevoli, invece, gli *hard data*, limitati alle informazioni direttamente fornite dal cliente all'istituto creditizio ovvero già presenti nelle banche dati creditizie pubbliche o private.

A questo riguardo, è lecito domandarsi se la valutazione del merito creditizio ottenuta tramite l'analisi di *soft information* sia efficace nella determinazione della esatta referenza creditizia [21] di un cliente anche in contesti e in sistemi bancari, come quello nostrano, già di per sé ricchi di informazioni di natura economico-finanziaria. Non si tratta di una questione di lana caprina o squisitamente dottrinale. Piuttosto, è un quesito legittimo da porsi alla luce delle conseguenze che ne possono derivare sul piano economico e giuridico di cui si darà qualche esemplificazione nel prosieguo. Uno scorretto processo di valutazione del merito creditizio può condurre, infatti, alla concessione del credito a un cliente immeritevole, alla determinazione di un tasso di interesse troppo oneroso per il debitore [22] ovvero al diniego di credito a un cliente invece che ne è meritevole.

Sul punto, non può sottacersi che sono molteplici le insidie che si vanno a prospettare a seguito di un processo di *social credit scoring* e cioè di un sistema di valutazione del merito di credito fondato sull'analisi dei *social data* ottenuti dai *social network*. Primi tra tutte, il pericolo della sua incapacità di predire il *default* del cliente [23] e il rischio di ottenere una referenza creditizia distorta, dalla quale si pro-

---

[17] P. BIFFIS, *L'affidamento della clientela*, in C. BALDAN-S. MIANI-M. POLATO-A. PROTO-U. RIGONI-F. ZEN (a cura di), *Le operazioni e i servizi bancari*, Torino, 2015, p. 93, ove, con riferimento della valutazione del merito creditizio, si parla di attività di «determinante funzione di controllo» per ridurre il rischio di credito.

[18] Con la locuzione «*social data*» s'intendono i dati derivanti dalle informazioni condivise da un utente sulle piattaforme di *social network*.

[19] Sul valore dei dati personali rispetto alla personalità dell'utente, v. F. BRAVO-J. V. TORRIJOS, *Data in the Public Sector and Data Valorisation*, in *European Review of Digital Administration & Law*, 2022, 3, p. 7.

[20] J. JIANG-L. LIAO-X. LU-Z. WANG-H. XIANG, *Can Big Data defeat traditional credit rating?*, in *Electronic Journal*, 2009, p. 2.

[21] F. MATTASSOGLIO, *Informazione tecnologica e valutazione del merito creditizio dei consumatori. Verso un* social credit system*?*, cit., p. 166.

[22] Per contro, v. G. ROSSI, *Il credito al consumo: dal fenomeno socio-economico alla fattispecie contrattuale*, Milano, 2017, p. 61, per la quale «(…) la differenziazione dei tassi di interesse applicati alla clientela sulla base della referenza creditizia, è un'innovazione ancora molto lontana dall'essere applicata».

[23] J. JIANG-L. LIAO-X. LU-Z. WANG-H. XIANG, *Can Big Data defeat traditional credit rating?*, *ivi.*

durrebbe un erroneo merito creditizio. Non secondario è, poi, il pericolo di ottenere un giudizio ad effetti discriminatori che limiti (o allarghi indebitamente) il diritto di accesso al credito sulla scorta di informazioni sensibili [24] come quelle informazioni condivise sui *social network*, piuttosto che di informazioni oggettive sullo status finanziario e reddituale di un individuo al profilo economico-finanziario. Alcuni algoritmi, infatti, possono direttamente o indirettamente discriminare un soggetto sulla base della sua etnia, del sesso, dell'orientamento religioso [25], escludendolo dalla concessione di credito in quanto appartenente ad una classe di individui con una cattiva storia creditizia ovvero con un basso punteggio di affidabilità. Tali effetti discriminatori nascono non solo dalla scelta di raccogliere e processare dati non oggettivi, ma anche dal modo di interpretare il risultato ottenuto dall'analisi degli stessi, dunque dalle conseguenze che sono messe in relazione ai singoli risultati. Un istituto di credito potrebbe riconoscere un legame tra le abitudini di un soggetto, i luoghi da questi frequentati, il sesso o l'età o persino la lingua, e il livello di affidabilità creditizia, attribuendo un determinato grado di merito creditizio a tutti gli individui classificati in un gruppo per caratteristiche comuni. Un esempio ne è il tasso di interesse imposto da un istituto di credito americano a clienti di etnia afroamericana e latino-americana, superiore del 30% rispetto al tasso di interesse pattuito con clienti di diversa etnia e di carnagione bianca [26].

---

[24] E. PELINO, *L'anonimato su internet*, in G. FINOCCHIARO (a cura di), *Diritto all'anonimato, in Trattato di diritto commerciale e di diritto pubblico dell'economia*, Padova, 2008, p. 298, secondo il quale le informazioni sensibili riguardano «nascita, il sesso, il CAP, l'occupazione, il settore di attività» e altri interessi. Invero, è necessario precisare che la nozione di «dati sensibili» (risalente al Decreto legislativo 30 giugno 2003, n. 196, che li definiva come «i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale» è, oramai, risalente alla luce del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016. Il Regolamento, pur non offrendo una definizione di dato sensibile, dispone che «è vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona» in assenza di esplicito consenso da parte dell'interessato e in altri casi specificamente indicati. Questa categoria di dati personali concerne, quindi, l'origine etnica, le propensioni politiche, l'orientamento sessuale, la fede religiosa i quali, dunque, sono idonei a ricostruire il profilo etico-sociale e psico-sanitario di un soggetto, ampliando lo spettro della definizione rispetto al passato. Sul punto, G. FINOCCHIARO, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Bologna, 2021, p. 57 ss.

[25] K. KEMP-R. P. BUCLEY, *Protecting Financial Consumer Data in developing countries. An alternative to the Flawed Consent Model*, in *Georgetown Journal of International Affairs*, 2017, 18, p. 37.

[26] A. GUMBUS-F. GROOZINSKY, *Era of Big Data: danger of discrimination*, in *Computers and society*, 2016, vol. 45, 3, p. 119.

3. Gli effetti discriminatori derivanti dall'uso dei *big data* nella valutazione del merito creditizio: la limitazione della facoltà di accesso al credito nel caso *Johnson c. American Express* e nel ricorso della *Non-Discrimination Obudsman* alla Corte finlandese.

Non è una rarità incorrere a limitazioni di accesso al credito a causa di pratiche discriminatorie condotte dagli istituti creditizi sulla scorta di informazioni soggettive attinte da piattaforme informatiche. Sono da annoverare, a titolo di esempio, due casi distinti ma entrambi di particolare interesse alla luce delle osservazioni che precedono: il caso Kevin Johnson contro American Express [27] e il caso della Non-Discrimination Ombudsman al Non-Discrimination and Equality Tribunal finlandese.

La prima delle due vicende citate vede protagonista Kevin Johnson, un cliente dall'impeccabile storia creditizia, al quale nel 2008, di ritorno da un viaggio, viene recapitata una lettera con cui la banca, American Express, lo informa del fatto che la soglia di credito disponibile sulla sua carta di credito era stata ridotta da $10.800,00 a $3.800,00. Nella lettera informativa recapitatagli, la banca adduce come motivo dell'abbassamento del limite di credito il fatto che il cliente avrebbe concluso compere, tramite carta di credito, presso esercizi commerciali ove avevano acquistato altri clienti che, successivamente, erano risultati insolventi nei confronti dell'istituto bancario. Il sistema di *credit scoring* adottato dall'istituto bancario, nel caso di specie, non ha tenuto conto del solido *rating* creditizio del sig. Johnson né della sua situazione patrimoniale [28], ma ha rivalutato la sua affidabilità creditizia sulla scorta dei *big data* concernenti i luoghi frequentati e i negozi ove questi ha acquistato. Qualora tali dati non fossero stati analizzati, ovvero qualora alla frequenza di questi non fosse stato collegato un basso merito creditizio, Johnson sarebbe stato considerato un cliente-modello dal punto di vista patrimoniale e finanziario, in quanto non solo è un imprenditore a capo di una propria società con discreti guadagni, ma è anche proprietario di casa e non è mai risultato insolvente nei confronti della banca o di terzi. Il cliente si rivela vittima, pertanto, del cd. *behavioural scoring* [29], ossia di un sistema di valutazione del merito creditizio che tiene conto delle sue abitudini di acquisto, per mezzo di un sistema di associazione che attribuisce ad un soggetto il merito creditizio di altri clienti a lui accomunati da medesime abitudini o luoghi frequentati, senza tenerne in considerazione lo status finanziario.

Il secondo caso menzionato ha riguardo, invece, alla decisione assunta nel 2015 da un istituto creditizio, la Svea Ekonomi AB, di negare il credito ad un cliente per

---

[27] Si precisa che non si tratta di un *legal case* in quanto il cliente non ha presentato ricorso in tribunale, preferendo, piuttosto, a seguito di ripetute sollecitazioni al servizio clienti di American Express, rendere pubbliche le sue doglianze tramite i *mass media*.

[28] L.B. ANDREWS, *I know who you are and I saw what you did: social networks and the death of privacy*, New York, 2014, p. 20.

[29] M. HURLEY-J. ADEBAYO, *Credit scoring in the era of big data*, in *Yale journal of Law and Technology*, 2017, 18, p. 148.

l'acquisto di materiale edile, sulla base dell'esito negativo della valutazione del merito creditizio condotta tramite l'analisi di dati sensibili. In merito, la *Non-Discrimination Ombudsman*, in rappresentanza e per conto del cliente, ha presentato ricorso alla Corte finlandese chiedendo l'accertamento della responsabilità dell'istituto di credito per pratiche discriminatorie. Le doglianze del ricorrente attengono alle ragioni che hanno determinato la discriminazione del cliente, da ravvisarsi nel metodo di *credit scoring* impiegato dalla banca, nel quale si attribuisce un *credit score* maggiore ai clienti aventi residenza in una zona ad alta densità di popolazione e un punteggio minore a coloro che risiedono in zone meno popolose. Invero, si è accertato che il luogo di residenza del richiedente il credito non fosse l'unico parametro di discutibile utilizzo nella determinazione del merito creditizio. Segnatamente, è stato scoperto che il punteggio di credito attribuito ad un soggetto nel sistema di valutazione utilizzato dall'istituto finlandese è determinato da molteplici variabili, quali il sesso, la lingua madre e l'età del richiedente. In particolare, nel sistema adottato dalla Svea Ekonomi AB, il *credit score* attribuito ai clienti è maggiore qualora parlino come primo idioma il Finlandese piuttosto che lo Svedese, ovvero siano donne piuttosto che uomini o siano adulti piuttosto che anziani. Nel caso di specie, al cliente, in quanto uomo adulto, la cui prima lingua è il Finlandese e con residenza in una zona poco popolosa, è stato attribuito dal sistema di *scoring* un punteggio basso e insufficiente per consentire l'accesso all'ammontare di credito richiesto. Qualora, invece, il richiedente fosse stato una donna e avesse parlato Svedese, sarebbe stata considerata idonea a ottenere l'ammontare di credito richiesto. Sulla questione si è pronunciato il *Non-Discrimination and Equality Tribunal*, il quale ha preliminarmente chiarito che, anche qualora si accerti l'esistenza di pratiche discriminatorie, non può riconoscersi in capo al cliente un diritto soggettivo al credito e, parimenti, non può vigere per un istituto creditizio privato l'obbligo di erogare il credito, seppur in presenza di una valutazione positiva del merito creditizio. Inoltre, la Corte ha chiarito che il creditore può discrezionalmente decidere di valutare non solo le informazioni relative alla situazione finanziaria del consumatore, ma di impiegare anche altri metodi, tra i quali i sistemi statistici, purché siano supplementari e non sostitutivi del tradizionale sistema di *credit scoring*. Quanto all'accertamento del carattere discriminatorio delle pratiche assunte dalla Svea Ekonomi AB, la Corte finlandese ha acclarato che la valutazione del merito creditizio del cliente è stata condotta senza tenere conto delle informazioni individualizzate relative al comportamento creditizio e alla posizione finanziaria del cliente, le quali, invece, se tenute in considerazione, avrebbero invece favorito l'estensione del credito al cliente. Trascurare la storia creditizia del cliente e non tenere conto della sua capacità patrimoniale e finanziaria, sulla scorta di dati sensibili, costituisce secondo i giudici finlandesi una pratica inaccettabile e discriminatoria. Discriminatoria risulta essere la valutazione del merito creditizio condotto dalla Svea Ekonomi AB in quanto non si basa sulla posizione finanziaria del cliente ma su una valutazione statistica, la quale tiene conto di fattori discriminatori, come la residenza, il sesso e la lingua. Inoltre, l'istituto creditizio non ha dimostrato il nesso tra i fattori utilizzati e la loro utilità nella determinazione del grado di solvibilità del cliente, né ha fornito prove statistiche che dimostrino l'attendibilità delle scelte discriminatorie assunte.

4. Valutazione erronea del merito creditizio per trattamento di dati personali derivanti da *social network* nell'ordinamento nostrano: cenni ai profili di responsabilità dell'intermediario.

La corretta valutazione del merito creditizio, intesa quale obbligo di *responsible lending* [30], riveste un ruolo centrale per le sorti del singolo rapporto di credito e per il sistema bancario [31] poiché tutela, d'un lato, il cliente-consumatore dal rischio di sovraindebitamento e il cliente-professionista dal rischio di fallimento e, dall'altro, il mercato del credito, garantendo la corretta allocazione delle risorse giacché consente all'intermediario di concedere prestiti, responsabili e sostenibili, sulla base della referenza creditizia [32] ottenuta dalla stessa valutazione e, pertanto, si dimostra essenziale per il raggiungimento di «pratiche responsabili nel rapporto di credito» [33].

Al fine di determinare correttamente il grado di solvibilità del cliente, l'intermediario deve valutare «tutti gli aspetti economici della posizione del soggetto a lui ben noti» [34], derivanti dall'assunzione di informazioni fornitegli dal cliente [35] nell'ambito di un rapporto diretto, ovvero ottenute dalla consultazione delle banche dati creditizie, pubbliche e private.

Per una corretta valutazione del merito creditizio del consumatore, ai sensi delle Linee guida emanate dall'European Banking Authority [36], l'intermediario dovrebbe anzitutto verificare la capacità di reddito attuale e pregressa del cliente, ed eventua-

---

[30] F. PASQUARIELLO-M. RANIELI, *L'omologazione del piano del consumatore sovraindebitato*, in *Giur. comm*., 2020, 2, p. 243, nota a Cass. civ., sez. I, 10 aprile 2019, n. 10095.

[31] F. QUARTA, *Assicurazione e costo totale del credito. Rilevanza della* payment protection insurance *nel computo del TAEG*, in *Banca, borsa e tit. cred.*, 2019, 1, p. 17.

[32] G. BIFERALI, Big Data *e valutazione del merito creditizio per l'accesso al* peer to peer lending, in *Dir. inf.*, 2018, 3, p. 483.

[33] G. LIBERATI BUCCIANTI, *Merito creditizio e obbligo di non concludere il contratto*, in *Nuova giur. civ. comm*., 2020, 1, p. 92.

[34] A. COLAVOLPE, *In tema di tutela cautelare atipica in relazione ad una segnalazione «erronea» da parte della banca alla Centrale dei rischi gestita dalla Banca d'Italia*, in *Giur. merito*, 2007, 2, p. 338, nota a Trib. Matera, 17 novembre 2005.

[35] Il processo di valutazione del merito creditizio, nonché gli elementi di cui tener conto, differiscono a seconda che il cliente sia un professionista o un consumatore. Nel primo caso, l'intermediario dovrà condurre una valutazione sulla «meritevolezza dell'impiego» del credito richiesto, sulla base del business plan presentato dal professionista. La valutazione del merito di credito di un consumatore è, invece, «ontologicamente diversa» rispetto alla valutazione del merito creditizio di un professionista, in quanto non ha riguardo alla meritevolezza dell'impiego del credito richiesto, ma si limita a valutare la capacità del consumatore di restituire il credito concesso. Pertanto, più che al futuro, la valutazione del merito creditizio del consumatore ha riguardo al passato, i.e. alla storia creditizia del cliente, secondo una prospettiva *ex ante*. Sul punto, A. SIMONATO, *La valutazione del merito creditizio del consumatore nella diretta 2008/48/CE*, in *Riv. dir. banc*, 2010, p. 4.

[36] EUROPEAN BANKING AUTHORITY, *Orientamenti ABE sulla valutazione del merito creditizio*, EBA/GL/2015/11, 19 agosto 2015.

li andamenti irregolari registrati nel tempo e, nel caso di redditi derivanti da un'attività autonoma o di carattere stagionale o saltuario, verificare la capacità di adempiere gli obblighi stabiliti dal contratto di credito nel tempo. Per acquisire maggiori informazioni, il creditore dovrebbe elaborare la documentazione relativa al credito e, se del caso, individuare le informazioni erronee fornite dal consumatore.

Per quanto attiene ai profili probatori circa l'adempimento dell'obbligo di una corretta valutazione del merito creditizio [37], il finanziatore deve provare di aver svolto correttamente le «specifiche attività istruttorie» [38] e di aver emesso un giudizio sulla solvibilità del cliente solo a valle di tali attività. Non grava sull'intermediario l'onere di provare di aver dato un «buon giudizio assoluto» [39] sul merito creditizio del cliente, in quanto sarebbe chiamato ad una *probatio diabolica*. La valutazione del merito creditizio può essere considerata correttamente svolta solo se l'intermediario prova di aver tenuto un comportamento ispirato alla diligenza professionale, tramite una valutazione *ex ante* della solvibilità del debitore. Il merito creditizio è correttamente attribuito solo se l'intermediario adempie al procedimento di valutazione e, pertanto, a nulla rileva il fatto che il creditore, a causa di eventi futuri e incerti, risulti inadempiente. Una valutazione erronea del merito creditizio può discendere, poi, da un trattamento illecito di dati personali [40], di cui l'istituto creditizio, quale titolare del trattamento, dovrebbe essere ritenuto responsabile. Il trattamento dei dati personali deve avvenire in modo lecito, corretto e trasparente nei confronti dell'interessato, solo per esplicite e legittime finalità determinate quali, ad esempio, l'espletamento di un'attività economica. Per definirsi lecito, il trattamento dovrà rispettare talune condizioni previste dalla normativa europea, tra le quali ottenere l'espresso consenso da parte dell'interessato ne rappresenta una delle

---

[37] In merito all'onere della prova troverebbe applicazione l'art. 2697 del codice civile, per il quale grava all'intermediario l'onere di provare di aver valutato correttamente il merito creditizio del proprio cliente. Così, M. FRANCISETTI BROLIN, *L'art. 124* bis *del TUB e gli incerti riflessi civilistici del cd. «merito creditizio» nel contratto al consumo: dalla* culpa in contrahendo *a vizi del volere*, in *Contr. e impr*., 2014, 2. p. 550; E. CARGNIEL-G. DE VELLIS, *Disciplina del credito ai consumatori: nuovi «strumenti di trasparenza» e dorma dei contratti bancari*, in *Resp. civ. e prev*., 2012, 1, p. 312.

[38] M. FRANCISETTI BROLIN, *L'art. 124* bis *del TUB e gli incerti riflessi civilistici del cd. «merito creditizio» nel contratto al consumo: dalla* culpa in contrahendo *a vizi del volere*, *ivi*.

[39] *Ibidem*.

[40] È bene precisare che i dati cui può ricorrere la banca possono essere di natura economica, quali sono i dati provenienti dalle Centrali dei rischi, richiesti direttamente al cliente in sede di contrattazione ovvero già presenti nell'istituto bancario se il cliente è già affidato, di dominio pubblico ovvero personali. È definito dato personale «qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale». Nel caso in cui il trattamento abbia ad oggetto dati non di dominio pubblico e non di natura economica, è necessario, generalmente, acquisire il consenso dell'interessato.

condizioni [41]. Si potrebbe ritenere che, nell'ambito della attribuzione di un *credit score* ad un cliente, non sia necessario acquisire il consenso del trattamento dei dati personali [42], dal momento che la valutazione del merito creditizio ha carattere di obbligatorietà *ex* art. 124-*bis* del Testo unico bancario e il trattamento dei dati rientra nell'ambito di un'attività economica. Si pone, però, un divieto al trattamento di dati personali, non pubblici, «che rivelino l'origine razziale o etnica, le opinioni politiche, le convenzioni religiose o filosofiche, o l'appartenenza sindacale» ovvero «dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona» [43], in assenza di uno specifico ed esplicito consenso al trattamento. Qualora la valutazione del merito creditizio avvenga tramite big data e social data, dal momento che le informazioni tratte saranno concernenti informazioni sensibili, il trattamento dei dati dovrà ricevere preliminarmente il consenso del cliente interessato. Pertanto, in mancanza di consenso, all'intermediario potrà attribuirsi una responsabilità di natura extracontrattuale da illecito trattamento dei dati personali [44].

Decisamente più complessa è, invece, l'ipotesi in cui, pur in presenza dell'adempimento dell'obbligo di valutazione del merito di credito e di un legittimo trattamento dei dati del cliente, la valutazione del merito creditizio risulti errata, cioè dipinga un quadro economico-finanziario distorto ed alterato rispetto a quello reale, a causa

---

[41] *Ex* art. 6 del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, si afferma che «il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: a) l interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità; b) il trattamento è necessario all'esecuzione di un contratto di cui l interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica; e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore. La lettera f) del primo comma non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti».

[42] Cfr. G. ALPA, *Aspetti della disciplina sui dati personali riguardanti gli enti e l'attività economica*, in *Riv. trim. dir. proc. civ*., 1998, p. 726, secondo il quale non sarebbe necessario acquisire il consenso nel caso in cui si tratti di clienti già affidati alla banca ovvero nel caso in cui intercorra tra il cliente e l'istituto bancario un contatto precontrattuale. Sarebbe, invece, necessario ottenere il consenso nel caso in cui i dati siano di terzi.

[43] Art. 9 del Reg. (UE) 2016/679.

[44] A. OTTOLIA, Big Data *e innovazione computazionale*, Torino, 2017, p. 93; F. IAQUINTA-A. INGRAO, *La privacy e i dati sensibili del lavoratore legati all'utilizzo di* social networks. *Quando prevenire è meglio che curare*, in *Dir. delle rel. industr*., 2014, 4, p. 1027; D. BARBIERATO, *Trattamento dei dati personale e «nuova» responsabilità civile*, in *Resp. civ. e prev*., 2019, 6, p. 2151; G. D'IPPOLITO, *Il principio di limitazione della finalità del trattamento tra* data protection *e antitrust*. *Il caso dell'uso secondario di* Big Data, in *Dir. inf*., 2018, 6, p. 943.

dell'impiego di informazioni non oggettive. Si pensi, ad esempio, ai casi già annoverati in precedenza, come il sistema adottato dalla Svea Ekonomi AB, ove il *credit score* attribuito ai clienti che parlino come primo idioma il Finlandese è maggiore rispetto a coloro che parlino come prima lingua lo Svedese, ovvero qualora siano donne piuttosto che uomini o siano adulti piuttosto che anziani. Le conseguenze condurrebbero ad effetti negativi tanto nei confronti del singolo cliente, quanto nei confronti del mercato poiché si attribuirebbe un credito superiore o inferiore all'effettivo grado di solvibilità del singolo cliente, ovvero si potrebbe limitare l'accesso al credito solo sulla base di informazioni discriminatorie, allocando le risorse bancarie in maniera distorta. In casi siffatti, dovrebbe riconoscersi all'intermediario responsabilità extracontrattuale *ex* art. 2050 del codice civile e il pregiudizio subìto dal cliente, affidato o non già affidato dovrà essere provato, anche tramite presunzioni semplici [45], negli stessi termini già esposti precedentemente in tema di responsabilità per danno da segnalazione illegittima in Centrale dei rischi.

5. *Ubi societas (technologica), ibi ius* [46]: la strategia europea dei dati a tutela di utenti e consumatori.

Dalle questioni finora affrontate emerge con chiarezza l'importanza che i *big data* hanno assunto gradatamente nell'odierna «economia digitale» [47] nella quale assurgono a «merce di scambio» [48] per la fornitura gratuita di beni e servizi [49], in

[45] Cass. civ., sez. III, 5 marzo 2015, n. 4443.

[46] Sul rapporto tra comunità globali informatizzate e diritto, in particolar modo privato, cfr. F. BRAVO, Ubi societas ibi ius *e fonti del diritto nell'età della globalizzazione*, in *Contr. e impr*., 2016, 6, pp. 1344-1390; T.E. FROSINI, *Il costituzionalismo nella società tecnologica*, in *Dir. inf.*, 2020, 3, p. 465.

[47] F. BASSAN-M. RABITTI, *I consumatori nella* social economy*, tra* big data *e* fake news*,* in *Astrid Rassegna*, 17, 2017, p. 3.

[48] G. D'IPPOLITO, *Commercializzazione dei dati personali: il dato personale tra approccio morale e negoziale*, in *Dir. inf.*, 3, 2020, p. 634.

[49] Torna opportuno citare, all'uopo, due provvedimenti. Il primo, la decisione dall'Autorità Garante della Concorrenza e del Mercato (di seguito AGCM) del maggio 2017, con la quale il Garante ha accertato la violazione da parte di WhatsApp Inc. di talune disposizioni del Codice del Consumo, comminando a WhatsApp Inc. una sanzione di 3 milioni di euro. L'AGCM ha accertato in questa sede che il Professionista all'epoca dei fatti ha, di fatto, indotto gli utenti di WhatsApp Messenger ad accettare integralmente i nuovi Termini di Utilizzo (i quali prevedevano, in particolare, la condivisione dei propri dati con Facebook) facendo loro credere che sarebbe stato, altrimenti, impossibile proseguire nell'uso dell'applicazione. Quanto qui specificamente rileva, tuttavia, non è l'accertamento della violazione delle norme a tutela del consumatore causata dall'apposizione di clausole vessatorie. Piuttosto, la considerazione dell'AGCM laddove esclude la natura di gratuità del contratto sottoscritto tra Whatsapp Inc. e i clienti-utenti giacché il servizio di messaggistica sarebbe offerto a fronte dell'ottenimento di dati, scambiati a fini pubblicitari. AGCM, quindi, ha ritenuto di considerare la gratuità del contratto del consumatore come fondamento giustificativo dell'utilizzo di clausole vessatorie e ha precisato che, ai fini della qualificazione come

virtù del valore patrimoniale loro attribuito in funzione della quantità e qualità delle informazioni che da essi si ricavano.

Questo fenomeno non ha lasciato indifferente il Legislatore eurounitario che si è determinato ad affrontare due sfide quali divenire un «polo di attrazione» [50] per i dati e, al contempo, tutelare i consumatori, proteggerne i dati [51] e i diritti fondamentali [52].

In linea con questi obiettivi, è stato avviato negli anni un articolato percorso [53] per

---

contrattuale del rapporto tra Whatsapp ed il consumatore, non rileva la gratuità del servizio. La prestazione è erogata gratuitamente ma ha un vantaggio economicamente apprezzabile che ottiene *aliunde*. Il secondo provvedimento, rilevante sul punto della (solo apparente) gratuità del servizio digitale fornito a fronte di uno sfruttamento commerciale dei dati degli utenti, è la sentenza n. 2631 del 29 marzo 2021, con cui il Consiglio di Stato ha respinto il ricorso presentato dalla società Facebook Ireland Limited avverso il provvedimento dell'AGCM del novembre 2018, già impugnato di fronte al TAR Lazio (TAR Lazio, sez. I, 10 gennaio 2020, n. 261). Il Consiglio di Stato, in tale sede, ha confermato la tesi del giudice di primo grado ritenendo di escludere la natura gratuita del contratto di fornitura del servizio allorché, sebbene non venga richiesto un compenso economico all'utente, vengano acquisiti i dati degli utenti come corrispettivo. Mette conto riprodurne il dato testuale: «i dati (…) sono già stati messi nella disponibilità dei soggetti che intendono sfruttarli commercialmente; la "deselezione" determina, quale conseguenza, il venire meno dei servizi social promessi come gratuiti ma che, evidentemente, gratuiti non sono, finendo per rappresentate il "corrispettivo" della messa a disposizione dei dati personali del singolo utente a fini commerciali».

[50] L. PETRONE, *Il mercato digitale europeo e le cooperative di dati*, in *Contr. e impr*, 2023, 3, p. 802.

[51] Sul concetto di protezione dei dati personali e sulla definizione di protezione dei dati personali, *cfr*. G. FINOCCHIARO, *Il quadro d'insieme sul regolamento europeo sulla protezione dei dati personali*, in G. FINOCCHIARO (a cura di), *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, p. 5, ove si afferma che «il diritto alla protezione dei dati personali consiste nel diritto del soggetto cui i dati si riferiscono, di esercitare un controllo, anche attivo, su detti dati, diritto che si estende dall'accesso alla rettifica».

[52] Come osservato da G. FINOCCHIARO, *Data and Digital Sovereignty*, in *European Review of Digital Administration & Law*, 2022, 3, p. 9, l'Europa si propone di giocare un ruolo primario, nel contesto geopolitico, rispetto alle nuove tecnologie anche rispetto a Stati Uniti e Cina. Non come produttore ma come legislatore leader, puntando a produrre una legislazione esemplare. Sul concetto di sovranità digitale ancora G. FINOCCHIARO, *La sovranità digitale*, in *Diritto pubblico*, 2022, 3, p. 809 ss.

[53] Già con la Comunicazione della Commissione europea "Verso una florida economia basata sui dati", Bruxelles, 2 luglio 2014, si era espressa la necessità di garantire la libera circolazione dei dati tra gli Stati membri la cui mancanza rischiava di «ostacolare l'ingresso di nuovi operatori sul mercato e frenare l'innovazione»; con Comunicazione della Commissione europea "Costruire un'economia dei dati europea", Bruxelles, 10 gennaio 2017, si era riconosciuta la necessità di un intervento legislativo al fine di incentivare e promuovere lo sviluppo di un terreno fertile rendere i dati accessibili e utilizzabili, e consentire la piena estrazione del loro valore. Percorso articolato, si è esordito, perché corroborato da molteplici interventi settoriali. In questo percorso, infatti, vi rientrano il GDPR (Regolamento Ue 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 «relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati»), il *Data Governance Act* (Regolamento Ue 2022/868 del Parlamento europeo e del consiglio del 30 maggio 2022 relativo alla *governance* europea dei dati, che modifica il Regolamento Ue 2018/1724 – Regolamento sulla governance dei dati), il *Digital Services Act* (Regolamento Ue 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE – Regolamento sui servizi digitali) e il *Digi-*

la costruzione di uno spazio unico europeo di dati ove far convergere i dati personali e non personali [54], compresi i dati commerciali sensibili, affinché «siano sicuri e le imprese abbiano facilmente accesso a una quantità pressoché infinita di dati industriali di elevata qualità, che stimolino la crescita e creino valore, riducendo nel contempo al minimo la nostra impronta di carbonio e ambientale» [55]. Un mercato unico, quindi, in cui i dati possono circolare liberamente tra gli Stati membri, a cui vengono applicati i medesimi standard europei a tutela dei consumatori e della loro *privacy*.

Nel percorso verso una strategia europea dei dati, rappresenta uno spartiacque la disciplina contenuta nel *Data Governance Act* che segna una linea di demarcazione rispetto al passato quanto alle finalità perseguite, non più volte alla mera salvaguardia dei dati in ottica «difensiva» [56] e protezionistica, ma sottese al potenziamento della circolazione degli stessi.

A compendio del percorso finora affrontato si pone, da ultimo, il Regolamento europeo sui dati [57] entrato in vigore a gennaio 2024, con il quale la Commissione mira a garantire la disponibilità di un maggior numero di dati e a regolare il loro utilizzo e accesso, adeguando le norme di diritto contrattuale e impedendo lo sfruttamento degli squilibri contrattuali che ostacolano l'accesso equo ai dati e il loro utilizzo.

6. I servizi di intermediazione dei dati: le cooperative di dati.

Nella strategia tracciata dal *Data Governance Act* che, come si diceva, è teso a rafforzare e potenziare il mercato dei dati, particolare peso assume la disciplina dei servizi di intermediazione dei dati personali tramite l'attività dei fornitori di servizi di intermediazione dei dati per mezzo delle c.d. cooperative di dati. Si tratta di una disciplina giovane ma (quanto agli ordinamenti esteri) già radicata nella realtà ove sono sorte cooperative di dati in settori svariati, dal *food delivery* alla pesca fino ai trasporti [58].

---

tal Markets Act (Regolamento Ue 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive Ue 2019/1937 e Ue 2020/1828 – Regolamento sui mercati digitali).

[54] Tale impostazione è discesa dalle novità normative introdotte dal *Data Governance Act*.

[55] Comunicazione della Commissione europea "Una strategia europea dei dati", Bruxelles, 19 febbraio 2020.

[56] G. RESTA, *La dimensione collettiva dei dati personali*, in *Parolechiave*, 2023, 1, p. 103.

[57] Regolamento (UE) 2023/2854 del Parlamento europeo e del Consiglio del 13 dicembre 2023 riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il regolamento (UE) 2017/2394 e la direttiva (UE) 2020/1828 (regolamento sui dati).

[58] Le esperienze citate si riferiscono, in particolare, alla cooperativa Driver's Seat nata – si legge sul loro sito internet – per aiutare i lavoratori a essere pagati di più ogni giorno, a combattere l'uso delle aziende di gestione algoritmica con la tecnologia che i lavoratori contribuiscono ad alimentare, a portare dati onesti sulla forza lavoro e sulla politica dei trasporti. I risultati non si sono fatti attendere. Grazie alla cooperativa di dati, migliaia di autisti e addetti alle consegne hanno incrementato la pro-

Le cooperative di dati sono regolate dall'art. 2, par. 1, n. 15 del Regolamento suddetto il quale definisce i «servizi di cooperative di dati» come «servizi di intermediazione dei dati offerti da una struttura organizzativa costituita da interessati, imprese individuali o da PMI, che sono membri di tale struttura, avente come obiettivi principali quelli di aiutare i propri membri nell'esercizio dei loro diritti in relazione a determinati dati, anche per quanto riguarda il compiere scelte informate prima di acconsentire al trattamento dei dati, di procedere a uno scambio di opinioni sulle finalità e sulle condizioni del trattamento dei dati che rappresenterebbero al meglio gli interessi dei propri membri in relazione ai loro dati, o di negoziare i termini e le condizioni per il trattamento dei dati per conto dei membri prima di concedere l'autorizzazione al trattamento dei dati non personali o prima che essi diano il loro consenso al trattamento dei dati personali».

La funzione delle cooperative di dati è, quindi, rendere edotto l'interessato[59] dei propri diritti in relazione ai propri dati al fine di condurlo a una scelta consapevole circa il loro utilizzo, influenzando i termini e le condizioni stabiliti dalle organizzazioni di utenti dei dati[60]. Il vantaggio che ne deriva non è (tanto) un guadagno in termini monetari, ma piuttosto un beneficio sul piano del controllo dei dati e di efficienza del servizio. Al fine di raggiungere l'obiettivo suddetto, il legislatore europeo ha adottato un modello – quello della cooperativa – che prevede il controllo dei dati, personali e non, da parte dei singoli membri con un approccio diffuso, cioè una *governance* collettiva esercitata dalla cooperativa secondo diversi modelli di operatività. D'un lato, resta ferma la *governance* individuale stante nel controllo in capo ai singoli membri sui propri dati; dall'altra, una *governance* collettiva sui dati dei singoli membri attraverso una gestione partecipata circa le modalità di utilizzo dei dati in forma cooperativa.

7. La struttura delle cooperative di dati: l'elemento soggettivo e oggettivo.

La definizione di «cooperativa di dati», così come ci perviene dalla norma europea, pone l'interprete dinanzi a non pochi nodi irrisolti. Fuori dai denti: si tratta di una definizione assai laconica.

---

pria retribuzione riprendendo il controllo del proprio lavoro utilizzando l'applicazione Driver's Seat per la trasparenza delle retribuzioni, il monitoraggio dei tempi e delle miglia, le informazioni di mercato basate sul *crowdsourcing* e gli strumenti di raccomandazione di intelligenza artificiale. Un'altra esperienza che vale menzionare è quella di Pescadata, una cooperativa di dati che ha dato vita a un'applicazione progettata secondo principi di inclusione, resilienza e innovazione tecnologica, per la gestione delle organizzazioni di pesca e per motivare il lavoro collettivamente e individualmente, affrontando le sfide della pesca su larga scala operante in Messico, America Latina e Caraibi.

[59] Le cooperative di dati possono rappresentare uno strumento utile non solo per gli interessati ma anche per le imprese individuali, le microimprese e le piccole e medie imprese parche di informazioni e dati al pari degli interessati individuali.

[60] È bene precisare, all'uopo, che a norma del Reg. (UE) 2016/679, i diritti succitati possono essere esercitati solo a titolo individuale, non potendo costituire oggetto di delega a una cooperativa di dati.

Anzitutto (e soprattutto), dal punto di vista dell'elemento soggettivo laddove il Legislatore europeo manca di precisare (forse volutamente) la ragione sociale che la «struttura organizzativa costituita da interessati, imprese individuali o da PMI» dovrebbe avere [61], lasciando maglie larghe circa la forma societaria che può assumere una cooperativa pur definendone, al contempo, i tratti essenziali che si sostanziano in una *governance* condivisa tra i membri, in capo a ciascuno dei quali è riconosciuto il controllo sui propri dati.

Quanto all'elemento oggettivo delle cooperative di dati, invece, è fuor di dubbio che la loro funzione abbia carattere mutualistico che si sostanzia in ciascuno dei tre obiettivi indicati in normativa: aiutare i membri nell'esercizio dei loro diritti in relazione a determinati dati; favorire il confronto tra i membri sulle finalità e sulle condizioni del trattamento dei dati; negoziare i termini e le condizioni per il trattamento dei dati prima di concedere l'autorizzazione al trattamento. I membri delle cooperative di dati, dunque, possono raggiungere alternativamente una delle finalità indicate, così traendone vantaggio non solo e non tanto a livello patrimoniale, quanto «sul piano del controllo sulle modalità di trattamento e utilizzo secondario dei dati» [62].

Le ombre si espandono anche sul fattore procedurale, giacché la normativa è parca di dettagli circa le modalità con cui le cooperative di dati possono operare sul mercato. Interessante, tuttavia, è la previsione al *considerando* n. 31 ove il legislatore precisa che «è importante riconoscere che i diritti a norma del regolamento (UE) 2016/679 sono diritti personali dell'interessato e che quest'ultimo non può rinunciarvi. Le cooperative di dati potrebbero altresì rappresentare uno strumento utile per imprese individuali e PMI che, in termini di conoscenze in materia di condivisione dei dati, sono spesso equiparabili ai singoli individui». Ne deriverebbe la possibilità di stipulare un contratto di mandato con rappresentanza che consenta alla cooperativa di dati di rappresentare i propri membri per la tutela dei diritti degli interessati. V'è da escludere, invece, la possibilità di conferire alla cooperativa i dati e i relativi poteri ad essi correlati stando a quanto disposto dall'art. 12, il quale dispone che «il fornitore di servizi di intermediazione dei dati non utilizza i dati per i quali fornisce servizi di intermediazione dei dati per scopi diversi dalla messa a disposizione di tali dati agli utenti dei dati e fornisce servizi di intermediazione dei dati attraverso una persona giuridica distinta». Stando così le cose, la funzione delle cooperative sembrerebbe circoscritta alle attività di consulenza ai propri membri e a quella di mera trasmissione a terzi delle manifestazioni di volontà dell'interessato che non può essere delegata a terzi [63].

---

[61] Sul punto si rimanda a F. BRAVO, *Le cooperative di dati*, in *Contr. e impresa*, 2023, 3, p. 762, il quale ha opportunamente evidenziato che ben potrebbe essere attribuita alle cooperative di dati la forma delle associazioni temporanee di imprese o dei raggruppamenti temporanei di impresa o delle reti di impresa.

[62] G. RESTA, *La regolazione digitale nell'Unione europea – Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, in *Riv. trim. dir. pub.*, 2022, 4, p. 971.

[63] L. LIONELLO, *La creazione del mercato europeo dei dati: sfide e prospettive*, in *Dir. del comm. intern.*, 2021, 3, p. 675.

8. Le cooperative di dati nel settore bancario a beneficio di banche cooperative e clienti: chimera o prossima realtà?

Le considerazioni fin qui svolte consentono di tracciare un primo, provvisorio bilancio, sebbene siano ancora tante le nubi che si addensano attorno alla disciplina delle cooperative di dati.

Le cooperative di dati rappresentano uno strumento inedito e un terreno (ancora) inesplorato nell'ordinamento nostrano e, in particolare, nel settore bancario ma non per questo sono immeritevoli di approfondimento. Pare lecito domandarsi, a tal proposito, se e in quali limiti sia possibile applicare il modello delle cooperative di dati al settore bancario, limitatamente alle banche di credito cooperativo a tutela della clientela da una valutazione del merito di credito basata sui *big data*. Siamo giunti al cuore della questione. Non essendo questa la sede per un'estesa analisi delle banche di credito cooperativo, che è un tema decisamente noto e arato, ci si limiterà solo a introdurre spunti in materia e, senza pretesa di esaustività, a rispondere all'interrogativo posto.

Ma andiamo con ordine. È noto che il tratto caratteristico delle banche di credito cooperativo sia la loro prossimità territoriale [64]. E, se da un lato, la loro territorialità consente di avere una maggiore conoscenza dei bisogni della clientela e del territorio, dall'altro espone il sistema bancario al rischio di pratiche distorte nella concessione del credito laddove gli intermediari potrebbero abdicare agli obblighi di valutazione del merito creditizio su loro incombenti, fondando il giudizio di credito su conoscenze personali [65] circa il grado di solvibilità del cliente ovvero facendo ricorso a sistemi di valutazione del merito di credito basati sull'analisi tanto di *hard data* quanto di *soft data*, incorrendo così nei pericoli già prospettati nel caso di concessione di credito al cliente immeritevole [66].

È rispetto a quest'ultimo caso che si potrebbe ritenere utile la costituzione, all'interno delle banche cooperative, di cooperative di dati sotto il *vestimentum* di società cooperativa tra i soci e i clienti, al fine di rendere edotti questi ultimi sull'utilizzo dei loro dati e sulla tutela della loro privacy, ed evitare un uso distorto dei dati dal quale possa discendere una valutazione erronea circa l'*an* e il *quantum* del finanziamento da concedere. Una tale ipotesi ha il vantaggio di rafforzare un elemento caratteristico delle cooperative di dati che risiede nella sua alternatività rispetto agli schemi imprenditoriali lucrativi tradizionali, stante la natura puramente mutualistica, e la loro capillarità a livello territoriale.

---

[64] Ai sensi dell'art. 33, co. 2, del Testo unico bancario «Per essere soci di una banca di credito cooperativo è necessario risiedere, aver sede ovvero operare con carattere di continuità nel territorio di competenza della banca stessa».

[65] I. SABBATELLI, *COVID-19 e merito di credito*, in *Nuova giur. civ. comm*., 2020, 2, p. 64; F. TRAPANI, *Riflessioni sulla verifica del merito creditizio di soci di banche cooperative*, in *Banca, borsa e tit. cred*., 2023, 5, p. 696.

[66] Non si prende in esame, in questa sede, il caso di diniego indebito di credito.

Capitolo XXXI

Le cooperative di dati nel settore dei servizi di *ride-hailing*

Carlo Basunti

Abstract: The paper analyses the applications of services of data cooperatives, as recently outlined by the European legislator in the Data Governance Act (EU Reg. 868/2022), in the context of ride-hailing services. In a framework in which the mobility sector is undergoing important evolutions, thanks to the use of data and artificial intelligence systems, the cooperative model stands out as a valid tool for the valorization of data, with a view to economic growth and social welfare.

1. Premesse.

Le scelte di politica legislativa adottate a livello europeo, pur nell'ambito di un bilanciamento tra contrapposti diritti ed interessi, tutti meritevoli di tutela, proiettano sempre più i dati (personali) entro logiche di scambio, incentivandone la circolazione e massimizzandone la valorizzazione. È ormai questa la strada che, dapprima con il Regolamento (UE) 2016/679 (GDPR) e oggi con il Regolamento (UE) 2022/868 (DGA), viene tracciata, nell'intento di promuovere il mercato digitale in cui i dati rappresentano, sempre più, *assets* di importanza strategica per i soggetti, pubblici e privati, che operano in tale mercato.

Precisamente, la Strategia europea per i dati [1], in cui il DGA si inserisce, mira ad

[1] COMMISSIONE EUROPEA, Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Una Strategia europea per i dati*, Bruxelles, 19 febbraio 2020 [COM (2020) 66 *final*].

assicurare all'Unione europea un ruolo guida nell'ambito dell'economia *data driven*, favorendo un sapiente utilizzo dei dati. In questa direzione, si intende delineare un paradigma di sviluppo in cui la persona, con i suoi diritti fondamentali (tra cui, soprattutto, il diritto alla protezione dei dati personali), mantiene la centralità che, a ragione, deve caratterizzarla, ma in cui è manifesta la convinzione che, attraverso i dati, tanto il settore privato quanto quello pubblico, ognuno secondo le proprie specificità, possano disporre di strumenti per adottare decisioni migliori e conoscere così nuove linee di crescita. È dunque cruciale la costruzione di una solida architettura – *in primis*, normativa – che consenta di cogliere le opportunità offerte dai dati, in modo da indirizzare i vantaggi che ne derivano (anche) al benessere sociale. Un simile quadro non può certo prescindere da un utilizzo responsabile dei dati che, improntato alla sostenibilità, faccia propri i principi dell'etica e, ponendo al centro la persona umana, miri alla creazione di un *digital ecosystem* più equo, inclusivo e solidale.

In questo contesto, le cooperative di dati [2] – disciplinate a partire dal DGA che le inserisce tra i servizi di intermediazione dei dati [3] e che, in realtà, fa riferimento ai servizi di cooperative di dati e non alle cooperative di dati in sé – si presentano quale nuovo paradigma per un utilizzo sostenibile dei dati (personali e non personali), secondo le logiche del neomutualismo [4], nella sua moderna declinazione di neomutualismo digitale [5].

---

[2] Sul tema, v. F. BRAVO, *Le cooperative di dati*, in *Contr. e impr*., 2023, 4, p. 757 ss.

[3] I servizi di intermediazione dei dati, elencati all'art. 10 DGA, sono: «a) servizi di intermediazione tra i titolari dei dati e i potenziali utenti dei dati, compresa la messa a disposizione di mezzi tecnici o di altro tipo per consentire tali servizi (…); b) servizi di intermediazione tra interessati che intendono mettere a disposizione i propri dati personali o persone fisiche che intendono mettere a disposizione dati non personali e potenziali utenti dei dati, compresa la messa a disposizione di mezzi tecnici o di altro tipo per consentire tali servizi, permettendo in particolare l'esercizio dei diritti degli interessati di cui al regolamento (UE) 2016/679; c) servizi di cooperative di dati»; il considerando n. 27 DGA afferma che: «si prevede che i servizi di intermediazione dei dati svolgano un ruolo essenziale nell'economia dei dati, in particolare nel sostenere e promuovere pratiche volontarie di condivisione dei dati tra imprese o nell'agevolare la condivisione dei dati nell'ambito degli obblighi stabiliti dal diritto dell'Unione o nazionale. Essi potrebbero diventare strumenti che agevolano lo scambio di quantità considerevoli di dati pertinenti. I fornitori di servizi di intermediazione dei dati, che possono includere anche enti pubblici, che offrono servizi che collegano i diversi soggetti dispongono del potenziale per contribuire alla messa in comune efficiente dei dati come pure all'agevolazione della condivisione bilaterale dei dati». Su tali servizi, cfr. F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al* Data Governance Act, in *Contr. e impr. Europa*, 2021, 1, p. 199 ss.; ID., *Data Governance Act and Re-Use of Data in the Public Sector*, in ID.-J. VALERO TORRIJOS (eds.), *Data Governance, Open Data and Data Protection in the Public Sector (Monographic Section)*, in *Eur. Rev. of Digital Administration & Law (ERDAL)*, 2022, 2, p. 15 parla di «*key role of data intermediaries*»; D. POLETTI, *Gli intermediari dei dati*, in *European J. of Privacy Law & Tech*., 2022, 1, p. 46 ss.; anche in ID., *Gli intermediari dei dati*, in A. MORACE PINELLI (a cura di), *La circolazione dei dati personali. Persona, contratto e mercato*, Pisa, 2023, p. 105 ss.

[4] V. P. VENTURI-F. ZANDONAI, *Neomutualismo. Ridisegnare dal basso competitività e* welfare, Milano, 2022.

[5] F. BRAVO, *Le cooperative di dati*, cit., p. 764 ss. e *passim*, a p. 766, l'Autore afferma: «mi pa-

È soprattutto attraverso le cooperative di dati che, nell'ambito della *European Strategy for Data*, il legislatore europeo mira a ridisegnare gli equilibri oggi presenti tra gli agenti del mercato digitale in cui si assiste a forme di sostanziale oligopolio da parte delle c.d. *Big Tech*. In questo senso, si vuole far emergere, nell'ambito dell'economia digitale, soggetti quali PMI e *start-up*, permettendo loro di avere un ruolo di rilievo. Tali soggetti, infatti, ben potrebbero divenire membri di una cooperativa di dati in qualità di *data holders* e inserirsi così attivamente nella circolazione dei dati secondo il modello mutualistico proprio della cooperativa (di dati). Questa prospettiva merita sicuro apprezzamento in quanto una simile concentrazione di potere nelle mani di pochi non solo mina il corretto funzionamento del mercato nel suo insieme, ma pone altresì in pericolo, tra gli altri, il diritto alla *privacy*, nella sua più attuale accezione di diritto all'autodeterminazione informativa, nonché l'autonomia contrattuale dei singoli.

Pare possibile affermare che le cooperative di dati possano svolgere un ruolo chiave, tra gli altri, nel settore della mobilità, caratterizzato sempre più, a maggior ragione avendo riguardo ad una prospettiva futura, da un'ampia condivisione di dati. L'ambito dei servizi di *ride-hailing* in particolare, su cui si intende incentrare la presente indagine con un approccio metodologico di tipo casistico, ben potrebbe rappresentare un terreno fertile per una proficua applicazione delle cooperative di dati. L'impiego del *cooperative model* in tale settore sarebbe, infatti, capace di apportare svariati benefici sia per gli utenti sia per i fornitori dei menzionati servizi, come pure per soggetti terzi, quali imprese private e pubbliche amministrazioni, che potrebbero rapportarsi con la cooperativa, accedendo ai dati trattati in guisa da sfruttarli al meglio, rispettivamente, per la loro crescita economica e per il benessere sociale.

2. Il fondamentale utilizzo dei dati nell'*automotive* e le relative criticità.

L'applicazione delle nuove tecnologie e, segnatamente, dei sistemi di intelligenza artificiale nella realtà quotidiana è ormai un dato assolutamente ineludibile: del resto, l'IA non è (più) fantascienza, ma fa già parte delle nostre vite [6]. Ciò impone l'adozione di un solido apparato di regole [7], (anche) attraverso il ricorso ai principi generali del diritto, che permette di attribuire opportuna rilevanza al quadro di insieme ed all'utilizzo, da parte degli interpreti, di soluzioni esegetiche

re che la cornice teorica del mutualismo digitale possa ben interpretare, sul piano economico, l'introduzione del modello giuridico delle cooperative di dati quale fattore di sviluppo per la *data governance*».

[6] Così COMMISSIONE EUROPEA, Comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, *L'intelligenza artificiale per l'Europa*, COM (2018) 237, *final*, Bruxelles, 25 aprile 2018, p. 1.

[7] G. FINOCCHIARO, *Intelligenza artificiale. Quali regole?*, Bologna, 2024; v. anche ID., *Diritto dell'intelligenza artificiale*, Bologna, 2024.

già consolidate[8]. Sul punto non può essere taciuta la recente adozione, a livello europeo, dell'*AI Act*[9].

È proprio l'intelligenza artificiale ad enfatizzare uno degli aspetti più pervasivi ed inquietanti del mondo digitale: la raccolta, l'elaborazione e l'impiego di un'enorme quantità di dati personali, i c.d. *Big Data*[10]. Si tratta di una sfida di primaria importanza imposta dall'avvento dell'IA: coniugare opportunamente la promozione dell'impiego dei sistemi intelligenti con la tutela di ogni individuo e, quindi, dei suoi dati personali che ne rappresentano attributi della personalità.

Banco di prova per l'applicazione dei sistemi di intelligenza artificiale e per le relative ricadute (anche) sul sistema giuridico – segnatamente, su quello della protezione dei dati personali – è sicuramente rappresentato dal settore dell'*automotive*[11], emblema di quei progressi tecnologici che hanno contribuito, contribuiscono e contribuiranno a trasformare la mobilità.

Nel futuro ormai prossimo, si assisterà ad una svolta epocale nella produzione dei mezzi di trasporto con modalità di guida sempre più automatizzate, *self driving cars*, o totalmente autonome, *driverless cars*, che guideranno come noi, ma al posto nostro e, come tali, saranno destinate a soddisfare le esigenze di una ancora più ampia platea di fruitori. La guida affidata all'intelligenza umana, propria dei veicoli a trazione meccanica, sarà sostanzialmente consegnata alla guida autonoma con evidenti vantaggi per la tutela dell'ambiente (grazie all'utilizzo di fonti di energia rinnovabili), per la sicurezza stradale e con importanti ricadute sul mercato assicurativo.

Il funzionamento dei sistemi di trasporto intelligente, nei relativi livelli di automazione[12], si fonda su un ingente flusso di dati[13]. Si tratta di veicoli connessi con

---

[8] In questo senso G. FINOCCHIARO, *Riflessioni su diritto e tecnica*, in *Dir. inf.*, 2012, 4-5, p. 838.

[9] Reg. (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale).

[10] Così, G. ALPA, *L'intelligenza artificiale. Il contesto giuridico*, Modena, 2021, p. 71.

[11] Ampiamente, sui vari aspetti che legano diritto ed *automotive*, in una prospettiva multidisciplinare (anche) con riferimento all'impatto dell'intelligenza artificiale, cfr. E. AL MUREDEN, *Diritto dell'*automotive. *Dalla fabbrica alla strada: tra regole, mercato, tecnologia e società*, Bologna, 2024.

[12] La *Society of Automotive Engineers* (SAE) *International* ha operato una classificazione dei veicoli intelligenti in funzione del diverso controllo umano esercitato. V. *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles* nella sua ultima versione del 30 aprile 2021, in *https://www.sae.org/standards/content/j3016_202104/*. Precisamente, si tratta: del livello 0 che corrisponde all'auto tradizionale non automatizzata; del livello 1 in cui sono presenti quei sistemi di *driver assistance* ormai presenti nella maggior parte dei veicoli di recente produzione (come, ad esempio, *stability control*, *cruise control*, *lane correction technology*); di un livello 2 in cui i dispositivi automatici controllano sia le funzioni di sterzata sia quelle di accelerazione e decelerazione in determinate situazioni, senza eliminare, comunque, il necessario costante controllo da parte del pilota; di un livello 3 in cui il *software* ha il pieno controllo dell'ambiente di guida e ne svolge tutte le funzioni, ma spetta al conducente un ruolo di monitoraggio, restando sempre pronto ad intervenire, laddove lo scenario prefigurato nella mappatura si modifichi, rendendo necessarie operazioni che non erano preventivabili in base alle informa-

devices come *smartphones*, *smartwatches*, *tablets*, *personal computers*, e così via (V2D); con le varie infrastrutture in cui si muovono (V2I); con altri veicoli (V2V). Il loro utilizzo, infatti, se, tra i numerosi benefici, promette una drastica diminuzione degli incidenti stradali e delle conseguenze negative sulle persone coinvolte, tanto che la loro diffusione è stata acutamente posta in parallelo a quella di un vaccino [14], lo stesso utilizzo determina altresì nuovi interrogativi per il giurista che non possono essere trascurati nella prospettiva di tutela della persona (e dei suoi dati) [15].

Le necessarie interconnessioni poste alla base della circolazione dei veicoli autonomi che, tra l'altro, richiedono un adattamento della stessa rete stradale in guisa

---

zioni a disposizione *ex ante*; di un livello 4 in cui la presenza umana è superflua a meno che non ci si trovi in situazioni in cui la guida automatizzata non è possibile o in cui sia il pilota stesso a voler condurre il veicolo; di un livello 5 in cui i veicoli svolgono in piena autonomia le funzioni di guida e, pertanto, possono anche essere prive degli strumenti (pedali, sterzo) attraverso cui la guida stessa si realizza.

[13] V. EDPB, *Linee guida 01/2020 sul trattamento dei dati personali nel contesto dei veicoli connessi e delle applicazioni legate alla mobilità*, versione 2.0, del 9 marzo 2021.

[14] Di particolare interesse sul punto le riflessioni di G. CALABRESI-E. AL MUREDEN, Driverless cars. *Intelligenza artificiale e futuro della mobilità*, Bologna, 2021, spec. p. 167 ss.

[15] Nell'ormai ampia letteratura sul tema, v. E. AL MUREDEN, *"*Autonomous cars*" e responsabilità civile tra disciplina vigente e prospettive "*de iure condendo*"*, in *Contr. e impr*., 2019, 3, p. 895 ss.; ID., Event Data Recorder *e* Advanced Driver Assistance System*: la "spinta gentile" verso la mobilità del futuro*, in *Contr. e impr*., 2022, 2, p. 390 ss.; ID., *La guida automatizzata di livello 3 tra principi sovrannazionali, armonizzazione eurounitaria e riflessi sul diritto nazionale*, in *Contr. e impr. Europa*, 2022, 3, p. 553 ss.; ID., Autonomous vehicles *e responsabilità civile nel sistema statunitense*, in U. RUFFOLO (a cura di), *XXVI lezioni di diritto dell'intelligenza artificiale*, Torino, 2021, p. 176 ss.; G. CALABRESI-E. AL MUREDEN, Driverless car *e responsabilità civile*, in *Riv. dir. banc*., 2020, 1, suppl., p. 7 ss.; U. RUFFOLO-E. AL MUREDEN, *"*Autonomous vehicles*" e responsabilità nel nostro sistema ed in quello statunitense*, in *Intelligenza artificiale e diritto*, a cura di Gabrielli e Ruffolo, in *Giur. it*., 2019, 7, p. 1704 ss.; U. RUFFOLO, *La responsabilità da produzione, proprietà e "conduzione" di veicoli autonomi*, in ID. (a cura di), *XXVI lezioni di diritto dell'intelligenza artificiale*, cit., p. 163 ss.; ID., Self-driving car, *auto* driverless *e responsabilità*, in ID. (a cura di), *Intelligenza artificiale e responsabilità*, Milano, 2017, p. 31 ss.; M. TAMPIERI, *L'intelligenza artificiale: una nuova sfida anche per le automobili*, in *Contr. e impr*., 2020, 2, p. 732 ss.; ID., *L'intelligenza artificiale e le sue evoluzioni. Prospettive civilistiche*, Milano, 2022, p. 243 ss.; G. CONTISSA-F. LAGIOIA-G. SARTOR, *La manopola etica: i veicoli autonomi eticamente personalizzabili e il diritto*, in *Sist. intell. Riv. quad. sci. cogn. e intell. art.*, 2017, 3, p. 601 ss.; A. ALBANESE, *La responsabilità civile per i danni da circolazione di veicoli ad elevate automazione*, in *Eur. dir. priv*., 2019, 4, p. 995 ss.; A. DAVOLA-R. PARDOLESI, *In viaggio col robot: verso nuovi orizzonti della r.c. auto ("*driverless*")*, in *Danno e resp*., 2017, 5, p. 616 ss.; K.S. ABRAHAM-R.L. RABIN, *Automated Vehicles and Manufacturer Responsibility for Accidents: A New Legal Regime for a New Era*, in *Virginia Law Rev*., 2019, 1, p. 127 ss.; B.W. SMITH, *Automated Driving and Product Liability*, in *Michigan St. Law Rev*., 2017, 1, p. 1 ss.; M.C. GAETA, *Liability rules and self-driving cars: The evolution of tort law in the light of new technologies*, Napoli, 2019; CEREA, *Responsabilità civile e sistemi "intelligenti"*, Torino, 2024, p. 35 ss.; con particolare riferimento al rapporto tra veicoli autonomi e tutela dei dati personali, v. ID., *La protezione dei dati personali nell'*Internet of things: *l'esempio dei veicoli autonomi*, in *Dir. inf*., 2018, 1, p. 147 ss.; S. SCAGLIARINI, *Smart Roads and Autonomous Driving vs. Data Protection: the Problem of the Lawfulness of the Processing*, in *Eur. Rev. of Digital Administration & Law (ERDAL)*, 2021, 2, p. 189 ss.; F. MOLLO, *I sistemi di trasporto intelligente tra sviluppo della robotica e tutela della persona*, in *Contr. e impr. Europa*, 2021, 2, p. 453 ss.

da permetterne il funzionamento [16], creano flussi di dati che non possono sfuggire al controllo degli interessati. Tali dati possono essere sia dati personali sia dati non personali: una simile distinzione, tutt'altro che facile nel caso concreto, appare di fondamentale importanza per le relative cautele che devono essere adottate.

I dati possono provenire sia dall'utente del veicolo autonomo (proprietario, conducente, passeggero) sia dal veicolo stesso. Nel primo caso (*customer provided data*) si tratterà certamente di dati personali cui risulta applicabile il GDPR, nel secondo (*vehicle generated data*) il problema è più complesso, dal momento che, in questa categoria, vi possono rientrare dati personali come pure semplici dati tecnici (*technical data*). Di più, tra i dati personali – provenienti da persone fisiche che utilizzano il veicolo o dal veicolo stesso – ben potrebbero rientrarvi, in determinate situazioni, anche dati appartenenti a categorie particolari di dati personali di cui all'art. 9 GDPR. Anche il mero dato tecnico, in combinazione con altri dati, potrebbe divenire dato personale se collegabile in via deduttiva ad una specifica persona fisica, fornendo informazioni di essa. Del resto, l'ampia nozione di dato personale accolta nell'architettura delineata dal GDPR comprende «qualsiasi informazione riguardante una persona fisica identificata o identificabile» (art. 4, par. 1, 1) GDPR) e, dunque, sia informazioni direttamente riguardanti l'interessato sia indirettamente collegabili a quest'ultimo. Dati relativi a componenti del veicolo come, ad esempio, il suo motore, oppure relativi al suo utilizzo, quali lo stato di usura degli pneumatici o il numero di chilometri percorsi, seppur, almeno ad una prima analisi, possono essere inquadrati come meri dati tecnici, potrebbero, indirettamente, attraverso l'unione con altri dati, permettere l'identificazione di una persona fisica e, quindi, divenire, dati personali.

Pertanto, appare preferibile, sul punto, l'adozione di una prospettiva restrittiva che vagli con stretto rigore la tipologia di dati trattati e qualifichi come dati tecnici solamente quei dati che non possono in alcun modo, né direttamente né indirettamente, essere riferibili ad un *data subject*.

Posto che l'innovazione tecnologica non può non andare di pari passo con la tutela della persona, la protezione dei dati personali richiede, da parte dei sistemi di trasporto intelligente e, dunque, da parte del titolare del trattamento, sulla scorta del principio di *accountability* [17], un puntuale rispetto della normativa *privacy*. Particolare attenzione dovrà essere prestata alle basi giuridiche capaci di legittimare il trattamento e, su tutte, il consenso. L'interessato, a prescindere dal ruolo rivestito nell'impiego degli *automated vehicles*, quindi anche laddove sia solamente un passeggero, deve ottenere un'adeguata informativa tale da porlo nella condizione di decidere liberamente se prestare il proprio consenso al trattamento o meno. Va da sé che, in taluni casi, il consenso non può rappresentare un'adeguata base giuridica per il trattamento. Si pensi, ad esempio, ad un soggetto che viene ripreso da una

[16] Cfr. sul punto il c.d. Decreto *Smart Roads*, Decreto 28 febbraio 2018, del Ministro delle infrastrutture e dei trasporti.

[17] Su tale principio, per tutti, si rinvia alle acute considerazioni di G. FINOCCHIARO, *Il principio di* accountability, in *Giur. it*., 2019, 12, p. 2778 ss.

smart car che transita nelle vicinanze: è quanto mai evidente che tale soggetto non abbia prestato alcun (valido) consenso al trattamento dei suoi dati e, pertanto, dovrà necessariamente essere ricercata un'altra base giuridica su cui fondare il trattamento.

L'impiego di una *disruptive technology*, quale è l'intelligenza artificiale, nell'*automotive*, determina una vera e propria rivoluzione della mobilità che dovrà essere ripensata e adattata, *in primis* con l'ausilio del legislatore, alle esigenze che emergono nella realtà.

Si stima che sempre meno persone saranno proprietarie di automobili, preferendo spostarsi con servizi di trasporto, gestiti comodamente da *apps* e che, presumibilmente, utilizzeranno veicoli *self-driving* o *driverless* di tipo elettrico. Dunque, servizi di taxi, *car sharing* e *ride-hailing* automatici dovrebbero contribuire a decongestionare il traffico grazie alla diminuzione del numero complessivo di automobili private in circolazione, presentando tra l'altro, importanti ricadute in termini di tutela ambientale. In altri termini, si presenterà un nuovo scenario nel quale l'auto diventerà (anche) un servizio condiviso.

In questo quadro, pare potersi affermare che le cooperative di dati possano assumere un ruolo di assoluto rilievo. Un simile modello sostenibile di *governance* dei dati (personali e non personali) appare assolutamente adeguato ai fini di una miglior gestione dei flussi di dati prodotti dall'impiego di *automated vehicles* e, più in generale, nell'ambito di realtà infrastrutturali che ne permettano la circolazione. E questo sia avendo riguardo all'*empowerment* che si mira a fornire all'interessato nella gestione dei propri dati sia alla possibilità, in capo a soggetti pubblici, di poter utilizzare (e riutilizzare) i dati raccolti per il bene della società intera.

3. Il caso Driver's Seat.

3.1. Driver's Seat quale modello di cooperativa di dati nel settore dei servizi di *ride-hailing*.

Nella prassi, si assiste, già da qualche tempo, all'applicazione del modello cooperativo tra i fornitori di servizi di *ride-hailing*.

Così nasce Driver's Seat [18] che si propone come alternativa al modello capitalistico

[18] Per maggiori informazioni, si rinvia al sito *web* della cooperativa: *https://driversseat.co*. V. anche F. BRAVO, *Le cooperative di dati*, cit., p. 770 ss.; H.A. CHAUDARI-J.W. BYERS-E. TERZI, *Putting Data in the Driver's Seat: Optimizing Earnings for On-Demand Ride-Hailing*, in *WSDM*, 2018, p. 90 ss.; M.M. BÜLER et al., *Unlocking the Power of Digital Commons: Data Cooperatives as a Pathway for Data Sovereign, Innovative and Equitable Digital Communities*, in *Digital*, 2023, 3, p. 146 ss.; V. DUBAL, *On Algorithmic Wage Discrimination*, in *Columbia Law Rev.*, 2023, 7, spec. p. 1985 ss.; A. FISHER-T. STREINZ, *Confronting Data Inequality*, in *Columbia J. of Trans. Law.*, 2022, 3, spec. p. 946; E. BIETTI-A. ETXEBERRIA-M. MANNAN-J. WONG, *Data Cooperatives in Europe: A Legal and Empirical Investigation*, *White Paper created as part* of *The New School's Platform Cooperativism Consortium and Harvard University's Berkman Klein Center for Internet & Society Research Sprint*,

tracciato da Uber e Lyft, esempio seguito, ma dal quale, ad un tempo, si intende prendere le distanze. Tale progetto è valso, tra le altre, le sovvenzioni della Rockefeller Foundation e della Ford Foundation. Si tratta di un'idea che da tempo albergava nelle menti dei lavoratori del settore, sempre più succubi di un sistema non trasparente che non permetteva loro un controllo effettivo sui dati. È, infatti, un dato comune che le *gig platforms* esercitino un controllo penetrante sul lavoro di chi opera attraverso la piattaforma stessa, per mezzo di algoritmi opachi e fornendo informazioni limitate circa l'organizzazione del lavoro, soprattutto nel rapporto tra tempo e guadagno.

Driver's seat è una cooperativa di dati creata da *gig workers* per *gig workers*: si includono tutti coloro che trasportano beni o persone ed il cui lavoro è mediato da una *app*. Come erogatore di servizi, essa si propone di offrire servizi di *ride-hailing* e *ride-sharing* (sul modello di Uber e Lyft) nonché di *food-delivering* (sul modello di Glovo, Deliveroo e Uber Eats). Non si presenta come una classica *ride-hailing company*, ma è progettata su misura per gli autisti, al fine di massimizzare le potenzialità dei loro dati, aumentare i loro margini di guadagno e promuovere il bene comune con riguardo al settore di pertinenza.

L'obiettivo centrale è quello di offrire benefici primariamente ai propri membri: il vero proposito non è la monetizzazione dei dati per finalità di guadagno (fine comunque presente, ma che assume una portata ancillare), ma quello di collazionare i dati ed analizzarli per condividere *insights* utili per i propri membri. Il tutto, nell'ambito di un rapporto fiduciario che lega la cooperativa ai soci. Tale fiducia affonda le radici nell'intento di ribaltare il sistema per come delineato dalle note e grandi piattaforme che offrono servizi analoghi. Si intende così incentivare la condivisione dei dati secondo modalità differenti da quelle a cui i lavoratori delle piattaforme digitali sono abituati, attraverso l'incentivo di una appropriata *data governance*. Anche in questo caso, si ha la raccolta di dati da parte dei *drivers*, ma questi vengono posti in prima linea sul controllo di tali dati, che non viene certo lasciato unicamente ai gestori della piattaforma.

In qualità di erogatore di servizi di cooperativa di dati, Driver's Seat opera in diverse città statunitensi. I membri devono scaricare una apposita *app* il cui *download* è permesso solo nelle zone di attività della cooperativa. In questo modo, tramite il proprio *smartphone*, gli autisti condividono – decidendo sull'*an*, *quando* e *quomodo*, e, dunque, mantenendo il controllo – i loro dati con la cooperativa che assume il compito di utilizzarli al meglio per massimizzarne le potenzialità sia a beneficio dei singoli membri sia della cooperativa nel suo complesso. In questo senso, Driver's Seat si impegna ad aumentare i margini di guadagno degli autisti tramite la condivisione di informazioni sugli orari più redditizi in cui lavorare, sulle zone in cui è solitamente presente una maggior richiesta del servizio, sui percorsi più trafficati e, quindi, da evitare nonché, al contrario, su quelli che sono da preferire per viaggi più rapidi. I membri possono monitorare in modo costante e traspa-

---

December 2021, in *https://cyber.harvard.edu/sites/default/files/2022-02/Data_Cooperatives_Europe-group2.pdf*, p. 8 ss.

rente il lavoro compiuto con particolare riguardo al rapporto tra tempo impiegato, chilometraggio complessivamente percorso e spese sostenute (carburante, pedaggi, riparazioni del veicolo, e così via). Di più, tramite l'*app*, è possibile confrontare i guadagni medi di altri soggetti che lavorano per le altre compagnie con i propri, al fine di permettere una scelta libera e consapevole ai lavoratori.

Il motto di Driver's Seat, che racchiude efficacemente il suo operato, è «*Know more. Earn more*» [19].

Se il maggior guadagno (*earn more*) promesso agli autisti è chiaro in base ad un uso mirato e particolarmente proficuo dei dati, seppur ne sembri opportuno un inquadramento in senso ampio, nell'ottica di migliori condizioni lavorative (in cui, certamente, viene ricompresa una miglior remunerazione); la maggior conoscenza (*know more*), a parere di chi scrive, deve essere letta in una triplice prospettiva. Nell'ambito di ciò che la cooperativa promette, la maggior conoscenza può essere riferita: i) alla maggior cognizione relativa al lavoro compiuto dal singolo autista, calato nel rapporto tra costi sostenuti e guadagni effettuati; ii) alla consapevolezza dell'operato degli altri colleghi che lavorano per Driver's Seat o per i *competitors*. Va da sé che i dati collazionati vengono crittografati e la cooperativa sottolinea di aver implementato misure di sicurezza amministrative, fisiche e tecnologiche per difendersi da eventuali *data breaches*. Si garantisce, inoltre, che chiunque abbia accesso ai dati personali presenti nel sistema sia soggetto ad obblighi contrattuali e professionali di salvaguardia di tali dati nel rispetto della normativa in tema di *data protection* [20]. Gli autisti conoscono, pertanto, dati che rappresentano valori di stima, non riferibili a singoli individui, così che, da un lato, essi possano ottenere informazioni utili per meglio improntare il lavoro e, dall'altro, nessuno subisca una lesione della propria *privacy*; iii) alla disponibilità di dati di cui gode la cooperativa, funzionale, in primo luogo, a migliorare le condizioni di lavoro, *lato sensu* intese, degli autisti. Maggiore è la quantità di dati utilizzabile dalla cooperativa, maggiori saranno i ritorni percepibili dai lavoratori: è, quindi, necessaria una maggior conoscenza – *sic*, il poter collazionare grandi quantità di dati – da parte della cooperativa.

Dunque, la condivisione dei dati (*know more*) viene funzionalizzata all'ottenimento di migliori condizioni di lavoro con più ampi margini di guadagno (*earn more*).

Driver's Seat, sempre nel solco improntato a garantire la massima trasparenza nelle operazioni sui dati [21], tenta altresì di sensibilizzare i propri membri, così come

---

[19] Lo *slogan* si rinviene nella pagina di apertura del sito *web* di Driver's Seat.

[20] Driver's Seat sottolinea, però, che: «*while we strive to use commercially acceptable means to protect your personal information, no method of transmission over the Internet or form of electronic storage is 100 percent secure. Therefore, we cannot guarantee its absolute security*». In tema di *data breach* cfr. A. MANTELERO, *La gestione del rischio*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, 2019, p. 473 ss.; ID., *Si rafforza la tutela dei dati personali: "*data breach notification*" e limiti alla profilazione mediante* cookies, in *Dir. inf.*, 2012, 4-5, p. 781 ss.

[21] Si afferma infatti: «*empowerment requires transparency*».

chiunque si interfacci con la cooperativa, ad interessarsi della sorte dei propri dati nelle dinamiche circolatorie. Non è solo importante la predisposizione di idonee misure di sicurezza da parte della cooperativa che raccoglie i dati, che, comunque, rimane un requisito fondamentale cui, si è detto, la cooperativa mostra dedizione, ma anche la consapevolezza del reale significato della condivisione dei dati. Non ci si deve limitare, infatti, a prestare attenzione ai, ben chiari, benefici che ai lavoratori derivano dalla loro partecipazione alla cooperativa. Un simile approccio aprirebbe la strada a facili abusi che, del resto, quotidianamente vengono perpetrati da parte delle grandi *data companies* che, nel cieco perseguimento del profitto, offrono servizi digitali spacciandoli per gratuiti, quando, invece, per accedervi, l'interessato è tenuto a fornire il consenso al trattamento dei propri dati [22].

In maniera diametralmente opposta rispetto alle *Big Tech*, Driver's Seat si prefigge, come obiettivo centrale, quello di rendere edotti i propri soci circa i benefici loro derivanti dalla partecipazione mutualistica alla cooperativa, ma soprattutto con riferimento ai soggetti cui i dati vengono trasferiti, per quali finalità e per quanto tempo se ne ammette il trattamento, il tutto con lo scopo di agevolare un utilizzo consapevole dei dati da parte dei soggetti cui tali dati si riferiscono: vero fulcro del diritto all'autodeterminazione informativa.

L'impegno di Driver's Seat, indirizzato a far sì che gli interessati comprendano la "gravità" dell'atto che compiono e delle relative conseguenze, acconsentendo al trattamento dei loro dati, merita di essere particolarmente apprezzato. In questo

---

[22] Cfr., sul punto, G. RESTA-V. ZENO ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim. dir. e proc. civ*., 2018, 2, p. 411; nonché G. RESTA, *Digital platform and the law: contested issues*, in *Media Laws*, 2018, 1, spec. p. 243 ss.; sulle c.d. operazioni di *tying* v. S. THOBANI, *Operazioni di "*tying*" e libertà del consenso*, in *Giur. it*., 2019, 3, p. 533 ss.; ID., *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, Milano, 2018, spec. p. 94 ss.; EDPB, *Linee guida 5/2020 sul consenso ai sensi del Regolamento (UE) 2016/679*, cit., p. 11. Dal punto di vista normativo, v. l'art. 3, par. 1 della Dir. (UE) 2019/770 del Parlamento europeo e del Consiglio del 20 maggio 2019, *relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali*, ai sensi del quale «la presente direttiva si applica a qualsiasi contratto in cui l'operatore economico fornisce, o si impegna a fornire, contenuto digitale o un servizio digitale al consumatore e il consumatore corrisponde un prezzo o si impegna a corrispondere un prezzo. La presente direttiva si applica altresì nel caso in cui l'operatore economico fornisce o si impegna a fornire contenuto digitale o un servizio digitale al consumatore e il consumatore fornisce o si impegna a fornire dati personali all'operatore economico, fatto salvo il caso in cui i dati personali forniti dal consumatore siano trattati esclusivamente dall'operatore economico ai fini della fornitura del contenuto digitale o del servizio digitale a norma della presente direttiva o per consentire l'assolvimento degli obblighi di legge cui è soggetto l'operatore economico e quest'ultimo non tratti tali dati per scopi diversi da quelli previsti»; sull'interessante rapporto tra la norma appena richiamata e la versione contenuta nella proposta di Direttiva – tra le quali vi è stato l'intervento dell'EDPS, *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for supply of digital content, 14 March 2017* – v. C. CAMARDI, *Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione di dati personali*, in *Giust. civ*., 2019, 3, p. 499 ss.; e sia consentito il rinvio a C. BASUNTI, *La (perduta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali*, in *Contr. e impr*., 2020, 2, spec. p. 893 ss.

modo, infatti, per quanto possibile, la cooperativa dà il proprio contributo alla alfabetizzazione circa l'utilizzo dei dati. Tale aspetto pare poter essere ricondotto entro una visione ampia dei vantaggi di cui godono i membri della cooperativa. Non si tratta, infatti, di un tratto comune agli agenti del mercato digitale e deve, quindi, essere inquadrato come un importante beneficio per gli interessati. Laddove le limitate conoscenze dei singoli non siano sufficienti, la cooperativa sopperisce, o, almeno tenta di sopperire, fornendo una sorta di *toolkit* ai soci affinché, in autonomia, possano effettuare liberamente le scelte loro più confacenti.

Driver's Seat non rinuncia certo allo sviluppo tramite i dati, ma agisce secondo i dettami dell'etica, aspetto che caratterizza l'operato delle cooperative di dati. Incoraggiando la composizione di un *team* di membri rispettoso delle diversità, la cooperativa trasferisce i dati secondo un modello che viene definito di «*shared ownership*»[23]. Sul punto, preme però precisare che una simile qualificazione non appare giuridicamente appropriata. La cooperativa non è di certo comproprietaria dei dati insieme agli interessati: precisamente, neppure con riguardo a questi ultimi, appare corretto parlare di diritto di proprietà[24]. I dati vengono condivisi dai soggetti cui si riferiscono alla cooperativa

[23] Tale espressione viene utilizzata nel sito *web* di Driver's Seat dove si afferma anche che la cooperativa «*sell driver data*».

[24] Cfr. V. ZENO ZENCOVICH, *Do "Data Markets" Exist?*, cit., spec. p. 25 ove l'Autore, da un punto di vista semantico, afferma: «*"Ownership" is not a notion which is engraved in some sacred tables. It is the result of centuries, millennia of theoretical, religious, political, social, economic evolution*» e aggiunge: «*ownership is a concept quite different from proprieté or from Eigentum*»; sul tema v. anche J.S. BERGÉ-S. GRUMBACH-V. ZENO ZENCOVICH, *The 'Datasphere', Data Flows beyond Control, and the Challenges for Law and Governance*, in *European J. of Comp. Law and Governance*, 2018, 2, p. 144 ss.; G. ALPA, *La "proprietà" dei dati personali*, in ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, 2019, p. 11 ss.; F. BRAVO, *La «compravendita» di dati personali?*, in *Dir. internet*., 2020, 3, p. 531 ss.; ID.-V. TORRIJOS, *Data in the Public Sector and Data Valorisation*, in EAD. (eds.), *Data Governance, Open Data and Data Protection in the Public Sector (Monographic Section)*, in *Eur. Rev. of Digital Administration & Law (ERDAL)*, 2022, 2, p. 7; F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al* Data Governance Act, cit., p. 203 in cui, nel commentare l'introduzione della figura soggettiva del titolare dei dati (*data holder*) da parte del *Data Governance Act*, si esprimono preoccupazioni per tale «cambio di paradigma che rischia di essere un preludio all'introduzione, per via normativa, di una reificazione dei dati personali, quali entità giuridicamente rilevanti *ex se* più che quali attribuiti della persona»; ID., *Data Governance Act and Re-Use of Data in the Public Sector*, cit., pp. 32-33 che, nell'approfondire il riutilizzo dei dati (anche) personali da parte delle pubbliche amministrazioni, afferma: «*when it comes to personal data one cannot identify an ownership of the public sector bodies or other entities holding personal data nor can contracts on the re-use of personal data have as their object the "sale" of data: when it comes to personal data that are not anonymised, one will have to take into account the specific aspects of the GDPR's regulations*», precisando poi che «*this must not lead to the conclusion that personal data cannot be the object of contracts regulating their use, but rather that the adopted contractual solutions must be compliant with the specific nature of the fundamental right attributed to the data subject. Personal data can be the temporarily used for legitimate and specific purposes and in compliance with the principles indicated by the GDPR (including those of lawfulness, transparency and fairness, data minimisation, purpose limitation, storage limitation), which (also) have a limitative scope of contractual autonomy, to safeguard the rights and fundamental freedoms of the data subject*»; P.B. HUGENHOLTTZ, *Against "data property"*, in G. GHIDINI-

che può, sulla base ed entro i limiti del consenso [25], utilizzarli per apportare benefici ai suoi membri e ad essa stessa, nel suo complesso. Ad essere condivisa è la possibilità di utilizzo dei dati, non i dati in sé secondo vincoli di carattere reale, e quindi, la cooperativa non è proprietaria dei dati dei suoi membri, ma titolare di una situazione giuridica soggettiva attiva (un diritto) che ne consente l'uso per il tempo stabilito o, comunque, fino alla revoca del consenso da parte dell'interessato.

Dunque, la natura non rivale dei dati – che possono essere trattati simultaneamente da più persone o organizzazioni, anche per finalità differenti, purché determinate, esplicite e legittime –, unitamente al fatto che essi costituiscono attributi della personalità, ne impone, un'esclusione dalle logiche di apprensione di tipo proprietario e dalla possibilità di effettuare scambi, aventi ad oggetto dati, tramite il modello del contratto ad effetti reali.

Al netto di tale puntualizzazione, Driver's Seat si impegna a condividere i dati raccolti e analizzati unicamente con soggetti che condividono i valori della cooperativa e sempre nell'ottica di apportare un beneficio ai singoli autisti. Questi ultimi devono essere i soggetti che ricevono un ritorno capace di stimolarne l'intento di aggregarsi in una struttura organizzativa di tal genere. Agendo in tal senso, e dunque, anche attraverso la condivisione dei dati con terzi, la cooperativa può crescere, affermandosi sul mercato digitale e, allo stesso tempo, creare profitto per i suoi membri.

Nel novero di coloro ai quali i dati collazionati dalla cooperativa possono essere condivisi, sempre in forma pseudonimizzata o anonimizzata, non vi sono unicamente soggetti privati, ma anche pubblici che ricercano dati al fine di utilizzarli per finalità di interesse generale. Tra questi, ad esempio, comuni o, in generale, pubbliche amministrazioni a livello locale che intendano porre in essere opere, relative alle infrastrutture, per migliorare la viabilità; attuare piani di sviluppo del trasporto pubblico; adottare politiche di gestione del traffico (anche) in una prospettiva *green*; e così via. I dati così raccolti dalla PA, in modo, tra l'altro, piuttosto agevole, sono di particolare utilità per poter agire in maniera mirata, realizzando le concrete esigenze della popolazione ed impiegando così il denaro pubblico in modo proficuo ed efficace.

In quest'ottica, le logiche solidaristiche e mutualistiche, proprie della cooperativa di dati, raggiungono il loro apice, potendo esternare un forte impatto non solo per i membri della cooperativa in sé, ma per la società intera. I membri della cooperativa ricevono, quindi, un duplice vantaggio: quello derivante dallo sviluppo della cooperativa, relativo ai benefici che la partecipazione ad essa garantisce loro, ma anche quello inerente alla condivisione, sociale, dei vantaggi che ne derivano per la collettività e, dunque, per i membri della cooperativa in quanto facenti parte di tale collettività.

H. ULLRICH-P. DRAHOS (eds.), *Kritika: Essays on Intellectual Property*, Cheltenham-Northampton, 2018, p. 48 ss.; e B.J. EVANS, *Much Ado About Data Ownership*, in *Harvard J. of Law & Tech*., 2011, 25, p. 78 secondo cui «*different assets call for different forms of ownership*».

[25] Sul sito *web* di Driver's Seat si riporta, infatti, la possibilità di inviare una richiesta di cancellazione dell'*account* che comporta anche la cancellazione di tutti dati raccolti dall'istante, e quindi anche l'interruzione della possibilità di uno sfruttamento di tali dati.

Driver's Seat appare come una cooperativa di dati che si inserisce a pieno titolo nell'architettura delineata dal DGA, unitamente al GDPR, per il mercato digitale. Si propone, infatti, di massimizzare il valore dei dati personali dei propri membri e così anche i loro guadagni, impegnandosi in una gestione etica dei dati, lontana dal modello adottato dalle *Big Tech*, perseguendo (anche) il fine del bene comune. Tutto ciò non deve rivelarsi, però, un mero specchio per le allodole, ma deve caratterizzare l'operato di Driver's Seat, così come delle altre cooperative di dati. È per tale ragione importante garantire controlli continui, da parte della autorità ad essi preposte, affinché dietro allettanti benefici, non si celino abusi.

Ad essere al centro della tutela deve essere la persona con i suoi diritti fondamentali, nelle difficoltà che incontra sul mercato digitale. La sua tutela non può essere obliterata, ma, in un certo qual modo, deve essere flessibilizzata nel quadro delle attuali esigenze imposte dalla *data driven society*. Solo in tal guisa, la persona viene realmente posta, come deve essere, nella gestione dei dati ad essa riferiti, "al posto del guidatore".

3.2. Driver's Seat: non è tutto oro ciò che luccica?

Driver's Seat, quale cooperativa di dati, si prefigge l'obbiettivo di aiutare i *gig workers* nel loro lavoro, massimizzandone i profitti. Un simile fine è tutt'altro che facile da raggiungere se ci confrontiamo con la realtà digitale che conosce un'evoluzione costante ed inarrestabile.

I membri della cooperativa aspirano, infatti, ad un certo grado di prevedibilità dei loro guadagni sulla base delle valutazioni operate dalla cooperativa grazie ai dati raccolti. Attualmente è, però, di particolare difficoltà poter raggiungere un livello di prevedibilità stabile a causa dei costanti cambiamenti che caratterizzano gli algoritmi sempre più demiurgici, il cui sviluppo deve assicurare la trasparenza e la correttezza del loro funzionamento, il rispetto dei diritti fondamentali, superando in tal guisa l'opacità propria del loro apprendimento automatico (c.d. effetto *black box*) [26]. A tal fine, risulta importante garantire un addestramento degli algoritmi basato su campioni rappresentativi di dati immessi nel sistema (*input*) di elevata qualità, perché i dati rappresentano il mezzo attraverso il quale l'algoritmo apprende ed emette un risultato (*output*), unitamente a efficaci controlli sul processo decisionale degli stessi algoritmi.

Sebbene la cooperativa possa fornire utili informazioni agli autisti per organizzare il lavoro e per costruire un piano elaborato su misura, in base alle aspettative di guadagno, essa non è in grado di esercitare un controllo stabile sui processi di automazione che controllano il lavoro dei *drivers* [27].

---

[26] Cfr. F. PASQUALE, *The Black Box Society: The Secret Algorithms That Control Money and Information*, Cambridge (Massachussets)-Londra, 2015; e S. ZUBOFF, *The age of surveillance capitalism: the fight for the future at the new frontier of power*, Londra, 2019.

[27] Tale problematica, propria delle cooperative di dati, viene prospettata da V. DUBAL, *On Algo-*

A ben vedere, i sistemi di intelligenza artificiale, in quanto in costante evoluzione, racchiudono uno straordinario potenziale per prevedere eventuali cambiamenti che possano ripercuotersi sui lavoratori e sui loro guadagni. Si aggiunga che la cooperativa si impone sempre di porre al primo posto il miglioramento delle condizioni dei propri membri e, anche laddove miri ad una propria crescita, essa è sempre funzionale a beneficiare i soci che la compongono. I membri della cooperativa, a differenza di coloro che lavorano per le piattaforme di stampo tradizionale, si trovano, pertanto, nel contesto di una entità che si impegna per il loro bene e che improntera in questa direzione le proprie azioni anche se adattate in base ai cambiamenti delle tecnologie utilizzate. Inoltre, la cooperativa si impegna a garantire la massima trasparenza anche con riguardo agli algoritmi utilizzati [28], rendendone edotti i singoli membri. Le conoscenze sul tema, proprie della cooperativa di dati, sono, con ogni probabilità, ampiamente superiori rispetto a quelle dei soci e verranno utilizzate per garantire le migliori condizioni possibili ai lavoratori.

Un aspetto delicato che appare di maggior rilievo e che può presentare risvolti problematici nell'ambito delle cooperative di dati è quello relativo all'affidamento che le cooperative, talvolta, ripongono in soggetti terzi che svolgono sostanzialmente il ruolo di *data brokers* [29].

Driver's Seat si avvale di Argyle, un fornitore di servizi digitali, che viene utilizzato dalla cooperativa per raccogliere i dati dei propri membri, che vengono messi a disposizione di questi ultimi tramite l'*app* dopo essere stati riorganizzati per ottimizzare i flussi di lavoro della cooperativa. In altri termini, Argyle raccoglie i dati relativi alla storia lavorativa dei *gig worker* sulle varie piattaforme per poi permetterne l'accesso ai suoi clienti come Driver's Seat. Precisamente, l'autista che desidera divenire membro di Driver's Seat è tenuto a scegliere tra l'opzione di *manual tracking* e quella di *automated tracking* [30], con riguardo al tracciamento dei dati (le ore di lavoro effettuate, i luoghi in cui si è lavorato, i pagamenti ricevuti, e così via) funzionali anche alla cooperativa per fornire importanti informazioni statistiche all'autista così da migliorarne il lavoro.

Nel primo caso, il soggetto è tenuto ad inserire manualmente nell'applicazione tutti i dati relativi ai viaggi effettuati e ai guadagni incassati (*work data*) così che possano essere utilizzati, aggregandoli con quelli di altri (auspicabilmente, nume-

---

rithmic Wage Discrimination, cit., p. 50 secondo la quale «*drivers who "figured out" a way to hit their income target for a few months (and came to rely on these techniques) would often be devastated when their knowledge about the system was inevitably upended by changes in the algorithms*» e aggiunge che «*workers cannot know whether the data collected will, at the population level, violate the civil rights of others or amplifies their own social oppression*».

[28] In argomento cfr. S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, Bologna, 1973; ID., *Tecnologie e diritti*, Bologna, 1995; ID., *Controllo e* privacy *della vita quotidiana. Dalla tutela della vita privata alla protezione dei dati personali*, in *Riv. crit. dir. priv*., 2019, 1, p. 9 ss.; ID., *Il mondo della rete. Quali i diritti, quali i vincoli*, Roma-Bari, 2014, spec. p. 33 ss.

[29] Esprime perplessità sul punto V. DUBAL, *On Algorithmic Wage Discrimination*, cit., pp. 50-51.

[30] Scelta esplicitata nella sezione *Terms of Service* del sito *web* di Driver's Seat.

rosi) utenti, per le finalità della cooperativa. Diversamente, nel secondo caso, Driver's Seat si avvale di Argyle che si occuperà di tracciare in modo automatico i *work data* e ritrasferirli all'*app* della cooperativa. L'autista deve creare un profilo con Argyle e collegarlo con quello di cui è già titolare con Driver's Seat, autorizzando così la cooperativa a ricevere le informazioni da Argyle che estrapola, riordina e ricondivide i dati relativi a tutte le *gig platforms* per cui il soggetto presta il proprio lavoro, e quindi a tutti i viaggi già effettuati nel passato o in programma per il futuro. Questo, pur sempre nei limiti dei dati inseriti nei vari profili, relativi all'attività lavorativa, alle informazioni del veicolo e alle valutazioni degli utenti. In tal guisa, viene svolto un compito non semplice, ossia quello di aggregare i dati provenienti da più piattaforme. Tale compito, tuttavia, può risultare particolarmente utile per la cooperativa. Driver's Seat, infatti, potrà utilizzare le informazioni ricevute per aggiornare in modo automatico i dati di lavoro così da permettere agli autisti di monitorare agevolmente il lavoro effettuato e i guadagni in base alle varie piattaforme, attraverso un confronto con le statistiche relative ai colleghi.

Occorre però sottolineare che Argyle è un *data broker* che, a sua volta, agisce sul mercato digitale per ottenere dei guadagni e non per i fini solidaristici propri delle cooperative di dati. Tale compagnia, che afferma di gestire i dati dell'80% dei *gig workers*, è stata segnalata da alcune organizzazioni di sorveglianza per potenziali pratiche di *phishing* in violazione della normativa *anti-hacking* statunitense [31].

Ogniqualvolta una cooperativa di dati si affidi ad un soggetto terzo per erogare il servizio di intermediazione dei dati, si aprono possibili scenari di violazione dei dati degli utenti del servizio, membri della cooperativa. Per tale ragione, si ritiene che l'attenzione alle politiche di sicurezza dei dati debba essere, in simili casi, duplice: indirizzata in primo luogo alla predisposizione di tecniche idonee ad evitare violazioni dei dati all'interno della cooperativa stessa, ma anche riferita alla scelta di soggetti affidabili con cui collaborare, che condividano i valori della cooperativa e si pongano in linea con il quadro delineato a livello europeo in tema di *data governance*. Se, da un determinato punto di vista, la cooperativa di dati viene agevolata dal lavoro effettuato dal *data broker*, su di essa vi è la responsabilità concernente la scelta ed il controllo dei soggetti di cui si avvale. La fiducia che si ingenera nei membri di una cooperativa si fonda anche sulla conoscenza profonda della materia detenuta dalla cooperativa stessa, sull'applicazione delle tecniche migliori per valorizzare al meglio il potenziale dei dati dei lavoratori, eventualmente interfacciandosi con i soggetti più adeguati.

Pare possibile affermare che, altrimenti, la cooperativa potrebbe incorrere in una violazione, seppur indiretta, della normativa *privacy*, secondo le ben note fattispecie della *culpa in eligendo* e della *culpa in vigilando*.

---

[31] Cfr., nell'ambito della *Coworker.org*, W. NEGRÓN, *Little Tech is Coming for Workers. A Framework for Reclaiming and Building Worker Power*, disponibile a *https://home.coworker.org/wp-content/uploads/2021/11/Little-Tech-Is-Coming-for-Workers.pdf*.; e V. DUBAL, *On Algorithmic Wage Discrimination*, cit., p. 51.

4. Il caso Eva Coop.

Nel novero delle cooperative di dati che offrono servizi di *ride hailing* e *food livering*, deve essere ricordata anche Eva Coop [32] che, fondata a Montréal, ha operato fino al 2023 tramite una *app* che funzionava unicamente nelle città in cui era attiva. Si tratta, proprio come nel caso di Driver's Seat, di una cooperativa nata con l'intento di offrire una soluzione alternativa e maggiormente sostenibile rispetto alle grandi piattaforme che offrono servizi analoghi.

Attraverso Eva Coop [33], gli autisti, da un lato, partecipavano attivamente alla gestione dei propri dati sulla base di meccanismi trasparenti e, dall'altro, ottenevano migliori condizioni lavorative rispetto a quelle offerte dalle piattaforme rivali, soprattutto in termini di guadagno. La ferma critica mossa, sin dal principio, dalla cooperativa in esame a piattaforme come Uber e Lyft era quella di aver costruito un sistema di *self-employment* solo fittizio, non potendo i lavoratori controllare, in modo diretto ed effettivo, il loro impiego. Invece, il modello cooperativo, utilizzato da Eva Coop, prende le distanze dalla deriva individualistica ed ha alla base una gestione democratica e paritaria, perpetrata con spirito mutualistico dai membri della cooperativa, a loro vantaggio, permettendo, tra l'altro, una adeguata *governance* relativa ai loro dati. Dunque, ponendo in contatto autisti e passeggeri, si è tentato di delineare una nuova idea di mobilità, più conforme alle odierne esigenze e, come tale, improntata alla sostenibilità, riferibile sia a chi lavora con la cooperativa sia alla società intera. In tal guisa, si era inteso creare un modello di *cooperative ecosystem* democratico ed equo nell'ambito della *gig economy*.

La cooperativa raccoglieva i dati personali degli autisti sulla base del consenso liberamente prestato e, in aggiunta, collazionava altre informazioni in modo automatico quando l'utente si collegava al sito *web*, quali: dati relativi al *log* del *server* ed al *device* utilizzato per collegarsi, metadati sugli *upload* effettuati, informazioni di tracciamento tramite *cookies*. La cooperativa si impegnava ad utilizzare i dati solo per gli obiettivi da essa perseguiti, e sempre nel quadro etico-valoriale posto alla sua base.

La peculiarità di Eva Coop consisteva nel fatto che la relativa piattaforma era basata sulla tecnologia *blockchain*, tramite la quale gli autisti venivano messi in contatto con i clienti, ed i loro dati venivano raccolti e condivisi in modo decentralizzato. Un simile controllo decentralizzato era reso possibile da un *database* condiviso da tutti i

---

[32] Cfr. E. BIETTI-A. ETXEBERRIA-M. MANNAN-J. WONG, *Data Cooperatives in Europe: A Legal and Empirical Investigation*, cit., p. 23; DUNCAN, *Data protection beyond data rights: governing data production through collective intermediaries*, in *Internet pol. rev*., 2023, 3, p. 13; I. CALZADA, *Data Co-Operatives through Data Sovereignty*, in *Smart cities*, 2021, 4, p. 1165; ID., *Postpandemic Technopolitical Democracy: Algorithmic Nations, Data Sovereignty, Digital Rights, and Data Cooperatives*, in J. ZABALO-I. FILIBI-L. ESCAJEDO SAN-EPIFANIO (eds.), *Made-to-Measure Future(s) for Democracy. Views from the Basque Atalaia*, Cham, 2023, p. 111; O. RAFELIS DE BROVES, *Les coopératives au secours des travailleurs de plateforme: quelles innovations contre l'ubérisation?*, in *Canadian J. of Nonprof. and Soc. Econ. Research*, 2022, suppl. 1, p. 92 ss.

[33] V. quanto riportato nel sito *web* di Eva: *https://eva.coop/#/*.

nodi della catena che conteneva dati certi, immutabili, unici e cronologicamente ordinati. In tal guisa, Eva Coop riusciva a garantire una maggior protezione dei dati che venivano condivisi e gestiti secondo logiche cooperative, nonché un'elevata qualità di tali dati. Il metodo adottato dalla cooperativa garantiva che i dati utilizzati venissero anonimizzati per essere poi sfruttati a vantaggio dei vari membri che la componevano, ottenendo informazioni utili per migliorare la loro condizione di lavoro. Ogni membro della cooperativa operava, infatti, come nodo della catena ed era posto a livello paritario con i colleghi, potendo controllare in modo crittografico ogni operazione, senza il coinvolgimento di intermediari. Era, quindi, anche la fiducia dei membri della cooperativa a non essere più trasferita su un soggetto terzo, ma, fondandosi sulla forma più progredita di disintermediazione, veniva riposta sui singoli nodi.

Di più, tramite la *blockchain*, Eva Coop permetteva a soggetti pubblici e privati di accedere facilmente ai dati raccolti sulla mobilità così da poter comprendere le aree dove i servizi di tal genere erano più richiesti, le strade più trafficate in base agli orari, il numero di autisti all'opera, e così via, in modo che le pubbliche amministrazioni potessero attuare le migliori politiche finalizzate al benessere sociale, e le imprese private potessero giovarne per fini di crescita e sviluppo imprenditoriale.

Da quanto affermato, emerge come Eva Coop mirasse a migliorare la vita delle persone attraverso una (nuova forma di) mobilità che fosse veloce, sicura e, soprattutto, sostenibile. Si può notare che il modello cooperativo (*governance structure*) si fondesse con la *blockchain* (*technological structure*) al fine di meglio perseguire gli obiettivi che la cooperativa si proponeva.

Nonostante Eva Coop rappresenti, nell'ambito delle cooperative di dati, un caso che non ha avuto un lungo corso, soprattutto per la mancanza di fondi capaci di sostenerla, appare opportuno sottolineare come l'utilizzo dei dati secondo logiche cooperative possa dar vita a modelli imprenditoriali che, impegnandosi per la crescita dell'economia, delle imprese, delle persone e, più in generale, della comunità e della democrazia, meritano sicuro apprezzamento. È quindi importante incentivare simili formazioni sociali, attraverso un imprescindibile quadro normativo che ne consenta lo sviluppo, garantendo risorse adeguate e promuovendo un clima di fiducia.

Quella intrapresa (anche) da Eva Coop è una strada che, tracciata solo in parte nella prassi, si inserisce a pieno titolo nelle direttrici del neomutualismo digitale che oggi si impone come la scelta migliore per una transizione digitale sostenibile, improntata alla tutela della persona e dei suoi diritti fondamentali, ma, al contempo, indirizzata a valorizzare massimamente le potenzialità dei dati.

5. Riflessioni conclusive.

Il settore della mobilità conosce al giorno d'oggi importanti evoluzioni, determinate dall'uso dei dati e dalle applicazioni dei sistemi di intelligenza artificiale che di tali dati si nutrono. Le modalità utilizzate per gli spostamenti sono destinate, in un futuro sempre più prossimo, a mutare considerevolmente (anche) in

una prospettiva di condivisione dei mezzi di trasporto (intelligenti).

L'impiego dell'IA nell'*automotive* presenta importanti benefici nella riduzione delle esternalità negative dei trasporti, quali la diminuzione del numero degli incidenti stradali e delle emissioni di Co2 nell'ambiente. Tuttavia, simili linee di sviluppo, cui sicuramente si deve mirare, devono necessariamente essere improntate alla sostenibilità e, in questo senso, risulta imprescindibile un adeguato utilizzo della pletora di dati, oggi più che mai necessaria in tale contesto.

In questa direzione pare muoversi il *Data Governance Act* e, segnatamente, il *cooperative model* ivi tratteggiato.

L'analisi delle applicazioni già emerse nella prassi – Driver's Seat ed Eva Coop – mostra come i servizi di cooperative di dati rappresentino uno strumento particolarmente efficace per la valorizzazione dei dati nel settore della mobilità. In quest'ambito, infatti, i dati collazionati dalla cooperativa vengono utilizzati eticamente ed in modo consapevole, da un lato, tutelando massimamente le persone cui i dati si riferiscono, e, dall'altro, promuovendo la crescita e lo sviluppo della cooperativa come pure di imprese private e pubbliche amministrazioni che, nell'ambito del quadro valoriale proprio della cooperativa, possono essere autorizzate all'accesso e all'utilizzo dei dati medesimi.

Il controllo duale sui dati che si determina nell'ambito delle cooperative di dati [34] rappresenta una delle principali caratteristiche di fornitori di servizi di intermediazione dei dati. Il riferimento è alla *governance* collettiva in capo alla società che si affianca alla, inderogabile, *governance* individuale, in capo all'interessato o titolare dei dati. Un tale sistema non è, infatti, volto a privare il *data subject* o il *data holder* del controllo sui dati, ma, al contrario, a potenziare le tutele loro offerte grazie al controllo ulteriore e maggiormente specializzato degli intermediari.

Se, però, il modello delle cooperative appare meritevole di apprezzamento, non deve essere tralasciato il fatto che le cooperative di dati devono, soprattutto, in fase iniziale, poter contare su adeguate risorse sulle quali sostenersi. È proprio il caso Eva Coop a dimostrare la necessità della predisposizione di un quadro di incentivi, volti a sostenere realtà che, come quelle in questione, difficilmente possono sopravvivere altrimenti sul mercato digitale. Va da sé che tali aspetti devono essere oggetto di un puntuale intervento del legislatore.

Dunque, con la consapevolezza di muoversi lungo una strada ancora da definirsi compiutamente, le cooperative di dati appaiono uno strumento capace di fornire un importante contributo all'evoluzione del settore della mobilità. Cogliendo le opportunità determinate dalla circolazione dei dati, si mira a valorizzare appieno tali dati e le loro potenzialità, in una prospettiva di implementazione delle tecnologie nell'*automotive*, di sviluppo imprenditoriale e di promozione del benessere della società complessivamente intesa, sempre nella consapevolezza che la persona umana e la tutela dei suoi diritti fondamentali debba rimanere l'elemento centrale.

---

[34] Tale aspetto viene posto in luce da F. BRAVO, *Le cooperative di dati*, cit., p. 762 ss. e *passim*.

Capitolo XXXII

Le cooperative di dati tra persona e mercato: casi di studio

Marina Federico-Beniamino Parenzo[*]

Abstract: This paper explores the relevance and potential of *data cooperatives*, as provided for by Regulation EU 2022/868 (the so-called *Data Governance Act*). Specifically, it formulates two main case studies where data cooperatives, as data intermediaries, could play a pivotal role in empowering data subjects and enhancing their collective self-determination. The first analysis is devoted to the case of health data, the second one to the right of data portability. Overall, this article aims to suggest data cooperatives as a playground for realizing a new "digital mutualism", promoting a more democratic and participatory model for data governance.

1. Introduzione: dal GDPR al DGA; ovvero, dalla protezione alla condivisione dei dati personali attraverso i «servizi di intermediazione dei dati».

Il Regolamento UE n. 2022/868 (c.d. *Data Governance Act*; in seguito, "DGA") ha segnato, nel panorama eurounitario di regolamentazione della c.d. *digital economy*, un deciso cambio di paradigma rispetto al GDPR [1]. Più precisamente, tale mutamento può sinteticamente descriversi nei termini di un passaggio da un siste-

[*] I paragrafi 1 e 2 sono da attribuire a Beniamino Parenzo, i paragrafi 3 e 4 a Marina Federico.

[1] Anche L. PETRONE, *Il mercato digitale europeo e le cooperative di dati*, in *Contratto e impresa*, 2023, 3, p. 803, rileva che il DGA «sembrerebbe porsi, almeno nelle intenzioni, in rapporto di discontinuità rispetto al panorama legislativo europeo in materia di protezione dati».

ma di *protezione* ad un quadro normativo per la *condivisione* dei dati personali.

Invero, già nel sistema del GDPR, come noto, la prospettiva non è affatto quella di una tutela "assolutistica" del dato personale (cfr. considerando 4, GDPR), "schermato" da qualsivoglia forma di interferenza esterna. Tutt'al contrario, *fin dal GDPR* (e, prima ancora, fin dalla Direttiva 95/46/CE), la protezione dei dati personali, lungi dal risolversi nella garanzia di una "chiusura" nella sfera del soggetto interessato, è chiamata a conciliarsi, ad essere posta in bilanciato contemperamento, con istanze del mercato che invece ne esigono la circolazione, istanze di fronte alle quali quella esigenza di protezione si esprime nella garanzia in capo all'interessato di un controllo sulla circolazione medesima, non nella inibizione di essa [2]: protezione e circolazione dei dati personali si svolgono, dunque, nell'impianto regolamentare, in un reciproco rapporto che è costruito all'insegna di un generale principio per cui la prima *non nega*, bensì *conforma* la seconda.

Se è, allora, senz'altro vero che la disciplina approntata dal GDPR si erge sulle fondamenta di un quadro assiologico che vede la garanzia di un «elevato livello di protezione dei dati personali» come valore co-essenziale all'esigenza di facilitare «ancora di più la [loro] libera circolazione» (cfr. considerando 6, GDPR), ebbene la disciplina predisposta dal DGA ne rappresenta una tanto "accelerata evoluzione" da potersi descrivere, come si diceva, nei termini di un vero e proprio mutamento di paradigma: da una protezione conformativa della circolazione, il focus del regolatore eurounionale si rivolge ora alla definizione di un quadro di *governance* per il *riutilizzo* e la *condivisione* dei dati (non solo) personali; là dove il GDPR guarda al rapporto tra titolare e interessato, l'uno portatore di un qualificato interesse a trattare i dati personali dell'altro, l'altro tutelato nell'interesse ad un controllo sul trattamento svolto dal primo, il DGA supera i confini di tale rapporto e apre il regolatorio angolo visuale alla *ulteriore* messa in circolo dei dati. Disciplinati dal GDPR gli obblighi che conformano l'attività di trattamento svolta dal titolare e i diritti che nei confronti di questo vanta l'interessato, il DGA trascende tale "individuale spazio", lo spazio di tale "relazione" tra i soggetti protagonisti del trattamento, per volgere invece il proprio sguardo ordinatore ai (nuovi) soggetti protagonisti del riutilizzo e della condivisione dei dati personali.

Ancora, se nell'ambito del GDPR la prospettiva è quella del rapporto "interessato-titolare del trattamento", la prospettiva del DGA e, in particolare, della disciplina che qui specialmente interessa sui servizi di intermediazione, è invece quella del *rapporto trilatero* che vede un soggetto (il quale, peraltro, non per forza coincide con l'"interessato" ai sensi del GDPR, potendo altresì qualificarsi come un "titolare dei dati" [3]) condividere dati, a titolo gratuito o a titolo oneroso (cfr. art. 2, n. 10,

---

[2] Emblematico in questo senso l'art. 1, par. 3, GDPR, ai sensi del quale «la libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali».

[3] Il quale per definizione non coincide con l'interessato, qualificandosi come tale, ai sensi dell'art. 2, n. 8, DGA, «una persona giuridica, compresi gli enti pubblici e le organizzazioni internazionali, o una

DGA)[4], con soggetti terzi (i cc.dd. "utenti dei dati"[5]) attraverso un "mediatore", il fornitore di "servizi di intermediazione dei dati"[6], che, analogamente al servizio svolto dalla tradizionale figura codicistica di cui all'art. 1754 ss. c.c., mette il primo in relazione con i secondi.

Tre sono, segnatamente, le tipologie di servizi di intermediazione assoggettati alla disciplina predisposta dal DGA (la quale disciplina, in estrema sintesi, consiste: *i*) in un obbligo di notifica alla competente autorità nazionale prima dell'inizio dell'attività – cfr. artt. 11 e 13, DGA; *ii*) nell'obbligo di rispetto delle condizioni previste dall'art. 12 DGA – la cui *ratio* può in definitiva individuarsi nella volontà di «garantire il ruolo neutrale degli intermediari rispetto ai dati scambiati»[7]; *iii*) nella previsione, ai sensi dell'art. 14 DGA, di un potere in capo alla competente autorità nazionale di monitoraggio e controllo della conformità dei servizi di intermediazione a quelle condizioni medesime): «*a)* servizi di intermediazione tra i titolari

---

persona fisica *che non è l'interessato* rispetto agli specifici dati in questione e che, conformemente al diritto dell'Unione o nazionale applicabile, ha il diritto di concedere l'accesso a determinati dati personali». Preoccupata perplessità esprime, peraltro, F. BRAVO, *Intermediazione di dati personali e servizi di* data sharing *dal GDPR al* Data Governance Act, in *Contratto e impresa. Europa*, 2021, 1, p. 203, rispetto a una simile qualificazione, rilevando come «fino ad ora l'UE aveva sempre rifiutato di introdurre il concetto di "*titolarità*" direttamente riferita ai *dati*: non era considerato "*titolare dei dati*" né il soggetto a cui si riferisce il dato personale, indicato come "*interessato al trattamento di dati personali*" […], né il soggetto che predispone il trattamento dei dati personali per finalità legittime dal medesimo stabilite, indicato come "*titolare del trattamento dei dati*". Mai fino ad ora s'è voluto riferire il concetto di "titolarità" direttamente al dato (e non al trattamento) e ciò denota un cambio di paradigma che rischia di essere un preludio all'introduzione, per via normativa, di una reificazione dei dati personali» (enfasi nel testo).

[4] Si coglie l'occasione per rilevare qui, in nota: alla luce della espressa possibilità di una condivisione onerosa dei dati personali, sono inesorabilmente destinate a cadere anche le ultime resistenze della dottrina più tradizionale a negarne (come attributi della persona, oggetto di un diritto fondamentale) la natura (altresì) patrimoniale e, quindi, la possibilità di una circolazione attraverso lo strumento del contratto. Nell'amplissima letteratura sul punto, si rinvia, su tutti, al contributo monografico di V. RICCIUTO, *L'equivoco della privacy. Persona* vs *dato personale*, Napoli, 2022.

[5] Utente dei dati qualificandosi, ai sensi dell'art. 2, n. 9, DGA, «una persona fisica o giuridica che ha accesso legittimo a determinati dati personali o non personali e che ha diritto, anche a norma del regolamento (UE) 2016/679 in caso di dati personali, a utilizzare tali dati a fini commerciali o non commerciali»; peraltro, come pure rileva F. BRAVO, *Intermediazione di dati personali e servizi di* data sharing *dal GDPR al* Data Governance Act, cit., p. 240, «se usassimo il lessico del GDPR […] l'"utente dei dati" personali altri non è che il titolare del trattamento».

[6] Definito dall'art. 2, n. 11, DGA, appunto, «un servizio che mira a instaurare, attraverso strumenti tecnici, giuridici o di altro tipo, rapporti commerciali ai fini della condivisione dei dati tra un numero indeterminato di interessati e di titolari dei dati, da un lato, e gli utenti dei dati, dall'altro». La letteratura che si è ad oggi occupata dei cc.dd. "intermediari dei dati" non è amplissima: si vedano, in particolare, oltre ai contributi già sopra citati, anche D. POLETTI, *Gli intermediari dei dati*, in *European Journal of Privacy Law and Technologies*, 2022, 1, pp. 45-56; G. RESTA, *La regolazione digitale nell'Unione europea – pubblico, privato, collettivo nel sistema europeo di governo dei dati*, in G. RESTA-V. ZENO-ZENCOVICH (a cura di), *Governance of/through big data*, Roma, 2023, p. 614 ss. e F. BRAVO, *Le cooperative di dati*, in *Contratto e impresa*, 2023, 3, p. 757 ss.

[7] D. POLETTI, *Gli intermediari dei dati*, cit., p. 51.

dei dati e i potenziali utenti dei dati […]; *b)* servizi di intermediazione tra interessati che intendono mettere a disposizione i propri dati personali o persone fisiche che intendono mettere a disposizione dati non personali e potenziali utenti dei dati, compresa la messa a disposizione di mezzi tecnici o di altro tipo per consentire tali servizi, permettendo in particolare l'esercizio dei diritti degli interessati di cui al regolamento (UE) 2016/679; c) servizi di cooperative di dati» (cfr. art. 10 DGA).

L'attenzione sarà focalizzata specialmente sul terzo tipo di servizi di intermediazione. Più in particolare, attraverso l'analisi di due esemplificativamente paradigmatici "casi di studio", rispettivamente in tema di circolazione dei dati sanitari e di diritto alla portabilità, si cercherà di mettere in rilievo come il servizio in parola, attuando un modello di «*governance* duale» [8] sui dati personali capace di affiancare al controllo individuale garantito dal GDPR una "struttura" che ne promuove la più efficiente gestione "collettiva", possa costituire un modello ottimale di *empowerment* dell'interessato, preferibile per ciò non solo all'altra tipologia di servizio di intermediazione tra interessati e utenti dei dati di cui all'art. 10, lett. b), DGA, ma altresì a quell'"alternativo" modello di circolazione pure disciplinato nell'ambito dello stesso Regolamento che è il c.d. «altruismo dei dati».

2. La circolazione dei dati sanitari tra "altruismo dei dati" e cooperative di dati.

I dati sanitari [9] costituiscono senz'altro una "particolare" categoria di dati personali. Ciò si ritiene di poter affermare non solo in luce del fatto che così essi sono formalmente qualificati sul piano normativo ai sensi dell'art. 9, GDPR (da cui consegue l'applicazione del peculiare regime appunto previsto per il «trattamento di categorie *particolari* di dati personali») [10], ma anche in virtù della evidentemente accentuata fattuale "tensione intrinseca" che essi esprimono (più di altre "categorie di dati") tra "esigenze di chiusura ed esigenze di apertura", ovvero tra l'interesse, dall'un lato, della persona cui si riferiscono a mantenere riservate le "sensibili" informazioni da essi inferibili e l'interesse, dall'altro lato, latamente "sociale" al più ampio utilizzo (e ri-utilizzo) dei medesimi per finalità di ricerca [11].

---

[8] Cfr. F. BRAVO, *Le cooperative di dati*, cit., pp. 762 e 785.

[9] O, più precisamente, secondo la locuzione di cui all'art. 2, n. 15, GDPR, «dati relativi alla salute», ovvero «i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute».

[10] Cfr., tra gli altri, i lavori monografici di M. CIANCIMINO, *Protezione e controllo dei dati in àmbito sanitario e intelligenza artificiale*, Napoli, 2020 e di P. AURUCCI, *Il trattamento dei dati personali nella ricerca biomedica. Problematiche etico-giuridiche*, Napoli, 2022, p. 129 ss., nonché i contributi del volume collettaneo a cura di A. THIENE-S. CORSO (a cura di), *La protezione dei dati sanitari. Privacy e innovazione tecnologica tra salute pubblica e diritto alla riservatezza*, Napoli, 2023.

[11] Sul trattamento di dati personali per finalità di ricerca scientifica, cfr., tra gli altri, A. BERNES,

Ora, non volendo essere questa la sede per una puntuale ricostruzione del bilanciamento realizzato dallo stesso GDPR (e dal legislatore nazionale, in attuazione del rinvio operato dall'art. 9, par. 4, GDPR) tra tali (potenzialmente) conflittuali esigenze, ma volendo qui piuttosto diversamente concentrare l'attenzione sul già richiamato versante del sistema normativo di circolazione approntato dal DGA [12], si cercherà immediatamente di mettere in evidenza come, rispetto alle due "modalità" da quest'ultimo previste per la volontaria, consensuale, condivisione dei dati personali, ovvero l'altruismo dei dati e il servizio di intermediazione dei dati (in particolare, *sub specie* cooperativa di dati), là dove il primo risulti più tendente a favorire quella "socialmente funzionale" apertura di cui si è appena sopra detto, il secondo sia invece più marcatamente rivolto ad un maggiore ed effettivo *empowerment* dell'interessato.

Definito l'«altruismo dei dati» dall'art. 2, n. 16, DGA, come «la condivisione volontaria di dati sulla base del consenso accordato dagli interessati al trattamento dei dati personali che li riguardano, […], senza la richiesta o la ricezione di un compenso che vada oltre la compensazione dei costi sostenuti per mettere a disposizione i propri dati, per obiettivi di interesse generale, stabiliti nel diritto nazionale, ove applicabile, quali l'assistenza sanitaria, la lotta ai cambiamenti climatici, il miglioramento della mobilità, l'agevolazione dell'elaborazione, della produzione e della divulgazione di statistiche ufficiali, il miglioramento della fornitura dei servizi pubblici, l'elaborazione delle politiche pubbliche o la ricerca scientifica nell'interesse generale», esso parrebbe costituire la modalità, per così dire, "naturale", "fisiologica", di condivisione dei dati sanitari: una solidale "donazione" di dati "sensibili" per contribuire alla realizzazione di obiettivi di interesse generale quali, tra gli altri, l'assistenza sanitaria e la ricerca scientifica.

La disciplina di dettaglio presenta, nei suoi snodi essenziali, struttura analoga a quella sopra succintamente riportata con riferimento ai servizi di intermediazione: *i*) in luogo della (mera) notifica all'autorità competente, è sancito per gli enti che intendano svolgere attività di altruismo dei dati un onere di registrazione presso il «registro pubblico nazionale delle organizzazioni per l'altruismo dei dati riconosciute» (cfr. artt. 17 ss. DGA), subordinata all'accertamento dei requisiti previsti dall'art. 18 DGA (tra cui, si richiede che l'organizzazione in parola sia una persona giuridica senza scopo di lucro); *ii*) l'attività svolta deve essere informata ad una serie di obblighi di trasparenza, che si concretano nella tenuta di registri e nell'invio di una relazione annuale all'autorità competente sulle attività svolte (cfr. art. 20 DGA), nonché ad una serie di obblighi specifici nei confronti dell'interessato (cfr. art. 21 DGA), sui quali si tornerà subito un poco più puntualmente; *iii*) è previsto da parte di un'autorità competente il monitoraggio e controllo della conformità alle

La protezione dei dati personali nell'attività di ricerca scientifica, in *Le nuove leggi civili commentate*, 2020, 1, pp. 175-205.

[12] Non mancando, peraltro, di segnalare, seppur in nota, la centralità che sul punto sarà destinata ad avere, se dovesse vedere la luce, la proposta di Regolamento sullo Spazio Europeo dei Dati Sanitari emanata dalla Commissione il 3 maggio 2022.

prescrizioni stabilite dal DGA medesimo (cfr. art. 24 DGA).

Che il modello circolatorio in parola sia, come poco sopra accennato, più "sbilanciato" a favorire una maggiore condivisione dei dati rispetto a uno "stretto controllo" su di essi da parte dell'interessato, con una conseguente accentuata "attenzione" ai terzi utenti che non a quest'ultimo (il che, peraltro, risulta affatto incoerente, ed anzi in linea, con il *carattere solidale* della condivisione stessa), [13] emerge con tutta evidenza dalla menzionata disposizione di cui all'art. 21 DGA.

In primo luogo, indicativa è, infatti, la previsione secondo la quale l'organizzazione per l'altruismo dei dati «*fornisce strumenti per ottenere il consenso degli interessati*» (art. 21, par. 3, DGA): sancito un generale divieto di ricorso «a pratiche commerciali ingannevoli per sollecitare la fornitura di dati» (art. 21, par. 2, DGA), l'organizzazione per l'altruismo dei dati si pone *ex latere* utente dei dati quale ("meno che neutro") intermediario, risultando la sua attività, tra l'altro, volta ad «*agevola[re]* il trattamento dei dati da parte dei terzi», dovendo essa, appunto, adoperarsi per fornire a questi "gli strumenti" per ottenere il consenso degli interessati (v. art. 21, par. 6, DGA).

Altresì emblematica, in secondo luogo, la previsione che pone in capo all'organizzazione per l'altruismo dei dati l'obbligo «di informare in maniera chiara e facilmente comprensibile gli interessati o i titolari dei dati, prima di qualsiasi trattamento dei loro dati, in merito […] agli obiettivi di interesse generale e, *se opportuno*, alla finalità determinata, esplicita e legittima per cui i dati devono essere trattati, e per i quali acconsentono al trattamento dei loro dati da parte di un utente dei dati» (così l'art. 21, par. 1, lett. a), DGA): salva la necessità di una più ampia riflessione in merito alla compatibilità di tale disposizione con le norme di cui all'art. 5, par. 1, lett. b), GDPR e all'art. 13, par. 1, lett. c), GDPR (ai sensi delle quali, si rammenta, l'interessato deve essere invece puntualmente informato delle esplicite, determinate e legittime finalità del trattamento), l'obbligo informativo sancito dalla disposizione in esame parrebbe, *nel suo contenuto minimo*, limitarsi ai soli "obiettivi di interesse generale" per i quali i dati vengono condivisi, riguardando solo *eventualmente*, «*se opportuno*», anche le specifiche finalità del trattamento. In via volutamente provocatoria, potrebbe azzardarsi ad affermare che, nella misura in cui le finalità del trattamento possano non esser rese note all'interessato (ammesso che così possa effetti-

[13] Se, come autorevolmente ed efficacemente affermato, nella sua eterogenea multiformità, «solidarietà evoca il sentimento altruistico della *pietà* per coloro che si trovano in una situazione deteriore dovuta a povertà, malattie, anzianità e allo status in genere; solidarietà è sinonimo di generosità e di aiuto economico, di *carità* per coloro che soffrono e sono nell'indigenza; la solidarietà è un sentimento di cameratismo e di *colleganza*, nei gruppi, nelle associazioni, nelle confraternite e nelle categorie economiche; la solidarietà è *vincolo* di classe; solidarietà significa *cooperazione* all'interno dei gruppi, tra lavoratori e datori di lavoro, e sul piano internazionale tra gli Stati; la solidarietà è *alleanza* tra le generazioni; la solidarietà è cobelligeranza e *sostegno* economico e militare tra Stati» (così G. ALPA, *Solidarietà. Un principio normativo*, Bologna, 2022, p. 55, enfasi nel testo); ebbene, i tratti in essenza identificativi del concetto possono essere, forse, rinvenuti nella *consapevole appartenenza a una comunità* e nella conseguente *"tensione" altruistica verso i terzi* che di quella stessa (più o meno ampia) comunità fanno parte, nonché nel *disinteressato slancio* ad adoperarsi per la realizzazione dell'interesse altrui.

vamente essere, attesa la rilevata difficile compatibilità con le richiamate disposizioni del GDPR), la solidale condivisione nella cornice dell'altruismo dei dati potrebbe risolversi in una sorta di "delega in bianco" al trattamento.

Infine, in terzo luogo, pure indicativo è il fatto che, se dall'un lato l'art. 21, par. 3, DGA, sancisce l'obbligo per l'organizzazione per l'altruismo dei dati di fornire «strumenti per l'agevole revoca» del consenso, null'altro viene, d'altra parte previsto: nessun accenno, in particolare, viene fatto all'esercizio dei diritti attribuiti all'interessato dal GDPR e, quindi, ad un obbligo in capo all'organizzazione per l'altruismo dei dati di approntare gli strumenti utili per agevolarne l'esercizio.

Affatto differente risulta il modello approntato dalla disciplina sui servizi di intermediazione e, in particolare, sulle cooperative di dati.

Là dove, in via generale, *per tutti* i servizi di intermediazione «che offrono servizi agli interessati», è fatto espresso obbligo al fornitore del servizio medesimo di agire «*nell'interesse superiore* di questi ultimi nel *facilitare l'esercizio dei loro diritti*, in particolare informandoli e, se opportuno, fornendo loro consulenza in maniera concisa, trasparente, intelligibile e facilmente accessibile sugli utilizzi previsti dei dati da parte degli utenti dei dati e sui termini e le condizioni standard cui sono subordinati tali utilizzi, prima che gli interessati diano il loro consenso» (cfr. art. 12, lett. m), DGA); per quanto riguarda in via particolare le cooperative di dati, queste appaiono «per vocazione»[14] i servizi che meglio di ogni altro riescono a declinare, nella propria struttura "partecipata", il perseguimento di quel "superiore interesse" degli interessati[15].

Come, infatti, può ricavarsi dalla definizione consegnata dall'art. 2, n. 15, DGA: *i*) le cooperative di dati costituiscono «strutture organizzative» (non meglio definite sul piano della loro natura giuridica – volutamente, peraltro, deve ritenersi, per favorire una maggiore "elasticità applicativa" all'istituto) *di cui fanno parte gli stessi interessati*; *ii*) e che hanno «come obiettivi principali quelli di aiutare i propri membri nell'esercizio dei loro diritti in relazione a determinati dati, anche per quanto riguarda il compiere scelte informate prima di acconsentire al trattamento dei dati, di procedere a uno scambio di opinioni sulle finalità e sulle condizioni del trattamento dei dati che rappresenterebbero al meglio gli interessi dei propri membri in relazione ai loro dati, o di negoziare i termini e le condizioni per il trattamento dei dati per conto dei membri […] prima che essi diano il loro consenso al trattamento dei dati personali».

Si tratta, in altri termini, di un servizio di intermediazione decisamente *sui generis* rispetto alle altre due tipologie di servizi previste dall'art. 10 DGA; un servizio che, affatto "neutro" nella sua stessa struttura costitutiva, ed anzi istituzionalmente "di parte", ha come proprio oggetto sociale precisamente quello – tipico di qualsiasi "organizzazione associativa" (volendo usare una formula tanto generica quanto

[14] F. BRAVO, *Le cooperative di dati*, cit., p. 784.

[15] «la cooperativa, strutturalmente, prevede un'operatività di impresa nell'interesse dei propri soci e una struttura democratica volta a favorire la discussione, il confronto e l'adozione delle decisioni da parte dei soci»; così F. BRAVO, *Le cooperative di dati*, cit., p. 783.

quella utilizzata dal legislatore europeo) a finalità mutualistica – di «aiutare i propri membri» nel compiere delle informate e consapevoli scelte rispetto alla circolazione dei propri dati personali e (per l'ipotesi di una circolazione a titolo oneroso) nella negoziazione con i terzi di migliori condizioni contrattuali. Senz'altro possibile, poi, deve altresì ritenersi la possibilità per l'interessato di delegare alla cooperativa di dati l'esercizio, *nel suo migliore interesse*, e comunque sempre nel dialettico e partecipato confronto attraverso il quale tipicamente si svolge la formazione della volontà collettiva dell'ente, i diritti che gli sono individualmente attribuiti dal GDPR, così come, tra l'altro, inferibile dalle vicende che hanno interessato la stesura del considerando 31, DGA, il quale, nella sua versione finale, non presenta più una specifica preclusione in tal senso [16].

Bene può, allora, senza retorica alcuna, farsi ricorso ad un alquanto scontato e tuttavia, in questo caso, indubbiamente centrato *slogan*: nella cooperativa di dati, "*l'unione fa la forza*".

Là dove, in altre parole ancora, infatti, nel caso dell'altruismo dei dati la condizione dell'interessato (al netto di quanto sopra riferito) non è invero differente da quella, per così dire, "standard", che gli è consegnata dal GDPR, per cui, pur titolare di una serie di diritti che vorrebbero garantirgli il controllo sulla circolazione dei suoi dati, l'effettività di quel medesimo controllo rischia di essere fattualmente compromessa dalle difficoltà che egli può incontrare nel loro esercizio [17]; diversamente, nel caso della cooperativa di dati, precisamente il fatto che la messa in circolazione ed il successivo controllo si svolgano per il tramite di una "struttura collettiva" che, nel dialettico confronto sociale, lo aiuta a comprendere finalità e condizioni del trattamento e che *per lui*, *nel suo migliore interesse*, negozia con i terzi i termini del trattamento ed esercita i diritti che gli garantiscono quel controllo, l'interessato è messo nelle effettive condizioni di fattualmente essere consapevole parte attiva dei processi che interessano la circolazione dei suoi dati.

Ancora e in sintesi, là dove l'interessato è, nel sistema del GDPR – applicabile ai meccanismi circolatori dell'altruismo dei dati – in definitiva "solo" nel momento in cui acconsente a un trattamento come in quello successivo in cui vuole esercitare i diritti che gli dovrebbero garantire un controllo sulla circolazione, nel sistema

---

[16] Cfr. F. BRAVO, *Le cooperative di dati*, cit., p. 791 ss., il quale ben rileva come, peraltro, una simile preclusione si sarebbe posta in distonia con le indicazioni ricavabili dal generale sistema regolatorio della circolazione dei dati personali, che invero una simile possibilità di delega non pare affatto vietare.

[17] Bene spiega A. BERNES, *Enhancing Transparency of Data Processing and Data Subject's Rights Through Technical Tools: The PIMS and PDS Solution*, in R. SENIGAGLIA-C. IRTI-A. BERNES (eds.), *Privacy and Data Protection in Software Services*, Singapore, 2022, pp. 199-200, «*even if data subject's rights have been boosted under the GDPR, the requests of access to data, to obtain copies, and to erase certain information (if they are aware of it), which are submitted to the data controllers, still remain slow and cumbersome. Individuals are less convinced to act, since sending just a single email seems, paradoxically, detrimental. What is missing here is not the development, but rather the rapid adoption of technical tools, which could permit, in a simple and clear manner, to increase user awareness over data flow across the digital world*».

cooperativo egli trova rinnovata forza appunto nella struttura collettiva, *per il cui tramite* riesce a farsi effettivo interlocutore di processi circolatori diversamente destinati a rimanergli opachi ed "estranei".

Tutto questo, naturalmente, senza mai perdere la possibilità di individualmente determinarsi rispetto al trattamento e individualmente esercitare i propri diritti, la dimensione collettiva mai risolventesi in una negazione o "sopraffazione" di quella individuale, ma anzi al contrario costituendone "amplificazione", "potenziamento".

In conclusione, per quanto specialmente attiene alla circolazione di quella particolare categoria di dati costituita dai dati sanitari, se ad un intuitivo sguardo di primo acchito l'altruismo dei dati potrebbe apparire come il "naturale", "fisiologico", modello entro il quale inquadrarne la circolazione, proprio in luce della loro stretta inerenza alla persona, della loro particolare, accentuata, "sensibilità", diversamente, ad uno sguardo un poco più approfondito, il partecipato modello rappresentato dalla cooperativa di dati deve ritenersi, per le ragioni di cui si è detto, senz'altro preferibile.

3. Cooperative di dati e mercato: l'esercizio del diritto alla portabilità delle informazioni personali.

Tra le dichiarate finalità del *Data Governance Act* vi è quella di promuovere la libera concorrenza e l'accesso ai mercati digitali. L'atto normativo consente di cogliere in maniera evidente il legame tra la circolazione dei dati, personali e non, ed il funzionamento del nuovo modello di mercato *data driven*, basato soprattutto sulla fornitura di servizi digitali forniti a seguito della messa a disposizione dei dati personali dei consumatori (cfr. considerando 67; art. 3, par. 1, Dir. UE 2019/770). Già qualche anno prima del DGA, la Dir. UE 2019/770, parte del c.d. *New Deal for Consumers Package* [18], ha reso normativamente evidente il valore patrimoniale dei dati personali, cristallizzando ciò che già emergeva dalla realtà fattuale, prevedendo espressamente l'applicazione dei rimedi contrattuali ai nuovi modelli di fornitura di servizi condizionati alla messa a disposizione del godimento dei dati da parte del consumatore [19].

Il Regolamento UE 2022/868, però, non si limita a prendere atto delle caratteristiche della *data-driven economy* cercando di regolarla, ma si propone, in maniera più ambiziosa, di cambiarla. È forse questo l'elemento più pregevole del DGA. In altre

[18] Su cui si rinvia a M. GROCHOWSKI, *European consumer law after the New Deal: a tryptich*, in *Yearbook of European Law*, 2020, 39, p. 389 ss.

[19] Ci si riferisce alla Direttiva europea 2019/770 del Parlamento europeo e del Consiglio del 20 maggio 2019 relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali, su cui, *ex multis*, si rinvia a C. CAMARDI, *Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione di dati personali*, in *Giust. civ.,* 2019, 3, p. 510 ss.; A. ADDANTE, *La circolazione negoziale dei dati personali nei contratti di fornitura di contenuti e servizi digitali*, *ivi*, 2020, 4, pp. 889 ss.

parole, il DGA intende favorire la circolazione e il trattamento dei dati stessi, ma senza rinunciare alla tutela della dignità della persona e dei consumatori, in quanto interesse generale della società. Da un lato, quindi, la circolazione dei dati viene incentivata soprattutto poiché motore propulsivo dell'innovazione e del progresso, anche scientifico, per il bene comune; dall'altro, il DGA certifica il passaggio ad una *data sovereignty*, una sovranità sui dati, non più individuale, bensì collettiva [20].

Lo sguardo del legislatore non si sofferma esclusivamente sul mercato unico digitale (come nel *Digital Markets Act*) e sugli interessi dei consumatori, ma si estende anche al settore pubblico ed a tutti gli utenti della rete. Al tempo stesso, le disposizioni normative non si concentrano tanto e soltanto sul tipo di dati (personali e non) che vengono trattati, quanto piuttosto sulle loro modalità di impiego [21].

Come è già stato evidenziato, le cooperative di dati, cui è dedicata la presente analisi, sono servizi di intermediazione di dati destinati ad avere un ruolo fondamentale nel sistema del "neomutalismo digitale" promosso dal DGA [22]. Il nuovo spazio europeo dei dati dovrebbe, idealmente, basarsi su una *governance* diffusa e partecipata, in grado di esaltare il valore collettivo dei dati, tenendo conto anche degli interessi delle generazioni future, e proprio le cooperative, insieme agli altri servizi di intermediazione dei dati, dovrebbero sostenere questo sistema [23].

Un modo per ottemperare a tale compito è quello di veicolare i "diritti degli interessati" [24]. I diritti previsti al Capo III dal GDPR possono, infatti, essere apprezzati anche nella loro dimensione di gruppo, che ben si coglie quando un intermediario si fa portavoce della pluralità dei soggetti interessati e delle loro esigenze. D'altra parte, non è difficile immaginare un certo numero di interessati azionare in via collettiva il diritto all'oblio, all'accesso, alla cancellazione o alla rettifica delle informazioni, nonché quello di opporsi ad eventuali trattamenti automatizzati che li riguardano, e che incidano sui loro diritti fondamentali, attraverso tecniche di profilazione. Come sottolineato dalla Commissione europea, «le persone fisiche si avvalgono sempre più di tali diritti, tuttavia è necessario facilitarne l'esercizio e la

---

[20] E. BIETTI-A. EXTEBERRIA-M. MANNAN-J. WONG, *Data Cooperatives in Europe: A Legal and Empirical Investigation*, 2021, p. 9, disponibile su: https://cyber.harvard.edu/sites/default/files/2022-02/Data_Cooperatives_Europe-group2.pdf.

[21] Alcuni Autori statunitensi si sono espressi, negli ultimi anni, a favore di un simile approccio; in particolare, si rinvia a D.J. SOLOVE, *Data Is What Data Does: Regulating Based on Harm and Risk Instead of Sensitive Data*, in *Northwestern Univ. Law Rev*., 118, 2024, p. 1081 ss. Già di questo avviso, E. NISSENBAUM, *Privacy as Contextual Integrity*, in *Washington Law Rev*., 2004, 79, p. 119 ss.

[22] P. VENTURI-F. ZANDONAI, *Neomutualismo. Ridisegnare dal basso competitività e welfare*, Milano, 2022; LEGACOOP-FONDAZIONE PICO (a cura di), *Le cooperative e la sfida all'innovazione digitale: il neomutualismo in 10 tesi* ["Manifesto" sul neomutualismo digitale di Legacoop e Fondazione PICO].

[23] LEGACOOP-FONDAZIONE PICO (a cura di), *Le cooperative e la sfida all'innovazione digitale: il neomutalismo in 10 tesi*, cit., p. 4 ss.

[24] V. F. BRAVO, *Le cooperative di dati*, cit., p. 791 ss.

piena applicazione»[25] e, con la collaborazione dei c.d. *data intermediaries*, questa potrebbe, effettivamente, risultare più immediata.

Tra i diritti degli interessati, il diritto alla portabilità (art. 20 GDPR) è espressione evidente del valore anche patrimoniale delle informazioni personali. È ormai acclarato che non è tanto il singolo dato dell'individuo consumatore ad avere valore per le imprese; piuttosto, è l'insieme di dati relativi a più soggetti possibili che, aggregati ed analizzati dai *softwares* di *big data analytics*, consente di effettuare delle analisi predittive comportamentali e di mercato che permettono alle imprese di orientare la loro condotta per ricavare maggior profitto[26].

Tra i servizi di intermediazione, il DGA annovera all'art. 10, alla lett. b), i «servizi di intermediazione tra interessati che intendono mettere a disposizione i propri dati personali o persone fisiche che intendono mettere a disposizione dati non personali e potenziali utenti dei dati, compresa la messa a disposizione di mezzi tecnici o di altro tipo per consentire tali servizi, permettendo in particolare l'esercizio dei diritti degli interessati di cui al regolamento (UE) 2016/679» ed alla lett. c) le «cooperative di dati», di cui non vengono precisate funzioni e caratteristiche, ma che, come anticipato, tra le loro attività, comprendono quella di «negoziare le condizioni di uso dei dati» degli interessati[27]. Rimane fermo che gli interessati non possono, in ogni caso, rinunciare ai loro diritti; pertanto, deve ritenersi preclusa agli intermediari la facoltà di effettuare rinunce o transazioni per loro conto, in assenza di un rapporto di mandato e di specifica delega.

Lo schema predisposto dal DGA sembra idealmente completare quanto previsto già all'art. 80 nel GDPR, dedicato alla rappresentanza degli interessati, che consente a determinati enti, dotati delle caratteristiche definite dalla legge, di rappresentare gli interessati, con o senza mandato, in sede giudiziale, esercitando per loro conto il diritto ad ottenere il risarcimento di un eventuale danno subito e di proporre un ricorso giurisdizionale[28].

---

[25] COMMISSIONE EUROPEA, Comunicazione al Parlamento Europeo e al Consiglio, COM(2020)264, *La protezione dei dati come pilastro dell'autonomia dei cittadini e dell'approccio dell'UE alla transizione digitale: due anni di applicazione del regolamento generale sulla protezione dei dati*, p. 8 ss.

[26] Cfr. G. FERRARI-M. MAGGIOLINO, *GAFAM's power across markets: how should we deal with it?*, in G. RESTA-V. ZENO-ZENCOVICH (a cura di), *Governance of/through big data*, cit., p. 389 ss.

[27] Su cui si rinvia anche all'analisi effettuata dal gruppo di ricerca CiTiP della Facoltà di Giurisprudenza dell'Università Cattolica di Leuven, a cura di J. BALOUP-E. BAYAMLIOĞLU-A. BENMAYOR-C. DUCUING-L. DUTKIEWICZ-T. LALOVA-Y. MIADZVETSKAYA-B. PEETERS, *White paper on the Data Governance Act*, in *Working paper series*, 2021, p. 27 ss.

[28] Sull'art. 80 del GDPR, si rinvia a G. VERSACI, *Trattamenti illeciti dei dati personali e tutele collettive dei consumatori*, in A. PALMIERI-F. ALTAMURA (a cura di), *Class action e meccanismi di tutela collettiva. Le prospettive di sviluppo e le sfide della dimensione digitale*, Torino, 2023, p. 95 ss.; S. THOBANI, *Art. 80 Regolamento Generale per la Protezione dei Dati Personali*, in *Commentario del Codice Civile*, diretto da E. Gabrielli, *Delle Persone*, *Leggi collegate*, V. BARBA-S. PAGLIANTINI (a cura di), II, Milano, 2019, p. 1202 ss. Si consenta altresì il rinvio a M. FEDERICO, *Rappresentanza degli interessati, diritti individuali e group data protection*, in *Persona e mercato*, 2023, 1, p. 676 ss.

Proprio l'art. 80 GDPR può essere un riferimento utile a comprendere se gli intermediari possano esercitare i diritti degli interessati esclusivamente previa delega, o anche in assenza di essa [29]. Un'interpretazione sistematica della normativa europea sembra deporre a favore della seconda opzione [30]; così anche un'interpretazione estensiva delle norme del solo DGA, che non fanno espresso riferimento alla delega da parte degli utenti dei dati, corroborando la possibilità di conferire agli intermediari una sorta di procura generale, nel momento in cui gli interessati si rivolgono a loro, associandovisi [31].

Se ad una prima lettura i soggetti più adatti ad esercitare in via collettiva i diritti degli interessati e, per quel che a noi interessa, il diritto alla portabilità dei dati personali, sembrano essere soprattutto i servizi di intermediazione di cui alla lett. b) dell'art. 10 [32], anche le cooperative di dati, a ben guardare, potrebbero essere idonee a tal fine. In particolare, la possibilità di negoziare i termini di trattamento dei dati degli utenti e lo scopo mutualistico, tipico delle società cooperative, si prestano all'esercizio del diritto alla portabilità dei dati, che si trova al confine tra persona e mercato, e che ha importanti risvolti sulla libera concorrenza tra imprese [33].

Il diritto alla portabilità, previsto all'art. 20 GDPR, attribuisce all'interessato dal trattamento dei dati il diritto di ricevere «in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano», nonché il diritto di trasmettere tali dati ad altri soggetti, «senza impedimenti da parte del titolare del trattamento», nei casi in cui il trattamento sia basato sul consenso dell'interessato o necessario per l'esecuzione di un contratto, ed effettuato con mezzi automatizzati.

Il diritto alla portabilità può essere esercitato per tutelare interessi di tipo non patrimoniale (per esempio, se si desidera trasferire i propri dati da una struttura sanitaria all'altra) o dotati di spiccata connotazione economica (si pensi a chi intende trasferire i propri dati personali da un servizio all'altro perché sa che dal terzo titolare riceverà un servizio più vantaggioso, come nei *social media*, o addirittura un ritorno economico immediato). Si intende concentrare la nostra attenzione proprio su quest'ultima fattispecie, perché rispetto ad essa le cooperative di dati potrebbero assumere la funzione di veri e propri intermediari che, nel rapporto consumatori/interessati ed utenti dei dati, potrebbero aiutare gli interessati ad acquisire piena

---

[29] Si veda D. POLETTI, *Il controllo dell'interessato e la strategia europea sui dati*, in *Osservatorio sulle fonti*, 2023, p. 373.

[30] Così G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit., p. 625.

[31] G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit., p. 625.

[32] ID., *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit., p. 618; F. BRAVO, *Intermediazione di dati personali e servizi di* data sharing *dal GDPR al* Data Governance Act, cit., p. 216 ss.

[33] Sul diritto alla portabilità dei dati e la sua natura ambivalente si vedano, tra i molti, S. TROIANO, *Il diritto alla portabilità dei dati personali*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, 2019, *passim*; G. SCORZA, *Il diritto alla portabilità tra privacy e regole del mercato*, in A. MANTELERO-D. POLETTI (a cura di), *Regolare la tecnologia: il reg. Ue 2016/679 e la protezione dei dati personali. Un dialogo fra Italia e Spagna*, Pisa, 2018, p. 308.

consapevolezza dei propri diritti e sfruttare a pieno il valore delle informazioni che li riguardano [34].

Le potenzialità del diritto alla portabilità risultano esaltate anche dal *Digital Markets Act*, il Regolamento europeo 2022/1925, relativo a mercati equi e contendibili nel settore digitale, rivolto ad incoraggiare una maggiore e migliore concorrenza tra imprese, e dal *Data Act*, il Regolamento europeo 2023/2854, recante norme armonizzate su accesso e utilizzo equo dei dati. Tali atti normativi intendono ridefinire le condizioni della concorrenza nel mercato digitale e consentire a nuovi modelli di *business*, basati sulla cooperazione, di prosperare, mediante agevolazioni all'accesso ai dati [35].

Secondo il GDPR, il trasferimento dei dati dovrebbe avvenire nella maniera più veloce ed immediata possibile, e l'interessato dovrebbe poter richiedere al titolare del trattamento di trasmettere i propri dati direttamente ad un terzo titolare (o ad un altro «utente dei dati», per adoperare la terminologia propria del DGA). Tuttavia, nella pratica, le grandi piattaforme non rendono sempre semplicissimo esercitare il diritto alla portabilità che, da un punto di vista tecnologico, richiede che i dati siano forniti attraverso una procedura non eccessivamente difficile ed in un formato interoperabile. Di conseguenza, le cooperative di dati potrebbero tentare, quando si rapportano con i titolari del trattamento, di richiedere delle migliori condizioni di esercizio del diritto alla portabilità, ed aumentare la consapevolezza degli interessati sul valore, anche economico, delle proprie informazioni personali.

D'altra parte, vi è già una società cooperativa la cui attività si avvicina a quella di un intermediario per la portabilità dei dati personali. Ci si riferisce a Polypoly, cooperativa con sede in Germania. Un'impresa che, invece, già svolge a tutti gli effetti il ruolo di intermediario per la portabilità dei dati personali, con sede in Italia, è Hoda s.r.l.; pur non essendo una società cooperativa, ma a responsabilità limitata, il suo servizio di trasferimento dei dati personali, Weople, sembra idoneo ad essere implementato anche attraverso un modello di *business* cooperativo.

L'obiettivo dichiarato di Polypoly è quello di «far recuperare ai titolari dei dati la sovranità sulle proprie informazioni personali». Da un punto di vista pratico, la cooperativa opera mediante un'applicazione, il polypod. Per la precisione, i dati degli individui che adoperano tecnologie di *internet of things* vengono archiviati mediante il polypod sul dispositivo di riferimento. Sta, a questo punto, ai cittadini, che hanno pieno accesso alle proprie informazioni digitali, scegliere come impiegarle; possono concederle in godimento a terzi o addirittura donarle. Se per il trasferimento delle

---

[34] E. BIETTI-A. EXTEBERRIA-M. MANNAN-J. WONG, *Data Cooperatives in Europe: A Legal and Empirical Investigation*, cit., p. 9 ss. ed A. FINK, *Data Cooperative*, in *Internet Policy Rev.*, 2024, 13, p. 4 («*The data cooperative space in Europe is rich, dynamic and diverse. It is a space the flourishing of which should be prioritized by digital and non-digital policy-makers in Europe and European Member States*»).

[35] E. BIETTI-A. EXTEBERRIA-M. MANNAN-J. WONG, *Data Cooperatives in Europe: A Legal and Empirical Investigation*, cit., p. 19.

informazioni personali viene corrisposto agli utenti un compenso da parte di soggetti terzi, alla cooperativa spetta una percentuale del ricavato, che viene impiegato per migliorare i propri servizi, conformemente allo statuto della società [36]. Pertanto, a ben vedere, l'attività svolta da PolyPoly assomiglia molto a quella di un soggetto intermediario che aiuta gli interessati ad avvalersi dei diritti di accesso e di portabilità dei propri dati, garantiti dal Regolamento europeo n. 679 del 2016 [37].

Un altro caso interessante riguarda la start-up Hoda s.r.l., cui si accennava, che recentemente è stata coinvolta in un procedimento dell'AGCM, nel caso *Google c. Hoda*. La Hoda s.r.l. è la società fondatrice di Weople, un'applicazione descritta dal suo ideatore come «una banca di dati». Weople, infatti, consente ai propri iscritti di individuare le modalità più redditizie per "investire" i propri dati [38]. A tal fine, agisce in qualità di intermediaria, nell'ambito di un rapporto che potrebbe assimilarsi a quello di un mandato da parte dei sottoscrittori, richiedendo i loro dati alle piattaforme che li trattano, su loro richiesta, per poi individuare altri titolari del trattamento cui "cederli", esercitando così, di fatto, in loro vece e per loro conto, il diritto alla portabilità [39].

Nel caso sottoposto all'attenzione dell'AGCM, Hoda ha richiesto a Google di ricevere i dati personali dei suoi iscritti. Al rifiuto opposto dalla piattaforma, Hoda ha effettuato un ricorso all'AGCM, descrivendo il comportamento del motore di ricerca come anticoncorrenziale, nello specifico un abuso di posizione dominante, contrario all'art. 102 TFUE. L'AGCM ha quindi intrapreso un'istruttoria *ex* art. 14 della l. n. 287/90 sulla condotta di Google, culminata nell'ordine, rivolto alla piattaforma, di adottare le misure dalla stessa proposte per agevolare l'esercizio del diritto alla portabilità dei suoi utenti, rendendolo *effettivo*.

L'attività di Hoda ben si inquadra nell'ideale di mercato che il DGA vorrebbe creare; l'impresa, infatti, mediante la raccolta e l'aggregazione dei dati dei suoi sottoscrittori, intende proporsi come potere di mercato alternativo a quello delle grandi piattaforme, esercitato in maniera democratica e partecipata, rivolto all'aumento del benessere e dell'autodeterminazione dei singoli utenti.

E proprio per queste ragioni l'attività di Hoda, ascrivibile alla categoria dei c.d.

---

[36] Si rinvia alla descrizione dell'attività di Polypoly presente online, al sito web: https://www.eu-startups.com/directory/polypoly-2/.

[37] Per altri modelli esistenti di cooperative che operano nel campo dei dati si rinvia a A. FINK, *Data Cooperative*, cit., p. 3 ss.

[38] Ci si riferisce al procedimento AGCM, A552, 31 luglio 2023, *Google/ostacoli alla portabilità dei dati*.

[39] Una descrizione più dettagliata del servizio offerto da Weople è presente in F. BRAVO, *Intermediazione di dati personali e servizi di* data sharing *dal GDPR al* Data Governance Act, cit., p. 215 ss. In un primo momento, anche il Garante della Privacy aveva attenzionato l'attività di Weople, chiedendo un parere di conformità al GDPR allo *European Data Protection Board*, richiesta poi ritirata; sulla vicenda, D. POLETTI, *Gli intermediari dei dati*, cit., p. 47 s. L'attività di Hoda è stata menzionata anche nell'analisi congiunta AGCM, AGCOM, GARANTE PRIVACY, *Indagine conoscitiva sui big data*, 2020, p. 99.

infomediaries [40], potrebbe, a noi pare, anche essere intrapresa da una cooperativa di dati, nell'ottica di valorizzare il ruolo di questi enti. Il vantaggio sarebbe non solo un mercato più libero, ma anche un *empowerment* maggiore degli interessati [41].

Nel concreto, le cooperative potrebbero aiutare i titolari dei dati e gli interessati nei loro rapporti commerciali con gli utenti dei dati, assicurare condizioni vantaggiose per l'esercizio del diritto alla portabilità, rendendolo veramente *effettivo*, incrementando la fiducia dei consumatori nell'economia digitale, in linea con gli obiettivi dell'Unione Europea [42], ma anche svolgere attività di consulenza legale [43].

Per quanto riguarda l'individuazione degli enti che, concretamente, possono rientrare nel modello delle cooperative di dati, nel nostro ordinamento, oltre alle società cooperative che operano sul territorio, non è da escludersi che si possa trattare anche di enti del terzo settore o associativi che hanno i requisiti per intraprendere le azioni rappresentative di cui all'art. 80 del GDPR.

Chiaramente sono numerose le implicazioni ed i rischi che derivano dall'affidare un simile servizio ad un intermediario; dovrebbero, dunque, essere definite con precisione le misure di sicurezza da adottare a tutela dei dati, *ex* art. 32 GDPR [44], nonché predisposti, *by design*, gli strumenti adeguati a garantire l'adempimento alle regole di minimizzazione e limitazione del trattamento dei dati [45].

---

[40] «Gli "infomediari" sono imprese che si propongono – almeno formalmente – di agire in favore e per conto degli interessati, di cui acquisiscono i dati, al fine di ottenere, presso fornitori terzi, il pagamento di un prezzo, che viene trasferito agli stessi previa decurtazione di una quota, destinata a remunerare i servizi resi»; così F. BRAVO, *Intermediazione di dati personali e servizi di* data sharing *dal GDPR al* Data Governance Act, cit., p. 214. Per un inquadramento degli infomediari nel contesto nordamericano, si rinvia a J.H. HAGEL-J.F. RAYPORT, *The new infomediaries*, in *The McKinsey Quarterly, Autumn* 1997, 4, p. 54 ss.

[41] F. BRAVO, *Intermediazione di dati personali e servizi di* data sharing *dal GDPR al* Data Governance Act, cit., p. 239.

[42] Si rinvia alla storica comunicazione della Commissione europea *Plasmare il futuro digitale dell'Europa,* 2020, accessibile su: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/shaping-europes-digital-future_it.

[43] L. PETRONE, *Il mercato digitale europeo e le cooperative di dati*, cit., p. 815. Per esempio, Federcoop Romagna già svolge attività di consulenza legale, come è possibile riscontrare dalla descrizione dei suoi servizi presente sul sito web e da uno sguardo allo statuto della società (v. https://www.federcoopromagna.it/federcoop-chi-siamo/).

[44] F. BRAVO, *Intermediazione di dati personali e servizi di* data sharing *dal GDPR al* Data Governance Act, cit., p. 233.

[45] F. BRAVO, *Intermediazione di dati personali e servizi di* data sharing *dal GDPR al* Data Governance Act, cit., p. 254. Inoltre, lo "sfruttamento" a fini commerciali dei dati personali non deve tradursi in un'erosione delle tutele degli interessati e, al contempo, occorre evitare il c.d. "sottoproletariato dei dati", ovvero una situazione in cui i soggetti meno abbienti sono spinti a cedere informazioni anche ad elevato tasso di sensibilità per ricavarne piccoli introiti, "con il rischio di svilimento dei diritti fondamentali della persona" (cfr. L. PETRONE, *Il mercato digitale europeo e le cooperative di dati*, cit., p. 806).

4. Considerazioni conclusive.

Il *Data Governance Act* si pone un obiettivo chiaro: incentivare la condivisione dei dati, nei settori pubblico e privato [46]. A tal fine, definisce alcuni punti fondamentali nel "sistema", ancora in fase di creazione e di definizione, del "diritto delle nuove tecnologie". Tra tutti, la nozione di "dato", che attenua la dicotomia tra dato personale e non personale sancita dal GDPR, e di "servizi di intermediazione dei dati", prevalentemente enti no-profit, da cui sono espressamente escluse le grandi piattaforme digitali, incoraggiando, così, la creazione di un nuovo modello di mercato, più equo e trasparente.

Risultano d'estremo interesse le disposizioni che sembrano assimilare le cooperative di dati, nella misura in cui si qualifichino come servizi di intermediazione che trattano dati personali, a dei "fiduciari informativi" (art. 12, lett. m) [47]. Il DGA enuncia espressamente che i fornitori di servizi di intermediazione debbono agire «nell'interesse superiore degli interessati» e stabilisce in capo a questi degli obblighi definiti che, se violati, possono radicare una responsabilità in capo agli enti (quest'ultima, da coordinare con un'eventuale responsabilità da illecito trattamento dei dati) [48].

L'applicazione dei doveri fiduciari ai professionisti e fornitori di servizi digitali, tra cui gli intermediari, è stata proposta di recente anche da un'autorevole dottrina statunitense. Negli Stati Uniti manca, infatti, un panorama normativo unitario in materia di circolazione dei dati, intelligenza artificiale ed attività delle piattaforme. Da tempo, oltreoceano, i *data intermediaries* operano nella rete [49], e la teoria dei doveri fiduciari potrebbe dimostrarsi risolutiva per imporre degli obblighi generali di liceità, correttezza e trasparenza in capo ai titolari del trattamento [50], nonché per risolvere alcuni problemi e criticità con riferimento all'*enforcement* della normativa consumeristica.

---

[46] G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit., p. 605 ss.

[47] Su cui si rinvia ancora a G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit., pp. 615 ss.

[48] Di cui all'art. 82, GDPR.

[49] In argomento, K. MILLER, *Radical Proposal: Data Cooperatives Could Give Us More Power Over Our Data*, in *HAI-Stanford University Human-Centered Artificial Intelligence*, 2021, disponibile su https://hai.stanford.edu/news/radical-proposal-data-cooperatives-could-give-us-more-power-over-our-data. Un esempio è rappresentato dalla società Lumeria, su cui F. BRAVO, *Intermediazione di dati personali e servizi di* data sharing *dal GDPR al* Data Governance Act, cit., p. 215 s.

[50] La proposta proviene da Autori come Jack Balkin e Woodrow Hartzog; tra i loro lavori, si rimanda in particolare a J.M. BALKIN, *Fixing Social Media's Grand Bargain*, in *Hoover WG on National Security, Technology, and the Law, Aegis Series Paper*, 2018, 1814, p. 11 ss. e da ultimo W. HARTZOG-N. RICHARDS, *Legislating Data Loyalty*, in *Notre Dame Law. Rev. Reflect*., 2022, 97, p. 356 ss. *Contra,* si rinvia a L. KHAN-D. POZEN, *A Skeptical View of Information Fiduciaries*, in *Harv. Law Rev*., 2019, 133, p. 497 ss.

In definitiva, il DGA cerca di delineare un modello economico alternativo a quello del capitalismo estrattivo. In questo contesto, preziose opportunità sembrano schiudersi specialmente con riferimento alle cooperative dei dati [51]. Questi enti, infatti, non soltanto potrebbero accelerare la transizione verso una gestione innovativa e condivisa, per il bene comune, delle "categorie speciali di dati", come i dati sanitari, ma possono anche proporsi, in settori più marcatamente legati ai rapporti commerciali, come nel caso della portabilità dei dati, come un modello alternativo di impresa, rispetto alle grandi piattaforme digitali, ed attenuare le strutturali asimmetrie (economiche, contrattuali) tra consumatori e fornitori di servizi *online* [52].

Appare apprezzabile il passaggio da una logica "difensiva" ad una di "apertura" rispetto alla circolazione dei dati [53]. Tale cambiamento dovrebbe, tuttavia, essere sugellato a livello nazionale, attraverso l'implementazione di politiche adeguate, anche fiscali, che incentivino lo sviluppo degli enti cooperativi [54]. Gli intermediari dei dati potrebbero effettivamente «rafforzare la capacità di agire degli interessati e, in particolare, il controllo dei singoli individui in merito ai dati che li riguardano» [55], agendo come strumenti di *empowerment* degli interessati e degli utenti della rete [56].

Le potenzialità applicative delle cooperative dei dati eccedono di gran lunga i casi di studio cui si è fatto cenno. In futuro, sarà interessante analizzare i rapporti tra intermediari ed utilizzatori dei dati, nonché tra intermediari e soggetti interessati; si tratta di uno studio che richiederà di coordinare GDPR, DGA e Data Act [57], ai fini di delineare una chiara e coerente *governance* dei dati [58]. La nuova disciplina europea, infatti, aggiunge complessità al quadro normativo sul digitale, evidenziando i limiti del GDPR e del modello individuale del controllo sui propri dati personali, ed enfatizzando il ruolo dei soggetti collettivi.

A ben guardare, il DGA sembra corroborare l'idea per cui un trattamento dei

---

[51] K. MILLER, *Radical Proposal: Data Cooperatives Could Give Us More Power Over Our Data*, cit., *passim*.

[52] D. POLETTI, *Gli intermediari dei dati*, cit., p. 53. Può evidenziarsi, nei nuovi atti normativi dell'Unione, l'intento di realizzare, a livello europeo, un'ideale di giustizia distributiva e un maggiore impegno sociale. Alcune considerazioni di natura generale sul tema della giustizia sociale nel diritto europeo sono presenti in U. MATTEI, *Social Justice in European Contract Law: A Manifesto*, in *European Law Journal*, 2004, 10, p. 657.

[53] G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit., p. 622.

[54] I G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit., p. 623; A. FINK, *Data Cooperative*, cit., p. 7.

[55] Considerando 30, DGA.

[56] Si rinvia ancora a D. POLETTI, *Gli intermediari dei dati*, cit., p. 47.

[57] Sul coordinamento tra tali atti normativi e il GDPR, si rinvia a P. DE HERT, *Post-GDPR Lawmaking in the Digital Data Society: Mimesis without Integration – Topological Understandings of Twisted Boundary Setting in EU Data Protection Law*, in D. CURTIN-M.V. CATANZARITI (a cura di), *Data at the boundaries of European law*, Oxford, 2023, p. 124.

[58] S. VILJOEN, *A Relational Theory of Data Governance*, in *Yale Law Journ*., 2021, 131, p. 573 ss.

dati (personali, e non) lecito, corretto e trasparente (cfr. art. 5, lett. a), GDPR) è interesse sopraindividuale e colonna portante di una società democratica, al di là del diritto fondamentale, individuale, alla protezione dei dati stessi. Affinché il progetto del *neomutalismo digitale*, come immaginato dal legislatore europeo, si possa effettivamente realizzare, le imprese e gli attori istituzionali dovranno impegnarsi a sviluppare a pieno le potenzialità offerte dal DGA; ciò potrà avvenire soltanto attraverso un dialogo, interdisciplinare, sinergico e proficuo, tra mondo accademico, imprenditoriale e settore pubblico.

Capitolo XXXIII

La cooperativa di dati quale strumento di sviluppo per l'impresa

Luca Petrone

Abstract: The present contribution, in addition to providing brief insights into the European regulation on data cooperatives, aims to offer some practical guidelines, particularly focusing on the characteristics that such collective entities should possess and the possible areas of intervention, also for the benefit of their members.

1. Cenni sulla disciplina unionale in tema di cooperative di dati.

Com'è noto il legislatore europeo ha scelto di sostenere la creazione di spazi europei dei dati, anche personali, incoraggiandone il mercato, al fine di sostenere e garantire nel tempo la competitività delle imprese europee di fronte allo sviluppo impetuoso e inarrestabile della c.d. *data economy*.

Il tentativo di creare un mercato dei dati [1] alternativo rispetto a quello sviluppatosi oltre i confini unionali e sostenuto da principi più coerenti a logiche democratiche e di sviluppo equo e solidale rappresenta certamente un obiettivo sfidante e tutt'altro che agevole e scontato e necessiterebbe di una disciplina razionale, in grado di dettare regole volte a garantire le libertà individuali di fronte all'immenso

[1] Cfr. *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni*. *Una Strategia europea per i dati*, Bruxelles, COM (2020) 66 final, p. 5, dove viene espressamente previsto che il mercato unico dei dati deve rappresentare uno spazio «(…) aperto ai dati provenienti da tutto il mondo (...) nel quale sia i dati personali sia quelli non personali, compresi i dati commerciali sensibili, siano sicuri e le imprese abbiano facilmente accesso a una quantità pressoché infinita di dati industriali di elevata qualità, che stimolino la crescita e creino valore, riducendo nel contempo al minimo l'impronta di carbonio e ambientale».

potere della tecnica, senza che ciò rappresenti una sterilizzazione delle possibilità che quest'ultima offre [2].

In questo contesto politico ed economico è stato pubblicato e divenuto applicabile il Regolamento (UE) 2022/868, più noto come *Data Governance Act* (*DGA*), ove si assiste al tentativo di conciliare le esigenze di protezione dei dati, fatte oggetto di apposito provvedimento normativo, ossia il Reg. UE 2016/679 (*General Data Protection Regulation*) con quelle del diritto al libero accesso e riuso dei dati.

In particolare tra gli i fronti principali sui quali il DGA interviene è quello dei servizi di intermediazione per lo scambio dei dati, tra i quali vi rientrano le cosiddette cooperative di dati.

Al solo fine di rendere più agevole la comprensione del presente contributo si riporta la definizione che il Regolamento (UE) 2022/868, all'art. 2, par. 1, n. 11, fornisce di *servizio di intermediazione dei dati* prevedendo espressamente che debba intendersi come un «(…) servizio che mira a instaurare, attraverso strumenti tecnici, giuridici o di altro tipo, rapporti commerciali ai fini della condivisione dei dati tra un numero indeterminato di interessati e di titolari dei dati, da un lato, e gli utenti dei dati, dall'altro, anche al fine dell'esercizio dei diritti degli interessati in relazione ai dati personali (…)». In primo luogo, sembrerebbe evidente [3] l'intenzione del legislatore unionale di voler promuovere un modello di condivisione di dati diverso rispetto a quello attualmente dominante nell'ambito della economia digitale, e proposto da quelle società che sposano un modello di *business* basato sullo sfruttamento industriale dei dati, basato su una condivisione più democratica degli stessi e perseguendo l'obiettivo di accrescere la fiducia dei cittadini europei nei confronti degli enti collettivi che, per loro conto, trattano e gestiscono dati applicando il principio della neutralità che dovrebbe comportare una separazione strutturale tra il servizio di condivisione dei dati e qualsiasi altro servizio fornito, in modo tale da evitare problemi di conflitto di interessi [4].

Ebbene tra le tipologie di servizi di intermediazione che il *DGA* all'art. 10,

---

[2] L. PETRONE, *Il mercato digitale europeo: le cooperative di dati*, in *Contratto e impresa*, 2023, 3, pp. 800-817.

[3] V. art. 2, n. 11, lett. *a*) del Reg. UE 2022/868, dove viene previsto espressamente che non rientrano tra i servizi di intermediazione quelli che «ottengono dati dai titolari dei dati e li aggregano, arricchiscono o trasformano al fine di aggiungervi un valore sostanziale e concedono licenze per l'utilizzo dei dati risultanti agli utenti dei dati, senza instaurare un rapporto commerciale tra i titolari dei dati e gli utenti dei dati».

[4] V. il *considerando* n. 33 del Reg. (UE) n. 868/2022 indica che «Un elemento essenziale attraverso il quale aumentare la fiducia e il controllo dei titolari dei dati, interessati e utenti dei dati nei servizi di intermediazione dei dati è la neutralità dei fornitori di servizi di intermediazione dei dati riguardo ai dati scambiati tra titolari dei dati o interessati e utenti dei dati. È pertanto necessario che i fornitori di servizi di intermediazione dei dati agiscano solo in qualità di intermediari nelle transazioni e non utilizzino per nessun altro fine i dati scambiati»; inoltre per un approfondimento sul tema v. F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in *Contratto e impresa Europa*, 2021, 1, pp. 199-256.

comma 1, contempla risultano quelli forniti da cooperative di dati, ossia un modello finalizzato a garantire che i singoli individui non siano incoraggiati a utilizzare i servizi messi a disposizione da parte dell'ente collettivo mettendo a sua disposizione più dati che li riguardano di quanto non sia nel loro stesso interesse e che non utilizza i dati per scopi diversi rispetto a quelli dichiarati, agendo nell'interesse degli interessati.

Non è nelle intenzioni del presente elaborato fornire un'analisi esaustiva dell'istituto delle cooperative di dati, per il quale si rimanda ad altri elaborati [5], tuttavia

[5] L. PETRONE, *Il mercato digitale europeo: le cooperative di dati*, cit., pp. 800-817; F. BRAVO, *Le cooperative di dati*, in *Contratto e impresa*, 2023, 3, pp. 757-799; F. BRAVO, *Il commercio elettronico dei dati personali*, in T. PASQUINO-A. RIZZO-M. TESCARO (a cura di), *Questioni attuali in tema di commercio elettronico*, Napoli, 2020, pp. 83-130; F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in *Contratto e impresa Europa*, 2021, 1, pp. 199-256, e, ivi, spt. par. 4.5; D. POLETTI, *Gli intermediari dei dati*, in *European Journal of Privacy Law & Technologies*, 2022, 1, p. 46 ss.; G. RESTA, *Pubblico, privato e collettivo nel sistema europeo di governo dei dati*, in *Riv. trim. dir. pubbl.*, 2022, 4, pp. 971-995, e, ivi, spt. par. 5, ripubblicato anche all'interno del volume seguente: G. RESTA-V. ZENO ZENCOVICH (a cura di), *Governance of/through data*, Roma, 2023, pp. 605-630 e, invi, spt. par. 5 (p. 622 ss.); per pubblicazioni in ambito interdisciplinare ed economico incentrate sulle cooperative di dati cfr. M. MICHELI-E. FARRELL-B. CARBALLA SMICHOWSKI-M. POSADA SANCHEZ-S. SIGNORELLI-M. VESPE, *Mapping the landscape of data intermediaries. Emerging models for more inclusive data governance*, *Publications Office of the European Union*, Luxembourg, 2023, pp. 47-52, https://publications.jrc.ec.europa.eu/repository/bitstream/JRC133988/JRC133988_01.pdf; SHEFALI GIRISH, *Exploring the value of adding a data layer to cooperatives*: *Megha farmer cooperative case study*, AAPTI Institute, 2022, https://aapti.medium.com/exploring-the-value-of-adding-a-data-layer-to-cooperatives-megha-farmer-cooperative-case-study-1c4fcfd08635; A. PENTLAND-T. HARDJONO, *Data Cooperatives*, in A. PENTLAND-A. LIPTON-T. HARDJONO (eds.), *Building the New Economy*, in *MIT Press Work in Progress*, 2020, Chapter 2, https://wip.mitpress.mit.edu/pub/pnxgvubq/release/2; T. HARDJONO-A. PENTLAND, *Empowering Innovation through Data Cooperatives*, in A. PENTLAND-A. LIPTON-T T. HARDJONO (eds.), *Building the New Economy*, *MIT Press Work in Progress*, 2020, Chapter 4, https://wip.mitpress.mit.edu/pub/xxpfeobg/release/2; A. PENTLAND-T. HARDJONO-J. PENN-C. COLCLOUGH-B. DUCHARME-L. MANDEL, *Data Cooperatives: Digital Empowerment of Citizens and Workers*, Whitepaper, in *MIT Connerction Science*, 1 February 2019, https://ide.mit.edu/sites/default/files/publications/Data-Cooperatives-final.pdf; J. TAIT, *The Case for Data Cooperatives*, in *Whitepaper Series, Open Data Manchester*, 6th September 2021, in https://thedataeconomylab.com/2021/09/06/the-case-for-data-cooperatives; S. METHA-M. DAWANDE-V. MOKERJE, *Can data cooperatives sustain themselves?*, in *LSE Business Review*, 2021, https://blogs.lse.ac.uk/businessreview/2021/08/02/can-data-cooperatives-sustain-themselves/; E. BIETTI-A. ETXEBERRIA-M. MANNAN-J. WONG, *Data Cooperatives in Europe: A Legal and Empirical Investigation*, White Paper created as part of The New School's Platform Cooperativism Consortium and Harvard University's Berkman Klein Center for Internet & Society, Research Sprint, December 2021, in https://cyber.harvard.edu/sites/default/files/2022-02/Data_Cooperatives_Europegroup2.pdf; T. HARDJONO-A. PENTLAND, *Data Cooperatives: Towards a Foundation for Decentralized Personal Data Management*, in *MIT Connection Science*, 15th May 2019, https://arxiv.org/pdf/1905.08819; T. SCHOLTZ, *Platform Cooperativism. Challenging the Corporate Sharing Economy*, in *Rosa Luxemburg Stiftung, New York*, 2016, https://rosalux.org.br/wp-content/uploads/2016/06/scholz_platformcooperativism_2016.pdf; M.F. MORELL-R. ESPELT-M.R. CANO, *Cooperativismo de plataforma: Análisis de las cualidades democráticas del cooperativismo como alternativa económica en en-*

si ritiene comunque opportuno tratteggiarne le caratteristiche più significative. In particolare per servizi forniti da cooperative di dati devono intendersi quelli «offerti da una struttura organizzativa costituita da interessati, imprese individuali o da PMI, che sono membri di tale struttura, avente come obiettivi principali quelli di aiutare i propri membri nell'esercizio dei loro diritti in relazione a determinati dati, anche per quanto riguarda il compiere scelte informate prima di acconsentire al trattamento dei dati, di procedere a uno scambio di opinioni sulle finalità e sulle condizioni del trattamento dei dati che rappresenterebbero al meglio gli interessi dei propri membri in relazione ai loro dati, o di negoziare i termini e le condizioni per il trattamento dei dati per conto dei membri prima di concedere l'autorizzazione al trattamento dei dati non personali o prima che essi diano il loro consenso al trattamento dei dati personali» [6].

L'intenzione sembrerebbe essere quella di organizzare enti collettivi, con poteri analoghi a quelli di un'associazione con funzioni di rappresentanza sindacale, in grado di rappresentare i diritti delle persone, fisiche e non, e governati da manager in grado di agire come fiduciari per conto dei loro soci e raggiungere così un modello di controllo e gestione dei dati che superi – o quantomeno possa diventare ad alternativo – a quello capitalistico.

Il modello cooperativo, almeno nella definizione che ne dà il codice civile italiano, si sposerebbe perfettamente con la necessità di garantire un controllo diffuso dei dati da parte dei relativi titolari ai quali sarebbe comunque garantito il mantenimento del relativo controllo, tenuto conto delle caratteristiche tipiche di questa particolare forma di impresa collettiva e dello scopo che la stessa persegue che non lucrativo, bensì mutualistico [7] che trascende gli interessi dei singoli individui che compongono l'ente, rispondendo ad esigenze di più ampia portata, che spesso hanno rilevanza pubblica; finalità mutualistica che, oltre ai principi [8] che connotano la società cooperativa, sarebbe confacente all'obiettivo di creare un mercato digitale europeo che sia distante dal modello adottato oltreoceano e in grado di garantire l'idoneità dell'organismo cooperativo a soddisfare astrattamente il medesimo bisogno in un numero indeterminato di soggetti, assicurando loro un trattamento equo e paritario, evidenziandone la naturale inclinazione a porsi a servizio di quanti appartengono alla categoria prevista nell'atto costitutivo.

---

tornos digitales, in *CIRIEC-España*, revista de economía pública, social y cooperativa, 2021, https://ojs.uv.es/index.php/ciriecespana/article/viewFile/18429/18962.

[6] V. Reg. UE 2022/868, art. 2, par. 1, n. 15.

[7] Malgrado l'incertezza gli interpreti concordano nel ritenere che lo scopo mutualistico trovi la sua essenza: (a) nello scopo di fornire beni, servizi e occasioni di lavoro a condizioni più vantaggiose di quelle che i soci otterrebbero rivolgendosi al mercato (*mutualità interna*); (b) nello scopo di contribuire al perseguimento di fini di interesse generale per la promozione e lo sviluppo della cooperazione (*mutualità esterna*).

[8] Tra gli altri meritano di essere citati il principio della «porta aperta» (art. 2528 c.c.) e quello relativo al voto capitario (art. 2538, co. 2, c.c.) che sono espressione della democraticità della struttura societaria.

Ovviamente la logica stessa di un modello societario come quello cooperativo, seppur con scopo mutualistico, suggerirebbe in ogni caso l'opportunità di riconoscere un conferimento dei dati con correlativi poteri dispositivi in capo alla società, nonostante le attuali formule legislative sembrino voler escludere tale possibilità [9], limitando il ruolo delle cooperative – e a maggior ragione degli altri intermediari dei dati – a un'attività di consulenza precedente alla manifestazione del consenso, o al massimo a quella di trasmissione a terzi della manifestazione di volontà dell'interessato.

Tale l'impostazione, certamente limitativa per una cooperativa di dati, la quale, per conseguire efficacemente i propri scopi sociali e per contendere il primato del modello imprenditoriale lucrativo, necessiterebbe di un più ampio margine di azione, sarebbe opportuno venisse superata o mediante interventi normativi diretti o attraverso un'attenta attività interpretativa, tenuto conto che, stante il perseguimento di scopi di natura mutualistica, tale limitazione apparirebbe irragionevolmente penalizzante [10].

2. La cooperativa di dati quale strumento di sviluppo per l'impresa: prime indicazioni operative.

I dati, non solo personali, sono divenuti oggetto di crescente attenzione non solo da parte delle imprese, ma anche da parte delle istituzioni, per la straordinaria capacità di sviluppo che la loro analisi consente e che sarebbe opportuno sfruttare, sempre tenuto debitamente conto delle esigenze di protezione della persona e delle relative libertà.

In merito ai modelli di operatività che le cooperative di dati potrebbero utilizzare per l'erogazione dei propri servizi, mentre è presente nella letteratura straniera, per lo più non giuridica, qualche contributo [11], in quella nazionale non risultano particolari approfondimenti, se non quelli recentemente pubblicati [12] alla luce della disciplina dettata dal *Data Governance Act*.

---

[9] Per un approfondimento sul tema vedi F. BRAVO, *Le cooperative di dati*, cit., pp. 757-799.

[10] L. PETRONE, *Il mercato digitale europeo: le cooperative di dati*, cit., pp. 800-817.

[11] V., ad es., J. TAIT, *The Case for Data Cooperatives*, in *Whitepaper Series, Open Data Manchester*, 6th September 2021, in https://thedataeconomylab.com/2021/09/06/the-casefor-data-cooperatives/; E. BIETTI-A. ETXEBERRIA-M. MANNAN-J. WONG, *Data Cooperatives in Europe: A Legal and Empirical Investigation, White Paper created as part of The New School's Platform Cooperativism Consortium and Harvard University's Berkman Klein Center for Internet & Society*, Research Sprint, December 2021, in https://cyber.harvard.edu/sites/default/ files/2022-02/Data_Cooperatives_Europe-group2.pdf; A. PENTLAND-T. HARDJONO-J. PENN-C. COLCLOUGH-B. DUCHARME-L. MANDEL, *Data Cooperatives: Digital Empowerment of Citizens and Workers, Whitepaper*, in cit., https://ide.mit.edu/sites/default/ files/publications/Data-Cooperatives-final.pdf; T. HARDJONO-A. PENTLAND, *Data Cooperatives: Towards a Foundation for Decentralized Personal Data Management*, cit., https://arxiv.org/pdf/ 1905.08819.

[12] V. L. PETRONE, *Il mercato digitale europeo: le cooperative di dati,* cit., pp. 800-817; F. BRAVO, *Le cooperative di dati*, in *Contratto e Impresa*, 2023, 3, pp. 757-799.

Ovviamente a seconda della scelta del modello di operatività di cui la cooperativa di dati intende avvalersi [13] può generare un impatto significativo sul relativo sistema di *governance* e, a seconda dei dati trattati, personali o non personali, potrebbero, altresì, derivare significative conseguenze in merito alla disciplina applicabile agli stessi e alle misure tecniche e organizzative che la struttura societaria dovrà adottare affinché nessun rilievo possa essere mosso da parte di interessati ed autorità.

Fermo restando la necessità del superamento delle criticità ad oggi esistenti in materia di servizi di intermediazione e, nello specifico, di servizi di intermediazioni offerti da cooperative di dati, oltre alla necessità di definire, a monte, quale modello operativo adottare, se da un lato sarebbe certamente possibile la costituzione *ex novo* di nuovi enti collettivi, dall'altro, almeno in questa prima fase applicativa, si potrebbe valutare l'opportunità offerta da operatori economici già esistenti, ampliandone l'oggetto sociale e beneficiando del relativo *know-how*, anche informazionale, che gli stessi già possiedono.

In tal senso, non appare secondario, a parere dello scrivente, neanche sottovalutare l'elemento fiduciario che deve necessariamente sussistere tra cooperativa di dati e *stakeholders*, siano essi soci, clienti o fornitori; anzi proprio la diffidenza, in particolare in merito alle misure tecniche ed organizzative adottate per la gestione dei dati, potrebbe rappresentare il principale ostacolo alla realizzazione di una cooperativa di dati. Ebbene, tale rapporto fiduciario, dovrebbe essere forgiato da nuovo, se si intendesse costituire una nuova organizzazione societaria; viceversa potrebbe già ritenersi esistente in enti collettivi già operativi sul mercato.

In particolare potrebbe rappresentare una idonea struttura d'impresa esistente quella rappresentata da una società che, tenuto conto del relativo *core business*, aves-

---

[13] Cfr. J. TAIT, *op. cit*., p. 5; F. BRAVO, *Le cooperative di dati*, cit., p. 768 e ss. secondo il quale le cooperative di dati potrebbero essere così classificate: «*(i) Member-to-Coopeative* – Secondo questo modello i dati conferiti dai soci sono condivisi all'interno della data cooperative per uso interno, per essere raccolti, conservati ed elaborati dalla cooperativa medesima al fine della fornitura del servizio; *(ii) Member-to-Member (intra-cooperative)* – In base a questo secondo modello i dati vengono condivisi tra i singoli membri della cooperativa, mentre quest'ultima assume un ruolo di facilitatore dello scambio di dati, ossia di "intermediario" tra i singoli "membri" o soci. In tal modo ad un socio verrebbe consentito di accedere a determinati dati, ritenuti utili in sé, per il riuso, oppure ai fini della formazione di un benchmark per la valutazione di una determinata attività o di un determinato servizio o per comprendere il livello di performance di una determinata azione; *(iii) Federated* – Un terzo modello prevede la circolazione e condivisione dei dati tra organizzazioni diverse, ad esempio tra differenti *data cooperatives*, aventi finalità analoghe o processi di data governance simili; *(iv) Third Party* – Questo ulteriore modello si basa su schemi di funzionamento più tradizionali, prevedendo che i dati, collazionati dalla cooperativa, siano condivisi con altre organizzazioni, aventi una struttura diversa dalla cooperativa di dati, in base all'autorizzazione o al consenso rilasciato dai singoli soci a cui i dati sono riferibili ovvero in base ad accordi di condivisione, incluso eventuali licenze, previa negoziazione su termini e condizioni del riuso ad opera della cooperativa di dati, che esercita il suo ruolo di intermediazione; *(v) Open Data* – In quest'ultimo modello i dati conferiti nella cooperativa vengono resi disponibili e liberamente accessibili a tutti».

se già in gestione dati – personali e non – dei propri soci o che, comunque, stante l'elevato grado di fiducia ad essa riconosciuta dai propri *stakeholders*, affronterebbe meno difficoltà nell'acquisizione di dati finalizzati a garantire un servizio specifico a vantaggio della propria base sociale e di terzi interessati.

A tal proposito potrebbe essere assunto a titolo esemplificativo il caso di Federcoop Romagna, società di servizi dell'associazione Legacoop Romagna, che offre ai propri soci e non, assistenza per la gestione della contabilità e delle paghe, oltre che consulenza in ambito legale, fiscale, direzionale, ambientale e in materia di diritto del lavoro.

La base sociale della citata società di servizi è per gran parte coincidente con quella dell'associazione di rappresentanza politico – sindacale e, conseguentemente, potrebbe essere dato per presupposto il rapporto fiduciario tra la stessa struttura di servizi e i propri soci che, vale la pena ricordarlo, sono rappresentati, per la stragrande maggioranza, da persone giuridiche.

Quest'ultimo aspetto ben potrebbe agevolare lo sviluppo di un'attività d'impresa finalizzata ed orientata a supportare le imprese socie nella valorizzazione delle relative risorse, umane ed organizzative, oltre che rappresentare anche un importante possibilità di crescita commerciale per la stessa Federcoop Romagna.

Ovviamente i destinatari elettivi di questi servizi, trattandosi di cooperativa, non potrebbero che essere i relativi soci, ma nulla escluderebbe di poter utilizzare i dati acquisiti anche al fine di poter offrire, a mercato, determinati servizi frutto di adeguate *data analysis*. Tale soluzione, inoltre, almeno in questa prima fase, potrebbe incontrare minori ostacoli applicativi laddove i dati raccolti non avessero carattere personale.

I servizi ad alto valore aggiunto che potrebbe essere forniti, oltre a quelli di consulenza in materia protezione dati, di assistenza per quanto concerne i diritti degli interessati e quelli rivolti a vantaggio degli enti pubblici [14], sgravando gli stessi dai

[14] In particolare sarebbe possibile sviluppare servizi a favore delle amministrazioni locali e nazionali (a seconda dell'estensione geografica della cooperativa), sia attraverso la fornitura di servizi diretti a soddisfare esigenze che le pp.aa. potrebbero avere in relazione alle esigenze di amministrazione del territorio, sia più specificamente attraverso l'interazione riguardo a progetti specifici, tra i quali ad esempio i Gemelli Digitali urbani, in riferimento al quale Bologna è città pioniere a livello internazionale; in particolare attraverso lo sviluppo di questo strumento, che si avvarrà di algoritmi utilizzati nei sistemi di Machine Learning e dell'Intelligenza Artificiale, sarà possibile sperimentare risorse all'avanguardia per far fronte ai cambiamenti climatici, alle disuguaglianze sociali ed economiche, per potenziare la sanità territoriale, nuove forme di partecipazione e la qualità della vita dei cittadini; oppure il progetto PNRR GRINS, il cui obiettivo è quello della produzione di una piattaforma dati georeferenziata a livello molto granulare, utile per diverse applicazioni, tra le quali la ricerca di base e applicata su imprese, famiglie e pubblica amministrazione, la finanza sostenibile, l'innovazione, le politiche di decarbonizzazione, i divari territoriali, la sostenibilità sociale; infine, ulteriore esempio, quello relativo al progetto finalizzato alla valorizzare del ruolo dei medici di medicina generale per sviluppare la sanità territoriale in termini di definizione dei servizi e degli operatori indispensabili per rispondere alla domanda di salute ed ai bisogni dei cittadini attraverso il protocollo di intesa siglato da Legacoop e FIMMG (Federazione italiana Medici di Medicina Generale).

relativi oneri di raccolta, analisi e conservazione, sarebbero finalizzati all'efficientamento dei processi aziendali attraverso lo studio, il confronto e l'aggregazione dei dati che i soci, aderendo all'impresa cooperativa, hanno deciso di conferire. Si pensi ai processi informativi, a quelli industriali, a quelli relativi alla sicurezza e la salute dei lavoratori negli ambienti di lavoro, all'analisi dei consumi energetici, dei metodi di coltivazione di terreni agricoli, ecc. ...

Dopotutto, nell'ambito dell'economia digitale e del *surplus* informazionale [15], ciò che può determinare il successo o l'insuccesso di una azienda è la tempestività con la quale vengono assunte le decisioni; tempestività che potrà essere certamente agevolata dall'avere a disposizione «*data clean*», ossia dati che sono stati preparati e trattati per essere privi di errori, incoerenze, duplicazioni e altre problematiche che possono influenzare negativamente le analisi. In tal senso il successo di un'impresa non potrebbe limitarsi, infatti, alla sola acquisizione di informazioni, ma dipenderebbe dall'efficacia delle decisioni, dalle attività operative e dalla strategia assunta.

Inoltre tale considerazione potrebbe altresì trovare una diretta connessione anche con il secondo comma dell'art. 2086. c.c., introdotto dall'art. 375 del d.lgs. n. 14/2019, e che impone all'imprenditore l'obbligo di dotarsi di un assetto organizzativo, amministrativo e contabile funzionale *anche* alla tempestiva rilevazione di segnali di crisi, al fine di poter assumere con la dovuta prontezza iniziative volte al superamento della stessa e recuperare la continuità aziendale. Fermo restando che un giudizio sulle iniziative assunte dagli amministratori non potrebbe non tenere conto delle dimensioni e della natura dell'attività di impresa, non potrebbe essere escluso a priori che, nel prossimo futuro, possa essere richiesto, per andare esenti da responsabilità, l'aver assunto decisioni sulla base di dati, anche economici, che se correttamente analizzati, avrebbero potuto, quanto meno, anticipare possibili segnali di crisi.

Attraverso la *data analysis* potremmo, infatti, avere a disposizione elementi che stabiliscono un fatto, identificano un «*pattern*», ossia uno schema, consentono una scelta, attivano un processo, determinano la conformità alle politiche, indirizzano un evento e/o fanno emergere la conoscenza dello stesso da parte di coloro che dovranno assumere delle decisioni razionali.

Trasformare i dati in informazioni potrebbe essere – ma lo è già oggi –essenziale per il buon governo dell'impresa perché permetterebbe alle aziende di prendere decisioni informate, rimanere competitive e prosperare, consentendo alle stesse di basare le proprie scelte su evidenze concrete e supportate da dati per pianificare strategie e azioni e non, viceversa, su mere intuizioni o ipotesi. Implementando l'analisi dei dati le aziende potrebbero ottenere una maggiore efficienza operativa,

---

[15] Il termine «*surplus informazionale*» si riferisce a una situazione in cui c'è una quantità eccessiva di informazioni disponibili, che può portare a una serie di problematiche, specialmente in ambito aziendale. Questo *surplus* può rendere difficile per le persone o le organizzazioni trovare, interpretare e utilizzare le informazioni più rilevanti e utili.

migliorando la qualità dei propri prodotti e servizi, aumentare la soddisfazione dei clienti e ottenere un vantaggio competitivo nel mercato.

A tal proposito, una corretta analisi dei dati potrebbe consentire all'imprenditore:

(i) una migliore comprensione del mercato e dei clienti, consentendo all'azienda di comprendere meglio i comportamenti, le preferenze e i bisogni dei propri clienti. Questo potrebbe portare a servizi più personalizzati, miglioramento del prodotto e a strategie di marketing più efficaci;

(ii) un'assistenza ai clienti più efficace, attraverso l'analisi dei relativi feedback, raccogliendoli e analizzandoli per migliorare prodotti e servizi e fornendo loro un supporto proattivo utilizzando l'analisi dei dati per anticipare le relative esigenze e risolvere i problemi prima che vengano segnalati;

(iii) l'identificazione di tendenze e schemi caratterizzanti il mercato di riferimento che non sarebbero evidenti solo osservando i dati grezzi. Tale circostanza potrebbe essere utile a prevedere cambiamenti di mercato, a identificare nuove opportunità e a reagire in modo proattivo a potenziali problematiche;

(iv) l'ottimizzazione dei propri processi aziendali e delle risorse ad essi dedicate, identificando aree di inefficienza, consentendo la razionalizzazione di operazioni, ridurre costi e migliorare la produttività; identificare i fattori che influenzano il *turnover* e sviluppare strategie per aumentare la soddisfazione e la fidelizzazione dei dipendenti;

(v) il miglioramento della produzione attraverso forme di manutenzione predittiva, utilizzando sensori e dati IoT per prevedere e prevenire guasti alle macchine, riducendo i tempi di inattività, il miglioramento dei processi produttivi analizzando i dati di produzione per identificare colli di bottiglia e migliorare l'efficienza operativa e la verifica della qualità del prodotto monitorando i dati di qualità per identificare e risolvere problemi di produzione in tempo reale;

(vi) una più efficiente gestione della *supply chain*, mediante, ad esempio, l'ottimizzazione dell'inventario utilizzando dati storici e predittivi per mantenere livelli dello stesso ottimali, riducendo i costi di stoccaggio e minimizzando le rotture di stock, analizzando i dati di trasporto per ottimizzare le rotte e migliorare l'efficienza delle consegne e valutare le performance dei fornitori e negoziare contratti migliori basati su dati concreti;

(vii) supportare l'innovazione e lo sviluppo di nuovi prodotti o servizi sfruttando le intuizioni per rimanere competitivi e guidare l'innovazione nel settore di riferimento, ad esempio utilizzando dati demografici e comportamentali per segmentare il mercato e personalizzare le campagne di *marketing*, analizzare il comportamento dei clienti tracciandone e analizzandone il comportamento per identificare opportunità di *cross-selling* e *up-selling*, prevedere le vendite utilizzando modelli predittivi per stimare quelle future e pianificare, di conseguenza, le risorse da destinarvi;

(viii) gestire il rischio d'impresa identificandolo e governandolo in modo efficace, anticipando possibili problemi e mitigando gli impatti negativi, in particolare

analizzando le performance finanziarie monitorando e analizzando le metriche finanziarie per prendere decisioni più informate, utilizzando modelli predittivi per prevedere flussi di cassa, entrate e spese future ed analizzare i dati per identificare e mitigare i rischi finanziari;

(ix) misurare il successo attraverso l'analisi dell'efficacia delle strategie e azioni assunte, fornendo dati concreti sul successo o sul bisogno di correzione dei percorsi intrapresi;

(x) confrontare le performance aziendali con quelle dei concorrenti per identificare opportunità di miglioramento.

Ovviamente, l'erogazione di tali servizi – o parte di essi – attraverso l'utilizzo di un «*veicolo*» societario già esistente, non potrebbe tradursi in una mera, seppur necessaria, modifica statutaria, consistente, almeno in prima approssimazione, nell'adattamento allo scopo dell'oggetto sociale e dello scambio mutualistico; l'aspetto più significativo e impattante, infatti, anche da un punto di vista economico, risulterebbe essere quello relativo all'investimento sulle risorse umane e tecniche; investimento indispensabile, non solo per analizzare i dati ed erogare efficacemente il servizio, ma anche per tutelare i dati stessi e le informazioni che, dalla relativa analisi, deriverebbero.

Capitolo XXXIV

Note per un discorso sul metodo delle cooperative di dati

Nicola Pagliarulo

Abstract: Everything is new in the discussion about data cooperatives. We already know something about data, cooperatives, models, markets, rules, but everything has to be re-invented or adapted – all the pieces of the puzzle have to be put together. The proposed approach to this task and the method deriving from it start from the easiest perspective, the technical one. However, it implies that the technical perspective is only one side of the coin and that on the other side there is the business perspective which must also be considered. From these perspectives follows a third one, which would suggest to spend this coin on real data markets and to realize a data cooperative in order to understand the whole picture even before the puzzle is complete.

1. Premesse.

L'unico modo per affrontare un tema complesso e poco conosciuto è tentare di partizionarlo in un insieme di argomenti più limitati. La sommatoria di questi argomenti dovrebbe consentire di ricostruire il tema nella sua interezza.

Questo dice che l'individuazione dell'insieme degli argomenti più limitati è già di per sé un avvio di soluzione concettuale: è la fase di analisi classificatoria, prima fase necessaria ad ogni conoscenza più profonda.

Alla conoscenza più profonda si giunge quando si è in grado di riorganizzare in unità l'insieme delle conoscenze parziali.

Se la fase di partizione rimanda a quel "divide et impera" di latina memoria, la successione di partizione e di riunificazione rimanda piuttosto agli algoritmi di "*map-reduce*", di "cataloga e riunifica", fondamento per il trattamento dei *Big Data*, per loro natura ingestibili e caotici.

Queste considerazioni valgono per affrontare di discorso sulle cooperative di

dati, scomponibile secondo diverse aree tematiche, ovvero, per dirla mutuando la nomenclatura degli analisti di dati (di certo tra gli attori principali del discorso), secondo diverse prospettive.

La visione complessiva è il risultato della sovrapposizione delle diverse prospettive, come la profondità risulta dalla vista binoculare.

Una delle prospettive è certamente quella tecnica e tecnologica (la seconda essendo l'attuazione della prima), poiché a livello tecnico il titolo "cooperative di dati" deve essere tradotto con il titolo "integrazione di dati" e il tema dell'integrazione dei dati è ormai, da alcuni decenni, fondamento della realizzazione di qualsiasi *data warehouse* e, da tempi più recenti, fondamento di ogni attività di scienza del dato.

Al tempo stesso una prospettiva tecnica che non abbia una visione degli obiettivi resterebbe limitata a se stessa. Ciò non la renderebbe inutile, come è indispensabile la scienza di base che solo a posteriori può scoprire quali siano i propri possibili obiettivi; ma qui alla prospettiva tecnica è posto l'obiettivo esplicito di «generare un impatto sociale, culturale ed economico nel settore imprenditoriale e nel contesto sociale, attraverso azioni efficaci e durature incentrare sul modello dell'impresa cooperativa» [1].

Gli obiettivi non possono confinarsi nell'orto delle idealità e dell'etica, perché questo ne limiterebbe, se non annullerebbe, l'impatto. Gli obiettivi debbono essere imprenditoriali e quindi produttivi e poi economici. Piaccia o meno, un'imprenditoria che produce fumo prima o poi si sgonfia. E un'imprenditoria che produce beni, eventualmente valori, ma non produce valore economico, prima o poi muore.

Come i dati, integrati in modo cooperativo, producono valore economico? Qual è, come si deve dire, il modello di *business*? Non è detto che questo modello (eventualmente plurimo) già esista, e, a maggior ragione, la prospettiva del mercato è indispensabile per affrontare il discorso delle cooperative di dati.

Ma un modello di *business* non è un *business*, nella realtà più spesso il secondo precede il primo, che poi interroga il secondo in un ciclo virtuoso. Quindi parlare della prospettiva del mercato non è sufficiente ed occorre parlare della prospettiva di diversi specifici mercati. Occorre, cioè, individuare delle realtà produttive che possano produrre valore economico dalle cooperative di dati. Le prime individuate non saranno le uniche, anzi serviranno da esempio e da traino per le altre.

La prospettiva tecnica, la prospettiva del modello di *business*, la realizzazione dell'una e dell'altra nella prospettiva di uno specifico mercato, costituiscono un triangolo che garantisce la solidità del discorso sulle cooperative dei dati. Chiunque affronti il discorso, indipendentemente dalla prospettiva di ingresso, non può non ragionare degli altri due lati.

---

[1] Cfr. la pagina «Obiettivi e contesto» del Progetto di Terza Missione sulla Cooperative di dati sul sito istituzionale dell'Università di Bologna, consultabile all'indirizzo seguente: https://site.unibo.it/cooperative-di-dati/it/progetto/obiettivi-del-progetto-contesto-di-riferimento-partner.

2. Prospettiva tecnica.

Semplificando all'estremo, l'implementazione di una cooperativa di dati, può sintetizzarsi nelle tre fasi di raccolta, organizzazione, fruizione dei dati condivisi.

Ricondotto a questo livello di astrazione, il processo è identico a qualsiasi processo di analisi dei dati.

Nella progettazione di un *data warehouse*, che definiremo tradizionale, ma sempre attuale, la prima fase è quella dell'identificazione delle fonti di dati: di quali dati si dispone, chi li detiene, come sono strutturati.

I dati identificati sono poi raccolti in un contenitore di decantazione, una base di dati che chiamiamo "*staging area*".

I dati sono poi puliti (*data cleaning*) e trasferiti in un contenitore organizzato, una base di dati che chiamiamo "*data warehouse*". È importante sottolineare che in questo caso tutti i dati sono uniformati per adattarsi ad un unico stampo che è il formato del *data warehouse*.

I dati raccolti ed organizzati sono poi fruiti in diversi modi, ma in generale sono utilizzati, con opportuna visualizzazione, come supporto alla decisione.

La progettazione di un sistema di *data warehouse* è basata su modelli che esistono ormai da un quarto di secolo e può disporre di un insieme sostanzialmente infinito di strumenti informatici a supporto, senza peraltro nulla perdere della sua complessità.

Concettualmente la progettazione di un sistema più recente di "*data analytics*" è identica, ma con alcune differenze sostanziali. Prima tra tutte la varietà dei formati delle fonti dati che ha condotto alla sostituzione, linguistica, ancor prima che tecnica, della "*staging area*" con il "*data lake*". Il lago ha il vantaggio di non costringere i dati all'interno dello stesso stampo.

L'organizzazione dei dati ripescati dal lago per consentirne la fruizione a valore aggiunto non è ancora basata su modelli consolidati, ma è piuttosto legata alle capacità e all'esperienza dei progettisti che pure dispongono già di un numero costantemente crescente di tecnologie a supporto. Quanto alla fruizione è sempre più legata alla realizzazione di sistemi esperti che, più o meno propriamente, vengono etichettati come Intelligenza Artificiale.

Tutto questo è strettamente collegato al metodo per la creazione di cooperative di dati.

Una varietà e quantità di produttori creano e condividono una varietà e quantità di dati. Questi dati dovranno essere raccolti, organizzati, trasformati in valore. Circa la raccolta, è ragionevole pensare che il conferimento dei dati da parte dei produttori debba avvenire con il minore impegno possibile o, meglio, senza nessun impegno.

Un concetto tecnico che può essere adeguato a questo tipo di raccolta è quello della "federazione di dati" (anche la parola non è così lontana da quella della "cooperativa di dati"). I dati non vengono più raccolti e concentrati in un ulteriore contenitore, *staging* o *lake*, ma ad essi viene sovrapposto un sistema informatico in gra-

do di concentrarli virtualmente. Esistono già alcuni strumenti per realizzare questa federazione (uno è Denodo [2]), ma altro si può creare o potrà essere prodotto.

La trasformazione in valore dei dati federati passa obbligatoriamente attraverso la loro interrogazione. Per consentire ai produttori dei dati (potrebbero anche essere chiamati "interessati", usando il linguaggio del GDPR) di conservare il controllo dei propri dati, e dei dati ad essi associati in cooperativa, occorre ipotizzare un linguaggio di interrogazione non formale, non tecnico. Gli strumenti di analisi del linguaggio naturale disponibili (a vario titolo inseriti nel grande contenitore dell'AI) possono essere utilizzati per trasformare una domanda in linguaggio naturale in un'interrogazione formale, tecnica, verso una base di dati. Ciò sarebbe a maggior ragione realizzabile se il linguaggio afferisse ad un unico dominio semantico, come potrebbe essere nel caso di cooperative di dati relative ad uno specifico mercato.

In conclusione, partendo dei metodi per la progettazione di *data warehouse*, passando attraverso i metodi per la progettazione di sistemi di *analytics*, tenendo conto dello stato dell'arte della tecnologia, è ragionevolmente possibile definire un metodo per la realizzazione tecnica di un sistema informativo a supporto delle cooperative di dati.

3. Prospettiva di *business.*

Nella realizzazione di un nuovo sistema informativo la parte più semplice, a prescindere dalla difficoltà, è quella tecnica. Dal punto di vista tecnico, magari con ritardo e con difficoltà inattese, è sempre possibile raggiungere l'obiettivo. Ma questo in nessun modo garantisce il successo del progetto, che è tale solo se il sistema è effettivamente utilizzato, e con soddisfazione, dagli attori a cui era destinato: cioè se il sistema effettivamente realizza un modello di *business* semplice da capire e facilmente condivisibile [3-4]. Se il modello di *business* delle cooperative di dati non fosse sostenibile, anche il miglior *software* sarebbe inutile.

Perché i produttori di dati dovrebbero consorziarsi in una cooperativa? Per la stessa ragione per la quale, ad esempio, i produttori d'uva si consorziano. Perché la quantità d'uva prodotta da un singolo produttore non è sufficiente per realizzare un buon vino, mentre una maggiore quantità di uva può essere utilizzata per realizzare un buon vino. Il valore della piccola quantità di uva è molto basso, il valore del vi-

---

[2] DENODO TECHNOLOGIES INC., *Denodo Platform*, Palo Alto, CA, 2024, https://www.denodo.com/en/denodo-platform/denodo-platform.

[3] M.M. BÜHLER-I. CALZADA-I. CANE-T. JELINEK-A. KAPOOR-M. MANNAN-S. MEHTA-V. MOOKERJE-K. NÜBEL-A. PENTLAND-T. SCHOLZ-D. SIDDARTH-J. TAIT-B. VAITLA-J. ZHU, *Unlocking the Power of Digital Commons: Data Cooperatives as a Pathway for Data Sovereign, Innovative and Equitable Digital Communities*, in *MDPI (Multidisciplinary Digital Publishing Institute)*, 2023, Vol. 3, n. 3, pp. 146-171.

[4] A. FINK, *Data cooperative*, in *Internet Policy Review*, 2024, Vol. 13, issue 2.

no è molto più alto. I produttori d'uva si consorziano perché il ritorno sull'investimento è alto, perché in un'ottica cooperativa 1 + 1 è sempre maggiore di 2.

Alcune difficoltà sono tipiche di questo approccio, mentre altre sono specifiche del bene da condividere, dei dati.

Intanto va considerata la frequente reticenza alla condivisione di un bene personale, che può essere vissuta come una perdita per sé e non un maggior guadagno per tutti. Certamente gli studi di psicoeconomia e delle molte discipline, con diversi nomi, afferenti debbono essere tenuti in conto nella definizione del modello di *business* delle cooperative di dati. Come pure devono essere tenuti in conto i modelli dell'interazione economica che derivano dalla teoria dei giochi.

Anche senza attendere le risultanze di studi di approfonditi, di certo il modello di *business* deve prevedere la possibilità che il conferimento dei dati avvenga senza necessità di specifiche finalità ideali, che limiterebbero molto il numero e la tipologia dei produttori coinvolti, confinandoli nel consueto recinto degli attori eticamente motivati.

Inoltre, il conferimento dei dati condivisi dovrebbe avvenire senza complessità aggiuntiva rispetto a quella già connessa alla loro produzione. Qualsiasi operazione aggiuntiva di trattamento alla fonte, cioè qualsiasi lavoro aggiuntivo richiesto al produttore, farebbe seccare presto il flusso di dati.

Una difficoltà specifica del dato come bene è l'evidente difficoltà di riconoscergli, anche solo psicologicamente, un valore. Coerentemente il modello di *business* dovrebbe trattare il dato come una materia prima, priva di valore intrinseco, ma che acquista valore con la sua trasformazione.

La vera scommessa della prospettiva di *business* è quella di individuare quali siano queste trasformazioni, o, per meglio dire, il risultato di queste trasformazioni, cioè il prodotto della cooperativa di dati. Quale metallo è prodotto dal minerale? Quale vino è prodotto dall'uva? La vera scommessa è quindi quella di mostrare al produttore e cooperante il metallo o il vino, perché gli sia evidente il valore della cooperazione.

La scommessa potrebbe apparire perdente, se già non fosse stata vinta dalle aziende che oggi dominano il mercato tecnologico. Quando queste aziende hanno iniziato a raccogliere dati attraverso i più vari servizi, probabilmente non avevano ancora stabilito come questi dati sarebbero stati valorizzati (almeno dal punto di vista commerciale, prescindendo quindi da eventuali altre finalità della raccolta). I servizi ad altissimo valore aggiunto sono stati ideati e sviluppati solo dopo avere avviato e consolidato la raccolta dei dati. Non c'è ragione per cui lo stesso percorso non possa essere attuato dalle cooperative di dati [5-6].

---

[5] M. Micheli-E. Farrell-B. Carballa-Smichowski-M. Posada-Sanchez.S. Signorelli-M. Vespe*, Mapping the landscape of data intermediaries. Emerging models for more inclusive data governance*, Publications Office of the European Union, Luxembourg, 2023.

[6] J. Zhu-O. Marjanovic, *A Different Kind of Sharing Economy: A Taxonomy of Platform Cooperatives*, in *Proceedings of the 57th Hawaii International Conference on System Sciences*, 2024.

È ovvio che con materie prime diverse saranno realizzati prodotti diversi. Dall'uva il vino, dalle mele il sidro; dai dati dei consumi energetici qualcosa, dai dati di maturazione del grano qualcos'altro.

Quando qui si parla di modello di *business*, sarebbe dunque più opportuno parlare di meta-modello, da istanziare poi negli specifici mercati.

E il modello o meta-modello di *business* non deve essere rappresentato con qualche saggio o dissertazione, ma in modo formale, utilizzando un qualche linguaggio formale, ad esempio (senza precludere altre possibilità) come un processo di *business* attraverso BPMN (*Business Process Modeling Notation*) [7].

Un linguaggio formale impone la definizione delle parti coinvolte del modello, elencate a seguire senza alcuna completezza e prima di qualsiasi approfondimento, solo per indicizzare quanto già espresso:

(i) *gli attori*: il produttore, il trasformatore (la cooperativa stessa o qualcuno per suo conto), il consumatore dei dati;

(ii) *gli input*: i dati prodotti e conferiti alla cooperativa;

(iii) *gli output*: i servizi o prodotti a valore aggiunto realizzati dal trasformatore;

(iv) *le attività*: acquisizione dati, pulizia, interrogazione, trasformazione, fruizione prodotti.

In conclusione, la realizzazione tecnica di un sistema di cooperazione dei dati ha un senso solo se precedentemente e contemporaneamente viene indagata la consistenza del modello di *business*, inteso sia come efficacia dell'interazione tra le parti che come efficienza economica. La fattibilità tecnica e quella economica debbono poi essere declinate sugli specifici mercati che possono fruire del prodotto dei dati.

4. Prospettiva di mercato.

Il discorso sulle cooperative di dati ha molti padri ideali: dalla condivisione dei beni, allo scambio mutualistico, alle cooperative che da un paio di secoli sono nate ed operano, specialmente in Europa, con le più diverse ispirazioni politiche. Ma, forse, nasce soprattutto con un'idea più o meno esplicitata.

Le cooperative, nella loro versione moderna, nascono a seguito della prima rivoluzione industriale, come reazione di difesa all'accentramento abnorme di capitali in poche persone.

La quarta rivoluzione industriale ha portato all'accentramento abnorme di dati in pochissimi soggetti industriali. Questi soggetti hanno, con una capacità inconcepibile fino a poco tempo fa, trasformato l'abnorme quantità di dati in loro possesso in valore economico. I dati sono stati o liberamente "donati" dagli interessati in cambio della fruizione dei servizi informatici resi disponibili dai soggetti "accumulatori", o generati dalla fruizione dei servizi informatici stessi. Il risultato per quan-

[7] OBJECT MANAGEMENT GROUP, *Business Process Model and Notation*, Vers. 2.0.2, 2014.

to possa essere analizzato, ammirato, demonizzato, suscita comunque stupore.

Le cooperative di dati possono nascere come reazione di difesa. I dati non sono più ceduti ad altri a vantaggio di pochissimi, in cambio di servizi più o meno necessari che poi diventano dei vincoli, ma sono condivisi con altri a vantaggio di tutti. Forse c'è anche un legittimo desiderio di rivalsa, attraverso l'imitazione dei metodi degli "accumulatori", che però non posso essere ripresi "*as is*", ma debbono essere ridisegnati "*to be*".

Il nuovo disegno passa, dunque, attraverso un nuovo approccio tecnico e contemporaneamente un nuovo modello di *business*, ma deve passare anche attraverso esperienze reali, su mercati reali; non può trattarsi di semplici dimostratori, prototipi malfunzionanti che lasciano solo intuire e sperare il risultato atteso.

Quali siano i mercati fin da ora accessibili alle cooperative di dati è l'obiettivo della terza prospettiva del metodo qui delineato. Di seguito, si avanzano alcune proposte, senza pretesa di anticipare i risultati di una più approfondita indagine.

Un primo mercato promettente è quello delle Comunità Energetiche Rinnovabili (CER) [8], istituite dal Decreto legislativo dell'8 novembre 2021, n. 199, anche a seguito del Decreto attuativo del Ministero dell'Ambiente e della Sicurezza Energetica dello scorso 24 gennaio 2024.

Per la loro stessa natura, tali Comunità già sono chiamate a condividere i dati di produzione e di consumo energetico, per ottenerne benefici in termini di riduzione delle tariffe e di contributo ai costi degli impianti.

In generale ogni mercato di "beni comuni" (di "*commons*", per dirla nel linguaggio dell'economia) si presta ad una gestione cooperativa dei dati di esercizio.

Sul fronte "privatistico" è noto che la GDO (Grande Distribuzione Organizzata) ricava non solo dalla vendita dei prodotti, ma dalla vendita dei dati relativi alle vendite. Una cooperativa fatta di piccoli esercizi potrebbe ottenere dalla somma dei propri dati di vendita vantaggi equivalenti a quelli ottenuti dalla GDO.

Nei distretti industriali [9-10], peculiarità del panorama produttivo italiano, le singole aziende traggono vantaggio anche solo dalla contiguità geografica, perché spesso sono tra di loro aspramente concorrenti. Una cooperativa di dati potrebbe ottenere forniture a miglior prezzo senza costringere le aziende a rinunciare alla loro gelosa individualità ed alla reciproca concorrenza e diffidenza.

---

[8] M. KUBLI-S. PURANIK, *A typology of business models for energy communities: Current and emerging design options*, in *Renewable and Sustainable Energy Reviews*, 2023, Vol 176, 113-165.

[9] M.M. BÜHLER-I. CALZADA-I. CANE-T. JELINEK-A. KAPOOR-M. MANNAN-S. MEHTA-V. MOOKERJE-K. NÜBEL-A. PENTLAND-T. SCHOLZ-D. SIDDARTH-J. TAIT-B. VAITLA-J. ZHU, *Harnessing Digital Federation Platforms and Data Cooperatives to Empower SMEs and Local Communities*, presented at G20 India, TF-2: *Our Common Digital Future: Affordable, Accessible, and Inclusive Digital Public Infrastructure*, 2023.

[10] P. BODENHAM, *Data cooperatives in agriculture: An opportunity for farmers*, in *Nova Itinera Percorsi del diritto nel XXI secolo*, 2023, n. 1, pp. 35-54.

5. Conclusione.

La motivazione alla cooperazione e quindi alla condivisione dei dati deriva principalmente dal vantaggio dei singoli cooperanti. Quindi la realizzazione tecnica di un sistema informativo dedicato alle cooperative di dati, né più né meno complessa di molte altre attività di integrazione dei dati, deve procedere assieme all'identificazione del prodotto a valore aggiunto dei dati condivisi e quindi del cliente di tale prodotto. Sistema informativo e modello di processo e di *business* sono due facce della stessa medaglia.

La novità operativa della proposta delle cooperative di dati inizialmente può lasciare increduli, come ogni novità, ma richiede di essere indagata, per non lasciare che pochissimi dispongano e sfruttino i dati di tutti.

L'indagine non può essere solo di natura progettuale o speculativa, ma richiede realizzazioni operative, per poter innestare quel volano di imitazione e superamento che trasforma un'idea in un'innovazione condivisa.

Questo lavoro ha la sola pretesa di suggerire alcune note per imprimere il primo impulso al volano.

Capitolo XXXV

Costruzione di una *data platform* per cooperative di dati e soluzioni tecnologiche: integrazione, anonimizzazione e fruizione responsabile

Matteo Mancini-Vladimiro Buda[*]

Abstract: The growing awareness of the importance of data as a primary resource has led to increased attention on how it is managed, processed, and shared. Within the realm of data cooperatives, there is a need to create an ecosystem where data can be shared collaboratively and securely, while also respecting data privacy and security. In this context, we propose the development of a Data Platform that acts as a catalyst for collaboration among companies and organizations. The mutualistic model adopted ensures fair exchange of data, allowing companies to contribute raw data to a shared repository and access anonymized data in return. This approach fosters the construction of a cohesive community based on trust and reciprocity. The Data Platform aims to achieve several key objectives: 1. Data Harmonization: Integrating and standardizing data from various sources to create a cohesive and homogeneous environment; 2. Data Anonymization: Applying advanced techniques to ensure privacy protection and regulatory compliance; 3. Data Exposure: Making data accessible to the contributors, allowing them to access anonymized data and use it for analysis and solution development; 4. Benchmark Creation and Data Marketplace: Providing tools for benchmark creation and implementation of a Data Marketplace, facilitating data exchange and sale through public or licensed catalogs. To ensure data security and privacy, the Data Platform adopts a robust and secure architecture. Data is encrypted and anonymized to protect it from unauthorized access and ensure compliance with privacy by design and privacy by default principles. Additionally, access control and monitoring measures are implemented to detect and prevent security breaches. At the technological level, the Data Platform leverages innovative concepts such as Data Federation and Virtual Data Lake. Data Federation enables integration and access to distributed data transparently, while the Virtual Data Lake provides a virtual environment for data analysis and exploration without the need for physical data transfer. In conclusion, our proposal aims to promote collaboration and responsible data sharing within data cooperatives and technological solutions. The Data Platform represents a step forward in creating a secure, transparent, and collaborative data ecosystem that fosters innovation and sustainable development.

[*] I singoli paragrafi del presente scritto sono da attribuire, congiuntamente, ad entrambi gli autori.

1. Introduzione.

1.1. Obiettivi del documento.

Nell'era digitale in cui i dati rappresentano una risorsa di valore fondamentale, la creazione di una *Data Platform* per cooperative di dati emerge come un'opportunità per favorire la collaborazione e lo scambio responsabile dei dati. Questo documento si propone di esplorare il processo di progettazione e implementazione di *Data Platform*, con particolare attenzione agli obiettivi, alle sfide e alle soluzioni proposte.

La *Data Platform* Cooperativa rappresenta un'infrastruttura fondamentale per la gestione collaborativa dei dati tra i membri di una cooperativa di dati. Questo capitolo introduttivo fornirà una panoramica sul concetto di *Data Platform* Cooperativa, esaminando il ruolo della cooperativa nella sua implementazione, i vantaggi derivanti dalla collaborazione e le sue applicazioni in contesti cooperativi.

1.2. Definizione e concetto.

Una *Data Platform* Cooperativa è un ambiente tecnologico integrato e condiviso che consente ai membri di una cooperativa di accedere, gestire e utilizzare in

modo collaborativo i dati condivisi. Si basa sull'idea che i dati siano un bene comune da condividere e utilizzare in modo responsabile per il beneficio collettivo dei membri della cooperativa.

Il concetto di *Data Platform* Cooperativa promuove la collaborazione e lo scambio di conoscenze tra i membri della cooperativa, consentendo loro di lavorare insieme per ottimizzare l'uso dei dati e generare valore aggiunto per l'intero ecosistema. La piattaforma serve da punto centrale per la raccolta, la gestione e l'analisi dei dati condivisi, facilitando la collaborazione e la condivisione delle risorse tra i membri.

1.3. Ruolo e vantaggi della cooperazione.

Il ruolo della cooperativa all'interno della *Data Platform* Cooperativa è fondamentale per facilitare la collaborazione e la condivisione dei dati tra i suoi membri. Tra i principali vantaggi derivanti dalla collaborazione cooperativa figurano:

(i) *condivisione responsabile dei dati*: la cooperativa promuove una cultura di condivisione responsabile dei dati tra i suoi membri, consentendo loro di accedere e utilizzare i dati in modo etico e conforme alle normative sulla *privacy*;

(ii) *centralizzazione dei dati*: una *Data Platform* consente di centralizzare i dati provenienti da diverse fonti e sistemi, facilitando la loro gestione e manutenzione;

(iii) *massimizzazione del valore dei dati*: grazie alla collaborazione e allo scambio di conoscenze, i membri della cooperativa possono massimizzare il valore dei dati condivisi, generando *insight* e informazioni utili per l'intero ecosistema;

(iv) *agilità operativa*: una *Data Platform* favorisce l'agilità operativa, consentendo alle aziende di rispondere rapidamente ai cambiamenti del mercato e alle esigenze dei clienti attraverso l'analisi dei dati in tempo reale;

(v) *incremento dell'innovazione*: la cooperazione tra i membri favorisce l'innovazione e lo sviluppo di nuove soluzioni e servizi basati sui dati condivisi, stimolando la crescita e la competitività dell'intero ecosistema.

1.4. Applicazioni e settori cooperativi.

Le applicazioni della *Data Platform* Cooperativa sono molteplici e possono essere trovate in una vasta gamma di settori e contesti cooperativi. Alcuni esempi di settori in cui le *Data Platform* Cooperative sono ampiamente utilizzate includono:

(i) *agricoltura*: le cooperative agricole utilizzano le *Data Platform* per condividere informazioni sui raccolti, monitorare le condizioni meteorologiche e ottimizzare le operazioni colturali;

(ii) *energia rinnovabile*: le cooperative energetiche utilizzano le *Data Platform* per monitorare e ottimizzare la produzione e la distribuzione di energia rinnovabile, facilitando la transizione verso un'economia a basse emissioni di carbonio;

(iii) *sanità*: le cooperative sanitarie utilizzano le *Data Platform* per gestire e analizzare i dati clinici dei pazienti, facilitare la condivisione sicura delle informa-

zioni tra i professionisti sanitari e migliorare la qualità delle cure attraverso l'analisi dei dati di *outcome* e di *performance*;

(iv) *cooperative di consumatori*: le cooperative di consumatori utilizzano le Data Platform per condividere informazioni sui prodotti e servizi, migliorare l'esperienza dei clienti e promuovere pratiche commerciali etiche e sostenibili.

In sintesi, la *Data Platform* Cooperativa rappresenta un'opportunità unica per i membri di una cooperativa di dati di collaborare e condividere conoscenze per ottimizzare l'uso dei dati condivisi.

Successivamente, approfondiremo i diversi aspetti della realizzazione e dell'utilizzo di una *Data Platform* Cooperativa, esaminando le migliori pratiche, le tecniche avanzate e le considerazioni pratiche per garantire il successo di tale iniziativa all'interno di un'organizzazione cooperativa.

2. Cooperative di dati e soluzioni IT per l'acquisizione dei soci e la gestione delle attività.

2.1. Ecosistema collaborativo.

La cooperativa di dati rappresenta un ecosistema collaborativo in cui diverse aziende ed entità lavorano insieme per condividere conoscenze, risorse e dati al fine di promuovere l'innovazione e lo sviluppo di soluzioni avanzate. Questa sezione esplorerà il ruolo e l'importanza della cooperativa all'interno della *Data Platform*, nonché i benefici derivanti dalla collaborazione e dalla condivisione delle risorse.

2.2. Ruolo della cooperativa nella *Data Platform.*

La cooperativa svolge un ruolo centrale nella *governance* e nello sviluppo della *Data Platform*, fungendo da catalizzatore per la collaborazione e lo scambio di conoscenze tra le diverse parti interessate. I suoi membri rappresentano una vasta gamma di competenze e *expertise*, che vengono messe insieme per affrontare sfide comuni e sfruttare opportunità di mercato.

Tra i compiti principali della cooperativa vi è la definizione delle strategie e delle linee guida per l'utilizzo dei dati all'interno della *Data Platform*, nonché la promozione di pratiche di condivisione e collaborazione che favoriscano l'innovazione e lo sviluppo di soluzioni condivise. La cooperativa funge anche da punto di incontro per facilitare la comunicazione e la collaborazione tra i suoi membri, fornendo un ambiente inclusivo e collaborativo in cui condividere risorse e conoscenze.

2.3. Benefici della collaborazione nella cooperativa.

La collaborazione all'interno della cooperativa porta una serie di benefici per i suoi membri e per l'intero ecosistema. Tra i principali vantaggi figurano:

(i) *accesso a risorse e expertise*: i membri della cooperativa hanno accesso a una vasta gamma di risorse e competenze, che possono essere utilizzate per affrontare sfide complesse e sviluppare soluzioni innovative;

(ii) *condivisione di conoscenze*: la cooperativa facilita lo scambio di conoscenze e *best practice* tra i suoi membri, consentendo loro di imparare gli uni dagli altri e di sviluppare soluzioni condivise basate sull'esperienza collettiva;

(iii) *riduzione dei costi*: la condivisione delle risorse e delle infrastrutture tra i membri della cooperativa consente di ridurre i costi operativi e di sviluppo, aumentando l'efficienza complessiva dell'ecosistema;

(iv) *innovazione accelerata*: la collaborazione tra aziende e entità diverse favorisce l'innovazione accelerata e lo sviluppo di soluzioni avanzate che possono avere un impatto significativo sul mercato e sulla società nel suo complesso.

2.4. Soluzioni IT per l'acquisizione dei soci e la gestione delle attività.

I modelli cooperativi prevedono l'integrazione di soluzioni IT per acquisire nuovi soci e gestire le attività in modo efficiente. Le piattaforme di gestione dei membri consentono ai potenziali soci di registrarsi *online*, compilando moduli digitali personalizzati e fornendo le informazioni necessarie. Ad esempio, soluzioni *CRM* (*Customer Relationship Management*) personalizzate per le cooperative possono automatizzare il processo di registrazione e fornire un sistema centralizzato per gestire le interazioni con i soci. Questi strumenti consentono alle cooperative di semplificare la raccolta delle informazioni dei soci, migliorando l'efficienza e riducendo il tempo necessario per l'iscrizione. Inoltre, le soluzioni di *marketing automation* consentono alle cooperative di raggiungere nuovi potenziali soci attraverso campagne di marketing mirate e personalizzate. Utilizzando strumenti di analisi dei dati avanzati, le cooperative possono identificare i segmenti di mercato più promettenti e adottare strategie di acquisizione dei soci basate sui dati. Queste soluzioni IT consentono alle cooperative di ampliare la propria base di soci e migliorare l'efficacia complessiva delle loro operazioni.

2.5. *Governance* e struttura della cooperativa.

La *governance* e la struttura della cooperativa sono fondamentali per garantire un funzionamento efficace e trasparente dell'ecosistema. La cooperativa stabilisce meccanismi di governance che regolano l'adesione dei membri, la partecipazione alle decisioni e la gestione delle risorse condivise.

Tra i principali organi decisionali vi sono il consiglio di amministrazione e l'assemblea dei membri, che si occupano rispettivamente della definizione delle strategie e delle politiche della cooperativa e dell'approvazione delle decisioni chiave. Inoltre, possono essere istituiti comitati specializzati per affrontare specifiche aree di interesse, come ad esempio la sicurezza dei dati, la conformità normativa o lo sviluppo tecnologico.

La cooperativa adotta una struttura aperta e inclusiva che incoraggia la partecipazione attiva dei suoi membri e promuove la trasparenza e la condivisione delle risorse e delle conoscenze. Le decisioni vengono prese in modo collaborativo e democratico, garantendo che gli interessi di tutti i membri siano presi in considerazione e rispettati.

Le soluzioni IT giocano un ruolo fondamentale nel promuovere la partecipazione democratica dei soci all'interno delle cooperative di dati. Tra le principali soluzioni che favoriscono un coinvolgimento e una diffusione delle pratiche collaborative tra i soci delle cooperative di dati possiamo elencare:

(i) *piattaforme di social collaboration*: le piattaforme di *social collaboration* offrono agli utenti uno spazio virtuale per condividere idee, discutere tematiche rilevanti e votare su questioni importanti. Ad esempio, l'implementazione di una piattaforma di *social collaboration* aziendale consente ai soci di interagire in modo informale, scambiare opinioni e partecipare attivamente al dibattito interno;

(ii) *strumenti di votazione elettronica*: le soluzioni di votazione elettronica consentono ai soci di esprimere le proprie opinioni su questioni cruciali attraverso sondaggi online o votazioni virtuali. Questi strumenti garantiscono un'ampia partecipazione e assicurano un processo decisionale equo e trasparente. Ad esempio, l'utilizzo di *software* di votazione elettronica consente ai soci di esprimere facilmente il proprio voto su questioni complesse, senza dover partecipare fisicamente a riunioni o assemblee;

(iii) *forum online e gruppi di discussione*: i *forum online* e i gruppi di discussione forniscono un ambiente strutturato per il dibattito e lo scambio di idee tra i soci. Attraverso questi strumenti, i soci possono proporre argomenti di discussione, condividere risorse pertinenti e collaborare alla definizione di strategie aziendali. Ad esempio, la creazione di *forum* tematici su argomenti specifici consente ai soci di approfondire la comprensione di questioni complesse e contribuire alla definizione di soluzioni innovative;

(iv) *dashboard e report interattivi*: le soluzioni di *business intelligence* offrono *dashboard* e *report* interattivi per visualizzare e analizzare i dati in modo intuitivo e accessibile. Questi strumenti consentono ai soci di monitorare le prestazioni dell'organizzazione, esplorare *trend* e identificare opportunità di miglioramento. Ad esempio, l'implementazione di un *dashboard* personalizzato consente ai soci di accedere facilmente a metriche chiave e dati pertinenti, consentendo loro di prendere decisioni informate e partecipare attivamente al processo decisionale.

Questi esempi illustrano come le soluzioni IT possano favorire la partecipazione democratica dei soci all'interno delle cooperative di dati, garantendo un coinvolgimento significativo e contribuendo alla creazione di un ambiente di governance inclusivo e trasparente.

2.6. Gestione del Consenso e Controllo dei Dati da Parte dei Soci.

Per la realizzazione della *Data Platform*, è fondamentale che le cooperative forniscano strumenti che permettano ai soci di mantenere un controllo costante e selet-

tivo sui propri dati personali, in linea con il Regolamento Generale sulla Protezione dei Dati (*GDPR*) e il Regolamento UE n. 868/2022 [1], altrimenti noto come *Data Governance Act*, in particolare l'art. 12. Questo controllo deve includere la possibilità di dare e revocare il consenso all'uso dei propri dati o di specifiche categorie di dati che confluiscono nel *Data Lake*. In questo modo, i soci possono gestire dinamicamente le loro informazioni personali, adattando le autorizzazioni alle proprie esigenze nel tempo.

Ad esempio, una *dashboard* intuitiva consentirebbe ai soci di visualizzare e gestire i propri dati conferiti, controllando quali dati sono disponibili nel *Data Lake* e modificando le autorizzazioni per l'uso di tali dati. *Un design user-friendly* della dashboard renderebbe semplice revocare il consenso quando necessario, utilizzando interfacce chiare e accessibili. Inoltre, è cruciale assicurarsi che le modifiche effettuate dai soci siano propagate immediatamente attraverso tutti i sistemi, per evitare ritardi nella revoca dei consensi.

Un'altra soluzione pratica è rappresentata dall'implementazione di applicazioni *mobile* o *web-based* che permettono ai soci di aggiornare le loro preferenze di *privacy* e gestire i consensi in tempo reale. Ad esempio, le notifiche push possono informare i soci ogni volta che vi è una richiesta di accesso ai loro dati, consentendo loro di approvare o negare l'accesso in tempo reale. Questo approccio non solo aumenta la sicurezza, ma anche la trasparenza, mantenendo i soci informati sulle attività relative ai loro dati.

Oltre agli strumenti specifici, è importante considerare due aspetti chiave della governance dei dati, quella individuale e quella collettiva:

(i) *Governance Individuale*: ogni socio deve avere la possibilità di gestire autonomamente le autorizzazioni relative ai propri dati. Ad esempio, un tool di gestione dei consensi permette ai soci di concedere o revocare il permesso per l'uso dei loro dati in modo semplice e immediato. Un approccio basato sulla "*privacy by design*" assicura che il controllo sui dati sia nelle mani degli utenti sin dalle fasi iniziali della raccolta delle informazioni. Per garantire trasparenza e conformità, è utile implementare audit trail che traccino tutte le modifiche ai consensi, offrendo un registro dettagliato delle autorizzazioni concesse o revocate.

(ii) *Governance Collettiva e Sociale:* all'interno della cooperativa, i processi democratici devono consentire ai soci di discutere e decidere collettivamente sull'uso dei dati. Piattaforme di discussione e strumenti di voto permettono ai soci di

[1] Il Regolamento (UE) 2022/868 del Parlamento Europeo e del Consiglio del 30 maggio 2023, noto come Data Governance Act, si concentra sulla gestione europea dei dati e modifica il Regolamento (UE) 2018/1724. Questo regolamento, pubblicato nella Gazzetta Ufficiale dell'Unione Europea il 3 giugno 2022, è entrato in vigore venti giorni dopo e si applica dal 24 settembre 2023, come specificato nell'art. 38. Il Data Governance Act è un elemento chiave della strategia digitale europea, mirato a rafforzare il mercato dei dati. Integra le disposizioni della Direttiva UE 2019/1024, che riguarda l'apertura e il riutilizzo dei dati del settore pubblico. Sul termine «*governance*» si può fare riferimento a D. POLETTI, *A proposito di fonti nell' "ecosistema digitale"* in F. RICCI (a cura di), *Principi, clausole generali, argomentazione e fonti del diritto*, Milano, 2018, p. 345.

partecipare attivamente alla *governance* dei dati, esprimendo le loro opinioni e contribuendo alle decisioni collettive. Tuttavia, è essenziale che le decisioni collettive rispettino le preferenze individuali di consenso, evitando che le scelte della maggioranza compromettano il controllo personale sui dati sensibili.

In sintesi, una gestione efficace del consenso e della *governance* dei dati richiede un bilanciamento tra le esigenze di controllo individuale e le dinamiche democratiche collettive della cooperativa. Implementando strumenti adeguati, si può garantire che ogni socio mantenga il controllo sui propri dati personali, rispettando al contempo le decisioni e le necessità della comunità cooperativa [2].

3. Costruzione della *Data Platform*.

3.1. Fasi chiave.

La realizzazione di una *Data Platform* efficace per cooperative di dati richiede una pianificazione e un'implementazione oculate. Questo capitolo esplorerà le fasi chiave coinvolte nella costruzione di tale piattaforma, concentrandosi sull'armonizzazione, l'anonimizzazione e l'esposizione dei dati ai soci.

3.2. Armonizzazione dei dati.

L'armonizzazione dei dati costituisce il primo passo fondamentale nella costruzione della *Data Platform*. Le aziende partecipanti alla cooperativa possono contribuire con dati provenienti da una varietà di fonti e in diversi formati. L'obiettivo è integrare questi dati in un unico ambiente coeso e standardizzato, in modo che possano essere facilmente accessibili e utilizzati per analisi e sviluppo di soluzioni.

Per raggiungere questo obiettivo, è necessario implementare processi e strumenti per l'acquisizione, la pulizia e la trasformazione dei dati. Tecnologie di integrazione dei dati, come ETL (*Extract*, *Transform*, *Load*), possono essere impiegate per automatizzare questi processi e garantire la coerenza e l'accuratezza dei dati.

Inoltre, è importante stabilire standard e linee guida per la qualità dei dati al fine di garantire che i dati armonizzati siano affidabili e utilizzabili per le analisi e le decisioni aziendali. Questo può includere la definizione di metadati e ontologie per descrivere e organizzare i dati in modo coerente.

L'armonizzazione dei dati è una fase cruciale della realizzazione della *Data Platform*, che coinvolge l'integrazione, la standardizzazione e la normalizzazione dei dati provenienti da fonti diverse. Di seguito si riportano alcune indicazioni utili

---

[2] Per approfondire la questione della circolazione dei dati e il loro sfruttamento economico, si possono consultare diverse fonti. Tra queste, F. BRAVO, *Il diritto a trattare dati personali nello svolgimento dell'attività economica*, Milano, 2018 e N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, 2019.

da tenere in considerazione in fase di armonizzazione dei dati all'interno del proprio sistema cooperativo:

(i) *Criticità*: durante l'armonizzazione dei dati, è possibile imbattersi in dati provenienti da sistemi *legacy* con formati diversi, dati non strutturati da sensori IoT e dati semistrutturati da fonti esterne come social media o fonti *web*;

(ii) *Semantica:* utilizzare *tool* e tecniche di integrazione dei dati per unire e consolidare le fonti di dati eterogenee, definire uno schema unificato per la rappresentazione dei dati e creare un *data dictionary* per documentare la semantica e la struttura dei dati;

(iii) *Strategia*: valutare attentamente le esigenze degli utenti finali e definire una strategia di armonizzazione dei dati che tenga conto delle loro necessità e dei requisiti di *business*, garantendo al contempo la conformità normativa e la qualità dei dati.

3.3. Anonimizzazione dei dati.

Una volta armonizzati, i dati devono essere anonimizzati per proteggere la *privacy* e la riservatezza delle informazioni sensibili. L'anonimizzazione dei dati comporta la rimozione o la trasformazione delle informazioni identificative in modo che i dati non possano essere collegati a individui specifici.

Esistono diverse tecniche di anonimizzazione dei dati, tra cui l'eliminazione diretta delle informazioni identificative, la sostituzione con valori generici o la generazione di dati sintetici. È importante valutare attentamente le tecniche da utilizzare in base al contesto e alle esigenze specifiche della cooperativa e dei suoi soci. Ad esempio, l'applicazione di tecniche di *k-anonymity*[3] garantisce che ogni registrazione non sia distinguibile da almeno altre k-1 registrazioni, riducendo il rischio di re-identificazione.

Un'altra tecnica avanzata è la *privacy* differenziale[4], che aggiunge rumore ai dati in modo controllato per garantire che le informazioni aggregate non compromettano la *privacy* dei singoli individui. Questa tecnica è particolarmente utile quando si desidera pubblicare statistiche aggregate senza rivelare dati sensibili.

Inoltre, è essenziale garantire che l'anonimizzazione dei dati non comprometta l'utilità e l'integrità delle informazioni. Ciò significa che i dati anonimizzati devo-

---

[3] L'articolo di L. SWEENEY, *K-anonymity: A model for protecting privacy*, in *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, Pittsburgh, 2002, 10(5), pp. 557-570, introduce il modello di *k-anonymity* per la protezione della *privacy*, proponendo un metodo per anonimizzare i dati in modo che ogni individuo non sia distinguibile da almeno altri $k-1$ individui nei dati rilasciati, riducendo così il rischio di re-identificazione.

[4] C. DWORK*, Differential privacy: A survey of results*, in M. AGRAWAL *et al.* (eds.), *Theory and Applications of Models of Computation*, Springer, 2008, pp. 1-19, fornisce una panoramica sui risultati della *privacy* differenziale, un quadro matematico che garantisce la protezione della *privacy* degli individui nei set di dati statistici. La *privacy* differenziale limita il rischio che la partecipazione di un singolo individuo in un database possa essere rilevata, assicurando che le analisi statistiche effettuate sul *database* rimangano accurate e utili.

no ancora essere utili per le analisi e le elaborazioni previste senza rivelare informazioni sensibili sugli individui.

Si riportano di seguito una serie di considerazioni da tenere in conto in fase di anonimizzazione dei dati in un contesto cooperativo:

(i) *Protezione dei dati*: durante l'anonimizzazione dei dati, è possibile sostituire le informazioni identificative con identificatori anonimi, rimuovere attributi sensibili o applicare tecniche di *masking* per proteggere la riservatezza dei dati.

(ii) *Tecniche a disposizione*: è consigliabile applicare tecniche di anonimizzazione come la generalizzazione, l'*hashing* e la randomizzazione per proteggere i dati sensibili. Tecniche avanzate come la *k-anonymity* e la privacy differenziale sono fondamentali per garantire la privacy dei dati e la conformità alle normative. Non meno importante è il coinvolgimento di esperti di sicurezza e *privacy* dei dati nella progettazione delle politiche di anonimizzazione, oltre alla conduzione di valutazioni di rischio per identificare e mitigare potenziali vulnerabilità nella protezione dei dati.

(iii) *Normativa*: assicurarsi di comprendere le normative sulla protezione dei dati applicabili e adottare un approccio basato sul rischio per determinare il livello appropriato di anonimizzazione dei dati, bilanciando la necessità di proteggere la *privacy* degli utenti con l'utilità e l'accessibilità dei dati per fini legittimi.

3.4. Esposizione dei dati.

Una volta armonizzati e anonimizzati, i dati devono essere resi accessibili ai soci all'interno della cooperativa. Questo può essere realizzato attraverso l'esposizione dei dati tramite *API* (*Application Programming Interface*) o altri meccanismi di accesso.

Le *API* consentono ai soci di accedere ai dati in modo programmatico e di integrarli nelle proprie applicazioni e processi aziendali. È importante progettare *API* robuste e sicure che garantiscano un accesso controllato e protetto ai dati, rispettando al contempo i requisiti di sicurezza e *privacy*.

Inoltre, possono essere sviluppati strumenti e *dashboard* per consentire ai soci di esplorare e visualizzare i dati in modo intuitivo e interattivo. Questi strumenti possono facilitare l'analisi dei dati e favorire la scoperta di *insight* e tendenze significative.

La *Data Platform* deve anche fornire meccanismi per monitorare e tracciare l'accesso e l'utilizzo dei dati da parte dei soci, al fine di garantire la conformità normativa e la sicurezza dei dati.

L'esposizione dei dati risulta quindi fondamentale per consentire agli stakeholder di accedere e utilizzare i dati in modo sicuro e conforme alle normative sulla *privacy*. Ecco alcuni esempi, *best practice* e considerazioni pratiche:

(i) *Accesso ai dati*: è possibile fornire accesso ai dati tramite API, dashboard interattive, o report personalizzati, consentendo agli utenti di esplorare e analizzare i dati in base alle proprie esigenze;

(ii) *Controllo e Monitoraggio*: implementare meccanismi di controllo degli accessi per garantire che solo gli utenti autorizzati possano accedere ai dati, fornire strumenti di governance dei dati per monitorare e tracciare l'utilizzo dei dati, e garantire la sicurezza dei dati attraverso l'uso di crittografia e autenticazione forte;

(iii) *Condivisione*: coinvolgere gli *stakeholder* chiave nella progettazione delle interfacce utente e delle *API* per garantire che soddisfino le loro esigenze e aspettative, e fornire documentazione dettagliata e supporto tecnico per facilitare l'adozione e l'utilizzo dei dati da parte degli utenti finali.

4. Utilizzo dei dati e obiettivi della *Data Platform.*

4.1. Creazione di *Benchmark* – analisi di un caso pratico.

La *Data Platform* non è solo un contenitore per i dati, ma un ecosistema dinamico che facilita l'utilizzo dei dati per raggiungere obiettivi specifici e creare valore per i suoi membri. In questo capitolo, esploreremo i diversi modi in cui i dati possono essere utilizzati all'interno della piattaforma e gli obiettivi che essa mira a raggiungere.

Uno degli obiettivi principali della *Data Platform* è facilitare la creazione di *Benchmark* per valutare le prestazioni e le tendenze nel settore. I *Benchmark* forniscono un punto di riferimento per confrontare le prestazioni aziendali e identificare aree di miglioramento. La creazione di B*enchmark* implica processi rigorosi di standardizzazione e confronto, come descritto da Gray (1993)[5] e Bechhofer et al. (2013)[6]. Utilizzando i dati anonimizzati forniti dai soci, è possibile creare *Benchmark* accurati e significativi che consentano alle aziende di valutare le proprie prestazioni rispetto ai concorrenti e al mercato nel suo complesso.

La *Data Platform* può fornire strumenti e metriche standardizzate per la creazione di *Benchmark*, nonché la possibilità di confrontare le prestazioni su diverse dimensioni, come ad esempio la produttività, l'efficienza operativa e la soddisfa-

---

[5] J. GRAY, *The Benchmark Handbook for Database and Transaction Processing Systems*, San Francisco, 1993 fornisce un approfondito quadro di riferimento e una serie di *Benchmark* per valutare le prestazioni dei sistemi di gestione di database e transazioni. Questo tipo di risorse sono fondamentali per gli sviluppatori e gli esperti del settore per valutare le prestazioni dei loro sistemi e confrontarli con altri sul mercato.

[6] L'articolo di S. BECHHOFER-I. BUCHAN-D. DE ROURE-P. MISSIER-J. AINSWORTH-J. BHAGAT-C. GOBLE, *Why linked data is not enough for scientists*, in *Future Generation Computer Systems*, 2013, 29(2), pp. 599-611, mette in discussione l'idea che i dati collegati siano sufficienti per gli scienziati. I dati collegati, un concetto centrale nel web semantico, si concentrano sulla connessione dei dati per consentire una migliore interoperabilità e scoperta delle informazioni. Tuttavia, Bechhofer et al. evidenziano le sfide che gli scienziati affrontano nell'utilizzo dei dati collegati nel loro lavoro quotidiano, sottolineando che ciò potrebbe non essere abbastanza per soddisfare le esigenze complesse della ricerca scientifica.

zione del cliente. Inoltre, i *Benchmark* possono essere aggiornati regolarmente per riflettere le ultime tendenze e cambiamenti nel settore, consentendo alle aziende di rimanere competitive e reattive.

Nel contesto delle cooperative di dati, un esempio significativo è rappresentato dalla creazione di *Benchmark* nel settore della sanità. Questo caso di studio illustra come una cooperativa di dati possa utilizzare una *Data Platform* per migliorare la qualità delle cure e ottimizzare i processi sanitari attraverso l'analisi comparativa dei dati.

Immaginiamo una rete di ospedali e cliniche che decidono di collaborare per condividere dati sanitari in modo sicuro e anonimo. L'obiettivo principale è creare un sistema di *Benchmark* che consenta a ciascuna struttura di confrontare le proprie prestazioni con quelle di altre organizzazioni simili, identificando le migliori pratiche e le aree di miglioramento.

La prima fase del progetto prevede la raccolta dei dati da ciascun ospedale partecipante. I dati possono includere informazioni sui pazienti, trattamenti, esiti clinici, tempi di attesa, e altre metriche rilevanti. La *Data Platform* armonizza questi dati, standardizzandoli in un formato comune. Questo passaggio è cruciale per garantire che i dati provenienti da diverse fonti siano comparabili e integrati senza discrepanze.

Per proteggere la *privacy* dei pazienti, i dati raccolti vengono anonimizzati rimuovendo le informazioni personali identificabili e garantendo che i dati possano essere utilizzati per analisi senza compromettere la riservatezza dei pazienti. La *Data Platform* implementa anche robusti protocolli di sicurezza per proteggere i dati da accessi non autorizzati e garantire il rispetto delle normative sulla *privacy*, come il *GDPR*.

Con i dati armonizzati e anonimizzati, la cooperativa può iniziare l'analisi comparativa. La *Data Platform* utilizza strumenti di intelligenza artificiale e machine learning per analizzare le performance degli ospedali su diverse metriche. Ad esempio, può confrontare i tassi di successo delle operazioni chirurgiche, i tempi di recupero dei pazienti, o la gestione delle malattie croniche.

I risultati di queste analisi vengono presentati sotto forma di *Benchmark*, che mostrano come ciascun ospedale si posiziona rispetto agli altri. Questi *Benchmark* non solo identificano le strutture con le migliori performance, ma evidenziano anche le pratiche e i protocolli che contribuiscono ai risultati superiori.

Gli ospedali partecipanti possono utilizzare i *Benchmark* per identificare le aree in cui sono necessari miglioramenti e adottare le migliori pratiche identificate. Ad esempio, se un ospedale scopre che il suo tempo medio di recupero post-operatorio è più lungo rispetto ad altri, può analizzare le procedure degli ospedali con tempi di recupero più brevi e implementare modifiche nei propri protocolli.

La cooperativa di dati assicura che i *Benchmark* siano aggiornati regolarmente con nuovi dati. Questo monitoraggio continuo consente agli ospedali di vedere i progressi nel tempo e di adattare le loro strategie in base ai cambiamenti nelle performance. Inoltre, la piattaforma può fornire alert automatici quando vengono rilevate variazioni significative nei dati, permettendo interventi tempestivi.

L'adozione di una *Data Platform* per la creazione di *Benchmark* nel settore sanitario offre numerosi benefici. Gli ospedali possono migliorare la qualità delle cure offerte, ridurre i costi operativi e aumentare la soddisfazione dei pazienti. La cooperativa di dati favorisce una cultura di collaborazione e condivisione delle conoscenze, promuovendo l'innovazione e l'adozione di pratiche basate su evidenze concrete.

In conclusione, questo caso di studio dimostra come una cooperativa di dati, supportata da una *Data Platform* avanzata, possa trasformare il settore sanitario attraverso l'analisi comparativa e la condivisione delle migliori pratiche, migliorando così la qualità delle cure e l'efficienza operativa.

4.2. *Data Marketplace* – analisi di un caso pratico.

Un'altra importante funzione della *Data Platform* è facilitare lo scambio e la vendita responsabile dei dati attraverso un *Data Marketplace*. Il *Data Marketplace* offre un ambiente sicuro e strutturato in cui i soci possono acquistare e vendere dati in base alle proprie esigenze e interessi.

Attraverso il *Data Marketplace*, le aziende possono monetizzare i propri dati fornendo accesso a terzi interessati a utilizzarli per analisi, ricerca di mercato o sviluppo di prodotti e servizi. Allo stesso tempo, le aziende possono accedere a nuovi dati e fonti di informazione che possono arricchire le loro analisi e decisioni aziendali.

La *Data Platform* può implementare un sistema di catalogo per consentire ai soci di visualizzare e cercare i dati disponibili nel *Data Marketplace*, nonché meccanismi per gestire le transazioni e garantire la sicurezza e la *privacy* dei dati durante lo scambio (Gopal & Goyal, 2014 [7]; Spiekermann, 2015 [8]). Inoltre, possono essere introdotti modelli di licenza flessibili per consentire agli acquirenti di pagare in base all'uso o alla quantità di dati richiesti.

Descriviamo ora un caso di studio che illustra l'implementazione di un *Data Marketplace* all'interno di una *Data Platform* per una cooperative di dati. Nel set-

---

[7] Il lavoro di R. GOPAL-M. GOYAL, *Privacy and security in the age of big data: An empirical study of user awareness, behavior, and concerns*, in *Journal of Information Privacy and Security*, 2014, 10(2), pp. 21-40, si basa su un'indagine empirica che esplora come gli utenti percepiscano e affrontino le questioni legate alla *privacy* e alla sicurezza nell'era del *big data*. Questo studio fornisce un'analisi approfondita sul livello di consapevolezza degli utenti, i loro comportamenti e le preoccupazioni riguardanti la protezione dei dati personali.

[8] Dall'altro lato, lo studio di S. SPIEKERMANN, *The challenges of personal data markets and privacy*, in *Electronic Markets*, *The International Journal on Networked Business*, 2015, 22(4), pp. 161-167, si concentra sulle sfide dei mercati dei dati personali, sottolineando le complessità e le implicazioni etiche associate alla commercializzazione dei dati personali. L'A. esamina criticamente le dinamiche dei mercati del dato e le questioni di privacy che sorgono quando i dati personali diventano oggetto di scambio commerciale, offrendo un'analisi informativa delle implicazioni di questo fenomeno emergente.

tore delle telecomunicazioni ad esempio, l'implementazione di un *Data Marketplace* rappresenta un'opportunità significativa per le aziende di condividere, acquistare e vendere dati in modo sicuro e regolamentato. Questo caso di studio esplora come una cooperativa di dati possa creare un ecosistema di *Data Marketplace* che promuove l'innovazione e l'efficienza attraverso l'uso strategico dei dati.

Iniziamo considerando diverse compagnie di telecomunicazioni che decidono di unirsi in una cooperativa di dati per creare un *Data Marketplace*. Ogni azienda contribuisce con diversi tipi di dati, tra cui dati di rete, dati sui clienti, dati sulle prestazioni e dati di utilizzo. La *Data Platform* armonizza questi dati, standardizzandoli in formati compatibili e assicurando che siano facilmente accessibili e interpretabili da tutti i membri della cooperativa.

Per rispettare le normative sulla *privacy* e proteggere le informazioni sensibili, i dati condivisi vengono anonimizzati. In questo modo si cerca di garantire che i dati utilizzati per le analisi non rivelino informazioni personali identificabili. La *Data Platform* implementa anche rigorose misure di sicurezza per prevenire accessi non autorizzati e garantire la sicurezza complessiva dei dati.

Una volta che i dati sono stati raccolti, standardizzati e anonimizzati, la cooperativa può iniziare a costruire il *Data Marketplace*. Questo mercato digitale consente alle aziende di telecomunicazioni di pubblicare i loro *dataset* in cataloghi strutturati, dove possono essere ricercati e acquistati da altri membri della cooperativa o da terze parti autorizzate. Il *marketplace* offre strumenti avanzati di ricerca e filtro, permettendo agli utenti di trovare rapidamente i dati rilevanti per le loro esigenze.

Vengono riportati di seguito alcuni esempi di utilizzo dei dati nel *Marketplace*:

(i) analisi delle Prestazioni di Rete: un'azienda di telecomunicazioni può acquistare dati sulle prestazioni di rete da altre aziende per confrontare le proprie metriche di prestazione con quelle dei concorrenti. Questi dati possono aiutare a identificare aree di miglioramento nella qualità del servizio e nelle operazioni di rete;

(ii) personalizzazione dei Servizi ai Clienti: i dati sui clienti provenienti da diverse fonti possono essere utilizzati per creare modelli di comportamento dei consumatori più accurati. Le aziende possono quindi utilizzare queste informazioni per personalizzare le offerte di servizi e migliorare l'esperienza del cliente;

(iii) sviluppo di Nuovi Prodotti e Servizi: accedendo ai dati di utilizzo e alle tendenze di mercato, le aziende possono identificare nuove opportunità di business e sviluppare prodotti e servizi innovativi. Ad esempio, analizzando i dati di utilizzo delle *app*, un'azienda potrebbe decidere di sviluppare una nuova funzione per migliorare l'*engagement* degli utenti.

Il *Data Marketplace* offre diverse modalità di monetizzazione dei dati. Le aziende possono vendere i loro dataset a pagamento, offrire abbonamenti per l'accesso continuo a dati aggiornati o partecipare a modelli di revenue sharing basati sull'uso dei dati. Questo crea nuove fonti di reddito per le aziende di telecomunicazioni e incentiva la condivisione dei dati all'interno della cooperativa.

L'implementazione di un *Data Marketplace* nel settore delle telecomunicazioni offre numerosi vantaggi. Le aziende possono ottimizzare le loro operazioni, miglio-

rare la qualità dei servizi offerti e sviluppare nuovi prodotti basati su *insights* derivati dai dati. La cooperativa di dati favorisce una maggiore collaborazione e trasparenza tra le aziende, promuovendo un ecosistema di innovazione e crescita.

In conclusione, questo caso di studio dimostra come una cooperativa di dati, supportata da una *Data Platform* robusta e sicura, possa trasformare il settore delle telecomunicazioni attraverso la creazione di un *Data Marketplace*. Questo approccio non solo migliora l'efficienza e la qualità dei servizi, ma apre anche nuove opportunità di *business* e incentiva la collaborazione tra le aziende.

4.3. Sviluppo di nuovi prodotti e servizi personalizzati.

Un altro utilizzo significativo dei dati all'interno della *Data Platform* è la facilitazione dello sviluppo di nuovi prodotti e servizi personalizzati.

Ad esempio, consideriamo il *settore della sanità*. Utilizzando i dati raccolti dai vari membri della cooperativa, è possibile analizzare i modelli di salute della popolazione, identificare tendenze e predire potenziali rischi per la salute individuale. Con queste informazioni, è possibile sviluppare applicazioni e servizi digitali che offrono consigli personalizzati per uno stile di vita sano, monitoraggio delle condizioni di salute e gestione delle terapie. Questo approccio non solo migliora l'esperienza del paziente, ma contribuisce anche a ridurre i costi sanitari complessivi attraverso la prevenzione e la gestione proattiva delle malattie.

In ambito *e-commerce*, i dati raccolti possono essere impiegati per analizzare i comportamenti degli utenti, le preferenze di acquisto e le tendenze di mercato. Utilizzando queste informazioni, le aziende possono personalizzare l'esperienza di shopping online, offrendo raccomandazioni di prodotti mirate, sconti personalizzati e promozioni speciali. Questo approccio non solo migliora la soddisfazione del cliente e aumenta le vendite, ma consente anche alle aziende di ottimizzare la gestione dell'inventario e la pianificazione della domanda, riducendo gli sprechi e migliorando l'efficienza operativa.

Un ulteriore esempio può essere individuato nel *settore dei trasporti e della logistica*, in cui i dati raccolti dalla cooperativa possono essere impiegati per ottimizzare le rotte di consegna, migliorare la pianificazione dei trasporti e ridurre i tempi di attesa per i clienti. Utilizzando queste informazioni, le aziende possono implementare sistemi di gestione della flotta basati sull'intelligenza artificiale per prevedere e prevenire guasti, pianificare itinerari efficienti e ridurre i costi operativi. Questo approccio non solo migliora l'efficienza e la puntualità dei servizi di trasporto, ma contribuisce anche a ridurre l'impatto ambientale attraverso una gestione più sostenibile delle risorse e dei carichi.

4.4. Obiettivi della *Data Platform.*

Oltre a facilitare la creazione di *benchmark* e il funzionamento di un *Data Marketplace*, la *Data Platform* mira a raggiungere una serie di obiettivi chiave:

(i) *favorire la collaborazione*: la *Data Platform* promuove la collaborazione tra società informatiche e altri attori interessati, consentendo loro di condividere conoscenze, risorse e dati per raggiungere obiettivi comuni;

(ii) *promuovere l'innovazione*: fornendo accesso ai dati e alle risorse necessarie, la *Data Platform* stimola l'innovazione e lo sviluppo di nuove soluzioni e servizi basati sui dati;

(iii) *sostenere la crescita economica*: facilitando lo scambio e l'accesso ai dati, la *Data Platform* contribuisce alla creazione di un'economia dati più dinamica e inclusiva, che favorisce la crescita economica e la creazione di posti di lavoro;

(iv) *garantire la conformità normativa*: la *Data Platform* si impegna a rispettare le normative sulla *privacy* e la protezione dei dati, garantendo che l'utilizzo dei dati avvenga in conformità con le leggi e i regolamenti applicabili.

In conclusione, l'utilizzo dei dati all'interno della *Data Platform* è orientato verso il raggiungimento di obiettivi concreti che contribuiscono alla creazione di valore per i suoi membri e per l'intero ecosistema. La piattaforma fornisce gli strumenti e le risorse necessarie per sfruttare appieno il potenziale dei dati e favorire l'innovazione e lo sviluppo sostenibile.

5. Sicurezza e *privacy* dei dati.

5.1. Introduzione.

La sicurezza e la *privacy* dei dati sono di fondamentale importanza all'interno di una *Data Platform* cooperativa, specialmente quando si tratta di dati sensibili provenienti da fonti diverse. In questo capitolo, esploreremo le misure e le pratiche adottate per garantire un'adeguata protezione dei dati e rispettare la *privacy* degli utenti.

5.2. Architettura sicura.

L'architettura della *Data Platform* deve essere progettata con un focus particolare sulla sicurezza, garantendo che i dati siano protetti da accessi non autorizzati e minacce esterne. Ciò richiede l'implementazione di misure di sicurezza a più livelli, inclusi *firewall*, crittografia dei dati, controlli di accesso e monitoraggio dell'attività.

Una pratica comune è quella di adottare un approccio a difesa in profondità, che prevede la stratificazione di diversi livelli di protezione per garantire una sicurezza completa. Ciò include la segmentazione della rete, la crittografia *end-to-end* e l'implementazione di politiche di sicurezza rigorose per proteggere i dati in ogni fase del loro ciclo di vita.

5.3. Crittografia e pseudonimizzazione.

La crittografia dei dati è uno strumento fondamentale per proteggere la riservatezza e l'integrità dei dati all'interno della *Data Platform*. La crittografia *end-to-end* viene utilizzata per proteggere i dati durante il trasporto e lo storage, garantendo che solo gli utenti autorizzati possano accedere alle informazioni sensibili.

Inoltre, la pseudonimizzazione dei dati viene utilizzata per sostituire le informazioni identificative con identificatori anonimi, proteggendo la *privacy* degli utenti mentre consentendo comunque l'analisi e l'utilizzo dei dati per fini legittimi. È importante adottare un approccio basato sul rischio per determinare il livello appropriato di crittografia e pseudonimizzazione da applicare ai dati in base alla loro sensibilità e al contesto operativo.

5.4. Applicazione dei principi di *privacy by design* e *privacy by default*

La *Data Platform* è progettata e implementata conformemente ai principi di *Privacy by Design* e *Privacy by Default*, garantendo che la *privacy* degli utenti sia integrata sin dall'inizio nel processo di progettazione e che le impostazioni predefinite proteggano la privacy degli utenti senza necessità di interventi aggiuntivi.

Questo include la definizione di politiche di gestione dei dati che regolano la raccolta, l'elaborazione e l'archiviazione dei dati, nonché l'implementazione di meccanismi di consenso e controllo per gli utenti sulle proprie informazioni personali. Inoltre, vengono adottate misure per minimizzare la raccolta e l'elaborazione dei dati personali solo ai fini strettamente necessari.

5.5. Considerazioni pratiche.

Al fine di garantire la sicurezza e la protezione dei dati possono essere adottate alcune misure all'interno della propria organizzazione. A titolo esemplificativo, si indicano di seguito le principali:

(i) *formazione del personale*: il personale deve essere adeguatamente addestrato sulle migliori pratiche di sicurezza e *privacy* dei dati per garantire la conformità e la sicurezza continua dei dati;

(ii) *monitoraggio, audit e gestione dei log*: vengono implementati sistemi di monitoraggio e audit per rilevare e rispondere prontamente alle minacce alla sicurezza e alle violazioni della *privacy* dei dati. È inoltre importante mantenere registri dettagliati delle attività di accesso ai dati e monitorare i *log* per individuare e rispondere tempestivamente a eventuali anomalie o accessi non autorizzati;

(iii) *collaborazione con le autorità di regolamentazione*: la cooperazione con le autorità di regolamentazione e le organizzazioni di standardizzazione è essenziale per garantire la conformità alle leggi e ai regolamenti sulla protezione dei dati.

In conclusione, la sicurezza e la *privacy* dei dati sono priorità fondamentali all'interno della *Data Platform*, e vengono adottate misure e pratiche per garantire

una protezione efficace dei dati sensibili e rispettare la *privacy* degli utenti in conformità con le normative vigenti.

6. Tecnologie chiave della *Data Platform.*

6.1. Innovazione e scalabilità.

La realizzazione di una *Data Platform* efficace richiede l'adozione di tecnologie innovative e scalabili in grado di gestire grandi volumi di dati in modo efficiente e sicuro. Questo capitolo esplorerà le tecnologie chiave utilizzate nella costruzione e nell'operatività della *Data Platform*, con particolare attenzione alla *Data Federation*, al *Virtual Data Lake* e ad applicazioni di tecniche di Intelligenza Artificiale. Concetti come la *Data Federation* e i *Virtual Data Lake* permettono un'integrazione e un accesso trasparente ai dati distribuiti [9].

6.2. *Data Federation*.

La *Data Federation* è una tecnologia che consente l'integrazione e l'accesso a dati distribuiti in modo trasparente attraverso una rete di sistemi eterogenei. Essenzialmente, la *Data Federation* permette di creare una vista unificata dei dati provenienti da fonti diverse, senza la necessità di trasferire fisicamente i dati in un unico *repository* centrale.

Un esempio di *Data Federation* è l'utilizzo di strumenti di virtualizzazione dei dati che consentono agli utenti di accedere e interrogare dati provenienti da database distribuiti, servizi *cloud* e altre fonti, come se fossero memorizzati in un unico *database* virtuale. Questo approccio riduce la complessità dell'integrazione dei dati e consente agli utenti di ottenere una visione completa e aggiornata dei dati senza dover eseguire operazioni di trasferimento e sincronizzazione.

Le *best practice* per l'implementazione della *Data Federation* includono la definizione di una strategia di virtualizzazione dei dati chiara e scalabile, la valutazione delle prestazioni e della sicurezza delle soluzioni di virtualizzazione dei dati

---

[9] L'articolo di A.Y. HALEVY-M.J. FRANKLIN-D. MAIER, *Principles of dataspace systems*, in *ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems*, 2006, pp. 1-9, introduce i principi dei sistemi di *dataspace*. Un *dataspace* è un ambiente che integra dati provenienti da diverse fonti e formati senza richiedere uno schema unificato, il che è correlato al concetto di *Data Federation*. La *Data Federation* implica l'accesso e la gestione di dati da fonti multiple mantenendole nel loro formato originale, permettendo di eseguire *query* senza spostare i dati. Il sistema di *dataspace* va oltre la federazione tradizionale poiché consente l'integrazione incrementale, supportando livelli variabili di schema e qualità del servizio, facilitando l'accesso a dati eterogenei per diverse applicazioni. Inoltre, un *Virtual Data Lake* può essere considerato come un'estensione di questo concetto, dove un ambiente virtuale aggrega dati da diverse fonti senza spostare fisicamente i dati in un unico *repository*, consentendo un accesso centralizzato e analisi su dati distribuiti.

e l'adozione di standard e protocolli aperti per garantire l'interoperabilità tra sistemi e applicazioni.

6.3. *Virtual Data Lake.*

Il *Virtual Data Lake* è un concetto che si basa sull'idea di un "lago" centralizzato di dati virtuali, in cui i dati sono archiviati in un formato nativo e possono essere accessibili e analizzati in modo flessibile e scalabile [10]. Il *Virtual Data Lake* offre un ambiente unificato per l'archiviazione e l'analisi dei dati provenienti da fonti diverse, consentendo agli utenti di esplorare e interrogare i dati in modo autonomo e senza vincoli di prestazioni.

Un esempio di *Virtual Data Lake* è l'implementazione di un'infrastruttura basata su *cloud* per l'archiviazione e l'elaborazione dei dati, che consente di creare un ambiente di analisi centralizzato e distribuito su più regioni geografiche. Attraverso strumenti di gestione dei dati e analisi avanzata, gli utenti possono accedere e analizzare i dati in tempo reale, ottenendo insight significativi per supportare decisioni aziendali critiche.

Le *best practice* per l'implementazione del *Virtual Data Lake* includono la progettazione di un'architettura scalabile e resiliente per gestire grandi volumi di dati, l'adozione di tecnologie di sicurezza avanzate per proteggere i dati sensibili e la definizione di politiche di *governance* dei dati per garantire l'integrità e la conformità dei dati.

6.4. Soluzioni IT di IA per l'estrazione delle informazioni a supporto delle decisioni.

Vengono applicate sempre più tecnologie avanzate di intelligenza artificiale (IA) per estrarre informazioni significative dai dati e supportare il processo decisionale. L'integrazione dell'AI e del machine learning nelle piattaforme dati ne potenzia le capacità, fornendo approfondimenti analitici avanzati (Jordan & Mitchell, 2015 [11];

---

[10] Nel suo articolo D.J. ABADI, *Data management in the cloud: Limitations and opportunities*, in *IEEE Data Eng. Bull*., 2009, 32(1), pp. 3-12 discute le sfide e i vantaggi della gestione dei dati negli ambienti *cloud*. Tra le limitazioni, evidenzia i problemi di coerenza dei dati, latenza e i compromessi tra modelli di coerenza forte e eventuale. Tra le opportunità, Abadi sottolinea i benefici della scalabilità, efficienza dei costi e flessibilità del cloud, che possono trasformare le applicazioni data-intensive fornendo risorse e servizi *on-demand*, rendendo la gestione dei dati più dinamica e robusta.

[11] Cfr. M.I. JORDAN-T.M. MITCHELL, *Machine learning: Trends, perspectives, and prospects*, in *Science*, 2015, 349(6245), pp. 255-260, i quali esplorano le tendenze attuali e future del *machine learning*, sottolineando l'importanza di questo campo in vari settori. Gli autori discutono come il machine learning possa beneficiare dalla cooperativa di dati, dove la condivisione collaborativa dei dati tra diverse entità può migliorare l'addestramento dei modelli grazie alla disponibilità di *dataset* più ampi e diversificati. Tuttavia, evidenziano anche le sfide legate alla *privacy*, alla sicurezza e all'etica dei dati in un contesto cooperativo.

Goodfellow et al., 2016 [12]). Di seguito sono riportati alcuni esempi di soluzioni IT in cui viene applicata l'IA:

(i) *analisi predittive*: le soluzioni di IA utilizzano algoritmi predittivi per identificare pattern e tendenze nei dati storici, consentendo alle cooperative di anticipare eventi futuri e prendere decisioni proactive. Ad esempio, un modello predittivo basato su IA può essere utilizzato per prevedere la domanda di prodotti o servizi in base alle condizioni di mercato e alle stagionalità, consentendo alle cooperative di ottimizzare la pianificazione e la produzione;

(ii) *raccomandazioni personalizzate*: le tecnologie di IA analizzano i dati sui comportamenti e le preferenze degli utenti per generare raccomandazioni personalizzate su prodotti, servizi o contenuti. Ad esempio, un sistema di raccomandazione basato su IA può suggerire ai soci della cooperativa i prodotti o i servizi più rilevanti in base al loro storico di acquisti o alle loro interazioni precedenti, migliorando così l'esperienza complessiva dei soci e aumentando la fedeltà;

(iii) *analisi testuale e del sentiment*: gli algoritmi di analisi del linguaggio naturale (NLP) e di *sentiment analysis* consentono alle cooperative di estrarre *insight* dai dati testuali, come recensioni dei clienti, commenti sui *social media* o *feedback* degli utenti. Ad esempio, un sistema di analisi sentimentale basato su IA può analizzare i sentimenti espressi nei commenti dei soci sulla piattaforma *online* della cooperativa, identificando eventuali preoccupazioni o opinioni negative e consentendo alla cooperativa di rispondere prontamente per migliorare l'esperienza dei soci;

(iv) *automazione dei processi decisionali*: le soluzioni di IA possono automatizzare i processi decisionali complessi, riducendo la dipendenza dall'intervento umano e accelerando i tempi di risposta. Ad esempio, un sistema di supporto decisionale basato su IA può analizzare i dati finanziari e operativi della cooperativa, identificare anomalie o tendenze significative e suggerire azioni correttive o opportunità di ottimizzazione per il *management*;

(v) *rilevamento delle frodi*: gli algoritmi di IA possono essere utilizzati per rilevare comportamenti fraudolenti o anomali nei dati finanziari o transazionali della cooperativa. Ad esempio, un sistema di rilevamento delle frodi basato su IA può analizzare i pattern di transazioni dei soci e identificare comportamenti sospetti, come transazioni non autorizzate o tentativi di frode, consentendo alla cooperativa di intervenire tempestivamente e mitigare i rischi associati.

---

[12] L'opera di I. GOODFELLOW-Y. BENGIO-A. COURVILLE, *Deep Learning*, MIT Press, 2016, offre una trattazione completa del *deep learning*, coprendo principi teorici, architetture e applicazioni pratiche. Nell'ambito di una cooperativa di dati, il *deep learning* può trarre vantaggio dalla condivisione di dati tra diverse organizzazioni, permettendo l'addestramento di modelli neurali su *dataset* più ricchi e vari. Questo approccio collaborativo può migliorare le prestazioni dei modelli, ma richiede anche l'implementazione di robusti meccanismi di gestione della *privacy* e della sicurezza dei dati condivisi.

6.5. Considerazioni pratiche.

Al momento di implementare le tecnologie chiave della *Data Platform*, è importante considerare alcuni aspetti pratici, tra cui:

(i) *scalabilità*: le tecnologie devono essere in grado di gestire grandi volumi di dati e di scalare in modo efficiente per soddisfare le esigenze in continua evoluzione della *Data Platform*;

(ii) *sicurezza*: è fondamentale implementare misure di sicurezza robuste per proteggere i dati da accessi non autorizzati e garantire la conformità normativa;

(iii) *interoperabilità*: le tecnologie devono essere interoperabili con i sistemi esistenti e compatibili con gli standard del settore per garantire l'interconnessione e l'interoperabilità dei dati;

(iv) *facilità d'uso*: le tecnologie devono essere intuitive e *user-friendly* per consentire agli utenti di accedere e utilizzare i dati in modo efficace e senza difficoltà.

In conclusione, l'adozione delle tecnologie chiave della *Data Platform* come la *Data Federation* e il *Virtual Data Lake* è essenziale per creare un ambiente flessibile e scalabile per la gestione e l'analisi dei dati. Utilizzando queste tecnologie in modo efficace e conforme alle *best practice*, è possibile massimizzare il valore dei dati e favorire l'innovazione e lo sviluppo all'interno della cooperativa di dati e soluzioni tecnologiche.

7. Implementazione della *Data Platform* per la cooperativa.

7.1. Introduzione.

L'implementazione della *Data Platform* richiede una pianificazione attenta, l'identificazione dei requisiti specifici dei membri della cooperativa e l'adozione di tecnologie e processi adeguati a garantire il successo dell'iniziativa. In questo capitolo, esamineremo i passaggi chiave coinvolti nell'implementazione della *Data Platform* per la Cooperativa, fornendo dettagli su ciascuna fase e offrendo suggerimenti pratici per massimizzare i benefici ottenuti.

7.2. Analisi dei requisiti e definizione degli obiettivi.

La fase iniziale dell'implementazione della *Data Platform* per la Cooperativa prevede l'analisi dei requisiti e la definizione degli obiettivi. È essenziale comprendere le esigenze specifiche dei membri della cooperativa, nonché gli obiettivi strategici dell'organizzazione nel suo complesso. Alcuni passaggi chiave in questa fase includono:

(i) *raccolta dei requisiti*: coinvolgere attivamente i membri della cooperativa per comprendere le loro esigenze e aspettative in termini di gestione dei dati e analisi;

(ii) *definizione degli obiettivi*: stabilire obiettivi chiari e misurabili per l'implementazione della *Data Platform*, tenendo conto delle esigenze e degli obiettivi dei membri della cooperativa;

(iii) *valutazione delle risorse*: valutare le risorse disponibili, inclusi *budget*, personale e tecnologia, necessarie per l'implementazione e il mantenimento della *Data Platform*.

7.3. Progettazione e architettura della *Data Platform.*

La realizzazione della *Data Platform* nel contesto cooperativo si sviluppa in tre passaggi fondamentali. In primo luogo, si procede con la selezione delle tecnologie, identificando e valutando le opzioni disponibili in base alle esigenze specifiche della cooperativa. Il secondo passaggio riguarda la progettazione dell'infrastruttura, definendo l'architettura necessaria, inclusi *server*, *storage*, reti e strumenti di monitoraggio. Infine, si implementano politiche di sicurezza e *governance* dei dati per garantire la protezione e la conformità normativa dei dati condivisi tra i membri della cooperativa.

7.4. Sviluppo e implementazione della *Data Platform.*

Il processo comprende lo sviluppo e l'integrazione dei componenti della piattaforma, insieme alla configurazione dei processi di gestione e analisi dei dati. Inizia con lo sviluppo e l'integrazione di componenti *software* e hardware necessari, come database, strumenti di analisi, *API* e interfacce utente. Si prosegue con la configurazione dei processi di ingestione, trasformazione e analisi dei dati, assicurando prestazioni ottimali e conformità alle normative sulla *privacy* e sicurezza. Infine, si eseguono test approfonditi per verificare il corretto funzionamento della piattaforma e garantire la qualità e affidabilità dei dati elaborati.

7.5. Formazione e supporto agli utenti.

Una volta completata l'implementazione, è essenziale fornire formazione e supporto agli utenti della *Data Platform* per garantire il suo utilizzo efficace ed efficiente. In questa fase sono previste la creazione di materiali didattici, sessioni di formazione e supporto agli utenti:

(i) *creazione di materiali didattici*: creare manuali utente, video *tutorial* e guide rapide per aiutare gli utenti a comprendere e utilizzare la *Data Platform*;

(ii) *sessioni di formazione*: organizzare sessioni di formazione pratiche per familiarizzare gli utenti con le funzionalità e le possibilità della *Data Platform*;

(iii) *supporto continuo*: fornire supporto tecnico continuo agli utenti per risolvere eventuali problemi o domande che possono sorgere durante l'utilizzo della piattaforma.

7.6. Monitoraggio e ottimizzazione continua.

Una volta che la *Data Platform* è operativa, è importante monitorare le sue prestazioni e ottimizzarla continuamente per garantire il suo funzionamento ottimale nel tempo. Questa fase coinvolge il monitoraggio delle metriche chiave, l'identificazione e la risoluzione dei problemi e l'implementazione di miglioramenti incrementali.

8. Benefici e impatti della *Data Platform* Cooperativa.

8.1. Introduzione.

La *Data Platform* Cooperativa offre una serie di benefici tangibili e impatti positivi sia per i membri della cooperativa che per l'intero ecosistema. In questo capitolo, esamineremo i principali benefici e impatti derivanti dall'implementazione e dall'utilizzo della piattaforma.

8.2. Benefici per i membri della cooperativa.

La creazione di una *Data Platform* porta numerosi vantaggi ai membri della cooperativa. In primo luogo, l'accesso ai dati diventa notevolmente più semplice. La piattaforma permette ai membri di accedere facilmente ai dati condivisi, eliminando la complessità e riducendo i tempi che normalmente sarebbero necessari per cercare e ottenere i dati necessari.

In secondo luogo, la piattaforma migliora significativamente la collaborazione tra i membri. Grazie a questo strumento, diventa più facile scambiare conoscenze e lavorare insieme per risolvere problemi comuni. Questo ambiente collaborativo stimola anche lo sviluppo di nuove soluzioni innovative, favorendo un continuo miglioramento delle pratiche operative.

Un altro importante beneficio è la riduzione dei costi. Condividere le risorse e le infrastrutture della *Data Platform* tra i vari membri della cooperativa permette di abbattere i costi operativi, migliorando l'efficienza complessiva dell'organizzazione. Questo approccio condiviso riduce la necessità di investimenti individuali in tecnologie costose, consentendo un utilizzo più efficace delle risorse disponibili.

Infine, l'accesso a dati di alta qualità e a strumenti analitici avanzati permette ai membri della cooperativa di prendere decisioni più informate e basate sui dati. Questo vantaggio non solo migliora le performance individuali, ma aumenta anche la competitività dell'intera organizzazione. Grazie a decisioni più accurate e tempestive, la cooperativa può rispondere meglio alle sfide del mercato e cogliere nuove opportunità di crescita.

8.3. Impatti sull'ecosistema cooperativo.

La cooperativa di dati ha un impatto significativo sull'intero ecosistema in vari modi.

Per prima cosa, promuove la crescita economica. La condivisione e l'utilizzo dei dati stimolano l'innovazione e favoriscono lo sviluppo di nuove soluzioni e servizi. Questo dinamismo non solo beneficia i singoli membri, ma contribuisce alla crescita economica complessiva dell'ecosistema cooperativo, creando nuove opportunità di mercato e migliorando la competitività.

In secondo luogo, migliora la qualità della vita dei membri della comunità. Le soluzioni e i servizi sviluppati grazie ai dati condivisi possono avere un impatto positivo diretto sulle persone. Ad esempio, miglioramenti nei servizi sanitari basati su analisi avanzate dei dati possono offrire cure migliori e più accessibili. Allo stesso modo, soluzioni innovative per l'agricoltura sostenibile possono aumentare la produttività e la sostenibilità, migliorando le condizioni di vita degli agricoltori e delle comunità rurali.

Un altro importante impatto riguarda lo sviluppo sostenibile. La cooperativa di dati promuove pratiche commerciali responsabili che rispettano l'ambiente e le comunità locali. Utilizzando i dati in modo etico e sostenibile, si favorisce un approccio che contribuisce al benessere generale dell'ecosistema, proteggendo le risorse naturali e sostenendo lo sviluppo a lungo termine.

Infine, la cooperativa di dati aumenta la resilienza e l'adattabilità dell'ecosistema. Grazie alla capacità di analizzare e rispondere rapidamente ai cambiamenti socio-economici, la cooperativa aiuta a costruire un sistema più resiliente e sostenibile. Questa capacità di adattamento è cruciale per affrontare le sfide future e garantire la sostenibilità dell'ecosistema nel lungo periodo, permettendo alle comunità di prosperare anche in condizioni avverse.

In sintesi, la *Data Platform* Cooperativa offre una serie di benefici tangibili e impatti positivi sia per i membri della cooperativa che per l'intero ecosistema. Sfruttando il potenziale dei dati condivisi in modo collaborativo e responsabile, la cooperativa promuove la crescita economica, il miglioramento della qualità della vita e lo sviluppo sostenibile dell'intero ecosistema.

9. Sfide e possibili soluzioni nell'implementazione della *Data Platform* Cooperativa.

L'implementazione e la gestione di una *Data Platform* Cooperativa possono essere affrontate con fiducia, ma non senza sfide. Questo capitolo esplorerà le principali difficoltà che le aziende possono incontrare nel processo di implementazione della *Data Platform* Cooperativa e fornirà suggerimenti pratici per superarle con successo.

Le sfide di natura tecnologica sono spesso tra le prime da affrontare. Integrare i

sistemi esistenti all'interno della *Data Platform* può richiedere tempo e risorse significative. Una possibile soluzione è quella di adottare un approccio graduale, identificando i requisiti chiave e implementando soluzioni pilota per testare l'efficacia dell'integrazione. Inoltre, garantire la scalabilità della piattaforma è essenziale per far fronte ai crescenti volumi di dati nel tempo. Utilizzare tecnologie e architetture scalabili può aiutare a garantire che la piattaforma possa crescere e adattarsi alle esigenze mutevoli della cooperativa nel tempo.

Oltre alle sfide di natura tecnologica, ci sono anche sfide di natura organizzativa da considerare. Adottare una cultura basata sulla condivisione dei dati e sulla collaborazione può essere difficile per alcune organizzazioni, richiedendo un cambiamento culturale significativo. Coinvolgere attivamente i membri della cooperativa nel processo di cambiamento culturale e fornire formazione e supporto possono aiutare a promuovere una mentalità aperta e collaborativa. Inoltre, definire politiche e procedure per la *governance* dei dati può essere complesso e richiedere un consenso tra i membri della cooperativa. Coinvolgere tutti i membri nel processo decisionale e sviluppare politiche chiare e trasparenti può aiutare a garantire che le esigenze e le normative di tutti i partecipanti siano rispettate.

Un'altra sfida significativa riguarda la sicurezza e la *privacy* dei dati. Garantire la protezione dei dati sensibili all'interno della *Data Platform* è fondamentale per mantenere la fiducia tra i membri della cooperativa. Implementare robuste misure di sicurezza e crittografia dei dati, così come procedure di accesso e controllo degli utenti, può aiutare a proteggere i dati sensibili da accessi non autorizzati. Inoltre, rispettare le normative sulla *privacy* dei dati e altre regolamentazioni può essere complesso e richiedere un costante monitoraggio e aggiornamento. Collaborare con esperti legali e consulenti per garantire la conformità normativa e aggiornare regolarmente le politiche e le procedure può aiutare a ridurre il rischio di violazioni della *privacy* dei dati.

Infine, affrontare sfide di adozione e utilizzo è essenziale per garantire il successo a lungo termine della *Data Platform* Cooperativa. Assicurarsi che gli utenti adottino attivamente la piattaforma e ne sfruttino appieno le funzionalità può essere una sfida. Fornire formazione e supporto agli utenti, così come creare incentivi e ricompense per promuovere l'utilizzo e l'adozione della piattaforma, può aiutare a superare questa sfida. Inoltre, mantenere il supporto e l'interesse per la *Data Platform* nel tempo può essere difficile senza una governance efficace e un continuo coinvolgimento dei membri. Implementare un modello di governance solido e coinvolgere attivamente i membri della cooperativa nel processo decisionale e nell'evoluzione continua della piattaforma può contribuire a garantire il successo e la sostenibilità a lungo termine della *Data Platform* Cooperativa.

Affrontare queste sfide richiede un approccio strategico e collaborativo da parte di tutti i membri della cooperativa, nonché un impegno a lungo termine per garantire il successo e la sostenibilità della *Data Platform* Cooperativa. Con la giusta pianificazione e le giuste risorse, queste sfide possono essere superate con successo, consentendo ai membri della cooperativa di trarre pieno vantaggio dai benefici della condivisione dei dati e della collaborazione.

10. Conclusioni.

La creazione e l'implementazione di una *Data Platform* Cooperativa rappresentano un passo significativo verso una gestione più efficace e collaborativa dei dati all'interno delle organizzazioni. Attraverso questo percorso, abbiamo esplorato i molteplici benefici che una cooperativa di dati può offrire, insieme alle sfide che possono sorgere lungo il cammino.

In primo luogo, abbiamo visto come una *Data Platform* Cooperativa possa migliorare l'accesso ai dati, promuovere la collaborazione tra i membri dell'organizzazione e migliorare la qualità delle decisioni aziendali attraverso l'analisi avanzata dei dati. Questi vantaggi possono tradursi in un maggiore successo operativo, una migliore competitività sul mercato e un impatto positivo sulla crescita e la sostenibilità dell'organizzazione nel lungo periodo.

Tuttavia, il viaggio verso l'implementazione di una *Data Platform* Cooperativa non è privo di sfide. Abbiamo esaminato le complessità tecniche, organizzative, di sicurezza e di adozione che le aziende possono affrontare durante questo processo. Tuttavia, abbiamo anche fornito una serie di possibili soluzioni e suggerimenti pratici per superare queste sfide con successo, sfruttando al meglio i benefici della condivisione dei dati e della collaborazione all'interno della cooperativa.

Infine, abbiamo riflettuto sull'importanza della *governance* dei dati, della trasparenza e dell'*engagement* continuo dei membri della cooperativa nel garantire il successo e la sostenibilità a lungo termine della *Data Platform* Cooperativa. Con il giusto impegno e una *leadership* efficace, una cooperativa di dati può diventare un motore di innovazione e crescita per l'organizzazione e per l'intera comunità.

In conclusione, la *Data Platform* Cooperativa rappresenta un'opportunità unica per le aziende di collaborare e condividere conoscenze per ottimizzare l'uso dei dati condivisi. Attraverso una pianificazione oculata, una governance solida e un impegno costante per l'innovazione e la collaborazione, le aziende possono realizzare il pieno potenziale della condivisione dei dati e guidare il cambiamento positivo all'interno della propria organizzazione e oltre.

Capitolo XXXVI

Cooperative di dati e principio di neutralità dei fornitori di servizi di intermediazione dei dati: questioni critiche

Daniele Sborlini

Abstract: The introduction of the "services of data cooperatives" by Reg. EU 2022/868 (Data Governance Act, DGA) aims to enhance control by data subjects, one-person undertakings and SMEs over data that relates to them, while addressing the distortions of competition currently present in the internal market. Data cooperatives may lead to a more inclusive and equitable society, ensuring the respect of European values, fundamental rights and rules. However, the inclusion of the services of data cooperatives among "data intermediation services" and the "one-size-fits-all" approach pursued in regulating the latter by the DGA present significant critical issues. In particular, the application to data cooperatives of the DGA requirements relating to the "neutrality" of data intermediaries with regard to the data exchanged set out in Art. 12(a) DGA risks severely limiting the ability of data cooperatives to achieve their objectives and thus preventing the beneficial effects expected from them. This paper therefore aims to investigate the functions pursued by the provisions on neutrality established by the DGA in order to deepen their application in the specific case of data cooperatives and offer first suggestions that may contribute to tackle the aforementioned issues, so as to ensure an application of these provisions consistent with the goals of the EU data strategy.

1. Introduzione.

In coerenza con gli obiettivi della strategia europea per i dati [1], l'Unione europea ha adottato il Reg. UE n. 868/2022 sulla *governance* europea dei dati [2], con cui è stato delineato anche un quadro di notifica e controllo per la fornitura di «servizi di intermediazione dei dati» [3], all'interno dei quali è stata introdotta la categoria, prima inedita a livello legislativo, dei «servizi di cooperative di dati» [4].

Le cooperative di dati, variamente definite in letteratura ed emerse nella prassi in molteplici forme [5], possono intendersi essenzialmente come organizzazioni composte da singoli individui o imprese, i quali si associano entro un soggetto collettivo, normalmente facendo confluire al suo interno i dati (personali e non) di propria afferenza in modo da socializzarne il "valore" [6], per esigenze connesse al potenzia-

[1] COMMISSIONE EUROPEA, Comunicazione del 19 febbraio 2020, intitolata «*Una strategia europea per i dati*», COM(2020)86 final.

[2] Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo alla *governance* europea dei dati e che modifica il regolamento (UE) 2018/1724 (Regolamento sulla *governance* dei dati), nella traduzione in inglese denominato "*Data Governance Act*" ("DGA").

[3] Sull'oggetto del *Data Governance Act*, v. l'art. 1, par. 1, Reg. cit. Per la definizione di «servizio di intermediazione dei dati», v. l'art. 2, n. 11, Reg. cit. In Italia, l'autorità competente per i servizi di intermediazione dei dati, preposta ai compiti relativi alla procedura di notifica e al monitoraggio della conformità dei fornitori di tali servizi al regolamento, è stata individuata dal d.lgs. 7 ottobre 2024, n. 144 (recante norme di adeguamento della normativa nazionale alle disposizioni del Reg. cit.) nell'Agenzia per l'Italia digitale (AgID).

[4] I «servizi di cooperative di dati» sono definiti all'art. 2, n. 15, Reg. cit., su cui v. *infra*, par. 3.1.

[5] Sulle cooperative di dati (definizione, tratti caratterizzanti, modelli operativi emersi nella prassi), v. ad es. G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, in *Rivista trimestrale di diritto pubblico*, 2022, 4, p. 985 ss.; F. BRAVO, *Le cooperative di dati*, in *Contratto e impresa*, 2023, 3, p. 768 ss.; AA.VV., *Mapping the Landscape of Data Intermediaries – Emerging Models for More Inclusive Data Governance*, Publications Office of the European Union, Luxembourg, 2023, p. 47 ss.; E. BIETTI-A. ETXEBERRIA-M. MANNAN-J. WONG, *Data Cooperatives in Europe: A Legal and Empirical Investigation*, White Paper created as part of *The New School's Platform Cooperativism Consortium and Harvard University's Berkman Klein Center for Internet & Society* Research Sprint, 2021, p. 8 ss.; M. MICHELI-M. PONTI-M. CRAGLIA-A. BERTI, *Emerging Models of Data Governance in the Age of Datafication*, in *Big Data & Society*, 2020, Vol. 7, n. 2, p. 7 ss.; AA.VV., *Unlocking the Power of Digital Commons: Data Cooperatives as a Pathway for Data Sovereign, Innovative and Equitable Digital Communities*, in *Digital*, 2023, Vol. 3, n. 3, p. 147 ss.; AA.VV., *White Paper on the Data Governance Act*, in *CiTiP Working Paper Series*, 2021, p. 29 ss.; T. HARDJONO-A. PENTLAND, *Data Cooperatives: Towards a Foundation for Decentralized Personal Data Management*, in *arXiv.org*, 2019, p. 2 ss.

[6] Sulla nozione di "valore" dei dati, v. ad es. F. BRAVO-J. VALERO TORRIJOS, *Data in the Public*

mento del loro controllo su tali dati sia in termini di rafforzare la tutela dei propri diritti e libertà rispetto al trattamento di tali dati sia per valorizzare gli stessi nel perseguimento di scopi altruistici, commerciali o di altra natura, tramite la condivisione di tali dati con soggetti terzi e lo svolgimento di altre attività. Le cooperative di dati, riportabili al più ampio fenomeno della cooperazione e, segnatamente, del *platform cooperativism* [7], agiscono nell'interesse dei propri membri sulla base di una "*governance*" collettiva sui dati "conferiti" da questi ultimi, al cui esercizio è deputata l'organizzazione stessa, secondo le decisioni assunte dai membri tramite le logiche democratiche caratterizzanti il movimento cooperativo, seppur nel rispetto delle scelte dei singoli sui dati di loro afferenza.

Con l'introduzione dei servizi di cooperative di dati nel DGA, l'UE ha dunque inteso promuovere un fenomeno innovativo, collocabile entro la cornice del "neomutualismo digitale" [8], il quale è caratterizzato, in opposizione alle dinamiche capitalistiche dominanti, dalle logiche mutualistiche e solidaristiche della cooperazione che, quando applicate ai processi di trasformazione digitale, aprono a un modello di crescita non solo dell'economia, ma anche della società in cui tali imprese operano [9]. Ciò, invero, è coerente con la visione dell'Unione, la cui strategia per i dati è improntata sulla centralità della persona e la solidarietà sociale, in contrasto alle dinamiche "estrattive" che caratterizzano allo stato la *data economy*, per realizzare invece un ecosistema ove i benefici ottenibili dai dati siano distribuiti equamente tra tutti gli attori sociali e, specialmente, in favore di quelli più piccoli e vulnerabili [10].

A ogni modo, la riconduzione delle cooperative di dati tra i «servizi di intermediazione dei dati» e la conseguente applicazione a tali soggetti delle condizioni stabilite per la fornitura di tali servizi (art. 12 Reg. cit.) [11], prive di differenziazioni che tengano conto delle peculiarità delle cooperative di dati stesse, presenta significati-

---

Sector and Data Valorisation, in *European Review of Digital Administration & Law (ERDAL)*, 2022, Vol. 3, n. 2, p. 7 ss.; V. ZENO-ZENCOVICH, *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, in *Media Laws*, 2018, 2, p. 2 ss.

[7] V. ad es. M. MANNAN-S. PEK, *Solidarity in the Sharing Economy: The Role of Platform Cooperatives at the Base of the Pyramid*, Berlin/Heidelberg, 2021; G. BUZZAO-F. RUSTICHELLI, Who Owns the World*? Il cooperativismo di piattaforma oggi. Intervista a Trebor Sholz*, in *Pandora rivista*, 2020, 3, pp. 168-177.

[8] Cfr. F. BRAVO, *Le cooperative di dati*, cit., p. 764 ss. (anche in riferimento al documento «*Le cooperative e le sfide dell'innovazione digitale: il neomutualismo in dieci tesi*», elaborato da esponenti del mondo accademico per Legacoop e Fondazione PICO Innovazione Cooperativa, richiamato al suo interno).

[9] *Ibidem*.

[10] *Ibidem*, p. 765 ss. V. altresì L. PETRONE, *Il mercato digitale europeo e le cooperative di dati*, in *Contratto e impresa*, 2023, 3, p. 800 ss. Questi profili sono approfonditi *infra*, par. 2 ss.

[11] Il rispetto delle condizioni per la fornitura di servizi di intermediazione dei dati previste dall'art. 12 Reg. cit. è assistito dalla previsione di sanzioni in caso di violazioni, la cui determinazione è rimessa agli Stati membri (art. 34 Reg. cit.): in Italia, è stato previsto che l'AgID possa adottare sanzioni amministrative pecuniarie di entità variabile, che per le imprese possono giungere fino al 6 per cento del fatturato mondiale totale annuo del precedente esercizio (art. 4 d.lgs. n. 144/2024).

ve criticità [12]. Tra queste, risultano di particolare rilievo le questioni poste dall'applicazione dei requisiti del DGA relativi alla "neutralità" degli intermediari dei dati con riguardo ai dati scambiati, ossia del divieto per l'intermediario di utilizzare i dati per i quali fornisce i servizi di intermediazione per scopi diversi dalla messa a disposizione degli stessi agli "utenti dei dati" e del correlato obbligo di fornire i medesimi servizi attraverso una persona giuridica distinta (art. 12, lett. *a*), Reg. cit.) [13].

Detta neutralità, infatti, rischia di limitare fortemente l'operatività delle cooperative di dati e il potenziale benefico che tali organizzazioni possono apportare all'intera collettività. Diversamente dai modelli diffusi nella prassi, ad esempio, è dubbio se nella costruzione delineata dal DGA le cooperative di dati possano implementare modalità di valorizzazione dei dati direttamente in favore dei membri, mediante la condivisione dei dati all'interno dell'organizzazione o sulla base di funzioni e servizi *data-driven*; non è chiaro, peraltro, se risultino legittime le attività di analisi sui dati dei membri cooperatori, svolte ad esempio per ottenere le informazioni necessarie per supportare efficacemente questi ultimi nelle attività di negoziazione dei termini di utilizzo dei dati con soggetti esterni alla cooperativa di dati o nell'esercizio dei loro diritti, oppure da licenziare all'esterno per garantire la sostenibilità economica della cooperativa stessa [14].

In questo scenario, il presente contributo si propone di indagare le funzioni perseguite dalle disposizioni sulla neutralità stabilite dal Reg. UE n. 868/2022, per approfondirne l'operatività allo specifico caso delle cooperative di dati e offrire dei primi spunti interpretativi che possano contribuire alle ricerche necessarie per affrontare le suddette criticità, affinché si possa addivenire a un'applicazione delle stesse coerente con le esigenze del neo-mutualismo digitale e l'obiettivo ricercato dall'Unione di realizzare un mutamento di paradigma nella *data economy*, tale da assicurare in detto contesto il rispetto dei valori e dei diritti fondamentali dell'UE.

2. La neutralità dei fornitori di servizi di intermediazione dei dati riguardo ai dati scambiati nel *Data Governance Act.*

2.1. Le funzioni della neutralità nel contesto della nuova modalità "europea" di *governance* dei dati.

Le disposizioni sulla neutralità dei fornitori di servizi di intermediazione dei dati rispetto ai dati scambiati tra "interessati" o "titolari dei dati" da una parte e "uten-

[12] Per una specifica panoramica delle questioni giuridiche ravvisabili rispetto alle cooperative di dati, v. F. BRAVO, *Le cooperative di dati*, cit., p. 798 ss.

[13] La riconduzione dell'art. 12, lett. *a*), Reg. cit. alla neutralità dei fornitori di servizi di *data intermediation* riguardo ai dati scambiati tra titolari dei dati o interessati e utenti dei dati emerge dal *considerando* n. 33 Reg. cit., rispetto al quale si v. *infra*, par. 2.1. Sulla definizione di «utente dei dati», v. *infra*, nota n. 15.

[14] Questi profili sono approfonditi *infra*, par. 3.

ti dei dati" dall'altra [15] hanno un rilievo centrale nel *Data Governance Act*, in quanto funzionali al conseguimento degli stessi obiettivi perseguiti dal regolamento, rappresentati essenzialmente *(i)* dall'aumento della fiducia nel *data sharing*, in particolare per il tramite dell'istituzione di meccanismi che assicurino il controllo da parte di interessati e titolari dei dati sui propri dati e *(ii)* dalla garanzia del buon funzionamento di un'economia *data-driven* competitiva [16].

Il DGA mira infatti al superamento del presente stato delle cose, connotato da una ridotta circolazione e, dunque, valorizzazione dei dati nell'UE e dalla presenza di distorsioni della concorrenza nel mercato interno [17], derivante principalmente dalle dinamiche del capitalismo estrattivo che caratterizzano attualmente l'economia dei dati [18].

---

[15] Per la definizione di "interessato" ("*data subject*"), v. l'art. 4, n. 1, Reg. UE n. 679/2016, al quale rinvia l'art. 2, n. 7, Reg. UE n. 868/2022. Le definizioni di «titolare dei dati» e «utente dei dati» sono stabilite rispettivamente all'art. 2, nn. 8 e 9, Reg. cit. Nella presente sede, interessati e titolari dei dati saranno anche definiti collettivamente come "fornitori dei dati" o "*data suppliers*".

[16] Rispetto agli obiettivi perseguiti dall'UE mediante il DGA, v. il *considerando* n. 5 Reg. cit.

[17] Cfr. *considerando* nn. 1-3 Reg. cit.

[18] In questa sede, non è possibile né d'interesse addentrarsi nel complesso dibattito relativo al "mercato dei dati" (o meglio, ai "mercati dei dati") e alle differenziazioni ravvisabili per descrivere i fenomeni variamente riportati alle dinamiche dei "*two-sided markets*" nel mercato digitale (su tali questioni, v. V. ZENO-ZENCOVICH, *Do "Data Markets" Exist?*, in *Media Laws*, 2019, 2, pp. 1-17; J. BERGÉ-S. M. GRUMBACH-V. ZENO-ZENZOVICH, *The 'Datasphere', Data Flows beyond Control, and the Challenges for Law and Governance*, in *European Journal of Comparative Law and Governance*, 2018, Vol. 5, n. 2, pp. 144-178; G. RESTA, *Digital Platforms and the Law: Contested Issues*, in *Media Laws*, 2018, 1, pp. 231-248). Basti ricordare, in estrema sintesi, che i modelli commerciali prevalenti in questi contesti, adottati in particolare dalle società che dominano tali mercati (le "*Big Tech*"), si basano sullo sfruttamento commerciale dei dati (personali e non) degli utenti. Ne deriva, in particolare per gli utenti costituiti da singoli individui e operatori economici di più ridotte dimensioni (imprese individuali, *start up* e PMI), uno scarso controllo sui dati di propria afferenza, secondo un modello che li esclude dalla definizione delle scelte sull'utilizzo degli stessi e dalla partecipazione alla loro valorizzazione, basato invero sull'imposizione di condizioni unilaterali e sulla logica del "prendere o lasciare", aggravata dai rilevanti effetti di rete e di dipendenza ("*lock-in*") che si riscontrano nelle piattaforme digitali (in merito, rispetto in particolare ai profili di *data protection*, v. S. RODOTÀ, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Roma-Bari, 2014, p. 27 ss.; F. BRAVO, *Il commercio elettronico di dati personali*, in T. PASQUINO-A. RIZZO-M. TESCARO (a cura di), *Questioni attuali in tema di commercio elettronico*, Napoli, 2020, p. 83 ss.; G. BUTTARELLI, *Le sfide dei "*Big Data*" tra evoluzione tecnologica, etica e interessi collettivi*, in *Gnosis*, 2017, 2, p. 31 ss.; con specifico riguardo alla patrimonializzazione del dato personale, v. altresì V. RICCIUTO, *L'equivoco della* privacy*. Persona* vs *dato personale*, Napoli, 2022, p. 105 ss.). Più ampiamente, tali dinamiche determinano una progressiva concentrazione dei dati e dei fattori per estrarne il valore in capo alle *Big Tech*, con plurimi impatti negativi sulla concorrenza (su tali profili, v. ad es. A. MANTELERO, Big Data*: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, in *Il diritto dell'informazione e dell'informatica*, 2012, 1, p. 135 ss.; G. COLANGELO, Big data*, piattaforme digitali e* antitrust, in *Mercato Concorrenza Regole*, 2016, 3, pp. 425-460). Per affrontare le questioni *antitrust* dei mercati digitali, com'è noto, l'Unione europea ha da ultimo adottato il Reg. UE n. 1925/2022 ("*Digital Markets Act*"), avente il fine di «contribuire al corretto funzionamento del mercato interno stabilendo

Per sviluppare ulteriormente il mercato interno digitale e una società e un'economia dei dati «antropocentriche, affidabili e sicure» [19], coerentemente ai valori e ai diritti fondamentali dell'UE [20], il DGA ravvisa l'esigenza di migliorare le condizioni per il *data sharing* realizzando un quadro armonizzato per gli scambi di dati e stabilendo alcuni requisiti orizzontali per la *governance* dei dati, riconoscendo ai servizi di intermediazione dei dati un «ruolo essenziale nell'economia dei dati» per promuovere e sostenere la condivisione dei dati [21].

In questo contesto, la neutralità dei servizi di intermediazione dei dati emerge nel Reg. UE n. 868/2022 quale "requisito chiave" mediante il quale conseguire entrambi gli obiettivi del regolamento. La neutralità riguardo ai dati scambiati ha infatti un duplice rilievo, operando come «elemento essenziale» per aumentare la fiducia e il controllo nei servizi di infomediazione di tutte le parti coinvolte nelle transazioni di dati, abilitando al contempo un «ambiente competitivo» per la condivisione dei dati [22]; ciò, in funzione, più ampiamente, della realizzazione di uno "spazio europeo comune dei dati" connotato da quella parità di condizioni che consente alle imprese di competere «sulla qualità dei servizi e non sulla quantità dei dati che controllano» [23].

Nell'articolato del regolamento sulla *governance* dei dati, la neutralità trova la sua principale espressione all'art. 12, lett. *a*), Reg. cit. [24], che impone ai fornitori di servizi di intermediazione dei dati due requisiti interdipendenti: *(i)* il divieto di impiego dei dati per i quali sono forniti servizi di intermediazione dei dati per scopi diversi dalla messa a disposizione degli stessi verso gli utenti dei dati e *(ii)* l'obbligo di fornire detti servizi tramite una persona giuridica distinta.

---

norme armonizzate volte a garantire, per tutte le imprese, che i mercati nel settore digitale nei quali sono presenti *gatekeeper* (controllori dell'accesso) siano equi e contendibili in tutta l'Unione, a vantaggio degli utenti commerciali e degli utenti finali» (art. 1, par. 1, Reg. cit.).

[19] *Considerando* n. 3 Reg. UE n. 868/2022.

[20] L'UE come «unione di valori» è espressamente sancita dall'art. 2 del Trattato sull'Unione europea. Sul rilievo della dimensione valoriale nell'approccio UE ai dati e alla sovranità digitale, v. G. FINOCCHIARO, *Data and Digital Sovereignty*, in *European Review of Digital Administration & Law (ERDAL)*, 2022, Vol. 3, n. 2, p. 10.

[21] *Considerando* n. 27 Reg. cit.

[22] *Considerando* n. 33 Reg. cit.

[23] *Considerando* n. 2 Reg. cit. Al riguardo, si è parlato del DGA anche come misura di «*demonopolization of data*» (AA.VV., *Towards a Digital Ecosystem of Trust: Ethical, Legal and Societal Implications*, in *Opinio Juris in Comparatione*, 2021, 1, p. 143 ss.).

[24] Sul requisito di cui all'art. 12, lett. *a*), Reg. cit. quale espressione della neutralità imposta ai fornitori di servizi di intermediazione dei dati, cfr. ad es. G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit., p. 982 (ove è sottolineato come il principio di neutralità sia formulato quale «primo tra i requisiti sostanziali» per la fornitura di tali servizi); F. BRAVO, *Le cooperative di dati*, cit., p. 798; L. VON DITFURTH, *Datenmärkte, Datenintermediäre und der Data Governance*, Berlin/Boston, 2024, p. 340; AA.VV., *White Paper on the Data Governance Act*, cit., p. 31 ss.; G. CAROVANO-M. FINCK, *Regulating Data Intermediaries: The impact of the Data Governance Act on the EU's Data Economy*, in *Computer Law & Security Review*, 2023, 50, p. 8.

Il divieto di utilizzo dei dati scambiati ha una duplice portata [25]. Da un lato, impedisce all'intermediario di utilizzare tali dati per proprie finalità (neutralità come limitazione della finalità), le quali potrebbero sostanziarsi in forme di uso dei dati "dirette" (ad esempio, attività di *data analytics* per sviluppare propri prodotti o servizi) o "indirette" (è il caso della comunicazione o cessione di tali dati a terzi per scopi di lucro); dall'altro, vieta la prestazione verso gli interessati, i titolari dei dati e gli utenti dei dati di servizi *data-based* differenti da quelli di intermediazione (neutralità come limitazione dei servizi basati sui dati scambiati) [26].

Questa prima componente della neutralità si rinviene anche in altre condizioni stabilite per la fornitura dei servizi di *data intermediation* dall'art. 12 DGA, che precisano la portata del divieto di utilizzo dei dati rispetto a profili specifici. Trattasi, in particolare: *(i)* della limitazione imposta agli intermediari circa l'uso dei metadati raccolti ai fini della fornitura del servizio di intermediazione, ammessa solo per scopi di "sviluppo" di tale servizio (art. 12, lett. *c*), Reg. cit.) [27]; *(ii)* della limitazione per il fornitore dei servizi di intermediazione di convertire in altri formati i dati oggetto dello scambio, ammessa solo laddove la conversione abbia lo scopo di migliorare l'interoperabilità dei dati e sia richiesta dell'utente dei dati o prescritta dal diritto UE o sia volta ad assicurare l'armonizzazione con le norme internazionali o europee sui dati e sia offerta ai fornitori dei dati la possibilità di non partecipare alla conversione (art. 12, lett. *d*), Reg. cit.), parimenti stabilita per circoscrivere le operazioni effettuabili sui dati dall'intermediario a quelle che siano nell'interesse degli attori della transazione o della libera circolazione dei dati [28]; *(iii)* della possibilità per l'intermediario di offrire agli interessati o ai titolari dei dati servizi diversi da quello di intermediazione, limitata al caso di strumenti e servizi supplementari, aventi lo specifico scopo di facilitare lo scambio dei dati, laddove tali servizi siano richiesti o approvati dai *data suppliers* (art. 12, lett. *e*), Reg. cit.).

Proseguendo oltre, il secondo requisito previsto dall'art. 12, lett. *a*), Reg. cit., che impone la fornitura dei servizi di infomediazione tramite una persona giuridica sepa-

---

[25] Cfr. ad es. L. VON DITFURTH, *Datenmärkte, Datenintermediäre und der Data Governance*, cit., pp. 340 ss. e 355 ss.

[26] Rispetto alla neutralità riguardo ai dati scambiati, il *considerando* n. 33 Reg. cit. prevede la necessità che «i fornitori di servizi di intermediazione dei dati agiscano solo in qualità di intermediari nelle transazioni e non utilizzino per nessun altro fine i dati scambiati».

[27] La disposizione in esame amplia il divieto di utilizzo dei dati imposto agli intermediari dei dati al di là dell'ambito applicativo dell'art. 12, lett. *a*), Reg. cit., comprendendo, in aggiunta ai dati oggetto dello scambio, ogni altro dato comunque raccolto o generato nel contesto dell'erogazione del servizio di infomediazione (v. ad es. L. VON DITFURTH, *Datenmärkte, Datenintermediäre und der Data Governance*, cit., p. 356), precisando, al contempo, talune forme di utilizzo di tali specifici dati ritenute ammissibili.

[28] Tale requisito mira a prevenire che l'intermediario imponga alle parti della transazione i propri *standard* dei dati, pratica funzionale a scopi propri dell'intermediario e che pertanto frustrerebbe gli obiettivi sottesi alla neutralità (cfr. L. VON DITFURTH-G. LIENEMANN, *The Data Governance Act: – Promoting or Restricting Data Intermediaries?*, in *Competition and Regulation in Network Industries*, Vol. 23, n. 4, p. 283).

rata ("*legal unbundling*"), realizza la neutralità riguardo ai dati scambiati con un obbligo che opera sempre in via preventiva, ma sul piano soggettivo, tramite una segregazione di tali servizi a livello strutturale, volta ad impedire conflitti di interesse che potrebbero aversi in caso di fornitura da parte dell'intermediario sia del servizio di intermediazione sia di prodotti o servizi di altra natura – circostanza che potenzialmente costituisce un incentivo all'utilizzo dei dati oggetto dell'attività di intermediazione per scopi propri dell'intermediario, nel contesto degli altri prodotti o servizi offerti. Detto requisito estende la limitazione dei servizi erogabili oltre quelli basati sui dati scambiati, impedendo la prestazione da parte dell'intermediario di qualsiasi altro servizio diverso da quelli di *data intermediation* [29].

Tra le condizioni previste dall'art. 12 del DGA, in ultimo è opportuno richiamare anche quella stabilita alla lett. *b*), la quale contribuisce a rafforzare gli obiettivi perseguiti dalla neutralità nelle varie dimensioni descritte [30]. Tale requisito prevede il divieto delle cc.dd. pratiche leganti e, in particolare, delle vendite abbinate e aggregate [31], stabilendo che le condizioni commerciali per la fornitura dei servizi di intermediazione dei dati, inclusa la fissazione dei prezzi, non dovrebbero essere subordinate al fatto che un potenziale titolare dei dati o utente dei dati utilizzi altri servizi forniti dall'intermediario stesso o da un'entità collegata (vendita abbinata) e, se così fosse, dalla misura in cui il titolare dei dati o gli utenti dei dati fruiscano di tali altri servizi (vendita aggregata).

Tratteggiata una panoramica delle disposizioni del DGA relative alla neutralità dei fornitori dei servizi di intermediazione dei dati rispetto ai dati scambiati, occorre evidenziare alcune prime conclusioni.

Anzitutto, dalla stessa sembra potersi trarre induttivamente un principio giuridico di neutralità [32], che di per sé non parrebbe espressivo di determinati valori, emer-

---

[29] In merito, il *considerando* n. 33 Reg. cit. esplicita la strumentalità di tale requisito alla neutralità riguardo ai dati scambiati, chiarendo come a tali fini sia necessaria «una separazione strutturale tra il servizio di intermediazione dei dati e qualsiasi altro servizio fornito, in modo tale da evitare conflitti di interessi. Ciò significa che il servizio di intermediazione dei dati dovrebbe essere fornito mediante una persona giuridica distinta dalle altre attività di tale fornitore di servizi di intermediazione dei dati».

[30] La collocazione di tale requisito nell'alveo della neutralità intesa in senso ampio emerge dal *considerando* n. 33 Reg. cit. In dottrina, cfr. ad es. L. VON DITFURTH-G. LIENEMANN, *The Data Governance Act: – Promoting or Restricting Data Intermediaries?*, cit., pp. 284-285; AA.VV., *Data Access and Sharing in Germany and in the EU: Towards a Coherent Legal Framework for the Emerging Data Economy. A Legal, Economic and Competition Policy Angle*, Final Report, 2022, p. 287.

[31] Sulle nozioni di "vendita abbinata" ("*tying*") e "vendita aggregata" ("*bundling*") cfr. ad es. COMMISSIONE EUROPEA, *Orientamenti relativi alla valutazione delle concentrazioni non orizzontali a norma del regolamento del Consiglio relativo al controllo delle concentrazioni tra imprese*, 2008/C 265/07, 18 ottobre 2008, pt. 96 ss.

[32] La neutralità, come emergente in particolare dall'art. 12, lett. *a*), Reg. cit., è declinata come principio, ad es., in G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit., p. 982; F. BRAVO, *Le cooperative di dati*, cit., p. 798; L. VON DITFURTH, *Datenmärkte, Datenintermediäre und der Data Governance*, cit., p. 340 (ove si richiama un "*Neutralitätsprinzip*").

gendo piuttosto come principio "funzionale", ossia strumentale a soddisfare dei valori previsti al suo esterno, ivi rappresentati da quelli sottesi alle due "macro-funzioni" della neutralità anzidette [33]. La ricostruzione della neutralità in termini di principio risulta utile per porre in evidenza le funzioni perseguite dalle relative disposizioni del DGA e il piano degli interessi giuridici tutelati e, così, meglio identificare la portata applicativa delle stesse rispetto ai casi più critici, tra cui quello delle cooperative di dati [34].

Proseguendo oltre, va evidenziato che dalle citate disposizioni emerge un regime che pone significativi limiti alla prestazione dei servizi di *data intermediation*, erogabili infatti solo a opera di soggetti giuridici che svolgano esclusivamente l'attività di intermediazione dei dati, i quali non possono fornire servizi diversi da questi ultimi né impiegare i dati raccolti nell'esecuzione di tale attività per propri scopi, fatte salve le limitate eccezioni stabilite dal regolamento.

Traspare, allora, una precisa direzione impressa dal legislatore europeo, volta a realizzare un isolamento dei servizi di intermediazione dei dati da quelli di ogni altra natura, nonché, contestualmente, una segregazione del relativo mercato, allo stato nella sua fase nascente. Ciò, senza alcuna differenziazione, almeno a livello espresso, rispetto all'applicazione di questo stringente regime verso le differenti tipologie di servizi di *data intermediation* finora emerse nella prassi e, almeno in parte, accolte nel regolamento stesso [35].

---

[33] Ad esempio, rispetto all'obiettivo di garantire un controllo effettivo sui dati rileverebbero, avuto riguardo agli "interessati", i valori sottesi al diritto alla protezione dei dati personali di cui all'art. 8, par. 1, Carta dir. fond. UE, mentre dall'angolo prospettico dei "titolari dei dati", le libertà fondamentali di volta in volta implicate nell'esercizio del diritto di concedere l'accesso ai dati (ad es., la libertà di impresa di cui all'art. 16 Carta dir. fond. UE). Sulla distinzione tra "principi-valore" e "principi-funzionali", in particolare nel contesto della normativa sulla protezione e la libera circolazione dei dati personali, v. F. BRAVO, *Il consenso e le altre condizioni di liceità*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla* privacy *e sulla protezione dei dati personali*, Bologna, 2017, spec. p. 103 ss. In detto ambito, rispetto al d.lgs. n. 30 giugno 2003, n. 196 anteriore alla riforma operata con il d.lgs. 10 agosto 2018, n. 101, era stata delineata anche una distinzione tra "principi-valori" e "principi-orientativi": v. F. PIRAINO, *Il codice della* privacy *e la tecnica del bilanciamento di interessi*, in R. PANETTA (a cura di), *Libera circolazione e protezione dei dati personali*, Milano, 2006, I, p. 715 ss.

[34] In ogni caso, va precisato che quello di neutralità non sarebbe un "principio generale", posto che simili principi devono essere attinenti al diritto comune e non possono ricavarsi dal diritto speciale, il quale è circoscritto a singole fattispecie o settori dell'ordinamento (cfr. G. ALPA, *I principi generali. Una lettura giusrealistica*, in *Giustizia civile*, 2014, 4, p. 957; più ampiamente, sui principi generali v. ID, *I principi generali*, in *Tratt. dir. priv.* a cura di Iudica e Zatti, Milano, 2023). Ancora, detto principio non deve essere confuso con i principi di neutralità rilevanti in altri contesti, tra i quali, su tutti, quello emergente dalla direttiva *eCommerce* (dir. 2000/31/CE; v. ora il Reg. UE n. 2065/2022, "*Digital Services Act*"), rilevante rispetto alla responsabilità degli *Internet Service Providers*, posto che i fornitori dei servizi di intermediazione dei dati, nella prestazione dei propri servizi, hanno la necessità di assumere contezza dei dati intermediati (sul rilievo della neutralità emergente dalla dir. *eCommerce* nel contesto del DGA, v. ad es. AA.VV., *White Paper on the Data Governance Act*, cit., p. 31 ss.).

[35] Per una panoramica delle tipologie di servizi di infomediazione già operanti nel mercato, v. AA.VV., *Mapping the Landscape of Data Intermediaries – Emerging Models for More Inclusive Data*

Il passaggio è di centrale importanza nell'economia del *Data Governance Act* e, più ampiamente, nella visione UE circa lo spazio comune europeo dei dati, sostanziando quella che risulta espressamente definita come la modalità "europea" di *governance* dei dati ("*European way of data governance*"): trattasi di una nuova modalità di *data governance* che dovrebbe essere offerta dai fornitori di servizi di intermediazione di dati, in particolare «garantendo una separazione, nell'economia dei dati, tra fornitura, intermediazione e utilizzo dei dati» [36].

L'elemento della novità è percepibile considerando le logiche di gestione dei dati sottese ai modelli commerciali che caratterizzano allo stato la *data economy*, alle quali la *data governance* "all'europea" si oppone [37], ove i dati, le tecnologie per valorizzarli e i prodotti e i servizi basati sugli stessi sono concentrati in pochi soggetti di grandi dimensioni, che tendono ad esercitare il proprio potere in ogni fase della *data value chain*, secondo logiche che impediscono ai *data suppliers* di mantenere un effettivo controllo sui propri dati e, in ultimo, determinano una distribuzione iniqua dei benefici derivanti dalla loro elaborazione, nonché distorsioni della concorrenza [38].

Per completezza, va anche rilevato che la modalità europea di *governance* dei dati appare connotata, oltre che da una separazione a livello oggettivo, sul piano delle attività previste nel processo di scambio dei dati (fornitura, intermediazione e utilizzo dei dati), anche da un certo distanziamento, sul piano soggettivo, tra gli attori coinvolti in detto processo, elemento che può parimenti intendersi come espressione della neutralità degli intermediari, seppur rispetto alle parti dello scambio e

---

Governance, cit., p. 40 ss.; L. VON DITFURTH, *Datenmärkte, Datenintermediäre und der Data Governance*, cit., p. 142 ss.; M. MICHELI-M. PONTI-M. CRAGLIA-A. BERTI, *Emerging Models of Data Governance in the Age of Datafication*, cit., p. 7 ss. V. altresì COMMISSIONE EUROPEA, *Impact Assessment on enhancing the use of data in Europe*, Report on Task 1 – Data governance, SMART 2020/694 | D2, 2020, p. 38 ss. Il DGA prevede tre macro-tipologie di servizi di intermediazione dei dati, elencate all'art. 10.

[36] Cfr. *considerando* n. 32 Reg. cit.

[37] Cfr. *considerando* n. 27 Reg. cit. In dottrina, è stato sottolineato che «Il modello di gestione europeo dei dati, voluto dal legislatore europeo, prende le distanza dal modello di *business* perseguito dalle c.d. *Big Tech*, caratterizzato dal capitalismo della sorveglianza, ed è orientato sia ad affermare una visione antropocentrica, che porta ad assicurare la tutela della persona e la solidarietà sociale, sia a ristabilire un regime concorrenziale tra le imprese, contrastando il sostanziale oligopolio delle multinazionali nel mercato digitale, favorendo l'emersione di imprese europee di ben più piccole dimensioni» (F. BRAVO, *Le cooperative di dati*, cit. p. 766 ss.). V. anche D. POLETTI, *Gli Intermediari dei dati*, in *EJPLT*, 2022, 1, p. 48; L. PETRONE, *Il mercato digitale europeo e le cooperative di dati*, cit., p. 807 ss.

[38] Quella UE è pertanto considerabile, in una certa misura, come una *data governance* "inclusiva", posto che, coerentemente ai valori e ai principi di fondo del diritto eurounitario, promuove un impiego dei dati più equo, fondato su un maggior coinvolgimento e controllo sui dati da parte dei *data suppliers* che allo stato hanno un minor potere nel mercato digitale (interessati, imprese individuali, PMI e *start-up*), nonché sulla condivisione dei benefici estraibili dai dati distribuita tra i vari attori del mercato e la collettività (in merito, v. AA.VV., *Mapping the Landscape of Data Intermediaries – Emerging Models for More Inclusive Data Governance*, cit., p. 18 ss.).

non invece ai dati scambiati: i servizi di intermediazione dei dati «specializzati», infatti, sarebbero «indipendenti» dalle parti della transazione [39].

Ricostruite brevemente funzioni e collocazione del principio di neutralità, a seguire saranno meglio approfonditi i tratti principali della neutralità con specifico riguardo ai dati scambiati (art. 12, lett. *a*), Reg. cit.), analizzando quest'ultima nelle dimensioni della limitazione della finalità, dei servizi erogabili (siano essi basati sui dati oggetto dello scambio o meno) e della separazione soggettiva, per identificare le funzioni e gli interessi tutelati da tale principio, da tenere in considerazione nel successivo esame della sua portata applicativa nel peculiare caso dei servizi di cooperative di dati.

2.2. La neutralità riguardo ai dati scambiati in base all'art. 12, lett. *a*), Reg. UE n. 868/2022.

2.2.1. *Il divieto di utilizzo dei dati oggetto dello scambio per scopi propri dell'intermediario (limitazione della finalità).*

Si è detto che il limite relativo all'utilizzabilità dei dati oggetto della transazione per scopi diversi dalla loro messa a disposizione al *data user* (art. 12, lett. *a*), Reg. cit.) comprende anzitutto il divieto di impiego dei dati per finalità proprie dell'intermediario, differenti dalla mera realizzazione dello scambio tra fornitori e utenti dei dati cui mira il servizio.

La neutralità, come accennato, opera in tale disposizione quale «elemento essenziale» per aumentare la fiducia e il controllo delle parti delle *data transactions* nei servizi di intermediazione e al contempo abilitare un ambiente competitivo per

---

[39] Cfr. il *considerando* n. 27 Reg. cit., dal quale emerge che l'indipendenza degli intermediari dei dati è ravvisata come potenziale facilitatore dell'emersione di nuovi ecosistemi di dati che siano, a loro volta, indipendenti dagli attori che allo stato detengono un significativo potere nel mercato digitale, nonché tale da consentire un accesso non discriminatorio alla *data economy* per le imprese di ogni dimensione, incluso PMI e *start-up*. L'indipendenza dei fornitori dei servizi di intermediazione dei dati emerge in una certa misura anche dall'art. 12, lett. *f*), Reg. cit., che impone al fornitore di tali servizi il rispetto del paradigma "FRAND" ("*fair, reasonable and non-discriminatory*") relativamente alla procedura di accesso ai servizi offerti per tutte le parti della transazione (per un inquadramento di tale paradigma, in generale e negli specifici scenari di *data sharing*, v. H. RICHTER-P.R. SLOWINSKIPP, *The Data Sharing Economy: On the Emergence of New Intermediaries*, in *IIC*, 2019, Vol. 50, n. 1, p. 17 ss.; sull'art. 12, lett. *f*), Reg. cit. come espressione di tale paradigma, v. ad es. H. RICHTER, *Looking at the Data Governance Act and Beyond: How to Better Integrate Data Intermediaries in the Market Order for Data Sharing*, in *GRUR International*, 2023, Vol. 72, n. 5, p. 468). Dal DGA emergono importanti scostamenti dal requisito dell'indipendenza: in due delle tre macro-tipologie di servizi di intermediazione dei dati previste, infatti, l'intermediario è tenuto *ex lege* ad operare nell'interesse dei fornitori dei dati: trattasi dei *(i)* servizi offerti verso gli "interessati" (art. 10, lett. *b*), Reg. cit.), rispetto ai quali, conformemente all'art. 12, lett. *m*), Reg. cit., l'intermediario è obbligato ad agire nell'interesse superiore di questi ultimi nel facilitare l'esercizio dei loro diritti, nonché dei *(ii)* servizi di cooperative di dati (art. 10, lett. *c*), Reg. cit.), rispetto ai quali v. *infra*, par. 3.

la condivisione dei dati[40], in opposizione alle descritte logiche dell'attuale economia dei dati, tali per cui consumatori e professionisti che intendono fruire di prodotti e servizi digitali devono sottostare a condizioni che abilitano lo sfruttamento dei loro dati per scopi propri del *provider*.

L'impostazione adottata dal DGA prevede che l'intermediario possa utilizzare i dati solo per un'attività di "pura" intermediazione, ossia per porre gli stessi a disposizione dell'utente dei dati, in conformità a quanto convenuto con le parti dello scambio. Ogni forma di "uso secondario" dei dati – da intendersi come utilizzo per finalità diverse dall'esecuzione del servizio di intermediazione – ne risulta pertanto vietata. Dall'angolo prospettico della normativa in materia di protezione e libera circolazione dei dati personali, segnatamente, il fornitore non potrà effettuare alcun trattamento c.d. ulteriore dei dati personali oggetto dello scambio per finalità diverse dalla realizzazione di quest'ultimo, a prescindere dalla compatibilità o meno di tali differenti finalità con quella del trattamento iniziale (art. 5, par. 1, lett. *b*), Reg. UE n. 679/2016)[41].

Il divieto è stato inteso come misura di contrasto al deficit di fiducia causato dall'asimmetria informativa *ex post* che si rinviene nella condivisione intermediata dei dati, ove la possibilità di mantenere il controllo sui dati di propria afferenza per *data subjects* e titolari dei dati è interessata da una significativa riduzione una volta che i dati entrano nella sfera di governo dell'intermediario[42]. Il rischio è implicito in ogni fenomeno di circolazione dei dati, ma presenta una maggiore intensità quando è previsto il passaggio dei dati tra più soggetti[43], come nel caso della *data intermediation*. La scelta del legislatore europeo è stata di tentare l'eliminazione in radice del problema.

Il principio di neutralità inteso come limitazione della finalità impatta anche sulla libertà di iniziativa economica degli intermediari dei dati, impedendo loro di prestare l'attività di infomediazione sulla base di modelli commerciali che prevedano la "monetizzazione" di tali dati[44] o, comunque, la valorizzazione degli stessi per

---

[40] Cfr. il *considerando* n. 33 Reg. cit.

[41] Sotto questo profilo, la disposizione in esame, escludendo qualsivoglia utilizzo dei dati scambiati per finalità diverse dalla messa a disposizione degli stessi all'utente dei dati (fatte salve le eccezioni previste), sembra impedire anche il trattamento di tali dati per scopi di archiviazione nel pubblico interesse, ricerca scientifica, storica o statistici, nonostante la particolare meritevolezza di tali trattamenti che emerge dal vigente quadro normativo in materia di protezione e libera circolazione dei dati personali (si considerino, ad es., la c.d. presunzione di compatibilità stabilita dal principio di limitazione della finalità di cui all'art. 5, par. 1, lett. *b*), Reg. UE n. 679/2016 o il peculiare regime previsto dall'art. 89 Reg. cit. applicabili a detti trattamenti; su questi profili, v. ad es. EDPS, *A Preliminary Opinion on data protection and scientific research*, 6 January 2020, p. 18). Ciò, nonostante il DGA non pregiudichi il diritto UE o nazionale sulla protezione dei dati personali, il quale, in caso di conflitti, prevale sul primo (art. 1, par. 3, Reg. UE n. 868/2022).

[42] Cfr. L. VON DITFURTH, *Datenmärkte, Datenintermediäre und der Data Governance*, cit., p. 341.

[43] Ciò, anche in ragione del carattere di non rivalità del dato, che consente lo sfruttamento contestuale di esso a opera di più soggetti senza determinarne l'esaurimento (cfr. ad es. V. ZENO-ZENCOVICH, *Do "data markets" exist?*, cit., p. 419).

[44] COMMISSIONE EUROPEA, *Impact Assessment on enhancing the use of data in Europe*, cit., p. 12. V. altresì L. PETRONE, *Il mercato digitale europeo e le cooperative di dati*, cit., p. 807.

scopi loro propri. La separazione delle attività di utilizzo dei dati da quelle di intermediazione, propria della *governance* dei dati di stampo UE, comporta che gli intermediari non intervengano in alcun modo nella catena del valore dei dati, sul presupposto che gli unici beneficiari di tale valore debbano essere i fornitori e gli utenti dei dati [45].

La limitazione della finalità emergente dall'art. 12, lett. *a*), Reg. cit. risponde all'interesse dei *data suppliers*, rafforzandone il controllo sui dati scambiati [46] e, in tal senso, manifesta la funzione della neutralità volta in ultimo a migliorare la fiducia nella condivisione intermediata dei dati [47]. Più in particolare, in quest'ottica la neutralità è espressiva delle esigenze relative al potenziamento degli interessati ("*data subjects' empowerment*") e alla sovranità dei dati ("*data sovereignity*") [48], parimenti connesse alle dinamiche che ostacolano persone e imprese nel giovarsi in prima persona dei benefici ottenibili dai dati di propria spettanza, anche a causa degli squilibri di potere, informativo e non, verso le società che dominano il mercato [49]. In tal senso, il principio in esame tende a contrastare quello che è stato definito come un «*provider centric system*» per contribuire alla creazione di uno «*human centric system*» [50], ossia di un ambiente digitale più equo, coerente con i valori, i diritti e le libertà fondamentali dell'UE, secondo il citato approccio antropocentrico emergente anche dalla strategia europea per i dati [51].

---

[45] Cfr. AA.VV., *Mapping the Landscape of Data Intermediaries – Emerging Models for More Inclusive Data Governance*, cit., p. 23, secondo cui sarebbero perciò esclusi anche i modelli fondati sulla generazione di profitto tramite l'analisi dei dati intermediati, nei quali si avrebbe un conflitto di interessi tra intermediario e parti della transazione (*Ibidem*, p. 64).

[46] Cfr. ad es. il *considerando* n. 32 Reg. cit.

[47] Cfr. ad es. L. VON DITFURTH, *Datenmärkte, Datenintermediäre und der Data Governance*, cit., p. 341 ss.

[48] *Empowerment* e sovranità dei dati sono espressioni alle volte impiegate per indicare la medesima esigenza, ma la prima è utilizzata per lo più con riferimento alle persone fisiche (qualificate, a seconda dell'angolo visuale adottato, come "interessati" o "consumatori"), mentre la seconda – che non va confusa con quella, più ampia, di *sovranità digitale* – in modo tale da ricomprendere anche i bisogni di imprese ed altre organizzazioni. Sullo *empowerment* degli interessati tramite il «controllo intermediato», specialmente mediante il paradigma della tutela collettiva nel contesto delle cooperative di dati, v. F. BRAVO, *Le cooperative di dati*, cit., p. 783 ss.; v. altresì D. POLETTI, *Gli intermediari dei dati*, cit., pp. 55-56, ma anche EAD., *Il controllo dell'interessato e la strategia europea sui dati*, in *Osservatorio sulle fonti*, 2023, 2, spec. p. 372 ss.

[49] V. ad es. M. MICHELI-M. PONTI-M. CRAGLIA-A. BERTI, *Emerging Models of Data Governance in the Age of Datafication*, cit., pp. 3 ss. e 8 ss.; G. CAROVANO-M. FINCK, *Regulating Data Intermediaries: The impact of the Data Governance Act on the EU's Data Economy*, cit., pp. 2 e 8.

[50] Cfr. EDPS, *EDPS Opinion on Personal Information Management Systems. Towards More User Empowerment in Managing and Processing Personal Data*, 20 October 2016, p. 3.

[51] COMMISSIONE EUROPEA, *Una strategia europea per i dati*, cit., p. 5. Nel *Data Governance Act*, le principali disposizioni volte a realizzare l'*empowerment* degli interessati si rinvengono in riferimento ai servizi di intermediazione dei dati offerti verso le persone fisiche e ai servizi di cooperative

Il rilievo della neutralità come limitazione della finalità in chiave di miglioramento del controllo sui dati per i *data suppliers*, a ogni modo, non deve oscurare la circostanza che la stessa, seppur in misura secondaria, è funzionale anche alla tutela degli interessi dei soggetti che intendono fruire dei dati scambiati, posto che le descritte criticità sul controllo dei dati si rinvengono anche in riferimento ai *data users* [52].

Proseguendo oltre, la seconda funzione perseguita dal principio di neutralità come limitazione della finalità consiste nel contribuire alla realizzazione di un mercato privo di distorsioni della concorrenza, le quali potrebbero emergere in caso di conflitti di interesse tra intermediario e parti della transazione. I fornitori dei servizi di intermediazione (o società collegate o parte del medesimo gruppo), invero, potrebbero essere incentivati a impiegare i dati intermediati per propri scopi, nel contesto di attività concorrenti con quelle dei *data suppliers* o degli utenti dei dati o comunque con modalità tali da determinare indebiti vantaggi concorrenziali [53].

La premessa da cui muove il DGA, al riguardo, è rappresentata dall'esperienza sui profili di diritto della concorrenza maturata specialmente nel contesto dei fenomeni di integrazione verticale che interessano le piattaforme digitali, nelle quali i relativi fornitori (o le imprese variamente "connesse" a questi ultimi) rivestono il duplice ruolo di intermediari e soggetti concorrenti con le parti della transazione [54]. Il mercato delle piattaforme tende ad essere connotato da fenomeni di concentrazione di mercato, in estrema sintesi a causa dei significativi effetti di rete riscontrabili in tali contesti, ai quali si ricollegano conseguenze negative in termini di *lock-in* sul versante dell'utenza, nonché degli effetti delle economie di scala e di scopo, i quali incentivano la piattaforma ad espandere continuamente la propria attività in nuovi settori, così amplificandone il potere di mercato grazie all'aumento delle fon-

---

di dati, previsti rispettivamente alle lett. *b*) e *c*) dell'art. 10. Le cooperative di dati sono rilevanti anche come mezzo per contribuire alla *data sovereignity* di imprese individuali e PMI, soggetti che parimenti subiscono gli effetti negativi, tra gli altri, dello squilibrio di potere informativo verso le *Big Tech* (cfr. ad es. i *considerando* nn. 2 e 31 Reg. cit.).

[52] Gli interessi di cui sono portatori gli utenti dei dati sono parimenti rilevanti per promuovere la fiducia nei servizi di intermediazione dei dati (cfr. ad es. il *considerando* n. 32 Reg. cit.). Che la garanzia di neutralità risponda anche all'interesse degli utenti dei dati è evidente in considerazione del valore, economico e strategico, dell'*asset* dati e dunque delle informazioni relative alle operazioni economiche aventi per oggetto il medesimo, anche sotto il profilo della riservatezza commerciale (su tali aspetti, v. ad es. L. VON DITFURTH, *Datenmärkte, Datenintermediäre und der Data Governance*, cit., pp. 341 ss. e 355 ss.).

[53] Sui profili *antitrust* dell'art. 12, lett. *a*), Reg. UE n. 868/2022, v. ad es. L. VON DITFURTH, *Datenmärkte, Datenintermediäre und der Data Governance*, cit., p. 342 ss.; ID.-G. LIENEMANN, *The Data Governance Act: – Promoting or Restricting Data Intermediaries?*, cit., p. 276 ss.

[54] In merito, v. ad es. L. VON DITFURTH, *Datenmärkte, Datenintermediäre und der Data Governance*, cit., p. 341; ID.-G. LIENEMANN, *The Data Governance Act: – Promoting or Restricting Data Intermediaries?*, cit., p. 276 ss.; I. GRAEF-R. GELLERT, *The European Commission's Proposed Data Governance Act: Some Initial Reflections on the Increasingly Complex EU Regulatory Puzzle of Stimulating Data Sharing*, in *TILEC Discussion Paper* No. DP2021-006, 2021, p. 12; AA.VV., *White Paper on the Data Governance Act*, cit., p. 26.

ti di accumulazione dei dati e della capacità di sfruttamento dei dati stessi, dai quali derivano vantaggi competitivi che possono concretizzarsi in pratiche *antitrust* di vario tipo e comportare altresì effetti di "chiusura" dei mercati [55].

La neutralità declinata come limitazione della finalità opera nelle direzioni di tutela della concorrenza limitando la creazione di nuove concentrazioni di potere o il consolidamento di quelle esistenti. Sotto tale profilo, pur essendo posta a tutela anche delle parti della transazione [56], la neutralità ha primariamente rilievo pubblicistico, configurandosi quale mezzo di regolazione del mercato degli intermediari dei dati a opera delle istituzioni UE, con disposizioni il cui rispetto è affidato ad autorità istituite allo specifico scopo di monitorare la conformità degli intermediari alle stesse (artt. 13-14 Reg. cit.). Al riguardo, la disciplina del DGA cui è assoggettata la fornitura dei servizi di intermediazione, inclusa la neutralità nelle sue diverse dimensioni, è pertanto sottratta all'autonomia privata [57].

2.2.2. *Il divieto di fornire servizi diversi da quelli di intermediazione dei dati (limitazione dei servizi).*

La neutralità intesa come limite all'impiego dei dati per i quali l'intermediario fornisce i propri servizi per scopi diversi dalla messa a disposizione degli stessi agli utenti dei dati (art. 12, lett. *a*), Reg. cit.) implica altresì il divieto di prestare alle parti della transazione servizi basati su tali dati differenti da quelli di *data intermediation*. Sul punto, la neutralità come "separazione soggettiva", più ampiamente, impedisce anche la prestazione di ogni altro servizio diverso da quello di intermediazione, sia esso basato o meno sui dati oggetto dello scambio.

Da tali norme, dunque, può trarsi la dimensione del principio di neutralità come limitazione dei servizi erogabili, volta ad impedire all'intermediario di impiegare i dati oggetto dello scambio, direttamente o indirettamente, in servizi diversi da quello volto alla realizzazione della transazione, sulla base della medesima logica della separazione tra fornitura, intermediazione e utilizzo dei dati sottesa alla modalità UE di *data governance* e in funzione degli stessi obiettivi di aumentare la fiducia negli intermediari dei dati e assicurare il rispetto della disciplina sulla concorrenza.

L'impossibilità di offrire servizi di altra natura alle parti della transazione mira a

---

[55] V. i riferimenti riportati alla nota precedente.

[56] Come accennato, ad es., l'intermediario potrebbe impiegare i dati raccolti dalle transazioni intermediate per sviluppare servizi concorrenti con quelli offerti dai titolari o dagli utenti dei dati oppure potrebbe esso stesso offrire ai *data users* pacchetti di dati più "ricchi", ottenuti dall'aggregazione dei dati per cui ha gestito l'intermediazione (v. ad es. L. VON DITFURTH, *Datenmärkte, Datenintermediäre und der Data Governance*, cit., p. 342 ss.).

[57] *Ibidem*, p. 359. V. altresì AA.VV., *Data access and sharing in Germany and in the EU: Towards a coherent legal framework for the emerging data economy*, cit., p. 294 ss.; H. RICHTER, *Looking at the Data Governance Act and Beyond: How to Better Integrate Data Intermediaries in the Market Order for Data Sharing*, cit., p. 467 ss.

prevenire possibili incentivi all'utilizzo incrociato ("*cross-use*") dei dati da parte dell'intermediario [58], circostanza che ostacolerebbe il raggiungimento di entrambe le finalità anzidette. Per quanto concerne, in particolare, l'obiettivo di garantire alle parti della transazione un effettivo controllo sui dati di propria afferenza, così creando un mercato dell'intermediazione dei dati affidabile, il divieto in esame limita altresì il rischio della "*function creep*", ossia di estensione indebita delle finalità per cui sono trattati i dati, di rilievo specialmente in caso di intermediazione di dati personali [59].

A ogni modo, le funzioni più rilevanti del divieto in questione si rinvengono in relazione agli obiettivi di tutela della concorrenza [60]. La fornitura di determinati servizi aggiuntivi a quelli di intermediazione, invero, potrebbe risultare di significativo interesse per le parti della transazione e, nonostante ciò, anche laddove non implicasse l'impiego dei dati intermediati per scopi ulteriori propri dell'intermediario e fosse congegnata con modalità tali da garantire il pieno controllo delle stesse su tali dati, risulterebbe comunque impedita dalla disposizione in esame, quale strumento di regolazione preventiva del mercato sottratto all'autonomia privata [61].

---

[58] Si pensi, ad esempio, a un intermediario che offra servizi di analisi dei dati in favore degli utenti dei dati e che impieghi i dati oggetto delle transazioni intermediate per scopi di miglioramento di tale servizio (ad es., per l'addestramento degli algoritmi di *machine learning* su cui si basa tale servizio). Norme sul *cross-use* dei dati sono previste anche nel Reg. UE n. 1925/2022 in riferimento ai "*gatekeeper*" (cfr. art. 5, par. 2, lett. *c*), Reg. cit.; v. altresì il *considerando* n. 36): in merito, su analogie e differenze tra DGA e DMA, v. ad es. AA.VV., *White Paper on the Data Governance Act*, cit., p. 32; H. RICHTER, *Looking at the Data Governance Act and Beyond: How to Better Integrate Data Intermediaries in the Market Order for Data Sharing*, cit., p. 463).

[59] La *function creep* è una pratica in contrasto con il principio di *data protection* di limitazione della finalità (art. 5, par. 1, lett. *b*), Reg. UE n. 679/2016), la quale pone rischi per i diritti e le libertà degli interessati in termini di utilizzi dei dati personali non coerenti con le ragionevoli aspettative di questi ultimi e, dunque, di perdita del controllo su tali dati (cfr. ad es. EDPB, *Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679*, v. 1.1, 13 maggio 2020, p. 15; ART. 29 WORKING PARTY, *Opinion 03/2013 on purpose limitation*, 2 April 2013, p. 4).

[60] Cfr. L. VON DITFURTH-G. LIENEMANN, *The Data Governance Act: – Promoting or Restricting Data Intermediaries?*, p. 278 ss. Sui profili di diritto della concorrenza del divieto in esame, v. altresì ID, *Datenmärkte, Datenintermediäre und der Data Governance*, cit., p. 342 ss.; AA.VV., *White Paper on the Data Governance Act*, cit., p. 32 ss. Come anticipato, l'integrazione di più servizi, specie se *data-based*, presso un medesimo fornitore può generare plurime criticità in termini *antitrust*: *(i)* la fornitura di servizi aggiuntivi a quelli di infomediazione, anche se non aventi per oggetto i dati scambiati, è un potenziale incentivo per il fornitore a utilizzare questi dati nel contesto di tali altri servizi; *(ii)* il fornitore potrebbe essere portato a sfruttare il potere di mercato detenuto rispetto a tali altri servizi per trasferirlo nel contesto di quelli di intermediazione dei dati (le *Big Tech*, nella specie, potrebbero così estendere la loro posizione dominante nei nuovi mercati dell'infomediazione); *(iii)* l'integrazione di più servizi presso il medesimo fornitore potrebbe determinare effetti di *lock-in* per l'utenza, con correlati impatti negativi verso gli altri attori del mercato. Pratiche di questo tipo, dunque, a seconda del caso potrebbero risultare anti-concorrenziali e incidere negativamente sugli interessi sia delle parti delle transazioni sia delle imprese che intendano operare nei suddetti mercati.

[61] Ciò, anche laddove la fornitura del servizio nel singolo caso dovesse ritenersi in linea con gli

Il rischio che la possibilità di offrire servizi aggiuntivi ostacoli gli obiettivi dell'UE di creare un ambiente competitivo per il *data sharing* è dunque affrontato, anche in tal caso, con una rigida disciplina *ex ante*. A ogni modo, per l'intermediario resta possibile offrire servizi diversi da quelli di intermediazione dei dati o comunque non funzionali alla prestazione di questi ultimi costituendo un soggetto giuridico distinto [62]. Le parti della transazione, dunque, potranno beneficiare dei servizi offerti da società collegate o parte del medesimo gruppo dell'intermediario e, in questi scenari, a limitare possibili pratiche *antitrust* e, dunque, a contribuire alla realizzazione degli obiettivi della neutralità, vi sarebbe il citato requisito di cui all'art. 12, lett. *b*), Reg. UE n. 868/2022 in materia di pratiche leganti [63].

In ultimo, va ricordato che una rilevante eccezione al principio di neutralità come limitazione dei servizi erogabili è stabilita all'art. 12, lett. *e*), Reg. cit., ove è previsto che i servizi di *data intermediation* possono comprendere «l'offerta di strumenti e servizi supplementari specifici ai titolari dei dati o agli interessati allo scopo specifico di facilitare lo scambio dei dati», purché utilizzati solo su richiesta o esplicita approvazione del titolare dei dati o dell'interessato [64]. Detti servizi e strumenti supplementari potrebbero essere offerti anche per il tramite di terze parti e, sul punto, per evitare agevoli elusioni, a rafforzare il principio di neutralità vi è la precisazione che «gli strumenti di terzi offerti in tale contesto non utilizzano i dati per altri scopi» [65].

---

artt. 101 e 102 TFUE (cfr. L. VON DITFURTH, *Datenmärkte, Datenintermediäre und der Data Governance*, cit., p. 358 ss.; H. RICHTER, *Looking at the Data Governance Act and Beyond: How to Better Integrate Data Intermediaries in the Market Order for Data Sharing*, cit., p. 464).

[62] Cfr. ad es. AA.VV., *Mapping the Landscape of Data Intermediaries – Emerging Models for More Inclusive Data Governance*, cit., p. 38.

[63] Cfr. *Ibidem*, p. 356 ss.; ID.-G. LIENEMANN, *The Data Governance Act: – Promoting or Restricting Data Intermediaries?*, cit., p. 279 ss.

[64] La disposizione abilita gli intermediari, entro certi limiti, a godere dei benefici derivanti dall'integrazione verticale, così rendendo più economicamente sostenibile la fornitura di tali servizi (H. RICHTER, *Looking at the Data Governance Act and Beyond: How to Better Integrate Data Intermediaries in the Market Order for Data Sharing*, cit., p. 463). La circostanza che i servizi aggiuntivi possano essere forniti soltanto in favore dei *data suppliers* e, in ogni caso, su richiesta o esplicita approvazione di questi ultimi, nonostante possano risultare di interesse anche per gli utenti dei dati, conferma la descritta prevalenza della funzione della neutralità relativa all'aumento del controllo sui dati ("*data subjects empowerment*" e "*data sovereignity*") dal precipuo lato di interessati e titolari dei dati, ossia dei soggetti rispetto ai quali è necessario implementare meccanismi partecipativi e redistributivi che consentano di riequilibrare le dinamiche di potere del mercato digitale in coerenza con i valori e il diritto UE.

[65] Ciò, posto che le terze parti non sono assoggettate al divieto di utilizzo dei dati *ex* art. 12, lett. *a*), Reg. cit., rivolto ai soli intermediari. Sul punto, la lett. *e*) dell'art. 12 Reg. cit. pare far propria l'esperienza maturata nell'ambito della protezione dei dati personali, ove l'integrazione di elementi di terze parti nei servizi digital ha rivelato significative criticità per i diritti e le libertà degli interessati: si pensi, su tutti, al caso *Cambridge Analytica*, rispetto al quale si v. i provvedimenti adottati in Italia dal Garante per la protezione dei dati personali (GPDP, 10 gennaio 2019, doc. *web* n. 9080914; GPDP, 14 giugno 2019, doc. *web* n. 9121486) e, per ulteriori dettagli, sia consentito il rinvio a D.

2.2.3. *L'obbligo di fornitura di servizi di intermediazione dei dati tramite una persona giuridica distinta.*

Il principio di neutralità, in ultimo, prevede che i servizi di intermediazione dei dati siano forniti «attraverso una persona giuridica distinta» (art. 12, lett. *a*), Reg. cit.), così imponendo, come detto, una separazione strutturale tra detti servizi e quelli di qualsiasi altra natura, volta ad evitare conflitti di interessi tra intermediario e attori della *data transaction* [66].

Questa dimensione della neutralità, dunque, precisa i confini della modalità europea di *governance* dei dati, stabilendo come la separazione tra intermediazione e utilizzo dei dati operi non solo in termini di attività, ma altresì sul piano soggettivo [67].

L'obbligo previsto, complementare alle altre dimensioni della neutralità già esaminate, risulta funzionale ai medesimi obiettivi di rafforzamento del controllo sui dati per le parti della transazione e, dunque, della fiducia di queste ultime nella condivisione intermediata nei dati, nonché di prevenzione di possibili pratiche anti-concorrenziali. L'isolamento dei servizi di infomediazione in capo a un soggetto giuridico apposito, invero, limita gli incentivi all'utilizzo incrociato dei dati, ossia all'impiego dei dati acquisiti nel corso della transazione nel contesto degli altri servizi offerti dell'intermediario [68]. Per quanto concerne le società collegate o parte dello stesso gruppo di quest'ultimo che potrebbero giovarsi dei dati intermediati, vi è anche in tal caso il divieto di pratiche leganti a rafforzare il conseguimento degli obiettivi della neutralità (art. 12, lett. *b*), Reg. cit.).

Per quanto concerne le specificità di questa dimensione della neutralità, distinte da quelle già descritte rispetto alla "limitazione dei servizi", occorre rilevare come la separazione prevista dal *Data Governance Act* risulti puramente formale e non invece di tipo operativo [69]. L'art. 12, lett. *a*), Reg. cit., infatti, non impone l'adozione di meccanismi volti a garantire che, sul piano fattuale, l'entità giuridica separata non sia influenzata da altre società [70]. A ogni modo, a realizzare, almeno in una cer-

---

SBORLINI, *Profilazione elettorale e protezione dei dati personali. Prospettive di soluzione in ambito europeo*, in *Il diritto dell'informazione e dell'informatica*, 2022, 6, spec. p. 1174 ss.

[66] Cfr. *considerando* n. 33 Reg. cit. Su tale requisito, v. ad es. H. RICHTER, *Looking at the Data Governance Act and Beyond: How to Better Integrate Data Intermediaries in the Market Order for Data Sharing*, cit., p. 463; L. VON DITFURTH, *Datenmärkte, Datenintermediäre und der Data Governance*, cit., p. 361 ss.; AA.VV., *White Paper on the Data Governance Act*, cit., p. 33 ss. Com'è stato notato, la separazione strutturale è prevista anche dal *Digital Markets Act*, ma soltanto come possibile rimedio *ex post* per le situazioni di *non-compliance* aventi carattere sistematico (cfr. art. 18, par. 1, Reg. UE n. 1925/2022) (su tali profili, v. AA.VV., *White Paper on the Data Governance Act*, cit., pp. 33-34).

[67] Sulla neutralità come criterio di separazione soggettiva tra fornitore dei servizi di intermediazione e utilizzatore dei dati intermediati, v. F. BRAVO, *Le cooperative di dati*, cit., p. 774 ss.

[68] La *ratio* della disposizione in esame è parimenti ravvisata nella prevenzione del *cross-use* dei dati in AA.VV., *White Paper on the Data Governance Act*, cit., p. 33 ss.

[69] L. VON DITFURTH, *Datenmärkte, Datenintermediäre und der Data Governance*, cit., p. 363 ss.

[70] *Ibidem*. In tal senso, la separazione strutturale non impedisce, di per sé, l'emersione di possibili pratiche *antitrust* (cfr. altresì AA.VV., *White Paper on the Data Governance Act*, cit., p. 33 ss.).

ta misura, una separazione "informativa" vi sono le altre componenti del principio di neutralità relative alla limitazione della finalità e dei servizi erogabili [71], le quali, ad esempio, impediscono all'intermediario di porre in essere pratiche come la trasmissione alla capogruppo dei dati o dei metadati acquisiti nella fornitura del servizio di infomediazione [72]. In tal senso, rispetto ai rischi di elusioni della norma in esame nell'ambito di gruppi societari o di collegamenti tra imprese, ove una di esse opera come intermediario e un'altra quale utilizzatrice dei dati [73], le carenze del requisito della separazione soggettiva sarebbero mitigate, seppur soltanto in parte, dall'operatività della neutralità come limitazione della finalità [74].

Ciò rilevato, stante la specularità tra la descritta dimensione del principio di neutralità e le altre già esaminate, sulle più ampie funzioni della separazione soggettiva si rinvia a quanto già osservato in precedenza.

3. Cooperative di dati e principio di neutralità: questioni critiche.

3.1. Il modello delle cooperative di dati delineato dal DGA: caratteristiche e attriti con la neutralità riguardo ai dati scambiati.

Delineate per sommi capi le funzioni del principio di neutralità riguardo ai dati scambiati, è possibile approfondirne l'operatività rispetto ai servizi di cooperative di dati.

Anzitutto, come già accennato, le disposizioni sulla neutralità dei fornitori di servizi di intermediazione dei dati appaiono in conflitto con i modelli di cooperative di dati emersi nella prassi, i quali, in breve, prevedono attività di valorizzazione dei dati in favore dei propri membri che vanno oltre la mera prestazione di servizi di intermediazione dei dati [75].

In aggiunta, come si dirà a seguire, la neutralità non risulta pienamente coerente con lo stesso modello di cooperative di dati delineato dal DGA.

---

[71] L. VON DITFURTH, *Datenmärkte, Datenintermediäre und der Data Governance*, cit., p. 366 ss.

[72] Al contempo, altri requisiti di cui all'art. 12 Reg. cit. ridurrebbero, almeno in parte, alcuni dei rischi derivanti dalla possibile influenza esercitabile dalle altre società del gruppo sull'intermediario: la condizione di cui all'art. 12, lett. *f*), Reg. cit., ad esempio, vincola il fornitore a garantire una procedura di accesso al proprio servizio equa, trasparente e non discriminatoria, così limitandolo nell'avvantaggiare le società consorelle a discapito di altri soggetti, almeno nel contesto delle procedure di accesso al servizio.

[73] In merito, v. F. BRAVO, *Le cooperative di dati*, cit., p. 775 ss.; G. CAROVANO-M. FINCK, *Regulating Data Intermediaries: The impact of the Data Governance Act on the EU's Data Economy*, cit., p. 8.

[74] Possibili elusioni potrebbero aversi quando un intermediario offra servizi diversi da quelli di *data intermediation* mediante un'entità separata e quest'ultima trasmetta al primo i dati acquisiti nell'erogazione di tali servizi, il quale potrebbe allora impiegarli per propri scopi (ad es., per analisi interne volte al miglioramento dei propri servizi di intermediazione).

[75] V. *supra*, par. 1, nonché quanto meglio si dirà *infra*.

Al riguardo, conviene anzitutto ricordare che quelli di cooperative di dati sono definiti come «servizi di intermediazione dei dati», in particolare «offerti da una struttura organizzativa costituita da interessati, imprese individuali o da PMI, che sono membri di tale struttura, avente come obiettivi principali quelli di aiutare i propri membri nell'esercizio dei loro diritti in relazione a determinati dati, anche per quanto riguarda il compiere scelte informate prima di acconsentire al trattamento dei dati, di procedere a uno scambio di opinioni sulle finalità e sulle condizioni del trattamento dei dati che rappresenterebbero al meglio gli interessi dei propri membri in relazione ai loro dati, o di negoziare i termini e le condizioni per il trattamento dei dati per conto dei membri prima di concedere l'autorizzazione al trattamento dei dati non personali o prima che essi diano il loro consenso al trattamento dei dati personali» [76].

Le cooperative di dati, dunque, dal punto di vista soggettivo sono connotate da una struttura composta dagli stessi *data suppliers*, i quali devono necessariamente essere rappresentati dagli "interessati" o dai titolari dei dati equiparabili ai singoli individui «in termini di conoscenze in materia di condivisione dei dati» [77], ossia da imprese individuali e PMI [78]. In termini "funzionali", inoltre, le cooperative di dati sono caratterizzate dal perseguimento di specifici «obiettivi principali» predeterminati dal legislatore, da cui discende, in sintesi, che le stesse devono prestare la propria attività nel precipuo interesse dei propri membri [79].

La considerazione degli obiettivi previsti dall'art. 2, n. 15, Reg. cit. lascia emergere la più rilevante delle criticità poste dall'applicazione del principio di neutralità (art. 12, lett. *a*), Reg. cit.) alle cooperative di dati: le attività serventi a tali obiettivi non richiedono necessariamente di essere collocate nel contesto di un'operazione di "intermediazione dei dati"; tali obiettivi potrebbero utilmente essere conseguiti tramite attività poste al di fuori di un'operazione di tal fatta o di "condivisione dei dati". Il

---

[76] Art. 2, n. 15, Reg. cit. Sulla definizione e i tratti connotanti le «cooperative di dati», v. F. BRAVO, *Le cooperative di dati*, cit., p. 759 ss.

[77] *Considerando* n. 31 Reg. UE n. 868/2022.

[78] Sulle nozioni di imprese individuali e PMI, v. COMMISSIONE EUROPEA, *Raccomandazione della Commissione, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese*, Gazzetta ufficiale n. L 124 del 20 maggio 2003, pp. 36-41.

[79] A fronte di tali obiettivi, considerati nella più ampia economia del DGA, emerge che le cooperative di dati svolgono una duplice funzione: *(i)* verso l'interno, supportano i propri membri fornendo loro l'assistenza necessaria a rimediare alle asimmetrie di potere informativo sussistenti tra di essi e gli utenti dei dati; *(ii)* verso l'esterno, esercitano una funzione di "raggruppamento" dei propri membri, dunque dei dati di loro afferenza, nei confronti degli utenti dei dati (cfr. L. VON DITFURTH, *Datenmärkte, Datenintermediäre und der Data Governance*, cit., p. 268). Tale schematizzazione è utile per rendere evidente il rilievo della dimensione collettiva nelle cooperative di dati, che rappresenta il tratto distintivo di tale "intermediario" e il presupposto necessario – ma, come si vedrà, non sufficiente – per abilitare le cooperative di dati a realizzare i propri obiettivi, ad esempio aumentandone il potere negoziale verso l'esterno (cfr. ad es. AA.VV., *Data access and sharing in Germany and in the EU: Towards a coherent legal framework for the emerging data economy*, cit., p. 86).

DGA, invero, non definisce le cooperative di dati, ma i «servizi di cooperative di dati», quali servizi di *data intermediation* offerti da un'organizzazione (la cooperativa di dati) avente gli obiettivi principali poc'anzi richiamati, la quale, pertanto, di fatto ben potrebbe prestare anche servizi di altra natura, in riferimento sia ai citati obiettivi sia ad altri (da considerarsi necessariamente come obiettivi "secondari").

Al riguardo, tuttavia, la scelta del DGA di inquadrare i servizi di cooperative di dati tra quelli di *data intermediation* innesca l'applicazione del principio di neutralità (art. 12, lett. *a*), Reg. cit.), che nelle dimensioni della limitazione della finalità, dei servizi erogabili e della separazione soggettiva opera nel senso di isolare tali servizi, quali servizi di intermediazione dei dati, in capo a un soggetto che può essere deputato esclusivamente alla loro prestazione.

Il passaggio, evidentemente, è di centrale importanza. In attesa di possibili chiarimenti, che potranno emergere anche dall'operato delle autorità competenti per il monitoraggio della conformità di tali servizi[80], quanto allo stato rilevabile dal combinato disposto degli artt. 2, n. 15 e 12, lett. *a*), Reg. cit. e dalle complessive trame del DGA porta a collocare le attività effettuabili dalle cooperative di dati necessariamente entro un contesto di *data sharing* intermediato. Le cooperative di dati previste dal Reg. UE n. 868/2022, quali fornitori di "servizi di intermediazione dei dati", potrebbero supportare i propri membri nella valorizzazione dei dati solo tramite la prestazione di servizi di tal fatta (ferme le altre attività limitatamente consentite dall'art. 12 Reg. cit.). Conseguentemente, rispetto alle questioni poste dalla neutralità, occorre indagare quali siano le attività effettuabili dalle cooperative di dati, intese come fornitori di servizi di intermediazione dei dati, a fronte delle peculiarità di tali organizzazioni (emergenti dallo stesso regolamento europeo) e, in particolare, se queste ultime giustifichino, come parrebbe, una maggiore operatività di tali intermediari rispetto ai dati "conferiti" dai propri membri.

Tanto premesso, anzitutto l'applicazione del principio di neutralità alle *data cooperatives* potrebbe ritenersi, in una certa misura, carente della giustificazione che ne sorregge l'operatività nel caso delle altre tipologie di servizi di intermediazione. Sul piano delle funzioni della neutralità, infatti, stante la sostanziale coincidenza, a monte, tra fornitori dei dati (membri della cooperativa di dati) e cooperativa di dati stessa (quale soggetto composto dai fornitori dei dati) e alla luce degli obiettivi principali di quest'ultima, le *data transactions* realizzate dalla cooperativa di dati soddisferanno di necessità gli interessi sia dei *data suppliers* sia dell'intermediario, ciò rendendo apparentemente superflua l'applicazione della neutralità come mezzo per limitare conflitti di interessi tra intermediario e fornitori dei dati e per garantire il controllo di questi ultimi sui propri dati[81]. Sotto questo profilo, la

---

[80] Cfr. art. 13 Reg. cit. e art. 2 d.lgs. n. 144/2024 (quest'ultimo, per l'autorità competente italiana, rappresentata dall'AgID).

[81] Cfr. ad es. L. VON DITFURTH, *Datenmärkte, Datenintermediäre und der Data Governance*, cit., p. 267, ove è evidenziato come le cooperative di dati, a differenza degli altri fornitori di servizi di intermediazione, che mediano tra le parti della transazione senza rappresentare gli interessi di una parte,

sostanziale coincidenza tra fornitura e intermediazione dei dati e la carenza di indipendenza della cooperativa rispetto ai propri membri, d'altra parte, determinano un certo distacco dallo stesso paradigma della *European way of data governance*[82].

Proseguendo oltre, per quanto riguarda gli attriti tra il modello dei servizi di cooperative di dati previsto dal DGA e le disposizioni sulla neutralità, basti anticipare che nei servizi di cooperative di dati l'intermediario, per definizione, deve perseguire degli obiettivi che richiedono di svolgere in favore dei propri membri attività (ad esempio, quelle di stimolo del dialogo interno sulle condizioni del trattamento dei

---

cercano di far valere gli interessi dei propri membri nei confronti dei terzi. Questi aspetti sono meglio analizzati *infra*.

[82] La tendenziale coincidenza tra gli interessi delle cooperative di dati e dei relativi membri e la centralità, in dette organizzazioni, della dimensione collettiva non possono oscurare le esigenze di protezione delle singole persone che le compongono. La questione rileva specialmente per le cooperative di dati che coinvolgono gli "interessati": i dati personali, quali attributi della personalità, non possono essere considerati alla stregua di un bene giuridico suscettibile di un conferimento con efficacia reale in cooperativa (in merito, cfr. G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit. p. 993; F. BRAVO, *Le cooperative di dati*, cit., p. 792). Di più, l'interessato in ogni caso deve poter esercitare pienamente il potere di governo sui propri dati personali, dunque l'autodeterminazione informativa nella quale si sostanzia il diritto fondamentale alla protezione dei dati personali. Ecco allora che la necessità di massimizzare le esigenze della libera circolazione dei dati mantenendo fermo il rispetto del diritto alla protezione dei dati personali trova un paradigma coerente nel modello di *governance* che è stato definito "duale", ove alla dimensione collettiva delle scelte assunte dai soci deve sempre accostarsi quella individuale di ciascuno di essi, quale "interessato" (cfr. F. BRAVO, *Le cooperative di dati*, cit., spec. pp. 762-763). Detto modello deve essere inteso alla luce della «funzione sociale» che connota il diritto alla protezione dei dati personali, da contemperare secondo proporzionalità con gli altri diritti e libertà rilevanti nel singolo caso (*Ibidem*, p. 768), ciò consentendo di sviluppare la dimensione relazionale di tale diritto nelle nuove direzioni delle *data cooperatives*, in aderenza alla «funzione sociale» assegnata alla cooperazione dall'art. 45 Cost. (sulla "funzione sociale" della cooperazione, v. F. GALGANO-R. GHENGHINI, *Il nuovo diritto societario*, III ed., Padova, 2006, I, p. 923 ss.; A. BASSI, *Principi generali della riforma delle società cooperative*, Milano, 2004, p. 33 ss.; ID., *Le società cooperative*, Torino, 1995, p. 87 ss.). Per la riconduzione del diritto alla protezione dei dati personali tra i diritti della personalità, v. F. GALGANO, *Tratt. dir. civ.*, III ed., Padova, 2014, I, pp. 171 ss. e 195 ss., mentre sui dati personali come "attributi" della personalità, v. G. RESTA, *Autonomia privata e diritti della personalità*, Napoli, 2005, *passim*. Sull'accezione "moderna" del diritto alla protezione dei dati personali, quale «diritto a mantenere il controllo sulle proprie informazioni e di determinare le modalità di costruzione della propria sfera privata», v. S. RODOTÀ, *Tecnologie e diritti*, Bologna, 2021, p. 98 (p. 122 prima ed.). Per una panoramica del dibattito sulla natura del dato personale, sviluppatosi specialmente con riguardo alla sua commerciabilità, v. G. ALPA, *La "proprietà" dei dati personali*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, 2019, p. 18 ss. Sulle due "anime" della protezione e della libera circolazione dei dati personali, v. N. ZORZI GALGANO, *Le due anime del GDPR e la tutela del diritto alla* privacy, in EAD. (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, cit., p. 35 ss., mentre specificamente sulla "funzione sociale" del diritto alla protezione dei dati personali, ora esplicitata al *considerando* n. 4 Reg. UE n. 679/2016, v. F. BRAVO. *Sul bilanciamento proporzionale dei diritti e delle libertà "fondamentali", tra mercato e persona: nuovi assetti nell'ordinamento europeo?*, in *Contratto e impresa*, 2018, 1, p. 205 ss.; I. SPEZIALE, *L'ingresso dei dati personali nella prospettiva causale dello scambio: i modelli contrattuali di circolazione*, in *Contratto e impresa*, 2021, 2, p. 607.

dati che soddisferebbero al meglio gli interessi dei membri o di negoziazione dei termini di utilizzo di tali dati per loro conto) che, con ogni evidenza, sono diverse e ulteriori da quelle di pura intermediazione dei dati e che, perciò, appaiono in conflitto con la neutralità, in particolare come limitazione dei servizi [83].

In breve, le peculiarità delle cooperative di dati nel modello definito dallo stesso DGA richiedono di riconoscere a queste ultime un'operatività che va oltre i limiti emergenti da una lettura isolata delle disposizioni sulla neutralità e ciò, innanzi all'approccio "*one-size-fits-all*" che connota la disciplina dei servizi di intermediazione di cui all'art. 12 Reg. cit., lascia all'interprete il compito di identificare la portata applicativa del *principio* di neutralità al caso specifico di tali intermediari.

La neutralità, pertanto, presenta diversi aspetti problematici nel caso delle cooperative di dati. In questa sede, saranno esaminate solo alcune questioni specifiche, rappresentate nella specie da quelle riguardanti *(i)* la possibilità per le *data cooperatives* di prestare servizi di intermediazione dei dati al loro interno, abilitando forme di valorizzazione basate sulla condivisione dei dati tra i membri della cooperativa stessa, nonché *(ii)* di impiegare funzioni di *data analytics*, tali da abilitare la cooperativa alla prestazione di servizi *data-driven* [84]. Al riguardo, le attività di *data sharing* "interne" e di analisi dei dati di primario interesse per le cooperative di dati sono, in particolare, quelle aventi per oggetto i *dataset* risultanti dalla "integrazione" dei dati conferiti dai membri, le quali infatti consentono di trarre i benefici derivanti dalla dimensione collettiva e relazionale del fenomeno in esame: sul punto, va chiarito che il DGA consente ai servizi di cooperative di dati e agli altri servizi di *data intermediation* di svolgere attività di "*data pooling*", cioè di messa in comune dei dati forniti dai membri, quanto meno in funzione della loro condivisione [85].

---

[83] Sotto tale profilo, non rileva se le attività di supporto ai membri prevedano o meno il compimento di operazioni sui dati da loro forniti, posto che la neutralità, come descritto *supra* (par. 2.2.3), di base esclude la prestazione di qualsiasi servizio diverso da quello volto a mettere a disposizione i dati verso i *data users*.

[84] L'analisi dei dati conferiti dai membri risulta essenziale per consentire una proficua valorizzazione degli stessi a opera della cooperativa di dati A ogni modo, l'analisi dei dati, nelle *data cooperatives* diffuse nella prassi è impiegata anche quale mezzo per generare utilità in favore dei membri della cooperativa a prescindere dal compimento di operazioni di *data sharing*: il riferimento è all'analisi per generare utilità in favore dei soci direttamente (ad es., prestando servizi *data-based* a loro vantaggio) o indirettamente (come nel caso dello sfruttamento commerciale dei risultati dell'analisi sul mercato, al di fuori del paradigma del *data sharing*, ossia senza instaurare rapporti commerciali tra membri della cooperativa e utenti dei dati esterni). In merito, si consideri il modello commerciale della cooperativa di dati *Driver's Seat* (https://www.driversseat.co/), rispetto al quale si v. F. BRAVO, *Le cooperative di dati*, cit., p. 771 ss. (ove è altresì evidenziato il significativo rilievo della *data analytics* nel contesto delle cooperative di dati), nonché E. BIETTI-A. ETXEBERRIA-M. MANNAN-J. WONG, *Data Cooperatives in Europe: A Legal and Empirical Investigation*, cit., p. 8 ss. Simili attività, a ogni modo, non parrebbero implementabili nelle cooperative di dati previste dal DGA, nella misura in cui siano svincolate da un'operazione di *data sharing* intermediata.

[85] Il *data pooling* emerge dalla prassi e dalla letteratura come uno dei principali tratti caratterizzanti le cooperative di dati (in merito, v. ad es. AA.VV., *Data Access and Sharing in Germany and in the EU:*

3.2. Il *data sharing intra*-cooperativa di dati.

In base alla definizione di «servizi di cooperative di dati» prevista dall'art. 2, n. 15, Reg. cit. e al correlato *considerando* n. 31 Reg. cit., i membri della cooperativa di dati sembrano doversi qualificare come "interessati" o "titolari dei dati" e non anche quali "utenti dei dati". I membri, cioè, sarebbero soltanto dei *data suppliers* che la cooperativa di dati mira a supportare nel *data sharing* con utenti dei dati collocati all'esterno della stessa. Sul punto, l'applicazione del principio di neutralità, il quale impedisce agli intermediari dei dati di utilizzare i dati per scopi diversi dalla loro messa a disposizione dei *data users* (art. 12, lett. *a*), Reg. cit.), potrebbe allora far ritenere che le cooperative di dati non possano valorizzare i propri dati internamente alla cooperativa, mediante l'offerta di servizi di *data sharing* tra i propri membri.

Una simile configurazione risulterebbe limitante rispetto alle potenzialità del modello delle cooperative di dati, presupponendone una considerazione meramente parziale, ove le *data cooperatives* sono ravvisate in sostanza solo come mezzi per colmare le asimmetrie di potere informativo tra i soggetti allo stato ai margini della *data economy* (interessati, imprese individuali e PMI) e le *Big Tech*, senza considerare altre direzioni che potrebbero garantire a tali soggetti di partecipare attivamente alla valorizzazione dei propri dati, così restituendo loro un effettivo controllo sugli stessi e, contestualmente, appianando le distorsioni della concorrenza rilevabili nel mercato digitale.

Occorre chiedersi, allora, se i servizi di cooperative di dati contemplati dal DGA siano davvero limitati esclusivamente a quelli afferenti al modello di operatività "*Third Party*", nel quale i dati dei membri sono condivisi esclusivamente con soggetti esterni alla cooperativa di dati, oppure possano includere anche le forme di *data sharing* proprie del modello "*Member-to-Member*" (o "*intra-cooperative*") [86].

Towards a Coherent Legal Framework for the Emerging Data Economy, cit., p. 86; AA.VV., *White Paper on the Data Governance Act*, cit., p. 29; T. HARDJONO-A. PENTLAND, *Data Cooperatives: Towards a Foundation for Decentralized Personal Data Management*, cit., p. 2; AA.VV., *Mapping the Landscape of Data Intermediaries – Emerging Models for More Inclusive Data Governance*, cit., pp. 43, 47 e 50; E. BIETTI-A. ETXEBERRIA-M. MANNAN-J. WONG, *Data Cooperatives in Europe: A Legal and Empirical Investigation*, cit., p. 9). Nel Reg. UE n. 868/2022, la messa in comune dei dati risulta citata espressamente nel solo preambolo (cfr. *considerando* nn. 27-28 Reg. cit.), ma è comunque ravvisabile nell'articolato, sia in quanto il *data pooling* è da considerarsi come una delle possibili modalità tramite la quale realizzare la «condivisione dei dati» (art. 2, n. 10, Reg. cit.), sia perché il medesimo appare contemplato nel contesto della tassonomia dei servizi di intermediazione dei dati del DGA, in particolare rispetto al "tipo" di servizio di intermediazione di cui all'art. 10, lett. *a*), Reg. cit., laddove si legge che i servizi di tal fatta «possono includere scambi di dati bilaterali o multilaterali o la creazione di piattaforme o banche dati che consentono lo scambio o l'utilizzo congiunto dei dati, nonché l'istituzione di altra infrastruttura specifica per l'interconnessione di titolari dei dati con gli utenti dei dati» (in tal senso, cfr. ad es. AA.VV., *Mapping the Landscape of Data Intermediaries – Emerging Models for More Inclusive Data Governance*, cit., p. 41; AA.VV., *Data Access and Sharing in Germany and in the EU: Towards a Coherent Legal Framework for the Emerging Data Economy*, cit., p. 284).

[86] Per le distinzioni tra questi modelli, v. F. BRAVO, *Le cooperative di dati*, cit., p. 769.

Al riguardo, per valutare se la prestazione di servizi di condivisione dei dati internamente alla cooperativa di dati possa ritenersi conforme al principio di neutralità (art. 12, lett. *a*), Reg. cit.), preliminarmente occorre indagarne la coerenza con la stessa definizione di «servizi di cooperative di dati».

In merito, nonostante gli «obiettivi principali» delle cooperative di dati appaiano riferiti ad attività di *data sharing* esterno, sul presupposto dell'esistenza di un *gap* di potere informativo tra i membri della cooperativa e le imprese del mercato digitale che operano al di fuori della stessa [87], si ravvisano almeno due elementi che lasciano intendere come la prestazione di servizi di *data sharing* "interno" sia coerente con tale definizione: *(i)* l'art. 2, n. 15, Reg. cit. esplicita i soli obiettivi «principali» delle cooperative di dati e, in tal senso, non parrebbe ostare all'attribuzione in capo a tali soggetti, quali obiettivi "secondari", di attività di valorizzazione dei dati mediante l'offerta di servizi di intermediazione tra i membri della cooperativa stessa, i quali pertanto si qualificherebbero, a seconda del caso, come fornitori oppure utenti dei dati; *(ii)* la definizione dei «servizi di cooperative di dati» è ampia, limitandosi a indicare che sono tali i servizi di *data intermediation* offerti da una «struttura organizzativa» di cui si precisano i requisiti di composizione soggettiva e "funzionali", così offrendo una certa flessibilità per quanto concerne le caratteristiche dei servizi erogabili per raggiungere tali obiettivi, senza escludere la possibilità di implementare forme di *data sharing intra*-cooperativa.

Ciò rilevato, per quanto concerne la conformità della prestazione di simili servizi al principio di neutralità, si rileva come: *(i)* rispetto alla dimensione della limitazione della finalità, la condivisione dei dati internamente alla cooperativa comporti l'impiego dei dati oggetto dello scambio per il precipuo scopo di mettere questi ultimi a disposizione degli utenti dei dati, ivi rappresentati dagli stessi membri della cooperativa e, perciò, non consisterebbe in un utilizzo ultroneo a quanto previsto dall'art. 12, lett. *a*), Reg. cit.; *(ii)* in riferimento alla limitazione dei servizi erogabili, la condivisione interna sarebbe a tutti gli effetti un «servizio di intermediazione dei dati» e, pertanto, risulterebbe coerente con la disposizione poc'anzi citata; *(iii)* in ultimo, per le stesse ragioni appena indicate si avrebbe anche la piena conformità al requisito della separazione strutturale di cui alla medesima disposizione.

A ogni modo, rispetto al punto *(ii)* deve rilevarsi che il *data sharing* interno alla cooperativa di dati risulterà coerente con il principio di neutralità solo se tecnicamente considerabile quale erogazione di un «servizio di intermediazione dei dati» ai sensi dell'art. 2, n. 11, Reg. cit. [88]. In merito, è bene chiarire anzitutto che la condivisione all'interno di una certa organizzazione e tra i membri di quest'ultima non risulta in conflitto con il requisito dei servizi di *data intermediation* tale per cui i medesimi de-

---

[87] Cfr. ad es. il *considerando* n. 31 Reg. cit., correlato all'art. 2, n. 15, Reg. cit.

[88] A monte, resta ferma, infatti, la descritta criticità tale per cui le cooperative di dati delineate dal DGA sembrano potersi qualificare solo come fornitori di "servizi di intermediazione dei dati" (v. *supra*, par. 3).

vono essere finalizzati al *data sharing* tra un «numero indeterminato» di interessati, titolari e utenti dei dati (art. 2, n. 11, Reg. cit.). Gli stessi servizi di cooperative di dati, infatti, sono qualificati come "servizi di intermediazione dei dati" nonostante i *data suppliers*, nel loro contesto, appaiano costituiti esclusivamente dai membri di tale struttura. In ogni caso, con specifico riferimento alle cooperative di dati in forma societaria di cooperativa, un simile conflitto sarebbe scongiurato dall'operatività del principio della "porta aperta"[89]. D'altra parte, per quanto già rilevato non si avrebbe neppure un caso di utilizzo dei dati all'interno di un «gruppo chiuso», escluso dal perimetro dei servizi di infomediazione dall'art. 2, n. 11, lett. *c*), Reg. cit. Va poi ricordato che la coerenza al principio di neutralità come limitazione dei servizi richiederà che i servizi di intermediazione offerti dalla cooperativa di dati tra i propri membri siano diretti a instaurare «rapporti commerciali» tra gli stessi.

La fornitura di servizi di intermediazione dei dati tra gli stessi membri di una cooperativa di dati può dunque ritenersi compatibile con il principio di neutralità degli intermediari riguardo ai dati scambiati[90], purché sia progettata ed erogata coerentemente ai requisiti richiamati poc'anzi. Detti servizi sembrano doversi collocare tra gli obiettivi "secondari" delle cooperative di dati e, dunque, non potranno costituire il *core business* di tali organizzazioni: le tipologie di attività sottese agli obiettivi definiti dal DGA come «principali», infatti, in base al tenore letterale dell'art. 2, n. 15, Reg. cit. e alle indicazioni emergenti dal correlato *considerando*

---

[89] Il principio della porta aperta – il quale, dopo la riforma delle società di capitali e società cooperative realizzata con il d.lgs. 17 gennaio 2003, n. 6, risulta stabilito nel diritto positivo all'art. 2528 c.c. relativo al «carattere aperto della società» (ma v. anche l'art. 2527 c.c.) – al pari della causa mutualistica è qualificante la fattispecie della cooperativa, forma associativa strutturalmente aperta, ed è pertanto sottratto all'autonomia privata, la quale non può derogarvi con la previsione di apposite clausole statutarie o regolamenti (v. ad es. A. MAZZONI, *La porta aperta delle cooperative*, in P. ABBADESSA-G.B. PORTALE (diretto da), *Il nuovo diritto delle società.* Liber amicorum *Gian Franco Campobasso*, 2007, IV, p. 767 ss.). Sul principio della porta aperta, v. altresì F. GALGANO-R. GHENGHINI, *Il nuovo diritto societario*, cit., p. 957 ss.; A. BASSI, *Principi generali della riforma delle società cooperative*, cit., spec. p. 59 ss. (con riguardo all'impatto della riforma delle società cooperative); ID., *Le società cooperative*, cit., p. 147 ss. (su detto principio come tratto organizzativo "qualificante e indefettibile" delle società cooperative anche prima della sua introduzione con la citata riforma, anche in base alla caratteristica di variabilità del capitale). I requisiti e le procedure per l'ammissione di nuovi soci stabiliti dall'art. 2527 c.c. appaiono coerenti al paradigma FRAND stabilito per i fornitori di servizi di intermediazione dei dati all'art. 12, lett. *f*), Reg. cit.

[90] Più ampiamente, la conformità al DGA dei modelli di cooperative di dati che prevedano quali destinatari del servizio di intermediazione i soci cooperatori stessi è stata evidenziata anche in dottrina (cfr. F. BRAVO, *Le cooperative di dati*, cit., p. 778). Resta fermo che la gestione di tali transazioni di dati presenta dei profili di complessità, alla luce dei conflitti di interesse che potrebbero aversi, internamente alla cooperativa di dati, tra i membri parti dello scambio e quelli deputati a gestire quest'ultimo, rispetto ai quali si risente della criticità relativa all'assenza, tra le condizioni di cui all'art. 12 Reg. cit., di disposizioni *ad hoc* relative alla prevenzione e alla gestione del conflitto di interessi tra fornitore del servizio di intermediazione dei dati e utenti dei dati (v. F. BRAVO, *Intermediazione di dati personali e servizi di* data sharing *dal GDPR al* Data Governance Act, *Contratto e impresa Europa*, 2021, 1, p. 252).

n. 31 Reg. cit., letti alla luce degli obiettivi del *Data Governance Act* (nonché della sua base giuridica, costituita dall'art. 114 TFUE relativo all'instaurazione e al funzionamento del mercato interno), collocato nel contesto della strategia UE per i dati, appaiono infatti da riferirsi a forme di condivisione dei dati verso l'esterno. Il presupposto, invero, è che, allo scopo ultimo di addivenire a un mutamento di paradigma nel mercato interno, sia necessario supportare gli interessati, le imprese individuali e le PMI con specifico riguardo a detta condivisione, in ragione dello squilibrio di potere sussistente tra tali soggetti e quelli che dominano il mercato, i quali non sono (né possono essere) membri di una *data cooperative*, rappresentati dalle *Big Tech* o, comunque, da imprese operanti secondo modelli commerciali che limitano la possibilità per i citati fornitori dei dati di avvantaggiarsi "in prima persona" dei benefici estraibili dai dati [91].

In ultimo sul punto, benché la condivisione dei dati *intra*-cooperativa possa avvenire secondo una pluralità di modalità, come già rilevato la forma di condivisione interna maggiormente coerente con gli obiettivi delle cooperative di dati è costituita dalla messa in comune dei dati, che prevede la creazione di un *pool* dei dati dei membri volto ad agevolare questi ultimi nello scambio tra di essi dei propri dati. Il *data pooling* è invero particolarmente rispondente al modello delle cooperative di dati sia in generale, valorizzandone la dimensione collettiva, sia per come detto modello è delineato nel DGA, posto che, oltre ad abilitare un'agevole condivisione interna, contestualmente risulterebbe funzionale al perseguimento degli «obiettivi principali» affidati a tali intermediari, comportando infatti un aumento significativo della capacità delle cooperative di dati di supportare i propri membri nel *data sharing* esterno (ad esempio, nella negoziazione delle condizioni di utilizzo dei dati) [92], grazie appunto agli effetti dell'integrazio-

---

[91] Seguendo la logica del movimento cooperativo (al riguardo, v. F. GALGANO-R. GHENGHINI, *Il nuovo diritto societario*, cit., pp. 924 ss. e 957 ss.), le cooperative di dati tendono ad aggregare entro un soggetto collettivo soggetti afferenti a una "categoria sociale" che, dalle trame del regolamento europeo, appare predeterminata essenzialmente in termini oppositivi, in modo da comprendere i soli soggetti portatori di esigenze e interessi omogenei in quanto oggi ai margini dell'economia dei dati. Anche da tale elemento la cooperativa emerge come forma societaria "naturale" delle *data cooperatives*, posto che fin dalle origini la stessa si presenta come «espressione organizzata di classi economicamente subalterne, mosse dall'intento di sottrarsi all'egemonia delle classi economicamente dominanti» (*Ibidem*, p. 925), ma anche perché, comunque, come chiarito dalla Corte Costituzionale, «(…) alla protezione costituzionale della cooperazione si attribuisce una finalità che va oltre la generica tutela di categorie produttive deboli», estesa «al riconoscimento e alla promozione di una forma di produzione alternativa a quella capitalistica» (Corte cost., sent. n. 408/1989, richiamata altresì in L. PETRONE, *Il mercato digitale europeo e le cooperative di dati*, cit., p. 812).

[92] Si consideri che, laddove vi sia un terzo intermediario dei dati incaricato della materiale gestione del *dataset* integrato da offrire a terzi potenziali utenti dei dati, il *data pool* può essere finalizzato anche esclusivamente a tale tipo di *data sharing*, senza prevedere l'instaurazione di rapporti commerciali tra i *data suppliers* (in merito, v. ad es. AA.VV., *Business to Business Data Sharing: an Economic and Legal Analysis*, in *Digital Economy Working Paper* 2020-05, European Commission, Seville, 2020, pp. 6 e 29). Resta fermo che il *data pooling* può essere impiegato anche al di fuori dei servizi di

ne dei dati [93]. A ogni modo, di nuovo, il *data pooling* sarà coerente con la neutralità solo se inteso come meccanismo per la condivisione intermediata dei dati [94].

3.3. Cooperative di dati e *data analytics*.

3.3.1. *La* data analytics *nel Reg. UE n. 868/2022.*

La possibilità per le cooperative di dati e gli altri fornitori di servizi di intermediazione di dati delineati dal Reg. UE n. 868/2022 di effettuare attività di *data analytics* risulta dibattuta in dottrina e tendenzialmente esclusa, principalmente in ragione dei limiti derivanti dal principio di neutralità [95].

---

data intermediation, casistica che, allo stato, non parrebbe rilevante nel contesto delle cooperative di dati delineate dal DGA, in ragione dell'applicazione del principio di neutralità.

[93] V. ad es. AA.VV., *Data Aaccess and Sharing in Germany and in the EU: Towards a Coherent Legal Framework for the Emerging Data Economy*, cit., spec. p. 86. In ogni caso, le cooperative di dati sono un modello di *data governance* che presenta vantaggi anche per gli utenti dei dati, alla luce della funzione di "raggruppamento" operata nei loro confronti (v. *supra*, par. 3.1), posto anche che l'interesse di costoro è normalmente rivolto verso i *dataset* risultanti dall'integrazione di dati provenienti da più fonti, visto che le banche di dati aggregate sono soggette agli effetti positivi delle economie sia di scala (*dataset* con più *record*) sia di scopo (*dataset* con più variabili relative ai medesimi *record*) e che, in tali casi, la *value proposition* dell'intermediario dei dati consiste precipuamente nell'offrire *dataset* che siano integrati (cfr. AA.VV., *Mapping the Landscape of Data Intermediaries – Emerging Models for More Inclusive Data Governance*, cit., p. 36 e riferimenti bibliografici ivi riportati).

[94] In dottrina, vi è chi ha ritenuto che le cooperative di dati non possano effettuare il *pooling* dei dati, in quanto quest'ultimo non sarebbe riportabile agli obiettivi stabiliti all'art. 2, n. 15, Reg. cit. In merito, è sufficiente richiamare le osservazioni sulla circostanza che l'ampia definizione dei «servizi di cooperative di dati» non reca alcuna limitazione rispetto ai servizi di *data intermediation* erogabili dalle cooperative di dati, consentendo l'implementazione di qualsivoglia modalità di *data sharing* che sia coerente con i requisiti soggettivi e teleologici prestabiliti dalla stessa. Le interpretazioni volte ad escludere tale possibilità, allora, sembrano confondere gli obiettivi (principali) attribuiti dal DGA alle cooperative di dati con le attività che queste ultime sono abilitate a svolgere e, nella specie, con le modalità che, nell'esercizio della propria libertà d'impresa, possono liberamente adottare per l'erogazione dei servizi di intermediazione dei dati. Si consideri, ad esempio, quanto rilevato in E. BIETTI-A. ETXEBERRIA-M. MANNAN-J. WONG, *Data Cooperatives in Europe: A Legal and Empirical Investigation*, cit., p. 17, ove è indicato che, alla luce della definizione di servizi di cooperative di dati offerta dal DGA, «*For instance, cooperatives that seek to pool and process aggregated data would not fit within the three functions*»: in tal caso, è evidente che vi è una sostituzione tra obiettivi ("*functions*") della cooperative e attività effettuabili da queste ultime per il perseguimento degli stessi. Quelle di *pooling* dei dati e di elaborazione del dataset così integrato sono attività che possono essere rivolte al perseguimento di molteplici finalità, tra le quali certamente quelle previste dall'art. 2, n. 15, Reg. cit.

[95] In tal senso, v. ad es. G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit. p. 993; L. PETRONE, *Il mercato digitale europeo e le cooperative di dati*, cit., p. 815; G. CAROVANO-M. FINCK, *Regulating Data Intermediaries: The impact of the Data Governance Act on the EU's Data Economy*, cit., p. 8; L. VON DITFURTH-G. LIENEMANN, *The Data Governance Act: – Promoting or Restricting Data Intermediaries?*, cit., p. 291. Altri autori ritengono le attività di *data analytics* incompatibili con le cooperative di dati anche in virtù della stessa definizione di «servizi di

Il *Data Governance Act*, a ogni modo, non reca espliciti divieti relativamente allo svolgimento di attività di analisi dei dati nel contesto dei servizi di cooperative di dati, né in riferimento alle altre tipologie di servizi di intermediazione dei dati [96].

A ben vedere, dalle trame del *Data Governance Act* emergono piuttosto diversi casi in cui i fornitori di servizi di intermediazione dei dati potrebbero ritenersi legittimati ad effettuare attività di *data analytics*.

Anzitutto, l'intermediario potrebbe compiere attività di analisi dei dati per propri scopi, in deroga al principio di neutralità come limitazione della finalità, nell'esercizio della facoltà di effettuare attività *data-based*, aventi per oggetto i metadati generati nella fornitura del servizio, per finalità di "sviluppo" ("*development*") o, secondo il *considerando* n. 33 Reg. cit., "miglioramento" ("*improvement*") del servizio, conformemente all'art. 12, lett. *c*), Reg. cit. In merito, va infatti rilevato come il perseguimento di detto scopo possa certamente comprendere l'implementazione di tecnologie di analisi dei dati: basti considerare le "micro-finalità" di individuazione delle frodi e di cibersicurezza che la disposizione citata esemplifica come ipotesi di utilizzo a tale scopo dei metadati, rispetto al soddisfacimento delle quali, a seconda del caso, potrebbe rendersi opportuna o anche necessaria l'adozione di strumenti che, allo stato dall'arte, siano basati su funzionalità di *data analytics* [97].

---

cooperative di dati» prevista dal DGA: v. E. BIETTI-A. ETXEBERRIA-M. MANNAN-J. WONG, *Data Cooperatives in Europe: A Legal and Empirical Investigation*, cit., p. 17; AA.VV., *Mapping the Landscape of Data Intermediaries – Emerging Models for More Inclusive Data Governance*, cit., p. 38 (ma v. p. 64, ove è precisato, rispetto alle incertezze poste dai requisiti di neutralità previsti dal DGA, che ad essere vietate non sono le attività di aggregazione ed analisi dei dati come tali, bensì il loro sfruttamento per realizzare servizi con fini di lucro).

[96] L'impostazione del DGA sull'effettuazione delle attività *data-based* da parte degli intermediari dei dati è di tipo funzionale: di base, non sono vietate determinate attività in quanto tali, ma ne è limitato lo svolgimento a seconda dello scopo perseguito (cfr. ad es. i requisiti di cui all'art. 12, lett. *a*), *c*), *d*), *e*), Reg. cit.). Per quanto concerne la *data analytics*, espresse disposizioni del regolamento in merito si rinvengono nel solo preambolo: *(i)* al *considerando* n. 28 Reg. cit., ove è indicato che la fornitura di servizi di analisi, al pari di altri servizi, non dovrebbe essere considerata come fornitura di un «servizio di intermediazione dei dati» ai sensi del DGA (art. 2, n. 11, Reg. cit.), per chiarire il perimetro della definizione di tali servizi evidenziando come la mera fornitura di determinati strumenti o servizi *data-based* non rientri in detta definizione, a meno che risulti accompagnata dagli altri elementi richiesti dalla stessa; *(ii)* al *considerando* n. 33 relativo alla neutralità degli intermediari dei dati, in riferimento al divieto di pratiche leganti di cui all'art. 12, lett. *b*), Reg. cit., nel quale sono esemplificati alcuni degli "altri servizi" rispetto ai quali opera tale divieto, includendo tra questi l'analisi dei dati (così come la conservazione dei dati, le applicazioni di *AI*, ecc.), per poi prevedere che «ciò renderà altresì necessaria una separazione strutturale tra il servizio di intermediazione dei dati e qualsiasi altro servizio fornito». Questo *considerando* conferma che l'analisi dei dati, così come le altre attività aventi per oggetto i dati, se prestate come servizio andrebbero distinte da quello di intermediazione dei dati, rispetto al quale si qualificherebbero alla stregua di "altri servizi", ma non esclude che gli intermediari dei dati, cooperative di dati incluse, possano prestare attività di *data analytics*, come meglio si vedrà a seguire.

[97] Sull'impiego di tecnologie di analisi dei dati per scopi di cibersicurezza, v. ad es. V.P. JANEJA, *Data Analytics for Cybersecurity*, Cambridge, 2022.

L'utilizzo di strumenti di tal fatta potrebbe risultare rilevante altresì per l'adempimento di taluni obblighi imposti dal DGA agli intermediari dei dati, come nel caso dell'adozione delle misure occorrenti per garantire un livello adeguato di sicurezza dei dati non personali (art. 12, lett. *j*) e *l*), Reg. cit.) o il massimo livello di sicurezza delle informazioni sensibili sotto il profilo della concorrenza (art. 12, lett. *l*), Reg. cit.) o, ancora, la prevenzione di pratiche fraudolente o abusive (art. 12, lett. *g*), Reg. cit.).

La necessità di implementare tali strumenti nel contesto dell'adozione di misure di *data security* può discendere anche dall'applicazione di normative diverse dal DGA e, segnatamente, dagli obblighi di sicurezza imposti agli intermediari dei dati in base alla normativa in materia di protezione dei dati personali [98].

Ulteriore indice della possibilità o doverosità per gli intermediari dei dati di offrire strumenti o servizi di analisi dei dati si rinviene nel contesto della tipologia dei servizi di intermediazione erogati verso gli interessati (art. 10, lett. *b*), Reg. cit.), in riferimento a quanto previsto dal *considerando* n. 30 Reg. cit. Tali servizi, infatti, comprenderebbero la fornitura dei cc.dd. "spazi di dati personali", quali contesti in cui far confluire i dati personali degli interessati «affinché il trattamento possa aver luogo all'interno di tale spazio senza che i dati personali siano trasmessi a terzi, al fine di ottimizzare la protezione dei dati personali e della vita privata», segnatamente abilitando un maggior controllo sull'impiego dei dati a opera dei *data users*, tale da mitigare i rischi presentati dal trattamento per i diritti e le libertà degli interessati. Il fornitore del servizio di intermediazione dei dati, in tal caso, per rendere possibile l'impiego dei dati nel *personal data space* deve evidentemente poter implementare al suo interno ogni strumento in tal senso necessario, inclusi, se del caso, quelli di *data analytics*: in questi scenari, dunque, l'utilizzo dei dati da parte dell'intermediario per mettere questi ultimi a disposizione degli utenti dei dati (art. 12, lett. *a*), Reg. cit.) comprende anche la fornitura dei mezzi necessari al *data user* per fruire di tali dati; ciò, nell'interesse dei *data subjects*. L'esempio degli spazi di dati personali è particolarmente significativo per le questioni in esame, perché sottende un'interpretazione della neutralità come limitazione dei servizi erogabili orientata dalla specifica funzione *ex lege* attribuita agli intermediari afferenti alla tipologia di cui all'art. 10, lett. *b*), Reg. cit.: a costoro è imposto l'obbligo fiduciario di agire nel superiore interesse dei *data subjects* (art. 12, lett. *m*), Reg. cit.) e ciò richiede di contemperare il principio di neutralità con le esigenze della *data protection*, in modo da consentire la condivisione dei dati con modalità maggiormente conformi a queste ultime.

---

[98] Rispetto all'esigenza di adottare misure di sicurezza basate sull'analisi dei dati (ad es., sistemi di *Data Loss Prevention*, strumenti di analisi dei *log* delle attività compiute dagli utenti e dei tentativi di accesso a una piattaforma *web*, ecc.) per garantire la conformità al principio di integrità e riservatezza e ai correlati obblighi di sicurezza imposti dal regolamento generale sulla protezione dei dati (artt. 5, par. 1, lett. *f*) e 32, Reg. UE n. 679/2016), va ricordato che il *Data Governance Act* non pregiudica il diritto eurounitario in materia di *data protection* (art. 1, par. 3, Reg. UE n. 868/2022).

Una simile conclusione, a ogni modo, deve essere raccordata con la complessiva disciplina che governa la fornitura dei servizi di intermediazione dei dati. In particolare, occorre considerare la descritta eccezione al principio di neutralità di cui all'art. 12, lett. *e*), Reg. cit., la quale, nel disciplinare le condizioni in base alle quali i servizi di *data intermediation* possono comprendere l'offerta di strumenti e servizi supplementari specifici a interessati e titolari dei dati, adotta un'impostazione profondamente granulare, tale da attrarre nel suo spettro applicativo, in sostanza, qualsiasi tipo di attività sui dati, prevista nel contesto di uno strumento o servizio offerto ai *data suppliers*, che sia diversa dalla mera "messa a disposizione" dei dati verso gli utenti dei dati [99]. Ferma restando la prevalenza sul DGA della normativa in materia di protezione dei dati personali, occorre allora comprendere se gli spazi di dati personali debbano essere collocati entro tale norma: al riguardo, va rilevato come non sia chiaro se e in quale misura i servizi per ottimizzare la protezione dei dati personali (da implementare anche in base al richiamato obbligo fiduciario di cui all'art. 12, lett. *m*), Reg. cit.) debbano considerarsi quali "servizi aggiuntivi" assoggettati alla citata lett. *e*); a monte, più ampiamente, ad essere opaco è lo stesso rapporto tra le differenti condizioni che regolano la fornitura dei servizi di *data intermediation* (art. 12) [100]. Ciò detto, stante la granularità ravvisabile nell'art. 12, lett. *e*), Reg. cit. e la sua natura di eccezione rispetto al principio di neutralità, di base le attività sui dati da svolgere nell'ambito di un servizio o uno strumento offerto dagli intermediari ai fornitori dei dati paiono doversi collocare nel perimetro di tale requisito, il quale contribuisce a delineare la complessiva portata applicativa del principio di neutralità come limitazione dei servizi erogabili.

Proseguendo oltre, si evidenzia che la disciplina sui servizi supplementari prevista dall'art. 12, lett. *e*), Reg. cit., al di là del caso dei *personal data spaces*, rappresenta un altro possibile alveo entro il quale collocare la legittima prestazione di attività di *data analytics* a opera dei fornitori di servizi di intermediazione dei dati, cooperative di dati incluse, come meglio approfondito a seguire [101].

3.3.2. *La necessità di un'interpretazione della disciplina sulla fornitura dei servizi di intermediazione dei dati coerente con gli obiettivi assegnati alle cooperative di dati dal* Data Governance Act*, con specifico riferimento alle attività* data-driven *di analisi dei dati.*

Chiarito come il DGA non impedisca agli intermediari dei dati di svolgere attività di *data analytics*, per comprendere entro quali limiti l'impiego di servizi di tal fatta sia ammissibile nello specifico contesto delle cooperative di dati, in via preli-

---

[99] Nell'ottica dell'art. 12, lett. *e*), Reg. cit., ad esempio, anche la mera "conservazione temporanea" è un servizio da ritenersi aggiuntivo a quelli di intermediazione dei dati, in quanto tale erogabile solo entro i limiti previsti da tale norma.

[100] Più in generale, sulle difficoltà interpretative che interessano l'art. 12 DGA, v. ad es. L. VON DITFURTH, *Datenmärkte, Datenintermediäre und der Data Governance Act*, cit., p. 558 ss.

[101] V. *infra*, par. 3.3.3.

minare occorre muovere da alcune considerazioni sui limiti che mostra l'approccio "*one-size-fits-all*" seguito dal DGA quando posto innanzi alle peculiarità di tali intermediari [102].

I servizi di cooperative di dati, pur afferendo al *genus* dei servizi di intermediazione dei dati, presentano dei rilevanti tratti distintivi rispetto agli altri tipi di intermediari e si pongono a una certa distanza dal modello che prevede una netta separazione tra le attività di fornitura, intermediazione e utilizzo dei dati, nonché l'indipendenza dell'intermediario dalle parti della transazione. Ciò, segnatamente, non è un'anomalia, ma un mezzo per realizzare gli stessi obiettivi sottesi alla *European way of data governance* e alla strategia europea per i dati: le cooperative di dati sono state delineate come intermediari che si distaccano dai pilastri di tale modello in virtù della specifica conformazione ravvisabile nella dimensione fattuale del fenomeno che si è inteso regolare; innanzi a un mercato connotato dal predominio delle *Big Tech* e mosso dalle dinamiche auto-referenziali dell'accumulazione del capitale, invero, le *data cooperatives* si presentano come uno strumento di contrasto per ristabilire il rispetto dei valori e del diritto UE.

Questi elementi si riflettono necessariamente nella disciplina della fornitura dei servizi di intermediazione dei dati e, per quanto qui di interesse, impongono un'interpretazione delle disposizioni da cui emerge il principio di neutralità riguardo ai dati scambiati, previste in particolare all'art. 12, lett. *a*), *c*) ed *e*), Reg. cit., che tenga conto delle peculiarità delle cooperative di dati alla luce dei complessivi obiettivi e finalità del *Data Governance Act* [103].

In tal senso, la limitazione dello scopo di utilizzo dei dati oggetto dello scambio alla "messa a disposizione" degli stessi verso gli utenti dei dati (art. 12, lett. *a*), Reg. cit.) che è alla base della neutralità deve essere intesa nella logica delle cooperative di dati, con una perimetrazione che includa le forme di utilizzo dei dati occorrenti per consentire di soddisfare l'interesse dei membri della cooperativa e, così, gli obiettivi perseguiti dallo stesso DGA mediante tali intermediari. La disciplina che regola l'operatività delle *data cooperatives* sui dati forniti dai propri membri non può essere sciolta dagli «obiettivi principali» che tali organizzazioni sono tenute per legge a perseguire, il raggiungimento dei quali può richiedere necessariamente il compimento di determinate operazioni sui dati forniti dai membri.

---

[102] Sui limiti di tale approccio, v. ad es. L. VON DITFURTH, *Datenmärkte, Datenintermediäre und der Data Governance Act*, cit., p. 268; ID.-G. LIENEMANN, *The Data Governance Act: – Promoting or Restricting Data Intermediaries?*, cit., p. 290 ss.; G. CAROVANO-M. FINCK, *Regulating Data Intermediaries: The impact of the Data Governance Act on the EU's Data Economy*, cit., p. 3.

[103] Ciò, anche in ragione delle necessità di interpretare le disposizioni del diritto dell'Unione tenendo conto non solo della loro formulazione, ma anche del contesto in cui le stesse si inseriscono, così come degli obiettivi e delle finalità perseguite dall'atto di cui tali disposizioni fanno parte, in conformità alla consolidata giurisprudenza della Corte di giustizia UE (cfr. di recente, ad es., CGUE, 7 marzo 2024, *IAB Europe*, causa C-604/22, pt. 34; CGUE, 22 giugno 2023, *Pankki S*, causa C-579/21, pt. 38; CGUE, 12 gennaio 2023, *Österreichische Post*, causa C-154/21, pt. 29; più lontano nel tempo, v. CGUE, 6 ottobre 1982, *Srl CILFIT and Lanificio di Gavardo SpA v Ministry of Health*, causa C-283/81).

Le attività *data-driven*, analisi dei dati inclusa, possono infatti risultare indispensabili per il funzionamento delle cooperative di dati. Si consideri l'obiettivo attribuito a tali soggetti di «procedere a uno scambio di opinioni sulle finalità e sulle condizioni del trattamento dei dati che rappresenterebbero *al meglio* gli interessi dei propri membri in relazione ai loro dati» (art. 2, n. 15, Reg. cit.). Nell'attuale contesto tecnologico, non è pensabile che quest'obiettivo possa essere raggiunto senza l'analisi del *dataset* integrato risultante dai dati "conferiti" dai membri. Lampante, sul punto, è il caso della *Big Data Analytics*: com'è noto, nella stessa è soltanto grazie all'analisi dei dati che possono essere individuati i possibili scopi di impiego dei dati che consentono di valorizzare al meglio il patrimonio informativo a disposizione, in virtù dell'emersione di correlazioni tra i dati che aprono a scenari di utilizzo non altrimenti immaginabili *ex ante* [104]. L'analisi dei dati è pertanto necessaria per individuare in che modo utilizzare i dati e, dunque, quali siano le condizioni che consentano di valorizzare gli stessi *nel modo più vantaggioso possibile* per realizzare gli interessi dei membri [105].

La medesima necessità è ravvisabile anche rispetto agli altri obiettivi delle cooperative di dati: in breve, le informazioni estraibili dal *dataset* integrato mediante l'analisi dei dati possono costituire il presupposto necessario per l'effettivo conseguimento degli stessi, ossia per stimolare una proficua dialettica interna alla cooperativa sui migliori utilizzi dei dati, per influenzare i termini e le condizioni di utilizzo dei dati nel modo meglio rispondente all'interesse dei membri, così come per dotare tali intermediari delle informazioni necessarie per dirigere le negoziazioni verso il medesimo risultato [106]. D'altra parte, per le *data cooperatives* di "interessati" una simile conclusione è rafforzata dall'obbligo dell'intermediario di agire nel superiore interesse di costoro [107].

---

[104] Sull'analisi dei *Big Data*, v. V. MAYER-SCHÖNBERGER-K. CUKIER, *Big data. Una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*, Milano, 2013. Sulle questioni giuridiche poste dai *Big Data*, con particolare attenzione ai profili di protezione dei dati personali, v. ad es. G. BUTTARELLI, *Le sfide del "*Big Data*" tra evoluzione tecnologica, etica e interessi collettivi*, cit., pp. 30-39; V. ZENO-ZENCOVICH, *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, cit., pp. 1-7; A. MANTELERO, *Big Data and Data Protection*, in G. GONZÁLEZ-FUSTER-R. VAN BRAKEL-P. DE HERT (eds.), *Research Handbook on Privacy and Data Protection Law. Values, Norms and Global Politics*, Cheltenham, 2022, pp. 335-357.

[105] In mancanza, i *data suppliers* associati nella cooperativa non avrebbero la capacità di rimediare effettivamente allo squilibrio informativo sussistente verso gli operatori economici che dominano il mercato: la dialettica tra i membri, pur agevolata dalla dimensione collettiva della cooperativa di dati, potrebbe consentire, tutt'al più, di identificare condizioni di impiego dei dati migliori di quelle che avrebbero individuato i singoli membri da sé, ma non sarebbe certamente sufficiente per il raggiungimento dell'obiettivo di identificare quelle che rappresenterebbero "al meglio" gli interessi dei membri (art. 2, n. 15, Reg. cit.).

[106] Il rilievo essenziale della *data analytics* per un'efficace attività negoziale con i terzi è evidenziato ad es. in G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit., p. 993.

[107] Ad esempio, nell'influenzare in tal senso i termini e le condizioni preconfezionati dagli utenti dei dati (cfr. *considerando* n. 31 e art. 12, lett. *m*), Reg. cit.).

Di conseguenza, non appare ammissibile un'interpretazione delle condizioni previste per la generalità dei servizi di intermediazione dei dati tale da limitare, fino ad impedire, la possibilità per le cooperative di dati di raggiungere i propri obiettivi [108]. La specificità di tale intermediario impone, in ottica sistematica, una coerente applicazione delle condizioni di cui all'art. 12 del DGA e, dunque, una differente configurazione della portata applicativa del principio di neutralità.

Escludere le cooperative di dati dalla possibilità di svolgere le attività in esame potrebbe privare le disposizioni del *Data Governance Act* che regolano tali intermediari del loro effetto utile [109], impedendo in ultimo che tale regolamento, mediante questi tipi di servizi di intermediazione, possa effettivamente raggiungere i propri obiettivi (come detto, coincidenti in larga parte con quelli cui tende lo stesso principio di neutralità).

Per completezza, si rileva altresì come non appaiano convincenti le ricostruzioni alternative in base alle quali i membri della cooperativa di dati dovrebbero reperire i servizi per analizzare i dati da loro forniti al di fuori della cooperativa di dati. In tali scenari, permarrebbe la criticità di una fattispecie che non riuscirebbe a raggiungere gli obiettivi stabiliti dal proprio schema legale, posto che la cooperativa di dati non sarebbe nelle condizioni di realizzare al meglio gli interessi dei propri membri, i quali dovrebbero rimediare a un congegno legislativo difettoso procurandosi in altri contesti gli strumenti necessari per valorizzare adeguatamente i propri dati mediante la cooperativa stessa. Comunque sia, tali modalità, oltre che macchinose, confliggerebbero con gli obiettivi del DGA di aumentare il controllo di interessati e imprese sui dati di propria afferenza e di assicurare la sicurezza dei dati, nonché, per quanto concerne i dati personali, con le esigenze di tutela delle persone con riguardo al trattamento di tali dati discendenti dal quadro normativo UE in materia [110].

---

[108] Le cooperative di dati devono essere poste nelle condizioni di supportare i propri membri confrontandosi ad armi pari con le società che dominano il mercato, le quali hanno a loro disposizione l'immenso capitale informativo già accumulato e le tecnologie *data-driven* sviluppate essenzialmente sulla base di tale patrimonio. In mancanza, il rischio è che le cooperative di dati non abbiano modo di supportare al meglio i propri membri, mentre le *Big Tech* manterrebbero il proprio vantaggio competitivo e, con ciò, la possibilità di perpetuare le distorsioni della concorrenza attualmente rilevabili nel mercato interno, estendendole in ultimo ai nascenti mercati dell'infomediazione.

[109] In base al criterio interpretativo dell'"effetto utile", com'è noto, quando una disposizione del diritto UE è suscettibile di più interpretazioni va privilegiata quella che riconosce alla stessa maggiore effettività, consentendone di raggiungere in modo più efficace i propri obiettivi. Sull'effetto utile, v. I. INGRAVALLO, *L'effetto utile nell'interpretazione del diritto dell'Unione europea*, Bari, 2017.

[110] In detti scenari, infatti, si avrebbe un'amplificazione dell'ambito di circolazione dei dati e una duplicazione dei *dataset* da analizzare verso soggetti esterni alla cooperativa di dati, circostanze che espongono i membri della stessa a conseguenze negative in termini di aumento del rischio di perdita del controllo sui dati e delle conseguenti lesioni per i diritti e le libertà connessi al trattamento di questi ultimi che potrebbero derivarne (rispetto al trattamento di dati personali, sulla circostanza che la presenza dei dati personali in più fonti rafforzi l'ingerenza nel diritto alla vita privata, cfr. CGUE, 7 dicembre 2023, *Schufa*, cause riunite C-26/22 e C-64/22, pt. 100; CGUE, 3 maggio 2014, *Google*

3.3.3. *Collocazione dei servizi di* data analytics *prestati dalle cooperative di dati nel DGA.*

Tanto precisato, occorre brevemente approfondire la collocazione dei servizi di *data analytics* nel contesto delle cooperative di dati, offrendo degli spunti di riflessione con specifico riguardo ai requisiti di cui all'art. 12, lett. *c*) ed *e*), Reg. UE n. 868/2022 [111].

Anzitutto, i servizi di analisi potrebbero essere impiegati rispetto ai metadati, per le finalità proprie della cooperativa di dati di sviluppare o migliorare il proprio servizio (art. 12, lett. *c*), Reg. cit.), intendendo detta finalità in coerenza con gli obiettivi principali di questo tipo di intermediario. Nelle cooperative di dati, quali organizzazioni deputate a fornire supporto ai propri membri, lo sviluppo del servizio potrà allora comprendere, oltre ai profili accessori relativi alle esigenze di prevenzione delle frodi e cibersicurezza, anche le attività funzionali a migliorare la stessa capacità della cooperativa di perseguire i propri obiettivi di legge. Si consideri, a titolo indicativo, l'effettuazione di analisi statistiche periodiche dei metadati generati nel contesto delle negoziazioni e delle transazioni di dati eventualmente risultanti dalle stesse che la cooperativa ha gestito nell'interesse dei membri, la quale potrà fornire informazioni utili, ad esempio, per individuare più efficaci modalità di gestione delle negoziazioni stesse in futuro e, dunque, rafforzare la capacità dell'ente di fornire consulenza e assistenza ai propri membri.

Proseguendo oltre, ben più pregnante è il rilievo, in questa chiave di lettura, dei servizi di analisi dei dati prestati dalle cooperative di dati in favore dei propri membri quali servizi "supplementari" ai sensi dell'art. 12, lett. *e*), Reg. cit., disposizione nel contesto della quale pare infatti da collocare la prestazione dei servizi di analisi, esemplificati appena sopra, che si rendono necessari per abilitare la cooperativa di dati a soddisfare i propri obiettivi.

La facoltà riconosciuta da tale norma agli intermediari dei dati di prestare strumenti e servizi aggiuntivi a quelli consistenti nella messa a disposizione dei dati verso i *data users* è connotata da limiti particolarmente rigorosi, discendenti anche dalla natura eccezionale di tale disposizione, che ne impone una stretta interpretazione. In sintesi, per quanto qui interessa, detti servizi potrebbero essere prestati solo allo «scopo specifico di facilitare lo scambio», in base pertanto a un vincolo funzionale "forte", che *prima facie* parrebbe tale da consentire l'erogazione dei soli servizi aventi intrinsecamente caratteristiche che limitino la valorizzazione dei dati a quanto necessario per l'agevolazione dello scambio, ad esclusione invece di quelli che abiliterebbero l'intermediario stesso ad estrarre il contenuto informativo del dato, incentivandolo ad operare nella *data value chain*. A supporto di una simile

---

Spain, causa C-131/12, ptt. 86 e 87). Nel caso di fruizione dei servizi di analisi offerti dalle *Big Tech*, peraltro, per i membri il rischio è anche quello di accettare condizioni inique per il trattamento previsto nell'analisi dei dati, ciò riproponendo il problema che si intende risolvere.

[111] La conformità della prestazione di simili servizi con il principio di neutralità è invece approfondita *infra*, par. 3.3.4.

interpretazione, vi sarebbe la circostanza che le attività indicate nell'elenco esemplificativo di cui all'art. 12, lett. *e*), Reg. cit. non comprenderebbero servizi *data-driven*, come appunto l'analisi dei dati.

Tanto premesso, interpretando questa disposizione alla luce degli obiettivi prestabiliti dal DGA per le *data cooperatives*, i servizi supplementari dovrebbero ritenersi comprensivi anche di quelli necessari per «facilitare lo scambio dei dati» secondo la peculiare logica delle cooperative di dati, ossia di quegli strumenti o servizi che facilitino lo scambio in termini tali da supportare i membri dell'organizzazione nell'esercizio dei loro diritti o nell'individuazione delle finalità e delle condizioni di impiego dei dati che consentano di realizzare al meglio i loro interessi o ancora nella negoziazione delle condizioni di trattamento nella medesima ottica.

Così intesa, la disposizione ben si presta ad accogliere la possibilità per la cooperativa di dati di offrire servizi *data-driven*, laddove necessari, appunto, per lo specifico scopo di agevolare lo scambio in armonia al perseguimento degli obiettivi principali di cui all'art. 2, n. 15, Reg. cit.[112]. Ciò, considerato anche che l'art. 12, lett. *e*), Reg. cit. riguarda la fornitura di servizi aggiuntivi solo in favore della parte della transazione costituita da interessati o titolari di dati, su loro richiesta o approvazione esplicita, limitazione coerente con la struttura della cooperativa di dati quale soggetto tenuto ad agire nell'interesse dei *data subjects* o dei titolari dei dati che ne sono membri. La logica di fondo, come si accennava, è analoga a quella ravvisabile nell'implementazione degli spazi di dati personali (*considerando* n. 30 Reg. cit.) entro i servizi di intermediazione *ex* art. 10, lett. *b*), Reg. cit., ove la neutralità risulta contemperata dal rilievo delle altre esigenze concorrenti, relative alla protezione dei dati personali (le quali, peraltro, si rinvengono anche nelle *data cooperatives* di "interessati").

Ciò rilevato, la sistemazione delle attività di analisi dei dati a opera delle *data cooperatives* tra i servizi aggiuntivi previsti dalla disposizione citata non esaurisce certamente le questioni e criticità rilevanti, di grande impatto pratico, il cui approfondimento tuttavia dovrà essere demandato a future ricerche[113].

3.3.4. *Conformità della prestazione di servizi di analisi dei dati a opera delle cooperative di dati al principio di neutralità.*

Si è detto che le condizioni di cui all'art. 12 Reg. UE n. 868/2022 devono essere interpretate in modo da salvaguardare la possibilità per i servizi di cooperative di dati di raggiungere gli obiettivi principali loro attribuiti dal regolamento europeo.

---

[112] Sul punto, rispetto alla natura eccezionale di questa disposizione, che è perciò da interpretarsi restrittivamente, va rilevato che la lett. *e*) dell'art. 12 DGA reca un elenco meramente esemplificativo dei possibili servizi aggiuntivi e si presta, pertanto, ad accoglierne degli altri, laddove coerenti con i requisiti previsti dalla norma e, specialmente, con il vincolo della facilitazione dello scambio, il quale, come detto, ivi deve essere letto, in ottica sistematica, in armonia con gli obiettivi legali di supporto dei membri che connotano le cooperative di dati.

[113] Si pensi, ad esempio, alla questione relativa alla legittimità dell'impiego delle informazioni risultanti dall'analisi dei dati come oggetto di successive transazioni intermediate.

Occorre ora approfondire più specificamente la conformità delle proposte interpretative evidenziate al principio di neutralità, considerando in particolare le funzioni perseguite da quest'ultimo.

Anzitutto, rispetto alla funzione di rafforzamento del controllo sui dati di interessati e titolari dei dati nel contesto dei servizi di intermediazione dei dati, in modo da incrementare la fiducia in tali servizi, la fornitura di servizi di analisi dei dati da parte delle cooperative di dati, nei termini poc'anzi descritti, non appare particolarmente problematica. Ciò, grazie almeno a due elementi atti a limitare possibili impatti negativi: *(i)* la circostanza che le cooperative di dati sono composte dai fornitori dei dati e vincolate dalla necessità di supportare questi ultimi, la quale mitiga i possibili conflitti di interesse tra questo intermediario e i propri membri con riguardo ai dati scambiati [114]; *(ii)* la disciplina stabilita per il tipo societario "fisiologico" delle cooperative di dati, ossia la società cooperativa [115], che è tale da limitare possibili utilizzi dei dati a opera dell'intermediario con modalità che ne riducano il controllo da parte dei membri, posto che le cooperative operano secondo dinamiche di autogestione [116], democratiche, dialogiche, sulla base del principio del voto per teste [117], necessariamente per scopi mutualistici e senza fini di speculazione privata (art. 45 Cost.) [118].

Si consideri, ad esempio, la neutralità come limitazione della finalità. Al riguardo, il divieto di cui all'art. 12, lett. *a*), Reg. cit. è stato inteso come misura di contrasto all'asimmetria informativa *ex post*, rischio che nelle cooperative dei dati appare limi-

---

[114] Cfr. L. VON DITFURTH, *Datenmärkte, Datenintermediäre und der Data Governance Act*, cit., p. 268. Sulla coincidenza di interessi tra cooperativa e membri della stessa, v. altresì CESE, *Parere del Comitato economico e sociale europeo su «Proposta di regolamento del Parlamento europeo e del Consiglio relativa alla governance europea dei dati (Atto sulla governance dei dati)»*, COM(2020) 767 final, 27 aprile 2021, pt. 4.15. Resta fermo che i membri della cooperativa di dati potrebbero svolgere attività in conflitto con quelle dell'organizzazione: come detto, il DGA non prevede disposizioni sulla prevenzione e gestione di conflitti di interesse tra intermediari, cooperative di dati incluse, e interessati o utenti dei dati (cfr. F. BRAVO, *Le cooperative di dati*, cit., p. 780).

[115] Sulla società cooperativa come forma soggettiva fisiologica delle cooperative di dati v. ID., *Le cooperative di dati*, cit., p. 797. Al riguardo, è stato anche evidenziato che la messa in comune dei dati con forme soggettive che non riflettano la dimensione sociale e relazionale della "aggregazione" dei dati, in considerazione del valore collettivo degli stessi, non consentirebbe alle cooperative di dati di fungere da mezzo di riequilibrio del potere e contrasto alle logiche del capitalismo informazionale (cfr. E. BIETTI-A. ETXEBERRIA-M. MANNAN-J. WONG, *Data Cooperatives in Europe: A Legal and Empirical Investigation*, cit., p. 9).

[116] Sulla circostanza che le società cooperative siano connotate dall'autogestione, al posto della gestione capitalistica, v. ad es. F. GALGANO-R. GHENGHINI, *Il nuovo diritto societario*, cit., p. 925.

[117] Il principio «una testa un voto» è tuttavia derogabile per i soci persone giuridiche (art. 2538, co. 3, c.c.).

[118] Sulla circostanza che le caratteristiche dell'impresa cooperativa siano particolarmente coerenti con le esigenze di mantenimento del controllo sui dati dei soci, v. anche L. PETRONE, *Il mercato digitale europeo e le cooperative di dati*, cit., p. 811.

tato, in quanto detto intermediario è tenuto alla realizzazione degli interessi dei propri membri e, perciò, non potrà impiegare gli strumenti di analisi o le informazioni generate tramite gli stessi con modalità tali da indebolire il controllo sui loro dati. Di più, le richiamate logiche democratiche, di confronto tra i membri, e le altre caratteristiche della forma sociale della cooperativa si prestano ad applicazioni idonee ad escludere l'opacità nei successivi utilizzi dei dati da parte della cooperativa [119]; ciò, unitamente al citato modello della *governance* duale collettiva-individuale [120] discendente dalla necessità di garantire la conformità alla normativa sulla protezione dei dati personali, nel caso in cui sia previsto il trattamento di tali dati [121].

Proseguendo oltre, risulta più complessa la coerente riconduzione della prestazione dei servizi in esame a opera delle cooperative di dati alle funzioni del principio di neutralità quale mezzo di regolazione del mercato, a tutela della concorrenza.

L'offerta di servizi di analisi dei dati da parte di queste organizzazioni recherebbe con sé il rischio di possibili impatti anti-concorrenziali: in breve, potrebbero aversi effetti di *lock-in* verso i membri delle cooperative di dati, con possibili impatti negativi anche nei confronti degli altri operatori del mercato; più ampiamente, il rischio è quello della progressiva concentrazione di dati in capo alle cooperative di dati, con gli effetti *antitrust* che potrebbero conseguirne [122].

Si ha, apparentemente, un contrasto tra le due funzioni del principio di neutralità: per garantire agli interessati e ai piccoli operatori economici un effettivo con-

---

[119] Si considerino in merito anche gli altri specifici tratti della disciplina delle società cooperative, specialmente per quanto concerne l'organizzazione interna, tra i quali, in aggiunta al principio del voto capitario (art. 2538, co. 2 e 3, c.c.), si richiamano l'ammissione soltanto limitata del voto per rappresentanza (art. 2539 c.c.), che è posta a salvaguardia sia del principio del voto per teste stesso sia degli interessi mutualistici innanzi ai contrapposti interessi capitalistici, evitando che estranei possano esercitare ingerenze nella gestione della cooperativa (cfr. F. GALGANO-R. GHENGHINI, *Il nuovo diritto societario*, cit., p. 969) e, ancora, la circostanza che almeno la maggioranza degli amministratori sia costituita da soci della cooperativa (art. 2542, co. 2, c.c.), avente la medesima *ratio* dei limiti della procura in assemblea verso soggetti estranei, affinché la maggior parte degli amministratori sia portatrice degli stessi interessi di "categoria" di cui la società è espressione (*Ibidem*).

[120] Sulla *governance* duale, v. *supra*, par. 3.1.

[121] Gli stessi rilievi possono svolgersi rispetto alla neutralità come limitazione dei servizi, per quanto concerne i rischi di perdita del controllo dei dati che potrebbero aversi relativamente all'uso incrociato dei dati conferiti dai membri nel contesto dei servizi di analisi. Va detto che la prestazione di servizi di analisi potrebbe risultare d'incentivo, per la cooperativa di dati, nell'utilizzare i dati oggetto degli scambi per propri scopi di miglioramento di tali servizi (ad es., per addestrare gli algoritmi su cui si basano detti servizi), scenari nei quali potrebbe aversi un impiego dei dati in contrasto con l'art. 12, lett. *a*) ed *e*), Reg. cit. Questa è tuttavia un'eventualità fisiologica, comune a tutti i servizi supplementari previsti dal regolamento europeo: l'interesse a evitare scenari di questo tipo, dunque, è ritenuto dallo stesso DGA come recessivo rispetto alle esigenze di erogare simili servizi, una volta collocati entro i limiti dell'art. 12, lett. *e*), Reg. cit.

[122] Su tali profili, si rinvia a quanto detto *supra*, par. 2.2.2, e relativi riferimenti bibliografici. Sui rischi *antitrust* posti dalla concentrazione dei dati in quanto tale (ossia, anche in mancanza di una concentrazione tra imprese), cfr. F. BRAVO, *Il commercio elettronico di dati personali*, cit., p. 125 ss.

trollo sui propri dati è necessario consentire alle *data cooperatives* di affacciarsi sul valore informativo dei dati, prestando servizi *data-driven* di analisi dei dati in favore dei membri; al contempo, così facendo si determinano effetti potenzialmente distorsivi del regime concorrenziale ideale ricercato dal legislatore europeo per il mercato dell'infomediazione *tout court*.

In questa sede, non è possibile approfondire debitamente questi scenari. Ciò che preme, è svolgere delle considerazioni di carattere generale, prendendo le mosse, ancora una volta, dalla peculiarità del tipo di servizio di intermediazione dei dati rappresentato dalle *data cooperatives*.

L'azione dell'Unione realizzata mediante il DGA prevede la promozione dei servizi di cooperative di dati, i quali, oltre ad atteggiarsi come misura di contrasto, sono portatori di un mutamento di paradigma volto a realizzare, in opposizione alle logiche del capitalismo estrattivo, quella «parità di condizioni nell'economia dei dati» [123] tali da abilitare la concorrenza «sulla qualità dei servizi e non sulla quantità dei dati» [124], nonché in ultimo «una società e un'economia dei dati antropocentriche, affidabili e sicure» [125] in linea con i valori e il diritto UE. Gli scambi di dati realizzati secondo lo schema delle *data cooperatives* comporterebbero non solo il soddisfacimento degli interessi dei membri cooperatori, ma anche una redistribuzione del valore dei dati e pertanto una rimodulazione delle relazioni di potere presenti nel mercato interno in senso coerente all'assiologia e all'ordinamento UE [126].

---

[123] Cfr. *considerando* n. 2 Reg. cit.

[124] *Ibidem*.

[125] Cfr. *considerando* n. 3 Reg. cit.

[126] Sotto questo profilo, dal punto di vista del diritto delle società cooperative la disciplina del DGA relativa alle cooperative di dati potrebbe ritenersi esemplificativa della c.d. mutualità *esterna* (contrapposta a quella contrattuale "in senso stretto"), secondo la quale le cooperative hanno lo scopo di soddisfare non solo i bisogni dei propri soci, ma anche quelli della categoria sociale cui questi ultimi appartengono, che nell'ottica del DGA risulta predeterminata, almeno nel *genus*, in quella degli interessati, delle imprese individuali e delle PMI, quali soggetti posti ai margini della *data economy*. D'altra parte, considerando le *data transactions* gestite dall'intermediario nell'interesse dei membri come gli scambi che sostanziano la mutualità consentendo ai soci di ottenere il "vantaggio cooperativo", la necessità per le cooperative di dati di operare anzitutto nella direzione degli obiettivi principali prestabiliti dal DGA, inerenti al *data sharing* verso l'esterno della cooperativa, limita le modalità tramite le quali tali società possono realizzare la propria finalità mutualistica, in modo da tendere verso il soddisfacimento degli interessi afferenti alla categoria sociale di appartenenza dei soci nel complesso, in funzione del raggiungimento degli obiettivi del DGA quale strumento di regolazione del mercato nei termini sopra descritti. Sulla mutualità esterna v. ad es. A. BASSI, *Principi generali della riforma delle società cooperative*, cit., p. 70 (il quale evidenzia la specificità della mutualità "esterna" rispetto a quella di "sistema"). Sui rapporti tra cooperative e sottostante categoria produttiva o ceto sociale, nel senso invece di valorizzare il "momento contrattuale del fenomeno" e, così, di intendere la categoria produttiva di cui la cooperativa è espressione come un *posterius* e non invece un *prius*, escludendo dunque che le società cooperative, di per sé, debbano perseguire anche l'interesse di soggetti non soci solo perché appartenenti alla medesima categoria, v. quanto indicato in F. GALGANO-R. GHENGHINI, *Il nuovo diritto societario*, cit., p. 957 ss., in particolare richiamando G. OPPO, *L'essenza della società cooperativa*, in *Riv. dir. civ.*, 1959, I, p. 370.

Valorizzare quest'ottica, in coerenza con gli obiettivi del DGA e della strategia europea per i dati, del quale tale misura legislativa è "attuazione", potrebbe allora consentire di inquadrare in modo differente le possibili criticità ravvisabili sul piano degli obiettivi *antitrust* del regolamento. Fornire alle *data cooperatives* un più incisivo margine di operatività sui dati conferiti dai membri è indispensabile per abilitarne l'effettiva capacità di raggiungere i propri obiettivi, essi stessi collegati al superamento degli ostacoli oggi frapposti al buon funzionamento della *data economy* e, in tal senso, i possibili impatti negativi in termini *antitrust* potrebbero ritenersi compensati dai contestuali effetti pro-concorrenziali che ne discenderebbero [127].

4. Alcune riflessioni conclusive.

La scelta del legislatore europeo di attrare le cooperative di dati tra i servizi di intermediazione dei dati e di prevedere una disciplina priva di differenziazioni per il complesso di tali servizi mostra evidenti limiti.

Il rigido regime stabilito per i servizi di intermediazione dei dati potrebbe limitare il potenziale innovativo degli stessi e, nel contesto di un settore ancora nella sua fase germinale, impedire l'emersione di nuovi modelli, costringendo inoltre i fornitori già operanti nel mercato a rimodulare la propria struttura e attività in un senso peggiorativo rispetto alle loro potenzialità per l'economia e la società [128].

A monte, si è detto, vi è la limitatezza della considerazione delle cooperative di dati come meri fornitori di "servizi di intermediazione dei dati", impediti nell'offrire attività di natura differente, alla quale, allo stato attuale, sembra costringere l'applicazione del principio di neutralità ai «servizi di cooperative di dati» quali, appunto, *species* dei servizi di *data intermediation*.

L'applicazione della neutralità alle cooperative di dati ne riduce drasticamente l'operatività sui dati "conferiti" dai membri e dunque la capacità di supportare que-

---

[127] D'altra parte, negli scenari poc'anzi accennati, alla luce della struttura e della funzione delle cooperative di dati, si avrebbero conseguenze ben differenti da quelle che caratterizzerebbero i medesimi fenomeni nel contesto di imprese mosse da logiche puramente lucrative. Le concentrazioni, ad esempio, potrebbero invero supportare un riequilibrio del mercato, fornendo i mezzi per contrastare gli oligopoli già esistenti, e agevolerebbero la trasformazione di quest'ultimo in modo coerente all'ordinamento e ai valori UE, ponendo al centro la persona e le esigenze degli operatori economici più deboli, diversamente da quanto avviene nell'attuale «*provider centric system*» (v. *supra*, par. 2.2.1.).

[128] Cfr. L. VON DITFURTH, *Datenmärkte, Datenintermediäre und der Data Governance Act*, cit., p. 268 ss. V. altresì *Ibidem*, p. 583 ss., ove è evidenziato come tale disciplina, con specifico riguardo alle obbligazioni di neutralità, presenterebbe il rischio di restringere senza obiettiva giustificazione l'operatività di certi tipi di intermediari e specialmente delle cooperative di dati. In merito, v. altresì ID.-G. LIENEMANN, *The Data Governance Act: – Promoting or Restricting Data Intermediaries?*, cit., p. 290; H. RICHTER, *Looking at the Data Governance Act and Beyond: How to Better Integrate Data Intermediaries in the Market Order for Data Sharing*, cit., p. 465 ss.

sti ultimi nella *data valorisation*. La disciplina disegnata dal DGA non coglie appieno le opportunità del neo-mutualismo digitale e, nonostante le premesse, non appare credibile nell'obiettivo di contribuire a un mutamento di paradigma nella *data economy* mediante l'operato delle cooperative di dati.

L'esame delle disposizioni del DGA da cui emerge il principio di neutralità, in rapporto ai caratteri e alle finalità dei servizi di cooperative di dati emergenti dal modello stabilito nello stesso regolamento, svolto nell'ottica dell'interpretazione teleologica del diritto eurounitario in considerazione degli obiettivi di tale regolamento e della più ampia strategia UE per i dati, ha tuttavia mostrato alcune possibili aperture. Entro certi limiti, in particolare, potrebbe ritenersi coerente con tale disegno ammettere le cooperative di dati a fornire servizi di intermediazione dei dati anche al loro interno, mediante *data pools* sui quali, tra l'altro, innestare strumenti di analisi dei dati che consentirebbero a detti intermediari di prestare servizi *data-driven* in favore dei propri membri, laddove questi ultimi siano strettamente funzionali al miglioramento di tale servizio o alla facilitazione degli scambi nella logica di supporto ai membri che connota per definizione tali organizzazioni [129].

Al riguardo, è necessario sottolineare altresì l'importanza di una lettura della disciplina delle *data cooperatives* che vada oltre la dimensione individualistica del diritto alla protezione dei dati personali, la quale, seppur insopprimibile, alla luce della "funzione sociale" di tale diritto risulta soltanto parziale. È dunque indispensabile procedere verso una dilatazione collettiva della tutela della persona con riguardo ai propri dati personali [130], per affrontare le sfide della contemporaneità in termini sia di valorizzazione dei dati sia di mitigazione dei rischi derivanti dal trattamento di tali dati, che oggi si atteggiano anche come possibili impatti negativi a livello di categorie o formazioni sociali [131].

---

[129] Resta fermo che i servizi descritti, in conformità alla neutralità come separazione soggettiva (art. 12, lett. *a*), ult. per., Reg. cit.), dovranno essere offerti da soggetti giuridici appositamente deputati alla prestazione dei «servizi di cooperative di dati», fatta salva la possibilità di un'interpretazione più flessibile di tale limite alle cooperative di dati, in virtù della natura mutualistica e della necessità di valorizzare la funzione svolta dalle stesse a beneficio dei propri membri (in tal senso, v. F. BRAVO, *Le cooperative di dati*, cit., p. 775), che non è possibile approfondire in questa sede.

[130] Esigenza, com'è noto, evidenziata da lungo tempo, rispetto alla quale il rinvio obbligato è a S. RODOTÀ, *Tecnologie e diritti*, cit., p. 23 ss. Nello specifico contesto delle cooperative di dati, v. G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit., p. 983 ss.; F. BRAVO, *Le cooperative di dati*, cit., p. 784 ss. Più ampiamente, sulla tutela collettiva delle persone con riguardo al trattamento dei dati personali, v. A. MANTELERO, *Personal Data for Decisional Purposes in the Age of Analytics: from an Individual to a Collective Dimension of Data Protection*, in *Computer Law & Sec. Rev.*, 2016, 32, pp. 238-255; ID., *From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era*, in L. TAYLOR-L. FLORIDI-B. VAN DER SLOOT (eds.), *Group Privacy: New Challenges of Data Technologies*, Cham, 2017, pp. 139-158.

[131] Ciò, nel senso che gli effetti del trattamento di dati personali di persone afferenti a un certo "gruppo" si riverbera anche sugli altri appartenenti a quest'ultimo, a prescindere dalla qualificazione di essi come "*data subjects*". Basti pensare ai rischi della discriminazione algoritmica nel contesto dell'impiego di tecnologie di *AI*, ove i *bias* generati dal trattamento di dati personali svolto durante la

Più in generale, in quest'ottica, le cooperative di dati, coerentemente alla finalità mutualistica e alla funzione sociale che caratterizza il modello delle società cooperative, non possono essere intese come strutture ove la natura collettiva rilevi in termini meramente rafforzativi della capacità dei singoli di realizzare i propri interessi. Occorre invece valorizzare le potenzialità delle *data cooperatives* per il soddisfacimento dei bisogni delle categorie sociali cui afferiscono i loro membri, sottesi al patto associativo alla base della loro costituzione, con effetti positivi per l'intera comunità nella quale operano [132]. Anche a fronte del descritto rilievo relazionale del diritto alla protezione dei dati personali, allora, i membri della cooperativa di dati devono essere sempre considerati come "persone" e non quali meri "individui", dunque come soggetti relazionali, che possono pienamente sviluppare la propria personalità soltanto entro le formazioni sociali in cui operano concretamente, attraversate dai doveri di solidarietà che integrano il "sociale" e il "collettivo" nella dimensione del singolo [133] e che si rinvengono a più livelli nelle trame della Costituzione e del diritto UE [134].

---

fase di addestramento dell'algoritmo potrebbero manifestare i propri effetti lesivi nella fase di impiego della tecnologia, verso persone diverse dagli interessati coinvolti nel *training.* Rispetto a questi scenari, v. ad es. A MANTELERO, *La* privacy *all'epoca dei* Big Data, in V. CUFFARO-R. D'ORAZIO-V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, spec. p. 1196 ss., con riguardo ai limiti dell'approccio individuale innanzi al fenomeno dei *Big Data*.

[132] D'altra parte, la differenza tra servizi di intermediazione dei dati per consentire ai *data subjects* di esercitare i propri diritti (art. 10, lett. *b*), Reg. cit.) e servizi di cooperative di dati si ravvisa essenzialmente nella circostanza che, in quest'ultimo contesto, gli interessati si riuniscono per fare valere i propri diritti in un'ottica collettiva (cfr. L. VON DITFURTH, *Datenmärkte, Datenintermediäre und der Data Governance Act*, cit., p. 267).

[133] Sulla distinzione tra "persona" e "individuo" e il mutamento di passo introdotto in tal senso dalla Costituzione italiana, così andando oltre il rifiuto "moderno" (o meglio, illuministico) della dimensione collettiva, v. P. GROSSI, *Il mondo delle terre collettive*, Macerata, 2019, spec. p. 24 ss.

[134] Sulla solidarietà come principio costituzionale, seppur dotato di autonoma rilevanza, strettamente connesso agli altri principi di «un ordine giuridico inteso nella sua accezione più ampia, dunque anche oltre il perimetro dello Stato nazionale», v. S. RODOTÀ, *Solidarietà. Un'utopia necessaria*, Roma-Bari, 2014, spec. pp. 39 ss. e 48 ss. Sull'operatività della solidarietà specificamente rispetto al diritto alla protezione dei dati personali, seppur con diverse accezioni, v. D. MESSINETTI, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *Riv. crit. dir. priv.*, 1998, p. 385 ss.; E. NAVARRETTA, *Commento sub art. 11*, in C.M. BIANCA-F.D. BUSNELLI (a cura di), *La protezione dei dati personali. Commentario al D. Lgs. 30 giugno 2003, n. 196 («Codice della* privacy*»)*, Padova, 2007, I, p. 247 ss.; F. BRAVO, *Il consenso e le altre condizioni di liceità*, cit., p. 117 ss.; ID., *Il principio di solidarietà in materia di protezione dei dati personali nelle decisioni del Garante e della Corte di Cassazione*, in *Contratto e impresa*, 2023, 2, p. 405 ss. (ove è evidenziato il collegamento tra «funzione sociale» del diritto alla protezione dei dati personali e principio costituzionale di solidarietà); ID., *Il principio di solidarietà*, in ID. (a cura di), *Dati personali. Protezione, libera circolazione e* governance – Vol. I, Pisa, 2023, p. 541 ss.; ID., *Il principio di solidarietà tra* data protection *e* data governance, in *Il diritto dell'informazione e dell'informatica*, 2023, 3, p. 481 ss.; più ampiamente, sulla necessità di bilanciare il diritto alla *privacy* con i doveri di ognuno verso la comunità, v. M.G. LOSANO, *Dei diritti e dei doveri: anche nella tutela della* privacy, in ID. (a cura di), *La legge italiana sulla* privacy*. Un bilancio dei primi cinque anni*, Bari, 2001, pp. V-XX.

Sotto quest'ultimo profilo, le aperture interpretative che sono state proposte, invero, potrebbero utilmente essere sorrette dall'operatività del principio "normativo" di solidarietà [135], di particolare rilievo nel contesto delle cooperative di dati [136]. Detto principio, coerentemente alla funzione sociale della cooperazione e del diritto alla protezione dei dati personali, dovrebbe comportare un contemperamento degli altri rilevanti, tale da consentire la realizzazione delle istanze sottese al modello delle cooperative di dati oltre i limiti emergenti da una lettura formale ed isolata della rigida disciplina del DGA [137], grazie anche alla capacità della solidarietà di operare entro le relazioni commerciali per definirne la portata e i limiti, abilitando l'ingresso al loro interno di valori irriducibili alla mera convenienza economica [138].

Una lettura che offra alle cooperative di dati maggiori margini per esprimere il proprio potenziale, oltre che coerente con le finalità del DGA e gli obiettivi della strategia europea per i dati, risulta in linea altresì con le più ampie politiche UE in materia, a partire dai principi espressi nella Comunicazione «relativa alla definizione di una dichiarazione europea sui diritti e i principi digitali» [139] prima e nella «Dichiarazione europea sui diritti e i principi digitali per il decennio digitale» [140]

---

[135] Sulla solidarietà come principio normativo, v. G. ALPA, *Solidarietà. Un principio normativo*, Bologna, 2022; v. altresì ID, *I Principi generali*, cit., p. 736 ss.

[136] Il riferimento è a F. BRAVO, *Le cooperative di dati*, cit., p. 783 ss., ove è evidenziato che il modello delle cooperative di dati ben si presta ad interpretare il principio di solidarietà, considerato che «strutturalmente, prevede un'operatività di impresa nell'interesse dei propri soci e una struttura democratica volta a favorire la discussione, il confronto e l'adozione delle decisioni da parte dei soci»; v. altresì *ibidem*, p. 799.

[137] Con il principio di solidarietà, opererebbero nella medesima direzione anche altri principi dell'ordinamento: si pensi all'uguaglianza sostanziale e ai correlati doveri imposti alla Repubblica di rimozione degli ostacoli di ordine economico e sociale che oggi limitano la partecipazione, segnatamente, di interessati, imprese individuali e PMI alla *data economy* (art. 3, co. 2, Cost.), unitamente a quelli di promozione dell'incremento della cooperazione (art. 45 Cost.). Sulla necessaria operatività della solidarietà in connessione al principio di uguaglianza e agli altri principi costituzionali, v. S. RODOTÀ, *Solidarietà. Un'utopia necessaria*, cit., p. 39 ss.

[138] *Ibidem*, p. 70. Ciò, tanto più nello scenario critico presupposto dagli obiettivi di concorrenza del DGA, posto che l'esigenza di operare una redistribuzione del valore dei dati mira altresì a rendere effettivi i diritti fondamentali – su tutti, quello alla protezione dei dati personali – oggi compressi a causa delle attuali logiche che attraversano il mercato digitale, diritti che non possono essere considerati pari-ordinati a quelli espressione di esigenze puramente economiche (su tale ultimo profilo, con specifico riferimento al diritto alla protezione dei dati personali, v. ad es. F. BRAVO, *Sul bilanciamento proporzionale dei diritti e delle libertà "fondamentali", tra mercato e persona: nuovi assetti nell'ordinamento europeo?*, cit., p. 190 ss.; F. MOLLO, *Il trattamento dei dati genetici tra libera circolazione e tutela della persona*, in *Jus Civile*, 2022, 1, p. 94 ss.).

[139] COMMISSIONE EUROPEA, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni relativa alla definizione di una dichiarazione europea sui diritti e i principi digitali*, Bruxelles, 26 gennaio 2022, COM(2022) 27 final.

[140] PARLAMENTO EUROPEO-CONSIGLIO-COMMISSIONE EUROPEA, *Dichiarazione europea sui diritti e i principi digitali per il decennio digitale*, in G.U.U.E., 23 gennaio 2023, C 23/01. Su tali documenti,

poi, i quali presentano anche diversi punti di contatto con quelli che connotano il modello cooperativo [141]. Occorre dunque collocare i valori sottesi alla neutralità degli intermediari dei dati su uno sfondo più ampio, comprensivo degli altri emergenti da tali fonti, in base ai quali è necessario porre al centro della trasformazione digitale le persone, rafforzare la democraticità della società e dell'economia digitali, sostenere la solidarietà e l'inclusione in un ambiente digitale equo, pur promuovendo al contempo l'innovazione tecnologica [142].

La *European way of a data governance*, inserita nella più ampia *European way for the digital transformation* [143], può allora consentire l'identificazione di un modello di cooperative di dati che sia tale da contribuire effettivamente a «una società e a un'economia eque e inclusive nell'UE» [144].

A ogni modo, l'occasione persa di porre una regolamentazione concretamente idonea a promuovere i modelli alternativi di circolazione e valorizzazione dei dati riportabili alle cooperative di dati è recuperabile soltanto limitatamente in via interpretativa. L'effetto promozionale di una siffatta disciplina, lasciato all'interpretazione degli operatori e delle autorità competenti, non potrà che essere ridotto, rispetto a un settore che, invece, ha estremamente bisogno di un quadro regolatorio chiaro e, in ogni caso, di misure agevolanti ulteriori rispetto a quelle finora approvate [145].

---

v. F. BRAVO, *I principi in materia di protezione dei dati personali. Dalla "riscrittura" delle tavole dei valori alla "rilettura" nel diritto vivente, nel solco delle* rules of construction, in ID. (a cura di), *Dati personali. Protezione, libera circolazione e* governance, cit., p. 15 ss., ove l'A. sottolinea la valenza giuridica dei diritti e principi digitali espressi al loro interno, nonostante il tentativo di limitarne la portata in termini meramente programmatici e politici (cfr. COMMISSIONE EUROPEA, *Comunicazione relativa alla definizione di una dichiarazione europea sui diritti e i principi digitali*, cit., p. 5; PARLAMENTO EUROPEO-CONSIGLIO-COMMISSIONE EUROPEA, *Dichiarazione europea sui diritti e i principi digitali per il decennio digitale*, cit., *Preambolo*, par. 10).

[141] Nell'ottica di plasmare la trasformazione digitale secondo i valori e le norme europee (COMMISSIONE EUROPEA, *Comunicazione relativa alla definizione di una dichiarazione europea sui diritti e i principi digitali*, cit., p. 1), infatti, sono stati approvati dei principi digitali, basati sui comuni valori europei, che fungano da guida «per un ambiente digitale antropocentrico, sicuro, inclusivo e aperto, che non escluda nessuno» (*Ibidem*), che siano «al servizio di tutti gli europei» (*Ibidem*, p. 4), con l'obiettivo di promuovere «un modello europeo per la trasformazione digitale, che metta al centro le persone, sia basato sui valori europei e sui diritti fondamentali dell'UE, riaffermi i diritti umani universali e apporti benefici a tutte le persone, alle imprese e alla società nel suo complesso» (PARLAMENTO EUROPEO-CONSIGLIO-COMMISSIONE EUROPEA, *Dichiarazione europea sui diritti e i principi digitali per il decennio digitale*, cit.).

[142] *Ibidem*, *Preambolo*.

[143] *Ibidem*.

[144] *Ibidem*, Capitolo II «*Solidarietà e inclusione*», ove si evidenzia anche l'impegno di «sviluppare quadri adeguati affinché tutti gli operatori del mercato che traggono vantaggio dalla trasformazione digitale si assumano le proprie responsabilità sociali e contribuiscano in modo equo e proporzionato ai costi delle infrastrutture, dei servizi e dei beni pubblici, a beneficio di tutte le persone che vivono nell'UE».

[145] Ciò, a fronte delle problematiche che il fenomeno delle cooperative di dati presenta in termini di sostenibilità economica, comuni, ma più incisive, a quelle che interessano la generalità dei servizi

Per soddisfare le citate esigenze di certezza del diritto e stimolare le formazioni sociali a organizzarsi entro i modelli cooperativi del neo-mutualismo digitale, l'auspicio, in tal senso, è in un intervento legislativo ulteriore, che rimedi alla collocazione delle cooperative di dati entro gli stringenti limiti della categoria dei "servizi di intermediazione dei dati" o che, almeno, possa levigare le criticità emergenti dall'approccio "*one-size-fits-all*" che informa la disciplina stabilita per detti servizi. Una simile iniziativa, se del caso, potrà emergere dal processo di valutazione e riesame del *Data Governance Act* previsto entro il settembre 2025, all'esito del quale è infatti contemplata la possibilità per la Commissione europea di corredare di proposte legislative la relazione da presentare al Parlamento europeo, al Consiglio e al Comitato economico e sociale [146].

di intermediazione dei dati. Dette criticità sono particolarmente rilevanti rispetto ai temi esaminati, posto che tipicamente è grazie alla fornitura dei servizi a valore aggiunto che gli intermediari possono competere sul mercato ed essere sostenibili. In merito, v. ad es. AA.VV., *Mapping the Landscape of Data Intermediaries – Emerging Models for More Inclusive Data Governance*, cit., p. 34 ss.; G. CAROVANO-M. FINCK, *Regulating Data Intermediaries: The impact of the Data Governance Act on the EU's Data Economy*, cit., p. 11 ss.; M. MICHELI-M. PONTI-M. CRAGLIA-A. BERTI, *Emerging Models of Data Governance in the Age of Datafication*, cit., p. 9 ss.

[146] Cfr. art. 35 Reg. cit. Detta opportunità è stata evidenziata anche in L. VON DITFURTH-G. LIENEMANN, *The Data Governance Act: – Promoting or Restricting Data Intermediaries?*, cit., p. 292, in riferimento alle più ampie questioni problematiche poste dalla complessiva disciplina dei fornitori di servizi di intermediazione dei dati stabilita dal DGA. L'opportunità di rimediare alle manchevolezze di tale regolamento per quanto concerne la disciplina delle cooperative di dati con un nuovo intervento normativo, in alternativa a possibili soluzioni interpretative, è evidenziata altresì in F. BRAVO, *Le cooperative di dati*, cit., p. 775, rispetto alla possibilità per la cooperativa di dati di utilizzare i dati dei soci, «nello spirito mutualistico che la contraddistingue e la contrappone al modello più tipicamente capitalistico».

Capitolo XXXVII

La (im)possibile subordinazione della fornitura di servizi di intermediazione dei dati ad ulteriori servizi

Carlo Basunti

Abstract: The paper, within the category of the conditions for the provision of data intermediation services that have recently been introduced by the Data Governance Act (EU Reg. 868/2022), analyses the condition under art. 12, lett. b) DGA. This condition, relating to the (im)possibility of subordinating the provision of a data intermediation service to the provision of further services, is, at first, compared with the tying arrangements and, subsequently, analyzed in its critical aspects.

1. Cenni introduttivi.

La strada intrapresa dal legislatore europeo nel disciplinare il mercato digitale appare chiara. Dapprima con il Regolamento (UE) 2016/679 (GDPR) e oggi con il Regolamento (UE) 2022/868 (DGA), emerge come i dati rappresentino *assets* di importanza strategica nello scenario economico che, appunto, appare sempre più *data based*. Il vigente apparato normativo, pur nell'ambito di un bilanciamento tra contrapposti diritti ed interessi, tutti meritevoli di tutela, proietta sempre più i dati (personali) entro logiche di scambio, incentivandone la circolazione e massimizzandone la valorizzazione.

Precisamente, la Strategia europea per i dati [1], in cui il *Data Governance Act* si inserisce, favorendo un sapiente utilizzo dei dati personali e non personali, intende

[1] COMMISSIONE EUROPEA, Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Una Strategia europea per i dati*, Bruxelles, 19 febbraio 2020 [COM (2020) 66 *final*].

delineare un paradigma di sviluppo in cui la persona, con i suoi diritti fondamentali (tra cui, soprattutto, il diritto alla protezione dei dati personali), mantiene la centralità che, a ragione, deve caratterizzarla, ma in cui è manifesta la convinzione che, attraverso i dati, tanto i soggetti privati quanto quelli pubblici possano disporre di strumenti per adottare decisioni migliori e conoscere così nuove linee di crescita.

È proprio il DGA che mira a ridisegnare gli equilibri tra gli agenti del mercato digitale, in un'opera, che si potrebbe definire di "*digital market reshaping*". Sotto questo aspetto, il Regolamento è funzionale ad arginare lo strapotere delle *Big Tech* il cui sostanziale oligopolio ha innegabilmente contribuito a causare il c.d. *data divide*, e a favorire la posizione di vari soggetti (deboli), quali individui singolarmente intesi, *start-up*, PMI e *communities*. Questa prospettiva merita sicuro apprezzamento in quanto una simile concentrazione di potere nelle mani di pochi non solo mina il corretto funzionamento del mercato nel suo insieme, ma pone altresì in pericolo, tra gli altri, il diritto alla *privacy*, nella sua più attuale accezione di diritto all'autodeterminazione informativa, come pure l'autonomia contrattuale dei singoli.

Il DGA si snoda lungo tre direttrici principali: i) il riuso dei dati personali e non personali, che sono nella disponibilità della pubblica amministrazione la quale ha la facoltà di coinvolgere soggetti terzi nelle attività di trattamento dei dati per finalità, commerciali o non commerciali, ulteriori rispetto a quelle che hanno giustificato il primo trattamento; ii) l'altruismo dei dati, ossia la condivisione volontaria di dati, personali o non personali, che prescinde dalla richiesta o ricezione di un compenso che vada oltre il recupero dei costi di messa a disposizione del dato, per il perseguimento di obiettivi di interesse generale; iii) i servizi di intermediazione dei dati [2],

[2] I servizi di intermediazione dei dati, elencati all'art. 10 DGA, sono: «*a*) servizi di intermediazione tra i titolari dei dati e i potenziali utenti dei dati, compresa la messa a disposizione di mezzi tecnici o di altro tipo per consentire tali servizi (…); *b*) servizi di intermediazione tra interessati che intendono mettere a disposizione i propri dati personali o persone fisiche che intendono mettere a disposizione dati non personali e potenziali utenti dei dati, compresa la messa a disposizione di mezzi tecnici o di altro tipo per consentire tali servizi, permettendo in particolare l'esercizio dei diritti degli interessati di cui al regolamento (UE) 2016/679; *c*) servizi di cooperative di dati»; il *Considerando* n. 27 DGA afferma che: «si prevede che i servizi di intermediazione dei dati svolgano un ruolo essenziale nell'economia dei dati, in particolare nel sostenere e promuovere pratiche volontarie di condivisione dei dati tra imprese o nell'agevolare la condivisione dei dati nell'ambito degli obblighi stabiliti dal diritto dell'Unione o nazionale. Essi potrebbero diventare strumenti che agevolano lo scambio di quantità considerevoli di dati pertinenti. I fornitori di servizi di intermediazione dei dati, che possono includere anche enti pubblici, che offrono servizi che collegano i diversi soggetti dispongono del potenziale per contribuire alla messa in comune efficiente dei dati come pure all'agevolazione della condivisione bilaterale dei dati». Su tali servizi, cfr. F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al* Data Governance Act, in *Contr. e impr. Europa*, 2021, 1, p. 199 ss.; ID., *Data Governance Act and Re-Use of Data in the Public Sector*, in ID.-J. VALERO TORRIJOS (eds.), *Data Governance, Open Data and Data Protection in the Public Sector (Monographic Section)*, in *Eur. Rev. of Digital Administration & Law (ERDAL)*, 2022, 2, p. 15 parla di «*key role of data intermediaries*»; D. POLETTI, *Gli intermediari dei dati*, in *European J. of Privacy Law & Tech*., 2022, 1, p. 46 ss.; anche in ID., *Gli intermediari dei dati*, in A. MORACE PINELLI (a cura di), *La circolazione dei dati personali. Persona, contratto e mercato*, Pisa, 2023, p. 105 ss.

personali e non personali, offerti dai c.d. fornitori di servizi di intermediazione dei dati che mediano tra gli utenti e le imprese, le quali svolgono operazioni sui dati.

In questo contesto, preme sottolineare che un ruolo di rilievo è assunto dalle cooperative di dati [3] che – disciplinate a partire dal DGA che le inserisce tra i servizi di intermediazione dei dati e che, in realtà, fa riferimento ai servizi di cooperative di dati e non alle cooperative di dati in sé – si presentano quale nuovo paradigma per un utilizzo sostenibile dei dati (personali e non personali), secondo le logiche del neomutualismo [4] nella sua moderna declinazione di neomutualismo digitale [5].

Nell'ambito dei servizi di intermediazione dei dati, il DGA interviene prevedendo, *ex* art. 12, un elenco articolato di condizioni per la loro fornitura. Tali condizioni muovono da molteplici prospettive, tenendo conto, tra gli altri, dei profili legati alla tipologia dei singoli servizi offerti, alle condizioni commerciali di fornitura, alla raccolta dei dati oggetto dei servizi, al loro formato, all'interoperabilità con altri servizi connessi, all'ipotesi di insolvenza del fornitore, e così via.

In questo elenco, non ordinato sistematicamente dal legislatore, emerge quanto disposto *sub* lett. b) su cui intende concentrarsi il presente lavoro e ai sensi della quale: «le condizioni commerciali, compresa la fissazione del prezzo, per la fornitura di servizi di intermediazione dei dati a un titolare dei dati o a un utente dei dati non sono subordinate al fatto che il titolare dei dati o l'utente dei dati utilizzi altri servizi forniti dallo stesso fornitore di servizi di intermediazione dei dati o da un'entità collegata, e, in caso affermativo, in che misura il titolare dei dati o gli utenti dei dati utilizzano tali altri servizi».

2. Il necessario confronto tra l'art. 12, lett. *b*), DGA e le operazioni di *tying* nel GDPR e nella prassi giurisprudenziale.

L'art. 12, lett. *b*) DGA, nel fare riferimento alla «fornitura di servizi di intermediazione dei dati» «subordinat[a] al fatto che il titolare dei dati o l'utente dei dati utilizzi altri servizi forniti dallo stesso fornitore di servizi di intermediazione dei dati», sembra richiamare le c.d. operazioni di *tying*.

Tali operazioni, che non conoscono una specifica definizione legislativa, costituiscono uno strumento per "costringere" gli interessati ad acconsentire al trattamento dei propri dati, di modo da poter accedere a servizi, spesso prestati "gratui-

---

[3] Sul tema, v. F. BRAVO, *Le cooperative di dati*, in *Contr. e impr*., 2023, 4, p. 757 ss.

[4] Cfr. P. VENTURI-F. ZANDONAI, *Neomutualismo. Ridisegnare dal basso competitività e* welfare, Milano, 2022.

[5] F. BRAVO, *Le cooperative di dati*, cit., p. 764 ss. e *passim*, in particolare, a p. 766, l'Autore afferma: «mi pare che la cornice teorica del mutualismo digitale possa ben interpretare, sul piano economico, l'introduzione del modello giuridico delle cooperative di dati quale fattore di sviluppo per la *data governance*».

tamente"[6], ossia senza la previsione di un pagamento in denaro, dal momento che l'erogatore del servizio trae la propria utilità dal trattamento dei dati[7].

Simili operazioni, che, tra l'altro, vengono vietate dal TFUE ai sensi dell'art. 101, par. 1, lett. *e*) a tutela del mercato interno dell'Unione europea, poiché potrebbero «impedire, restringere o falsare il gioco della concorrenza», sono state viste con particolare sfavore dal Garante per la protezione dei dati personali, sin da un suo storico provvedimento[8].

---

[6] Sul tema, con impostazione critica, v. G. RESTA-V. ZENO ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim. dir. e proc. civ*., 2018, 2, p. 411 ss. Sul punto, si inserisce la Dir. (UE) 2019/770, relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e servizi digitali, che, all'art. 3, definisce l'ambito di applicazione della disciplina. La norma distingue i contratti in cui il consumatore corrisponde o si impegna a corrispondere un prezzo in cambio del contenuto o servizio digitale offerto dal professionista dal «caso» in cui il consumatore fornisce (o si impegna a fornire) dati personali. L'art. 3 della Dir. (UE) 2019/770 parrebbe così addirittura escludere una qualsivoglia relazione di corrispettività tra le due forniture – di servizi digitali, da un lato, e di informazioni personali, dall'altro – da parte dei due contraenti. Una conclusione, questa, forse, fin troppo drastica, anche alla luce del *considerando* n. 24 della medesima Direttiva ai sensi del quale «la fornitura di contenuti digitali o di servizi digitali spesso prevede che, quando non paga un prezzo, il consumatore fornisca dati personali all'operatore economico», secondo modelli commerciali «utilizzati in diverse forme in una parte considerevole del mercato». Il menzionato *considerando* n. 24 afferma altresì che «la presente direttiva dovrebbe [allora] garantire che i consumatori abbiano diritto a rimedi contrattuali [anche] nell'ambito di tali modelli commerciali». Si parla qui espressamente di «contratti in cui il consumatore fornisce o si impegna a fornire dati personali», diversamente dal «caso» menzionato nel suddetto art. 3. La formulazione della norma risponde alle preoccupazioni espresse dall'EDPS nella sua *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content*, che, invece, equiparava appieno le due fattispecie oggi distinte dall'art. 3. In particolare, l'EDPS ha sottolineato l'importanza di una *data-driven economy* per lo sviluppo dell'Unione, rilevando al contempo che sarebbe inaccettabile poter pagare il "prezzo" di un servizio, in modo ambivalente, con una somma di denaro o per mezzo del consenso dell'interessato al trattamento dei suoi dati personali. Nell'occasione, l'EDPS ha anche ribadito il divieto di utilizzare i dati personali a scopo di lucro, affermando che espressioni come "moneta digitale" o "pagamento per mezzo dei dati personali" non siano solamente fuorvianti, ma addirittura pericolose; in tema, per tutti, v. C. CAMARDI, *Prime osservazioni sulla direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione di dati personali*, in *Giust. civ*., 2019, 3, p. 499 ss.

[7] Cfr. S. THOBANI, *Operazioni di* tying *e libertà del consenso*, in *Giur. it*., 2019, 3, p. 538.

[8] Si fa riferimento alla celebre pronuncia GPDP, 28 maggio 1997, doc. *web* n. 40425, commentata da R. PARDOLESI, in *Foro it*., 1997, 3, c. 317; V. ZENO ZENCOVICH, *Il "consenso informato" e la "autodeterminazione informativa" nella prima decisione del Garante*, in *Corr. giur*., 1997, 8, p. 915 ss.; C. LO SURDO, *Commento ai provvedimenti adottati dall'autorità garante in merito al problema del consenso informato*, in *Danno e resp*., 1998, 7, p. 638 ss.; e M. CATALLOZZI, *I provvedimenti del Garante per la protezione dei dati personali*, in *Nuova giur. civ*., 1998, 2, p. 447 ss. In tale pronuncia sul caso BNL, il Garante distingue le finalità del trattamento a seconda che i dati siano riferiti ai rapporti (strettamente intesi) con i clienti, e servano per adempiere a obblighi imposti *ex lege* o, comunque, siano meramente funzionali rispetto all'attività posta in essere dalla banca. In merito alla libertà del consenso, il Garante afferma che «il consenso può essere ritenuto effettivamente libero solo se si pre-

Il GDPR, sul punto, ha adottato una soluzione di compromesso, tenendo conto anche della tensione emersa, nel corso dei lavori preparatori del Regolamento, tra le istituzioni UE e gli operatori di settore, dal momento che il Parlamento europeo aveva proposto di vietare *tout court* le operazioni di *tying*[9]. Il co. 4 dell'art. 7 del GDPR suggerisce, infatti, di tenere in «massima considerazione» il fatto che l'esecuzione di un contratto venga condizionata ad un consenso al trattamento dei dati personali, fornito per fini non collegati all'esecuzione del contratto stesso.

Detta norma fa riferimento all'*aut-aut* dinanzi al quale l'interessato, in questi casi, è posto: o accetta di prestare il proprio consenso o il titolare-fornitore non gli permetterà di accedere al servizio desiderato. Va sottolineato che il consenso che viene qui richiesto ha ad oggetto un trattamento di dati che non è necessario, in quanto non logicamente collegato, e quindi non è funzionale alla conclusione del contratto. Il Regolamento, dunque, non vieta i *tying arrangements* in sé, ma invita a prestare la massima attenzione al consenso, *rectius* alla sua libertà in queste circostanze. In altri termini, il GDPR non crea una diretta consequenzialità tra l'operazione di *tying* e l'invalidità del consenso al trattamento dei dati per mancanza del requisito di libertà dello stesso.

Diversamente, il Garante, nelle sue decisioni, si spinge ben oltre il (più) semplice tenere «in massima considerazione» la circostanza. È costante, infatti, l'orientamento[10] che vieta di subordinare l'accesso ad un servizio ad un consenso per il

---

senta come manifestazione del diritto all'autodeterminazione informativa, e dunque al riparo da qualsiasi pressione, e se non viene condizionato all'accettazione di clausole che determinano un significativo squilibrio dei diritti e degli obblighi derivanti dal contratto»; *amplius* v. P. MANES, *Il consenso al trattamento dei dati personali*, Padova, 2001, p. 136 ss., in particolare p. 139, nt. 43.

[9] V. EUROPEAN PARLIAMENT, *Committee on Civil Liberties, Justice and Home Affairs, Draft report* del 12 dicembre 2012, 2012/0011(COD), *amendment* n. 107. con cui veniva proposta l'aggiunta del par. 4 b) all'art. 7: «*the execution of a contract or the prevision of a service may not be made conditional on the consent to the processing or use of data that is not necessary for the execution of the contract or the provision of the service pursuant to Article 6(1)(b)*».

[10] Nell'ambito delle numerosissime pronunce dell'Autorità Garante, ci si limita a richiamare i seguenti provvedimenti: GPDP, 12 marzo 2003, doc. *web*. n. 29844, in cui si ammette che gli operatori telefonici possano «prescindere dal consenso dell'interessato solo in presenza della necessità di rispettare un obbligo normativo, evenienza che può ricorrere in caso di disastri e calamità naturali, nei quali l'invio dei messaggi in deroga alla disciplina sulla protezione dei dati può essere specificamente disposto da un soggetto pubblico, centrale o locale, all'atto dell'adozione»; GPDP, 3 febbraio 2005, doc. *web* n. 1109503, secondo cui «tutti i dati personali e le varie modalità del loro trattamento nelle singole fasi ed occasioni di utilizzazione devono essere pertinenti e non eccedenti rispetto alle finalità perseguite» e in cui si afferma come non sia ammissibile da parte del titolare del trattamento «adottare comportamenti suscettibili di incidere sulle scelte libere e consapevoli degli abbonati rispetto ad eventuali iniziative di profilazione che portino, anche attraverso codici numerici, a monitorare le scelte degli interessati e la loro sfera personale», e si aggiunge che gli scopi ulteriori di utilizzo dei dati dell'interessato debbano essere indicati con chiarezza e che «il conferimento dei dati e il consenso sono liberi e facoltativi rispetto all'ordinaria prestazione dei servizi, e non possono ottenersi sulla base di pressioni o condizionamenti»; GPDP, 22 luglio 2010, doc. *web* n. 1741988, nel quale si afferma che nel caso di specie non solo «non è lasciata all'interessato la possibilità di prestare un consenso specifico per ciascuna finalità perseguita dal

trattamento di dati personali per fini non necessari all'erogazione del servizio stesso. Ciò perché, a detta del Garante, in simili situazioni, manca un consenso libero.

Sull'argomento è intervenuta la Corte di Cassazione nel noto caso AdSpray [11]. La decisione dei giudici di legittimità era incentrata proprio sulla verifica delle condizioni di libertà e specificità del consenso, al fine di comprendere se potesse ritenersi valido il generico consenso al trattamento dei dati personali, prestato nell'ambito di una operazione di *tying* relativa all'accesso ad un servizio di *newslettering*.

Il Supremo Collegio ha richiamato il sopracitato art. 7, co. 4 del GDPR e ha affermato che la valutazione in merito alla libertà del consenso debba essere effettuata in base alla fungibilità sul mercato del servizio offerto. Infatti, secondo la Cassazione, subordinare il consenso per la fruizione del servizio all'ulteriore consenso prestato a fini promozionali diversi rispetto a quelli del servizio a monte, non integrerebbe di per sé un'ipotesi di coartazione, purché, però, quel servizio non rappresenti un *unicum* sul mercato, ma sia, appunto, fungibile. Ecco, quindi, che il gestore di un servizio fungibile e non irrinunciabile potrebbe rifiutarsi di offrire detto servizio a colui che non presti il proprio consenso al trattamento dei dati personali per fini differenti alla fruizione del servizio stesso, dal momento che l'interessato ben potrebbe rivolgersi ad un altro fornitore ed ottenere un servizio (almeno) analogo.

La previsione del DGA qui in commento pare condividere la *ratio* sottesa all'art. 7, par. 4 GDPR, laddove, in entrambe le disposizioni, il legislatore europeo mostra cautela nel subordinare l'accesso ad un servizio che ha ad oggetto dati, alla fruizione di un altro servizio avente lo stesso oggetto. La cautela del legislatore si spiega nell'intento di garantire una massima tutela all'interessato, nonché – riprendendo le ulteriori figure soggettive introdotte dal DGA – al titolare dei dati o all'utente dei dati.

---

titolare del trattamento ma, inoltre, l'unico consenso richiesto non può neanche definirsi liberamente prestato dall'utente, dal momento che la registrazione al sito *web* o la partecipazione ad un concorso sono subordinati all'autorizzazione dell'interessato di trattare i propri dati personali per finalità diverse, quali sono quelle promozionali, di profilazione e di cessione dei dati ad altre società per ulteriori scopi»; GPDP, 22 maggio 2018, doc. *web* n. 8995274, in cui il Garante vieta il trattamento per finalità diverse da quelle di esecuzione del servizio qualora non venga richiesto un consenso ulteriore e specifico. Più ampiamente, si rinvia alle ricostruzioni delle pronunce del Garante presenti in F. PIZZETTI (a cura di), *Sette anni di protezione dati in Italia. Un bilancio e uno sguardo sul futuro. 2005-2012*, Torino, 2012; e in S. THOBANI, *Diritti della personalità e contratto: dalle fattispecie più tradizionali al trattamento in massa dei dati personali*, Milano, 2018, in particolare, p. 95, nt. 107.

[11] Cass., 2 luglio 2018, n. 17278, in *Nuova giur. civ.*, 2018, 12, p. 1775 ss., con nota di F. ZANOVELLO, *Consenso libero e specifico alle e-mail professionali*; in *Giur. it*., 2019, 3, p. 530 ss., con nota di S. THOBANI, *Operazioni di* tying *e libertà del consenso*; in *Corr. giur*., 2018, 11, p. 1459 ss.; e in *Giust. civile.com*, 21 marzo 2019, con nota di F. RUGGERI, *Sulla nozione di consenso nella nuova disciplina* privacy*: alcune prime considerazioni*; vedi anche l'analisi condotta, a partire da questa pronuncia, da F. BRAVO, *Lo "scambio di dati personali" nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto*, in *Contr. e impr*., 2019, 1, p. 34 ss.; infine, si consenta il rinvio a C. BASUNTI, *La (perduta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali*, in *Contr. e impr*., 2020, 2, p. 886 ss.

È chiaro, infatti, che in queste ipotesi gli stessi dati confluirebbero in più servizi e, quindi, sarebbero oggetto di operazioni di trattamento, le quali devono pur sempre essere giustificate da una autonoma base giuridica *ex* art. 6 GDPR (o, nel caso di categorie particolari di dati, *ex* art. 9 GDPR) [12]. Il rischio che si vuole arginare è quello di favorire pratiche (commerciali o, propriamente, contrattuali) in cui un soggetto presti una sorta di "consenso *omnibus*" con cui autorizza [13] più trattamenti di dati o, comunque, in cui una sola condizione di liceità giustifichi più trattamenti di dati.

3. Questioni aperte e profili critici emergenti dall'interpretazione dell'art. 12, lett. *b*), e del *considerando* n. 33 DGA.

L'esegesi dell'art. 12, lett. *b*), DGA è tutt'altro che semplice e si espone a diversi rilievi critici.

La formulazione della norma appare, infatti, poco lineare, specie nella sua seconda parte – tanto nella versione italiana quanto in quella inglese [14] – laddove, do-

---

[12] Sulle condizioni di liceità del trattamento, v. F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, 2019, p. 110 ss.; D. POLETTI, *Le condizioni di liceità del trattamento dei dati personali*, in *Giur. it*., 2019, 12, p. 2783 ss.; ID., *Art. 6 GDPR. Liceità del trattamento*, in R. D'ORAZIO-G. FINOCCHIARO-O. POLLICINO-G. RESTA (a cura di), *Codice della* privacy *e* data protection, Milano, 2021, p. 191 ss.; M. DELL'UTRI, *Principi generali e condizioni di liceità del trattamento dei dati personali*, in V. CUFFARO-R. D'ORAZIO-V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, p. 179 ss.; con particolare riguardo al consenso al trattamento dei dati, *ex multis*, v. P. GALLO, *Il consenso al trattamento dei dati personali come prestazione*, in *Riv. dir. civ*., 2022, 6, p. 1054 ss.; C. IRTI, *Consenso "negoziato" e circolazione dei dati personali*, Torino, 2021; P. MANES, *Il consenso al trattamento dei dati personali*, cit.; V. BACHELET, *Il consenso oltre il consenso: dati personali, contratto, mercato*, Pisa, 2023; E. TOSI, *Circolazione dei dati personali tra contratto e responsabilità: riflessioni sulla fragilità del consenso e sulla patrimonializzazione dei dati personali nella società della sorveglianza digitale*, Milano, 2023; S. THOBANI, *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità*, in *Eur. dir. priv*., 2016, 2, p. 513 ss.; G. COMANDÈ, *Leggibilità algoritmica e consenso al trattamento dei dati personali*, in *Danno e resp.*, 2022, 1, p. 33 ss.; A. VIVARELLI, *Il consenso al trattamento dei dati personali nell'era digitale: sfide tecnologiche e soluzioni giuridiche*, Napoli, 2019; e sia consentito il rinvio a C. BASUNTI, *La (perduta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali*, cit., p. 860 ss.

[13] La ricostruzione del consenso-condizione di liceità come consenso di tipo autorizzatorio, idoneo a rimuovere un ostacolo posto dall'ordinamento al preesistente potere del titolare, viene efficacemente prospettata da F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, cit., p. 140 ss.; ID., *Lo "scambio di dati personali" nei contratti di fornitura di servizi digitali e il consenso dell'interessato tra autorizzazione e contratto*, cit., *passim*.

[14] Nella versione inglese, l'art. 12, lett. *b*), DGA dispone: «*the commercial terms, including pricing, for the provision of data intermediation services to a data holder or data user shall not be dependent upon whether the data holder or data user uses other services provided by the same data in-*

po aver chiarito che le condizioni commerciali per la fornitura di servizi di intermediazione dei dati non sono subordinabili all'utilizzo di altri servizi forniti dallo stesso fornitore o da un soggetto a lui collegato, prospetta l'eventualità di un «caso affermativo». In tale evenienza, che già di per sé non viene enucleata compiutamente, la disposizione si limita ad aggiungere: «in che misura il titolare dei dati o gli utenti dei dati utilizzano tali altri servizi».

La prospettazione di un «caso affermativo» parrebbe riferibile alla possibilità, seppur scoraggiata dal legislatore europeo, di subordinare la fornitura di servizi di intermediazione dei dati – o, più precisamente, le condizioni commerciali di tale fornitura e, *in primis*, la fissazione del prezzo (che è l'unica condizione esplicitata dalla norma) – alla fornitura di altri servizi. Tale interpretazione, più che dalla lettera della previsione, è supportata dalla visione sistematica della normativa *privacy*. Infatti, a simili operazioni che, come si è detto, risultano affini le operazioni di *tying*, pare possibile estendere quanto previsto dal GDPR che, appunto, non le vieta, ma le ammette con la massima cautela.

Poco chiara è altresì la successiva espressione «in che misura il titolare dei dati o gli utenti dei dati utilizzano tali altri servizi» che sembra, in un certo qual modo, scollegata dalla prima parte della norma.

A rigor di logica, l'unica interpretazione percorribile sembra quella che intende la precisazione della misura di utilizzo degli altri servizi come condizione di cui dover tenere conto nel «caso affermativo», ossia nel caso in cui il fornitore di servizi di intermediazione dei dati subordini la fruizione di tale servizio all'utilizzo di altri servizi parimenti offerti. Sul punto, preme evidenziare che l'idea secondo la quale la misura di cui discorre la norma vada precisata emerge all'esito dell'interpretazione della disposizione e non dalla lettera della legge.

L'onere di puntualizzare la misura di utilizzo degli ulteriori servizi, nel silenzio della norma, dovrebbe incombere sul fornitore dei servizi di intermediazione dei dati, quale titolare del trattamento, sulla scorta del principio di *accountability* [15]. Il che richiederebbe, tra l'altro, l'integrazione in tal senso dell'informativa da fornire agli utenti dei servizi. È vero pure però che il DGA predilige una separazione – definita, anzi, necessaria – tra i fornitori dei due paralleli tipi di servizi, sicché potrebbe essere il fornitore di quegli ulteriori servizi, quale titolare dei trattamenti ad essi relativi, il soggetto tenuto alla suddetta precisazione.

In una prospettiva *de iure condendo*, nell'eventuale (il Regolamento, in quanto tale, è pur sempre direttamente applicabile) adozione di atti delegati *ex* art. 32 DGA o di atti legislativi dei singoli Stati membri, è auspicabile un intervento integrativo che espliciti in modo adeguato il collegamento tra le due parti della norma, nonché il corretto significato della seconda.

---

termediation services provider or by a related entity, and if so to what degree the data holder or data user uses such other services».

[15] Su tale principio, per tutti, si rinvia alle acute considerazioni di G. FINOCCHIARO, *Il principio di* accountability, in *Giur. it*., 2019, 12, p. 2778 ss.

L'art. 12, lett. *b*) DGA va letto in combinato disposto con il *considerando* n. 33 DGA che ripete, almeno in parte, il contenuto della norma, ma offre qualche indicazione aggiuntiva, fornendo alcuni esempi di «altri servizi forniti dallo stesso fornitore di servizi di intermediazione dei dati o da un'entità collegata», ossia «l'archiviazione, l'analisi, l'intelligenza artificiale o altre applicazioni basate sui dati».

Sebbene, su questo punto, il menzionato *considerando* appaia chiarificatore, tuttavia, esso, nel prosieguo, lungi dal semplificare la norma, ne accresce i profili di incertezza.

Si legge, infatti, che, laddove si ammetta, nel caso concreto, la subordinazione del servizio di intermediazione dei dati alla fornitura di un altro servizio sui dati (tra cui quelli esemplificati nel *considerando* stesso), si renderebbe «necessaria una separazione strutturale tra il servizio di intermediazione dei dati e qualsiasi altro servizio fornito, in modo tale da evitare conflitti di interessi. Ciò significa che il servizio di intermediazione dei dati dovrebbe essere fornito mediante una persona giuridica distinta dalle altre attività di tale fornitore di servizi di intermediazione dei dati. Tuttavia, i fornitori di servizi di intermediazione dei dati dovrebbero poter utilizzare i dati forniti dal titolare dei dati per migliorare i loro servizi di intermediazione dei dati».

A ben vedere, il testo del *considerando* n. 33 DGA appare contraddittorio in sé, come pure in rapporto alla lett. *b*) dell'art. 12 DGA. Precisamente, sia il *considerando* sia la norma richiedono che l'ulteriore servizio (cui subordinare la fornitura di servizi di intermediazione dei dati) venga offerto dallo stesso «fornitore di servizi di intermediazione dei dati o da un'entità collegata».

La «necessaria separazione strutturale» richiesta dal *considerando* ben si coniuga con l'idea di «un'entità collegata» che offra l'ulteriore servizio, ma contrasta con la possibilità, contemplata da entrambe le previsioni, che sia il medesimo professionista ad offrire, ad un tempo, i due servizi.

La contraddizione prospettata svela, in realtà, un'altra criticità del dettato legislativo.

L'obbiettivo di evitare un conflitto di interessi o, quantomeno, di attenuarlo è sicuramente condivisibile. Esso potrebbe essere attuato, nell'ottica di una massima tutela del fruitore dei servizi sui dati, imponendo che le due tipologie di servizi in questione siano forniti solamente mediante persone giuridiche tra loro distinte. In questa prospettiva, il cumulo delle due forniture in capo al medesimo soggetto appare meno garantista. È vero pure, però, che nell'ottica del bilanciamento dei contrapposti interessi del fornitore e dell'utente dei servizi, potrebbe essere ammessa la possibilità che la gestione dei due servizi sia (solo) demandata a due organi distinti facenti parte della medesima struttura organizzativa.

Il *considerando* n. 33 DGA, nel tentativo, forse, di ammettere più opzioni, finisce però per prescrivere soluzioni fra loro inconciliabili.

Non potendosi demandare la scelta, sul punto, al singolo fornitore di servizi di intermediazione dei dati, dovrebbe essere il legislatore a decidere, a monte, come separare le due forniture, nell'ottica del più corretto bilanciamento tra la tutela dell'utente dei servizi e lo sviluppo dell'attività di impresa del fornitore, pubblico o privato che sia.

Un ulteriore profilo critico, che connota entrambe le disposizioni, è l'assenza di ogni riferimento alla figura dell'interessato, quale possibile fruitore dei servizi ivi menzionati. Esse, infatti, citano esclusivamente il titolare dei dati e l'utente dei dati.

In merito, il DGA non appare ben coniugato con il GDPR: l'interessato potrebbe, in effetti, accedere ad uno o più dei servizi di intermediazione dei dati, come pure a qualsivoglia servizio relativo ai dati. È lo stesso DGA, del resto, che, con l'obbiettivo di affermare sul mercato digitale la posizione di quei soggetti fino ad ora considerati (più) deboli, ad esempio nell'ambito dei servizi di cooperative di dati, non si limita ad includere, quali possibili fruitori di tali servizi – e, quindi, quali membri della cooperativa di dati –, i *data holders*, ma estende tale possibilità anche agli interessati.

Il susseguirsi di discipline europee mistilinee in ambito *privacy*, è evidente, ha dato (e tuttora dà) luogo al moltiplicarsi di soggetti e di possibilità di utilizzo dei dati che richiede un'imprescindibile e puntuale attività di coordinamento. Assistiamo, invece, da più punti di vista, al sovrapporsi di concetti giuridici non ordinati sistematicamente. Dunque, nella prospettiva di un costante aggiornamento, nonché incremento, del dato normativo, occorre che sia lo stesso legislatore a promuovere un proficuo dialogo tra le regole, via via formulate, sulla materia. Solo così pare possibile affrontare le sfide che il mercato digitale impone, promuovendo la massima valorizzazione dei dati e tutelando, ad un tempo, la persona nei suoi diritti e nelle sue libertà fondamentali.

Capitolo XXXVIII

Le condizioni per la raccolta e l'utilizzo dei metadati nei servizi di intermediazione di dati prestati da cooperative di dati

Stefania Calosso

Abstract: The article examines the condition for the provision of data intermediation services referred to in art. 12, letter c), Reg. 2022/868 so-called DGA related to the use of data and metadata generated by natural and legal persons who use the data intermediation service, placing it in the reality of the data cooperative. The paper proposes a preliminary reconstruction of the notion of metadata, their main functions and uses, focusing on the most relevant ones for data intermediation services, then it argues the legislation reference frame, paying close attention to traffic and location data in the field of electronic communication services, highlighting critical issues and application problems. In the end, starting from the examination of a recent provision of the Italian Data Protection Authority relating to the storage of metadata of employees' emails, it highlights the various application criticalities within the scope of data intermediation are highlighted, on the basis of an exemplification of data cooperative.

1. Il tema.

L'art. 12, lett. *c*), del Reg. UE 2022/868, c.d. *Data Governance Act* (DGA), dispone che «i dati raccolti su qualsiasi attività di una persona fisica o giuridica ai fi-

ni della fornitura del servizio di intermediazione dei dati, compresi la data, l'ora e i dati di geolocalizzazione, la durata dell'attività e i collegamenti con altre persone fisiche o giuridiche stabiliti dalla persona che utilizza il servizio di intermediazione dei dati, sono utilizzati solo per lo sviluppo di tale servizio di intermediazione dei dati, il che può comportare l'uso di dati per l'individuazione di frodi o a fini di cibersicurezza, e sono messi a disposizione dei titolari dei dati su richiesta».

Sebbene la norma non utilizzi espressamente il termine "*metadati*", ad essi possono sicuramente essere ricondotti la data, l'ora, l'ubicazione, la durata dell'attività e i collegamenti con altri soggetti posti in essere dall'utente del servizio di intermediazione di dati, richiamati nella disposizione poc'anzi citata.

Pertanto, per comprendere l'esatta portata di tale disposizione, si rende necessario chiarire preliminarmente la nozione di metadati, quali siano le loro funzioni e i loro utilizzi, in particolare nell'ambito dei servizi di intermediazione di dati, per poi definirne l'inquadramento normativo generale, nonché nello specifico ambito dei servizi delle comunicazioni elettroniche.

Infine, verranno svolte alcune considerazioni in ordine al possibile impatto che la disciplina dei metadati presenta in relazione all'attività di intermediazione delle cooperative di dati mediante una esemplificazione che prende spunto dal recente provvedimento dell'Autorità Garante per la protezione dei dati personali sulla conservazione dei metadati delle e-mail nel contesto lavorativo.

2. Nozione, funzione e utilizzo dei metadati.

Il prefisso greco "meta", che si può tradurre con "oltre", "al di là", ma anche "con", "insieme", "in mezzo", nell'espressione «*metadati*» può essere reso con "riguardo a": in senso letterale, quindi, i "metadati" sono "dati che riguardano altri dati", o dati che si uniscono ad altri dati e che attribuiscono un particolare significato ai dati cui si riferiscono, conferendo loro molteplici funzionalità e utilità [1].

Premesso che non v'è una definizione univoca di *metadati* [2] e che il più delle

[1] Cfr. P.G. WESTON-L. SARDO, *Metadati*, Roma, 2017, p. 6, secondo cui «La difficoltà di individuare gli oggetti digitali di natura non commerciale e l'esigenza di disporre, unitamente alla descrizione dei contenuti, di un adeguato corredo di informazioni sulla struttura logica e fisica degli oggetti digitali stessi indispensabile a consentirne il trattamento, la gestione e il controllo, hanno determinato lo sviluppo e l'applicazione di strutture descrittive, talvolta semplici, talvolta assai complesse, destinate ad accogliere tali dati. A queste strutture è stato attribuito il nome di metadati, dal momento che l'etimologia del termine "metadati" significa esattamente "dati intorno ai dati"».

[2] Cfr. P.G. WESTON-L. SARDO, *Metadati*, cit., p. 6, ove si legge che «In letteratura sono via via apparse varie definizioni, da quella iniziale quasi tautologica "i metadati sono dati relativi a dati, informazione relativa ad informazione" ad altre, più articolate volte a coglierne caratteristiche e funzioni, come quella proposta dal NISO (*National Information Standard Organisation*): "Con metadati si intendono informazioni strutturate che descrivono, spiegano, localizzano o rendono altrimenti più facile recuperare, usare o gestire una risorsa informativa"». Viene altresì ricordata, ivi, anche «(…) la

volte essi vengono richiamati unicamente in relazione alle loro funzionalità, ai loro utilizzi e, in particolare, ai loro molteplici impatti[3], in generale può dirsi, seppur tautologicamente, che i *metadati* sono "i dati dei dati", in quanto informazioni che descrivono, definiscono o forniscono contesto ad altri dati.

Essi di solito sono generati in maniera automatica dal sistema operativo del dispositivo utilizzato o dall'applicativo e, quindi, indipendentemente dalla volontà della persona che lo utilizza e che, a seconda della procedura in base alla quale vengono creati, sono collocati all'interno[4] o all'esterno[5] della risorsa che rappresentano.

---

definizione presente nel DCMI *Glossary* del 2005: "Dati associati con un sistema informativo con finalità di descrizione, amministrazione, requisiti legali, funzionalità tecnica, uso e utilizzo, e conservazione." (…) La *task Force on Metadata* dell'*Association for Library Collection & Technical Services* riporta un elenco di ben 27 significati"».

[3] Nella letteratura giuridica, i contesti in cui vengono affrontati i metadati attengono alla disamina dei differenti impatti che gli stessi sono suscettibili di avere in rapporto a determinate fattispecie, e solo talvolta ne vengono proposte esemplificazioni dalle quali è possibile trarne una definizione, come ad esempio, in O.S. KERR, *The next generation communications privacy act*, 2014, reperibile in ssrn.com al link https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2302891, ove si legge «*In any communications network, a fundamental distinction exists between the actual message to be sent over the network and information on the network that relates to the how, when, and where of the message. The former is the content of the communication; the latter are noncontent records known as metadata or envelope information. In the context of Internet communications, the contents include the actual messages in emails, together with their subject lines, as well as the contents of files stored on the network. In contrast, the metadata includes IP addresses, to- from information on emails, login times, and locations*»; P. OHM, *Sensitive information,* reperibile in SSRN al link https://papers.ssrn.com/sol3/papers.cfm?abstract_id =2501002, in cui viene ascritto il carattere di informazione sensibile ad alcune tipologie di metadati richiamate: «*some forms of communications metadata should be considered sensitive, for example the list of URLs visited by users of the web*»; D. WATTS, *COVIDSafe, Australia's digital contact tracing app: the legal issue*, reperibile in ssrn.com al link https://papers.ssrn.com/sol3/papers.cfm?abstract_id =3591622 in cui si rinviene un elenco di tipologie di metadati la cui raccolta è consentita: «*The subscriber of, and accounts, services, telecommunications devices and other relevant services relating to, the relevant service, the source of communication, the destination of communication, the date, time and duration of a communication, or of its connection to a relevant service, the type of a communication or of a relevant service used in connection with a communication, the location of equipment, or a line, used in connection with a communication*»; P. ORMEROD-L. TRAUTMAN, *A descriptive analysis of the fourth admendment and the third-party doctrine in the digital age*, reperibile in ssrn.com al link https://papers.ssrn.co m/sol3/papers.cfm?abstract_id=3005714, in cui si affrontano i criteri di distinzione tra contenuti e metadati alla luce della giurisprudenza e della dottrina statunitensi, ove si legge «*Courts have not (yet, at least) extended [Fourth Amendment] protections to the internet analogue to envelope markings, namely the metadata used to route internet communications, like sender and recipient addresses on an email, or IP addresses*»; P. DE FILIPPI, *The interplay between decentralization and privacy: the case of blockchain technologies*, 2016, reperibile in ssrn.com al link https://ssrn.com/abstract= 2852689, ove si evidenzia come l'analisi dei metadati può costituire il *vulnus* di alcune tipologie di architetture decentralizzate.

[4] Cfr. P.G. WESTON-L. SARDO, *Metadati*, cit., p. 8, ove si spiega che i metadati possono «essere incapsulati nella risorsa, ossia collocati all'interno del documento elettronico nella sua parte iniziale, che non viene visualizzata al lettore (*head* o *header*)».

[5] Cfr. P.G. WESTON-L. SARDO, *Metadati*, cit., pp. 8-9, ove si indica che i metadati possono «essere

Per agevolare la comprensione della nozione di metadato, si forniscono alcune esemplificazioni.

I metadati di un'*email* descrivono il tipo di *computer* che ha creato l'*email*, dove e quando essa è stata generata, chi sono mittente e destinatario, quando sono avvenuti l'invio, la ricezione e la lettura.

I metadati di una telefonata rivelano la data e l'ora in cui è stata effettuata la chiamata, la sua durata, il numero dell'utenza che è stata chiamata e di quella chiamante, la localizzazione dei dispositivi utilizzati per quella chiamata.

I metadati di un *file* ne descrivono la denominazione, le dimensioni, la data, l'ora di creazione e di ultima modifica, la tipologia (testo, documento, immagine, video, audio, etc.), il formato, i permessi di accesso, il *path*[6], la proprietà, gli attributi (ad esempio, il numero di revisioni del file, l'autore delle modifiche, etc.), l'eventuale codifica di testo utilizzata[7], *etc*.

Così, a seconda dello scopo e della loro natura i metadati possono essere suddivisi in diverse categorie, tra cui le più comuni sono quelle di seguito indicate: metadati c.d. descrittivi (*descriptive metadata*), «deputati alla identificazione e al recupero degli oggetti digitali, sono costituiti da descrizioni normalizzate dei documenti fonte (o dei documenti digitali nativi)»[8]: ad esempio, i metadati descrittivi di un file audio potrebbero includere il titolo della canzone, l'artista, l'album e il genere musicale; metadati c.d. strutturali (*structural metadata*), in quanto definiscono la struttura interna dei documenti e gestiscono le diverse relazioni tra di essi[9]: ad

---

collocati esternamente alla risorsa, ossia far parte di un archivio elettronico distinto da quello che ospita il documento che i metadati descrivono, con la predisposizione di un opportuno sistema di puntamento fra i metadati e le rispettive risorse».

[6] Il *path* di un *file* è la specifica del percorso o della posizione di un file all'interno della struttura gerarchica del sistema di *file* del *computer*. Il *path* fornisce le istruzioni per raggiungere il *file* partendo da una posizione di riferimento, che può essere il disco rigido principale, una cartella specifica o anche un altro file. Il *path* di un file è importante per localizzare e accedere al *file* da parte di un programma o di un utente e può essere utilizzato in operazioni come l'apertura di file, la copia, la modifica e la rimozione. Un *path* corretto è essenziale per garantire che il *file* corretto venga localizzato e manipolato correttamente.

[7] La codifica del testo di un *file* si riferisce al modo in cui i caratteri e i simboli all'interno del file sono rappresentati in formato binario per essere memorizzati e interpretati da un *computer*. Poiché i *computer* trattano le informazioni in forma binaria (1 e 0), è necessario un sistema di codifica per convertire i caratteri, che sono simboli visuali, in sequenze di bit che il computer può comprendere e manipolare. Ci sono diverse codifiche del testo, o metodi di rappresentazione dei caratteri, che sono utilizzate per gestire la visualizzazione e l'interpretazione dei testi in diversi linguaggi e alfabeti.

[8] Cfr. P.G. WESTON-L. SARDO, *Metadati*, cit., p. 17, secondo cui i metadati descrittivi «risiedono generalmente nelle basi dati dei sistemi di *Information Retrieval* all'esterno degli archivi degli oggetti digitali, e sono collegati a questi ultimi tramite appositi *link*: – descrizione della risorsa – autore, titolo, soggetto».

[9] Cfr. P.G. WESTON-L. SARDO, *Metadati*, cit., p. 17, secondo cui la correlazione avviene tramite un link del tipo «organizzazione interna della risorsa – identificativi univoci, numeri di pagina, caratteristiche peculiari (indice dei contenuti, indici, ecc.».

esempio, in un *database*, i metadati strutturali possono indicare le tabelle, i campi e le relazioni tra i dati; metadati c.d. amministrativi e gestionali (*administrative metadata*), poiché gestiscono gli aspetti amministrativi dei dati, come i diritti di accesso e le politiche di conservazione, cruciali per garantire la sicurezza dei dati[10] siccome tracciano l'origine e la storia dei dati, registrando informazioni come l'autore, le modifiche apportate, le relazioni[11], etc.

A seconda della tipologia cui appartengono e delle relative caratteristiche, i metadati svolgono quindi diverse funzioni che variano a seconda degli ambiti in cui vengono impiegati.

Essi possono svolgere la funzione di ricerca e recupero di un elemento, aiutando l'utente di un servizio a individuare e accedere ai dati pertinenti più rapidamente e in modo efficiente [12]; la funzione di integrazione di altri dati, consentendo il coordinamento e l'interoperabilità tra diversi sistemi e fonti di dati; la funzione di gestione dei dati cui si riferiscono, semplificandone la manutenzione e il governo attraverso l'indicazione di informazioni dettagliate sulla loro struttura, provenienza e utilizzo; la funzione di analisi a supporto dei processi decisionali, fornendo un contesto critico per un'analisi dei dati ai quali si riferiscono orientata all'assunzione di decisioni informate.

Ancora, i metadati, grazie alle loro molteplici caratteristiche, possono essere utilizzati per monitorare, controllare e prevenire le frodi attraverso la tracciabilità, il controllo degli accessi, la verifica dell'integrità dei dati, l'analisi dei *pattern* [13].

---

[10] Cfr. P.G. WESTON-L. SARDO, *Metadati*, cit., p. 17, ove si legge che i metadati amministrativi e gestionali vengono impiegati «per le svariate operazioni di gestione degli oggetti digitali all'interno dell'archivio: – gestione e amministrazione della risorsa – versione. Fonti degli originali, date di creazione, modifica, ecc.; – conservazione della risorsa nel lungo periodo – formati di file, per il trattamento digitale, formato di compressione (…)».

[11] Cfr. P.G. WESTON-L. SARDO, *Metadati*, cit., p. 18, secondo cui metadati di conservazione garantiscono «il processo di conservazione digitale all'interno di un deposito appositamente allestito: – tenuta, accessibilità, intelligibilità, autenticità delle risorse digitali – documentazione relativa alla provenienza (la storia dell'oggetto) e delle relazioni fra oggetti diversi (soprattutto interne al deposito digitale)».

[12] Cfr. P.G. WESTON-L. SARDO, *Metadati*, cit., p. 8, ove si afferma che «Il riferimento alle funzioni svolte dai metadati mette in risalto la loro inedita specificità rispetto alle tradizionali notizie catalografiche. Se da un lato, infatti, essi sono finalizzati a rendere possibile, idealmente, la catalogazione "automatica" della risorsa al momento della sua indicizzazione da parte di strumenti di ricerca appositamente predisposti, dall'altro lato essi forniscono anche notizie riguardanti, tra l'altro, la struttura, l'autenticità, la disponibilità, le modalità di accesso e di riuso nonché la storia della risorsa stessa». Con riguardo, ad esempio, all'ambito della ricerca accademica, cfr. C. ARMBRUSTER, *Access, usage and citation metrics: what function for digital libraries and repositories in research evaluation*, reperibile in ssrn.com al link https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1088453, in cui si evince il ruolo fondamentale dei metadati per la costruzione delle biblioteche digitali e dei repository per la valutazione della ricerca metrica.

[13] Il termine *pattern* in informatica può avere diversi significati a seconda del contesto. In relazione ai file, il concetto di *pattern* si riferisce a un insieme di caratteri che descrive una sequenza specifica di caratteri o di dati all'interno di un file. Nell'ambito dell'analisi dei dati, il termine *pattern* fa riferimento a una struttura o a un formato specifico che si cerca di individuare o analizzare all'interno

Nell'ambito della prevenzione delle frodi, in particolare, i metadati sono funzionali al tracciamento delle modifiche apportate ai documenti, ai file o ai database, che può aiutare a identificare attività sospette o non autorizzate; al controllo degli accessi, permettendo di individuare eventuali comportamenti anomali; a validare l'integrità dei dati, ad esempio attraverso firme digitali o marche temporali garantendo che i dati cui si riferiscono non sono stati alterati in modo fraudolento o non autorizzato; ad analizzare i *pattern* [14] di comportamenti che potrebbero indicare attività fraudolente, quali ad esempio, l'accesso ripetuto a determinati dati da parte di un singolo utente; l'auditabilità dei processi, ad esempio, mediante la registrazione dei dettagli delle operazioni sui dati, permettendo di provare che sono stati seguiti determinati protocolli e procedure volte a prevenire le frodi.

Infine, i metadati sono essenziali nell'ambito della *cybersecurity*, in particolare per la gestione delle vulnerabilità, in quanto contengono informazioni sulle versioni del *software* e sulle *patch* [15] installati su un sistema, indispensabili per identificare e gestire le vulnerabilità onde garantire che i sistemi siano aggiornati e protetti da minacce note, nonché nello svolgimento delle indagini forensi, per ricostruire eventi, determinare l'origine di un'attività dannosa e identificare possibili punti di ingresso per gli attaccanti.

Per quanto concerne gli utilizzi cui i metadati sono suscettibili, va da sé che essi possano essere impiegati in qualsiasi ambito in cui vengano svolte attività e operazioni di gestione dei dati: nelle aziende, per la gestione delle varie tipologie di dati aziendali; nelle istituzioni governative, per la gestione dei dati anagrafici, fiscali e sanitari, per fini di ricerca, statistici, di sicurezza; nelle biblioteche e negli archivi per catalogare libri, documenti o altri elementi; nelle istituzioni di ricerca per gestire i dati sperimentali e i dati di simulazione, e via dicendo.

In sintesi, può dirsi che i metadati sono una componente fondamentale per una gestione efficace dei dati, poiché essi permettono di strutturare, organizzare, trovare, comprendere, proteggere e migliorare la qualità dei dati.

Tuttavia, i metadati, in ragione delle caratteristiche che li connotano e del potenziale conoscitivo in essi racchiuso, sono altresì suscettibili di utilizzi che, a differenza di quelli dianzi richiamati, si configurano come illegittimi.

I metadati possono, infatti, essere modificati per alterare l'aspetto o il significato dei dati cui si riferiscono [16] e per eludere il *copyright* mediante l'alterazione dei

---

di un file. Ad esempio, si potrebbe cercare un pattern specifico all'interno di un file binario o di un file di log per identificare determinati comportamenti o informazioni.

[14] Cfr. nota 13.

[15] Le *patch* sono porzioni di *software* progettate per correggere o migliorare una parte specifica di un programma, di un'applicazione o di un sistema operativo. Sono deputati alla risoluzione di *bug* (errori di programmazione), di vulnerabilità di sicurezza dei software, e alla introduzione di nuove funzionalità o miglioramenti nelle prestazioni di un sistema, e sono distribuiti dagli sviluppatori dei *software* sotto forma di file o pacchetti che gli utenti possono scaricare e installare sulle proprie macchine.

[16] Ad esempio, manipolando i metadati di file di documento, l'ordine cronologico degli eventi può

c.d. *right management metadata* [17]; attraverso i metadati è possibile tracciare le attività sia *online* che *offline* di una persona e in tal modo sorvegliarla o monitorarla [18]; manipolando i metadati è possibile creare documenti o *file* falsi il cui aspetto appare autentico, ma il cui contenuto è fraudolento; alcuni metadati associati a documenti aziendali riservati possono essere estrapolati ed esfiltrati per poi, ad esempio, essere ceduti alla concorrenza; i metadati delle *e-mail* possono essere adoperati per mettere a punto tecniche di attacco informatico, quale il *phishing* [19] e, in taluni contesti, come ad esempio quello lavorativo, possono essere utilizzati per realizzare forme di sorveglianza e controllo vietate dalla legge; ancora, avvalendosi dell'analisi dei metadati si possono creare profili dettagliati delle persone, inclusi i loro interessi, le attività che svolgono online e, in generale, le loro abitudini di navigazione senza che essi ne siano consapevoli per poi compiere azioni per le quali è invece richiesto il consenso.

Tale breve esemplificazione di alcuni dei possibili utilizzi illegittimi dei metadati, pur senza alcuna pretesa di esaustività, mira a evidenziare che il patrimonio informativo in essi contenuto, poiché intrinsecamente e indissolubilmente legato alla persona fisica e/o alla realtà cui si riferiscono i dati dei quali essi sono attributo, imponga il pieno rispetto della normativa sulla protezione dei dati personali e sulla cibersicurezza da parte di qualsiasi soggetto che tratti dati e i relativi metadati, anche, e ancor più, nella modalità della prestazione di servizi di intermediazione di dati in relazione alla quale le potenziali risorse e le implicazioni dell'impego di questi ultimi impattano in maniera considerevole.

---

essere alterato cambiando la data di creazione, oppure può essere aggirato il *copyright*; i metadati di una immagine o di un video possono essere modificati per farli apparire come se fossero stati realizzati in luoghi e momenti diversi, etc.

[17] Cfr. P.G. WESTON-L. SARDO, *Metadati*, cit., p. 17. Una particolare tipologia di metadati è quella che concerne i diritti della risorsa volti a «esplicitare la titolarità dei diritti e l'uso consentito dei contenuti: – fruizione e controllo della risorsa e dei suoi contenuti – proprietà intellettuale e commerciale, restrizione dell'uso, ecc.».

[18] Si pensi a quanto accaduto nel c.d. *data gate*, cui ha dato avvio l'*hacker* e attivista Edward Snowden con una serie di rivelazioni sulle attività di sorveglianza di massa nei confronti dei cittadini statunitensi e stranieri da parte dell'agenzia per la sicurezza nazionale degli Stati Uniti, *National Security Agency* c.d. NSA, dal 2006 al 2013. Al riguardo, e in generale sul tema della sorveglianza governativa, e al ruolo che al riguardo possono rivestire i metadati, cfr. W. HARTZOG-E. SELINGER, *Surveillance as loss off obscurity*, reperibile in ssrn.com al link https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2711816.

[19] Il *phishing*, che è una delle tecniche tipiche del c.d. *social engineering*, grazie alla fraudolenta creazione di messaggi che sembrano provenire da fonti legittime pur non essendolo, spinge l'utente a compiere azioni che altrimenti non porrebbe in essere e che si concretizzano, solitamente, nel fornire informazioni personali. Il più delle volte tale illecito viene perpetrato alterando messaggi e-mail, ma può anche riguardare altre forme di comunicazione.

3. (*segue*) La funzione dei metadati nell'ambito dei servizi di intermediazione di dati.

Nell'ambito dei servizi di intermediazione di dati i metadati, grazie alle intrinseche caratteristiche che li connotano, svolgono un ruolo fondamentale potendo assolvere a molteplici funzioni chiave.

Essi facilitano, innanzi a tutto, la ricerca e la scoperta dei dati: i metadati, fornendo informazioni descrittive sui dati cui attengono, quali la tipologia, l'origine, il formato, la data di creazione, le parole chiave e le relazioni con altri dati, aiutano a identificare e comprendere rapidamente i dati oggetto di analisi, facilitando la ricerca e il reperimento di data set specifici in base a ogni singola esigenza.

Grazie ai metadati è possibile migliorare la comprensione e l'utilizzo dei dati, atteso che essi possono arricchire i dati cui si riferiscono con informazioni contestuali, come la metodologia di raccolta, le licenze d'uso, la qualità e le limitazioni, migliorandone, in tal modo, la comprensione, la corretta interpretazione, e favorendone, tra l'altro, un uso e un riuso responsabile.

I metadati possono essere utilizzati per definire un vocabolario comune e una struttura per la descrizione dei dati permettendone la standardizzazione, attributo che ne agevola l'interoperabilità in particolar modo qualora provengano da *dataset* differenti, così come avviene in seno a una struttura che svolge attività di intermediazione di dati.

Alfine di rendere la gestione dei dati più efficiente e scalabile, i metadati possono essere utilizzati per automatizzare attività come la classificazione, l'aggregazione e la sussistenza di relazioni, operazioni indispensabili allo svolgimento dell'attività di intermediazione dei dati.

Ancora, l'utilizzo dei metadati per documentare la qualità dei dati, la loro provenienza, la loro conformità agli standard nonché la loro correttezza, ne consente la valutazione in termini di affidabilità, attributo che funge da indicatore della qualità del servizio di intermediazione dei dati [20].

Infine, i metadati possono essere utilizzati per definire i diritti di accesso e le regole di utilizzo dei dati, garantendo la protezione e la sicurezza dei dati stessi, elementi irrinunciabili e imprescindibili dei dati intermediati.

Le esemplificazioni delle molteplici funzioni dei metadati dianzi proposte, ne evidenziano il ruolo cruciale nell'ambito dei servizi di intermediazione di dati nell'ottica del loro riuso [21], in quanto strumenti indispensabili per favorire e garantire

---

[20] Cfr. P.G. WESTON-L. SARDO, *Metadati*, cit., p. 19, in cui si osserva che «Se è vero che una risorsa digitale priva di metadati è a forte rischio di opacità nel *web* e finisce per essere sostanzialmente inutilizzabile, è altrettanto vero che metadati di scarsa qualità o non conformi agli standard costituiscono un serio ostacolo alla visibilità della risorsa stessa e rendono, in prospettiva, molto problematica la sua gestione».

[21] Cfr. P.G. WESTON-L. SARDO, *Metadati*, cit., p. 13, ove si afferma che «per consentire il riuso

la corretta comprensione, interoperabilità, affidabilità, sicurezza e valorizzazione dei dati, personali e non personali.

4. Inquadramento normativo dei metadati.

Premesso che non v'è una fonte normativa specificamente dedicata alla regolamentazione dei metadati in sé e per sé considerati che ne fornisca una definizione, una classificazione e una disciplina organica, il primo discrimine che sotto il profilo giuridico l'interprete è chiamato a effettuare concerne il carattere personale o non personale di volta in volta da essi rivestito, al quale consegue o meno l'applicazione del Reg. UE 2016/679, *General Data Protection Regulation* (GDPR).

Si è detto che i metadati sono i "dati dei dati": se, a prima vista, si potrebbe essere portati a ritenere che i metadati di dati personali siano anch'essi dati personali e, viceversa, che i metadati di dati non personali non siano dati personali, in realtà il discrimine non è così lineare.

Al fine di accertare la natura personale o non personale di un metadato, è necessario prendere le mosse dalla definizione contenuta nell'art. 4, n. 1, Reg. UE 2016/679, GDPR, secondo cui s'intende per dato personale «qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale»: sarà quindi la possibilità di identificare in maniera diretta o indiretta una persona fisica in base ai metadati a costituire il discrimine per la loro qualificazione come dati personali o non personali, cui conseguirà la necessità di applicare o meno la normativa sulla protezione dei dati personali [22], e ciò a pre-

della risorsa è essenziale l'esistenza dei metadati che ne documentino la struttura logica e fisica e la sintassi a un livello di dettaglio assai maggiore di quello occorrente per la semplice ricerca. La condizione perché l'utente possa servirsi efficacemente della risorsa e procedere all'elaborazione dei dati in essa contenuti è che disponga di metadati di tipo strutturale. (…) In questo senso, i metadati hanno, quindi, la funzione di fornire contesto all'informazione, ad esempio documentando le metodologie applicate nella raccolta, nella preparazione e nella formulazione dei dati, una volta che la risorsa sia entrata nello spazio di lavoro dell'utente».

[22] Si vedano anche i *considerando* nn. 26 e 30 del Reg. UE 2016/679, ove, rispettivamente, si legge: «È auspicabile applicare i principi di protezione dei dati a tutte le informazioni relative a una persona fisica identificata o identificabile. (…) Per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente. Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identifi-

scindere dal fatto che essi siano attribuiti a un dato personale o non personale.

Qualora i metadati non consentano di identificare in maniera diretta né indiretta la persona fisica, e siano perciò da ritenersi dati non personali, a essi sarà applicabile il Reg. UE 2018/1807 relativo alla libera circolazione dei dati non personali nell'Unione Europea, c.d. Regolamento FFD («*Free Flaw Data Regulation*»)[23].

Quest'ultimo, unitamente al GDPR, delinea parte della cornice normativa entro la quale dati personali e dati non personali possono «circolare liberamente tra gli Stati membri, consentendo agli utenti dei servizi di trattamento di dati di utilizzare i dati raccolti nei diversi mercati dell'UE per migliorare la loro produttività e competitività. Gli utenti possono quindi beneficiare pienamente delle economie di scala create dal grande mercato dell'UE, migliorando la propria competitività globale e aumentando l'interconnettività dell'economia dei dati europea»[24].

All'interno del Reg. FFD è contenuta la disciplina di una tipologia di dati che vengono comunemente denominati dati "misti" o "composti"[25] e che costituiscono la maggior parte degli insiemi di dati utilizzati nella c.d. "*data* economy" ormai comunemente denominati megadati o *big data,* in relazione ai quali i metadati svolgono un ruolo fondamentale: mentre i *big data*, infatti, si riferiscono alla grande quantità e complessità dei dati stessi, i metadati sono le informazioni che

---

cazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici (…)» e «Le persone fisiche possono essere associate a identificativi online prodotti dai dispositivi, dalle applicazioni, dagli strumenti e dai protocolli utilizzati, quali gli indirizzi IP, marcatori temporanei (*cookies*) o identificativi di altro tipo, quali i tag di identificazione a radiofrequenza. Tali identificativi possono lasciare tracce che, in particolare se combinate con identificativi univoci e altre informazioni ricevute dai server, possono essere utilizzate per creare profili delle persone fisiche e identificarle».

[23] L'art. 1 del Reg. UE 2018/1807 afferma che esso «mira a garantire la libera circolazione dei dati diversi dai dati personali all'interno dell'Unione stabilendo disposizioni relative agli obblighi di localizzazione dei dati, alla messa a disposizione dei dati alle autorità competenti e alla portabilità dei dati per gli utenti professionali». Più in generale, il Regolamento FFD aspira alla formazione di un contesto giuridico ed economico stabile in tema di trattamento e circolazione di dati; all'abbattimento delle barriere in materia di mobilità dei dati per le imprese, le amministrazioni pubbliche e i cittadini; ad un migliore sfruttamento del potenziale dell'economia europea dei dati (c.d. *data economy*) e alla creazione del Mercato Unico Digitale.

[24] Cfr. *Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, COM(2019) 250 final. Tali Linee Guida sono fornite dalla Commissione europea esclusivamente a titolo informativo, non costituendo una decisione ovvero un'opinione della Commissione stessa e trovano la loro fonte nell'obbligo previsto dall'articolo 8 del Regolamento FFD, ai sensi del quale «la Commissione pubblica orientamenti informativi sull'interazione tra il presente regolamento e il GDPR, in particolare per quanto concerne gli insiemi di dati composti sia da dati personali che da dati non personali» con l'obiettivo di aiutare gli utenti, specialmente le piccole e medie imprese, a comprendere meglio l'interazione tra il GDPR e il Regolamento FFD.

[25] Il Reg. FFD non li definisce né in questo né in altro modo, ma si riferisce a essi all'art. 2, par. 2 come a «un insieme di dati composto sia da dati personali che dati non personali».

forniscono contesto, struttura e significato a questa enorme mole di dati consentendo l'estrazione del valore che in essi è racchiuso [26].

Riguardo ai dati misti, il Reg. FFD dispone testualmente all'art. 2, par. 2, che esso si applica «alla parte dell'insieme contenente i dati non personali. Qualora i dati personali e non personali all'interno di un insieme di dati siano indissolubilmente legati, il presente regolamento lascia impregiudicata l'applicazione del Regolamento UE 2016/679».

Né il GDPR né il Reg. FFD definiscono, tuttavia, il concetto di "indissolubilmente legato", il quale potrebbe esemplificarsi in una «situazione in cui un insieme di dati contiene sia dati personali che dati non personali e separarli sarebbe impossibile o ritenuto dal titolare del trattamento economicamente inefficiente o non tecnicamente realizzabile» [27]; non senza rilevare che, anche laddove la separazione fosse possibile, ciò comporterebbe verosimilmente una severa diminuzione di valore [28].

In relazione alla non agevole interpretazione di tale norma, che potrebbe condurre a sostenere contrapposte posizioni, si è espressa a chiarimento la Commissione Europea affermando che i diritti e gli obblighi in materia di protezione dei dati derivanti dal GDPR si applicano all'insieme di dati misti, anche quando i dati personali rappresentano soltanto una piccola parte dell'insieme di dati [29].

Con riguardo ai metadati, a prescindere dal fatto che essi afferiscano a dati misti oppure no, l'interprete è chiamato a un ulteriore sforzo di analisi dovendo tenere in considerazione che essi possono essere ritenuti dati personali oppure non personali a seconda delle correlazioni che vengono instaurate tra di essi, perciò, laddove tali correlazioni non siano chiaramente definite o definibili a priori, la scelta di applicare al loro trattamento il GDPR pare essere quella maggiormente rispondente alla visione antropocentrica sposata dall'Unione Europea in materia di tutela della persona fisica e di protezione dei suoi dati personali.

---

[26] La maggior parte dei *big data* è costituita dai dati effettivi, che possono essere strutturati, semi-strutturati o non strutturati, che provengono da varie fonti quali ad esempio transazioni commerciali, dati di sensori, social media, registrazioni di server, log di sistema etc. I metadati sono essenziali per organizzare, gestire e interpretare l'enorme quantità di tali dati facendo loro acquisire quel valore che diversamente non avrebbero e che è talmente grande da aver indotto a considerare i big data "*the new oil"*.

[27] Cfr. le Linee Guida COM (2019) 250 final, cit., p. 9.

[28] Cfr. le Linee Guida COM (2019) 250 final, cit., p. 10.

[29] Cfr. le Linee Guida COM (2019) 250 final, cit., secondo cui «questa interpretazione è conforme con il diritto alla protezione dei dati personali sancito dalla Carta dei diritti fondamentali dell'Unione europea e con il *considerando* 8 del regolamento sulla libera circolazione dei dati non personali. Il *considerando* 8 dispone che "il quadro giuridico relativo alla protezione delle persone fisiche con riguardo al trattamento di dati personali (...) e segnatamente [il regolamento generale sulla protezione dei dati, *n.d.a.*] (...), nonché le direttive (UE) 2016/680 e 2002/58/CE (...), non sono pregiudicati dal presente regolamento"».

5. (*segue*) La disciplina dei dati relativi al traffico e all'ubicazione nell'ambito dei servizi di comunicazione elettronica nel d.lgs. n. 196/2003, codice *privacy*. Cenni.

L'esame della condizione di cui all'art. 12, lett. *c*), DGA rende necessario un breve richiamo alla disciplina dei dati relativi al traffico e all'ubicazione nell'ambito dei servizi di comunicazione elettronica contenuta nel d.lgs. n. 196/2003 cod. *privacy* atteso che la data, l'ora, i dati di geolocalizzazione, la durata dell'attività e i collegamenti stabiliti dall'utente del servizio di intermediazione di dati il cui utilizzo è consentito unicamente per lo sviluppo di quest'ultimo, afferiscono a tutte quelle forme di comunicazione elettronica attraverso le quali gli utenti usufruiscono di detti servizi, tra le quali, ad esempio, il *cloud*[30] che, per le sue caratteristiche, pare potersi ritenere essere una di quelle che più frequentemente verrà utilizzata nell'attività di intermediazione dei dati.

La richiamata disciplina è stata introdotta dalla Direttiva 2002/58/CE sulle comunicazioni elettroniche[31] in relazione ai dati relativi al traffico[32] e all'ubicazione[33] ed è stata recepita nel Titolo X della Parte II del Codice *Privacy*.

L'art. 123, co. 1, cod. *privacy* dispone che i dati relativi al traffico «sono cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione della comunicazione elettronica», salvo poi al comma successivo prevedere che qualora essi siano «strettamente necessari a fini di fatturazione per il contraente, ovvero di pagamenti in caso di interconnessione» al fornitore ne è consentito il trattamento «a fini di documentazione in caso di contestazione della fattura o per la pretesa del

---

[30] Un servizio *cloud*, o servizio di *cloud computing*, è un servizio informatico erogato tramite internet su server remoti, anziché su server locali o su un'infrastruttura fisica dell'utente, e consente di accedere a risorse informatiche, come server, archiviazione, database, software e altre risorse, attraverso internet dietro corrispettivo. Ci sono diverse tipologie di servizi *cloud*: l'*Infrastructure as a Service (IaaS)*, fornisce risorse informatiche virtualizzate su internet, come server virtuali, storage e reti; la *Platform as a service (PaaS)*, offre un ambiente di sviluppo e distribuzione completo per applicazioni, senza doversi preoccupare dell'infrastruttura sottostante; il *Software as a service (SaaS)*, consente di utilizzare applicazioni software su internet, senza doverle installare localmente; lo *Storage as a Service (STaaS)*, che fornisce servizi di archiviazione dati in *cloud*, permettendo di memorizzare e accedere ai dati da qualsiasi dispositivo connesso a internet; il *Database as a Service (DaaS)*, che offre servizi di gestione di *database* su cloud, consentendo di creare, gestire e accedere a *database* senza dover gestire l'infrastruttura sottostante.

[31] Disciplina che sostituisce quella già contenuta nel previgente d.lgs. n. 171/1998 di attuazione dell'abrogata direttiva 97/66/CE.

[32] L'art. 2, lett. *b*), Dir. 2002/58/CE definisce tale tipologia di dati come «qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione».

[33] L'art. 2, lett. *c*), Dir. 2002/58/CE definisce tale tipologia di dati come «ogni dato trattato in una rete di comunicazione elettronica che indichi la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico».

pagamento, per un periodo non superiore a sei mesi, salva l'ulteriore specifica conservazione necessaria per effetto di una contestazione anche in sede giudiziale».

Ancora, il terzo comma dell'articolo in esame consente al fornitore del servizio di comunicazione elettronica il trattamento dei dati relativi al traffico di cui al comma secondo «nella misura e per la durata necessarie a fini di commercializzazione di servizi di comunicazione elettronica o per la fornitura di servizi a valore aggiunto, solo se il contraente o l'utente cui i dati si riferiscono hanno manifestato preliminarmente il proprio consenso, che è revocabile in ogni momento» [34].

Per quanto concerne invece i dati relativi all'ubicazione, l'art. 126 cod. *privacy* sancisce, al co. 1, che «possono essere trattati solo se anonimi o se l'utente o il contraente ha manifestato previamente il proprio consenso, revocabile in ogni momento, e nella misura e per la durata necessari per la fornitura del servizio a valore aggiunto richiesto».

Sia l'art. 123 che l'art. 126 cod. *privacy*, forniscono poi ulteriori prescrizioni in ordine alle informazioni da rendere a contraenti e utenti [35] e sulle persone autorizzate a effettuare il trattamento [36].

---

[34] L'art., lett. *g*), Dir. 2002/58/CE, definisce il servizio a valore aggiunto come quel «servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all'ubicazione diversi dai dati relativi al traffico, oltre a quanto è necessario per la trasmissione di una comunicazione o della relativa fatturazione» e il *considerando* n. 18 della direttiva medesima indicando che i «servizi a valore aggiunto possono consistere ad esempio in consigli sui pacchetti tariffari meno costosi, orientamento stradale, informazioni sul traffico, previsioni meteorologiche, e informazioni turistiche» ne fornisce una esemplificazione.

[35] Al riguardo, gli artt. 123, co. 4, e 126, co. 2, cod. *privacy*, indicano rispettivamente che «Nel fornire le informazioni di cui agli articoli 13 e 14 del Regolamento il fornitore del servizio informa il contraente o l'utente sulla natura dei dati relativi al traffico che sono sottoposti a trattamento e sulla durata del medesimo trattamento ai fini di cui ai commi 2 e 3» e «Il fornitore del servizio, prima di richiedere il consenso, informa gli utenti e i contraenti sulla natura dei dati relativi all'ubicazione diversi dai dati relativi al traffico che saranno sottoposti al trattamento, sugli scopi e sulla durata di quest'ultimo, nonché sull'eventualità che i dati siano trasmessi ad un terzo per la prestazione del servizio a valore aggiunto».

[36] In relazione alle persone autorizzate al trattamento, gli artt. 123, co. 5, e 126, co. 4, cod. *privacy*, dispongono, rispettivamente, che «Il trattamento dei dati personali relativi al traffico è consentito unicamente a persone che, ai sensi dell'articolo 2-*quaterdecies*, risultano autorizzate al trattamento e che operano sotto la diretta autorità del fornitore del servizio di comunicazione elettronica accessibile al pubblico o, a seconda dei casi, del fornitore della rete pubblica di comunicazioni e che si occupano della fatturazione o della gestione del traffico, di analisi per conto di clienti, dell'accertamento di frodi, o della commercializzazione dei servizi di comunicazione elettronica o della prestazione dei servizi a valore aggiunto. Il trattamento è limitato a quanto è strettamente necessario per lo svolgimento di tali attività e deve assicurare l'identificazione della persona autorizzata che accede ai dati anche mediante un'operazione di interrogazione automatizzata» e «Il trattamento dei dati relativi all'ubicazione diversi dai dati relativi al traffico, ai sensi dei commi 1, 2 e 3, è consentito unicamente a persone autorizzate al trattamento, ai sensi dell'articolo 2-*quaterdecies*, che operano, sotto la diretta autorità del fornitore del servizio di comunicazione elettronica accessibile al pubblico o, a seconda dei casi, del fornitore della rete pubblica di comunicazioni o del terzo che fornisce il servizio a valore aggiunto. Il

Infine, l'art. 126, co. 3, cod. *privacy* prescrive che «l'utente e il contraente che manifestano il proprio consenso al trattamento dei dati relativi all'ubicazione, diversi dai dati relativi al traffico, conservano il diritto di richiedere, gratuitamente e mediante una funzione semplice, l'interruzione temporanea del trattamento di tali dati per ciascun collegamento alla rete o per ciascuna trasmissione di comunicazioni» [37].

La condizione per la fornitura di servizi di intermediazione di dati attenzionata dal presente scritto, consente l'utilizzo di tali dati unicamente per lo sviluppo del servizio di intermediazione medesimo, circostanza che assume particolare pregnanza con riferimento alle cooperative di dati posto che «le cooperative di dati mirano a raggiungere una serie di obiettivi, in particolare a rafforzare la posizione dei singoli individui, affinché compiano scelte informate prima di acconsentire all'utilizzo dei dati, influenzando i termini e le condizioni, stabiliti dalle organizzazioni di utenti dei dati, cui è subordinato l'utilizzo dei dati, in modo da offrire scelte migliori ai singoli membri del gruppo, o trovando possibili soluzioni alle posizioni contrastanti dei singoli membri di un gruppo in merito alle modalità di utilizzo dei dati laddove tali dati riguardino più interessati all'interno di tale gruppo» [38].

Al netto della questione, tutt'altro che chiara, relativa a cosa esattamente il legislatore europea abbia voluto intendere con il termine "sviluppo" del servizio di intermediazione, diversamente da quanto accade per la fornitura di "servizi a valore aggiunto" da parte dei fornitori di servizi di comunicazione elettronica [39], occorre domandarsi se il trattamento di (meta)dati relativi all'attività di una persona fisica o giuridica ai fini della fornitura del servizio di intermediazione di dati, quali la data, l'ora, i dati di geolocalizzazione, etc. sia condizionato all'acquisizione del consenso da parte degli interessati qualora essa si realizzi attraverso forme di comunicazione elettronica prestati dall'intermediario.

La risposta a tale quesito pare debba essere positiva, atteso che, come detto, i metadati in questione sono dati personali in quanto per mezzo di essi è possibile

---

trattamento è limitato a quanto è strettamente necessario per la fornitura del servizio a valore aggiunto e deve assicurare l'identificazione della persona autorizzata che accede ai dati anche mediante un'operazione di interrogazione automatizzata».

[37] Trattasi di un diritto ulteriore al diritto di limitazione di trattamento di cui all'art. 18 GDPR e che si basa su diversi presupposti, essendo, quello qui attenzionato, esercitabile su semplice richiesta senza che sia necessario il ricorrere di ipotesi particolari, a differenza di quanto avviene nel caso di esercizio del diritto di cui all'art. 18 GDPR. Esso potrebbe diversamente considerarsi, ad avviso di chi scrive, come una sorta di revoca temporanea del consenso prestato in precedenza al trattamento dei dati di ubicazione, e ciò sulla scorda della lettera dell'art. 9, co. 2, Dir. 2002/58/CE che recita: «Se hanno dato il consenso al trattamento dei dati relativi all'ubicazione, diversi dai dati relativi al traffico, l'utente e l'abbonato devono continuare ad avere la possibilità di negare, in via temporanea, mediante una funzione semplice e gratuitamente, il trattamento di tali dati per ciascun collegamento alla rete o per ciascuna trasmissione di comunicazioni».

[38] Cfr. *considerando* n. 31, Reg. 2022/868.

[39] Cfr. nota 34.

identificare la persona fisica alla quale si riferiscono e a essi è, pertanto, applicabile il Reg. UE 2016/679, GDPR.

Tuttavia, la condizione attenzionata si applica anche ai metadati di traffico e di ubicazione delle persone giuridiche, in relazione ai quali il GDPR non è applicabile [40]: la genericità della norma, anche nel non fornire alcuna indicazione aggiuntiva alla dicitura «*attività della persona fisica e giuridica*» onde poterla meglio qualificare e individuare, non agevola l'interprete, che viene così chiamato a muoversi su di un terreno insidioso e dai confini non chiaramente delineati in relazione al quale sarebbe auspicabile un intervento orientativo da parte dell'EDPB [41].

Ulteriori problematiche, non solo interpretative ma anche applicative, si prospetteranno, inoltre, al momento dell'adozione della proposta di Regolamento relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettronica e che abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche), COM(2017) 10 final, c.d. proposta di Regolamento *e-Privacy*, la quale, al *considerando* n. 8 afferma che «i dati delle comunicazioni elettroniche possono altresì rivelare informazioni relative a entità giuridiche, come segreti aziendali o altre informazioni sensibili aventi valore economico. Pertanto le disposizioni del presente regolamento dovrebbero applicarsi sia alle persone fisiche, sia alle persone giuridiche. Il presente regolamento dovrebbe inoltre garantire che le disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio si applichino anche agli utenti finali aventi natura di persone giuridiche. Questo include la definizione di consenso contenuta nel regolamento (UE) 2016/679. Qualora si faccia riferimento al consenso di un utente finale, comprese le persone giuridiche, si dovrebbe applicare tale definizione».

E infatti, l'art. 1 della proposta di Regolamento e-*Privacy* che ne definisce l'oggetto, afferma che quanto disposto dal Regolamento medesimo «precisa e integra il regolamento (UE) 2016/679 stabilendo norme specifiche ai fini di cui ai paragrafi 1 e 2» [42].

---

[40] Cfr. l'art. 1, par. 1, GDPR, secondo cui «Il presente regolamento stabilisce le norme relative alla protezione delle *persone fisiche* con riguardo al trattamento dei dati personali (…)».

[41] EDPB è l'acronimo di *European Data Protection Board*, organismo europeo indipendente sotto la cui egida si riuniscono le Autorità nazionali per la protezione dei dati personali dei paesi dello Spazio economico europeo, nonché il Garante europeo della protezione dei dati. L'EDPB garantisce che il Regolamento generale sulla protezione dei dati e la Direttiva "polizia e giustizia" sia applicato in modo coerente, nonché la cooperazione tra gli Stati membri, anche in materia di attuazione della normativa.

[42] I par. 1 e 2 dell'art. 1 della proposta di Regolamento *e-Privacy* stabiliscono, rispettivamente che «Il presente regolamento stabilisce norme in materia di tutela dei diritti e delle libertà fondamentali delle persone fisiche e giuridiche per quanto attiene alla fornitura e all'uso di servizi di comunicazione elettronica, in particolare il diritto al rispetto della vita privata e delle comunicazioni nonché la tutela delle persone fisiche in merito al trattamento dei dati personali» e che «Il presente regolamento garantisce la libera circolazione dei dati delle comunicazioni elettroniche e dei servizi di comunicazione elettronica nell'Unione, i quali non sono limitati né proibiti per motivi connessi al rispetto della vita privata e delle comunicazioni delle persone fisiche e giuridiche nonché la tutela delle persone fisiche per quanto attiene al trattamento dei dati personali».

Qualora il regolamento *e-Privacy* dovesse essere adottato in tale versione, l'estensione dell'applicazione del GDPR anche alle persone giuridiche, sebbene limitatamente all'ambito delle comunicazioni elettroniche, andrebbe a incidere grandemente sull'attuale paradigma della protezione dei dati, imponendo parallelamente il ripensamento sistematico della disciplina dei metadati che, come detto, sono una componente essenziale dei dati cui sono indissolubilmente legati.

6. (*segue*) La *data retention* dei dati relativi al traffico e all'ubicazione nell'ambito dei servizi di comunicazione elettronica. Cenni.

Sotto altro profilo, si pone un ulteriore problema relativamente al periodo di conservazione di tale tipologia di (meta)dati, in relazione al quale l'art. 132, co. 1, cod. *privacy* dispone che «i dati relativi al traffico telefonico sono conservati dal fornitore per ventiquattro mesi dalla data della comunicazione, per finalità di accertamento e repressione dei reati, mentre, per le medesime finalità, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati dal fornitore per dodici mesi dalla data della comunicazione» [43].

La conservazione dei metadati per scopi securitari, infatti, non risulta essere unicamente regolata dall'art. 132 cod. *privacy*, poiché la c.d. Legge Europea [44] dal 2017 ne impone l'obbligo di conservazione in deroga a quanto previsto dal cod. *privacy* per 72 mesi qualora vengano perseguiti scopi di repressione e accertamento di reati di particolare gravità quali il terrorismo, il saccheggio, l'associazione di tipo mafioso e simili, termine la cui durata già all'epoca ebbe ad allarmare il Garante per la protezione dei dati che ne denunciò sin da subito la contrarietà al principio di proporzionalità [45].

---

[43] Ai successivi co. 3 e 3-*bis*, l'art. 132 cod. *privacy* ne disciplina le modalità di acquisizione.

[44] L. n. 167/2017 recante le disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea.

[45] Cfr. Dichiarazione di Antonello Soro, Presidente del Garante per la protezione dei dati personali, 25 luglio 2017, reperibile al link https://www.garanteprivacy.it/home/docweb/-/docweb-display/content/id/6651720, secondo cui: «È evidente che il contrasto al terrorismo rappresenti un obiettivo di interesse generale e quindi non è in discussione la raccolta e la conservazione di dati, quanto i tempi di conservazione e le modalità di accesso agli stessi. Le norme e la giurisprudenza europea precludono una raccolta generale e indiscriminata dei dati di traffico telefonico e telematico, perché non e proporzionata alle esigenze investigative e al nucleo essenziale del diritto alla protezione dati e non può quindi essere giustificata in una società democratica. Gli stati membri possono invece prevedere obblighi di raccolta dei dati per obiettivi specifici al solo fine di contrasto di reati gravi, purché siano limitati temporalmente in misura proporzionata alle esigenze investigative e riguardino le sole informazioni a ciò strettamente necessarie. L'acquisizione dei dati stessi, inoltre, deve secondo la corte di giustizia essere soggetta a specifiche condizioni, incluso il controllo da parte di un giudice o un'autorità indipendente. La sorveglianza non può mai essere generalizzata e massiva ma, lo precisa la corte

Sebbene l'approfondimento di tale *vexata quaestio* esonderebbe dai fini del presente contributo [46], se ne è ritenuto opportuno, per completezza, un breve richiamo alla luce del fatto che essa, oltre essere a tutt'oggi irrisolta, pone questioni di non poco conto anche relativamente al termine di conservazione dei metadati in funzione dello sviluppo del servizio di intermediazione dei dati, per il quale, al momento, parrebbe potersi prospettare l'applicazione in via analogica dell'art. 126, co. 1, cod. *privacy*, quanto meno per le persone fisiche, ferma restando la prestazione del consenso e il diritto di interruzione temporanea del trattamento di cui all'art. 126, co. 3, cod. *privacy*.

Infine, le criticità dianzi evidenziate dovranno anch'esse in futuro essere (ri)considerate alla luce della disciplina dei metadati contenuta nella proposta del c.d. Regolamento *e-Privacy* [47] che stabilisce le norme «in materia di tutela dei diritti e del-

---

di giustizia nella recente sentenza tele2, deve fondarsi su requisiti individualizzanti, rivolgendosi cioè nei confronti di soggetti coinvolti, in qualche misura, in attività criminose ovvero limitandosi a specifici luoghi nei quali emergano esigenze investigative relative, sempre, a gravi reati e previa adeguata delimitazione temporale della durata della conservazione. Pur essendo consapevole dell'esigenza di non ritardare l'approvazione della legge europea con una terza lettura», ha concluso Soro, «penso che sia comunque indispensabile che il legislatore riconduca questa disciplina al criterio della proporzionalità. In futuro si dovrà meglio definire, con una disciplina organica e meno estemporanea, una materia così ricca di implicazioni sui diritti dei cittadini e sulle esigenze di giustizia». Nonché GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Segnalazione sulla disciplina della conservazione, a fini di giustizia, dei dati di traffico telefonico e telematico*, 22 luglio 2021, doc-web 9685978, reperibile al link https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9685978, ove si legge: «La carenza di proporzionalità della disciplina interna è risultata poi accentuata dalla novella di cui alla legge 167 del 2017, che ha esteso a sei anni (72 mesi) il termine massimo di conservazione dei tabulati, con acquisibilità dei dati, in questo caso, limitata tuttavia ai procedimenti per reati di competenza delle Procure distrettuali o per i quali la durata delle indagini preliminari è ampliata a due anni (artt. 51, c. 3-*quater* e 407, c. 2, lett. *a*, c.p.p.). E benché l'acquisibilità dei dati raccolti oltre il termine ordinario (ventiquattro mesi prima per i tabulati telefonici, dodici mesi prima per i telematici e trenta giorni prima per le chiamate senza risposta) sia limitata a tale categoria di reati particolarmente gravi, proprio la natura retrospettiva di questo strumento investigativo implica la conservazione generalizzata dei dati di traffico per sei anni, salvo poi limitarne l'utilizzabilità processuale ai soli casi normativamente considerati».

[46] Per un approfondimento della disciplina della conservazione e accesso ai metadati per scopi securitari nell'UE e nel contesto italiano, cfr. G. FORMICI, *Le Conclusioni dell'Avvocato Generale nel rinvio pregiudiziale C-178-22 promosso dal Tribunale di Bolzano: quo vadis, data retention*, in *Media Laws*, 2023, 2, p. 158 ss.; G. FORMICI, *The three ghosts of data retention: passato, presente e futuro della disciplina italiana in materia di conservazione e acquisizione dei metadati per scopi investigativi. Commento a margine del d.l. 30 settembre 2021, n. 132 e relativa legge di conversione*, in *Osservatorio Costituzionale*, 2022, 1, p. 125 ss.; G. FORMICI, *La* data retention *saga al capolinea? Le ultime pronunce della CGUE in materia di conservazione dei metadati per scopi securitari, tra conferme e nuove aperture*, in *DPCE online*, 2021, 1, p. 1361 ss.

[47] Cfr. Proposta di Regolamento relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettronica e che abroga la direttiva 2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche), COM(2017) 10 final.

le libertà fondamentali delle persone fisiche e giuridiche per quanto attiene alla fornitura e all'uso di servizi di comunicazione elettronica, in particolare il diritto al rispetto della vita privata e delle comunicazioni nonché la tutela delle persone fisiche in merito al trattamento dei dati personali» che andranno a precisare e integrare il Reg. UE 2016/679, GDPR [48] ma che, come espressamente affermato nella relazione al Regolamento medesimo, «non contiene disposizioni specifiche in materia di conservazione dei dati» [49].

La regola generale contenuta nell'art. 7, par. 2, proposta di Regolamento *e-Privacy* è, infatti, quella secondo cui il fornitore del servizio di comunicazioni elettroniche cancella i metadati delle comunicazioni elettroniche o anonimizza tali dati quando non sono più necessari al fine di trasmettere una comunicazione, salvo prevedere alcune eccezioni, tra le quali quella di cui all'art. 6, par. 2, lett. *c*), in virtù del quale il fornitore può trattare i metadati delle comunicazioni elettroniche «se l'utente finale ha prestato il suo consenso al trattamento dei metadati delle sue comunicazioni per uno o più fini specificati, compresa l'erogazione di servizi di traffico a tali utenti finali, purché il o i fini in questione non possano essere realizzati mediante un trattamento anonimizzato delle informazioni», consentendone in tal modo la conservazione per periodi che potrebbero essere anche molto lunghi per finalità che devono essere specificate, ma che la norma non individua, neppure in relazione all'ambito, una delle quali potrebbe quindi essere la prestazione del servizio di intermediazione di dati e il suo sviluppo.

De iure condendo, il già difficile coordinamento delle attuali molteplici disposizioni domestiche e unionali relativamente alla *data retention* di queste specifiche tipologie di metadati dovrebbe indurre i legislatori a una riflessione sistematica più ampia al fine di ripensare e riformare tale disciplina nel modo più armonico possibile e al contempo meglio rispondente alle molteplici e differenti esigenze, pubbliche e private, che nel corso degli ultimi hanno sono andate formandosi in ragione dell'importanza vieppiù crescente che i dati hanno assunto nella società e nell'economia.

---

[48] Cfr. art. 1, par. 1 e 3, proposta Regolamento sulla vita privata e le comunicazioni elettroniche, COM (2017) 10 final.

[49] Cfr. punto 1.3., cpv. 3, della Relazione alla Proposta di Regolamento sulla vita privata e le comunicazioni elettroniche, COM(2017) 10 final, che prosegue indicando che «Essa mantiene l'essenza dell'articolo 15 della direttiva sulla vita privata elettronica, allineandosi con il testo specifico dell'articolo 23 del regolamento generale sulla protezione dei dati, che disciplina i motivi per i quali gli Stati membri possono restringere l'ambito di applicazione dei diritti e degli obblighi in articoli specifici della direttiva sulla vita privata elettronica. Gli Stati membri sono pertanto liberi di mantenere o creare quadri di riferimento nazionali in materia di conservazione dei dati che prevedano fra l'altro misure di conservazione mirate, purché essi siano conformi al diritto dell'Unione e tengano conto della giurisprudenza della Corte di giustizia sull'interpretazione della direttiva sulla vita privata elettronica e della carta dei diritti fondamentali».

7. I documenti di indirizzo dell'Autorità Garante per la protezione dei dati del 21 dicembre 2023 e del 6 giugno 2024 relativi al trattamento dei metadati della posta elettronica nel contesto lavorativo: riflessioni e una esemplificazione del possibile impatto sui servizi di intermediazione dei dati da parte di cooperative di dati.

Nell'ambito di accertamenti condotti dal Garante su trattamenti di dati personali effettuati nel contesto lavorativo, è emerso il rischio che i *software* e i servizi informatici per la gestione della posta elettronica commercializzati in modalità *cloud*, possano raccogliere, per impostazione predefinita e non modificabile dall'utente, i metadati degli *account* di posta elettronica in uso ai dipendenti e conservarli per un lungo periodo di tempo [50].

Sulla base di tale circostanza, con provvedimento del 21 dicembre 2023, n. 9978728 [51], il Garante ha adottato il documento di indirizzo denominato «Programmi e servizi informatici di gestione della posta elettronica nel contesto lavora-

[50] Uno di tali accertamenti ha esitato in un'ordinanza di ingiunzione nei confronti della Regione Lazio in data 1 dicembre 2022, doc web 9833530, reperibile al link https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9833530. Nel relativo comunicato stampa pubblicato sul sito istituzionale dell'Autorità, reperibile al link https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9833616 si legge: «No al controllo dei metadati della posta elettronica dei dipendenti senza adeguate tutele per la riservatezza e in violazione delle norme che limitano il controllo a distanza dei lavoratori. Questa la decisione del Garante per la privacy nei confronti della Regione Lazio, cui ha comminato una sanzione di 100.000 euro e vietato i trattamenti tuttora in corso. Il caso nasce dalla segnalazione di un sindacato che aveva lamentato un monitoraggio posto in essere dall'amministrazione sulla posta elettronica del personale in servizio presso gli uffici dell'avvocatura regionale. Nel corso dell'istruttoria, l'ente pubblico aveva dichiarato di aver avviato una verifica interna sulla base del sospetto di una possibile rivelazione a terzi di informazioni protette dal segreto d'ufficio. Oggetto del monitoraggio, i metadati relativi ad orari, destinatari, oggetto delle comunicazioni, peso degli allegati. Il Garante ha accertato che la Regione aveva potuto effettuare il monitoraggio del personale dell'avvocatura, in particolare dei dipendenti che inviavano messaggi a uno specifico sindacato, sfruttando i dati conservati per generiche finalità di sicurezza informatica per 180 giorni, in assenza di idonei presupposti giuridici violando così i principi di protezione dei dati e delle norme sul controllo a distanza. Nel provvedimento, l'Autorità ha chiarito che la generalizzata raccolta e l'estesa conservazione dei metadati della posta elettronica – che in quanto forma di corrispondenza è tutelata dalla Costituzione – non sono strumentali allo "svolgimento della prestazione" del dipendente, ai sensi dello Statuto dei lavoratori. In questi casi, infatti, il datore deve avviare le specifiche procedure di garanzia (accordo sindacale o autorizzazione pubblica) previste dalla legge. Il trattamento di dati personali posto in essere ha, tra l'altro, consentito al datore di lavoro di entrare in possesso di informazioni relative anche alla sfera privata dei dipendenti, a partire dalle loro opinioni, contatti e fatti non attinenti all'attività lavorativa.

Oltre alla sanzione amministrativa di 100.000 euro, il Garante ha vietato alla Regione Lazio ogni ulteriore operazione di trattamento dei metadati relativi all'utilizzo della posta elettronica dei lavoratori e disposto la cancellazione di quelli illecitamente raccolti».

[51] Il documento è reperibile al link https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9978728.

tivo e trattamento dei metadati» con il quale ha ritenuto che «l'impiego dei predetti programmi e servizi di gestione della posta elettronica, in assenza dell'espletamento delle procedure di garanzia di cui all'art. 4, comma 1, della l. n. 300/1970, prima di dare avvio alla preventiva e sistematica raccolta dei metadati relativi all'utilizzo della posta elettronica da parte dei dipendenti, e alla conservazione degli stessi per un ampio arco temporale (superiore a sette giorni estensibili di ulteriori 48 ore, alle condizioni indicate al par. 3 – ovvero in caso di esperimento della procedura di cui all'art. 4, c. 1, L. 300/1970, c.d. Statuto dei lavoratori [52], *n.d.a.*), si pone in contrasto con la normativa in materia di protezione dei dati personali e con la richiamata disciplina di settore, in violazione degli artt. 5, par. 1, lett. *a*), 6 e 88, par. 1, del Regolamento, nonché 114 del Codice (in relazione all'art. 4, comma 1, della l. n. 300/1970)».

In particolare, il Garante ha affermato che «l'attività di raccolta e conservazione dei soli c.d. metadati necessari ad assicurare il funzionamento delle infrastrutture del sistema della posta elettronica, per un tempo che, all'esito di valutazioni tecniche e nel rispetto del principio di responsabilizzazione – affinché sia ritenuto applicabile il comma 2 dell'art. 4 della l. n. 300/1970 [ovvero che la posta elettronica sia ritenuta strumento utilizzato dal lavoratore per rendere la prestazione lavorativa [53], *n.d.a.*] – non può essere superiore di norma a poche ore o ad alcuni giorni, in ogni caso non oltre sette giorni, estensibili, in presenza di comprovate e documentate esigenze che ne giustifichino il prolungamento, di ulteriori 48 ore» e che «diversamente, la generalizzata raccolta e la conservazione di tali metadati, per un lasso di tempo più esteso – ancorché sul presupposto della sua necessità per finalità di sicurezza informatica e tutela dell'integrità del patrimonio, anche informativo, del datore di lavoro –, potendo comportare un indiretto controllo a distanza dell'attività dei lavoratori, richiede l'esperimento delle garanzie previste dall'art. 4, comma 1, della predetta l. n. 300/1970».

Il Documento dianzi richiamato ha suscitato severe critiche e dato impulso a

---

[52] L'art. 4, co. 1, l. n. 400/70 dispone che «Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'Ispettorato nazionale del lavoro. I provvedimenti di cui al terzo periodo sono definitivi».

[53] L'art. 4, co. 1, l. n. 400/70 dispone che «La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze».

molteplici richieste di chiarimenti che ne hanno valso la sospensione e l'avvio di una consultazione pubblica [54] il cui esito ha indotto il Garante ad apportare ad esso specifiche modifiche e integrazioni.

Nella versione aggiornata di tale documento [55], l'Autorità garante ha rivisto le indicazioni sulla conservazione dei metadati, chiarendone il perimetro applicativo, la natura, nonché la *ratio*. In particolare, il Garante: (i) ha fornito una definizione di metadati, precisando che le indicazioni contenute nel provvedimento non riguardano la gestione della posta elettronica data in uso ai lavoratori, quanto, piuttosto, la gestione dei cc.dd. "*log* di trasporto", vale a dire quelle informazioni raccolte automaticamente dai sistemi di posta elettronica e funzionali a garantire le operazioni di invio e recapito delle *e-mail*; (ii) ha specificato la natura di indirizzo del Provvedimento, sottolineando che da questo non discendono prescrizioni, nuovi obblighi o responsabilità a carico del datore di lavoro e conformando la gestione dei metadati un un'ottica di *accountability*, indicando, al riguardo, un termine di conservazione orientativo – di 21 giorni – superabile, senza attivare le garanzie di cui all'art. 4, co. 1, dello Statuto dei lavoratori, in presenza di comprovate esigenze tecniche e organizzative; (iii) ha evidenziato che l'obiettivo del Provvedimento è di sensibilizzare e "responsabilizzare" i datori di lavoro sui trattamenti aventi ad oggetto i metadati e, in particolare, sui relativi tempi di conservazione da parte dei fornitori.

Inoltre, nel ricordare che la "responsabilità generale" dei trattamenti dei metadati ricade sui datori di lavoro, in qualità di titolari del trattamento, il Garante ha invitato i fornitori dei servizi di posta elettronica a tenere conto del diritto alla protezione dei dati conformemente allo stato dell'arte e a contribuire a far sì che i datori di lavoro possano adempiere ai loro obblighi di protezione dei dati.

La riconsiderata posizione del Garante e il conseguente allungamento del termine di conservazione dei metadati, in ogni caso di natura non perentoria ma meramente indicativa, rafforza ulteriormente, a modesto avviso di chi scrive, l'esigenza, più volte dianzi evidenziata, di una riflessione sistematica più ampia della disciplina dei metadati, nell'ottica di una sua riforma inclusiva, nel complesso e delicato bilanciamento dei diritti e degli interessi dei diversi attori in gioco, del ruolo e del potenziale sempre più importante che i dati, e i dati che li descrivono, hanno nella società e nella economia moderne, e del quale il legislatore europeo ha da tempo preso atto.

Appuntando l'attenzione sul servizio di intermediazione di dati da parte di una cooperativa di dati, intendendo per tale «una cooperativa di servizi consistenti, a titolo meramente esemplificativo, nella gestione condivisa dei dati, anche attraverso la conservazione degli stessi, con misure tecniche e organizzative adeguate,

---

[54] Il provvedimento del 22 febbraio 2024 [doc web 9987885], Avviso pubblico di avvio della consultazione, è reperibile al link https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9988018.

[55] Crf. GPDP, provvedimento n. 364 del 6 giugno 2024, doc. web n. 10026277, reperibile al link https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10026277.

nell'aggregazione e nell'interazione degli stessi, nella prospettiva di creare valore per eventuali iniziative commerciali, ma anche solo per la stessa comunità che quegli stessi dati condivide, nell'assistenza e nel supporto all'esercizio dei diritti dei titolari dei dati, nonché dei soci della cooperativa, siano essi persone fisiche o persone giuridiche» [56], il provvedimento in esame induce a domandarsi se e quale impatto possa avere nei riguardi di una cooperativa di dati costituita, ad esempio, da cooperative di produzione e lavoro ove il rapporto di lavoro dei soci ha natura subordinata.

Si ponga ad esempio il caso di una cooperativa di dati italiana costituita sul modello mutualistico della *data cooperative* americana operante nel settore dei trasporti *Driver's Seat*, in cui l'analisi dei dati relativi all'attività svolta dai *rider* è orientata alla massimizzazione del vantaggio per i lavoratori medesimi, oltre che per la cooperativa e i soggetti terzi [57] i cui membri siano a loro volta cooperative di lavoro operanti nel settore delle consegne a domicilio e i cui soci lavoratori svolgano le proprie mansioni nell'ambito di un rapporto di lavoro subordinato.

Nella fattispecie, i dati oggetto di analisi e destinati alla intermediazione per il tramite della cooperativa di dati, sarebbero in larga parte costituiti dai dati di geolocalizzazione dei soci lavoratori generati da *software* e applicazione acquistati dalle cooperative di lavoro e a essi assegnati.

Poiché appare verosimile ritenere che le suddette applicazioni non consentano, similmente agli applicativi in *cloud* di gestione della posta elettronica, alcun margine di intervento in capo all'acquirente – e datore di lavoro – relativamente alle impostazioni predefinite di generazione, raccolta e periodo di conservazione dei metadati, aderendo in via analogica all'interpretazione del Garante, l'impiego di tali applicativi, imporrebbe l'adozione della procedura di codeterminazione con le rappresentanze sindacali o, in mancanza di accordo, dell'autorizzazione dell'Ispet-

---

[56] Cfr. L. PETRONE, *Il mercato digitale europeo e le cooperative di dati*, in *Contratto e Impresa*, 2023, n. 3, p. 813.

[57] Cfr. F. BRAVO, *Le cooperative di dati*, in *Contratto e Impresa*, 2023, n. 3, p. 771, ove, in relazione all'esempio di Driver's Seat, si legge: «Il lavoratore – ad esempio – potrà giovarsi dell'analisi dei dati generati dal sistema per incrementare a proprio vantaggio l'efficienza nella fornitura del servizio, individuando le fasce orare più redditizie, i percorsi più redditizi e le modalità più redditizie di remunerazione (nel trasposto di persone o cose, ad esempio, se sia più vantaggiosa la remunerazione calcolata in base al tempo impiegato o alla distanza percorsa), etc. Potrà anche valorizzare in termini monetari i dati qualora, tramite la cooperativa, siano concessi (in forma aggregata) a soggetti terzi, pubblici o privati. L'aggregazione dei dati di traffico generata dai molteplici "*drivers*" o "*riders*", con relativa data analysis, consente – ad esempio – ad enti pubblici di sviluppare mirate politiche sulla viabilità, sul traffico, sullo sviluppo urbano. In favore di società commerciali, invece, l'analisi dei dati generati da *Driver's Seat* potrebbe essere utilizzata per pianificare e decidere in ordine all'eventuale apertura di punti vendita da parte di esercizi commerciali e alla necessità o meno di acquisire ulteriori aree da destinare al parcheggio delle autori dei clienti, in una realtà urbana segnata dal crescente sviluppo dell'*e-commerce* e del *food delivery*, che potrebbero compromettere la bontà delle analisi di business plan effettuate secondo tecniche più tradizionali».

torato nazionale del lavoro territorialmente competente qualora di volessero conservare tali dati per un periodo ulteriore a quello indicato dall'Autorità garante.

Il che, oltre a comportare indubbie difficoltà, sfocerebbe in ogni caso nella impossibilità di far confluire tali metadati in questione nella logica di intermediazione in quanto estranea, *ex se*, alle finalità di cui all'art. 4, co. 1, della l. n. 300/1970[58], vanificando di fatto l'impatto di eccezionale valore di una cooperativa di dati quale quella illustrata, la cui «funzione (…) non è solo quella di collettore di dati grezzi, da cedere a soggetti terzi affinché vengano da questi analizzati e utilizzati: la cooperativa di dati può generare ulteriore valore dalla raccolta dei dati ove proceda ad un'ulteriore analisi, i cui risultati possono essere veicolati direttamente a favore dei propri soci, che ne avranno un ritorno immediato nelle direzioni che la cooperativa è in grado di percorrere a loro beneficio, in termini non necessariamente solo monetari. Le analisi dei dati consentono di adottare decisioni migliori, di incrementare il benessere, di ottenere migliori condizioni di vita e di lavoro, oltre che possibilità di fornitura di servizi di analisi dati a beneficio di soggetti terzi, da cui poter ricavare forme di monetizzazione a vantaggio degli stessi soggetti "produttori" di dati»[59].

Tali considerazioni pare valgano a incentivare, non solo da parte della comunità accademica e scientifica, bensì anche da parte del mondo imprenditoriale e istituzionale, una sistematica rivisitazione dell'attuale disciplina dei metadati, il cui ruolo decisivo per la comprensione e gestione efficiente dei dati li colloca in una posizione di primario rilievo nel momento storico che stiamo vivendo, ormai comunemente denominato *data era* proprio in ragione dell'influenza pervasiva e sempre più massiva che i dati hanno sulla società e sull'economia globale.

[58] Ossia finalità legate a organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale.

[59] Cfr. F. BRAVO, *Le cooperative di dati*, cit., p. 772.

Capitolo XXXIX

Scambio di dati, conversione di formati e interoperabilità nella fornitura del servizio intermediazione svolto dalle cooperative di dati

Cristina Chilin

Abstract: The purpose of this paper is to comment on the condition for the provision of intermediary services under Section 12(1)(d) of the Data Governance Act, and in particular, the following issues will be analyzed: the different parties involved by the legislation and the activities they are deputized to perform, the exchange aid and the conversion into specific formats by the cooperative of data belonging to the data subject or the data owner for the benefit of the user, and finally, whether the legislation under comment constitutes a kind of continuity of the right to data portability.

1. Premesse.

L'art. 12 del Regolamento (UE) 2022/868 del Parlamento Europeo e del Consiglio del 30 maggio 2022 relativo alla *governance* europea dei dati e che modifica il regolamento (UE) 2018/1724 (Regolamento sulla *governance* dei dati) [1] (in seguito

[1] Il Regolamento sulla *governance* dei dati: Regolamento (UE) 2022/868 del Parlamento Europeo e del Consiglio del 30 maggio 2022 relativo alla governance europea dei dati e che modifica il Regolamento (UE) 2018/1724 è stato pubblicato in G.U.U.E. con l. n. 152/1 il 3 giugno 2022 ed è entrato in vigore venti giorni dopo la data di pubblicazione, ma risulta applicabile ai sensi dell'art. 38 DGA dal 24 settembre 2023. Tale fonte normativa disciplina essenzialmente tre argomenti: *a*) il riuso dei dati personali e non personali gestiti dalla pubblica amministrazione; *b*) i servizi di intermediazione dei dati personali e non personali; *c*) l'altruismo dei dati.

per brevità anche solo «DGA») disciplina quali sono le condizioni per la fornitura di servizi di intermediazione dei dati.

Il presente contributo si pone l'obiettivo di commentare la condizione di cui all'art. 12, lett. *d*), del DGA, ove si prevede che «il fornitore di servizi di intermediazione dei dati agevola lo scambio dei dati nel formato in cui li riceve da un interessato o da un titolare dei dati, li converte in formati specifici solo allo scopo di migliorare l'interoperabilità a livello intrasettoriale e intersettoriale, se richiesto dall'utente dei dati, se prescritto dal diritto dell'Unione o per garantire l'armonizzazione con le norme internazionali o europee in materia di dati e offre agli interessati o ai titolari dei dati la possibilità di non partecipare a tali conversioni, a meno che la conversione non sia prescritta dal diritto dell'Unione».

L'analisi di tale normativa sarà svolta tenendo in debita considerazione l'intento del legislatore europeo, che sta cercando di attuare strumenti che portino ad una progressiva fiducia nei confronti della condivisione e del riutilizzo dei propri dati in un *common European data space* (spazio comune europeo di dati).

Tale scopo, ci spiega il DGA, potrà essere attuato anche attraverso la fornitura di servizi di intermediazione di dati, caratterizzati (o quanto meno dovrebbero) da un grado elevato di affidabilità e neutralità [2].

Ai fini di una corretta analisi delle condizioni per la fornitura di servizi di intermediazione dei dati di cui all'art. 12, lett. *d*), del DGA si dovrà prestare particolare attenzione a come l'attività dei fornitori dei servizi di intermediazione dei dati – e, per quel che ci interessa, quelli offerti dalle cooperative di dati – si rapporti con il diritto alla protezione dei dati personali, in un contesto in cui il legislatore vuole garantire contemporaneamente anche la libera circolazione dei dati, pure con Paesi terzi, che risulta soggetta a restrizioni ed eccezioni solamente «per ragioni di pubblica sicurezza, ordine pubblico e nell'ottica di altri legittimi obiettivi di politica pubblica dell'Unione, in linea con gli obblighi internazionali, anche in materia di diritti fondamentali» [3].

Per l'analisi di tali aspetti si partirà dalla definizione del concetto di servizio di cooperative di dati per poi proseguire nella disamina della condizione di cui alla lett. *d*) dell'art. 12 DGA, focalizzando l'attenzione sui diversi soggetti coinvolti, sulle attività che la norma richiede a ognuno di loro e sui rispettivi diritti e doveri garantiti dall'ordinamento europeo. Ci si soffermerà, in particolare, ad analizzare i contenuti di tali attività, nella parte in cui alla cooperativa viene chiesto di agevolare lo scambio, la condivisione e la conversione dei dati, "appartenenti" all'interes-

---

[2] Il *considerando* n. 33 del Reg. (UE) n. 868/2022 indica che «Un elemento essenziale attraverso il quale aumentare la fiducia e il controllo dei titolari dei dati, interessati e utenti dei dati nei servizi di intermediazione dei dati è la neutralità dei fornitori di servizi di intermediazione dei dati riguardo ai dati scambiati tra titolari dei dati o interessati e utenti dei dati. È pertanto necessario che i fornitori di servizi di intermediazione dei dati agiscano solo in qualità di intermediari nelle transazioni e non utilizzino per nessun altro fine i dati scambiati».

[3] Cfr. *considerando* n. 2 del Reg. (UE) n. 868/2022.

sato o al titolare dei dati, in formati specifici, a favore dell'utente dei dati. Da ultimo si verificherà se l'unico obiettivo indicato dalla disposizione in esame, che la cooperativa dei dati dovrà perseguire nella conversione dei dati in formati specifici, ossia il miglioramento dell'interoperabilità dei dati a livello intrasettoriale e intersettoriale, si ponga o meno in una sorta di continuità con il diritto alla portabilità dei dati, previsto all'art. 20 GDPR.

2. Scambio di dati, conversione di formati e interoperabilità nella fornitura del servizio intermediazione svolto dalle cooperative di dati *ex* art. 12, par. 1, lett. *d*), DGA: i soggetti coinvolti.

Le categorie giuridiche soggettive citate alla lett. *d*) dell'art. 12 del DGA sono quattro: il fornitore del servizio di intermediazione di dati, l'interessato, il titolare dei dati e l'utente dei dati.

Come si avrà modo di notare a breve, la definizione di ognuno di tali soggetti è contenuta in normative europee diverse e ciò comporta l'esigenza da parte dell'interprete di armonizzare tra loro concetti giuridici diversi, ma talvolta in parte sovrapponibili, con i rispettivi strumenti di tutela.

Partendo dal primo soggetto, il fornitore del servizio di intermediazione di dati (intermediario di dati)[4] è colui che offre servizi di intermediazione mettendo in relazione l'interessato e/o il titolare dei dati (*data holder*) con l'utente dei dati (*data user*). Grazie a tale servizio il fornitore offre quindi un servizio di raccolta, elaborazione, trasmissione e condivisione di dati tra un numero indeterminato di interessati e titolari dei dati, da un lato, e di utenti dei dati, dall'altro lato.

Più specificamente, i servizi di intermediazione vengono individuati dall'art. 10 del DGA in tre tipologie, tra loro molto diverse: *a*) servizi di intermediazione tra i

[4] Si noti come il DGA non definisce il soggetto fornitore *ex se*, ma si limita a definire in generale il servizio di intermediazione dei dati, *ex* art. 2, par. 1, n. 11, DGA come «un servizio che mira a instaurare, attraverso strumenti tecnici, giuridici o di altro tipo, rapporti commerciali ai fini della condivisione dei dati tra un numero indeterminato di interessati e di titolari dei dati, da un lato, e gli utenti dei dati, dall'altro, anche al fine dell'esercizio dei diritti degli interessati in relazione ai dati personali, ad esclusione almeno di: *a)* servizi che ottengono dati dai titolari dei dati e li aggregano, arricchiscono o trasformano al fine di aggiungervi un valore sostanziale e concedono licenze per l'utilizzo dei dati risultanti agli utenti dei dati, senza instaurare un rapporto commerciale tra i titolari dei dati e gli utenti dei dati; *b)* servizi il cui obiettivo principale è l'intermediazione di contenuti protetti da diritto d'autore; *c)* servizi utilizzati esclusivamente da un titolare dei dati per consentire l'utilizzo dei dati detenuti da tale titolare dei dati, oppure utilizzati da varie persone giuridiche all'interno di un gruppo chiuso, anche nel quadro di rapporti con i fornitori o i clienti o di collaborazioni contrattualmente stabilite, in particolare quelli aventi come obiettivo principale quello di garantire la funzionalità di oggetti o dispositivi connessi all'internet delle cose; *d)* servizi di condivisione dei dati offerti da enti pubblici che non mirano a instaurare rapporti commerciali». Per un maggior approfondimento sul tema si veda F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in *Contratto e impresa europea*, fasc. 1, 2021, p. 199 e ss.

titolari dei dati e i potenziali utenti di dati; *b*) servizi di intermediazione tra interessati e utenti di dati; *c*) servizi di cooperative di dati.

Proprio con riferimento a tale ultimo servizio – oggetto di disamina del presente articolo – si intende, ai sensi dell'art. 2, par. 1, n. 15, del DGA, il «servizi[o] di intermediazione dei dati offerti da una struttura organizzativa costituita da interessati, imprese individuali o da PMI, che sono membri di tale struttura avente come obiettivi principali quelli di aiutare i propri membri nell'esercizio dei loro diritti in relazione a determinati dati, anche per quanto riguarda il compiere scelte informate prima di acconsentire al trattamento dei dati, di procedere a uno scambio di opinioni sulle finalità e sulle condizioni del trattamento dei dati che rappresenterebbero al meglio gli interessi dei propri membri in relazione ai loro dati, o di negoziare i termini e le condizioni per il trattamento dei dati per conto dei membri prima di concedere l'autorizzazione al trattamento dei dati non personali o prima che essi diano il loro consenso al trattamento dei dati personali» [5].

Il legislatore europeo non ha fornito una definizione di cooperativa di dati *ex se* ma si è limitato, come abbiamo appena visto, a porre l'accento sull'elemento oggettivo, ossia sul servizio in sé [6].

Si può certamente ricavare dalla dottrina [7] quali siano le caratteristiche peculiari che contraddistinguono le cooperative di dati [8]. In termini generali e dal punto di vista del diritto societario, la cooperativa è contraddistinta, rispetto alle altre realtà giuridiche, da uno scopo mutualistico [9] e ciò comporta che i soci collaboreranno tra

---

[5] Con riferimento ai servizi di cooperative di dati si veda anche il *considerando* n. 31, DGA: «Le cooperative di dati mirano a raggiungere una serie di obiettivi, in particolare a rafforzare la posizione dei singoli individui, affinché compiano scelte informate prima di acconsentire all'utilizzo dei dati, influenzando i termini e le condizioni, stabiliti dalle organizzazioni di utenti dei dati, cui è subordinato l'utilizzo dei dati, in modo da offrire scelte migliori ai singoli membri del gruppo, o trovando possibili soluzioni alle posizioni contrastanti dei singoli membri di un gruppo in merito alle modalità di utilizzo dei dati laddove tali dati riguardino più interessati all'interno di tale gruppo. In tale contesto è importante riconoscere che i diritti a norma del regolamento (UE) 2016/679 sono diritti personali dell'interessato e che quest'ultimo non può rinunciarvi. Le cooperative di dati potrebbero altresì rappresentare uno strumento utile per imprese individuali e PMI che, in termini di conoscenze in materia di condivisione dei dati, sono spesso equiparabili ai singoli individui». V. D. POLETTI, *Gli intermediari dei dati*, in *EJPLT*, p. 50.

[6] Cfr. F. BRAVO, *Le Cooperative di dati,* in *Contratto e impresa*, 2023, 3, p. 759 ss.

[7] In dottrina è stata avanzata la seguente classificazione delle cooperative di dati: a) *Member-to-Cooperative*; b) *Member-to-Member (intra-cooperative*); c) *Federated*; d) *Third Party*; e) *Open Data*. Per un approfondimento si veda J. TAIT, *The Case for Data Cooperatives, Whitepaper Series*, in *Open Data Manchester*, 6th September 2021, consultabile in https://thedataeconomylab.com/2021/09/06/the-casefor-data-cooperatives/.

[8] Si evidenzia come le cooperative dei dati non sono una nuova realtà giuridica, ma sono già presenti in altri ordinamenti, come quello americano o tedesco. Si veda ad esempio con riferimento all'ordinamento americano l'attuazione della cooperativa di dati *Driver's Seat*, consultabile in https://driversseat.co.

[9] Manca nell'ordinamento italiano una definizione di scopo mutualistico. Tuttavia, copiose sono le norme che lo disciplinano, senza pretesa esaustiva se ne citano alcune: art. 45 Cost., d.lgs. 17 gennaio 2003, n. 6; artt. 2511, 2512, 2513, 2527 c.c.

loro per soddisfare con effetti più vantaggiosi i propri bisogni economici, sociali e culturali, che altrimenti non sarebbero in grado di raggiungere singolarmente.

Calato al contesto europeo del DGA, i membri della cooperativa di dati trasferiranno alla cooperativa i propri dati – siano essi di natura personale e/o non personale – al fine di vedere rafforzata la loro posizione nell'esercizio dei loro diritti sui dati, di godere di una migliore informazione in merito alle finalità e alle condizioni del trattamento dei dati, nonché alla negoziazione dei termini e delle condizioni a fronte delle quali concedere l'autorizzazione a trattare i dati non personali o a prestare il consenso al trattamento dei dati personali.

In tal modo la cooperativa dei dati dovrà garantire a ogni suo membro l'utilizzazione "informata" sui propri dati, dati che potranno essere da parte del singolo membro consapevolmente concessi, divulgati, riutilizzati o condivisi con terzi, anche per finalità commerciali, ma sempre sotto il controllo dell'interessato, socio della cooperativa di dati (c.d. "*governance* interna") [10].

Indubbiamente si tratta di vantaggi che ogni membro della cooperativa non sarebbe in grado di perseguire singolarmente o comunque avrebbe difficoltà a compiere senza l'ausilio del fornitore del servizio di intermediazione, per l'appunto la cooperativa di dati di cui l'interessato fa parte.

Allo stesso tempo, la cooperativa di dati dovrà garantire, nello svolgimento dell'attività di intermediazione, che sia comunque perseguito il superiore interesse dei propri membri, i quali concorrono, in forma societaria, alle decisioni collettive sull'utilizzo dei dati (c.d. "*governance* collettiva") [11].

Le attività ed i servizi svolti dal fornitore di servizi di intermediazione di dati, ovvero dalla cooperativa di dati, dovranno essere svolti garantendo a ogni membro il rispetto della normativa sui dati, disciplinata, per quanto attiene a quelli di natura personale, dal Reg. (UE) 2016/679 (c.d. GDPR) [12] e, a quelli di natura non personale, dal Reg. (UE) 2018/1807 [13].

---

[10] V. F. BRAVO, *Le Cooperative di dati*, cit., p. 762.

[11] *Ibidem*, pp. 762-763.

[12] Così il *considerando* n. 35 «Il presente regolamento dovrebbe lasciare impregiudicati l'obbligo incombente ai fornitori di servizi di intermediazione dei dati di rispettare il regolamento (UE) 2016/679 e la responsabilità delle autorità di controllo di garantire il rispetto di tale regolamento. Qualora i fornitori di servizi di intermediazione dei dati trattino dati personali, il presente regolamento non dovrebbe pregiudicare la protezione degli stessi. Qualora siano titolari del trattamento o responsabili del trattamento dei dati quali definiti nel regolamento (UE) 2016/679, i fornitori di servizi di intermediazione dei dati sono vincolati dalle norme di tale regolamento». Anche se la normativa appare chiara nel rispetto del GDPR, in dottrina sono state avanzate perplessità in merito al rischio di abusi nell'utilizzo di dati da parte dei fornitori dei servizi, i quali ricevono quantità ingenti di dati dai loro membri. Sul punto v. L. PETRONE, *Il mercato digitale europeo e le cooperative di dati*, in *Contratto e impresa*, 2023, 3, p. 10.

[13] Il Reg. (UE) 2018/1807 del Parlamento europeo e del Consiglio del 14 novembre 2018 relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea, è stato pubblicato in G.U.U.E. con L. n. 303/59 il 28 novembre 2018 ed è entrato in vigore il 28 maggio 2019. Sul rapporto tra il GDPR e il Reg. (UE) 2018/1807 si rimanda a COMMISSIONE EUROPEA, *Gui-*

In questo contesto si inserisce la condizione per la fornitura di servizi di intermediazione di cui all'art. 12, lett. *d*), DGA, in forza della quale la cooperativa di dati avrà il compito: *a*) di aiutare (supportare) l'interessato o il titolare dei dati in determinati casi («se richiesto dall'utente dei dati, se prescritto dal diritto dell'Unione o per garantire l'armonizzazione con le norme internazionali o europee in materie di dati») a realizzare uno scambio "agevole" dei propri dati con soggetti terzi, mediante una conversione del formato originario – che non sempre potrà risultare leggibile e comprensibile al destinatario – in un formato interoperabile; nonché *b*) di offrire all'interessato o al titolare dei dati «la possibilità di non partecipare a tali conversioni» di formato «a meno che la conversione non sia prescritta dal diritto dell'Unione».

Tale condizione con riferimento alla categoria dei servizi di cooperative di dati, per come è stata scritta, reca molteplici problemi interpretativi. In primo luogo, sembrerebbe stridere con la definizione resa dall'art. 2, par. 1, n. 15 di servizi di cooperative di dati, ove si identificano i suoi membri in «interessati, imprese individuali o da PMI», mentre nella citata lett. *d*) si contempla, quali destinatari del servizio fornito dalla cooperativa di dati, anche altri soggetti, quali il «titolare dei dati» e l'«utente dei dati», concetti su cui si tornerà a breve. Il disallineamento è solo apparente se si pensa che la cooperativa di dati, nello svolgere l'attività di intermediazione, aggrega dati provenienti dai propri «membri» (che possono essere gli «interessati» e/o i «titolari dei dati», ossia «imprese individuali» e «PMI») per poi metterli a disposizione di soggetti terzi, appunto gli «utenti dei dati», negoziando termini e condizioni per conto degli «interessati» e dei «titolari dei dati».

In secondo luogo, la condizione in commento presenta problemi interpretativi con riferimento allo strumento di conversione dei dati in formati specifici in quanto, secondo quanto precisato nei *considerando* nn. 32 e 33 del DGA, può essere svolto dalla cooperativa dei dati solamente se richiesta e autorizzata dall'interessato o dal titolare dei dati [14]; invece, nella condizione in commento si legge che la ge-

---

dance on the Regulation on a framework for the free flow of non-personal data in the European Union, 29 maggio 2019, COM (2019) 250 final.

[14] Nel *considerando* n. 32 del DGA viene chiarito che «(…) I fornitori di servizi di intermediazione dei dati dovrebbero essere *autorizzati* a offrire strumenti e servizi supplementari specifici ai titolari dei dati o agli interessati allo scopo specifico di facilitare lo *scambio dei dati*, come la conservazione temporanea, la cura, la *conversione*, l'anonimizzazione e la pseudonimizzazione. Tali strumenti e servizi dovrebbero essere utilizzati *solo su richiesta o approvazione esplicita del titolare dei dati o dell'interessato* e gli strumenti di terzi offerti in tale contesto non dovrebbero utilizzare i dati per altri scopi. Dovrebbe nel contempo essere consentito ai fornitori di servizi di intermediazione dei dati di adattare i dati scambiati, ad esempio *convertendoli in formati specifici*, per migliorarne l'usabilità dei dati per l'*utente dei dati* qualora quest'ultimo lo desideri, o migliorare l'interoperabilità (…)». Analogamente, nel *considerando* n. 33 del DGA si trova affermato che «(…) I fornitori di servizi di intermediazione dei dati dovrebbero essere in grado di mettere a disposizione dei titolari dei dati, degli interessati o degli utenti dei dati strumenti propri o di terzi al fine di agevolare lo scambio di dati, ad esempio strumenti per la conversione o la cura di dati, *solamente su richiesta esplicita o con l'esplicita approvazione dell'interessato o del titolare dei dati* (…)».

stione di tale strumento di conversione è attribuita alla *richiesta* di un altro soggetto: all'*utente dei dati* [15].

Un'interpretazione restrittiva di tale condizione porterebbe a spogliare il membro della cooperativa dai propri "privilegi", con esclusione – o riduzione – del controllo sui propri dati, lasciando a un altro soggetto – l'utente dei dati – e poi alla cooperativa un concorrente potere di gestione per il raggiungimento, di altre finalità connesse con l'esigenza di circolazione dei dati, incluse quelle ad esempio legate a logiche commerciali.

Infine, la disposizione in commento risulta di dubbia comprensione anche nella parte in cui prevede che la cooperativa di dati «offre agli interessati o ai titolari dei dati la possibilità di non partecipare a tali conversioni, a meno che la conversione non sia prescritta dal diritto dell'Unione» (art. 12, lett. *d*), DGA cit.). Non è dato comprendere né le modalità attraverso cui l'interessato o il titolare dei dati esprimano la propria "volontà di non partecipazione alla conversione dei dati", né se sia possibile un "ripensamento", con conseguente revoca di tale volontà.

Per come è stata redatta tale parte della norma, fa presagire che vi sia il rischio di una sottrazione dalla sfera di controllo dell'interessato e del titolare dei dati sull'utilizzo dei dati da questi conferiti in cooperativa, con difficoltà di armonizzazione tra il DGA e il GDPR.

Proseguendo poi il discorso con alcune considerazioni sui soggetti coinvolti dalla norma in commento, va rimarcato, preliminarmente, che per individuare la nozione di interessato (*data subject*) occorre far riferimento all'art. 4, n. 1, del Reg. (UE) 2016/679 (c.d. GDPR): è la persona fisica identificata o identificabile a cui si riferisce qualsiasi informazione [16] e che potrà esercitare nei confronti del titolare del trattamento i propri diritti (diritto all'informazione, diritto di accesso, diritto di rettifica, diritto di cancellazione, diritto di limitazione del trattamento, diritto alla portabilità dei dati, ai sensi degli artt. 15-22 GDPR). L'interessato è quindi la persona fisica a cui si riferiscono i dati di natura personale: ove il dato conferito da una persona fisica sia "non personale", il soggetto non si qualificherà, rispetto a tale dato, come "interessato" e la disciplina di cui al GDPR non troverà applicazione.

Pertanto, l'interessato che sia membro della cooperativa di dati è quella persona fisica che fornisce alla cooperativa i propri dati personali, ai fini dell'intermediazione: ove fornisse dati non personali, con volontà di condividerli in un formato digitale interoperabile ad altri soggetti, sarà considerato «titolare dei dati» e non «interessato». Nello svolgimento dei servizi di intermediazione, ai sensi dell'art. 12,

---

[15] L'art. 12, lett. *d*), del DGA prevede espressamente che «fornitore di servizi di intermediazione dei dati agevola lo *scambio dei dati* nel *formato* in cui li riceve da un interessato o da un titolare dei dati, li *converte in formati specifici* solo allo scopo di migliorare l'*interoperabilità* a livello intrasettoriale e intersettoriale, *se richiesto dall'utente dei dati* (…)».

[16] L'art. 2, par. 1, n. 7, DGA rimanda alla definizione dell'art. 4, n. 1 del GDPR, tale ultima disposizione non ha una definizione *ex* sé di interessato ma questa viene ricavata da quella di dato personale.

lett. *d*), DGA la cooperativa di dati dovrà aiutare l'interessato non solo a favorire l'accesso e/o lo scambio dei propri dati mediante la conversione in un formato digitale leggibile, ma anche consentire in qualsiasi momento che l'interessato possa esercitare i propri diritti nei confronti dell'effettivo titolare del trattamento dei dati o del soggetto a cui i dati verranno trasmessi («utente dei dati», secondo le categorie soggettive del DGA). Per far questo sarà necessario che la cooperativa di dati adotti delle *policy ad hoc* a tutela dell'interessato, diversificando a seconda che esso sia anche il titolare del trattamento o possa essere identificato in altro ruolo soggettivo ai fini della disciplina in materia di protezione dei dati personali, se del caso (ad es., responsabile del trattamento).

Per il titolare di dati (*data holder*) – soggetto distinto dal titolare del trattamento (*data controller*) – si intende invece, ai sensi dell'art. 2, par. 1, n. 8, DGA, «una *persona giuridica*, compresi gli enti pubblici e le organizzazioni internazionali, o una *persona fisica che non è l'interessato* rispetto agli specifici dati in questione e che, conformemente al diritto dell'Unione o nazionale applicabile, ha il diritto di concedere l'accesso a determinati dati personali o dati non personali o di condividerli» [17].

Secondo la condizione di cui la lett. *d*) anche il titolare dei dati, come l'interessato, potrà usufruire del servizio di agevolazione di scambio fornito dalla cooperativa di dati con conseguente conversione in un formato strutturato.

La norma risulta lacunosa con riferimento agli strumenti posti a tutela del titolare dei dati nella gestione da parte della cooperativa della condizione di cui alla lett. *d*) [18]. Tali strumenti si ritiene che difficilmente potranno essere ricavati da altri testi normativi e in particolare dal GDPR, in quanto il titolare di dati risulta essere per sua stessa definizione un soggetto (persona giuridica o persona fisica diversa dall'interessato) a cui la normativa in materia di dati personali non risulta applicabile [19]. Si reputa che anche nel caso in cui al titolare dei dati venga attribuita la qualifica di persona fisica, non potrà essere applicato il GDPR, in quanto sempre per espressa definizione del DGA tale persona è diversa dal soggetto «interessato».

Infine, l'ultima categoria soggettiva citata dalla normativa in commento riguarda l'utente di dati o utilizzatore dei dati (*data user*) che, ai sensi dell'art. 2, par. 1, n. 9, DGA, risulta definito come «una persona fisica o giuridica che ha accesso legittimo a determinati dati personali o non personali e che ha diritto, anche a norma del regolamento (UE) 2016/679 in caso di dati personali, a utilizzare tali dati a fini commerciali o non commerciali». Sostanzialmente nel GDPR esso sarebbe inqua-

---

[17] Tale nozione è stata introdotta con il DGA e riferisce il concetto di titolarità non al trattamento ma al dato. Per un'analisi della categoria soggettiva del titolare dei dati si rinvia a F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, cit., p. 202 ss.

[18] Secondo il *considerando* n. 33 del DGA «i fornitori di servizi di intermediazione dei dati dovrebbero poter utilizzare i dati forniti dal titolare dei dati per migliorare i loro servizi di intermediazione dei dati».

[19] Ai sensi dell'art. 1 GDPR tale regolamento si applica alle persone fisiche, identificate o identificabili, a cui i dati si riferiscono.

drabile nella categoria del titolare del trattamento dei dati personali [20].

L'«utente dei dati» viene citato nella condizione in commento come quel soggetto che è in grado di esercitare un potere discrezionale sulla cooperativa dei dati in merito alla possibilità, a sua semplice richiesta, di convertire in un formato specifico e interoperabile i dati che l'interessato o il titolare dei dati trasmettono alla cooperativa e siano a lui destinati.

Orbene se con riferimento ai dati di natura non personale non si rinvengono particolari problemi interpretativi ed applicativi sulla condivisione di tali dati da parte dell'interessato o del titolare dei dati al *data user*, anche alla luce di quanto stabilito nel Reg. (UE) 2018/1807 e del principio della libera circolazione dei dati non personali [21], appare invece più complessa la questione – in relazione alla condizione in commento – qualora la conversione a richiesta dell'utente in formati specifici dei dati riguardi dati di natura personale dell'interessato o dati personali conferiti dal titolare dei dati, membro della cooperativa.

Anche il GDPR favorisce il principio di libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso Paesi terzi e organizzazioni internazionali nel rispetto del principio di protezione dei dati personali [22], ma richiede, ai fini del trattamento dei dati personali da parte del titolare del trattamento, un *quid pluris* per "un'accesso legittimo", ossia la presenza di una base giuridica che lo autorizzi al trattamento dei dati per finalità determinate.

Nel momento in cui l'interessato o il titolare dei dati trasmettono i dati personali alla cooperativa per destinarli all'utilizzatore (*data user*), si dà per assodato che il servizio di intermediazione debba essere fornito nel rispetto del GDPR.

I problemi applicativi nascono soprattutto nel momento successivo qualora l'interpretazione restrittiva dell'art. 12, lett. *d*), DGA portasse a ritenere che l'interessato e il titolare dei dati non abbiano la facoltà di esercitare il diritto di richiedere la conversione in formati interoperabili per lo scambio all'utilizzatore, relativamente ai dati conferiti alla cooperativa. Tale facoltà, che la norma sembra concedere espressamente solo all'utilizzatore, non può essere di esclusiva prerogativa di quest'ultimo, in quanto porrebbe un ingiustificabile limite ai poteri di controllo da

---

[20] Ai sensi dell'art. 4, par. 1, n. 7, del GDPR il titolare del trattamento è «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali, quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri».

[21] Cfr. art. 1 Reg. (UE) 2018/1807 «Il presente regolamento mira a garantire la libera circolazione dei dati diversi dai dati personali all'interno dell'Unione stabilendo disposizioni relative agli obblighi di localizzazione dei dati, alla messa a disposizione dei dati alle autorità competenti e alla portabilità dei dati per gli utenti professionali» e art. 4 Reg. (UE) 2018/1807.

[22] L'art. 1, part. 3 del GDPR prevede che il diritto di libera circolazione dei dati personali non possa essere limitato né tantomeno vietato per motivi attinenti alla protezione dei dati personali. Per un approfondimento sul tema si veda G. FINOCCHIARO, *Commento all'art. 1 GDPR*, in R. D'ORAZIO-G. FINOCCHIARO-O. POLLICINO-G. RESTA (a cura di), *Codice della privacy e data protection*, Milano, 2021, p. 113 e ss.; R. PANETTA (a cura di), *Libera circolazione e protezione dei dati personali*, Milano, 2006.

parte dell'interessato sui propri dati personali e quindi verrebbe snaturato il diritto di protezione dei dati personali.

Con questo non si ritiene che l'utilizzatore non possa chiedere alla cooperativa di dati la conversione in formati specifici dei dati, ma che tale facoltà possa essere esercita solamente previa autorizzazione del soggetto a cui i dati appartengono.

3. L'interoperabilità: continuità del diritto alla portabilità dei dati *ex* art. 20 GDPR?

Prima di soffermarci sul concetto di interoperabilità citato nella condizione oggetto di commento del presente scritto è opportuno brevemente analizzare le caratteristiche del diritto alla portabilità [23], che costituisce un'integrazione del diritto di accesso *ex* art. 15 GDPR.

Il diritto alla portabilità consente all'interessato di controllare i propri dati e allo stesso tempo costituisce un valido strumento a supporto della libera circolazione dei dati personali all'interno dell'Unione Europea; l'obiettivo infatti di tale diritto consiste proprio nel «promuovere il controllo degli interessati sui propri dati personali, facilitando la circolazione, la copia o la trasmissione dei dati da un ambiente informatico all'altro (che si tratti dei propri sistemi, dei sistemi di soggetti terzi fidati, o di quelli di un diverso titolare del trattamento)» [24].

---

[23] Tale diritto è stato introdotto per la prima volta nell'ambito del trattamento dei dati personali con il GDPR. Per un approfondimento sul diritto alla portabilità si veda S. TROIANO, *Il diritto alla portabilità dei dati*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, 2019, p. 195 ss. F. PEZZA, *Commento all'Art. 20*, in G.M. RICCIO-G. SCORZA-E. BELISARIO (a cura di), *GDPR e normativa privacy*, Milano, 2022, p. 257 ss.; V. FALCE, *Commento all'art. 20*, in R. D'ORAZIO-G. FINOCCHIARO-O. POLLICINO-G. RESTA (a cura di), *Codice della privacy e data protection*, cit., p. 348 ss. Si evidenzia come il diritto alla portabilità era presente in altri ambiti diversi da quello delle tutela dei dati personali, ad es. nella Direttiva 2002/22/CE del Parlamento europeo e del Consiglio del 7 marzo 2002 relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica (direttiva servizio universale), abrogata dalla Direttiva (UE) 2018/1972 del Parlamento europeo e del Consiglio dell'11 dicembre 2018, che istituisce il codice europeo delle comunicazioni elettroniche, che ha introdotto la portabilità del numero telefonico oppure la portabilità dei conti correnti bancari, prevista dagli artt. 2 e 2 *bis* della l. 24 marzo 2015, n. 33 recante «*Misure urgenti per il sistema bancario e gli investimenti*». Il tema della portabilità era già conosciuto anche in ambito internazionale sul punto si rimanda a S. TROIANO, *Il diritto alla portabilità dei dati*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, cit., pp. 196-197; M. GIORGIANNI, *Il «nuovo» diritto alla portabilità dei dati personali. Profili di diritto comparato*, in *Contratto e impresa*, 2019, 4, pp. 1399-1400. Sull'utilità dello strumento della portabilità dei dati v. GARANTE EUROPEO DELLA PROTEZIONE DEI DATI, *Parere del Garante europeo sulla protezione dei dati sulla comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato e sociale europeo e al Comitato regioni – «Un approccio globale alla protezione dei dati personali nell'Unione europea*, in G.U.U.E. C181/01, 14 gennaio 2011, p. 19.

[24] Così GRUPPO DI LAVORO ARTICOLO 29 IN MATERIA DI PROTEZIONE DEI DATI PERSONALI, *Linee guida sul diritto alla "portabilità dei dati"*, adottate il 13 dicembre 2016, p. 3.

Il suo riferimento normativo lo rinveniamo all'art. 20 del GDPR, rubricato «*Diritto alla portabilità dei dati*», secondo cui «L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora: *a)* il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lett. a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e *b)* il trattamento sia effettuato con mezzi automatizzati». Ancora, il legislatore specifica al par. 3 che tale «diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento» [25] ed, al par. 4, che non dovrà ledere i diritti e le libertà di altri interessati e pertanto il titolare del trattamento non potrà trasmettere al nuovo titolare informazioni relative ad altri soggetti, salvo che la trasmissione non venga legittimata da una propria base giuridica.

Quindi, i dati portabili di cui all'art. 20 del GDPR sono solo i dati personali [26] che riguardano l'interessato e che sono stati forniti da quest'ultimo a un titolare del trattamento, il quale provvederà a trasmetterli – nei soli casi delineati dall'art. 20 cit. – ad altro titolare del trattamento, instaurando una comunicazione tra due sistemi in modo sicuro e che consenta tecnicamente al sistema del titolare "destinatario" di ricevere il *set* di dati personali in un formato apribile e "comprensibile".

Il titolare dovrà quindi trasmettere i dati personali in un formato specifico, ossia in un formato strutturato, di uso comune e leggibile da dispositivo automatico e *interoperabile*, che ne consente il riutilizzo da parte del titolare c.d. ricevente. Tuttavia, non di rado accade nella prassi che il titolare c.d. ricevente non sia in grado di supportare il formato, e quindi di leggere il *file* ricevuto e pertanto, il Gruppo di Lavoro *ex* art. 29 chiarisce che «qualora impedimenti di ordine tecnico precludano la trasmissione diretta, il titolare deve illustrarne l'esistenza agli interessati poiché, in caso contrario, la sua decisione sarà nei fatti analoga a un diniego di intervento nei confronti della richiesta formulata dall'interessato (art. 12, paragrafo 4)» [27].

---

[25] Precisa il *considerando* n. 68 GDPR «per sua stessa natura, tale diritto non dovrebbe essere esercitato nei confronti dei titolari del trattamento che trattano dati personali nell'esercizio delle loro funzioni pubbliche. Non dovrebbe pertanto applicarsi quando il trattamento dei dati personali è necessario per l'adempimento di un obbligo legale cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento».

[26] Il diritto alla portabilità non si applica ai dati anonimi, ma si applica invece ai dati pseudononimizzati. Cfr. GRUPPO DI LAVORO ARTICOLO 29 IN MATERIA DI PROTEZIONE DEI DATI PERSONALI, cit., p. 10.

[27] GRUPPO DI LAVORO ARTICOLO 29 IN MATERIA DI PROTEZIONE DEI DATI PERSONALI, cit., p. 17. Lo stesso Gruppo di Lavoro a pagina 19 delle citate Linee Guida aggiunge che in ogni settore di attività i titolari dovrebbero utilizzare formati di impiego comune, ma se ciò non fosse possibile essi «dovrebbero fornire i dati personali utilizzando formati aperti di impiego comune (per esempio: XML, JSON, CSV, ecc.) unitamente a metadati utili, al miglior livello possibile di granularità, mantenendo un livello elevato di astrazione».

Si evidenzia infine che proprio con riferimento al formato dei dati personali il GDPR non contiene alcuna indicazione specifica sulle modalità, la cui scelta dovrà ricadere sul titolare del trattamento e avere come obiettivo quello di garantire il diritto di portabilità dei dati e la loro interoperabilità all'interessato [28].

Passando ora alla disciplina della condizione di cui all'art. 12, lett. *d*), del DGA per la fornitura di servizi di intermediazione dei dati, questa consente alla cooperativa di dati di agevolare lo scambio dei dati dell'interessato o del titolare dei dati convertendoli in formati specifici solo se ciò serve a migliorare «l'interoperabilità a livello intrasettoriale e intersettoriale» e se richiesto dall'utilizzatore dei dati.

Si tratta di una disposizione che, alla luce di quanto sopra accennato in merito al diritto di portabilità, pare collocarsi in una prospettiva di continuità con quest'ultimo diritto.

Necessarie sono tuttavia alcune precisazioni in merito al concetto di interoperabilità e al contesto in cui esso si colloca, al fine di evitare abusi e storture nell'applicazione della norma.

Per interoperabilità si intende «la capacità di organizzazioni diverse e disparate di interagire in vista di obiettivi comuni concordati e reciprocamente vantaggiosi, ricorrendo alla condivisione di conoscenze e informazioni tra le organizzazioni, per mezzo dei processi aziendali che su di esse si basano, tramite lo scambio di dati fra i rispettivi sistemi TIC» [29]. Ancora più specificatamente, lo standard ISO/IEC 2382-01 definisce l'interoperabilità come «*the capability of a program to be executed on various types of data processing systems without converting the program to a different language and with little or no modification*» [30].

L'Unione europea sta cercando, ormai da anni, di rafforzare l'interoperabilità

---

[28] Il *considerando* n. 68 GDPR chiarisce che «Il diritto dell'interessato di trasmettere o ricevere dati personali che lo riguardano non dovrebbe comportare l'obbligo per i titolari del trattamento di adottare o mantenere sistemi di trattamento tecnicamente compatibili», ciò comporta – a detta del Gruppo di Lavoro ex art. 29 – che «la portabilità intende produrre sistemi interoperabili, non sistemi compatibili». GRUPPO DI LAVORO ARTICOLO 29 IN MATERIA DI PROTEZIONE DEI DATI PERSONALI, cit., p. 19.

[29] Art. 2 della Decisione n. 922/2009/CE del Parlamento europeo e del Consiglio, del 16 settembre 2009, relativa a soluzioni interoperabili per le amministrazioni pubbliche europee (ISA) – G.U.C.E. L 260, 03 ottobre 2009. Il concetto di interoperabilità lo troviamo in molteplici norme del diritto dell'unione europea, e in particolare nella Direttiva (UE) 2016/797 del Parlamento europeo e del Consiglio, dell'11 maggio 2016, relativa all'interoperabilità del sistema ferroviario dell'Unione europea; al *considerando* n. 68 del GDPR, al *considerando* nn. 2, 32, 34, 54 del DGA, al *considerando* nn. 4, 102, 151 e gli artt. 44, part. 1, lett. f, art. 85 del *Digital Service Act* e da ultimo anche nella Legge sull'intelligenza artificiale al *considerando* n. 81. Inoltre, il concetto di interoperabilità lo troviamo anche nella normativa italiana, al d.lgs. n. 196/2003, così come modificato dal d.lgs. n. 101/2018, all'art. 2-*sexies*, e nell'ambito pubblico nelle Linee guida sull'interoperabilità tecnica delle Pubbliche Amministrazioni e nelle Linee guida Tecnologie e standard per la sicurezza dell'interoperabilità tramite API dei sistemi informatici, art. 73, co. 3-*ter*, lett. *b*), del d.lgs. 7 marzo 2005, n. 82, entrambe adottate dall'AgID.

[30] Consultabile in *Information technology*, *Vocabulary*, Part 1: *Fundamental terms*, https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:-1:ed-3:v1:en.

non solo nell'ambito delle amministrazioni pubbliche [31] per migliorare i servizi offerti a favore dei cittadini, riducendone i relativi costi, ma anche più in generale nel settore privato per promuoverla nell'ambito di uno spazio comune europeo dei dati [32], con non poche difficoltà.

Le problematiche nel settore privato possono essere ricondotte essenzialmente a ostacoli di natura tecnica, ossia alla mancata adozione di protocolli *standard* per raccogliere, elaborare e condividere i dati, provenienti dall'interessato, a un altro titolare del trattamento: il c.d. soggetto ricevente, il quale non riesce materialmente in molte occasioni ad aprire ed utilizzare il *set* di dati trasmesso dal titolare del trattamento "mittente" e/o dall'utilizzatore dei dati, in quanto il *file* risulta non supportato da un formato "leggibile" e quindi non interoperabile.

In questo contesto è stato varato il DGA, che consente alla cooperativa di dati e solo su richiesta dell'utilizzatore («o se prescritto dal diritto dell'unione o per garantire l'armonizzazione con le norme nazione o europee in materia di dati») di convertire i dati (personali e non personali) in formati specifici per garantire un miglioramento dell'interoperabilità.

Già dalla formulazione della norma si rilevano alcune criticità, che necessitano di essere quanto prima arginate: in primo luogo bisognerà identificare la natura di *set* di dati che viene trasferito a un soggetto terzo da parte della cooperativa di dati, in particolare la cooperativa dovrà verificare se i dati che riceve dall'interessato o dal titolare dei dati abbiano natura personale o natura non personale, oppure siano di entrambi le categorie.

L'importanza di tale individuazione risiede nel fatto che, in un'ottica garantistica di protezione dei dati personali dell'individuo, l'interoperabilità del formato dei dati messi a disposizione dalla cooperativa dei dati costituisce una modalità, quindi

---

[31] Cfr. Decisione n. 922/2009/CE del Parlamento europeo e del Consiglio, del settembre 2009, sulle soluzioni di interoperabilità per le pubbliche amministrazioni europee (ISA), poi sostituita dalla Decisione (UE) 2015/2240 del Parlamento europeo e del Consiglio, del 25 novembre 2015, che istituisce un programma sulle soluzioni di interoperabilità e quadri comuni per le pubbliche amministrazioni, le imprese e i cittadini europei (programma ISA²) come mezzo per modernizzare il settore pubblico, abrogata dal Regolamento (UE) 2021/694 del Parlamento europeo e del Consiglio del 29 aprile 2021 che istituisce il programma Europa digitale e abroga la decisione (UE) 2015/2240. Ed ancora si veda: COMMISSIONE EUROPEA, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni "Verso l'interoperabilità dei servizi pubblici europei"*, 16 dicembre 2010, COM(2010) 744 final, che contiene la Strategia europea per l'interoperabilità (SEI) e il quadro europeo di interoperabilità (QEI); COMMISSIONE EUROPEA, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, Quadro europeo di interoperabilità* (FEI), 23 marzo 2017, COM (2017) 134 final, CONSIGLIO DELL'UNIONE EUROPEA, *Dichiarazione ministeriali sulla società digitale e su un governo digitale fondato sui valori*, Berlino, 8 dicembre 2020, CONSIGLIO DELL'UNIONE EUROPEA, *Normativa su un'Europa interoperabile*, 29 settembre 2023.

[32] Cfr. COMMISSIONE EUROPEA, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, Una strategia europea per i dati,* 19 febbraio 2020, COM (2020) 66 final.

lo strumento, dell'applicazione di un diritto – quello della portabilità appunto – esercitabile da un soggetto che goda di pieno controllo sui propri dati.

Il diritto alla portabilità, come si è visto poco sopra, si applica esclusivamente a dati di natura personale quando il trattamento dei dati è basato sul consenso oppure su un contratto e consiste in un'elaborazione elettronica. Ciò comporta che la cooperativa di dati non solo è soggetta, per lo svolgimento del servizio di intermediazione, al rispetto della condizione di cui alla lett. *d*) dell'art. 12 del DGA, ma anche al rispetto dell'art. 20 del GDPR. Fuori dai casi espressi da quest'ultimo articolo, però, non sarebbe stato possibile procedere a una conversione dei dati personali in formato interoperabile, in quanto, in assenza dell'art. 12, lett. *d*), DGA, sarebbe mancata una espressa previsione normativa che legittimasse la cooperativa di dati alla trasmissione (e l'utente dei dati alla loro richiesta).

La cooperativa di dati dovrà a monte – quindi prima di aiutare l'interessato allo scambio dei dati – filtrare le informazioni personali che ricadono nell'ambito della portabilità, verificando il rispetto dell'art. 20 del GDPR.

Un'altra questione di interesse riguarda il controllo dei dati dopo il loro trasferimento all'utente dei dati, grazie alla conversione dei formati e all'interoperabilità. La cooperativa di dati, sorretta da uno scopo mutualistico, è in grado di controllare termini e condizioni negoziandoli per conto degli interessati e dei titolari dei dati che siano membri della propria struttura organizzativa, ma non potrà controllare la successiva circolazione che, grazie all'interoperabilità, potrà avvenire più facilmente anche tra un utente di dati e altri soggetti terzi.

La successiva circolazione dei dati potrebbe cioè avvenire con i connotati tipici delle logiche capitalistiche tradizionali, non mutualistiche, che potrebbero far sorgere rischi di compressione dei diritti dell'interessato, come ad esempio quelli che il Garante per la protezione dei dati personali aveva inizialmente ravvisato nel caso *Weople*[33].

La vicenda ha riguardato un'impresa italiana, la società Hoda S.r.l., che in qualità di fornitore di servizi di intermediazioni, raccoglieva con apposita delega i dati personali dell'interessato, non direttamente dallo stesso ma da altri *provider* (ad es. *Facebook, Amazon, Google* etc.), in applicazione del diritto alla portabilità dei dati di cui all'art. 20 GDPR. I dati raccolti presso altri *providers* venivano poi inseriti all'interno di una propria banca dati, con relativa possibilità di essere utilizzati da parte dell'utente per ottenere, grazie all'intermediario, una "monetizzazione" dei propri dati o altri vantaggi.

Il Garante per la protezione dei dati personali aveva aperto un'istruttoria sull'esercizio del diritto di portabilità da parte del servizio *Weople* su delega dell'interessato e sulla "commercialità dei dati", interessando anche l'*European Data Protection Board* (EDPB)[34], il quale ad oggi non si è ancora pronunciato sul punto.

---

[33] Per un commento del caso *Weople* si veda F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, cit. p. 216 ss.

[34] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Lettera del Presidente del Garante per la protezione dei dati personali al Presidente dell'European Data Protection Board (EDPB), avente ad*

In assenza del parere del EDPB e fino all'emanazione delle disposizioni del DGA sull'intermediazione dei dati, si faticava a rinvenire una soluzione in altre disposizioni normative o nelle Linee guida sulla portabilità [35], le quali non affrontano – per una mera questione temporale di adozione delle disposizioni – il tema dei servizi di intermediazione presente nel DGA.

Tuttavia, non si può non evidenziare che, se tale sistema di delega e poi di commerciabilità dei dati fosse consentito *tout court* senza alcuna limitazione consentirebbe all'*infomediario* di sacrificare le logiche di protezione dei diritti e delle libertà degli interessati per la vendita dei dati con conseguente perdita di controllo dell'interessato sui dati personali [36], ed indebolimento del diritto alla protezione dei dati personali. I correttivi sono stati inseriti, invece, proprio nel DGA, con un sistema di controllo dell'operato degli intermediari di dati, tramite le condizioni di cui all'art. 12 e il monitoraggio del loro rispetto ad opera di un'apposita *Authority*.

Sempre con riferimento al diritto alla portabilità di dati e all'obiettivo finale dell'interoperabilità, si ritiene che l'art. 20 GDPR possa trovare applicazione solamente con riferimento al soggetto c.d. interessato e non anche con il titolare dei dati, posto che tale soggetto per sua stessa definizione non risulta in alcun modo identificabile con l'interessato.

Pertanto, la condivisione, l'utilizzo e la conversione in formati specifici di dati (personali e non personali) del titolare dei dati da parte della cooperativa all'utente non potrà costituire una sorta di continuità con il diritto di portabilità *ex* art. 20 GDPR, ma consiste in un nuovo diritto concesso al titolare dei dati che ha caratteristiche oggettive diverse: dalla modalità di attuazione, al contenuto e alla relativa tutela e che può essere accomunato al diritto di portabilità solo dal punto di vista del miglioramento dell'interoperabilità, ossia dal lato tecnico-sistematico nella ricerca da parte della cooperativa dei dati del formato specifico da utilizzare, che in ogni caso non dovrà escludere il titolare dal controllo sui propri dati.

Sempre con riferimento alla norma in commento, non si rilevano particolari cri-

---

oggetto «*Richiesta di parere in tema di commercializzazione dei dati personali e diritto alla portabilità*» (doc web n. 9126725 del 1° agosto 2019).

[35] GRUPPO DI LAVORO ARTICOLO 29, *Linee guida sul diritto alla portabilità dei dati*, cit.

[36] Cfr. F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, cit. p. 228. L'A. sostiene che «Il potere di controllo dell'interessato sui propri dati personali, tuttavia, sembra dileguarsi o esistere solamente in senso formale, dato che comunque, per poter essere esercitato, occorre che vi sia una infrastruttura tecnica e tecnologica, elemento indefettibile oggi per l'effettivo esercizio di un controllo sui dati. In un contesto sostanzialmente tecnocratico, qual è quello che si sta delineando attualmente, l'effettivo potere di controllo non risiede, come vorrebbe il legislatore, nelle mani dell'interessato, ma in quelle del titolare del trattamento che esercita il potere di predisposizione dell'apparato tecnologico per il trattamento dei dati e che, tramite esso, è in grado di utilizzare tali dati per finalità commerciali e di controllo sociale e, come s'è visto, anche politico». Ed ancora v. D. POLETTI, *Gli intermediari di dati*, cit., p. 55, «il diritto alla portabilità finisce per esaltare maggiormente questo suo secondo volto (libera circolazione dei dati), tanto da apparire più funzionale al controllo dei *data holders*, che detengono i dati, piuttosto che a quello dei *data subiects*».

ticità per lo scambio in un formato specifico di dati di natura non personale, se non quelle legate all'eventuale perdita di controllo dei dati da parte del titolare dei dati (persona fisica o giuridica) a fronte dell'ingerenza dell'utente di dati nella conversione degli stessi per un miglioramento dell'interoperabilità.

Si evidenzia infine che, come nel GDPR, la condizione di cui alla lett. *d*) dell'art. 12 del DGA prevede genericamente la conversione in «*formati specifici*», e pertanto anche in questo caso pare ipotizzabile che la scelta del formato di trasmissione verrà definita dalla cooperativa di dati, su richiesta del *data user* e, dunque, tenendo conto delle sue necessità. Ciò dovrebbe consentire di contenere il rischio che la scelta intrapresa non consenta al soggetto ricevente di visualizzare o utilizzare i dati. Tale rischio purtroppo permarrà fintanto che non verrà varata una norma o una prassi che vada a definire il concetto di formato specifico e gli *standard* univoci a cui il titolare del trattamento o più in generale i fornitori dei servizi di intermediazione di dati dovranno conformarsi.

4. Conclusioni.

In una prospettiva europea di centralità del dato, di un mercato comune di dati, della libera circolazione degli stessi, e del progressivo avanzare della tecnologia, i servizi di intermediazione costituiscono indubbiamente una risorsa per consentire la disponibilità più rapida a più soggetti di una moltitudine di dati, dati che potranno essere ri-utilizzati anche per scopi diversi da quelli primari.

Astrattamente lo scambio di dati (personali e non) tra diversi soggetti porta a un miglioramento in ogni settore dei processi decisionali e dei risultati applicabili, tuttavia dal punto di vista pragmatico numerose problematiche impediscono all'Unione europea di realizzare compiutamente la circolazione "economica" dei dati.

Alcune di esse sono state affrontante nel presente scritto e riguardano: la (non) disponibilità dei dati da parte dell'interessato e del titolare dei dati e l'interoperabilità. La poca chiarezza terminologica della normativa del DGA e la difficoltà di armonizzazione con le altre normative in materia di trattamento dei dati sembrano descrivere un contesto in cui l'interessato e il titolare dei dati rischiano di venire spogliato del controllo degli stessi, allorché i dati (dopo essere stati condivisi con gli "utenti dei dati" grazie al servizio di intermediazione, a fronte dell'iniziale interoperabilità) possano poi sottrarsi al controllo dell'interessato, del titolare e dell'intermediario (cooperativa di dati), nelle ulteriori fasi di circolazione dei dati, destinati ad essere non più governabili tanto il perimetro della ricollazione quanto il ricorso ad ulteriori formati non facilmente accessibili.

Capitolo XL

Cooperative di dati e offerta di servizi a valore aggiunto

Daniele Sborlini

Abstract: In line with the European data strategy, Regulation (EU) 2022/868 (Data Governance Act, DGA) has introduced a horizontal regulatory framework for data intermediation services, including those of data cooperatives, with the objective of promoting such services, on the assumption that they play a key role in the data economy in order to foster data sharing. However, the discipline envisaged for these services is particularly strict with respect to the data operations permitted for data intermediaries and the services they can provide, with negative impacts on data cooperatives in particular, thus raising doubts as to its effectiveness in pursuing its intended goal. Essential in this context are the provisions on value-added services (Art. 12(e) DGA), which authorise data intermediaries, within certain limits, to provide tools and services other than those necessary for the mere implementation of data exchange. The aim of this paper is therefore to analyse the main characteristics of this discipline and then to examine some of the issues relating to its application in the case of data cooperatives, in order to provide some initial indications for an interpretation that is attentive to the specific needs underlying these peculiar organisations. Specific attention is paid to the possibility of benefiting from the provisions on additional services for the implementation of "data pools" within data cooperatives, which is of paramount importance to enable the data valorisation capabilities of these entities.

1. Note introduttive.

Il Reg. UE n. 868/2022 relativo alla *governance* europea dei dati [1], implementando la strategia europea per i dati [2], ha introdotto un quadro di notifica e controllo per la fornitura dei servizi di intermediazione dei dati [3], categoria che include altresì i servizi di cooperative di dati [4].

Il regolamento ha l'obiettivo di promuovere i servizi di intermediazione dei dati, sul presupposto che gli stessi svolgano un ruolo essenziale nell'economia dei dati [5], in particolare nel favorire la condivisione dei dati [6], la quale è a sua volta funzionale alla creazione dello "spazio unico europeo di dati" ricercata dalla citata *data strategy*, quale "mercato unico di dati" volto a stimolare la crescita e creare valore nel pieno rispetto del diritto dell'Unione europea [7].

L'impostazione seguita dal DGA nel disciplinare la fornitura dei servizi di *data intermediation* è basata su di una rigida regolazione *ex ante*, facente perno su stringenti obblighi di neutralità imposti ai fornitori di tali servizi rispetto sia ai dati scambiati per il loro tramite sia alle parti della transazione di dati, i quali mirano ad aumentare la fiducia di persone e imprese nei meccanismi della condivisione dei dati intermediata e a prevenire possibili distorsioni della concorrenza nei mercati dell'infomediazione [8].

---

[1] Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo alla *governance* europea dei dati e che modifica il regolamento (UE) 2018/1724 (Regolamento sulla *governance* dei dati o "*Data Governance Act*", noto anche con l'acronimo "DGA").

[2] COMMISSIONE EUROPEA, Comunicazione del 19 febbraio 2020, intitolata «*Una strategia europea per i dati*», COM(2020)86 final.

[3] Per la definizione di «servizio di intermediazione dei dati», v. l'art. 2, n. 11, Reg. cit. In Italia, per lo svolgimento dei compiti relativi alla procedura di notifica e al monitoraggio della conformità dei fornitori di servizi di intermediazione dei dati al regolamento, è stata individuata dal d.lgs. 7 ottobre 2024, n. 144 (recante norme di adeguamento della normativa nazionale alle disposizioni del Reg. cit.), quale «autorità competente per i servizi di intermediazione dei dati» (art. 13 Reg. cit.), l'Agenzia per l'Italia digitale (AgID).

[4] I «servizi di cooperative di dati» sono definiti dal DGA come «servizi di intermediazione dei dati offerti da una struttura organizzativa costituita da interessati, imprese individuali o da PMI, che sono membri di tale struttura, avente come obiettivi principali quelli di aiutare i propri membri nell'esercizio dei loro diritti in relazione a determinati dati, anche per quanto riguarda il compiere scelte informate prima di acconsentire al trattamento dei dati, di procedere a uno scambio di opinioni sulle finalità e sulle condizioni del trattamento dei dati che rappresenterebbero al meglio gli interessi dei propri membri in relazione ai loro dati, o di negoziare i termini e le condizioni per il trattamento dei dati per conto dei membri prima di concedere l'autorizzazione al trattamento dei dati non personali o prima che essi diano il loro consenso al trattamento dei dati personali».

[5] *Considerando* n. 27 Reg. cit.

[6] La condivisione dei dati (*data sharing*) è definita all'art. 2, n. 10, Reg. cit.

[7] COMMISSIONE EUROPEA, *Una strategia europea per i dati*, cit., p. 16 ss.

[8] In merito, v. *infra*, par. 2.1. Va precisato fin d'ora come il Reg. UE n. 868/2022, nonostante il si-

Al riguardo, è stato evidenziato come tale disciplina risulti finanche eccessivamente restrittiva e che ciò, in ultimo, potrebbe ripercuotersi altresì sulla possibilità di conseguire l'obiettivo di promuovere il *data sharing* intermediato [9]. Le rigide condizioni alle quali è assoggettata la fornitura dei servizi di intermediazione dei dati potrebbero anche impedire agli intermediari il godimento di quei margini di operatività necessari per assicurarne la sostenibilità economica [10].

Su queste premesse, risulta di rilevante interesse il regime previsto dal regolamento sulla *governance* dei dati relativamente alla fornitura di servizi "a valore aggiunto" (art. 12, lett. *e*), Reg. cit.), consistenti in strumenti o servizi supplementari a quelli strettamente necessari a realizzare lo scambio dei dati tra le parti della transazione [11]. Questa disciplina attenua la rigidità delle disposizioni sulla neutralità, abilitando gli intermediari a fruire, entro certi limiti, dei benefici dell'integrazione verticale, così rappresentando la possibile chiave per l'identificazione di modelli commerciali che garantiscano agli intermediari dei dati di competere sui mercati digitali [12].

---

curo rilievo dall'angolo visuale del diritto della concorrenza, non abbia come obiettivo specifico la protezione di quest'ultima e, infatti, rinviene la propria base giuridica nell'art. 114 TFUE, inerente all'armonizzazione delle legislazioni degli Stati membri per il funzionamento del mercato interno, politica seppur connessa, differente da quella sulla concorrenza. Ciò, al pari di quanto rilevabile rispetto al Reg. UE n. 1925/2022 relativo a mercati equi e contendibili nel settore digitale ("*Digital Markets Act*"), il quale è parimenti fondato su tale base giuridica, nonostante il suo indubbio rilievo "concorrenziale". Su tali profili, v. P. MANZINI, *Il* Digital Market Act *decodificato*, in ID-M. VELLANO (a cura di), *Unione europea 2020*, Milano, 2021, p. 319; S. SCALZINI, Digital Markets Act *e tutela della concorrenza*, in AIDA, 2024, p. 18 ss.

[9] Cfr. ad es. L. VON DITFURTH, *Datenmärkte, Datenintermediäre und der Data Governance Act*, Berlin/Boston, 2024, pp. 268 ss. e 583 ss.; ID.-G. LIENEMANN, *The Data Governance Act: – Promoting or Restricting Data Intermediaries?*, in *Competition and Regulation in Network Industries*, 2022, Vol. 23, n. 4, p. 290; H. RICHTER, *Looking at the Data Governance Act and Beyond: How to Better Integrate Data Intermediaries in the Market Order for Data Sharing*, in *GRUR International*, 2023, Vol. 72, n. 5, p. 465 ss.

[10] V. ad es. AA.VV., *Mapping the Landscape of Data Intermediaries – Emerging Models for More Inclusive Data Governance*, Publications Office of the European Union, Luxembourg, 2023, p. 34 ss.; G. CAROVANO-M. FINCK, *Regulating Data Intermediaries: The impact of the Data Governance Act on the EU's Data Economy*, in *Computer Law & Security Review*, 2023, 50, p. 11 ss.; M. MICHELI-M. PONTI-M. CRAGLIA-A. BERTI, *Emerging Models of Data Governance in the Age of Datafication*, in *Big Data & Society*, 2020, Vol. 7, n. 2, p. 9 ss.

[11] Sull'art. 12, lett. *e*), Reg. cit., v. ad es. L. VON DITFURTH, *Datenmärkte, Datenintermediäre und der Data Governance Act*, cit., p. 395 ss.; F. BRAVO, *Le cooperative di dati*, in *Contratto e impresa*, 2023, 3, p. 778; H. RICHTER, *Looking at the Data Governance Act and Beyond: How to Better Integrate Data Intermediaries in the Market Order for Data Sharing*, cit., p. 463; AA.VV., *Data Access and Sharing in Germany and in the EU: Towards a Coherent Legal Framework for the Emerging Data Economy. A Legal, Economic and Competition Policy Angle*, Final Report, 2022, p. 286; S. NARDI, *Articolo 12 – Condizioni per la fornitura di servizi di intermediazione dei dati*, in A. MORACE PINELLI (a cura di), *Dalla* Data Protection *alla* Data Governance: *il Regolamento (UE) 2022/868*, Pisa, 2024, pp. 252-253.

[12] V. *infra*, par. 2.2.

Per le cooperative di dati [13], l'offerta di servizi supplementari potrebbe consistere nel mezzo abilitante tali strutture organizzative a conseguire effettivamente gli obiettivi loro assegnati dal regolamento europeo, inerenti, in sintesi, alla prestazione di attività di supporto ai propri membri (interessati, imprese individuali e PMI) nell'ambito del *data sharing*. Dette attività vanno oltre la pura intermediazione dei dati e ciò ne rende complessa l'individuazione del fondamento giuridico e del relativo perimetro di legittimità entro le trame del DGA, il quale non prevede alcuna rimodulazione delle rigide condizioni cui è assoggettata la fornitura dei servizi di intermediazione dei dati, disposizioni sulla neutralità incluse, al caso delle cooperative di dati [14].

In tal senso, la presente ricerca si propone l'obiettivo di analizzare i principali tratti caratterizzanti la disciplina per la prestazione di servizi e strumenti aggiuntivi stabilita all'art. 12, lett. *e*), Reg. cit., per poi approfondire alcune questioni relative all'applicazione di tale regime al caso delle *data cooperatives*, in modo da fornire dei primi spunti ricostruttivi per un'interpretazione del medesimo che sia attenta alle specifiche esigenze sottese alle cooperative di dati, in ragione degli obiettivi attribuiti a tali organizzazioni dallo stesso *Data Governance Act*. Un approfondimento specifico riguarderà la possibilità di fruire delle disposizioni sui servizi a valore aggiunto per implementare forme di messa in comune dei dati ("*data pooling*") entro le cooperative di dati, le quali costituiscono modalità di valorizzazione dei dati specialmente rispondenti alle caratteristiche di tali intermediari, quali organizzazioni nelle quali la dimensione collettiva assume un rilievo centrale [15].

---

[13] Rispetto alle cooperative di dati (nozione, elementi caratterizzanti, modelli operativi emersi nella prassi), v. G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, in *Rivista trimestrale di diritto pubblico*, 2022, 4, p. 985 ss.; F. BRAVO, *Le cooperative di dati*, cit., p. 768 ss.; L. PETRONE, *Il mercato digitale europeo e le cooperative di dati*, in *Contratto e impresa*, 2023, 3, p. 810 ss.; AA.VV., *Mapping the Landscape of Data Intermediaries – Emerging Models for More Inclusive Data Governance*, cit., p. 47 ss.; E. BIETTI-A. ETXEBERRIA-M. MANNAN-J. WONG, *Data Cooperatives in Europe: A Legal and Empirical Investigation*, White Paper created as part of *The New School's Platform Cooperativism Consortium and Harvard University's Berkman Klein Center for Internet & Society* Research Sprint, 2021, p. 8 ss.; V. BELLOMIA, *Articolo 2 – Definizioni*, in A. MORACE PINELLI (a cura di), *Dalla* Data Protection *alla* Data Governance: *il Regolamento (UE) 2022/868*, cit., p. 183 ss.; S. NARDI, *Articolo 10 – Servizi di intermediazione dei dati*, in A. MORACE PINELLI (a cura di), *Dalla* Data Protection *alla* Data Governance: *il Regolamento (UE) 2022/868*, cit., p. 240 ss.; M. MICHELI-M. PONTI-M. CRAGLIA-A. BERTI, *Emerging Models of Data Governance in the Age of Datafication*, cit., p. 7 ss.; AA.VV., *Unlocking the Power of Digital Commons: Data Cooperatives as a Pathway for Data Sovereign, Innovative and Equitable Digital Communities*, in *Digital*, 2023, Vol. 3, n. 3, p. 147 ss.; AA.VV., *White Paper on the Data Governance Act*, in *CiTiP Working Paper Series*, 2021, p. 29 ss.; T. HARDJONO-A. PENTLAND, *Data Cooperatives: Towards a Foundation for Decentralized Personal Data Management*, in *arXiv.org*, 2019, p. 2 ss.

[14] V. *infra*, par. 3.

[15] V. *infra*, parr. 3.4.-3.5.

2. L'offerta di strumenti e servizi supplementari da parte dei fornitori di servizi di intermediazione dei dati (art. 12, lett. *e*), Reg. UE n. 868/2022).

2.1. La disciplina dei servizi a valore aggiunto quale eccezione al principio di neutralità riguardo ai dati scambiati.

Ai fini dell'inquadramento giuridico della disciplina stabilita dall'art. 12, lett. *e*), Reg. UE n. 868/2022 relativamente all'offerta di servizi a valore aggiunto nel contesto dei servizi di intermediazione dei dati, è bene prendere le mosse dal principio di neutralità dei fornitori di tali servizi riguardo ai dati scambiati, emergente principalmente dall'art. 12, lett. *a*), Reg. cit. [16], di centrale rilievo nel contesto delle condizioni cui il regolamento sulla g*overnance* dei dati assoggetta la fornitura dei servizi in esame.

Questo principio, in breve, impone ai fornitori di servizi di intermediazione dei dati due requisiti interdipendenti: *(i)* il divieto di impiego dei dati per i quali sono forniti servizi di intermediazione dei dati per scopi diversi dalla messa a disposizione degli stessi verso gli utenti dei dati [17] e *(ii)* l'obbligo di fornire detti servizi tramite una persona giuridica distinta [18].

Il divieto di utilizzo dei dati scambiati ha una duplice portata [19]: da un lato, impedisce all'intermediario di utilizzare tali dati per proprie finalità (neutralità come limitazione della finalità) e, dall'altro, vieta la prestazione verso gli interessati, i titolari dei dati [20] e gli utenti dei dati di servizi *data-based* differenti da quelli di intermediazione (neutralità come limitazione dei servizi basati sui dati scambiati) [21].

---

[16] Sul requisito di cui all'art. 12, lett. *a*), Reg. cit. quale espressione della neutralità imposta ai fornitori di servizi di intermediazione dei dati, v. G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit., p. 982 (ove è sottolineato come il principio di neutralità sia formulato quale «primo tra i requisiti sostanziali» per la fornitura di tali servizi); F. BRAVO, *Le cooperative di dati*, cit., p. 798; L. VON DITFURTH, *Datenmärkte, Datenintermediäre und der Data Governance*, cit., p. 340; AA.VV., *White Paper on the Data Governance Act*, cit., p. 31 ss.; G. CAROVANO-M. FINCK, *Regulating Data Intermediaries: The impact of the Data Governance Act on the EU's Data Economy*, cit., p. 8; L. LIONELLO, *La creazione del mercato europeo dei dati: sfide e prospettive*, in *Diritto del commercio internazionale*, 2021, p. 687; S. NARDI, *Articolo 12 – Condizioni per la fornitura di servizi di intermediazione dei dati*, cit., p. 253 ss.

[17] Gli «utenti dei dati» sono definiti all'art. 2, n. 9, Reg. cit.

[18] L'art. 12, lett. *a*), Reg. cit., in particolare, dispone che «il fornitore di servizi di intermediazione dei dati non utilizza i dati per i quali fornisce servizi di intermediazione dei dati per scopi diversi dalla messa a disposizione di tali dati agli utenti dei dati e fornisce servizi di intermediazione dei dati attraverso una persona giuridica distinta».

[19] Cfr. ad es. L. VON DITFURTH, *Datenmärkte, Datenintermediäre und der Data Governance*, cit., pp. 340 ss. e 355 ss.

[20] Per la definizione di «titolare dei dati», v. l'art. 2, n. 8, Reg. cit.

[21] Rispetto alla neutralità riguardo ai dati scambiati, il *considerando* n. 33 Reg. cit. prevede la ne-

Il secondo requisito di cui all'art. 12, lett. *a*), Reg. cit., che impone la fornitura dei servizi di infomediazione tramite una persona giuridica a ciò appositamente deputata, implementa la neutralità mediante un obbligo parimenti operante in via preventiva, ma sul piano soggettivo, tramite una segregazione di tali servizi a livello strutturale, volta ad impedire i conflitti di interesse che potrebbero aversi in caso di fornitura da parte dell'intermediario sia del servizio di intermediazione sia di prodotti o servizi di altra natura; detta circostanza, invero, costituisce un incentivo, per il fornitore di tali servizi, all'utilizzo dei dati intermediati nel perseguimento di propri scopi, nel contesto degli altri prodotti o servizi offerti. Il requisito in questione ha l'effetto di estendere la limitazione dei servizi erogabili oltre quelli basati sui dati scambiati, impedendo la prestazione da parte dell'intermediario di qualsiasi altro servizio che sia diverso da quello di *data intermediation* [22].

La neutralità emerge altresì da ulteriori condizioni stabilite dall'art. 12 DGA, che ne precisano la portata o tendono a rafforzarne l'effettività [23]. Tra queste, vi è appunto la disciplina oggetto di interesse nella presente sede, relativa alla possibilità per l'intermediario di offrire agli interessati o ai titolari dei dati servizi a valore aggiunto (art. 12, lett. *e*), Reg. cit.), la quale introduce un'eccezione al descritto divieto di impiego dei dati, abilitando i fornitori dei servizi di intermediazione dei dati, entro i limiti prestabiliti da tale norma, a offrire strumenti e servizi "supplementari" o "aggiuntivi", i quali sono così definiti appunto perché comportano un utilizzo dei dati per scopi che vanno oltre il limite della mera messa a disposizione degli stessi ai *data users* imposto dall'art. 12, lett. *a*), Reg. cit.

Tanto premesso, la collocazione della disciplina sull'offerta di servizi aggiuntivi entro il principio di neutralità e, segnatamente, la sua natura di eccezione rispetto a tale principio rende opportuni alcuni cenni ulteriori sulle funzioni perseguite dalla neutralità dei fornitori di servizi di *data intermediation* rispetto ai dati oggetto della transazione.

La neutralità dei servizi di intermediazione dei dati emerge dal Reg. UE n. 868/2022 quale requisito chiave per il conseguimento degli obiettivi del regolamento, operando infatti in due direzioni a ciò strumentali: *(i)* essa costituisce un «elemento essenziale» per aumentare la fiducia e il controllo nei servizi di infome-

---

cessità che «i fornitori di servizi di intermediazione dei dati agiscano solo in qualità di intermediari nelle transazioni e non utilizzino per nessun altro fine i dati scambiati».

[22] Cfr. il *considerando* n. 33 Reg. cit., ove è rimarcata la necessità di «una separazione strutturale tra il servizio di intermediazione dei dati e qualsiasi altro servizio fornito, in modo tale da evitare conflitti di interessi. Ciò significa che il servizio di intermediazione dei dati dovrebbe essere fornito mediante una persona giuridica distinta dalle altre attività di tale fornitore di servizi di intermediazione dei dati».

[23] Le altre condizioni espressione della neutralità, diverse da quella di cui alla lett. *e*) dell'art. 12 esaminata a seguire, si rinvengono in particolare all'art. 12, lett. *c*), Reg. cit. (limitazione circa l'uso dei "metadati" raccolti ai fini della fornitura del servizio di intermediazione, ammessa solo per scopi di "sviluppo" di tale servizio) e all'art. 12, lett. *d*), Reg. cit. (limitazione per l'intermediario di convertire in altri formati i dati oggetto dello scambio, ammessa solo alle condizioni previste da tale norma).

diazione di tutte le parti coinvolte nelle transazioni di dati e, al contempo, *(ii)* abilita un «ambiente competitivo» per la condivisione dei dati [24], in funzione, più ampiamente, della realizzazione di uno "spazio europeo comune dei dati" che sia connotato da quella parità di condizioni tale da consentire alle imprese di competere «sulla qualità dei servizi e non sulla quantità dei dati che controllano» [25]. La neutralità, invero, mira al rafforzamento del controllo delle parti coinvolte nella *data transaction* sui dati di propria afferenza, specie quando dette parti siano costituite dai soggetti che, oggi, sono posti ai margini della *data economy* (ossia, interessati, imprese individuali e PMI); ciò, in modo da aumentare la fiducia nel *data sharing* intermediato e, dunque, la circolazione dei dati nel mercato interno, agendo contestualmente quale mezzo per realizzare un regime privo di distorsioni della concorrenza [26], prevenendo l'insorgenza nei nascenti mercati dell'infomediazione delle pratiche anticoncorrenziali emerse nella *platform economy* e oggi ampiamente diffuse nei mercati digitali [27].

Dal descritto stringente regime stabilito per la fornitura dei servizi di intermediazione dei dati traspare l'obiettivo del legislatore europeo di isolare tali servizi e segregare il relativo mercato, sulla base, segnatamente, di un approccio uniforme, ossia privo di differenziazioni che tengano conto delle peculiarità proprie delle varie tipologie di servizi di intermediazione dei dati finora emerse nella prassi e, in parte, accolte nel DGA stesso, cooperative di dati incluse (c.d. approccio "*one-size-fits-all*") [28].

---

[24] *Considerando* n. 33 Reg. cit.

[25] *Considerando* n. 2 Reg. cit. In merito, si è parlato del DGA anche come misura di «*de-monopolization of data*» (AA.VV., *Towards a Digital Ecosystem of Trust: Ethical, Legal and Societal Implications*, in *Opinio Juris in Comparatione*, 2021, 1, p. 143 ss.).

[26] *Considerando* nn. 1-3 Reg. UE n. 868/2022.

[27] Su tali profili, cfr. ad es. A. MANTELERO, Big Data*: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, in *Il diritto dell'informazione e dell'informatica*, 2012, 1, p. 135 ss.; P. MANZINI, *Il* Digital Market Act *decodificato*, cit., p. 320 ss.; G. COLANGELO, Big data*, piattaforme digitali e* antitrust, in *Mercato Concorrenza Regole*, 2016, 3, pp. 425-460. Con particolare riguardo alle questioni di protezione dei dati personali, v. ad es. S. RODOTÀ, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Roma-Bari, 2014, p. 27 ss.; F. BRAVO, *Il commercio elettronico di dati personali*, in T. PASQUINO-A. RIZZO-M. TESCARO (a cura di), *Questioni attuali in tema di commercio elettronico*, Napoli, 2020, p. 83 ss.; G. BUTTARELLI, *Le sfide dei "*Big Data*" tra evoluzione tecnologica, etica e interessi collettivi*, in *Gnosis*, 2017, 2, p. 31 ss. Più ampiamente, sulle questioni giuridiche dei mercati dei dati, cfr. V. ZENO-ZENCOVICH, *Do "Data Markets" Exist?*, in *Media Laws*, 2019, 2, pp. 1-17; J. BERGÉ-S.M. GRUMBACH-V. ZENO-ZENCOVICH, *The 'Datasphere', Data Flows beyond Control, and the Challenges for Law and Governance*, in *European Journal of Comparative Law and Governance*, 2018, Vol. 5, n. 2, pp. 144-178; G. RESTA, *Digital Platforms and the Law: Contested Issues*, in *Media Laws*, 2018, 1, pp. 231-248.

[28] Per una panoramica delle tipologie di servizi di *data intermedation* già operanti nel mercato, v. AA.VV., *Mapping the Landscape of Data Intermediaries – Emerging Models for More Inclusive Data Governance*, cit., p. 40 ss.; L. VON DITFURTH, *Datenmärkte, Datenintermediäre und der Data Governance*, cit., p. 142 ss.; M. MICHELI-M. PONTI-M. CRAGLIA-A. BERTI, *Emerging Models of Data*

È questa la "*European way of data governance*", una modalità di *governance* dei dati nuova, offerta mediante i fornitori di servizi di intermediazione di dati, «garantendo una separazione, nell'economia dei dati, tra fornitura, intermediazione e utilizzo dei dati» [29]. A detta separazione a livello oggettivo, attinente al piano delle attività previste nel processo di scambio dei dati, si accompagna un certo distanziamento, sul piano soggettivo, tra gli attori coinvolti in tale processo, elemento che può parimenti intendersi come espressione della neutralità degli intermediari, seppur rispetto alle parti dello scambio e non invece ai dati oggetto della transazione [30].

Governance in the Age of Datafication, cit., p. 7 ss. V. altresì COMMISSIONE EUROPEA, *Impact Assessment on enhancing the use of data in Europe*, Report on Task 1 – Data governance, SMART 2020/694 | D2, 2020, p. 38 ss.

[29] Cfr. *considerando* n. 32 Reg. cit. L'elemento della novità è percepibile considerando le logiche di gestione dei dati sottese ai modelli commerciali che caratterizzano allo stato l'economia dei dati, alle quali si oppone la *data governance* "all'europea", ove i dati, le tecnologie per valorizzarli e i prodotti e i servizi basati sugli stessi sono concentrati in pochi soggetti di grandi dimensioni, che tendono ad esercitare il proprio potere in ogni fase della *data value chain*, secondo logiche che impediscono ai *data suppliers* di mantenere un controllo effettivo sui propri dati e, in ultimo, determinano una distribuzione iniqua dei benefici derivanti dalla loro elaborazione, nonché distorsioni nella concorrenza. In dottrina, è stato sottolineato che «Il modello di gestione europeo dei dati, voluto dal legislatore europeo, prende le distanza dal modello di *business* perseguito dalle c.d. *Big Tech*, caratterizzato dal capitalismo della sorveglianza, ed è orientato sia ad affermare una visione antropocentrica, che porta ad assicurare la tutela della persona e la solidarietà sociale, sia a ristabilire un regime concorrenziale tra le imprese, contrastando il sostanziale oligopolio delle multinazionali nel mercato digitale, favorendo l'emersione di imprese europee di ben più piccole dimensioni» (F. BRAVO, *Le cooperative di dati*, cit. p. 766 ss.). V. anche D. POLETTI, *Gli Intermediari dei dati*, in *EJPLT*, 2022, 1, p. 48; L. PETRONE, *Il mercato digitale europeo e le cooperative di dati*, cit., p. 807 ss. Quella UE è pertanto considerabile, in una certa misura, come una *data governance* "inclusiva", posto che, coerentemente ai valori e ai principi di fondo del diritto eurounitario, promuove un impiego dei dati più equo, nonché una condivisione dei benefici estraibili dagli stessi distribuita tra i vari attori del mercato e la collettività (in merito, v. AA.VV., *Mapping the Landscape of Data Intermediaries – Emerging Models for More Inclusive Data Governance*, cit., p. 18 ss.).

[30] Il DGA, infatti, qualifica i servizi di intermediazione dei dati «specializzati» come «indipendenti» dalle parti della transazione (*considerando* n. 27 Reg. cit.). L'indipendenza degli intermediari dei dati è ravvisata come un potenziale elemento facilitatore dell'emersione di nuovi ecosistemi di dati che siano, a loro volta, indipendenti dagli attori che allo stato detengono un significativo grado di potere di mercato, nonché tale da consentire un accesso non discriminatorio alla *data economy* per le imprese di ogni dimensione, incluso PMI e *start-up* (*Ibidem*). A ogni modo, dal DGA emergono due importanti scostamenti dal requisito dell'indipendenza: oltre alle cooperative di dati (su cui v. *infra*, par. 3), vi sono i servizi offerti verso gli "interessati" di cui all'art. 10, lett. *b*), Reg. cit., rispetto ai quali, conformemente all'art. 12, lett. *m*), Reg. cit., l'intermediario è obbligato ad agire nell'interesse superiore di questi ultimi nel facilitare l'esercizio dei loro diritti.

2.2. I requisiti per la fornitura di servizi a valore aggiunto stabiliti dall'art. 12, lett. *e*), Reg. UE n. 868/2022.

L'art. 12, lett. *e*), Reg. UE n. 868/2022 prevede che i «servizi di intermediazione dei dati possono comprendere l'offerta di strumenti e servizi supplementari specifici ai titolari dei dati o agli interessati allo scopo specifico di facilitare lo scambio dei dati, come la conservazione temporanea, la cura, la conversione, l'anonimizzazione e la pseudonimizzazione, fermo restando che tali strumenti e servizi sono utilizzati solo su richiesta o approvazione esplicita del titolare dei dati o dell'interessato e gli strumenti di terzi offerti in tale contesto non utilizzano i dati per altri scopi».

Per quanto concerne le funzioni perseguite, la disciplina sulla prestazione di servizi a valore aggiunto, che non era prevista nel testo della proposta del DGA, appare giustificata dalla necessità di consentire l'effettivo soddisfacimento dell'obiettivo di promozione dei servizi di intermediazione dei dati ricercato dal regolamento, affinché gli stessi possano rivestire il citato «ruolo essenziale» nel sostenere il *data sharing* [31]. A fronte della rigida disciplina stabilita per la fornitura di tali servizi, infatti, la facoltà di offrire detti strumenti e servizi consente agli intermediari di fruire, entro certi limiti, dei benefici derivanti dall'integrazione verticale, altrimenti esclusi dall'isolamento dei servizi di *data intermediation* discendente dal principio di neutralità, così rendendo maggiormente sostenibile, in termini economici, l'erogazione degli stessi [32].

Rispetto ai medesimi fini promozionali, va altresì considerato che abilitare gli intermediari a fornire servizi aggiuntivi alla pura intermediazione è necessario affinché i *data suppliers* siano incentivati a rivolgersi agli stessi per curare le proprie operazioni di condivisione dei dati. La fornitura integrata di detti strumenti e servizi a opera di soggetti «specializzati» [33], invero, consente a interessati e titolari dei dati di affidarsi a questi ultimi, compensando le loro carenze in termini di conoscenze e competenze, specie di natura tecnica, per quanto concerne le attività complessivamente necessarie per la realizzazione di una *data transaction*, così riducendo i costi dell'operazione [34]. In breve, allo stato attuale la domanda dei servizi di intermediazione dei dati risulterebbe accompagnata da quella di simili servizi di "prevendita" e, dunque, per il successo di mercato dei primi si avrebbe la necessità dei secondi.

La previsione in esame, inoltre, si inserisce coerentemente negli obiettivi di instaurazione di un regime di concorrenza effettiva ricercati dai trattati (art. 3, par. 3,

---

[31] Cfr. *considerando* n. 27 Reg. cit.

[32] Cfr. ad es. H. RICHTER, *Looking at the Data Governance Act and Beyond: How to Better Integrate Data Intermediaries in the Market Order for Data Sharing*, cit., p. 463; AA.VV., *Data Access and Sharing in Germany and in the EU: Towards a Coherent Legal Framework for the Emerging Data Economy. A Legal, Economic and Competition Policy Angle*, cit., p. 286.

[33] Cfr. *Considerando* n. 27 Reg. cit.

[34] Cfr. L. VON DITFURTH, *Datenmärkte, Datenintermediäre und der Data Governance*, cit., p. 396.

TUE; artt. 101 e 102 TFUE): temperando gli obblighi della neutralità, essa riconosce agli intermediari la possibilità di competere sul diverso piano dei servizi a valore aggiunto (ad esempio, in termini di qualità, varietà e innovazione), così accrescendo la concorrenza e i potenziali effetti benefici che ne derivano per il mercato e i clienti finali, consumatori e non [35].

Proseguendo oltre, occorre soffermarsi sui requisiti sostanziali per la fornitura di strumenti e servizi supplementari. La disciplina di cui all'art. 12, lett. *e*), Reg. cit. ne prevede diversi, che è possibile suddividere in due gruppi interconnessi, entrambi, come si vedrà, volti a delimitare il perimetro applicativo dell'eccezione in esame in modo da prevenirne applicazioni che potrebbero risultare in conflitto con gli obiettivi perseguiti dal principio di neutralità [36].

Il primo, riguarda i profili soggettivi dell'offerta dei servizi a valore aggiunto, i quali possono essere prestati *(i)* esclusivamente in favore dei titolari dei dati o degli interessati e *(ii)* su richiesta o approvazione esplicita degli stessi. La limitazione dell'erogabilità dei servizi a valore aggiunto verso i soli *data suppliers* – in contrasto, peraltro, con il correlato *considerando* n. 33 Reg. cit. [37] – nonostante tali servizi possano rispondere anche all'interesse dei *data users* (com'è chiaro anche tenendo conto delle ipotesi esemplificate dalla medesima disposizione) [38], risulta connessa

---

[35] *Ibidem*, pp. 403-404.

[36] L'art. 12, lett. *e*), Reg. cit. apre infatti ad impieghi dei dati oggetto dello scambio che potrebbero risultare in conflitto con il principio di neutralità: la fornitura di servizi diversi da quello di pura intermediazione, come detto, costituisce un incentivo per l'utilizzo dei dati, da parte dell'intermediario, per scopi diversi dal completamento della transazione (ad esempio, analisi di tali dati per migliorare i servizi aggiuntivi), circostanza che indebolirebbe il controllo delle parti sui dati di propria afferenza, così incidendo negativamente sull'obiettivo di aumentare la fiducia nei servizi di *data sharing*; d'altra parte, la fornitura di servizi a valore aggiunto potrebbe entrare in conflitto con gli obiettivi *antitrust* ricercati dal principio citato, presentando il rischio, ad esempio, di produrre effetti di dipendenza ("*lock in*") per i fornitori dei dati e i *data users* che si avvalgono dei servizi di un certo intermediario dei dati; ancora, il fornitore potrebbe essere portato a sfruttare il potere di mercato detenuto rispetto ai servizi aggiuntivi per trasferirlo nel contesto di quelli di intermediazione dei dati. Su questi profili, v. ad es. L. VON DITFURTH, *Datenmärkte, Datenintermediäre und der Data Governance*, cit., p. 398.

[37] Il *considerando* n. 33 del DGA prevede infatti che «I fornitori di servizi di intermediazione dei dati dovrebbero essere in grado di mettere a disposizione dei titolari dei dati, degli interessati *o degli utenti dei dati* strumenti propri o di terzi al fine di agevolare lo scambio di dati (…)» (enfasi aggiunta), benché sempre soltanto «su richiesta esplicita o con l'esplicita approvazione dell'interessato o del titolare dei dati». La direttrice interpretativa offerta da questo *considerando*, in quanto tale privo di valore normativo (cfr. ad es. CGUE, 13 settembre 2018, *C˘eska' pojis˘t˘ovna a.s.*, causa C-287/17, pt. 33), non può comportare un'interpretazione dell'art. 12, lett. *e*), Reg. cit. diversa da quella emergente dal suo tenore letterale, posto che il preambolo di un atto comunitario non può essere fatto valere per derogare alle disposizioni stesse dell'atto di cui trattasi (cfr. ad es. CGUE, 19 novembre 1998, *Nilsson*, causa C-162/97, pt. 54; in senso conforme, CGUE, 12 maggio 2005, *Meta Fackler*, causa C-444/03, pt. 25; CGUE, 26 ottobre 2023, *FT (Copies du dossier me'dical)*, causa C-307/22, pt. 44).

[38] A ogni modo, si noti che la conversione dei dati, pur essendo ricompresa tra i servizi a valore aggiunto indicati nell'art. 12, lett. *e*), Reg. cit., è un'attività oggetto altresì del già richiamato requisito

all'obiettivo di rafforzare il controllo di queste specifiche parti della transazione rispetto ai dati di loro afferenza. Più ampiamente, tale limite appare espressivo delle esigenze riportabili al potenziamento degli interessati ("*data subjects' empowerment*") e alla sovranità dei dati ("*data sovereignity*")[39], nell'ottica di realizzare, nei mercati digitali, una più equa distribuzione del valore estraibile dai dati[40].

In tal senso, come detto, la norma condiziona l'offerta di tali servizi anche a una chiara manifestazione di volontà dei fornitori dei dati, nella forma di una richiesta o di un'approvazione che sia «esplicita»[41].

Il rilievo della volontà dei *data suppliers* nel contesto dei servizi supplementari, a ogni modo, lascia impregiudicata la circostanza che il regime stabilito per la fornitura dei servizi di intermediazione dei dati (art. 12 del DGA), oltre a rispondere all'interesse delle parti della transazione, ha un rilievo pubblicistico, quale disciplina di regolazione (*ex ante*) del mercato soggetta al controllo di apposite autorità competenti[42]. In tal senso, detta disciplina, incluse le disposizioni sui servizi supplementari, resta sottratta all'autonomia privata[43].

Il secondo gruppo di requisiti è invece inerente ai profili "oggettivi" della fattispecie, riguardando caratteristiche e scopo dei servizi e degli strumenti aggiuntivi.

---

di cui alla lett. *d*) del medesimo articolo, la quale prevede che il fornitore dei servizi di intermediazione dei dati possa convertire i dati in specifici formati anche su richiesta dall'utente dei dati. In tal caso, è comunque fatta salva la volontà dei fornitori dei dati, ai quali invero l'intermediario deve consentire di non partecipare alla conversione, a meno che la stessa sia prescritta dal diritto UE.

[39] *Empowerment* e sovranità dei dati sono espressioni talvolta impiegate per indicare la medesima esigenza, ma la prima è utilizzata per lo più con riguardo alle persone fisiche (qualificate, a seconda della prospettiva adottata, come "interessati" o "consumatori"), mentre la seconda – da non confondere con quella, più ampia, di *sovranità digitale* – in modo tale da ricomprendere anche i bisogni di imprese ed altre organizzazioni. Sullo *empowerment* degli interessati tramite il «controllo intermediato», in particolare mediante il paradigma della tutela collettiva nel contesto delle cooperative di dati, v. F. BRAVO, *Le cooperative di dati*, cit., p. 783 ss.; v. altresì D. POLETTI, *Gli intermediari dei dati*, in *EJPLT*, 2022, 1, p. 55-56 e EAD., *Il controllo dell'interessato e la strategia europea sui dati*, in *Osservatorio sulle fonti*, 2023, 2, spec. p. 372 ss.

[40] V. ad es. M. MICHELI-M. PONTI-M. CRAGLIA-A. BERTI, *Emerging Models of Data Governance in the Age of Datafication*, cit., pp. 3 ss. e 8 ss.; G. CAROVANO-M. FINCK, *Regulating Data Intermediaries: The impact of the Data Governance Act on the EU's Data Economy*, cit., pp. 2 e 8.

[41] Per individuare il contenuto del requisito che impone il carattere "esplicito" della richiesta o approvazione, appare utile richiamare le indicazioni fornite dal Comitato europeo per la protezione dei dati nel diverso contesto della normativa sulla *data protection*, segnatamente rispetto al consenso "esplicito" (artt. 9, par. 2, lett. *a*), 22, par. 2, lett. *c*) e 49, par. 1, lett. *a*), Reg. UE n. 679/2016), in base alle quali detto elemento escluderebbe sia i meccanismi basati sul "silenzio-assenso" sia le manifestazioni di volontà esternate in forme diverse dalla dichiarazione espressa (cfr. EDPB, *Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679*, ver. 1.1, 4 maggio 2020, ptt. 91 ss.).

[42] Cfr. L. VON DITFURTH, *Datenmärkte, Datenintermediäre und der Data Governance*, cit., p. 359; AA.VV., *Data Access and Sharing in Germany and in the EU: Towards a coherent legal framework for the emerging data economy*, cit., p. 294 ss.; H. RICHTER, *Looking at the Data Governance Act and Beyond: How to Better Integrate Data Intermediaries in the Market Order for Data Sharing*, cit., p. 467 ss.

[43] V. i riferimenti riportati alla nota che precede.

In merito, occorre anzitutto soffermarsi sulla circostanza che la lett. *e*) dell'art. 12 DGA si riferisca sia a «strumenti» sia a «servizi» supplementari. La differenza tra le due categorie, come rilevabile altresì dal *considerando* n. 33 Reg. cit., consiste in ciò che gli strumenti sono messi direttamente a disposizione di titolari dei dati e interessati, i quali potrebbero pertanto fruirne in autonomia allo scopo, prestabilito dalla norma, di agevolare lo scambio dei dati; i servizi, invece, comportano che sia l'intermediario a compiere materialmente le operazioni in tal senso necessarie [44].

È prevista anche la possibilità per i *providers* di mettere a disposizione «strumenti» offerti da terze parti, purché queste ultime non utilizzino i dati per scopi differenti dalla facilitazione dello scambio, disposizione che estende ai terzi il divieto di utilizzo dei dati di cui all'art. 12, lett. *a*), Reg. cit. altrimenti applicabile al solo intermediario.

In quanto "supplementari" e destinati a facilitare lo scambio, i servizi a valore aggiunto possono essere prestati esclusivamente nel contesto di una più ampia operazione economica avente per oggetto la condivisione dei dati per il tramite dell'intermediario. Ciò comporta l'impossibilità, per il fornitore, di offrire detti servizi in modo isolato, fermo restando l'eventualità contraria, posto che l'erogazione dei servizi aggiuntivi è una mera facoltà per l'intermediario [45].

Va altresì ricordato che, alla luce della disciplina in materia di pratiche leganti (art. 12, lett. *b*), Reg. cit.), all'intermediario è fatto divieto di subordinare le condizioni commerciali per la fornitura dei servizi di intermediazione dei dati al fatto che, per quanto qui interessa, il titolare dei dati utilizzi altri servizi offerti dal medesimo ("*tying*") e, in tal caso, alla misura dell'utilizzo di tali altri servizi ("*bundling*"), ove i "servizi" richiamati da tale previsione includono anche quelli di cui all'art. 12, lett. *e*), Reg. cit. [46].

Circa le caratteristiche, gli strumenti e i servizi previsti dalla disposizione in esame devono essere «specifici», ossia, può ritenersi, individuati secondo un sufficiente grado di determinatezza. Ciò, in modo da far fronte a una duplice necessità, emergente dagli obiettivi di fondo del DGA e dalla stessa previsione oggetto di

---

[44] Cfr. L. VON DITFURTH, *Datenmärkte, Datenintermediäre und der Data Governance*, cit., p. 398.

[45] Questi aspetti, dal punto di vista privatistico, lasciano emergere il rilievo di una fattispecie di collegamento contrattuale tra il contratto, accessorio, avente per oggetto i servizi aggiuntivi e quello, principale, riguardante l'intermediazione nella condivisione dei dati – contratti, entrambi, conclusi tra il *data supplier* e l'intermediario, fermo restando che vi è, poi, l'ulteriore contratto tra il primo e il *data user*, posto che i servizi di intermediazione dei dati devono necessariamente instaurare «rapporti commerciali» tra le parti della transazione di dati (art. 2, n. 11, Reg. cit.).

[46] Il divieto di pratiche leganti è di significativo rilievo in termini di prevenzione di possibili pratiche anticoncorrenziali che potrebbero distorcere la concorrenza nel mercato dell'infomediazione, ove imprese verticalmente integrate, operanti sia in tale mercato sia in altri a valle potrebbero sfruttare il potere di mercato detenuto in questi ultimi per ottenere indebitamente una posizione dominante nel mercato dei servizi di *data intermediation*. Al riguardo, anche il Reg. UE n. 1925/2022 ha introdotto diverse disposizioni in materia di pratiche leganti o "vendite collegate" (v. ad esempio l'art. 5, parr. 4 e 8, Reg. cit.).

analisi: *(i)* garantire l'effettivo rispetto della volontà dei fornitori dei dati, consentendo loro di richiedere o accettare servizi che siano ben definiti e le cui caratteristiche, specie per quanto concerne i trattamenti di dati previsti dal loro impiego, risultino perciò intelligibili, circostanza dalla quale dipende la possibilità per essi di mantenere il controllo sui dati di propria afferenza nello specifico contesto dei servizi a valore aggiunto; *(ii)* abilitare il rispetto del vincolo di scopo (specifico) previsto dalla norma in esame, consistente nella "facilitazione" dello scambio, posto che la fornitura di strumenti e servizi "generici" accrescerebbe i rischi di un loro utilizzo abusivo, per fini diversi da quello prestabilito [47].

2.3. (*segue*) La finalità specifica di facilitazione dello scambio.

Sul piano oggettivo, il requisito centrale dell'art. 12, lett. *e*), Reg. UE n. 868/2022 è quello del vincolo teleologico, tale per cui l'offerta dei servizi a valore aggiunto è legittima soltanto se servente allo «scopo specifico di facilitare lo scambio dei dati». Dalla sua interpretazione, invero, discendono conseguenze rilevanti sul perimetro e le caratteristiche delle attività effettuabili dagli intermediari dei dati, con impatti anche sui possibili modelli commerciali per la fornitura dei servizi di intermediazione dei dati e la loro sostenibilità economica.

Per identificare i contenuti e la portata di tale vincolo occorre comprendere in cosa consista la finalità della "facilitazione" dello scambio dei dati e quale sia il rilievo da attribuire all'aggettivo «specifico» che la contraddistingue.

A tali fini, utili indicazioni emergono dall'elenco esemplificativo degli strumenti e servizi supplementari riportato all'art. 12, lett. *e*), Reg. cit., il quale fa riferimento alla conservazione temporanea, alla cura, alla conversione, all'anonimizzazione e alla pseudonimizzazione dei dati.

Queste attività, anzitutto, lasciano emergere come l'intermediario, nell'esercizio della propria libertà di iniziativa economica, possa offrire anche strumenti e servizi a valore aggiunto che, in virtù delle loro caratteristiche intrinseche, potrebbero ben

---

[47] Il grado di specificità richiesto, alla luce della *ratio* di tale requisito, dipenderà anche dalla tipologia di strumento o servizio offerto: ad esempio, in caso di tecnologie innovative, fondate su algoritmi sofisticati (come quelli di intelligenza artificiale riportabili al *machine learning*), sarà necessario un maggior livello di dettaglio, accompagnato da informazioni adeguate sulla logica di funzionamento di tali algoritmi, onde far salvo il raggiungimento degli scopi poc'anzi citati. In queste ipotesi, potranno assumere rilievo anche gli obblighi di trasparenza previsti dalla normativa in materia di protezione dei dati personali per i trattamenti di tali dati mediante processi decisionali automatizzati (artt. 13, par. 2, lett. *f*), 14, par. 2, lett. *g*) e 22, parr. 3 e 4, Reg. UE n. 679/2016), normativa che, com'è noto, si applica a qualsiasi dato personale trattato in base al DGA e che non è pregiudicata dal medesimo (art. 1, par. 3, Reg. UE n. 868/2022), nonché, se del caso, quelli stabiliti dal regolamento sull'intelligenza artificiale (Reg. UE n. 1689/2024 o "*AI Act*"), come ad esempio gli «obblighi di trasparenza per i fornitori e i *deployers* di determinati sistemi di IA» (art. 50 Reg. cit.). Diversamente, la determinatezza richiesta nell'individuare ed esplicitare la descrizione dei servizi supplementari offerti potrà essere inferiore per servizi di tipo *standard*, connotati dalle comuni caratteristiche di mercato.

essere impiegati per scopi diversi dall'agevolare lo scambio dei dati. La conservazione dei dati, la cura di questi ultimi e le altre attività richiamate, infatti, di per sé possono servire a una pluralità di fini: ciò che rileva, dunque, non sono le caratteristiche "ontologiche" di un certo strumento o servizio, bensì che il medesimo, quando offerto nel contesto della disposizione in esame, sia impiegato solo allo «specifico» scopo di facilitare lo scambio dei dati.

Sul punto, tuttavia, si segnalano interpretazioni della disciplina relativa ai servizi di intermediazione dei dati prevista dal DGA che, facendo leva sul principio di neutralità e sulla separazione tra attività di intermediazione e utilizzo dei dati caratterizzante la citata *data governance* all'europea, tendono ad escludere dai servizi legittimamente erogabili dagli intermediari dei dati quelli, come la *data analytics* o i servizi *data-driven* di altro tipo, aventi di per sé caratteristiche abilitanti forme di valorizzazione dei dati a opera dell'intermediario stesso, ultronee alla mera agevolazione dello scambio e, in particolare, tali da consentire al medesimo di estrarre il contenuto informativo del dato, così incentivandolo ad operare nella *data value chain* [48].

Rispetto ai servizi a valore aggiunto, va poi indagato se gli stessi comprendano esclusivamente quelli "basati sui dati" oppure anche altri di natura differente, come quelli consulenziali, che potrebbero prescindere dal compimento di operazioni sui dati: per detta questione, di particolare interesse per le cooperative di dati, si rinvia al par. 3.3.

Tanto precisato, lo «scopo di facilitare lo scambio dei dati», in linea generale, sembra da riferirsi alle attività funzionali alla condivisione dei dati (la quale, d'altra parte, è la finalità che connota i "servizi di intermediazione dei dati" in base all'art. 2, n. 11, Reg. cit.) [49]: i servizi aggiuntivi, in breve, potrebbero essere prestati solo per agevolare il *data sharing.* In merito, va però rilevato che il riferimento dell'art. 12, lett. *e*), Reg. cit. allo «scambio dei dati» solleva ambiguità, in quanto potrebbe essere inteso come riguardante soltanto talune specifiche forme di condivisione dei dati e non qualsivoglia operazione di fornitura dei dati dall'una all'altra parte della *data transaction* [50].

Le modalità mediante le quali i servizi a valore aggiunto potrebbero facilitare il

---

[48] Cfr. ad es. AA.VV., *Mapping the Landscape of Data Intermediaries – Emerging Models for More Inclusive Data Governance*, cit., pp. 23, 37-38 e 64.

[49] Sul punto, v. V. BELLOMIA, *Articolo 2 – Definizioni*, cit., p. 176 ss.

[50] Va rilevato come l'impiego dell'espressione «scambio» dei dati non sia previsto nella definizione di «condivisione dei dati» (art. 2, n. 10, Reg. cit.), la quale si riferisce alla «fornitura di dati da un interessato o un titolare dei dati a un utente dei dati ai fini dell'utilizzo congiunto o individuale di tali dati, sulla base di accordi volontari o del diritto dell'Unione o nazionale, direttamente o tramite un intermediario (…)». Lo "scambio" dei dati è invece citato in altre disposizioni, tra le quali l'art. 10, lett. *a*), Reg. cit., ove è stabilito che i servizi tra titolari e potenziali utenti dei dati «possono includere *scambi* di dati bilaterali o multilaterali o la creazione di piattaforme o banche dati che consentono lo *scambio* o l'utilizzo congiunto dei dati», disposizione dal quale sembra emergere che lo "scambio" sia soltanto una delle possibili modalità di condivisione dei dati, alternativa allo "utilizzo congiunto".

"*data exchange*" sono molteplici. Anzitutto, rilevano certamente le attività che semplificano lo scambio in termini "materiali" od organizzativi: si consideri, a titolo indicativo, la «conservazione temporanea» dei dati, che rende possibile la condivisione dei dati anche laddove questi ultimi non possano essere oggetto di scambio immediato (ad esempio, per ragioni tecniche oppure contrattuali). La «cura dei dati», inoltre, consente di soddisfare il medesimo fine grazie ad attività che migliorano la qualità dei dati da scambiare (ad esempio, la metadatazione), le quali sono indispensabili per catalogare i dati e consentirne l'agevole reperimento da parte dei potenziali *data users*.

Può inoltre aversi una facilitazione dello scambio dei dati in termini "giuridici", intendendo con ciò che i servizi a valore aggiunto possono includere quelli utili a supportare i fornitori dei dati in attività necessarie per garantire la conformità della transazione di dati all'ordinamento. Ciò, segnatamente, emerge dai richiami alla pseudonimizzazione e all'anonimizzazione, modalità di trattamento di dati personali [51] che possono risultare, a seconda del caso, opportune o necessarie per realizzare la condivisione nel rispetto del quadro normativo sulla protezione e la libera circolazione di tali dati [52]. Simili servizi aggiuntivi, dunque, agevolano lo scambio rendendo più semplice per i *data suppliers* l'esecuzione di adempimenti di natura legale.

Per quanto concerne il requisito della "specificità" dello scopo, soccorre nuovamente l'elenco esemplificativo previsto all'art. 12, lett. *e*), Reg. cit. e, in particolare, il riferimento alla *data curation*. Questa attività comprende operazioni tipicamente svolte ai primi stadi del processo necessario per abilitare la condivisione in-

---

[51] La «pseudonimizzazione» è definita dall'art. 4, n. 5, Reg. UE n. 679/2016 come «il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile». L'anonimizzazione, che non è espressamente definita dalla normativa in materia di protezione e libera circolazione dei dati personali, né da quella sul *free flow* dei dati non personali (Reg. UE n. 1807/2018), può intendersi come il trattamento di dati personali volto a ottenere informazioni non riguardanti una persona fisica identificata o identificabile, in considerazione di tutti i mezzi di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica (cfr. *considerando* n. 26 Reg. UE n. 679/2016), ossia «dati non personali», i quali sono definiti all'art. 2, n. 4, Reg. UE n. 868/2022 per contrasto, come quelli «diversi dai dati personali» (questi ultimi definiti, com'è noto, all'art. 4, n. 1, Reg. UE n. 679/2016).

[52] Ciò potrebbe rendersi necessario, in particolare, in applicazione dei principi applicabili al trattamento di dati personali (art. 5 Reg. UE n. 679/2016), a partire da quelli di necessità, proporzionalità e minimizzazione, così come per adempiere obblighi generali, tra cui quelli di responsabilizzazione, protezione dei dati fin dalla progettazione e per impostazione predefinita, nonché di sicurezza (stabiliti, rispettivamente, agli artt. 24, 25 e 32 Reg. cit.), oppure disposizioni applicabili in settori specifici (su tutti, si pensi ai contenuti dell'obbligo di adozione di «garanzie adeguate» imposto dall'art. 89 Reg. cit. nel contesto dei trattamenti di dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici).

termediata dei dati (si considerino le già citate attività di metadatazione e di realizzazione dei "cataloghi dei dati") e ciò è indice del fatto che il requisito dello scopo «specifico», pur richiedendo un vincolo funzionale, per così dire, "forte", non escluda l'erogazione di servizi tali da semplificare lo scambio in modo soltanto indiretto.

Sul vincolo di scopo, vi è un'altra questione di rilevante impatto: trattasi di comprendere se la facilitazione dello scambio debba intendersi come riferita a specifiche transazioni verso uno o più potenziali utenti dei dati determinati oppure, in alternativa, come requisito che richieda un effetto di agevolazione della condivisione dei dati in "generale", ossia verso qualsivoglia possibile utente dei dati, anche non identificato al momento dell'erogazione del servizio.

Sul punto, l'art. 12, lett. *e*), Reg. cit., letto con i correlati *considerando* nn. 32 e 33, sembra supportare la conclusione circa l'ammissibilità di servizi supplementari aventi lo scopo di facilitare lo scambio dei dati "in generale", soluzione che accresce le prospettive di valorizzazione dei dati anche grazie all'ampliamento della platea di potenziali *data users* che deriverebbe dall'erogazione di tali servizi: sarebbero questi, invero, gli effetti dell'offerta, ad esempio, di strumenti per la cura dei dati, la conversione, la pseudonimizzazione o l'anonimizzazione. Si consideri, in particolare, la *data curation*: quest'ultima, si è detto, può intendersi come l'insieme delle attività volte ad agevolare il riutilizzo dei dati (metadatazione, catalogazione, ecc.), tipicamente svolte in una fase anteriore all'individuazione di un determinato utente dei dati e, di più, proprio per rendere più semplice l'incontro tra l'offerta dei dati messi a disposizione dai fornitori dei dati e la domanda degli utenti dei dati.

D'altra parte, la disposizione in esame, a monte, prevede che i servizi supplementari siano erogabili solo in favore dei fornitori dei dati e su loro richiesta o approvazione: non vi è alcun riferimento a un eventuale assenso degli utenti dei dati né, soprattutto, alla necessaria presenza di questi ultimi; ciò, pertanto, supporta la conclusione circa la possibilità che detti servizi siano prestati anche in fasi prodromiche alla gestione degli aspetti connessi a un certo scambio verso un potenziale utente dei dati determinato.

Tanto chiarito, va altresì rilevato che l'intermediario che intenda implementare servizi a valore aggiunto, in base al citato vincolo di scopo, avrà l'onere di adottare misure di natura giuridica (segnatamente, contrattuale), organizzativa o tecnica atte ad assicurare che lo strumento o il servizio supplementare sia impiegato solo per facilitare lo scambio dei dati, limitando possibili impieghi "abusivi". Il corollario è coerente con l'obbligo dell'intermediario di prevenzione di pratiche fraudolente o abusive in riferimento ai soggetti che richiedono l'accesso tramite i servizi di *data intermediation* (art. 12, lett. *g*), Reg. cit.) e risulta di particolare rilievo nel caso della messa a disposizione di "strumenti" aggiuntivi, i quali, essendo utilizzabili dai *data suppliers* in autonomia, presentano maggiori rischi di "abusi" [53].

[53] Si pensi, ad esempio, a un titolare dei dati che utilizzi un *software* di anonimizzazione dei dati personali integrato in una piattaforma offerta da un fornitore di servizi di intermediazione per ottenere dati anonimi da utilizzare direttamente e non, invece, da scambiare mediante l'intermediario. In simili

3. L'offerta di servizi a valore aggiunto nel contesto delle cooperative di dati.

3.1. Necessità di un'interpretazione del principio di neutralità e della correlata disciplina sui servizi a valore aggiunto coerente con gli obiettivi attribuiti dal DGA ai servizi di cooperative di dati.

In base al Reg. UE n. 868/2022, i «servizi di cooperative di dati» (art. 2, n. 15, Reg. cit.) costituiscono una *species* dei servizi di intermediazione dei dati, connotata dalle peculiarità *(i)* di essere prestati, dal punto di vista soggettivo, da una «struttura organizzativa» composta dagli stessi *data suppliers*, necessariamente rappresentati dagli "interessati" [54] o dai titolari dei dati equiparabili ai singoli individui «in termini di conoscenze in materia di condivisione dei dati» [55], cioè da imprese individuali e PMI [56], nonché, *(ii)* in termini "funzionali", dal fatto che detta struttura è tenuta al perseguimento di taluni «obiettivi principali» predeterminati dal regolamento, che impongono alle *data cooperatives*, in breve, di prestare la propria attività nell'interesse dei loro membri [57].

Per il corretto inquadramento della disciplina sui servizi a valore aggiunto al caso delle cooperative di dati, è bene rilevare come le descritte peculiarità di tali strutture organizzative non risultino del tutto coerenti con il principio di neutralità (art. 12, lett. *a*), Reg. cit.), rispetto al quale, come detto, la disciplina dell'art. 12, lett. *e*), Reg. cit. costituisce un'eccezione.

Nel caso delle cooperative di dati, anzitutto, la neutralità, almeno in parte, appare

---

scenari, una possibile misura potrebbe consistere in una limitazione tecnica atta a impedire al titolare dei dati di scaricare o altrimenti esportare i dati anonimizzati all'esterno della piattaforma per il *data sharing* intermediato, consentendo invece soltanto le operazioni funzionali a realizzare scambi dei dati (anonimizzati) tramite la stessa.

[54] Gli interessati ("*data subjects*") sono le persone fisiche, identificate o identificabili, cui si riferiscono le informazioni oggetto di trattamento, costituenti perciò "dati personali" (art. 4, n. 1, Reg. UE n. 679/2016).

[55] *Considerando* n. 31 Reg. UE n. 868/2022.

[56] Per le definizioni di "imprese individuali" e "PMI", v. COMMISSIONE EUROPEA, *Raccomandazione della Commissione, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese*, G.U. n. L 124 del 20 maggio 2003, pp. 36-41.

[57] Dagli obiettivi stabiliti all'art. 2, n. 15, Reg. cit., considerati nel complesso delle trame del DGA, emerge che le cooperative di dati svolgono una funzione duplice: *(i)* verso l'interno, supportano i propri membri fornendo loro l'assistenza occorrente per rimediare alle asimmetrie di potere informativo sussistenti tra di essi e gli utenti dei dati; *(ii)* verso l'esterno, svolgono una funzione di "raggruppamento" dei propri membri, dunque dei dati di loro afferenza, nei confronti degli utenti dei dati (cfr. L. VON DITFURTH, *Datenmärkte, Datenintermediäre und der Data Governance*, cit., p. 268). Tale schematizzazione rende evidente la centralità della dimensione collettiva in queste organizzazioni, la quale è servente anche alla realizzazione degli obiettivi legali delle stesse, ad esempio aumentandone il potere contrattuale verso i potenziali utenti dei dati (cfr. ad es. AA.VV., *Data Access and Sharing in Germany and in the EU: Towards a coherent legal framework for the emerging data economy*, cit., p. 86).

priva della giustificazione che, invece, ne sorregge l'operatività verso le altre tipologie di servizi di intermediazione dei dati [58]. Con riguardo all'obiettivo di aumentare la fiducia nei servizi di *data sharing* rafforzando il controllo delle parti della transazione sui dati di propria afferenza, dalle due caratteristiche della sostanziale coincidenza tra fornitori dei dati (membri della cooperativa di dati) e cooperativa di dati stessa (quale soggetto composto dai fornitori dei dati) e degli obiettivi prestabiliti dal regolamento per tale intermediario, si avrebbe infatti che le *data transactions* realizzate dalla cooperativa di dati, di regola, realizzerebbero gli interessi sia dei *data suppliers* sia dell'intermediario stesso, così rendendo apparentemente superflua l'applicazione della neutralità come strumento per limitare conflitti di interessi tra intermediario e fornitori dei dati e per garantire il controllo di questi ultimi sui propri dati [59].

Questi elementi, d'altra parte, determinano un certo distacco anche dal paradigma della *European way of data governance*, fondata sulla separazione tra fornitura e intermediazione dei dati, nonché tra fornitori dei dati e intermediario. Tale apparente "anomalia", a ben vedere, può ritenersi giustificata dagli obiettivi "*antitrust*" sottesi al modello delle cooperative di dati fatto proprio dal DGA: le *data cooperatives*, stante le richiamate caratteristiche soggettive e funzionali, risultano strutturate come mezzi per agevolare il superamento delle logiche del capitalismo estrattivo che connotano allo stato i mercati digitali e addivenire a quella «parità di condizioni nell'economia dei dati» [60] tale da abilitare la concorrenza «sulla qualità dei servizi e non sulla quantità dei dati» [61]; ciò, per contribuire al mutamento di paradigma ricercato fin dalla strategia europea per i dati, che realizzi «una società e un'economia dei dati antropocentriche, affidabili e sicure» [62], in linea con l'assiologia e il diritto UE, grazie a una redistribuzione più equa del valore dei dati, idonea a consentire anche alle imprese individuali e alle PMI di prosperare [63].

I servizi di cooperative di dati, inoltre, per come delineati dal DGA (art. 2, n.

---

[58] Il DGA, oltre a stabilire una definizione generale dei servizi di intermediazione dei dati (art. 2, n. 11, Reg. cit.), individua all'art. 10 Reg. cit. tre tipologie di tali servizi (cooperative di dati incluse), la cui fornitura è assoggettata da tale norma alle condizioni stabilite all'art. 12 Reg. cit. e alla procedura di notifica di cui all'art. 11 Reg. cit. Sulla tassonomia dei servizi di intermediazione dei dati accolta dal DGA, v. ad es. G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit., p. 982 ss.; D. POLETTI, *Il quadro normativo del* data governance act*: l'esercizio dei diritti dell'interessato nell'attività di intermediazione dei dati*, in A. MORACE PINELLI (a cura di), *Dalla* Data Protection *alla* Data Governance: *il Regolamento (UE) 2022/868*, cit., p. 73 ss.

[59] Cfr. ad es. L. VON DITFURTH, *Datenmärkte, Datenintermediäre und der Data Governance*, cit., p. 267, ove è evidenziato che le cooperative di dati, diversamente dagli altri fornitori di servizi di *data intermediation*, che non rappresentano gli interessi di una delle parti della transazione di dati, cercano invece di far valere gli interessi dei propri membri nei confronti dei terzi.

[60] Cfr. *considerando* n. 2 Reg. cit.

[61] *Ibidem*.

[62] Cfr. *considerando* n. 3 Reg. cit.

[63] Cfr. *considerando* n. 2 Reg. cit.

15, Reg. cit.), risultano per definizione in attrito con il principio di neutralità: basti considerare che il regolamento impone ai fornitori di tali servizi di perseguire degli obiettivi che richiedono all'intermediario di svolgere delle attività in favore dei propri membri (ad esempio, quelle di supporto nell'esercizio dei diritti sui dati o di negoziazione dei termini di utilizzo dei dati per loro conto) che vanno oltre la pura intermediazione dei dati – intesa, con le parole dell'art. 12, lett. *a*) del DGA, come messa a disposizione dei dati ai *data users* – e che, di conseguenza, confliggono con la neutralità nella dimensione della limitazione dei servizi, *data-based* e non [64].

In breve, le specificità delle cooperative di dati nel modello definito dallo stesso DGA richiedono di riconoscere a queste ultime un'operatività maggiore di quella che si avrebbe sulla base di una lettura delle disposizioni sulla neutralità sciolta dalla considerazione degli obiettivi attribuiti dal regolamento a tali intermediari [65]. Innanzi all'approccio "*one-size-fits-all*" seguito dall'art. 12 Reg. cit., allora, emerge la necessità di interpretare le condizioni cui è assoggettata la fornitura dei servizi di intermediazione dei dati, inclusa la disciplina sull'offerta dei servizi a valore aggiunto, in modo tale da consentire alle cooperative di dati di raggiungere gli obiettivi previsti dal proprio schema legale, così facendo salvo l'effetto utile delle relative disposizioni del *Data Governance Act* [66].

3.2. (*segue*) Il vincolo della "facilitazione dello scambio" inteso alla luce degli obiettivi legali delle cooperative di dati.

Si è già accennato alla centralità del vincolo di scopo (specifico), consistente nel facilitare lo scambio dei dati, nella disciplina sull'offerta dei servizi a valore aggiunto da parte dei fornitori di servizi di intermediazione dei dati. Per l'applicazione di tale regime al caso delle cooperative di dati, a fronte di quanto anticipato poc'anzi, occorre identificare l'interpretazione di tale disposizione che sia coerente con gli obiettivi stabiliti dal regolamento europeo per tali peculiari intermediari.

Al riguardo, benché la riconduzione dei servizi di cooperative di dati al *genus*

---

[64] Sul punto, la circostanza che le attività di supporto ai membri prevedano o meno il compimento di operazioni sui dati da loro forniti è irrilevante, in quanto la neutralità, come descritto *supra* (par. 2.1), esclude la prestazione di qualsiasi servizio diverso da quello che mira alla messa a disposizione dei dati verso i *data users*.

[65] Si consideri altresì che le disposizioni del diritto UE devono essere interpretate tenendo conto non solo della loro formulazione, ma anche del contesto in cui le stesse sono inserite, così come degli obiettivi e delle finalità perseguite dall'atto di cui fanno parte (cfr. ad es., CGUE, 7 marzo 2024, *IAB Europe*, causa C-604/22, pt. 34; CGUE, 22 giugno 2023, *Pankki S*, causa C-579/21, pt. 38; CGUE, 12 gennaio 2023, *Österreichische Post*, causa C-154/21, pt. 29; più lontano nel tempo, v. CGUE, 6 ottobre 1982, *Srl CILFIT and Lanificio di Gavardo SpA v Ministry of Health*, causa C-283/81).

[66] Secondo il criterio interpretativo dell'"effetto utile", com'è noto, tra le varie possibili interpretazioni di una disposizione del diritto UE va privilegiata quella che riconosce alla stessa una maggiore effettività, consentendo di raggiungere in modo più efficace gli obiettivi perseguiti dalla stessa. Sull'effetto utile, v. ad es. I. INGRAVALLO, *L'effetto utile nell'interpretazione del diritto dell'Unione europea*, Bari, 2017.

dei servizi di intermediazione dei dati richieda che le attività svolte dalle stesse siano finalizzate alla condivisione dei dati [67], la quale ha nello scambio dei dati curato dall'intermediario il proprio fulcro, va rilevato che nelle *data cooperatives* l'accento è posto piuttosto sulle modalità mediante le quali tale fine deve essere perseguito [68]. In primo piano, infatti, vi è la necessità per le cooperative di dati di perseguire degli scopi, espressamente qualificati come «principali» (art. 2, n. 15, Reg. cit.), che sono accomunati, in sintesi, dal sottendere lo svolgimento di attività di supporto ai membri della cooperativa nel contesto della condivisione dei dati, la quale, di per sé, è lasciata sullo sfondo. Ciò, affinché le operazioni di *data sharing* siano realizzate in modo rispondente alle specifiche esigenze di interessati, imprese individuali e PMI, soggetti oggi sostanzialmente esclusi dalla valorizzazione dei dati di loro afferenza nel mercato interno, specialmente in ragione delle asimmetrie di potere informativo tra di essi e le *Big Tech*.

L'art. 12, lett. *e*), Reg. cit. deve allora essere interpretato alla luce degli obiettivi prestabiliti dal DGA per le *data cooperatives*, secondo la logica propria di tali intermediari. In tal senso, gli strumenti e i servizi aggiuntivi che le cooperative di dati hanno facoltà di offrire ai propri membri potranno includere anche quelli necessari per «facilitare lo scambio dei dati», segnatamente, in termini tali da consentire a queste strutture organizzative di supportare i propri membri nell'esercizio dei loro diritti o nell'individuazione delle finalità e delle condizioni di impiego dei dati che rendano possibile di realizzarne al meglio gli interessi o di negoziare le condizioni di trattamento nella medesima ottica (art. 2, n. 15, Reg. cit.). Una simile interpretazione si rende necessaria per assicurare alle cooperative di dati la possibilità di raggiungere i loro obiettivi, superando i limiti derivanti da una lettura non sistematica delle disposizioni sulla neutralità.

In questo modo, si abilita altresì l'effettivo raggiungimento degli scopi ultimi ricercati dal regolamento sulla *governance* dei dati con l'introduzione di tali intermediari, relativi, come accennato, alla realizzazione del mutamento di paradigma nell'economia digitale previsto dalla strategia europea per i dati, anche per garantire l'assenza di distorsioni della concorrenza nel mercato interno [69].

Una siffatta perimetrazione dei servizi a valore aggiunto, comprensiva degli strumenti e dei servizi occorrenti per consentire il soddisfacimento degli interessi dei membri della cooperativa nel contesto del *data sharing* intermediato, come desu-

---

[67] La definizione di «servizio di intermediazione dei dati» prevede che sia tale il servizio che mira a instaurare rapporti commerciali «ai fini della condivisione dei dati» tra un numero indeterminato di *data suppliers* e utenti dei dati (art 2, n. 11, Reg. cit.).

[68] Cfr. ad es. L. VON DITFURTH, *Datenmärkte, Datenintermediäre und der Data Governance*, cit., p. 219, ove è indicato che per le cooperative di dati, a differenza dei fornitori di servizi di intermediazione dei dati *b-to-b* (cfr. art. 10, lett. *a*), Reg. cit.), il sostegno allo scambio di dati è uno scopo soltanto secondario, mentre la finalità principale è quella di aiutare i propri membri nelle attività richiamate dall'art. 2, n. 15, Reg. cit.

[69] Cfr. COMMISSIONE EUROPEA, *Una strategia europea per i dati*, cit., p. 5 ss.

mibili dalla stessa definizione dei «servizi di cooperative di dati», appare coerente con la struttura dell'art. 12, lett. *e*), Reg. cit. Tale disposizione, invero, prevede tra i propri elementi essenziali "soggettivi" la limitazione della fornitura dei servizi supplementari al caso in cui gli stessi siano prestati in favore della parte della transazione costituita dagli interessati o dai titolari di dati e che detti servizi siano stati richiesti o approvati da questi ultimi in modo esplicito, con un'impostazione che, come accennato, pare far proprie le esigenze riportabili al *data subjects' empowerment* e alla *data sovereignty*, con ogni evidenza sottese anche al modello di cooperative di dati fatto proprio dal *Data Governance Act*.

Esemplificando questa impostazione, le cooperative di dati, rispettando tutti i requisiti previsti dall'art. 12, lett. *e*), Reg. cit. e da ogni altra disposizione rilevante, nel perseguimento dell'obiettivo di aiutare i propri membri a compiere scelte informate prima di acconsentire al trattamento, potrebbero implementare, a titolo indicativo, strumenti *software* basati su algoritmi sofisticati per la lettura automatizzata dei termini di utilizzo dei dati proposti dai potenziali *data users* e la relativa individuazione di possibili clausole che prevedano operazioni di trattamento dei dati contrastanti con gli interessi dei membri, così facilitando lo scambio dei dati di questi ultimi secondo la precipua logica delle cooperative di dati [70]. Ancora, si pensi all'implementazione di *Personal Information Management Systems* ("PIMS") [71], rispetto all'obiettivo di supportare i membri nell'esercizio dei loro diritti sui dati, modalità che parimenti potrebbero agevolare il *data sharing* intermediato coerentemente alle specifiche esigenze di tutela sottese alle cooperative di dati.

3.3. I servizi a valore aggiunto come mezzi per il conseguimento degli "obiettivi principali" delle cooperative di dati, tramite attività basate sui dati e non.

Si è detto che, ai fini del perseguimento degli obiettivi principali loro attribuiti dal Reg. UE n. 868/2022, le cooperative di dati hanno necessità di svolgere attività

---

[70] Si pensi, ad esempio, al *software* basato su algoritmi di *machine learning* denominato "Claudette", il quale consente l'analisi automatizzata dei termini di utilizzo e delle informative sul trattamento dei dati personali per individuare possibili clausole abusive (Dir. 93/13/CEE) o in contrasto con le disposizioni del Reg. UE n. 679/2016. In merito, v. ad es. F. LAGIOIA-A. JABŁONOWSKA-R. LIEPINA-K. DRAZEWSK, *AI in Search of Unfairness in Consumer Contracts: the Terms of Service Landscape*, in *Journal of Consumer Policy*, 2022, Vol. 45, pp. 481-536; AA.VV., *CLAUDETTE meets GDPR: Automating the Evaluation of Privacy Policies using Artificial Intelligence*, Study Report, Funded by the European Consumer Organisation (BEUC), 2018.

[71] Sull'implementazione dei PIMS nel contesto dei servizi di intermediazione dei dati, v. F. BRAVO, *Intermediazione di dati personali e servizi di* data sharing *dal GDPR al* Data Governance Act, in *Contratto e impresa Europa*, 2021, 1, p. 254 ss., il quale sul punto richiama altresì le indicazioni fornite dal Garante europeo per la protezione dei dati (EDPS, EDPS, *Opinion No. 3/2020 on the European strategy for data*, 16 June 2020, p. 6 ss.; v. anche EDPS, *Opinion 9/2016 on Personal Information Management Systems*, 20 October 2016).

non limitate alla mera messa a disposizione dei dati verso gli utenti dei dati e che, sotto tale profilo, il modello di *data cooperatives* fatto proprio dal DGA appare confliggere con il principio di neutralità, inteso in particolare come limitazione dei servizi erogabili dall'intermediario. Occorre ora approfondire questo passaggio, per comprendere se ed entro quali limiti tali attività possano essere collocate entro la disciplina dei servizi a valore aggiunto di cui all'art. 12, lett. *e*), Reg. cit.

Sul punto, è bene premettere che le attività che le cooperative di dati hanno necessità di porre in essere nel perseguimento dei citati obiettivi possono essere di varia natura. Il distinguo maggiormente significativo, in questa sede, è tra quelle che non comportano il compimento di operazioni sui dati forniti dai membri e le attività *data-based*: le prime, possono riportarsi ad attività di natura latamente consulenziale [72] o assistenziale [73], mentre le seconde, tipicamente, prevedono l'elaborazione dei dati forniti dai membri mediante l'utilizzo di sistemi informatici [74].

La riconduzione di strumenti e servizi *data-based* all'art. 12, lett. *e*), Reg. cit. non appare complessa, posto che è proprio l'elenco esemplificativo previsto da tale norma a comprendere servizi di tal fatta.

È piuttosto la collocazione, entro tale disciplina, delle attività di altra natura a presentare delle criticità. La disciplina dell'art. 12, lett. *e*), Reg. cit., infatti, potrebbe intendersi come riferita esclusivamente alla prestazione di strumenti e servizi basati sui dati e ciò renderebbe problematica l'individuazione di una "base giuridica" nel DGA legittimante la prestazione di servizi di natura consulenziale o assistenziale da parte delle *data cooperatives* e, con ciò, la possibilità per tali organizzazioni di raggiungere gli obiettivi previsti dal proprio schema legale. Questa criticità, in particolare, si avrebbe per i soli servizi di tal fatta diversi da quelli che consistono in attività di informazione o consulenza «sugli utilizzi previsti dei dati da parte degli utenti dei dati e sui termini e le condizioni *standard* cui sono subordinati tali utilizzi», i quali, invece, per le cooperative di dati costituite da interessati trovano il proprio fondamento nel dovere dell'intermediario di agire nell'interesse superiore dei *data subjects* (art. 12, lett. *m*), Reg. UE n. 868/2022) [75].

---

[72] Si pensi, ad esempio, alle attività svolte dalle cooperative di dati per aiutare i propri membri, affinché possano compiere scelte informate prima di acconsentire al trattamento dei loro dati, oppure a quelle volte a stimolare una proficua dialettica interna tra i membri, in modo da abilitare uno scambio di opinioni sulle finalità e le condizioni del trattamento che rappresenterebbero al meglio gli interessi degli stessi rispetto ai loro dati (art. 2, n. 15, Reg. cit.).

[73] Sarebbe questo il caso della negoziazione dei termini e condizioni per il trattamento dei dati svolto dalle cooperative di dati per conto dei membri, prima di concedere l'autorizzazione al trattamento dei dati non personali o che essi diano il loro consenso al trattamento dei dati personali (art. 2, n. 15. Reg. cit.).

[74] Si considerino le attività esemplificate all'art. 12, lett. *e*), Reg. cit., nonché quelle prestate nel contesto di servizi *data-driven* (ad esempio, l'analisi dei dati).

[75] In tal caso, vi è un precipuo obbligo per i fornitori di servizi di intermediazione dei dati che offrono i propri servizi a tali categorie di *data suppliers* di fornire attività di informazione e consulenza nel facilitare l'esercizio dei loro diritti (cfr. altresì il *considerando* n. 30 Reg. cit.). Dette attività, se

Tanto precisato, la tesi che esclude dalla disciplina dei servizi supplementari quelli che non prevedano un'operatività sui dati si fonderebbe proprio sulle richiamate tipologie di attività esemplificate dall'art. 12, lett. *e*) del DGA (come detto, la conservazione temporanea, la cura, la conversione, l'anonimizzazione e la pseudonimizzazione dei dati), riguardanti infatti esclusivamente servizi *data-based*[76]; in aggiunta, vi sarebbe la precisazione contenuta in tale norma relativamente agli strumenti di terzi, i quali «non utilizzano i dati per altri scopi» e che, perciò, implicherebbero un'operatività sui dati.

A ogni modo, a ben vedere le suddette argomentazioni non appaiono tali da escludere la collocazione, entro l'art. 12, lett. *e*), Reg. cit., dell'offerta di strumenti e servizi non aventi per oggetto i dati forniti dai membri della cooperativa di dati.

Anzitutto, va rilevato che la tesi richiamata non trova riscontro negli elementi essenziali della disciplina, ma solo in disposizioni avente carattere esemplificativo. Si consideri, in particolare, l'elemento centrale del regime relativo ai servizi a valore aggiunto, rappresentato dal vincolo di scopo: al riguardo, per quanto finora rilevato, è manifesto che i servizi che non comportino operazioni sui dati possano comunque essere utili, se non indispensabili, per facilitare lo scambio dei dati; ciò, specie nelle cooperative di dati, ove tale facilitazione dovrebbe intendersi, come accennato, secondo la logica di supporto ai membri che informa tale peculiare intermediario. Ancora, per quanto concerne i requisiti soggettivi di tale disposizione, dalla circostanza che i servizi supplementari siano erogabili esclusivamente su richiesta o approvazione esplicita dei soli *data suppliers*, prevista a loro maggiore garanzia, non potrebbe desumersi che tale norma si applichi ai soli servizi basati sui dati, in quanto la fornitura di servizi di altra natura potrebbe ugualmente ledere l'interesse di tali soggetti a mantenere un effettivo controllo sui dati di propria afferenza. In merito, basti considerare che la presenza di qualsivoglia servizio aggiuntivo a quelli di pura intermediazione dei dati rappresenta, per l'intermediario, un incentivo al "*cross-use*" dei dati, fenomeno che impatta negativamente sull'inte-

necessarie per l'adempimento di tale obbligo, si collocheranno pertanto al di fuori della disciplina sui servizi a valore aggiunto e, perciò, potranno (*rectius*, dovranno) essere prestate anche in assenza dei requisiti previsti dall'art. 12, lett. *e*), Reg. cit. Sull'obbligo dell'intermediario di agire nel superiore interesse dei *data subjects*, con speciale riguardo alla questione della possibilità di delegare l'esercizio dei diritti dell'interessato, v. D. POLETTI, *Il quadro normativo del* data governance act*: l'esercizio dei diritti dell'interessato nell'attività di intermediazione dei dati*, cit., p. 73 ss.

[76] Cfr. L. VON DITFURTH, *Datenmärkte, Datenintermediäre und der Data Governance*, cit., p. 402, secondo il quale, più in particolare, la norma in esame, alla luce del vincolo di scopo della facilitazione dello scambio, riguarderebbe soltanto gli strumenti e i servizi volti a consentire l'implementazione "tecnica" del trasferimento dei dati, non potendo dunque includere le attività di assistenza relative alla struttura legale delle transazioni di dati. Tale posizione non risulta condivisibile, posto che lo stesso elenco esemplificativo previsto dalla disposizione in questione fa riferimento ad attività che non sono rilevanti in termini di implementazione tecnica del trasferimento, ma sotto altri profili (si pensi alla pseudonimizzazione o all'anonimizzazione, le quali, come rilevato *supra*, al par. 2.2, mirano piuttosto a facilitare lo scambio in termini "giuridici", semplificando gli adempimenti di *compliance* alla normativa sulla protezione dei dati personali).

resse dei fornitori dei dati a governare il flusso dei dati di propria afferenza; la presenza del citato requisito soggettivo, dunque, si giustifica anche in riferimento ai servizi che non siano basati sull'impiego dei dati [77].

Posto che la norma in esame afferisce al principio di neutralità, atteggiandosi come eccezione al medesimo, su questi profili è bene considerare anche il piano degli interessi protetti da tale principio, il quale, come detto, ha la funzione, da un lato, di rafforzare il controllo dei *data suppliers* sui loro dati, così aumentandone la fiducia nel *data sharing* intermediato, e dall'altro di tutelare la concorrenza nei mercati digitali [78]. Ebbene, l'integrazione di strumenti e servizi non basati sui dati nel contesto di un servizio di intermediazione dei dati presenta senz'altro delle criticità rispetto agli interessi sottesi a tali funzioni, ma dette criticità si rinvengono ugualmente in riferimento all'integrazione di strumenti e servizi *data-based*. Di più: questi ultimi consentono all'intermediario di impiegare *direttamente* i dati oggetto dello scambio in attività diverse dalla pura intermediazione e, perciò, potenzialmente pongono criticità di maggior intensità rispetto alle richiamate funzioni del principio di neutralità. In breve, se detta norma comprende la prestazione di servizi basati sui dati, a maggior ragione, allora, la stessa abilita le cooperative di dati a offrire strumenti e servizi che, come quelli di consulenza o assistenza, presentano rischi inferiori per gli interessi dei fornitori dei dati e quelli sottesi al DGA come mezzo di regolazione del mercato.

L'interpretazione dell'art. 12, lett. *e*), Reg. cit. tale da ricomprendere anche i servizi di questa natura appare pertanto coerente, a livello sistematico, con gli obiet-

---

[77] A limitare il fenomeno dell'utilizzo incrociato dei dati, nel *Data Governance Act* vi è anzitutto il principio di neutralità come limitazione dei servizi erogabili dall'intermediario, il quale, a fronte del descritto requisito di "separazione soggettiva", che impone la fornitura dei servizi di *data intermediation* mediante una persona giuridica distinta, vieta la prestazione a opera dell'intermediario di qualsivoglia servizio diverso da quelli di intermediazione dei dati, sia esso basato sui dati o meno (art. 12, lett. *a*), Reg. cit.). Sulla disposizione da ultimo richiamata come mezzo per prevenire il fenomeno del *cross-use* dei dati, cfr. ad es. AA.VV., *White Paper on the Data Governance Act*, cit., p. 33 ss.; H. RICHTER, *Looking at the Data Governance Act and Beyond: How to Better Integrate Data Intermediaries in the Market Order for Data Sharing*, cit., p. 463. Com'è noto, le misure adottate dall'UE per limitare l'utilizzo incrociato dei dati si rinvengono anche in altri atti legislativi, tra i quali, ad esempio, il Reg. UE n. 1925/2022, ove sono stabilite tra gli obblighi imposti ai *gatekeeper* per prevenire le pratiche sleali o che limitano la contendibilità dei mercati (cfr. art. 5, par. 1, lett. *b*)-*d*), Reg. cit.). Su questi ultimi profili, per quanto concerne gli aspetti di diritto della concorrenza, cfr. P. MANZINI, *Il* Digital Market Act *decodificato*, cit., p. 328 ss., ove le disposizioni sull'uso combinato dei dati sono inquadrate nella categoria generale del diritto *antitrust* delle pratiche di sfruttamento di cui all'art. 102 TFUE. Su punti di contatto e differenze tra DGA e DMA v. H. RICHTER, *Looking at the Data Governance Act and Beyond: How to Better Integrate Data Intermediaries in the Market Order for Data Sharing*, cit., p. 463.

[78] Rispetto alla neutralità come mezzo di tutela della concorrenza nel mercato interno, in particolare nella dimensione della limitazione dei servizi, cfr. L. VON DITFURTH-G. LIENEMANN, *The Data Governance Act: – Promoting or Restricting Data Intermediaries?*, p. 278 ss; AA.VV., *White Paper on the Data Governance Act*, cit., p. 32 ss.

tivi del principio di neutralità, così come con la necessità di interpretare tale disposizione, quale eccezione a detto principio, senza ricorrere all'analogia. Ciò, come detto, posto anche che la tesi che esclude detti servizi dall'ambito applicativo della norma in esame si fonda su elementi non essenziali della disciplina dei servizi a valore aggiunto, previsti in via meramente esemplificativa.

In tal senso, le cooperative di dati potranno conseguire i propri obiettivi principali di cui all'art. 2, n. 15, Reg. cit. mediante l'offerta di strumenti e servizi, *data-based* e non, offerti ai propri membri come servizi a valore aggiunto in piena coerenza con i limiti delle disposizioni del regolamento sulla neutralità degli intermediari riguardo ai dati scambiati.

3.4. Strumenti e servizi per la realizzazione di *data pools* nel contesto delle cooperative di dati.

La condivisione dei dati tramite creazione di un "*pool*" di dati (o "*data pool*")[79], ossia mediante messa in comune dei dati, emerge dalla prassi e dalla letteratura come uno dei principali tratti caratterizzanti le cooperative di dati[80], il quale consente loro di massimizzare il valore estraibile dai dati forniti dei membri coerentemente alla natura collettiva e relazionale di tali organizzazioni.

---

[79] Per un inquadramento giuridico dei *data pools*, v. A. OTTOLIA, Big Data *e innovazione computazionale*, Torino, 2017, p. 271 ss.

[80] In merito, v. ad es. AA.VV., *Data Access and Sharing in Germany and in the EU: Towards a coherent legal framework for the emerging data economy*, cit., p. 86 (ove è evidenziato che la condivisione svolta dai membri tramite il *pooling* dei propri dati è il tratto principale delle *data cooperatives*); AA.VV., *White Paper on the Data Governance Act*, cit., p. 29, ove è indicato che «*the concept [of data cooperatives] refers to entities established to facilitate the collaborative pooling of data by individuals or organisations for their mutual economic, social or cultural benefit*», richiamando gli esempi emersi nella prassi delle cooperative MiData, SalusCoop, Holland Health Data Cooperative e The Good Data Cooperative; T. HARDJONO-A. PENTLAND, *Data Cooperatives: Towards a Foundation for Decentralized Personal Data Management*, cit., ove a p. 2 si legge che «*The notion of a data cooperative refers to the voluntary collaborative pooling by individuals of their personal data for the benefit of the membership of the group or community*»; AA.VV., *Mapping the Landscape of Data Intermediaries – Emerging Models for More Inclusive Data Governance*, cit., pp. 43 (in cui, come fattori distintivi delle cooperative di dati, sono indicati questi tratti: «*Based on democratic principles through the production and management of common pools of data*»), 47 e 50; E. BIETTI-A. ETXEBERRIA ET AL., *Data Cooperatives in Europe: A Legal and Empirical Investigation*, cit., p. 9, nel quale il *pooling* è ravvisato come l'aspetto caratterizzante di almeno uno dei due modelli di cooperative di dati emergenti dalla prassi (in particolare, di quello fondato sull'"approccio collettivo"). Ciò detto, va comunque rilevato che il *data pooling* risulta implementato anche in tipologie di intermediari dei dati diverse dalle cooperative di dati, come ad esempio nelle "*data sharing pools*" (cfr. AA.VV., *Data Access and Sharing in Germany and in the EU: Towards a Coherent Legal Framework for the Emerging Data Economy*, cit., p. 84 ss.; AA.VV., *Mapping the Landscape of Data Intermediaries – Emerging Models for More Inclusive Data Governance*, cit., p. 40 ss.) o nelle "*data unions*" (*Ibidem*, p. 54 ss.).

Oltre ad abilitare un'agevole condivisione dei dati tra i membri del *pool*[81], la messa in comune dei dati facilita il raggiungimento degli «obiettivi principali» affidati alle cooperative di dati dal DGA, afferenti al *data sharing* verso utenti dei dati esterni all'organizzazione, così risultando particolarmente rispondente al modello di *data cooperatives* fatto proprio dal regolamento. Ciò, in quanto tali modalità aumentano significativamente la capacità della cooperativa di dati di supportare i propri membri nelle attività necessarie al perseguimento di questi obiettivi, ad esempio grazie all'incremento del potere contrattuale verso gli utenti dei dati discendente dalla possibilità di offrire loro *dataset* costituiti da dati provenienti da una molteplicità di fonti diverse[82], i quali peraltro sono di maggior interesse per i *data users*[83]. I vantaggi offerti dalla messa in comune dei dati, sotto questo profilo, derivano altresì dalla possibilità di implementare servizi a valore aggiunto sullo stesso *dataset* "integrato", in modo da aumentare le potenzialità di valorizzazione del medesimo[84].

Alla base della creazione dei *pool* di dati nel contesto dei servizi di intermedia-

---

[81] La possibilità per le cooperative di dati previste dal DGA di provvedere al *data sharing* "interno", ossia tra i membri stessi della cooperativa, secondo il modello "*Member-to-Member*" o "*intra-cooperative*" (cfr. F. BRAVO, *Le cooperative di dati*, cit., p. 769), potrebbe ritenersi dubbia, in quanto gli obiettivi principali attribuiti dall'art. 2, n. 15, Reg. cit. a tale intermediario sembrano riferiti esclusivamente a forme di condivisione con utenti dei dati esterni all'organizzazione, sul presupposto dell'esistenza di un *gap* di potere informativo tra i membri della cooperativa e le imprese dei mercati digitali, che le *data cooperatives*, appunto, sono chiamate a colmare tramite la loro attività di supporto dei membri. Nella presente sede, non è possibile approfondire questa tematica: basti segnalare che, da ultimo, il DGA non parrebbe escludere il *data sharing* tra i membri; ciò, in sintesi, in quanto gli obiettivi di tali organizzazioni richiamati dall'art. 2, n. 15, Reg. cit. sono espressamente qualificati come «principali», circostanza tale da non pregiudicare la realizzazione di tali forme di condivisione nel perseguimento di obiettivi "secondari".

[82] In merito, cfr. ad es. AA.VV., *Data Access and Sharing in Germany and in the EU: Towards a Coherent Legal Framework for the Emerging Data Economy*, cit., spec. p. 86, ove è così indicato: «*Members of individual cooperatives benefit by pooling their data, which among other advantages, gives the collective a better negotiating position vis-a-vis external parties*».

[83] Cfr. AA.VV., *Mapping the Landscape of Data Intermediaries – Emerging Models for More Inclusive Data Governance*, cit., p. 36.

[84] Si pensi, su tutti, ai servizi di *data analytics*, necessari per porre la cooperativa di dati nelle condizioni di perseguire adeguatamente i propri obiettivi, come nel caso dell'analisi dei dati prodromica alla gestione delle negoziazioni con gli utenti dei dati, oppure a quella occorrente per individuare le finalità e le condizioni del trattamento che «rappresenterebbero al meglio gli interessi dei propri membri in relazione ai loro dati» (art. 2, n. 15, Reg. cit.). In questa sede, non è possibile approfondire la questione circa la legittimità della prestazione di servizi di analisi dei dati a opera dei fornitori di servizi di intermediazione dei dati, cooperative di dati incluse, la quale è dibattuta in dottrina e, tendenzialmente, esclusa, specialmente in ragione delle disposizioni sulla neutralità degli intermediari dei dati (cfr. ad es. G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit. p. 993; L. PETRONE, *Il mercato digitale europeo e le cooperative di dati*, cit., p. 815; G. CAROVANO-M. FINCK, *Regulating Data Intermediaries: The impact of the Data Governance Act on the EU's Data Economy*, cit., p. 8).

zione dei dati vi è la fornitura, a opera dell'intermediario, di strumenti o servizi che abilitino l'"integrazione" dei dati (in questa sede, intesa come messa in comune degli stessi), e la loro successiva conservazione in questa forma: in tal senso, occorre chiedersi se dette modalità possano essere legittimamente implementate dalle cooperative di dati, in particolare come servizi a valore aggiunto ai sensi dell'art. 12, lett. *e*), Reg. cit.

Il *data pooling*, invero, non costituendo un'attività essenziale per la realizzazione delle operazioni di messa a disposizione dei dati verso i *data users* [85], parrebbe doversi riportare entro il perimetro di tale disposizione, a fronte della "granularità" dei servizi supplementari emergente dalla stessa: basti considerare che, tra questi, è richiamata anche la "conservazione temporanea", per comprendere come qualsiasi operazione sui dati non strettamente necessaria a realizzarne la citata messa a disposizione ricada necessariamente nello spettro applicativo di tale norma [86].

Ciò precisato, va anzitutto rilevato come l'offerta di strumenti e servizi di "integrazione" dei dati risulti connaturata alle cooperative di dati, le quali, come accennato, svolgono una funzione di raggruppamento dei membri, dunque dei dati di loro afferenza, verso i potenziali utenti dei dati, elemento che, peraltro, è alla base della stessa sostenibilità di tale intermediario, posto che è proprio in ragione di tale funzione che gli utenti dei dati hanno interesse a instaurare rapporti commerciali con i *data suppliers* per il tramite della cooperativa di dati [87].

Proseguendo oltre, per quanto concerne la conservazione dei dati, si è detto che la stessa risulta prevista nello stesso elenco esemplificativo riportato alla disposizione in esame, seppur soltanto come conservazione "temporanea". Quest'ultimo requisito, *prima facie* potrebbe sollevare perplessità circa la legittimità della realizzazione di *data pools* nel contesto di una cooperativa di dati, la quale infatti implica una conservazione dei dati caratterizzata da una certa stabilità. A ogni modo, non paiono esservi dubbi circa l'ammissibilità della creazione di *pool* di dati funzionali alla condivisione degli stessi da parte dei fornitori di servizi di intermediazione dei dati, cooperative di dati incluse, disciplinati dal DGA: è proprio detto re-

---

[85] Una cooperativa di dati, ad esempio, potrebbe consentire lo scambio di dati afferenti a un gruppo di propri membri verso un certo utente dei dati anche senza provvedere preventivamente alla loro messa in comune.

[86] In merito, è stato evidenziato che l'art. 12, lett. *e*), Reg. cit. si applicherebbe a tutti gli strumenti e servizi diversi da quelli funzionali a mettere direttamente i dati a disposizione dei *data users*, non essendo destinati esclusivamente all'elaborazione tecnica della transazione di dati (cfr. L. VON DITFURTH, *Datenmärkte, Datenintermediäre und der Data Governance*, cit., p. 398).

[87] Al riguardo, più in generale l'interesse degli utenti dei dati è infatti normalmente rivolto verso i *dataset* risultanti dall'integrazione dei dati provenienti da più fonti, posto che le banche di dati aggregate sono soggette agli effetti positivi delle economie sia di scala (*dataset* con più *record*) sia di scopo (*dataset* con più variabili relative ai medesimi *record*) e che, in tali casi, la "proposta di valore" dell'intermediario dei dati consiste precipuamente nell'offrire *dataset* che siano integrati (cfr. AA.VV., *Mapping the Landscape of Data Intermediaries – Emerging Models for More Inclusive Data Governance*, cit., p. 36 e riferimenti bibliografici ivi riportati).

golamento, infatti, a contenere plurimi riferimenti alla possibilità di realizzare *data pools* nel contesto di tali servizi.

Il *data pooling*, anzitutto, è richiamato nel preambolo del regolamento, che è l'unica sede ove risulta espressamente citato [88]. In riferimento ai servizi di intermediazione dei dati, al *considerando* n. 27 Reg. cit., sottolineato il «ruolo essenziale» di tali servizi nella *data economy* e che gli stessi potrebbero diventare mezzi che «agevolano lo scambio di quantità considerevoli di dati», è indicato che «I fornitori di servizi di intermediazione dei dati (…) che offrono servizi che collegano i diversi soggetti dispongono del potenziale per contribuire alla *messa in comune efficiente dei dati* come pure all'agevolazione della condivisione bilaterale dei dati» (enfasi aggiunta). A seguire, nel *considerando* n. 28 Reg. cit. il *data pooling* è individuato come un esempio di servizio di intermediazione dei dati: accanto ai mercati dei dati e agli orchestratori di ecosistemi di *data sharing* aperti a tutte le parti interessate, sono infatti richiamati i «*pool* di dati creati congiuntamente da più persone fisiche o giuridiche con l'intento di concedere licenze per il loro uso a tutte le parti interessate in modo che tutti i partecipanti che contribuiscono al *pool* siano ricompensati per il loro contributo», quali servizi funzionali, pertanto, al *data sharing* "esterno" al *pool* [89].

La messa in comune dei dati, seppur non espressamente citata, è ravvisabile altresì nell'articolato del Reg. UE n. 868/2022. Il *data pooling* è da considerarsi come una delle possibili modalità tramite la quale realizzare la «condivisione dei dati» [90], ossia la «fornitura dei dati di un interessato o un titolare dei dati a un utente

---

[88] Nella versione in lingua italiana del Reg. UE n. 868/2022 si fa riferimento ai "*pool* di dati" oppure al *pooling* come "messa in comune dei dati", in particolare nei *considerando* nn. 2 (ove è richiamata la strategia europea per i dati, la quale ha proposto di istituire spazi comuni europei di dati per dominio, «per la condivisione e la messa in comune dei dati»), 27-28 (relativamente ai servizi di intermediazione dei dati e su cui si v. *infra*) e 45-46 (nel contesto dell'altruismo dei dati) Reg. cit.

[89] Sul rilievo del *data pooling* previsto da tale *considerando* rispetto alle cooperative di dati, v. G. CAROVANO-M. FINCK, *Regulating Data Intermediaries: The impact of the Data Governance Act on the EU's data economy*, cit., p. 3. Più ampiamente, sulla circostanza che i citati *considerando* nn. 27 e 28 Reg. cit. si riferiscano alla possibilità, per gli intermediari dei dati, di effettuare il *data pooling*, cfr. Y.A. VOGEL, *Stretching the Limit, the Functioning of the GDPR's Notion of Consent in the Context of Data Intermediary Services*, in *EDPL*, 2022, 8(2), p. 242 ss., ove il *data pooling* è accostato alla condivisione dei dati "multilaterale".

[90] Seppure afferente a un diverso contesto, si consideri in merito anche quanto rilevato dalla Commissione europea nell'allegato alla comunicazione sulle linee guida relative all'applicabilità dell'art. 101 TFUE agli accordi di cooperazione orizzontali, ove rispetto al *data pooling b-to-b* è così indicato: «Il termine "condivisione dei dati" è utilizzato per descrivere tutte le forme e i modelli possibili su cui si basano l'accesso ai dati e il loro trasferimento tra imprese. Comprende i *pool* di dati nel contesto dei quali i titolari dei dati si riuniscono per condividere le risorse di dati» (Comunicazione della Commissione – *Linee direttrici sull'applicabilità dell'articolo 101 del trattato sul funzionamento dell'Unione europea agli accordi di cooperazione orizzontale*, *GUUE* del 21.07.2023, C 259/1, nota n. 228). V. altresì B. CARBALLA-SMICHOWSKI-N. DUCH-BROWN-B. MARTENS, *To Pool or to Pull Back? An Economic Analysis of Health Data Pooling*, in *JRC Digital Economy Working Paper* 2021-06,

dei dati ai fini dell'utilizzo congiunto o individuale di tali dati» [91]. In aggiunta, lo stesso appare contemplato nel contesto della tassonomia dei servizi di intermediazione dei dati prevista dal DGA, in particolare rispetto al "tipo" di servizio relativo al *data sharing* tra titolari dei dati e utenti dei dati (art. 10, lett. *a*), Reg. cit.) [92]: in questa disposizione, infatti, si legge che i servizi di tal fatta «possono includere scambi di dati bilaterali o multilaterali o la creazione di piattaforme o banche dati che consentono lo scambio o l'utilizzo congiunto dei dati, nonché l'istituzione di altra infrastruttura specifica per l'interconnessione di titolari dei dati con gli utenti dei dati».

Al riguardo, la circostanza che la messa in comune dei dati sia ravvisabile solo all'art. 10, lett. *a*), Reg. cit. e non anche rispetto alle cooperative di dati (lett. *c*) della medesima norma) non sembra impedire l'implementazione della stessa nel contesto di tali organizzazioni, essendo le richiamate disposizioni dell'art. 10, lett. *a*), Reg. cit. meramente illustrative delle modalità tecnico-organizzative di *data sharing* che possono essere "incluse" nella fornitura dei servizi di intermediazione dei

---

JRC126961, 2021, p. 3, ove il *data pooling* è definito come una forma di *data sharing* multilaterale nella quale più soggetti condividono i propri dati reciprocamente. La messa in comune dei dati è ricondotta al *data sharing* anche in L. VON DITFURTH, *Datenmärkte, Datenintermediäre und der Data Governance*, cit., p. 156 ss., al quale si rinvia per una panoramica dei vantaggi che detta modalità offre in termini di rendere più agevole ed efficiente la condivisione dei dati. Il *data pooling*, a ogni modo, è spesso indicato accanto al *data sharing* (oltre ai *considerando* nn. 2 e 27 del Reg. UE n. 868/2022, cfr. ad es. COMMISSIONE EUROPEA, *Una strategia europea per i dati*, cit., p. 16; EUROPEAN COMMISSION, *Commission Staff Working Document on Common European Data Spaces*, SWD(2024) 21 final, 24 gennaio 2024, pp. 3 e 51; EUROPEAN COMMISSION, *Commission Staff Working Document on Common European Data Spaces*, Brussels, SWD(2022) 45 final, 23 febbraio 2022, pp. 2 e 8; ENISA, *Engineering personal data protection in EU data spaces*, January 2024, p. 6), ma ciò non sembra ostare alla sua riconduzione alla condivisione dei dati stessa (la descritta circostanza appare dovuta alla volontà di porre in evidenza la peculiarità della messa in comune dei dati, rispetto al *data sharing* come "scambio" dei dati).

[91] Art. 2, n. 10, Reg. cit. Ciò, posto altresì che, come accennato, il *considerando* n. 28 Reg. cit. individua il *pooling* come un esempio di servizio di intermediazione dei dati e detti servizi, com'è noto, mirano per definizione a instaurare rapporti commerciali tra fornitori e utenti dei dati «ai fini della condivisione dei dati» (art. 2, n. 11, Reg. cit.). Un richiamo, seppur non esplicito, al *data pooling* come servizio offerto dagli intermediari dei dati previsti dal DGA sembra rinvenibile anche nel *Data Act* (Reg. UE n. 2854/2023), ove al *considerando* n. 26 è previsto che «I servizi di intermediazione dei dati, disciplinati dal regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio, potrebbero agevolare l'economia dei dati instaurando relazioni commerciali tra utenti, destinatari dei dati e terzi e possono aiutare gli utenti a esercitare il loro diritto di utilizzare i dati, ad esempio garantendo l'anonimizzazione dei dati personali o *l'aggregazione dell'accesso ad essi da parte di molteplici singoli utenti*» (enfasi aggiunta).

[92] In tal senso, cfr. ad es. G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, cit., p. 982; AA.VV., *Mapping the Landscape of Data Intermediaries – Emerging Models for More Inclusive Data Governance*, cit., p. 41; AA.VV., *Data Access and Sharing in Germany and in the EU: Towards a Coherent Legal Framework for the Emerging Data Economy*, cit., p. 284.

dati tra titolari e utenti dei dati, ma che non ne costituiscono elementi essenziali [93], potendo assumere rilievo nel contesto di qualsiasi tipologia di servizi di intermediazione di dati, consistendo semplicemente nei principali modi in cui può sostanziarsi il *data sharing* intermediato [94].

Non sembra contrastare con questa conclusione, d'altra parte, la circostanza che la medesima disposizione si riferisca al solo *data sharing* tra titolari e utenti dei dati, ad esclusione cioè degli interessati. Sul punto, basti segnalare che i «titolari dei dati» (art. 2, n. 8, Reg. cit.) sono persone (fisiche o giuridiche) titolari del diritto di concedere l'accesso o di condividere anche "dati personali", evenienza che esclude il possibile rilievo di argomentazioni fondate sulla necessità di garantire una maggior protezione agli "interessati", sul presupposto, cioè, che le modalità esemplificate dall'art. 10, lett. *a*), Reg. cit. siano incompatibili con il regime di protezione delle persone fisiche con riguardo al trattamento dei dati personali stabilito dal diritto UE [95]. Se tali operazioni sono effettuabili anche con riguardo ai dati personali, così ponendo un rischio per i diritti e le libertà delle persone cui quei dati si riferiscono, le stesse a maggior ragione potranno essere svolte anche nell'intermediazione effettuata direttamente su iniziativa degli interessati, coerentemente alle esigenze relative al *data subjects' empowerment* sottese al DGA.

Chiarita la possibilità di fornire servizi supplementari di "integrazione" e conservazione dei dati, va rilevato che l'art. 12, lett. *e*), Reg. cit. non osta alla combinazione di più strumenti e servizi aggiuntivi diversi tra loro [96]: in tal senso, l'inte-

---

[93] Cfr. L. VON DITFURTH, *Datenmärkte, Datenintermediäre und der Data Governance*, cit., p. 219 ss.

[94] Ciò risulta evidente considerando che l'elenco previsto dall'art. 10, lett. *a*), Reg. cit. fa riferimento altresì all'ipotesi, per così dire "elementare", dello scambio bilaterale o multilaterale dei dati. Se anche tale attività fosse "esclusiva" dei soli fornitori richiamati da tale norma, non resterebbe in sostanza alcuno spazio di operatività per la fornitura delle altre tipologie di servizi di intermediazione dei dati. D'altra parte, al *considerando* n. 27 del DGA le medesime modalità sono richiamate come esemplificazione dei servizi di intermediazione dei dati in generale e non solo in riferimento ai servizi tipizzati alla lett. *a*) dell'art. 10 Reg. cit.

[95] L'art. 10, lett. *a*), Reg. cit. si riferisce alla generalità dei titolari dei dati, inclusi perciò coloro che hanno il diritto di concedere l'accesso a determinati dati personali, essendo a ciò autorizzati dal consenso espresso dai relativi interessati o dalla sussistenza di altra valida condizione di liceità del trattamento. Sulle condizioni di liceità del trattamento di dati personali (art. 8 Carta dir. fond. UE; art. 6 Reg. UE n. 679/2016), v. ad es. F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, 2019, pp. 110-193; D. POLETTI, *sub* art. 6 Reg. UE n. 679/2016, in R. D'ORAZIO-G. FINOCCHIARO-O. POLLICINO-G. RESTA (a cura di), *Codice della* privacy *e* data protection, Milano, 2021, p. 199 ss.

[96] Così, in L. VON DITFURTH, *Datenmärkte, Datenintermediäre und der Data Governance*, cit., p. 399. La possibilità di realizzare servizi a valore aggiunto risultanti dalla combinazione di più operazioni di trattamento diverse tra loro – si pensi, ad esempio, alle operazioni di raccolta, registrazione, organizzazione, strutturazione, conservazione, modifica o comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione (richiamando la definizione di «trattamento» prevista nel contesto tanto della normativa in materia di protezione e libera circolazione dei dati per-

grazione dei dati e la loro successiva conservazione in tale forma possono essere realizzate, unitamente alle altre operazioni funzionali all'implementazione del *data pooling*, ai fini dell'offerta di strumenti o servizi di messa in comune dei dati in base all'art. 12, lett. *e*), Reg. cit.

Le cooperative di dati, dunque, potranno offrire strumenti o servizi per l'integrazione dei dati dei membri che abilitino la realizzazione di uno o più *data pools* nei quali conservare tali dati in forma integrata, da impiegare per facilitarne lo scambio, estraendo determinate porzioni (ossia, specifici *dataset*) da porre a disposizione degli utenti dei dati per il tramite delle attività di intermediazione della cooperativa di dati [97].

Resta fermo che le cooperative di dati potranno offrire il *data pooling* solo nel rispetto di tutti i requisiti di cui all'art. 12, lett. *e*), Reg. cit. e, segnatamente, solo se il medesimo sia un mezzo per facilitare lo scambio dei dati. Sotto questo profilo, richiamando le varie "tipologie" di agevolazione del *data exchange* precedentemente esemplificate [98], è evidente come la messa in comune dei dati faciliti senz'altro i successivi scambi dei dati, peraltro in piena aderenza alla logica di supporto ai membri propria delle cooperative di dati. Ciò, ad esempio, aumentando il potere contrattuale dei membri e, dunque, la capacità della cooperativa di dati di negoziare condizioni per il trattamento dei dati da scambiare meglio rispondenti agli interessi dei membri; ma anche dal punto di vista "materiale" o "organizzativo", consentendo la messa a disposizione dei dati afferenti a più membri tramite una singola operazione di "comunicazione" dei dati integrati.

La creazione di *data pools* a opera di una cooperativa di dati afferente al modello del DGA, inoltre, dovrà necessariamente risultare coerente con i requisiti stabiliti da tale regolamento per i "servizi di intermediazione dei dati" (art. 2, n. 11, Reg.

---

sonali dall'art. 4, n. 1, Reg. UE n. 679/2016, quanto, in modo analogo, di quella sui dati non personal, dall'art. 3, n. 2, Reg. UE n. 1807/2018) – emerge dai servizi esemplificati all'art. 12, lett. *e*), Reg. cit., i quali comprendono attività sia elementari (la citata conservazione temporanea dei dati) sia complesse, composte da un «insieme di operazioni» differenti combinate tra loro (si pensi, su tutte, all'anonimizzazione dei dati personali, rispetto alla quale, per maggiore chiarezza, cfr. le tecniche evidenziate in ART. 29 WORKING PARTY, *Opinion 05/2014 on Anonymisation Techniques*, 10 April 2014).

[97] Per completezza, si evidenzia che, in dottrina, vi è chi ha ritenuto che le cooperative di dati non possano effettuare il *pooling* dei dati, in quanto detta attività non sarebbe collocabile entro gli obiettivi stabiliti all'art. 2, n. 15, Reg. cit. (cfr. E. BIETTI-A. ETXBERRIA-M. MANNAN-J. WONG, *Data Cooperatives in Europe: A Legal and Empirical Investigation*, cit., p. 17). Simili interpretazioni sembrano confondere gli obiettivi (principali) attribuiti dal DGA alle cooperative di dati con le attività che queste ultime, nell'esercizio della propria libertà d'impresa, possono adottare per l'erogazione dei servizi di intermediazione dei dati. Si consideri, ad esempio, quanto indicato in *Ibidem*, ove è rilevato che, in base alla definizione di servizi di cooperative di dati prevista dal DGA, «*For instance, cooperatives that seek to pool and process aggregated data would not fit within the three functions*»: in tal caso, vi è una sostituzione tra obiettivi ("*functions*") delle cooperative e attività effettuabili da queste ultime per il perseguimento degli stessi. Il *data pooling* è un'attività che può essere rivolta al perseguimento di plurime finalità, tra le quali senz'altro quelle previste dall'art. 2, n. 15, Reg. cit.

[98] V. *supra*, par. 2.2.

cit.) e perciò non potrà consistere, a titolo indicativo, in una modalità per realizzare operazioni di condivisione dei dati (art. 2, n. 10, reg. cit.) senza instaurare rapporti commerciali tra le parti della transazione [99].

3.5. (*segue*) Cenni alle questioni di diritto della concorrenza e protezione dei dati personali poste dai *data pools*.

La progettazione di strumenti o servizi per la messa in comune dei dati entro le cooperative di dati deve tenere in debito conto anche le questioni in materia di diritto della concorrenza (per le cooperative di dati tra imprese) e protezione dei dati personali (in caso di trattamento di tali dati) poste dal *data pooling*.

In sintesi, rispetto alle questioni *antitrust* va segnalato come la creazione di *data pools* possa favorire pratiche anticoncorrenziali basate sullo scambio di informazioni tra imprese concorrenti, in termini sia di agevolazione di fenomeni collusivi sia di determinazione di fenomeni di preclusione anticoncorrenziale [100]. La questione interes-

---

[99] Il *data pooling*, come accennato, non comporta necessariamente la facoltà di accesso ai dati per i partecipanti al *pool* e, comunque, si rinviene anche al di fuori dei servizi di *data intermediation*. Si consideri, ad esempio, il caso in cui i partecipanti al *pool* mettano assieme i propri dati, affidandone la gestione alla cooperativa di dati, senza prevedere l'accesso dei singoli partecipanti ai dati forniti dagli altri (ciò escludendo la condivisione intermediata "interna"), sulla base di modelli di operatività che ruotano attorno all'analisi del *dataset* integrato per offrire servizi a vantaggio dei propri membri oppure sul mercato, in quest'ultimo caso senza però instaurare rapporti commerciali diretti tra membri e utenti dei dati (cfr. in particolare il caso contemplato dall'art. 2, n. 11, lett. *a*), Reg. cit.). Simili pratiche si rinvengono anche nelle *data cooperatives* diffuse nella prassi: si consideri, ad esempio, il modello commerciale della cooperativa di dati *Driver's Seat* (https://www.driversseat.co/), rispetto al quale si v. F. BRAVO, *Le cooperative di dati*, cit., p. 771 ss., nonché E. BIETTI-A. ETXBERRIA-M. MANNAN-J. WONG, *Data Cooperatives in Europe: A Legal and Empirical Investigation*, cit., p. 8 ss. L'implementazione di questo tipo di attività, nella misura in cui siano svincolate da un'operazione di *data sharing* intermediata (art. 2, n. 11, Reg. cit.), non risulta ammissibile nelle cooperative di dati previste dal DGA.

[100] Tali profili sono stati evidenziati dalla COMMISSIONE EUROPEA, *Linee direttrici sulla cooperazione orizzontale*, cit., pt. 366 ss. Pur riguardando lo scambio di informazioni tra imprese in generale, dette questioni pongono maggiori criticità nel caso dei *data pools*, specialmente a fronte del carattere strutturato che, in tali casi, viene ad assumere lo scambio di informazioni: basti segnalare che lo *information exchange* pone maggiori rischi per la tutela della concorrenza nel caso in cui i contatti siano plurimi e avvengano con una frequenza più elevata (cfr. ad es. P. MANZINI, *Diritto* antitrust *dell'Unione europea*, Torino, 2022, p. 93 ss.), circostanza che nei *data pools* tende a verificarsi con una maggiore facilità, anche grazie all'integrazione di appositi *software* che consentono ai membri di alimentare il *pool* in modo automatico, su base continua e in tempo reale (i quali, peraltro, potrebbero ritenersi anche algoritmi "collusivi": in merito, v. A. EZRACHI-M.E. STUCKE, *Virtual Competition: the Promise and Perils of the Algorithmic-driven Economy*, Cambridge, 2016; P. MANZINI, *Intelligenza artificiale e diritto della concorrenza*, in U. RUFFOLO (a cura di), *XXVI lezioni di diritto dell'intelligenza artificiale*, Torino, 2021, p. 422 ss.; A. PEZZOLI-A. TONAZZI, *Discriminazione e collusione tacita tra lessico, intelligenza artificiale e algoritmi*, in *Analisi Giuridica dell'Economia*, 2019, 1, p. 201 ss.; G. COLANGELO, Big data*, piattaforme digitali e* antitrust, cit., p. 449 ss.; D. QUAGLIONE-C.

sa principalmente la circolazione dei dati tra i membri del *pool*, la quale potrebbe integrare una forma di cooperazione tra imprese vietata dall'art. 101 TFUE (o, nell'ordinamento domestico, dall'art. 2 l. 10 ottobre 1990, n. 287), anche come pratica concordata, posto che, com'è noto, può aversi una concertazione rilevante per l'applicazione del divieto di intese restrittive della concorrenza anche laddove due o più imprese entrino in contatto in modo soltanto indiretto [101], incluso per il tramite di un terzo (ivi rappresentato dal fornitore dei servizi di cooperativa di dati) [102].

Al riguardo, il *considerando* n. 60 del DGA prevede che detto regolamento non dovrebbe incidere sull'applicazione delle norme in materia di diritto della concorrenza, nonché che le misure previste dal medesimo non dovrebbero essere impiegate per limitare la concorrenza in contrasto con il TFUE, specialmente con riguardo allo scambio di informazioni sensibili dal punto di vista della concorrenza tramite servizi di intermediazione dei dati tra concorrenti anche potenziali. Ancora, nel preambolo è rimarcata la "opportunità" per l'intermediario di adottare misure per garantire il rispetto del diritto della concorrenza, incluse procedure aventi tale scopo; ciò, specialmente nelle situazioni in cui «la condivisione dei dati consente alle imprese di venire a conoscenza delle strategie di mercato dei loro concorrenti effettivi o potenziali» (*considerando* n. 37 Reg. cit.) [103].

Tra le condizioni previste dall'art. 12 Reg. cit. vi sono diversi requisiti volti a limitare i rischi per la concorrenza poc'anzi citati, tra i quali si richiamano, in particolare, gli obblighi per l'intermediario: *(i)* di garantire che la procedura di accesso al suo servizio sia equa, trasparente e non discriminatoria per tutte le parti delle transazioni di dati (art. 12, lett. *f*), Reg. cit.) [104], rilevante rispetto ai rischi di preclu-

---

POZZI, *Economia dei* big data*: lineamenti del dibattito in corso e alcune riflessioni di* policy, in *L'industria*, 2018, 1, p. 7 ss.). Sulle questioni *antitrust* della messa in comune dei dati, v. ad es. B. LUNDQVIST, *Data Collaboration, Pooling and Hoarding under Competition Law*, in *Stockholm Faculty of Law Research Paper Series* no. 6, 2018. Sui profili di diritto della concorrenza nelle cooperative di dati, v. F. BRAVO, *Le cooperative di dati*, cit., p. 797 ss.

[101] Ciò, in base agli insegnamenti forniti dalla Corte di giustizia UE, in particolare in *Suiker Unie*, *leading case* relativamente alla nozione di "pratica concordata" (CGUE, 16 dicembre 1975, *Suiker Unie*, c.r. 40-48, 50, 54-56, 111, 113 e 114-73).

[102] *Ibidem*. V. altresì quanto evidenziato in COMMISSIONE EUROPEA, *Linee direttrici sulla cooperazione orizzontale*, cit., ptt. 368 e 401 ss.

[103] Sul punto, la proposta del *Data Governance Act*, a differenza del testo emanato, prevedeva espressamente, tra le condizioni per la fornitura di "servizi di condivisione dei dati" (poi rinominati in "servizi di intermediazione dei dati"), che «il fornitore dispone di procedure atte a garantire il rispetto delle norme dell'Unione e nazionali in materia di concorrenza» (art. 11, n. 9 della proposta del DGA).

[104] Detto requisito impone il rispetto del paradigma "FRAND" ("*fair, reasonable and non-discriminatory*"), emerso come mezzo di tutela della concorrenza nell'ambito brevettuale. In merito, rispetto a detto paradigma, sia in generale sia negli specifici scenari di *data sharing*, v. H. RICHTER-P.R. SLOWINSKIPP, *The Data Sharing Economy: On the Emergence of New Intermediaries*, in *IIC*, 2019, p. 17 ss. Sull'art. 12, lett. *f*), Reg. cit. come espressione di tale paradigma, v. ad es. G. CA-

sione anticoncorrenziale verso le imprese non appartenenti alla cooperativa nella quale è stato realizzato il *data pool* [105]; *(ii)* di assicurare il massimo livello di sicurezza per la conservazione e la trasmissione di informazioni sensibili sotto il profilo della concorrenza (art. 12, lett. *l*), Reg. cit.) [106].

Circa le questioni in materia di protezione dei dati personali, in questa sede si intende fare cenno a quelle relative ai principi applicabili al trattamento dei dati personali, le quali presentano alcuni punti di contatto con le questioni *antitrust*. Anzitutto, nei *data pools* occorre prestare particolare attenzione al rispetto dei principi di necessità e proporzionalità, nonché di minimizzazione [107], per garantire che

---

ROVANO-M. FINCK, *Regulating Data Intermediaries: The impact of the Data Governance Act on the EU's data economy*, cit., 2023, p. 9; L. VON DITFURTH, *Datenmärkte, Datenintermediäre und der Data Governance*, cit., pp. 407-408; H. RICHTER, *Looking at the Data Governance Act and Beyond: How to Better Integrate Data Intermediaries in the Market Order for Data Sharing*, cit., p. 468. Sul rilievo dell'art. 12, lett. *f*), Reg. cit. per limitare le pratiche *antitrust* nel contesto della messa in comune dei dati, v. AA.VV., *Data Access and Sharing in Germany and in the EU: Towards a Coherent Legal Framework for the Emerging Data Economy*, cit., p. 296.

[105] Rispetto alla preclusione anticoncorrenziale, cfr. COMMISSIONE EUROPEA, *Linee direttrici sugli accordi di cooperazione orizzontali*, cit., ptt. 382-383, ove è chiarito che la stessa può avvenire anzitutto sul medesimo mercato, quando lo scambio di informazioni sensibili sotto il profilo commerciale determini uno svantaggio concorrenziale considerevole per i concorrenti che non partecipano allo stesso rispetto a quelle che vi partecipano, laddove dette informazioni siano di importanza strategica per competere sul mercato e lo scambio inerisca a una quota significativa del mercato rilevante (come nel caso della condivisione di dati di importanza strategica, riguardanti un'ampia quota del mercato, con impedimento dell'accesso a tali dati per i concorrenti). A ogni modo, è evidenziato che lo scambio di informazioni può dare luogo anche a una preclusione anticoncorrenziale su un mercato collegato (ad esempio, le imprese integrate verticalmente scambiano informazioni in un mercato a monte, acquisendo un potere di mercato per attuare pratiche collusive, come l'aumento del prezzo di un fattore produttivo chiave, in un mercato a valle) (*Ibidem*).

[106] Tale disposizione sembra prevedere uno *standard* di tutela delle informazioni sensibili sotto il profilo della concorrenza superiore a quello previsto sia per i dati non personali (rispetto ai quali il medesimo art. 12, lett. *l*), Reg. cit. fa riferimento a un «adeguato» livello di sicurezza) sia, soprattutto, per i dati personali. Per questi ultimi, infatti, il Reg. UE n. 679/2016 impone a titolari e responsabili del trattamento l'adozione di misure «adeguate», per assicurare un livello di sicurezza, segnatamente «adeguato al rischio» per i diritti e le libertà delle persone fisiche (art. 32 Reg. cit. e, a monte, art. 5, par. 1, lett. *f*), Reg. cit.).

[107] Rispetto ai principi di necessità e proporzionalità, i quali non sono stabiliti espressamente nel Reg. UE n. 679/2016, v. G. BUTTARELLI, *Principio di necessità nel trattamento dei dati*, in C.M. BIANCA-F.D. BUSNELLI (a cura di), *La protezione dei dati personali. Commentario al D.Lgs. 30 giugno 2003, n. 196 («Codice della* privacy*»)*, Padova, 2007, p. 32 ss. (rispetto a quanto stabilito nel previgente art. 3 d.lgs. 30 giugno 2003, n. 196); F. BRAVO, *Sul bilanciamento proporzionale dei diritti e delle libertà "fondamentali", tra mercato e persona: nuovi assetti nell'ordinamento europeo?*, in *Contratto e impresa*, 2018, 1, p. 190 ss. (con riguardo all'applicazione di tali principi nel contesto della clausola generale di cui all'art. 52 Carta dir. fond. UE, per limitare il diritto alla protezione dei dati personali); C. CHILIN-D. SBORLINI, *Il principio di necessità*, in F. BRAVO (a cura di), *Dati personali. Protezione, libera circolazione e* governance*.* – Vol. 1, *Principi*, Pisa, 2023, p. 369 ss.; C. BASUNTI, *Il principio di proporzionalità*, in F. BRAVO (a cura di), *Dati personali. Protezione, libera circolazione e*

sia all'interno del *pool* sia nella gestione delle richieste degli utenti dei dati la circolazione di tali dati sia limitata a quanto strettamente necessario per il soddisfacimento della finalità del trattamento. Sul punto, risultano significative altresì le criticità poste dal principio di limitazione della finalità (art. 5, par. 1, lett. *b*), Reg. UE n. 679/2016) [108], anche in relazione alla base giuridica del consenso e, segnatamente, ai requisiti della manifestazione di volontà "specifica" e "informata" (artt. 4, n. 11, Reg. cit.) [109], rispetto alla possibilità di realizzare un "*personal data pool*" da impiegare per successive operazioni di condivisione (intermediata) dei dati funzionali al soddisfacimento di finalità che, al momento iniziale della messa in comune dei dati, non risultano individuate secondo il grado di determinatezza richiesto da tali disposizioni, posto che le stesse sono destinate ad essere identificate in modo specifico solo con la successiva presentazione delle richieste di accesso e utilizzo dei dati da parte degli utenti dei dati [110]. Tali questioni dovranno essere affrontate adottando adeguate misure tecniche e organizzative, anche ai fini del rispetto degli obblighi di responsabilizzazione, nonché protezione dei dati per impostazione predefinita e fin dalla progettazione (rispettivamente, artt. 24 e 25, par. 1 e 2, Reg. cit.) [111].

---

governance. – Vol. 1, *Principi*, cit., p. 411 ss. Sul principio di minimizzazione (art. 5, par. 1, lett. *c*), Reg. UE n. 679/2016), v. ad es. S.G. BATTISTINI-L. MATARAZZO-L. ZANETTI, *Il principio di minimizzazione dei dati*, in F. BRAVO (a cura di), *Dati personali. Protezione, libera circolazione e* governance. – Vol. 1, *Principi*, cit., p. 231 ss. Più ampiamente, sui principi applicabili al trattamento, v. altresì v. M. DELL'UTRI, *Principi generali e condizioni di liceità del trattamento dei dati personali*, in V. CUFFARO-R. D'ORAZIO-V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, p. 179 ss.; G. MALGIERI, *Principi applicabili al trattamento di dati personali (Comm. all'art. 5 GDPR)*, in R. D'ORAZIO-G. FINOCCHIARO-O. POLLICINO-G. RESTA (a cura di), *Codice della* privacy *e* data protection, cit., p. 176 ss.

[108] Sul principio di limitazione della finalità, v. E. NAVARRETTA, *Regole generali per il trattamento dei dati*, in C.M. BIANCA-F.D. BUSNELLI (a cura di), *La protezione dei dati personali. Commentario al D.Lgs. 30 giugno 2003, n. 196*, cit., p. 264 (rispetto a detto principio come stabilito nella normativa previgente, all'art. 11, co. 1, lett. *b*), d.lgs. n. 196/2003); A. INCERTI, *Il principio di limitazione della finalità*, in F. BRAVO (a cura di), *Dati personali. Protezione, libera circolazione e* governance. – Vol. 1, *Principi*, cit., p. 185 ss.

[109] Nell'ampia letteratura sulla condizione di liceità del consenso, v. F. BRAVO, *Le condizioni di liceità del trattamento di dati personali*, cit., p. 140 ss.; con riguardo a tale base giuridica nella normativa previgente, v. S. MAZZAMUTO, *Il principio del consenso e il problema della revoca*, in R. PANETTA (a cura di), *Libera circolazione e protezione dei dati personali*, Milano, 2006, p. 993 ss.

[110] Per quanto specificamente riguarda le criticità relative alla condizione di liceità del consenso dell'interessato nel contesto dei *data pools*, cfr. Y.A. VOGEL, *Stretching the Limit, the Functioning of the GDPR's Notion of Consent in the Context of Data Intermediary Services*, cit., spec. p. 246 ss.

[111] Sul principio di responsabilizzazione, v. G. FINOCCHIARO, *Il quadro d'insieme sul Regolamento europeo*, in EAD. (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, cit., p. 5 ss.; rispetto agli obblighi di protezione fin dalla progettazione e per impostazione predefinita, v. F. BRAVO, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, in V. CUFFARO-R. D'ORAZIO-V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit., p. 775 ss.; F. MOLLO, *Gli obblighi previsti in funzione di protezione dei dati personali*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, 2019, p. 255 ss.; S.

Le questioni *antitrust* e di *data protection* possono emergere contestualmente, laddove le informazioni sensibili sotto il profilo della concorrenza scambiate tra i membri del *pool* o verso l'esterno siano costituite da "dati personali"; in ogni caso, le stesse presentano plurimi punti di contatto [112]. La premessa dalla quale occorre muovere in entrambi i casi è costituita dal fatto che la messa in comune dei dati, grazie alla presenza dell'intermediario (ossia, della cooperativa di dati), non implica automaticamente la "comunicazione" di tali dati a tutti i membri del *pool*; al riguardo, l'intermediario dovrebbe contribuire ad assicurare che il *data pooling* avvenga con modalità che limitino l'ambito di circolazione dei dati in misura sufficiente a garantire il rispetto delle norme tanto di diritto della concorrenza [113] quanto in materia di *data protection* [114], definendo delle complessive politiche di *data governance* idonee al raggiungimento di questi obiettivi.

Per evidenziare talune delle interrelazioni tra le due discipline ravvisabili in questo ambito, è particolarmente utile considerare i punti di attenzione evidenziati dalla Commissione nelle citate Linee direttrici sugli accordi di cooperazione orizzontale [115], nel contesto degli interventi per ridurre il rischio di violazioni del diritto

---

FAILLACE, *Il principio di* privacy by design *e* privacy by default, in F. BRAVO (a cura di), *Dati personali. Protezione, libera circolazione e* governance. – Vol. 1, *Principi*, cit., p. 457 ss.

[112] Più ampiamente, sulle interrelazioni tra diritto della concorrenza e protezione dei dati personali, la Corte di giustizia UE ha avuto modo di chiarire che «l'accesso ai dati personali e la possibilità di trattamento di tali dati sono diventati un parametro significativo della concorrenza fra imprese dell'economia digitale» e che pertanto debbano essere considerate dalle autorità garanti della concorrenza degli Stati membri nell'analisi del contesto giuridico in sede di esame di un abuso di posizione dominante (art. 102 TFUE), in modo da assicurare l'effettività del diritto della concorrenza all'interno dell'Unione (CGUE, 4 luglio 2023, *Meta Platforms and Others*, causa C-252/21, pt. 51). In aggiunta, è stato evidenziato come la conformità o meno del comportamento di un'impresa in posizione dominante alle disposizioni del Reg. UE n. 679/2016 possa costituire «un importante indizio fra le circostanze rilevanti del caso di specie per stabilire se siffatto comportamento costituisca un ricorso a mezzi su cui s'impernia la concorrenza normale nonché per valutare le conseguenze di una determinata pratica sul mercato o per i consumatori» (*ibidem*, pt. 47), ai fini pertanto dell'accertamento di un possibile sfruttamento abusivo di posizione dominante. Sul caso *Meta Platforms*, v. ad es. P. MANZINI, Antitrust *e* privacy*: la strana coppia*, in ID. (a cura di), *I confini dell'*antitrust*. Diseguaglianze sociali, diritti individuali, concorrenza*, Torino, 2023, p. 123 ss.

[113] Segnatamente, per quanto riguarda il possibile rilievo anticoncorrenziale dello scambio di informazioni, l'ambito di circolazione dei dati deve essere definito in modo tale da «non ridurre o annullare il grado di incertezza in ordine al funzionamento del mercato di cui trattasi» (cfr. CGUE, 4 giugno 2009, *T-Mobile Netherlands*, causa C-8/08, pt. 23; v. altresì COMMISSIONE EUROPEA, *Linee direttrici sugli accordi di cooperazione orizzontale*, cit., pt. 384).

[114] Conformemente, in particolare, ai citati principi di necessità e proporzionalità, nonché di minimizzazione.

[115] Dette Linee guida, al pari del *Data Governance Act*, sono state adottate in attuazione della strategia europea per i dati, nella quale, in particolare, l'aggiornamento delle precedenti linee guida sugli accordi di cooperazione orizzontali (2011/C 11/01) era stato previsto tra le misure intersettoriali di implementazione della strategia (cfr. COMMISSIONE EUROPEA, *Una strategia europea per i dati*, cit. p. 16).

antitrust presentato dallo scambio di informazioni [116], ove, ad esempio, si incoraggiano le imprese: *(i)* ad implementare misure che limitino l'accesso alle informazioni o abilitino il controllo sulle modalità di utilizzo delle stesse, elementi coerenti con gli obblighi di protezione dei dati personali e, in particolare, con quelli in materia di protezione dei dati *by default* e di sicurezza (artt. 25, par. 2 e 32, Reg. cit.) e, a monte, con i citati principi di necessità e proporzionalità, minimizzazione, ma anche con il principio di integrità e riservatezza (art. 5, par. 1, lett. *f*), Reg. cit.); *(ii)* a limitare lo scambio a quanto necessario per la legittima finalità prevista, obiettivo analogo, lato *data protection*, a quelli dei principi di limitazione della finalità e minimizzazione (art. 5, par. 1, lett. *b*) e *c*), Reg. cit.).

In base alle Linee direttrici, inoltre, la realizzazione dello scambio di informazioni per il tramite di una terza parte indipendente è un elemento utile a diminuire i possibili impatti negativi per la concorrenza derivanti da tale fenomeno [117], grazie appunto alla gestione degli accessi e relativi utilizzi dei dati a opera dell'orchestratore del *data pool* [118]. La presenza dell'intermediario, sotto tale profilo, può parimenti agevolare la realizzazione di operazioni di *data sharing* in conformità alla normativa sulla protezione dei dati personali, ad esempio consentendo ai membri della cooperativa di dati di condividere i propri dati (in forma integrata) con terze parti, senza che ciò implichi che anche ognuno di essi abbia visibilità o tratti altrimenti i dati degli altri; va però ricordato che, dall'angolo visuale della *data protection*, il coinvolgimento di più attori nel trattamento di dati personali è comunque un fattore che, ampliando l'ambito di circolazione dei dati, aumenta i rischi per gli interessati, anche in termini di possibili dispersioni della responsabilità per eventuali trattamenti illeciti di dati personali [119]. La presenza di una terza parte, d'altronde,

---

[116] COMMISSIONE EUROPEA, *Linee direttrici sugli accordi di cooperazione orizzontale*, cit., pt. 406 ss.

[117] *Ibidem*, ptt. 406-408, ove è evidenziata l'utilità, a tali fini, di affidare la gestione di un *pool* di dati a un fiduciario. Al riguardo, cfr. altresì B. MARTENS-A. DE STREEL-I. GRAEF-T. TOMBAL-N. DUCH-BROWN, *Business to Business Data Sharing: an Economic and Legal Analysis*, Digital Economy Working Paper 2020-05, European Commission, Seville, 2020, pp. 6 e 29.

[118] Sul punto, viene precisato che, in linea di principio, i membri di un *data pool* per la condivisione reciproca di dati dovrebbero avere accesso solo alle proprie informazioni in forma individuale, mentre l'accesso a quelle degli altri partecipanti dovrebbe risultare possibile solo in forma aggregata (COMMISSIONE EUROPEA, *Linee direttrici sugli accordi di cooperazione orizzontale*, cit., pt. 408). Il passaggio si spiega in base al rilievo della forma con cui le informazioni sono scambiate rispetto all'integrazione di possibili pratiche anticoncorrenziali, sul presupposto che la circolazione delle informazioni commercialmente sensibili in forma aggregata (ossia, riferite globalmente a più imprese) non incida, di regola, sull'incertezza relativa alla dinamica del mercato (*Ibidem*, pt. 390 ss.).

[119] Cfr. ad es. CGUE, 7 dicembre 2023, *Schufa*, cause riunite C-26/22 e C-64/22, pt. 100, in cui è stato sottolineato che la presenza dei dati personali in più fonti rafforza l'ingerenza nel diritto alla vita privata degli interessati. V. altresì, ENISA, *Engineering Personal Data Protection in EU Data Spaces*, January 2024, p. 12, ove è evidenziato che la presenza di un responsabile del trattamento di cui si avvale, a sua volta, il fornitore dei servizi di intermediazione dei dati, di per sé introduce un nuovo vettore di rischi.

introduce possibili criticità anche dallo stesso lato *antitrust*, posto che, ad esempio, potrebbe agevolare, con lo "schermo" dell'intermediario, la realizzazione di pratiche collusive tra i membri.

In ultimo, rispetto al caso delle cooperative di dati, va rimarcato che, nonostante la disciplina del DGA abbia previsto elevate garanzie di neutralità per i fornitori di servizi di intermediazione dei dati, le *data cooperatives* sono intermediari del tutto peculiari, rispetto ai quali il requisito dell'indipendenza e le garanzie di neutralità sono attenuati in ragione della "sovrapposizione" tra *data suppliers* e intermediario stesso, quale organizzazione composta dai primi e agente *ex lege* nel loro interesse. Questa circostanza, pertanto, andrà tenuta in debita considerazione ai fini della corretta gestione dei profili qui richiamati soltanto per brevi cenni, anche relativamente all'implementazione delle citate procedure di *data governance* per assicurare il rispetto tanto del diritto della concorrenza quanto della normativa sulla protezione e la libera circolazione dei dati personali.

4. Osservazioni conclusive.

Analizzati i tratti principali della disciplina del *Data Governance Act* relativa ai servizi a valore aggiunto (art. 12, lett. *e*), Reg. cit.) e forniti alcuni primi spunti ricostruttivi sull'applicazione della stessa alle cooperative di dati, segnatamente in un senso che sia coerente con le peculiari esigenze di tali organizzazioni, in chiusura deve rilevarsi come la scelta del Reg. UE n. 868/2022 di ricondurre i servizi prestati da tali soggetti tra quelli di *data intermediation*, regolandoli con disposizioni piuttosto scarne e senza alcun temperamento o adeguamento del regime applicabile alla generalità dei servizi di intermediazione dei dati, generi rilevanti margini di incertezza sull'inquadramento e la stessa legittimità delle attività che le cooperative di dati hanno necessità di porre in essere per il perseguimento dei propri obiettivi.

Si pensi, d'altra parte, alla dibattuta possibilità, per queste organizzazioni, di erogare servizi *data-driven*, come quelli di analisi dei dati, i quali, nonostante il loro essenziale rilievo per il perseguimento dei citati obiettivi, come detto tende ad essere esclusa dai primi commentatori del regolamento in esame, sulla base di ricostruzioni fondate su di un'applicazione rigida delle condizioni cui il DGA assoggetta la fornitura dei servizi di *data intermediation*, aderente al descritto, infelice assetto basato sull'approccio "*one-size-fits-all*".

D'altronde, a monte è stato rilevato che il medesimo approccio esclude, per le *data cooperatives* ricadenti nell'ambito di applicazione del DGA, la possibilità di offrire ai propri membri strumenti e servizi emersi nella prassi come di significativo rilievo nei modelli commerciali adottati da tali organizzazioni. Si pensi, ad esempio, ai servizi collocati al di fuori degli schemi dell'intermediazione dei dati, ossia implementati non per condividere i dati forniti dai membri instaurando rapporti commerciali tra costoro e i *data users* (art. 2, n. 11, Reg. cit.), bensì per otte-

nere informazioni da licenziare all'esterno direttamente dalla struttura organizzativa, così garantendone la sostenibilità economica.

In conclusione, l'intervento legislativo realizzato con il Reg. UE n. 868/2022, per quanto concerne i servizi di cooperative di dati, nonostante gli spazi di manovra offerti dalla disciplina sui servizi a valore aggiunto, nel complesso non appare pienamente rispondente al ricercato obiettivo di favorire il *data sharing* intermediato quale mezzo essenziale per la realizzazione delle finalità della strategia europea per i dati. Per favorire l'emersione di modelli di circolazione dei dati alternativi, fondati su logiche solidaristiche tali da realizzare quel mutamento di paradigma nella *data economy* che abiliti anche gli interessati, le imprese individuali e le PMI a prosperare mediante la valorizzazione dei dati, appare allora opportuno un nuovo intervento legislativo che introduca più efficaci meccanismi promozionali, assicurando un sufficiente grado di certezza per gli operatori.

Capitolo XLI

La prevenzione da pratiche fraudolente o abusive tra *Data Governance Act* e fonti europee a tutela dei consumatori

Ilaria Speziale

Abstract: This paper analyses the condition for the provision of data intermediation services dictated by art. 12, lett. *g*) of the Data Governance Act, highlighting its critical aspects, in comparison with European consumer law, with particular reference to the Unfair Commercial Practices Directive and the Unfair Terms Directive.

1. Introduzione.

La Commissione europea, sin dalla Comunicazione del 19 febbraio 2020 «*A European Strategy for Data*» [1], ha avviato un percorso di marcata valorizzazione dei dati, personali e non personali, senza trascurare la tutela della persona umana e, dunque, la centralità del principio personalistico.

I dati rappresentano oggi la linfa vitale dello sviluppo economico, sono alla base di processi generativi di svariati nuovi prodotti e servizi e, al contempo, accrescono la produttività e l'efficienza delle risorse in tutti i settori dell'economia.

La *European Strategy for Data* intende porre le basi per assicurare all'Unione europea un ruolo guida nell'economia sempre più *data driven*, rendendola così un vero punto di riferimento per lo sfruttamento dei vantaggi derivanti da un sapiente utilizzo dei dati, *in primis* a livello imprenditoriale. In tale contesto, assume prima-

[1] COMMISSIONE EUROPEA, Comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Una strategia europea per i dati*, Bruxelles, 19 febbraio 2020, COM (2020) 66 *final*.

ria importanza la *European Data Governance*, scolpita nel *Data Governance Act*, Reg. (UE) n. 868/2022 (c.d. DGA) che è entrato in vigore il 3 giugno 2022 e si applica dal 24 settembre 2023.

Il DGA si snoda lungo tre direzioni principali: il riuso dei dati personali e non personali, che sono nella disponibilità della pubblica amministrazione, la quale ha la facoltà di coinvolgere soggetti terzi nelle attività di trattamento dei dati per finalità, commerciali o non commerciali, ulteriori rispetto a quelle che hanno giustificato il primo trattamento; l'altruismo dei dati, ossia la condivisione volontaria di dati, personali o non personali, che prescinde dalla richiesta o ricezione di un compenso che vada oltre il recupero dei costi di messa a disposizione del dato, per il perseguimento di obiettivi di interesse generale; i servizi di intermediazione dei dati, personali e non personali, offerti dai c.d. fornitori di servizi di intermediazione dei dati che mediano tra gli utenti e le imprese, le quali svolgono operazioni sui dati [2].

È proprio su questi ultimi servizi che occorre soffermarsi nella presente sede.

L'art. 10 DGA li qualifica come: «*a*) servizi di intermediazione tra i titolari dei dati e i potenziali utenti dei dati, compresa la messa a disposizione di mezzi tecnici o di altro tipo per consentire tali servizi; tali servizi possono includere scambi di dati bilaterali o multilaterali o la creazione di piattaforme o banche dati che consentono lo scambio o l'utilizzo congiunto dei dati, nonché l'istituzione di altra infrastruttura specifica per l'interconnessione di titolari dei dati con gli utenti dei dati; *b*) servizi di intermediazione tra interessati che intendono mettere a disposizione i propri dati personali o persone fisiche che intendono mettere a disposizione dati non personali e potenziali utenti dei dati, compresa la messa a disposizione di mezzi tecnici o di altro tipo per consentire tali servizi, permettendo in particolare l'esercizio dei diritti degli interessati di cui al regolamento (UE) 2016/679; *c*) servizi di cooperative di dati» [3].

Inoltre, il DGA, all'art. 2, par. 1, n. 15) riporta una definizione dei servizi di cooperative di dati e non delle cooperative di dati di per sé. Il rinvio normativo è ad una «struttura organizzativa» che ha come «membri» interessati, imprese individuali e/o PMI, senza che venga esplicitata in maniera chiara la forma societaria. Tale nozione è volutamente ampia e lascia intuire che i servizi di cooperative di dati possano essere forniti da svariati enti [4]. Nonostante ciò, l'ipotesi della società

---

[2] Cfr. F. BRAVO, *Intermediazione di dati personali e servizi di* data sharing *dal GDPR al* Data Governance Act, in *Contr. e impr./Europa*, 2021, 1, p. 199 ss.; D. POLETTI, *Gli intermediari dei dati*, in *EJPLT*, 2022, 1, p. 45 ss.

[3] Sul tema, v. F. BRAVO, *Le cooperative di dati*, in *Contr. e impr.*, 2023, 3, p. 757 ss.; L. PETRONE, *Il mercato digitale europeo e le cooperative di dati*, in *Contr. e impr.*, 2023, 3, p. 800 ss. In argomento, si segnala, altresì, il Progetto di Terza Missione dedicato alle cooperative di dati promosso dall'Università di Bologna (v. *https://site.unibo.it/cooperative-di-dati/it/progetto*), in cui anche tale contributo di inserisce.

[4] V., opportunamente, F. BRAVO, *Le cooperative di dati*, cit., p. 760 che ipotizza che la struttura organizzativa di cui all'art. 2, par. 1, n. 15), DGA venga costituita nella forma delle associazioni tem-

cooperativa parrebbe, fisiologicamente, quella applicabile alle cooperative di dati.

L'organizzazione a cui si riferisce il menzionato art. 2 DGA persegue vari obbiettivi, ossia: aiutare i propri membri nel far valere le facoltà che l'ordimento giuridico riconosce loro, favorendo l'acquisizione delle informazioni per l'esercizio dei diritti sui propri dati, specie se personali; promuovere un confronto interno tra i propri membri, basato sullo «scambio di opinioni sulle finalità e sulle condizioni del trattamento dei dati», al fine di rappresentare «al meglio gli interessi dei propri membri in relazione ai loro dati»; «negoziare i termini e le condizioni per il trattamento dei dati per conto dei membri», ossia concordare con soggetti terzi, che utilizzeranno i dati, quali siano le condizioni giuridiche ed economiche volte a regolare i rapporti aventi ad oggetto l'uso di dati, personali e non personali, dei propri membri, persone fisiche o giuridiche. L'attività di negoziazione, precisa la definizione del servizio in questione, va svolta in un momento antecedente rispetto all'autorizzazione o al consenso al trattamento dei dati da parte dei «membri» della «struttura organizzativa» fornitrice del servizio.

Il *Data Governance Act* riporta poi nell'art. 12 un composito elenco di condizioni per la fornitura dei citati servizi di intermediazione dei dati. Tali condizioni guardano al fenomeno sotto molteplici prospettive, tenendo conto, tra gli altri, dei profili legati alla tipologia dei singoli servizi offerti, alle condizioni commerciali di fornitura, alla raccolta dei dati oggetto dei servizi, al loro formato, all'interoperabilità con altri servizi connessi, all'ipotesi di insolvenza del fornitore, ecc.

Nella pletora di queste condizioni, emerge il disposto della lett. *g*): «il fornitore di servizi di intermediazione dei dati dispone di procedure per prevenire pratiche fraudolente o abusive in relazione a soggetti che richiedono l'accesso tramite i suoi servizi di intermediazione dei dati». È bene soffermarsi in dettaglio su tale previsione, inquadrandola nel più ampio contesto normativo europeo (specie) a tutela dei consumatori.

2. Il necessario confronto con le discipline europee sulle pratiche commerciali sleali e sulle clausole abusive.

Il diritto europeo (della concorrenza) ha avuto, sin dall'inizio, tre fini: 1) l'integrazione dei mercati nazionali in un mercato unico; 2) la difesa della libertà economica delle imprese contro le concentrazioni di potere economico privato; 3) il benessere dei consumatori [5]. Ciò che è mutato nel tempo è il peso specifico di ciascuno di essi che si è progressivamente spostato dal primo al terzo [6].

---

poranee di imprese (ATI) o dei raggruppamenti temporanei di impresa (RTI), ovvero nella forma delle reti di imprese, che svolgano servizi di intermediazione di dati mediante le logiche di cooperazione dettate dal legislatore UE.

[5] V. M. MONTI, *EC Competition Law*, Cambridge, 2007, cap. II e *passim*.

[6] V. M. LIBERTINI, *Concorrenza*, in *Enc. dir*., Milano, 2010, (Annali III), p. 218.

In particolare, a partire dalla metà degli anni Ottanta, dopo tre decenni di (mera) difesa della concorrenza [7], la Comunità europea ha iniziato ad edificare un diritto dello scambio armonizzato aderente alle concezioni economiche del libero mercato [8]. Le modifiche ai Trattati, sopraggiunte negli anni Novanta, hanno consentito i primi interventi di politica sociale che coniugavano gli obiettivi di pura efficienza economica con le esigenze (etiche) di giustizia (commutativa e distributiva) dei protagonisti del mercato. Di qui la formula «economia sociale di mercato» [9], confluita nell'art. 3, par. 3 TUE: «l'Unione si adopera per lo sviluppo sostenibile dell'Europa, basato (…) su un'economia sociale di mercato fortemente competitiva».

Essa indica chiaramente «l'ordine giuridico» impresso al mercato unico [10]: le istituzioni eurounitarie promuovono l'interesse pubblico alla libera concorrenza, sì da tutelare imprese e consumatori ed impedire che il potere economico guadagni la forza e la funzione del potere politico [11]. Tale obiettivo viene, però, ad essere declinato lungo la coordinata del bilanciamento degli interessi: il diritto, quale struttura conformatrice del mercato (unico), prescrive gli strumenti di attuazione dei principi

---

[7] Durante tale prima fase, la CEE aveva perseguito una politica economica volta soprattutto a creare uno «spazio senza frontiere interne» e, quindi, a favorire la libera circolazione delle merci all'interno del territorio comunitario. Un obiettivo, quest'ultimo, diverso da quello delle tradizionali norme antimonopolitistiche. Tanto è vero che, in quegli stessi anni, le istituzioni comunitarie prestavano maggiore attenzione alle intese verticali di distribuzione delle merci, le quali contenevano spesso clausole restrittive della circolazione dei beni fra i vari Paesi membri; mentre il fenomeno, pure diffuso, dei cartelli orizzontali veniva considerato meno pericoloso ai fini del buon funzionamento dei mercati. Ciò non toglie che la politica *antitrust* europea abbia promosso, sin dal principio, anche gli obiettivi più "tradizionali" delle discipline anticoncorrenziali, come la lotta ai cartelli e agli abusi dei monopoli. Sul tema, v. M. LIBERTINI, *op. cit*., p. 217, nt. 104 e p. 218.

[8] Così A. GENTILI, *Pratiche sleali e tutele legali: dal modello economico alla disciplina giuridica*, in *Riv. dir. priv*., 2010, 3, p. 45.

[9] La formula appartiene alla Scuola di Friburgo (il c.d. ordoliberalismo), un filone di pensiero liberale tedesco, portato alla ribalta dalla crisi *post* nazista, che ha avuto un ruolo ispiratore essenziale nella costruzione del diritto europeo della concorrenza. Tale Scuola riprende l'idea fondamentale del pensiero liberale, secondo cui i mercati concorrenziali sono strumenti indispensabili per la realizzazione del benessere collettivo. Ritiene, però, pure che i mercati, se sprovvisti di regolazione, tendano a degenerare, dando luogo alla formazione di strutture di potere privato, lesive della libertà di impresa e di consumo, nonché produttive di forme di ingiustizia e di diseguaglianza. Pertanto, lo Stato è chiamato a intervenire, al fine di proteggere le categorie socialmente deboli, assicurare la stabilità monetaria e mantenere una condizione di concorrenza effettiva nel mercato. Le idee ordoliberali, prima di influenzare la normativa europea, sono state assunte ufficialmente a base della politica economica della Repubblica federale tedesca e della legge a tutela della concorrenza del 1958 (poi più volte modificata). In argomento, si rinvia a M. LIBERTINI, *op. cit.*, pp. 214-217 e L. DI NELLA, *La scuola di Friburgo o dell'ordoliberalismo*, in N. IRTI (a cura di), *Diritto ed economia. Problemi e orientamenti teorici*, Padova, 1999, p. 171 ss.

[10] Nella nota espressione eletta a titolo di una celebre monografia: v. N. IRTI, *L'ordine giuridico del mercato*, Roma-Bari, 1998-2003.

[11] Così N. IRTI, *Economia di mercato e interesse pubblico*, in *Riv. trim. dir. e proc. civ*., 2000, 2, p. 444.

di solidarietà, di eguaglianza e di pieno sviluppo della persona umana, tesi a scongiurare il sacrificio delle posizioni più deboli a vantaggio di quelle più forti [12].

La normativa a protezione dei consumatori, di matrice europea, nel suo complesso, realizza proprio le due finalità-chiave dell'economia sociale di mercato: la giustizia sociale e l'efficienza economica. Il legislatore UE, nei suoi plurimi interventi legislativi, mostra, infatti, di aderire ad un generale principio di correttezza ed impone così una regola agli scambi perfettamente coerente con l'«ordine giuridico» del mercato europeo.

I concetti di buona fede, lealtà e correttezza compaiono ricorsivamente nelle fonti eurounitarie, nell'intento dichiarato di salvaguardare la struttura concorrenziale del mercato e di ridurre le asimmetrie informative esistenti tra professionisti e consumatori, al fine di riequilibrarne (anche) il rapporto contrattuale. Tali concetti vanno declinati oggi in relazione all'evoluzione tecnologica che caratterizza il mercato e, dunque, nella sua odierna connotazione in chiave digitale, oltre che analogica.

In questo contesto, l'art. 12, lett. *g*), DGA impone un obbligo a carico del fornitore di servizi che è chiamato a predisporre un sistema di protezione, nei confronti di chi acceda ai suoi servizi, dalle attività di mercato che presentino carattere di «fraudolenza» o di «abusività».

Simili attività richiamano chiaramente i noti concetti legislativi di pratiche commerciali sleali e di clausole abusive, su cui sono imperniate le due discipline europee, rispettivamente, della direttiva 2005/29/CE e della direttiva 1993/13/CEE. Si tratta dei due grandi pilastri del sistema delle regole a cui devono attenersi i professionisti nella pluralità di possibili rapporti contrattuali che essi promuovono, instaurano ed attuano con i consumatori [13].

La vicinanza fra le due normative trova conferma (anche) nei lavori preparatori della direttiva 2005/29, quando il Parlamento europeo, nel parere reso in prima lettura sul testo della proposta della Commissione del 2003, suggerì di esplicitare il requisito della buona fede, sia nel divieto generale dell'art. 5, sia nella definizione di diligenza professionale di cui all'art. 2, giacché «in linea con le disposizioni della direttiva 93/13/CEE concernente le clausole abusive nei contratti stipulati con i consumatori» [14].

---

[12] V. S. POLIDORI, *Nullità di protezione e interesse pubblico*, in *Rass. dir. civ.*, 2009, 4, p. 1025 ss. In tema, si rinvia a P. PERLINGERI, *Mercato, solidarietà e diritti umani*, in *Rass. dir. civ.*, 1995, 1, p. 106, che sottolinea: «la libertà economica e la concorrenza, anche sul piano strettamente economico, sono non un fine ma un mezzo, una regola, per realizzare l'utilità sociale, l'effettiva partecipazione di tutti all'organizzazione economica e sociale del Paese e il pieno sviluppo della persona».

[13] Così G. DE CRISTOFARO, *La nozione generale di pratica commerciale «scorretta»*, in G. DE CRISTOFARO (a cura di), *Pratiche commerciali scorrette e codice del consumo. Il recepimento della direttiva 2005/29/CE nel diritto italiano (decreti legislativi nn. 145 e 146 del 2 agosto 2007)*, Torino, 2008, p. 153.

[14] V. PARLAMENTO EUROPEO, *Progetto di Risoluzione legislativa sulla proposta di direttiva del Parlamento europeo e del Consiglio relativa alle pratiche commerciali sleali tra imprese e consumatori nel mercato interno e che modifica le direttive 84/450/CEE, 97/7/CE e 98/27/CE (direttiva sulle prati-*

La definizione di «pratiche commerciali tra imprese e consumatori» di cui all'art. 2, par. 1, lett. *d*), dir. 2005/29/CE comprende, precisamente, «qualsiasi azione, omissione, condotta o dichiarazione, comunicazione commerciale ivi comprese la pubblicità e il *marketing*, posta in essere da un professionista, direttamente connessa alla promozione, vendita o fornitura di un prodotto ai consumatori».

Tale previsione va letta in combinato disposto con l'art. 5, par. 1, dir. che pone il divieto generale di pratiche commerciali sleali. La slealtà ricorre in presenza di due requisiti, entrambi necessari: *a*) la contrarietà della pratica commerciale alla diligenza professionale; *b*) la falsità o idoneità a falsare in misura rilevante il comportamento economico, in relazione al prodotto del consumatore medio che la pratica raggiunge o alla quale è diretta (o del membro medio di un gruppo, qualora la pratica sia diretta ad un determinato gruppo di consumatori).

La scelta legislativa di creare una locuzione amplissima di pratica commerciale (sleale) risponde alla *ratio* di includere il maggior numero di illeciti nella clausola generale di divieto [15]. Per di più, la direttiva, nella sua struttura «a piramide» o «a cerchi concentrici» [16], prevede una molteplicità di livelli di divieto. Il movimento legislativo della fonte comunitaria procede, infatti, dal generale al particolare, con una progressione di proibizioni via via più dettagliate che, appunto, nella metafora proposta dagli interpreti, integrano i singoli livelli della «piramide normativa».

Ecco, dunque, che la previsione di più ampio respiro, contenuta nell'art. 5 dir., fissa il divieto generale di pratiche commerciali sleali, variamente arricchito dall'apparato definitorio dell'art. 2 dir.; il divieto generale è poi integrato da clausole «intermedie», che proibiscono le due *subspecies* di pratiche commerciali ingannevoli e aggressive, *ex* artt. 6-8 dir. Tali clausole sono dette anche *small general clauses*, in ragione della minore ampiezza che le caratterizza rispetto alla fattispecie dell'art. 5 dir. [17]; infine, l'allegato I dir. censisce le due «liste nere» di pratiche «in ogni caso» vietate, perché ritenute sempre ingannevoli o aggressive.

---

che commerciali sleali), (COM (2003) 356 – C5-0288/2003 – 2003/0134 (COD)), emendamento n. 29. La parte fra virgolette è ripresa dall'ulteriore COMMISSIONE EUROPEA, *Parere per l'ambiente, la sanità pubblica e la politica dei consumatori destinato alla commissione giuridica e per il mercato interno sulla proposta di direttiva del Parlamento europeo e del Consiglio relativa alle pratiche commerciali sleali tra imprese e consumatori nel mercato interno e che modifica le direttive 84/450/CEE, 97/7/CE e 98/27/CE (direttiva sulle pratiche commerciali sleali)*, 21 gennaio 2004, (COM (2003) 356 – C5-0288/2003 – 2003/0134 (COD)). Entrambi i testi citati sono consultabili su *www.europarl.europa.eu*.

[15] V. N. ZORZI GALGANO, *Il contratto di consumo e la libertà del consumatore*, in F. GALGANO (diretto da), *Tratt. dir. comm. e dir. pubblico dell'econom*., Padova, 2012, *passim* e spec. p. 104. Mi permetto di rinviare altresì a I. SPEZIALE, *Le pratiche commerciali scorrette nell'evoluzione della normativa e del mercato*, Milano, 2024, *passim* e spec. p. 9 e p. 119.

[16] Sul punto, v. M. LIBERTINI, *Clausola generale e disposizioni particolari nella disciplina delle pratiche commerciali scorrette*, in *Contr. e impr*., 2009, 1, p. 79 ss.

[17] Così H. MICKLITZ, *The General Clause On Unfair Practices*, in G. HOWELLS-H. MICKLITZ-T. WIHELMSSON (a cura di), *European Fair Trading Law. The Unfair Commercial Practices Directive*, Hampshire England-Burlington USA, 2006, p. 85.

Tra l'altro, il legislatore europeo ha preso atto della necessità di adattare il diritto dell'Unione sulla tutela dei consumatori all'evoluzione continua del mercato e degli strumenti digitali. Pertanto, la dir. 2019/2161/UE (c.d. direttiva *Omnibus*) è intervenuta ad integrare le definizioni intermedie di azioni e di omissioni ingannevoli, nonché ad aggiornare l'elenco delle pratiche «in ogni caso» ingannevoli. La stessa direttiva, peraltro, ha modificato la fonte comunitaria del 2005, sostituendo l'art. 13 sulle sanzioni, le quali sono state riviste e inasprite, e aggiungendo l'art. 11 *bis*, che ha introdotto rimedi «proporzionati ed effettivi», al fine di garantire tutela al singolo consumatore leso da una pratica commerciale vietata.

Si aggiunga che la direttiva 1993/13/CEE, all'art. 3, definisce abusiva una clausola contrattuale che non è stata oggetto di negoziato individuale e che, in contrasto con il requisito della buona fede, determina a danno del consumatore un significativo squilibrio dei diritti e degli obblighi derivanti dal contratto.

Tale direttiva ha natura di armonizzazione minima ed è stata, quindi, la base su cui i singoli ordinamenti nazionali hanno eretto una più dettagliata e stringente tutela in favore dei contraenti consumatori. Nel nostro sistema legislativo, ad esempio, l'art. 33 c. cons. prevede un elenco particolarmente strutturato di clausole che si presumono vessatorie fino a prova contraria. L'accertamento del carattere di vessatorietà di una clausola, secondo quanto previsto dal successivo art. 34, determina, quale conseguenza, la nullità parziale di protezione, di cui all'art. 36 c. cons. Quest'ultimo, al co. 2, individua poi tre tipologie di clausole che, quantunque oggetto di trattativa privata, sono da ritenersi comunque nulle. Si tratta, in particolare, delle clausole che abbiano per oggetto o per effetto: *a*) l'esclusione o la limitazione della responsabilità professionale in caso di morte o danno alla persona del consumatore risultante da un fatto commissivo o da un'omissione del professionista; *b*) l'esclusione o la limitazione dei diritti processuali del consumatore nei confronti del professionista in caso di inadempimento totale o parziale o di adempimento inesatto da parte del professionista stesso; *c*) l'estensione dell'adesione del consumatore a clausole che questi non ha avuto, di fatto, la possibilità di conoscere prima della conclusione del contratto.

La Corte di giustizia dell'Unione europea ha, inoltre, contribuito, tramite una lettura talvolta "creativa" della dir. 1993/13/CEE, ad estenderne ulteriormente i confini di tutela. Basti l'esempio delle pronunce sul potere-dovere del giudice di rilevare d'ufficio l'illiceità di una clausola abusiva. Tale potere-dovere è stato riconosciuto sin dal noto caso *Oceano* del 2000 [18], per poi essere progressivamente esteso fino al

[18] V. CORTE CE, 27 giugno 2000, *Océano Grupo Editorial*, procedimenti riuniti da C-240/98 a C-244/98, in *www.eur-lex.europa.eu*, punto 28, laddove la Corte ha riconosciuto come sia «difficilmente concepibile che il giudice, chiamato a dirimere una controversia su un contratto determinato contenente una clausola abusiva, non possa disapplicarla solo perché il consumatore non ne fa valere l'illiceità». Secondo i magistrati europei, tale potere-dovere del giudice costituisce, anzi, un mezzo idoneo per conseguire gli obiettivi fissati dalla fonte del 1993. «Del resto, (…) il sistema di tutela istituito dalla direttiva si basa sull'idea che la disuguaglianza tra il consumatore e il professionista possa

gruppo di decisioni del 17 maggio 2022 in cui la Grande Sezione ha ammesso la rilevabilità d'ufficio persino dopo che sia stata già promossa l'azione esecutiva sulla base di un decreto ingiuntivo non opposto e, quindi, divenuto definitivo. Nelle menzionate sentenze, la Corte di Giustizia non tace sulla rilevanza del giudicato, ma fa prevalere «l'esigenza di una tutela giurisdizionale effettiva», «tenuto conto della natura e dell'importanza dell'interesse pubblico sotteso alla tutela che la direttiva 93/13 conferisce ai consumatori». Il principio di diritto formulato dai magistrati europei ha trovato applicazione nella pronuncia della Cassazione a Sezioni unite del 6 aprile 2023 [19] che «piega alle necessità del caso "consumeristico" una serie di istituti processuali che, sinora, avevano ricevuto una diversa applicazione» [20].

Anche nel caso della disciplina sulle clausole abusive, la direttiva *Omnibus* è intervenuta ad aggiornare il testo legislativo europeo, senza tuttavia prevederne modifiche sostanziali, ma limitandosi ad inasprirne l'apparato sanzionatorio. Precisamente, nella trama della direttiva del '93, viene inserito l'art. 8 *ter* che, nel primo par., impone agli Stati membri di adottare misure effettive, proporzionate e dissuasive. Il par. 2 aggiunge una serie di criteri, «non esaustivi e indicativi», di cui tenere conto ai fini dell'erogazione delle sanzioni ove appropriati [21]. Lo stesso identico elenco è stato inserito, al contempo, nella direttiva sulle pratiche commerciali sleali, ad ulteriore conferma dei molteplici punti di contatto tra queste due discipline.

---

essere riequilibrata solo grazie ad un intervento positivo da parte di soggetti estranei al rapporto contrattuale» (punto 27). Analogo percorso interpretativo ricorre (pressoché) in tutta la giurisprudenza UE successiva: v., *ex multis*, Corte CE, 9 novembre 2010, *Pénzügyi Lìzing*, C-137/08, in *Racc*., 2010, p. I-10847 ss., che ammette la possibilità di un'istruttoria d'ufficio per accertare la natura abusiva di una clausola contrattuale; Corte CE, 14 giugno 2012, *Banco Español de Crédito SA*, C-618/10, in *Foro it*., 2013, IV, c. 170 (s.m.), sulla rilevabilità d'ufficio dell'abusività di una clausola già nella fase sommaria del procedimento monitorio; Corte UE, 14 marzo 2013, *Mohamed Aziz*, C-415/11, in *www.curia.europa.eu*, che ha riconosciuto al giudice dell'esecuzione il potere di emanare provvedimenti di provvisoria sospensione del processo esecutivo avviato sulla base di un titolo esecutivo contenente una clausola contrattuale abusiva.

[19] V. Cass., sez. un., 6 aprile 2023, n. 9479, in *judicium.it*, con nota di B. CAPPONI, *Il G.E. e la Cass., SS.UU., 6 aprile 2023, n. 9479*. Tale sentenza rivede quanto già deciso in Cass., sez. un., 12 dicembre 2014, n. 26242, commentata (insieme alla sua gemella n. 26243) su tutte le principali riviste scientifiche (v., *ex multis*, A. PROTO PISANI, *Rilevabilità d'ufficio della nullità contrattuale: una decisione storica delle sezioni unite*, in *Foro it.*, 2015, I, c. 944 ss.).

[20] Così B. CAPPONI, *Primissime considerazioni su SS. UU. 6 aprile 2023 n. 9479*, in *giustiziainsieme.it*, 19 aprile 2023.

[21] L'elenco dettagliato ricomprende: *a*) natura, gravità, entità e durata della violazione; *b*) eventuali azioni intraprese dal professionista per attenuare il danno subito dai consumatori o per porvi rimedio; *c*) eventuali violazioni commesse in precedenza dal professionista; *d*) i benefici finanziari conseguiti o le perdite evitate dall'imprenditore in conseguenza della violazione; *e*) le sanzioni inflitte per la medesima violazione in altri Stati membri, se simili informazioni sono disponibili; *f*) ulteriori fattori aggravanti o attenuanti applicabili alle circostanze del caso.

3. La portata precettiva dell'art. 12, lett. *g*), DGA ed i suoi profili critici.

Una volta inquadrato il contesto normativo richiamato dall'art. 12, lett. *g*), DGA, è bene soffermarci ora sulla portata precettiva di quest'ultima previsione.

Essa va letta unitamente al *Considerando* n. 36 DGA, secondo il quale «si prevede che i fornitori di servizi di intermediazione dei dati dispongano di procedure e misure tese a imporre sanzioni per le pratiche fraudolente o abusive in relazione ai soggetti che richiedono l'accesso tramite i loro servizi di intermediazione dei dati, anche attraverso misure quali l'esclusione degli utenti di dati che violano i termini del servizio o il diritto vigente».

Il legislatore parrebbe così esaminare lo stesso fenomeno in due momenti distinti, laddove, da un lato, l'art. 12, lett. *g*) richiede al fornitore di servizi di intervenire *ex ante*, adottando misure non meglio specificate volte a prevenire forme di abuso; dall'altro, il *Considerando* n. 36, nella prospettiva rimediale, richiede al medesimo fornitore di servizi di imporre sanzioni in capo al responsabile della violazione.

Appare significativo che la disposizione da ultimo richiamata, pur priva di diretta portata cogente, risulti più chiara e completa rispetto al successivo art. 12, lett. *g*), nella misura in cui, anche se a titolo meramente esemplificativo, ipotizza una possibile sanzione irrogabile a carico del soggetto – impresa privata, impresa pubblica o ente pubblico che agisca *iure privatorum*, ovvero ente pubblico che agisca in funzione autoritativa e nell'interesse generale – che «richied[a] l'accesso tramite i suoi servizi di intermediazione dei dati».

In merito, sorge un primo problema relativo ai soggetti cui la fattispecie legislativa si riferisce. Mentre è chiaro che il fornitore dei servizi di intermediazione dei dati sia il soggetto tenuto a rispettare l'obbligo prescritto dalla lett. *g*), tutt'altro che chiaro è, invece, chi siano i potenziali destinatari dell'intervento preventivo (e/o sanzionatorio, e, quindi, successivo stante il *Considerando* n. 36) inclusi nella locuzione di «soggetti che richiedono l'accesso [ai dati] tramite i (…) servizi di intermediazione dei dati».

Poniamo, ad esempio, il caso di un servizio di cooperativa di dati – che, come noto, rientra tra i servizi di intermediazione dei dati previsti dal DGA – che trasferisca i dati dei suoi membri ad un soggetto terzo, pubblico o privato, che li utilizzi nel contesto di un'attività di impresa. In una simile situazione, la menzionata lett. *g*) graverebbe di un obbligo di tutela (preventiva) la cooperativa di dati, quale figura soggettiva a sé, e, al contempo, proteggerebbe i singoli membri della cooperativa, quali destinatari della tutela (preventiva), di fronte al soggetto terzo che, nello svolgimento della propria attività di impresa, accede ai dati.

Tale risultato, pur convincente, è ottenuto – però – per via esegetica, dal momento che, si ribadisce, la normativa predilige una locuzione aperta che costringe l'interprete allo sforzo di individuare correttamente il relativo ambito soggettivo di applicazione.

Va rilevato che il DGA e, in particolare, l'art. 12, lett. *g*) richiede un necessario

collegamento con le discipline a tutela dei consumatori di matrice europea e, specialmente, con le summenzionate direttive 2005/29 e 1993/13, in ragione del rinvio espresso ai concetti di «pratiche fraudolente o abusive».

A dire il vero, quest'ultima scelta lessicale desta più di qualche perplessità perché, anziché attingere ai consolidati concetti giuridici di pratica commerciale sleale e/o di clausola abusiva, introduce termini finora inediti. Da un lato, l'aggettivo "fraudolento" rappresenta una vera e propria novità nel panorama della normativa consumeristica UE; dall'altro, la "pratica abusiva" sembra sommare in sé i due concetti, ben noti, di pratica commerciale scorretta e clausola abusiva [22].

Purtuttavia, la questione appare più teorica che pratica, laddove parrebbe davvero difficile ipotizzare che il legislatore europeo intendesse qui riferirsi ad altro rispetto alle fattispecie di abuso commerciale e contrattuale già previste e ampliamente sanzionate sul mercato unico. Tali fattispecie, riportate all'interno delle direttive del 2005 e del 1993, imprimono al mercato un principio generale di correttezza che oggi chiaramente riguarda anche le attività di trattamento e di scambio di dati e, quindi, le questioni legate alla loro *governance*.

Infine, occorre rilevare il silenzio del legislatore sulle singole procedure che il fornitore di servizi di intermediazione dei dati è chiamato ad attivare per prevenire le «pratiche fraudolente o abusive». Sarebbe (stato) opportuno che lo stesso legislatore europeo intervenisse per colmare tale silenzio esplicitando le menzionate procedure. A tal fine, sarebbe auspicabile anche solo un atto di *soft law* che definisca "a monte" le procedure necessarie, ovvero ne fissi (almeno) alcuni aspetti essenziali, demandando alla regolamentazione "a valle" dei singoli Stati membri la puntuale precisazione delle procedure stesse.

Nell'attesa di un intervento normativo *ad hoc*, il fornitore di servizi di intermediazione dei dati può modulare la propria azione preventiva, prendendo spunto dal *framework* europeo a tutela dei consumatori che, in più fonti, impone stringenti obblighi informativi a carico del professionista. Ecco, dunque, che il fornitore di servizi dovrà, nelle interazioni verbali e scritte con tutti i destinatari di tali servizi, predisporre un'informativa il più possibile dettagliata e completa, volta proprio ad arginare e/o prevenire possibili abusi.

Inoltre, il fornitore, nello stabilire le condizioni generali dei contratti atipici con cui realizza le proprie attività di *business*, dovrà evitare il ricorso a clausole definibili come abusive, perché idonee a determinare un significativo squilibrio fra i diritti e gli obblighi derivanti dal contratto; o, comunque, nell'ipotesi in cui il ricorso

---

[22] Si segnala qui anche il *Considerando* n. 28 del Reg. (UE) 1689/2024 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale), il quale paventa il rischio che l'intelligenza artificiale, se utilizzata impropriamente, possa «fornire strumenti nuovi e potenti per pratiche di manipolazione, sfruttamento e controllo sociale». E aggiunge: «Tali pratiche sono particolarmente dannose e *abusive* e dovrebbero essere vietate (…)» (il corsivo è mio).

a clausole siffatte dovesse apparire inevitabile, egli dovrà garantire che le stesse siano oggetto di apposite trattative individuali. In definitiva, le comunicazioni non aventi carattere negoziale, così come gli atti che integrino contratti (atipici), dovranno tutti essere predisposti in modo da risultare *compliant* alla normativa consumeristica e a tutela dei dati viste nel loro complesso.

Infine, come si è già anticipato, la lett. *g*) dell'art. 12 prevede unicamente un approccio preventivo, senza far riferimento all'eventuale apparato sanzionatorio che viene menzionato brevemente nel *Considerando* n. 36. Tale profilo sembra criticabile anche a fronte dell'assenza di carattere strettamente vincolante di quest'ultima disposizione.

La lett. *g*), limitandosi alla sola ottica di tutela *ex ante*, appare in tal senso incompleta. Al di là dello spunto offerto dal *Considerando* n. 36 che, lo si è detto, suggerisce, in via esemplificativa, la misura dell'esclusione degli utenti di dati che violino i termini del servizio o il diritto vigente, è possibile, ancora una volta, guardare alle discipline UE esistenti. Il dialogo tra il DGA e le due direttive sulle pratiche commerciali sleali e sulle clausole abusive lascia immaginare un dialogo (proficuo) anche tra le autorità amministrative preposte all'applicazione delle relative normative.

Nella ricostruzione qui ipotizzata, il fornitore di servizi di intermediazione dei dati che non rispetti la condizione di cui all'art. 12, lett. *g*), DGA si vedrà applicare dall'Agenzia per l'Italia digitale (AgID) le sanzioni pecuniarie oggi contemplate dall'art. 4 del d.lgs. 7 ottobre 2024, n. 144 [23]. L'AgID è, infatti, l'*Authority* che il nostro Paese ha indicato come competente per i servizi di intermediazione dei dati, adeguandosi a quanto richiesto, in proposito, dall'art. 13 DGA [24]. Al contempo, lo stesso fornitore di servizi di intermediazione dei dati e/o – forse più propriamente – chi richiede l'accesso ai suoi servizi, laddove si rendano responsabili di un'attività illecita riconducibile alle nozioni legislative di pratica commerciale scorretta o di clausola abusiva, potranno essere sanzionati dall'Autorità garante della concorrenza e del mercato (AGCM) nei termini previsti dal codice del consumo [25].

Diviene così necessario, oltre che opportuno, che le due autorità promuovano «una stretta e leale cooperazione», come d'altronde suggerito dall'art. 2, co. 2, d.lgs. n. 144/2024, in linea con l'art. 13, ult. par., DGA, «potendo, altresì, a tal fine, stipulare specifici accordi di collaborazione non onerosi».

---

[23] Tale decreto legislativo prevede le «Norme di adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio, del 30 maggio 2022, relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724». L'art. 4, comma 1 prevede la possibilità di comminare «sanzioni amministrative pecuniarie da un minimo di euro 10.000 fino a un massimo di euro 100.000, ovvero, per le imprese, fino al 6 per cento del fatturato mondiale totale annuo dell'esercizio precedente».

[24] V., sul punto, l'art. 2 d.lgs. n. 144 del 2024, menzionato *infra* anche nel testo.

[25] Cfr., rispettivamente, artt. 27 e 37-*bis* c. cons.

Capitolo XLII

Cooperative di dati e adozione di misure adeguate per garantire l'interoperabilità con altri servizi di *data intermediation*

Cristina Chilin

Abstract: The purpose of this paper is to analyse the condition for the provision of data intermediation services in Art. 12(1)(i) of the Data Governance Act, and in particular: the meaning attributable to the expression "appropriate measures" to be taken by the data cooperative to ensure interoperability; how to manage interoperability with other data brokering services; and finally, how to identify commonly used open standards useful for taking security measures.

1. Premesse.

L'art. 12 del Reg. (UE) 2022/868 del Parlamento Europeo e del Consiglio del 30 maggio 2022 relativo alla *governance* europea dei dati e che modifica il Reg. (UE) 2018/1724 (Regolamento sulla *governance* dei dati) [1] (in seguito per brevità anche solo *Data Governance Act* o DGA) disciplina quali sono le condizioni per la fornitura di servizi di intermediazione dei dati.

[1] Il Regolamento sulla *governance* dei dati: Regolamento (UE) 2022/868 del Parlamento Europeo e del Consiglio del 30 maggio 2022 *relativo* alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 è stato pubblicato in G.U.U.E. con L. 152/1 il 3 giugno 2022 ed è entrato in vigore venti giorni dopo la data di pubblicazione, ma risulta applicabile ai sensi dell'art. 38 DGA dal 24 settembre 2023. Tale fonte normativa disciplina essenzialmente tre argomenti: *a*) il riuso dei dati personali e non personali gestiti dalla pubblica amministrazione; *b*) i servizi di intermediazione dei dati personali e non personali; *c*) l'altruismo dei dati.

Il presente contributo si propone di commentare – con specifico riferimento al servizio di intermediazione svolto in forma di cooperative di dati – la condizione di cui alla lett. *i*) dell'art. 12 del DGA, ove si prevede che «*il fornitore di servizi di intermediazione dei dati adotta misure adeguate per garantire l'interoperabilità con altri servizi di intermediazione dei dati, tra l'altro mediante norme aperte di uso comune nel settore in cui opera il fornitore di servizi di intermediazione dei dati*».

Obiettivo del presente contributo è quello di analizzare criticamente il tenore di tale disposizione, prestando attenzione: *a*) al significato che il legislatore abbia voluto attribuire alla locuzione «misure adeguate», che la cooperativa di dati dovrà adottare per garantire l'interoperabilità; *b*) alle modalità di gestione dell'«interoperabilità con altri servizi di intermediazione dei dati»; ed infine *c*) a come vadano individuate le «norme aperte di uso comune».

2. Le «misure adeguate» per garantire l'interoperabilità previste dall'art. 12, par. 1, lett. *i*), DGA.

Primariamente bisogna comprendere quale sia il significato da attribuire al concetto di «misure adeguate», che l'intermediario dovrà adottare per garantire l'interoperabilità con altri servizi di intermediazione.

Nel DGA non si rinviene alcuna definizione di «misura», che quindi dovrà essere ricercata in alti testi normativi. Il regolamento si limita ad indicare la peculiarità della stessa, che dovrà essere caratterizzata da adeguatezza o ragionevolezza [2], concetti entrambi connotati da relatività, discrezionalità e ampiezza.

Nella ricerca di una definizione di "misure adeguate" non si può non citare anche altre due disposizioni contenute nel predetto regolamento che aiutano a comprendere il contesto in cui tali misure si inseriscono. Difatti, tra le condizioni per la fornitura dei servizi di intermediazione dei dati che sono richieste all'intermediario nello svolgimento del proprio servizio, emerge il concetto di «misura» alla lett. *j*) dell'art. 12 DGA ove «il fornitore di servizi di intermediazione dei dati mette in atto *adeguate misure* tecniche, giuridiche e organizzative al fine di impedire il trasferimento di dati non personali o l'accesso a questi ultimi nel caso in cui ciò sia illegale a norma del diritto dell'Unione o del diritto nazionale dello Stato membro interessato» ed anche alla lett. *l*) dell'art. 12 DGA, ove si prevede che «il fornitore di servizi di intermediazione dei dati adotta le *misure* necessarie per garantire un *adeguato* livello di sicurezza per la conservazione, il trattamento e la trasmissione di dati non personali, e il fornitore di servizi di intermediazione dei dati assicura inoltre il massimo livello di sicurezza per la conservazione e la trasmissione di informazioni sensibili sotto il profilo della concorrenza».

Si tratta di disposizioni che pare possano in qualche modo identificarsi o co-

[2] Cfr. *considerando* n. 34 del DGA.

munque rapportarsi, per la terminologia utilizzata («*misure adeguate*» «*adeguate misure tecniche, giuridiche e organizzative*» «*misure necessaria a garantire un adeguato livello di sicurezza*»), con le misure tecniche e organizzative di cui all'art. 32 GDPR, in una sorta di prospettiva di continuità [3], soprattutto con riferimento alla dimensione della disponibilità dei dati e dell'accesso ad essi.

Tale articolo prevede che il titolare e/o il responsabile del trattamento dovrà adottare nell'attività di trattamento misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio, tenendo conto dei seguenti criteri: lo stato dell'arte, i costi di attuazione delle misure di sicurezza, la natura, l'oggetto, il contesto e le finalità del trattamento e il rischio di compressione o violazione dei diritti e delle libertà delle persone fisiche [4].

La misura tecnica e organizzativa consiste in una vera e propria obbligazione *ex lege* da parte del titolare e/o del responsabile del trattamento [5], che ai sensi dell'art. 32 GDPR potrà essere identificata – a titolo meramente esemplificativo essendo questa una norma "aperta" – in: «*a)* la pseudonimizzazione e la cifratura dei dati personali; *b)* la capacità di assicurare su base permanente la riservatezza, l'integrità, la *disponibilità* e la resilienza dei sistemi e dei servizi di trattamento; *c)* la capacità di ripristinare tempestivamente la *disponibilità* e l'*accesso* dei dati personali in caso di incidente fisico o tecnico; *d)* una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento» [6]. Le misure a cui si fa riferimento nella lett. *i*) dell'art. 12 DGA, dunque, possono essere intese come tutti quegli accorgimenti (attività, dispositivi, procedure, etc.) di natura tecnica e organizzativa che consentono di assicurare l'interoperabilità dei dati con altri dati e servizi, rendendo il dato iniziale *disponibile* ed *accessibile* anche in altro contesto, per la fruizione da parte di altri (*data user*).

Con riferimento inoltre all'aggettivo "*adeguato*", l'*European Data Protection*

---

[3] Si evidenzia come il concetto di misure tecniche e organizzative non è una novità introdotta dal GDPR, ma una prosecuzione della previgente normativa. Infatti, il d.lgs. n. 196/2003 (c.d. Codice della privacy), prima dell'entrata in vigore del GDPR, disciplinava agli artt. 33-35 e all'allegato B le misure minime di sicurezza. Per un commento alla pregressa disciplina si rimanda a G. FINOCCHIARO, *Privacy e protezione dei dati personali. Disciplina e strumenti operativi*, Bologna, 2012, pp. 254 ss. Per un commento invece all'art. 32 si veda M.S. ESPOSITO, *Commento all'art. 32* GDPR, in R. D'ORAZIO-G. FINOCCHIARO-O. POLLICINO-G. RESTA (a cura di), *Codice della privacy e data protection*, Milano, 2021, p. 503 ss.

[4] A tal proposito *European Dara Protection Board* (EDPB) prevede che «Le espressioni misure tecniche e organizzative e necessarie garanzie possono essere intese in senso lato come qualsiasi metodo o mezzo che un titolare può impiegare nel trattamento». EDPB, *Linee Guida 4/2019 sull'articolo 25 – Protezione dei dati fin dalla progettazione e per impostazione predefinita*, adottate il 20 ottobre 2020, p. 6.

[5] In materia si veda l'ampia trattazione di S. FAILLACE, *La controversa categoria delle obbligazioni* ex lege, Milano, 2023, *passim* e, ivi, spec. p. 171 ss.

[6] Art. 32, par. 1, GDPR.

Supervisor (EDPS) ritiene che questo termine «*implies that the measures should take account of the context and the specific circumstances of the case*»[7], quindi le misure di sicurezza dovranno essere sia idonee alle finalità previste dal trattamento, che efficaci a garantire la tutela della protezione dei dati personali[8].

Appurato che nel *Data Governance Act* tali misure possano essere ricondotte a quelle, tecniche e organizzative, di cui all'art. 32 del GDPR, in una prospettiva di continuità e complementarità, è opportuno evidenziare come nei due testi normativi le misure vengono trattate da angolazioni diverse, presentando evidenti tratti differenziali: *(i)* una prima differenza riguarda i soggetti obbligati all'adozione di tali misure, *(ii)* una seconda differenza riguarda la natura dei dati oggetto di protezione da parte delle misure di sicurezza e, infine, *(iii)* un'ultima differenza si rinviene nello scopo per le quali tali misure dovranno essere adottate.

Con riferimento alla prima questione, le misure tecniche e di sicurezza nel GDPR sono adottate dal titolare o dal responsabile del trattamento, in virtù del principio di integrità e riservatezza (ovvero di sicurezza)[9] e del principio di *accountability*[10]; mentre nel DGA queste dovranno essere adottate dal fornitore dei servizi di intermediazione, quindi dalla cooperativa di dati, salvo poi a verificare se rivesta anche il ruolo di titolare o di responsabile del trattamento.

Con riferimento alla seconda differenza, le misure di sicurezza tecniche e organizzate nel GDPR vengono adottare dal titolare e/o dal responsabile per "proteggere" l'interessato dai rischi che derivano dal trattamento di dati a lui riferibili, avente pertanto ad oggetto di dati esclusivamente di natura personale[11]; mentre nel DGA,

---

[7] EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion on the data protection reform package*, adottata 7 marzo 2012, p. 28.

[8] Sulla connessione tra il requisito dell'adeguatezza e quello di efficacia delle misure tecniche e organizzative si rimanda a EUROPEAN DARA PROTECTION BOARD, *Linee Guida 4/2019 sull'articolo 25 – Protezione dei dati fin dalla progettazione e per impostazione predefinita*, cit., p. 7 e ss.

[9] G.M. BILOTTA-D. SBORLINI-I. SCARPELLI, *Il principio di integrità e riservatezza (rectius, di sicurezza)*, in F. BRAVO (a cura di), *Dati Personali. Protezione, libera circolazione e governance. 1. Principi*, Pisa, 2023, p. 333 ss.

[10] Per una disamina del principio dell'*accountability* si rimanda integralmente a F. ALBANESE-I. CARDINALI, *Il principio di responsabilizzazione (accountability)*, in F. BRAVO (a cura di), *Dati Personali. Protezione, libera circolazione e governance. 1. Principi*, cit., p. 501 ss.

[11] Per quanto riguarda i dati di natura non personale, il Reg. (UE) 2018/1807 del Parlamento europeo e del Consiglio del 14 novembre 2018 relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea nulla prevede sull'adozione di misure di sicurezza tecniche e organizzative se non limitatamente alla necessità di protezione dal rischio di incidenti a danni delle rete informatiche da parte dei «fornitori di servizi digitali di adottare misure tecniche e di sicurezza adeguate e proporzionate alla gestione dei rischi posti alla sicurezza della rete e dei sistemi informativi che utilizzano. Tali misure sono intese a garantire un livello di sicurezza adeguato al rischio esistente e dovrebbero tenere conto della sicurezza dei sistemi e degli impianti, del trattamento degli incidenti, della gestione della continuità operativa, del monitoraggio, degli audit e test e della conformità con le norme internazionali». Cfr. *considerando* n. 36. Sulla sicurezza delle reti e dei sistemi di in-

sia dalla norma oggetto di commento che dalle ulteriori condizioni rilevanti previste dall'art. 12 cit. (cfr. art. 12, par. 1, lett. *j*) ed *l*)), emerge che tali misure servono sia per i dati di natura personale che non personale.

Infine, anche con riferimento allo scopo che le normative prendono in considerazione per l'adozione delle misure di sicurezza tecniche e organizzative "adeguate", risultano ulteriori divergenze: secondo il GDPR la finalità della misura ha una portata più ampia, tanto che è volta a garantire per ogni trattamento un livello di sicurezza adeguato al rischio, in tutte le dimensioni in cui la sicurezza è declinabile (riservatezza, integrità, disponibilità, etc.); mentre secondo il DGA – e in particolare la norma oggetto di commento – l'adozione della misura servirebbe a soddisfare un ambito più circoscritto e un unico trattamento, ossia la sola interoperabilità con altri dati e con altri servizi di intermediazione dei dati, garantendo l'ampia *disponibilità* del dato per gli impieghi a cui tende l'attività di intermediazione.

Nel DGA lo scenario che si delinea è il seguente: la cooperativa di dati riceve dai propri membri (interessati, imprese individuali o PMI) una serie di dati, personali o non personali, per svolgere un servizio di intermediazione tra questi ultimi e l'utente di dati [12]. La fornitura di tale servizio, come recita l'art. 12 del DGA, richiede che vengano rispettate dall'intermediario una serie di condizioni, tra cui quella indicata alla lett. *i*), ove si prescrive l'azione di misure adeguate (quindi misure tecniche e organizzative idonee a raggiungere lo scopo, tenendo conto del contesto in cui vanno applicate) per garantire l'interoperabilità con altri (dati e) servizi di intermediazione dei dati.

Occorre quindi ora approfondire i concetti di interoperabilità e di servizi di intermediazione dei dati per comprenderne le modalità di gestione degli stessi da parte della cooperativa di dati.

Lo standard ISO/IEC 2382-01 definisce l'interoperabilità come «*the capability of a program to be executed on various types of data processing systems without converting the program to a different language and with little or no modification*» [13]. Tale concetto – per essere compreso appieno nel contesto del DGA – deve necessariamente essere letto in combinato disposto con l'altra condizione per la fornitura di servizi di intermediazione dei dati, prevista all'art. 12, par. 1, lett. *d*),

---

formazione si vedano anche Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione e la Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva 2016/1148 (direttiva NIS 2).

[12] La definizione di utente di dati è prevista dall'art. 2, par. 1, n. 9, DGA, ove si intende «una persona fisica o giuridica che ha accesso legittimo a determinati dati personali o non personali e che ha diritto, anche a norma del regolamento (UE) 2016/679 in caso di dati personali, a utilizzare tali dati a fini commerciali o non commerciali».

[13] Consultabile in *Information technology*, *Vocabulary*, Part 1: *Fundamental terms*, https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:-1:ed-3:v1:en.

ove si prevede che «il fornitore di servizi di intermediazione dei dati agevola lo scambio dei dati nel formato in cui li riceve da un interessato o da un titolare dei dati, li converte in formati specifici solo allo scopo di migliorare l'interoperabilità a livello intrasettoriale e intersettoriale, se richiesto dall'utente dei dati, se prescritto dal diritto dell'Unione o per garantire l'armonizzazione con le norme internazionali o europee in materia di dati e offre agli interessati o ai titolari dei dati la possibilità di non partecipare a tali conversioni, a meno che la conversione non sia prescritta dal diritto dell'Unione».

Da tali norme si può ricavare che l'intermediario in un primo momento riceva dati, personali o non personali, da parte di interessati o titolari dei dati, per richiedere il servizio di ausilio allo scambio (quindi all'utilizzazione e alla condivisione) con l'utente dei dati in un determinato formato digitale. Potrebbe capitare che il *set* di dati ricevuto non sia leggibile dal dispositivo dell'utilizzatore oppure che questi voglia leggerlo in un formato specifico, così quest'ultimo (il *data user*) per migliorarne l'interoperabilità (quindi la trasmissione e la leggibilità del *set* di dati) chiederà all'intermediario di dati di convertire il *file* (contenente i dati) nel formato che preferisce («*formato specifico*») (cfr. lett. *d*) art. 12 DGA). Pertanto, per consentire tale conversione l'intermediario – e questo è il passaggio delineato dalla lett. *i*), cit. – dovrà adottare delle "misure adeguate" ai fini dell'interoperabilità dei dati (anche) con altri servizi di intermediazione.

Soprassedendo sulla perplessità di formulazione della lett. *d*) dell'art. 12 cit. e concentrandoci sulla lett. *i*) emerge che primariamente bisognerà che l'intermediario dei dati identifichi la natura del *set* di dati (personale, non personale o mista) sul cui formato verranno adottate le misure per garantire l'interoperabilità dei dati. A seconda della natura del dato si dovranno infatti adottare misure proporzionate e adeguate al livello di rischio, che in caso di dati di natura personale saranno "più stringenti"; mentre in caso di dati di natura non personale potranno essere meno rigide. Per intenderci non sarà necessario adottare, per esempio, la misura di sicurezza della cifratura per dati di natura non personale, in quanto tale misura sarebbe irragionevole e non proporzionale rispetto alla finalità che il servizio di intermediazione dovrà perseguire nel trattamento richiesto dall'interessato o dal titolare dei dati, a meno che non si siano specifiche esigenze in relazione ad altri diritti da salvaguardare (ad es., tutela del *know-how* o di *data asset* di particolare rilevanza economica o strategica).

L'estrema genericità della norma in esame non consente di individuare nemmeno i criteri in base ai quali dovranno essere approntate le misure, né tantomeno consente di individuare la categoria di appartenenza di queste ultime: se di natura tecnica, di sicurezza o entrambe le tipologie, come sembrerebbe logico dedurre.

3. L'interoperabilità «con altri servizi di intermediazione di dati».

Alla cooperativa di dati, alla lett. *i*) cit., viene inoltre richiesto di adottare misure atte a garantire l'interoperabilità con altri servizi di intermediazione dei dati. Si tratta

di un passaggio anch'esso dotato di vaghezza ed estremamente difficoltoso da interpretare e da armonizzare con il restante testo del DGA.

Per servizio di intermediazione dei dati, definito dall'art. 2, par. 1, n. 11, DGA, si intende «un servizio che mira a instaurare, attraverso strumenti tecnici, giuridici o di altro tipo, rapporti commerciali ai fini della condivisione dei dati tra un numero indeterminato di interessati e di titolari dei dati, da un lato, e gli utenti dei dati, dall'altro, anche al fine dell'esercizio dei diritti degli interessati in relazione ai dati personali» [14] e all'art. 10 del DGA si catalogano i servizi di intermediazione in tre tipologie: *a*) servizi di intermediazione tra titolari dei dati e potenziali utenti di dati; *b*) servizi di intermediazione tra interessati e *c*) servizi di cooperative di dati.

Da una prima lettura della lett. *i*) cit. parrebbe che l'offerta di un servizio da parte dell'intermediario (ad es. per lo scambio di dati in un formato interoperabile) tra l'interessato-titolare dei dati e l'utente, non sia limitabile a un unico servizio ma utilizzabile anche per «*altri servizi*». Ciò porterebbe a ritenere che l'interessato o il titolare dei dati si rivolga alla cooperativa per il servizio di trasmissione dei dati all'utilizzatore che, nel rispetto della condizione di cui art. 12, par. 1, lett. *c*) del DGA, dovrà prevedere la conversione da parte dell'intermediario del *set* di dati fornito mediante formati specifici e in aggiunta consentirebbe l'utilizzazione di «altri servizi», servizi che, ai sensi dell'art. 12, par. 1, lett. *i*), sembrerebbero gli unici a essere "favoriti", sul piano dell'interoperabilità, dall'adozione di misure adeguate.

Una simile interpretazione non può certamente essere avallata, in quanto si creerebbe una differenziazione puramente discrezionale e non giustificabile – né giuridicamente, né tecnicamente – da parte del fornitore di servizi di intermediazione dei dati nella scelta di adozione delle misure adeguate per garantire l'interoperabilità solamente a favore di alcuni servizi di intermediazione. Il senso della norma, invece, è quello di garantire la possibilità di circolazione dei dati e la loro disponibilità, il che impone un'interpretazione quanto più ampia possibile, nel senso che l'interoperabilità dei dati deve essere effettuata sia per consentire l'utilizzo degli stessi in tutti i servizi offerti dal medesimo intermediario, sia per consentire il loro utilizzo con servizi forniti anche da altri intermediari, riconducibili alle lett. *a*), *b*) e *c*) dell'art. 10 del DGA.

---

[14] La norma prosegue escludendo i seguenti servizi: «*a*) servizi che ottengono dati dai titolari dei dati e li aggregano, arricchiscono o trasformano al fine di aggiungervi un valore sostanziale e concedono licenze per l'utilizzo dei dati risultanti agli utenti dei dati, senza instaurare un rapporto commerciale tra i titolari dei dati e gli utenti dei dati; *b*) servizi il cui obiettivo principale è l'intermediazione di contenuti protetti da diritto d'autore; *c*) servizi utilizzati esclusivamente da un titolare dei dati per consentire l'utilizzo dei dati detenuti da tale titolare dei dati, oppure utilizzati da varie persone giuridiche all'interno di un gruppo chiuso, anche nel quadro di rapporti con i fornitori o i clienti o di collaborazioni contrattualmente stabilite, in particolare quelli aventi come obiettivo principale quello di garantire la funzionalità di oggetti o dispositivi connessi all'internet delle cose; *d*) servizi di condivisione dei dati offerti da enti pubblici che non mirano a instaurare rapporti commerciali». Per un maggior approfondimento sul tema si veda F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in *Contratto e impresa europea*, 2021, 1, p. 199 e ss.

4. Interoperabilità e «norme aperte di diritto comune».

Infine, la lett. *i*) cit. dispone che l'intermediario adotti le predette misure «mediante norme aperte di uso comune nel settore in cui opera il fornitore di servizi dei dati». Si tratta di disposizione che va letta facendo riferimento a "norme tecniche" (standard tecnici), non a "norme giuridiche" [15]. Lo si evince dalla formulazione testuale della disposizione in esame, sia nella parte in cui richiama l'«uso comune» delle norme aperte, sia nella parte in cui rimarca una loro funzione strumentale («mediante») rispetto all'interoperabilità che deve essere attuata dall'intermediario.

L'obiettivo dell'Unione europea [16] è certamente quello di istituire spazi interoperabili comuni di dati in settori strategici (come quello dei trasporti e della sanità), tramite il dispiegamento di strumenti e piattaforme di condivisione di dati, la creazione di una *governance* di dati e un miglioramento a livello intrasettoriale ed intersettoriale dell'interoperabilità, ciò nonostante l'Europa non ha ancora fissato, sul piano giuridico, norme di dettaglio con cui prescrivere le condizioni tecniche per l'interoperabilità da attivare nei diversi settori.

Infatti, nonostante siano molteplici le norme [17] che trattano del concetto di interoperabilità – sia nell'ambito pubblico che nel settore privato – questo concetto viene disciplinato in termini solamente generali, tanto che – almeno nel settore privato – non si rinvengono, sul piano giuridico, norme *ad hoc* di dettaglio che stabiliscano le condizioni da soddisfare per realizzare l'interoperabilità dei dati [18].

---

[15] Nel primo caso il riferimento è all'uso di standard tecnico-informatici di uso comune nel settore di operatività dell'intermediario; nel secondo caso, invece, si alluderebbe alle c.d. *open norms* di natura giuridica, ossia a norme capaci di garantire flessibilità e adattamento agli sviluppi (ad es. tecnici ed economici) del sistema di riferimento. Si pensi, ad esempio, alle *open norms* in tema di *copyright*, definite come «*A broad and non-exhaustive copyright exception, where its scope is flexibly determined and interpreted through a set of general criteria that is complemented at the level of the courts by a holistic assessment of legal, cultural, societal, and technological developments*». Così D. MENDIS-B. WHITE-D. HONG, *Copyright and Open Norms in Seven Jurisdictions: Benefits, Challenges & Policy Recommendations*, 2024, p. 8, in *SSRN* (https://ssrn.com/abstract=4728782).

[16] Cfr. COMMISSIONE EUROPEA, *Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni, Una strategia europea per i dati*, 19 febbraio 2020, COM (2020) 66 final.

[17] Il concetto di interoperabilità lo troviamo in molteplici norme del diritto dell'unione europea, in particolare al *considerando* n. 68 del GDPR, al *considerando* nn. 2, 32, 34, 54 del DGA, al *considerando* nn. 4, 102, 151 e gli artt. 44, part. 1, lett. *f*), art. 85 del *Digital Service Act* e da ultimo anche nella Legge sull'intelligenza artificiale al *considerando* n. 81. Inoltre, il concetto di interoperabilità lo troviamo anche nella normativa italiana, al d.lgs. 196/2003, così come modificato dal d.lgs. n. 101/2018, all'art. 2-*sexies*, e nell'ambito pubblico nelle Linee guida sull'interoperabilità tecnica delle Pubbliche Amministrazioni e nelle Linee guida Tecnologie e standard per la sicurezza dell'interoperabilità tramite API dei sistemi informatici, art. 73, co. 3-*ter*, lett. *b*), del d.lgs. 7 marzo 2005, n. 82, entrambe adottate dall'AgID.

[18] Non si rinvengono, in materia di intermediazione dei dati, impianti normativi analoghi a quello contenuto nella Direttiva (UE) 2016/797 del Parlamento europeo e del Consiglio, dell'11 maggio

Risulta quindi confermato che, nel settore della fornitura del servizio di intermediazione dei dati, la seconda parte della condizione di cui alla lett. *i*) affida l'interoperabilità alle *norme tecniche* di uso comune affermatesi nella prassi di settore, di volta in volta selezionate dall'intermediario per garantire la corretta fornita del servizio.

2016, relativa all'interoperabilità del sistema ferroviario dell'Unione europea, in cui sono stabilite le condizioni da soddisfare per realizzare l'interoperabilità del sistema ferroviario in tutta l'UE, mediante un livello ottimale di armonizzazione tecnica a supporto dello sviluppo dei servizi di trasporto ferroviario.

Capitolo XLIII

Cooperative di dati e condizioni di sicurezza per i servizi di *data intermediation* nel *Data Governance Act*

Antonio Gammarota

Abstract: Article 12 of the Data Governance Regulation (EU) 2022/868 (DGA) sets out conditions that providers of data intermediation services must comply with. This contribution examines some issues relating to the security obligations set out in Article 12, points (g), (j), (l) DGA.

1. Premessa.

L'art. 2, n. 11, del Reg. UE n. 868/2022 [1], *Data Governance Act* (DGA), definisce il «Servizio di intermediazione dei dati» come «(...) un servizio che mira a instaurare, attraverso strumenti tecnici, giuridici o di altro tipo, rapporti commerciali ai fini della condivisione dei dati tra un numero indeterminato di interessati e di titolari dei dati, da un lato, e gli utenti dei dati, dall'altro».

I servizi di intermediazione sono assoggettati, fra le altre, alle norme del Capo III del DGA, e tra queste figurano quelle che riguardano i «Requisiti applicabili ai servizi di intermediazione dei dati».

Il Capo III viene aperto dall'art. 10, a tenore del quale la fornitura dei servizi di intermediazione dei dati è soggetta all'osservanza di due requisiti costituiti rispetti-

[1] Reg. UE n. 868/2022 (*Data Governance Act*), in Gazzetta ufficiale dell'Unione europea 3 giugno 2022, L 152/29.

vamente dall'onere di notifica all'autorità (art. 11 DGA) e dall'obbligo di conformità dei servizi alle condizioni (art. 12 DGA).

Va ricordato che al duplice requisito di notifica e di conformità previsto dall'art. 10 del DGA sono assoggettate diverse tipologie di intermediari di dati e, tra queste, anche le «Cooperative di dati» (art. 10, par. 1, lett. c), aspetto che costituisce particolare motivo di interesse ai fini della presente ricerca [2].

Quanto al requisito della notifica, si tratta dell'assoggettamento della fornitura di servizi alla procedura di notifica obbligatoria da svolgersi nei confronti dell'istituenda «autorità competente per i servizi di intermediazione dei dati» prevista e regolata dagli artt. 11, par. 1 e 13 DGA; per la disamina di tale requisito si rinvia al relativo commento in questa stessa opera.

Quanto invece al secondo requisito imposto dall'art. 10, esso è costituito dall'onere di conformità dei servizi di intermediazione alle condizioni elencate nell'art. 12 DGA.

Le norme che regolano tali requisiti, a loro volta, prevedono un'articolata serie di adempimenti posta a carico dell'intermediario.

2. L'art. 12 DGA sulle condizioni per la fornitura di servizi di intermediazione dei dati.

L'art. 12 [3] del DGA annovera un'articolata serie di «condizioni» alle quali la

---

[2] Cfr. F. BRAVO, *Le cooperative di dati*, in *Contratto e impresa*, 2023, 3, e in https://site.unibo.it/cooperative-di-dati, p. 16 ss.

[3] L'art. 12 DGA prevede quanto segue: «Condizioni per la fornitura di servizi di intermediazione dei dati. La fornitura di servizi di intermediazione dei dati di cui all'articolo 10 è soggetta alle condizioni seguenti:

a) il fornitore di servizi di intermediazione dei dati non utilizza i dati per i quali fornisce servizi di intermediazione dei dati per scopi diversi dalla messa a disposizione di tali dati agli utenti dei dati e fornisce servizi di intermediazione dei dati attraverso una persona giuridica distinta;

b) le condizioni commerciali, compresa la fissazione del prezzo, per la fornitura di servizi di intermediazione dei dati a un titolare dei dati o a un utente dei dati non sono subordinate al fatto che il titolare dei dati o l'utente dei dati utilizzi altri servizi forniti dallo stesso fornitore di servizi di intermediazione dei dati o da un'entità collegata, e, in caso affermativo, in che misura il titolare dei dati o gli utenti dei dati utilizzano tali altri servizi;

c) i dati raccolti su qualsiasi attività di una persona fisica o giuridica ai fini della fornitura del servizio di intermediazione dei dati, compresi la data, l'ora e i dati di geolocalizzazione, la durata dell'attività e i collegamenti con altre persone fisiche o giuridiche stabiliti dalla persona che utilizza il servizio di intermediazione dei dati, sono utilizzati solo per lo sviluppo di tale servizio di intermediazione dei dati, il che può comportare l'uso di dati per l'individuazione di frodi o a fini di cibersicurezza, e sono messi a disposizione dei titolari dei dati su richiesta;

d) il fornitore di servizi di intermediazione dei dati agevola lo scambio dei dati nel formato in cui li riceve da un interessato o da un titolare dei dati, li converte in formati specifici solo allo scopo di migliorare l'interoperabilità a livello intrasettoriale e intersettoriale, se richiesto dall'utente dei dati, se

fornitura del servizio di intermediazione di dati deve uniformarsi [4] e costituisce una

prescritto dal diritto dell'Unione o per garantire l'armonizzazione con le norme internazionali o europee in materia di dati e offre agli interessati o ai titolari dei dati la possibilità di non partecipare a tali conversioni, a meno che la conversione non sia prescritta dal diritto dell'Unione;

e) i servizi di intermediazione dei dati possono comprendere l'offerta di strumenti e servizi supplementari specifici ai titolari dei dati o agli interessati allo scopo specifico di facilitare lo scambio dei dati, come la conservazione temporanea, la cura, la conversione, l'anonimizzazione e la pseudonimizzazione, fermo restando che tali strumenti e servizi sono utilizzati solo su richiesta o approvazione esplicita del titolare dei dati o dell'interessato e gli strumenti di terzi offerti in tale contesto non utilizzano i dati per altri scopi;

f) il fornitore di servizi di intermediazione dei dati provvede affinché la procedura di accesso al suo servizio sia equa, trasparente e non discriminatoria sia per gli interessati e i titolari dei dati sia per gli utenti dei dati, anche per quanto riguarda i prezzi e le condizioni di servizio;

g) il fornitore di servizi di intermediazione dei dati dispone di procedure per prevenire pratiche fraudolente o abusive in relazione a soggetti che richiedono l'accesso tramite i suoi servizi di intermediazione dei dati;

h) in caso di insolvenza, il fornitore di servizi di intermediazione dei dati garantisce una ragionevole continuità della fornitura dei suoi servizi di intermediazione dei dati e, nel caso tali servizi di intermediazione dei dati garantiscono la conservazione dei dati, dispone di meccanismi che consentano ai titolari dei dati e agli utenti dei dati di ottenere l'accesso ai loro dati o il trasferimento o il recupero degli stessi, e che consentano agli interessati, nel caso in cui tale fornitura di servizi di intermediazione dei dati sia fornita tra interessati e utenti dei dati, di esercitare i propri diritti;

i) il fornitore di servizi di intermediazione dei dati adotta misure adeguate per garantire l'interoperabilità con altri servizi di intermediazione dei dati, tra l'altro mediante norme aperte di uso comune nel settore in cui opera il fornitore di servizi di intermediazione dei dati;

j) il fornitore di servizi di intermediazione dei dati mette in atto adeguate misure tecniche, giuridiche e organizzative al fine di impedire il trasferimento di dati non personali o l'accesso a questi ultimi nel caso in cui ciò sia illegale a norma del diritto dell'Unione o del diritto nazionale dello Stato membro interessato;

k) il fornitore di servizi di intermediazione dei dati informa senza ritardo i titolari dei dati in caso di trasferimento, accesso o utilizzo non autorizzati dei dati non personali che ha condiviso;

l) il fornitore di servizi di intermediazione dei dati adotta le misure necessarie per garantire un adeguato livello di sicurezza per la conservazione, il trattamento e la trasmissione di dati non personali, e il fornitore di servizi di intermediazione dei dati assicura inoltre il massimo livello di sicurezza per la conservazione e la trasmissione di informazioni sensibili sotto il profilo della concorrenza;

m) il fornitore di servizi di intermediazione dei dati che offre servizi agli interessati agisce nell'interesse superiore di questi ultimi nel facilitare l'esercizio dei loro diritti, in particolare informandoli e, se opportuno, fornendo loro consulenza in maniera concisa, trasparente, intelligibile e facilmente accessibile sugli utilizzi previsti dei dati da parte degli utenti dei dati e sui termini e le condizioni standard cui sono subordinati tali utilizzi, prima che gli interessati diano il loro consenso;

n) qualora un fornitore di servizi di intermediazione dei dati fornisca strumenti per ottenere il consenso degli interessati o le autorizzazioni a trattare i dati messi a disposizione dai titolari dei dati, esso specifica, se del caso, la giurisdizione del paese terzo in cui si intende effettuare l'utilizzo dei dati e fornisce agli interessati gli strumenti per dare e revocare il consenso e ai titolari dei dati gli strumenti per dare e revocare le autorizzazioni a trattare i dati;

o) il fornitore di servizi di intermediazione dei dati tiene un registro dell'attività di intermediazione dei dati».

[4] Sulla ricaduta di tali principi sulle Cooperative di dati, *ibidem*, p. 17 ss.

sorta di statuto di obblighi cui sono tenuti a conformarsi i soggetti ivi indicati, condizionando, appunto, la liceità del servizio stesso.

Come si dirà meglio nel prosieguo, il Regolamento non prevede direttamente sanzioni conseguenti all'inosservanza delle condizioni, ma ne rimette la previsione agli stati membri.

Infatti, l'art. 12 fa parte del novero delle norme previste dall'art. 34, per il quale il Regolamento rimanda agli Stati membri stabilire «(...) le norme relative alle sanzioni da applicare in caso di violazione (…) delle condizioni per la fornitura di servizi di intermediazione dei dati a norma dell'articolo 12, (…)».

Tornando all'art. 12 DGA, di seguito verranno ripercorse le condizioni previste dalle lett. *g*), *j*) e *l*) di detto articolo, in quanto, come è stato opportunamente notato [5], sono caratterizzate da un elemento comune per le quali possono essere definite «previsioni di sicurezza».

Si tratta di una serie di condizioni latamente omogenee, che impongono obblighi di protezione, non tanto e non soltanto dei dati e delle informazioni, quanto del corretto uso dei servizi di intermediazione e dei soggetti che vi entrano in contatto.

Sul piano letterale, va rilevato come i testi del DGA nelle altre lingue principali [6] utilizzino spesso una terminologia costituita da termini topici, ricorrenti e ormai usuali nell'ambito della normativa sul governo dei dati e del settore digitale [7].

Infatti, la normativa unionale di settore è caratterizzata da schemi uniformi e da un lessico tralaticio, come desumibile sia dall'elencazione nel testo regolamentare delle definizioni esplicative del significato da attribuire ai termini topici utilizzati, sia dal livello di coordinamento e coerenza normativa tipico della normativa unionale.

Tuttavia, in diversi casi, la coerenza presente ad esempio nei testi inglese e francese, è invece venuta meno in alcuni punti della versione italiana del Regolamento.

Alcune incoerenze letterali si rinvengono proprio nel ristretto novero di norme che verranno di seguito ripercorse, e che presentano alcune incertezze e approssimazioni che, mentre da un lato non agevolano la chiarezza del significato, dall'altro aumentano le difficoltà nella ricostruzione dell'ambito applicativo della norma.

Pertanto, la definizione della portata di tali norme imporrà una verifica e talvolta una ricostruzione esegetica sulla base della comparazione con altre versioni parimenti ufficiali del DGA.

---

[5] Cfr. F. BRAVO, *op. cit.*, p. 16 ss.

[6] Per il testo inglese del Regolamento, v. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R0868; per il testo francese, v. https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32022R0868.

[7] Sono i settori riguardanti gli ambiti, tra gli altri, della protezione dei dati personali, della strategia dell'UE sui dati, delineata dalla Commissione europea con la Comunicazione del 19 febbraio 2020 («*European Strategy for Data*») [COM (2020)66 final] in https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066, della cibersicurezza.

3. Sull'art. 12, lett. *g*), DGA: la prevenzione delle pratiche fraudolente o abusive.

La lett. *g*) dell'art. 12 DGA prevede che «il fornitore di servizi di intermediazione dei dati dispone di procedure per prevenire pratiche fraudolente o abusive in relazione a soggetti che richiedono l'accesso tramite i suoi servizi di intermediazione dei dati».

La norma è di esegesi tutt'altro che agevole, sia per alcune incertezze che caratterizzano la lettera del suo testo italiano, sia per la mancata previsione di definizioni che delimitino il significato e la portata dei termini utilizzati, sia, infine, per l'incerta tassatività della norma.

In primo luogo, non si possono tralasciare alcune incertezze letterali che affliggono il testo della norma.

Infatti, nella versione italiana del Regolamento è utilizzato il verbo «(…) dispone (…)», che non solo non è del tutto chiaro e non rende il senso e il contenuto dell'obbligo, ma che addirittura svia il senso e annichilisce la forza precettiva che invece i testi di altre versioni ufficiali del Regolamento rendono più efficacemente.

Infatti, il verbo «(…) dispone (…)» dovrebbe corrispondere all'espressione usata nel testo inglese del Regolamento DGA «(…) *shall have procedures in place* (…)», che significa «(…) dovrà mettere in atto procedure (…)». Parimenti, anche il testo francese «(…) *met en placemet des procédures* (…)» esprime in modo più completo il diverso concetto «(…) mette in atto procedure (…)».

Pertanto, in italiano, il senso più aderente a quello delle espressioni usate nei testi in lingua inglese e francese è reso proprio da quest'ultima espressione «(…) mette in atto (…)», e quindi «(…) predispone (…)».

La conferma è data dalla traduzione delle stesse espressioni previste anche della successiva lett. *j*) dell'art. 12 dei testi in versione inglese e francese, e che in italiano stavolta non vengono tradotte con il verbo «(…) dispone (…)», bensì, appunto, con la più efficace espressione «(…) mette in atto (…)».

Ciò precisato, e ricostruita la norma in esame con una lettera più aderente al testo di altre versioni linguistiche e alla ratio legislativa, essa obbliga l'intermediario a «(…) predisporre (…)» le procedure finalizzate alla prevenzione e quindi un insieme di azioni uniformi da seguire per raggiungere il risultato da realizzare.

Venendo poi all'espressione «pratiche abusive e fraudolente», la norma in esame non indica né cosa debba intendersi, né quali siano le pratiche di cui i singoli non possono avvalersi per vantaggiarsi fraudolentemente o abusivamente delle norme del diritto dell'Unione, né quali siano le procedure da predisporre per lo specifico ambito dell'intermediazione dei servizi.

Pertanto, anche in questo caso si rende necessario uno sforzo esegetico per tentare di circoscrivere l'oggetto dell'obbligo che, per quanto costituisca condizione di conformità e presupposto per l'applicazione delle sanzioni previste dall'art. 34 del Regolamento, è certamente afflitto da una vistosa carenza dell'indefettibile requisito della tassatività.

Orbene, sul piano oggettivo, il divieto di pratiche fraudolente ed abusive è generalmente ritenuto un presidio volto ad impedire che singoli possano avvalersi dell'esercizio dei diritti e delle facoltà previste dall'ordinamento dell'Unione Europea per trarne ingiusto vantaggio [8].

In linea di prima approssimazione, nell'ambito delle «pratiche abusive» si possono ricomprendere tutte quelle azioni che, mediante il ricorso formalmente corretto ad una norma che riconosce un titolo o una posizione di vantaggio previsto per realizzare determinate finalità, vengono invece utilizzate per perseguire finalità diverse e per conseguire un diverso vantaggio ingiusto, non corretto, non conforme e altrimenti non meritevole di tutela giuridica.

La giurisprudenza della Corte di giustizia riconosce il divieto di pratiche abusive come un principio generale dell'ordinamento unionale.

Per «pratiche fraudolente», invece, si intende l'insieme di azioni e comportamenti assunti dal soggetto il quale, per ottenere un vantaggio cui non avrebbe titolo, o per evitare una regola per lui svantaggiosa, ricorre a un'altra regola con modalità apparentemente, formalmente e tecnicamente legittime, ma sostanzialmente perseguite e realizzate con attività occulte e artificiali, mediante menzogne, inganni, artifizi, messe in scena e manovre di raggiro che ricostruiscono e manifestano una realtà diversa da quella reale, al fine di conseguire situazioni di vantaggio.

L'esperienza conosce pratiche fraudolente e abusive del diritto in molti ambiti sociali e giuridici oggetto dell'attività regolamentata dal diritto statale e unionale, con particolare rilevanza, tra gli altri, in quello commerciale, societario, alimentare, lavoristico [9], fiscale, e molti altri ancora. Tuttavia, non vi è alcuna corrispondenza tra le normative e i fenomeni ritenuti abusivi e fraudolenti.

La dottrina, muovendo dall'analisi delle varie giurisprudenze statali e unionale [10], è da tempo impegnata nella ricostruzione dei concetti di abuso del diritto e di

---

[8] Sui principî dell'abuso del diritto e della frode alla legge nel quadro dell'ordinamento della Comunità europea e della giurisprudenza della Corte di Giustizia europea, tra i molti, v. G. TESAURO, *L'abuso del diritto nel diritto internazionale e comunitario,* in G. FURGIUELE (a cura di), *Abuso del diritto. Significato e valore di una tecnica argomentativa in diversi settori dell'ordinamento*, Napoli, 2017, p. 69 ss., con i molti richiami bibliografici; F. LOSURDO, *Il divieto dell'abuso del diritto nell'ordinamento europeo. Storia e giurisprudenza*, Torino, 2011; K.E. SØRENSEN, *Abuse of rights in community law: a principle of substance or merely rhetoric?*, in *Common Market Law Review*, 43, 2006, p. 427; M. GESTRI, *Abuso del diritto e frode alla legge nell'ordinamento comunitario*, Milano, 2003; sull'abuso del diritto, v. G. FURGIUELE (a cura di), *Abuso del diritto. Significato e valore di una tecnica argomentativa in diversi settori dell'ordinamento*, cit.; L. CARPENTIERI, *L'abuso del diritto*, *Atti del Convegno 15 giugno 2017 a Napoli su «L'abuso del diritto. Profili privatistici e profili fiscali»*, Torino, 2019.

[9] Per un esempio di pratiche fraudolente e abusive in ambito lavoristico, cfr. D. VENTURI, *Il distacco transnazionale di lavoratori Luci e ombre del decreto legislativo n. 136/2016*, in *Working Paper* n. 2, in https://www.bollettinoadapt.it/, M. GESTRI, *Abuso del diritto e frode alla legge nell'ordinamento comunitario*, cit., p. 67.

[10] Cfr. M. GESTRI, *Abuso del diritto e frode alla legge nell'ordinamento comunitario*, cit., p. 24.

pratiche fraudolente, ciascuno dei quali comprenda e unifichi gli estremi comuni desumibili dalle rispettive fenomenologie.

Tuttavia, tali sforzi si concentrano sui casi nei quali l'abuso del diritto e le pratiche fraudolente rispetto alla legge costituiscono una sostanziale violazione/elusione degli obblighi previsti a presidio degli interessi degli Stati o dell'Unione.

Orbene, la norma in commento è afflitta da ulteriori incertezze riguardanti sia l'individuazione dei soggetti destinatari dell'attività preventiva, sia il fine perseguito, sia la descrizione della portata dell'attività di cui è onerato l'intermediario, atteso che:

1) non circoscrive il novero di tali «soggetti»;

2) sembra ispirata dall'intento di trasferire sugli intermediari il compito di tutelare i terzi e mediatamente gli interessi dell'Unione;

3) non affianca alcuno strumento pratico, né fornisce alcuna indicazione sugli strumenti o azioni idonee a indirizzare l'adempimento dell'onere gravante sull'intermediario.

In primo luogo, vanno quindi individuati i soggetti destinatari dell'attività preventiva delle pratiche fraudolente o abusive.

A prima lettura, l'espressione «in relazione a soggetti» non consente di determinare con precisione quali siano i soggetti interessati alle o dalle pratiche fraudolente o abusive da prevenire, e quali siano le relative proazioni da implementare per le azioni di contrasto.

Potrebbe trattarsi dei soggetti attivi che realizzano le pratiche fraudolente o abusive, ma potrebbe anche trattarsi dei soggetti passivi che subiscono le pratiche fraudolente o abusive, e quindi coloro che risultano persone offese o danneggiate.

Nel primo caso, l'intermediario sarebbe obbligato a predisporre procedure che prevengano la possibilità che soggetti terzi possano commettere tali attività nei confronti di ulteriori terzi.

Ove invece si addivenisse alla seconda opzione esegetica ipotizzabile, la norma imporrebbe all'intermediario di attivarsi per prevenire le pratiche fraudolente o abusive ai danni di chi richiede i propri servizi di intermediazione o che ne sia in qualche modo coinvolto.

Sarebbe poi ipotizzabile una terza opzione in cui la prevenzione dovrebbe essere svolta nei confronti di chi richiede i servizi forniti dall'intermediario.

In tal caso, la norma in esame prevederebbe un obbligo di protezione dai/dei soggetti che rientrano nel *genus* di «utenti», nel qual caso rileverebbe un vero e proprio obbligo di protezione definibile come "vittimologico", coerentemente con la declinazione che molti principi e norme unionali pongono tra gli obiettivi fondamentali dell'ordinamento.

Orbene, l'asimmetria tra la lettera della norma in commento e l'intenzione espressa dal legislatore non agevola la ricostruzione della sua portata.

Infatti, il *considerando* n. 36, esplicitando la *ratio* dell'art. 12 lett. *g*), DGA sembra delineare i contenuti di una norma nella quale «(…) Si prevede che i fornitori di servizi di intermediazione dei dati dispongano di procedure e misure tese a imporre sanzioni

per le pratiche fraudolente o abusive in relazione ai soggetti che richiedono l'accesso tramite i loro servizi di intermediazione dei dati, anche attraverso misure quali l'esclusione degli utenti di dati che violano i termini del servizio o il diritto vigente».

Come è dato constatare, la norma che attua l'intenzione del legislatore avrebbe dovuto comprendere anche la formulazione dell'obbligo dell'intermediario di imporre procedure e sanzioni «(…) in relazione ai soggetti (…)». E invece, il testo dell'art. 12, lett. *g*), DGA è più ristretto e impone all'intermediario solo l'obbligo di prevenzione nella misura in cui «dispone di procedure per prevenire pratiche fraudolente o abusive», senza attribuirgli alcun potere sanzionatorio nei confronti dei «(…) soggetti (…)».

È vero che in relazione all'art. 12, l'art. 34 DGA riconosce la facoltà di prevedere sanzioni, ma tale potere è attribuito ai Paesi membri ed al fine di sanzionare proprio gli intermediari che violino le condizioni dell'art. 12. Quindi, secondo il combinato disposto dell'art. 12 lett. *g*) e dell'art. 34 DGA, gli intermediari non sono titolari di un proprio potere sanzionatorio verso gli utenti e possono essere solo soggetti passivi di sanzione statale.

Quanto previsto dal *considerando* n. 36 non è stato completamente recepito dall'art. 12, lett. *l*), DGA, quantomeno in rapporto al potere sanzionatorio delle pratiche abusive o fraudolente.

Tuttavia, lo stesso *considerando* n. 36 offrirebbe un riferimento espresso delle intenzioni del legislatore unitario in relazione all'individuazione dei soggetti interessati dalla norma in commento. Infatti, una chiave di lettura che consentirebbe di superare tale incertezza, potrebbe essere costituita dal punto in cui la norma fa espresso riferimento all'obbligo dell'intermediario di predisporre procedure e misure tese a imporre sanzioni anche attraverso misure quali l'esclusione «(…) agli utenti di dati che violano i termini del servizio o il diritto vigente (…)»; la norma indicherebbe gli utenti quali soggetti passivi di sanzioni per le pratiche fraudolente o abusive, e quindi i soggetti attivi di tali pratiche.

Pertanto, ove i soggetti cui si farebbe riferimento nell'art. 12, lett. *g*), DGA fossero gli «utenti di dati» che commettono abusi o pratiche fraudolente, si potrebbe concludere che l'oggetto della tutela prevista dalla norma sia costituito non tanto, o non solo, da un'attenzione alle vittime delle pratiche abusive o fraudolente, quanto invece a garantire la regolarità formale e sostanziale, e quindi la «neutralità», del servizio di intermediazione in sé.

Poiché la norma in commento impone all'intermediario di servizi di svolgere l'azione preventiva verso e «(…) in relazione a soggetti che richiedono l'accesso tramite i suoi servizi di intermediazione dei dati», va altresì delineata la portata dell'attività preventiva da svolgere nei confronti degli «utenti dei dati» nel cui genere, ai sensi dell'art. 2, co. 1, n. 9, DGA rientra ogni «(...) una persona fisica o giuridica che ha accesso legittimo a determinati dati personali o non personali e che ha diritto, anche a norma del regolamento (UE) 2016/679 in caso di dati personali, a utilizzare tali dati a fini commerciali o non commerciali».

A tal proposito, il legislatore avrebbe potuto consentire agli Stati membri di allestire azioni preventive, procedure, sanzioni per le pratiche abusive e fraudolente,

servendosi degli efficaci strumenti messi a loro disposizione dalla normativa unionale, quali gli strumenti di vigilanza, di cooperazione internazionale, di scambio di informazioni, di indagine attraverso gli organi a ciò competenti, di procedure sanzionatorie, e quant'altro *aliunde* già previsto.

Invero, nel caso de quo, il legislatore ha optato per la responsabilizzazione degli intermediari, che vengono così gravati dell'attuazione di un'azione preventiva da svolgersi in un ambito puramente interprivatistico [11], da svolgersi solo con strumenti di prevenzione dei rischi messi a disposizione dalla prassi organizzativa e, al più, con strumenti di *soft law* [12].

Se da un lato è quindi vero che la condizione in esame impone all'intermediario di svolgere un'attività proattivamente tesa a prevenire, cioè a ridurre il rischio che si verifichino condotte fraudolente o abusive commesse dagli utenti del servizio di intermediazione, dall'altro nulla si indica in merito alle procedure che l'intermediario dovrà in concreto adottare nell'ambito specifico.

Pertanto, la norma responsabilizza l'intermediario, lasciandolo libero di scegliere le modalità e gli strumenti che riterrà più idonei per la realizzazione delle azioni preventive e per la realizzazione del fine indicato dalla condizione del Regolamento in esame.

Si tratterà quindi di individuare e implementare azioni preventive mediante procedure, strumenti, personale e competenze per organizzare piani di prevenzione di pratiche fraudolente o abusive [13].

Tale approccio presupporrà un'analisi preliminare che consenta all'intermediario di ipotizzare e delineare *ex ante* le pratiche fraudolente specifiche del settore dell'intermediazione, muovendo dai contenuti desumibili dalle normative e relativa giurisprudenza unionale e statale specifiche del settore dell'intermediazione dei dati.

Indi, potrà avvalersi e implementare quelle azioni e procedure che sono già indicate dalle organizzazioni internazionali o nazionali per la standardizzazione, il miglioramento e il controllo dei livelli di qualità dei servizi, in quanto potranno quantomeno costituire un valido criterio di riferimento iniziale.

L'intermediario potrà quindi decidere, ad esempio, di realizzare la condizione

---

[11] In merito all'utilizzo di strumenti civilistici quali, ad es., il ricorso all'art. 1344 c.c. sia per il contrasto della frode alla legge, sia per un'applicazione estensiva anche ai casi di abuso del diritto, al fine di colmare la carenza di previsione positiva per quest'ultima situazione, v. M. GESTRI, *Abuso del diritto e frode alla legge nell'ordinamento comunitario*, cit. p. 192.

[12] In tale contesto, è evidente la necessità del ricorso alle tecniche di GRC, *Governance, Risk and Compliance*, messe a disposizione da alcuni tipi di standard internazionali di organizzazione aziendale; su tali tecniche, v. C. PONTI, *GRC, un approccio integrato nel processo di auditing iso 27001*, 2023, in www.riskcompliance.it.

[13] Le tecniche di implementazione di tali procedure sono assimilabili a quelle previste da altre norme già operanti nel nostro ordinamento e che mirano a responsabilizzare gli operatori. E il pensiero corre immediatamente al sistema previsto dal d.lgs. n. 231/2001 mediante l'onere di implementazione del MOG, il Modello Organizzativo e di Gestione e gli altri strumenti collegati, al fine di prevenire ed evitare la responsabilità penale delle persone giuridiche.

seguendo le procedure di c.d. GRC, *Governance, Risk management, Compliance* [14], previsti dagli standard internazionali o di settore, e quindi adottando:

(i) atti di *soft law*, quali appendici contrattuali costituiti da codici etici, deontologici, regole di comportamento, raccomandazioni, policy di principi condivisi e accettati, linee guida, alla cui accettazione da parte degli utenti condizionare la fornitura dei servizi;

(ii) campagne di comunicazione, formazione e informazione degli utenti;

(iii) attività di periodico monitoraggio e controllo interno (c.d. procedure di *audit*), anche solo a campione;

(iv) analisi dei rischi con l'individuazione di indici e segnali di allerta e criticità;

(v) aggiornamento periodico delle pratiche e delle iniziative in relazione al perfezionamento delle attività di controllo e dell'evoluzione normativa e giurisprudenziale e tecnologica;

(vi) predisposizione di procedure di due diligence, di whistleblowing, di reazione e contrasto con strumenti contrattuali, commerciali, giudiziari e amministrativi;

(vii) informazione dell'istituenda Autorità per l'Intermediazione dei Dati prevista dall'art. 13 DGA, alla quale è affidata, tra le altre, l'attività di controllo e di monitoraggio della conformità al Regolamento;

(viii) coinvolgimento collaterale *ad hoc* delle altre autorità settoriali indipendenti che, a seconda delle situazioni, potrebbero essere evocate come competenti *ex* art. 13, par. 3, DGA, in via esclusiva *rationae materiae* o in via concorrente, quali l'Autorità garante per la concorrenza e il mercato (AGCM), l'Autorità garante per la protezione dei dati personali (GPDP), l'Autorità garante per le garanzie nelle comunicazioni AGCOM), l'Autorità nazionale anticorruzione (ANAC), o l'Agenzia per la cybersicurezza nazionale (ACN);

(ix) adempimento degli obblighi di conformità, segnalazione e notifica alle Autorità Garanti indipendenti settorialmente competenti, essendo l'azione preventiva rilevante trasversalmente.

Se allo stato queste azioni possono essere considerate punti di partenza per una prima attuazione della portata della norma, ulteriori e più precisi criteri di riferimento per la sua portata potranno essere attinti dalle indicazioni provenienti dall'istituenda Autorità e dalla giurisprudenza che si formerà in materia.

4. Sull'art. 12, lett. *j*), DGA: le misure di impedimento di trasferimento o accesso ai dati non personali.

L'ulteriore condizione di sicurezza in esame prevista dall'art. 12, lett. *j*), DGA, prevede che «il fornitore di servizi di intermediazione dei dati mette in atto adeguate misure tecniche, giuridiche e organizzative al fine di impedire il trasferimento di

[14] Cfr., C. PONTI, *GRC, un approccio integrato nel processo di auditing ISO 27001*, cit.

dati non personali o l'accesso a questi ultimi nel caso in cui ciò sia illegale a norma del diritto dell'Unione o del diritto nazionale dello Stato membro interessato».

Anche per condizione in commento, va preliminarmente operata una ricognizione della norma, al fine di specificarne la portata, individuare l'obiettivo perseguito e delimitarne l'ambito di operatività.

La lettera della norma in esame appare limitata al «trasferimento interno di dati non personali o l'accesso» nei casi in cui ciò non sia conforme alle norme dell'Unione e degli Stati membri.

In linea di prima approssimazione, si potrebbe ritenere che, dal punto di vista meramente tecnico, per trasferimento di dati personali possa intendersi l'attività di spostamento dei dati da/tra uno a più sistemi, anche informatici, compiute con o senza l'ausilio di processi automatizzati e applicata a dati o insiemi di dati, che può comportare o meno anche un passaggio dei dati da una persona fisica o giuridica ad altra persona [15].

Si tratta del nucleo di operatività tecnica disciplinato dal DGA, il cui fine è proprio quello di mettere in movimento i dati per consentire trattamenti che consentano di valorizzarli e di creare ulteriori attività a valore aggiunto a beneficio dell'economia, della ricerca, della società.

Ove i processi siano automatizzati, si tratta di operazioni tecnicamente non neutrali in quanto i risultati sono determinati dai sistemi utilizzati, quali il sistema di archiviazione, il database di organizzazione, l'applicazione di spostamento dei dati e memorizzazione e accesso.

Orbene, dal punto di vista della portata della norma in commento, si può muovere dall'analogo fenomeno del trasferimento dei dati personali all'estero, al quale il legislatore comunitario aveva già dedicato il Capo V del GDPR.

Il tema ha trovato impulso a seguito dell'attività giurisprudenziale esitata nelle c.d. sentenze Schrems, a seguito delle quali la questione del trasferimento dei dati personali all'estero è divenuta oggetto di rilevante approfondimento dottrinale e regolamentare [16].

---

[15] In ambito giuridico, il termine "trasferimento" non è usato né nel GDPR, nel quale si usa l'espressione più articolata di «comunicazione mediante trasmissione» (art. 4, lett. 2), né nel Regolamento 2018/1807 in tema di circolazione di dati personali, nel quale, all'art. 6 in punto di Portabilità dei dati, viene usata l'espressione «trasferire i dati nei propri sistemi informatici».

[16] Quanto al trasferimento di dati personali verso gli USA, e per estensione verso i Paesi extra UE, è ancora vivo il dibattito che ha anticipato e seguito le Sentenze c.d. Schrems, entrambe in https://curia.europa.eu, ed in particolare la Sentenza della Corte (Grande Sezione) del 6 ottobre 2015 (domanda di pronuncia pregiudiziale proposta dalla High Court (Irlanda) – Maximillian Schrems / Data Protection Commissioner (Causa C-362/14)1, e la Sentenza della Corte (Grande Sezione) del 16 luglio 2020 (domanda di pronuncia pregiudiziale proposta dalla High Court – Irlanda) – Data Protection Commissioner / Facebook Ireland Limited, Maximillian Schrems (Causa C-311/18)1, con ricostruzione al comunicato stampa «La Corte dichiara invalida la decisione 2016/1250 della Commissione sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy» in https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091it.pdf.

Le decisioni appena menzionate hanno compulsato l'attività del Comitato Europeo per la Protezione dei dati (*European Data Protection Board*, anche «EDPB») [17] e del Garante per la protezione dei dati personali [18].

L'eco di tali attività si riflette anche nel DGA, nel quale la previsione di modalità, limiti e condizioni per il trasferimento dei dati non personali è reiterata e trasversale a diversi *considerando* (4, 19, 20, 21, 22, 24, 59) e all'articolato (5, 12, 20, 21, 30, 31, 34).

Tale ricorrenza è indice dell'attenzione (o preoccupazione) che il legislatore pone al tema di rilevante delicatezza ed importanza strategica costituito dalla libera circolazione dei dati per consentire il loro sfruttamento economico, sociale e scientifico. Ma l'attenzione alla circolazione dei dati dovrà peròdovrà essere accompagnata dal controllo dei flussi di dati, e in particolare a quelli che hanno ad oggetto «(…) dati non personali che possono essere ritenuti altamente sensibili (…)» per i quali si dimostra molta attenzione, ad esempio, nel *considerando* nn. 24 e 58 e nell'art. 5.

Deve osservarsi come nel DGA l'espressione «trasferimento dei dati» non sia univoca e ricorra in almeno una duplice accezione e di diversa ampiezza, ovvero sia come «trasferimento dei dati» *tout court* (ad es. *considerando* nn. 26, 30), sia come «trasferimento dei dati all'estero» (ad esempio nei *considerando* nn. 19, 20, 21, 22, 24, 58, 59 e negli artt. 5, 30, 31, 34).

Appare quindi corretto poter distinguere tra due diverse previsioni, ovvero tra quella del trasferimento interno di dati e quella del trasferimento di dati all'estero rispetto all'area UE, ciascuna delle quali riguarda aree diverse e comporta effetti sistematici diversi.

Quanto invece all'estensione dell'area UE all'interno della quale e dall'esterno della quale va consentito, o controllato o impedito il trasferimento o l'accesso, essa va considerata coincidente con lo Spazio Economico Europeo allargato, SEE, cioè l'Unione europea più la Norvegia, Liechtenstein e Islanda, come espressamente indicato nella rubrica del Regolamento, nella quale lo si indica come «Testo rilevante ai fini del SEE».

La condizione in esame, non menzionando alcun criterio di specialità o altra limitazione, sembrerebbe fare riferimento ad ogni trasferimento, e quindi sia ai trasferimenti interni all'UE, sia ai trasferimenti verso paesi terzi.

Quanto invece al concetto di accesso ai dati, l'interprete può fare riferimento alla definizione espressa fornita dall'art. 2, n. 13, DGA: «accesso»: l'utilizzo dei dati, conformemente a specifici requisiti tecnici, giuridici o organizzativi, che non im-

---

[17] Per l'attività dell'EDPB, v. https://www.edpb.europa.eu/edpb_it; in relazione al tema oggetto di commento, si vedano in particolare le «Raccomandazioni 01/2020 relative alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE Adottate il 10 novembre 2020».

[18] Sull'impostazione del trasferimento dei dati personali all'estero e sugli strumenti per la sua disciplina e regolamentazione, v. https://www.garanteprivacy.it/temi/trasferimento-di-dati-all-estero.

plica necessariamente la trasmissione o lo scaricamento di dati».

Pertanto, si potrebbe intendere la possibilità per un soggetto di «usare» e quindi compiere operazioni di trattamento dati, inclusa la mera presa di conoscenza.

A tal proposito, sarebbe fuorviante associare l'espressione «accesso ai dati» all'assonante espressione «diritto di accesso» riconosciuto all'interessato dall'art. 15 GDPR, atteso che quest'ultimo caso riguarda l'insieme di diritti ad ottenere informazioni sui dati personali trattati dal titolare, mentre nel caso della norma in commento è evidente come si faccia riferimento al ben diverso concetto di accesso fisico e/o logico ai dati per consentirne l'uso.

Passando all'esame della limitazione della portata della condizione in esame ai soli «dati non personali», si tratta di un ambito oggettivo palesemente diverso da quello previsto dagli artt. 24, 25, 32 GDPR a tutela della sicurezza dei dati personali e in merito ai quali dette norme sarebbero comunque presupposte ed efficaci.

Invero, la previsione dell'art. 12, lett. *j*), DGA si focalizza sul diverso ambito oggettivo che è quello dei «dati non personali».

A tal proposito, va innanzitutto ricordato come tale categoria trovi specifica disciplina nel Reg. (UE) 2018/1807 sulla circolazione dei dati non personali [19], che all'art. 3 vengono definiti in negativo come «(…) 1) "dati": i dati diversi dai dati personali definiti all'articolo 4, punto 1, del regolamento (UE) 2016/679». A loro volta, i dati personali sono definiti nel GDPR come «qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato"); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo *online* o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale».

Pertanto, ogni dato costituito da dati diversi da «(…) qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato») (…)» è da considerarsi come rientrante nel *genus* dei «dati non personali» [20].

I dati non personali possono essere tali *ab origine*, come ad esempio i dati tipicamente naturalistici ed ambientali, quali i dati metereologici, i dati relativi al traffico e sulla viabilità stradale, quelli sull'inquinamento ambientale, oppure i dati relativi al comportamento di soggetti indistinti, quali quelli relativi all'afflusso agli uffici pubblici, al sistema dei trasporti, alle preferenze alimentari, ecc.

Ma può anche trattarsi di dati originariamente personali, successivamente anonimizzati e quindi resi «non personali».

Quanto al contenuto precettivo della condizione in esame, la norma impone al-

---

[19] Reg. (UE) 2018/1807 relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea.

[20] La stessa distinzione dei dati non personali in negativo rispetto ai dati personali è ripresa anche dall'art. 2, par. 1, nn. 3 e 4, del c.d. Regolamento sui dati (*Data Act*), Reg. (UE) 2023/2854 del Parlamento europeo e del Consiglio del 13 dicembre 2023 riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il Reg. (UE) 2017/2394 e la dir. (UE) 2020/1828.

l'intermediario di dati l'obbligo di adottare «(…) adeguate misure tecniche, giuridiche e organizzative (…)».

A tal proposito va preliminarmente ricordato come l'intermediazione dei dati non personali, al pari degli altri istituti previsti dal DGA quali l'uso, il riuso, l'altruismo dei dati non personali, ha lo scopo di rimettere in circolo dati indispensabili per la creazione di valore, a beneficio di molteplici attività sociali quali, tra le altre, l'economia e la ricerca scientifica.

Tuttavia, la reimmissione in circolo dei dati è stata frenata da diversi fattori, secondo una fenomenologia ricorrente che è ben spiegata nel Considerando 6 DGA a proposito degli enti pubblici, ma valevole anche per gli altri soggetti: «(…) Spesso talune categorie di dati conservati in basi di dati pubbliche, quali dati commerciali riservati, dati soggetti a segreto statistico e dati protetti da diritti di proprietà intellettuale di terzi, compresi segreti commerciali e dati personali, spesso non sono messe a disposizione, nemmeno per attività di ricerca o di innovazione nel pubblico interesse, nonostante tale disponibilità sia possibile in conformità del diritto dell'Unione applicabile, in particolare del regolamento (UE) 2016/679 e delle direttive 2002/58/CE e (UE) 2016/680. A causa della sensibilità di tali dati, prima che essi siano messi a disposizione si devono soddisfare alcuni requisiti procedurali tecnici e giuridici al fine, se non altro, di garantire il rispetto dei diritti di terzi sui dati in questione o di limitare l'effetto negativo sui diritti fondamentali, sul principio di non discriminazione e sulla protezione dei dati. L'adempimento di tali requisiti risulta abitualmente molto dispendioso in termini di tempo e richiede un livello molto elevato di conoscenze. Ciò ha determinato un utilizzo insufficiente di tali dati. Per quanto alcuni Stati membri stiano istituendo strutture, procedure o adottando norme per agevolare tale tipo di riutilizzo, ciò non accade in tutta l'Unione. Al fine di agevolare l'utilizzo dei dati per la ricerca e l'innovazione europee da parte di soggetti pubblici e privati, sono necessarie condizioni chiare per l'accesso a tali dati e il loro utilizzo in tutta l'Unione».

La condizione in commento non indica espressamente quali siano le misure da mettere in atto ma, secondo il ben noto schema di atipicità alla base del principio di responsabilizzazione [21] del titolare, cosicché il concetto di «adeguatezza» delle misure è un attributo privo di specificazione circa il suo contenuto e la portata.

Non si fa riferimento solo alle misure di sicurezza, ma si tratta di uno spettro di azioni molto più ampio.

Una prima serie di strumenti tecnici che certamente indirizza e agevola l'intermediario nella direzione da intraprendere, può essere considerata quella di cui all'art. 7 del DGA il quale, nel prevedere l'assistenza a favore degli enti pubblici da parte dell'istituendo organismo competente per specifici settori, in tema di tutela

[21] Sul principio di responsabilizzazione o *accountability*, v. F. ALBANESE-I. CARDINALI, *Il principio di responsabilizzazione (accountability)*, in F. BRAVO (a cura di), *Dati personali. Protezione, libera circolazione e governance*. – Vol. 1. *Principi*, Pisa, 2023, p. 501 ss.; G. FINOCCHIARO, *Il principio di accountability*, in *Giur. it.*, 2019, 12, pp. 2778-2783.

della riservatezza menziona espressamente gli strumenti a tutela dell'integrità e l'accessibilità delle informazioni contenute nei dati per i quali è consentito il riutilizzo, e quindi, senza intento esaustivo, le «tecniche di anonimizzazione, generalizzazione, soppressione e randomizzazione dei dati personali o altri metodi all'avanguardia di tutela della vita privata, e la cancellazione di informazioni commerciali riservate, tra cui segreti commerciali o contenuti protetti da diritti di proprietà intellettuale; (…)».

Ulteriori misure tecniche sono quelle previste dal *considerando* n. 7 nel quale si indica quanto segue:«(…) Esistono tecniche che consentono l'analisi di banche dati contenenti dati personali, quali l'anonimizzazione, la *privacy* differenziale, la generalizzazione, la soppressione e la casualizzazione, l'utilizzo di dati sintetici o metodi analoghi, nonché altri metodi all'avanguardia di tutela della vita privata che potrebbero contribuire a un trattamento dei dati maggiormente rispettoso della vita privata. Gli Stati membri dovrebbero fornire sostegno agli enti pubblici affinché utilizzino in maniera ottimale tali tecniche, rendendo così disponibili quanti più dati possibili per la condivisione. L'applicazione di tali tecniche, unite a valutazioni d'impatto globali in materia di protezione dei dati e ad altre tutele può contribuire a una maggiore sicurezza nell'utilizzo e riutilizzo dei dati personali e dovrebbe garantire il riutilizzo sicuro dei dati commerciali riservati a fini statistici, di ricerca e di innovazione. In molti casi l'applicazione di tali tecniche, valutazioni d'impatto e altre tutele implica che i dati possano essere utilizzati e riutilizzati solamente in un ambiente di trattamento sicuro fornito o controllato dall'ente pubblico. L'uso di simili ambienti di trattamento sicuro è già stato sperimentato a livello dell'Unione ai fini della ricerca su microdati statistici, sulla base del regolamento (UE) n. 557/2013 della Commissione (25). Per quanto concerne i dati personali, il trattamento dei dati personali dovrebbe in generale essere basato su una o più delle basi giuridiche per il trattamento dei dati personali previste agli articoli 6 e 9 del regolamento (UE) 2016/679 (…)».

Quanto alle misure giuridiche, l'ultimo periodo del *considerando*, richiamando per i dati personali le condizioni di liceità del trattamento previsto dall'art. 6 del GDPR e le condizioni per il trattamento dei dati particolari previsto dall'art. 9 del GDPR, in realtà sembrerebbe concretizzare la previsione delle adeguate misure «giuridiche» cui fa riferimento la condizione del DGA in commento, se non fosse che quest'ultima, però, si applica solo ai dati non personali. La questione richiederà certamente ulteriori e specifici approfondimenti per verificare se si tratti un'eccezione o di un'antinomia.

Va inoltre prestata attenzione alle modalità di concreta attuazione della norma, tenuto conto anche delle esperienze mutuabili da contesti contigui e affini quali quelli del ricorso a strumenti di *soft law*, quali strumenti contrattuali, modelli organizzativi e di gestione, regolamenti interni, codici etici, di comportamento e deontologici che prevedano obblighi di comportamento e sistemi di *audit* e controllo periodiche e/o a campione sia per le azioni di verifica di applicazione e di miglioramento, sia per l'applicazione di relative sanzioni disciplinari in caso di inosservanza.

E tuttavia, a parte l'ultronea previsione delle misure «giuridiche», la condizione del GDA in esame ricalca parzialmente quanto già previsto dall'art. 24 del GDPR in tema di responsabilizzazione del titolare del trattamento per le misure di sicurezza da adottarsi a protezione dei dati personali [22]. Pertanto, alla norma *de qua* relativa ai dati non personali sembrerebbe mutuabile l'ampia teorica sviluppata in ambito GDPR intorno al concetto di adeguatezza delle misure.

Infine, la norma in commento seleziona le situazioni in relazione ai quali l'intermediario è tenuto ad implementare le adeguate misure.

Egli infatti non è tenuto ad impedire in assoluto ogni trasferimento di dati non personali o l'accesso a questi ultimi, che invece è proprio il fine perseguito dal DGA, quanto ad impedirli solo «(…) nel caso in cui ciò sia illegale a norma del diritto dell'Unione o del diritto nazionale dello Stato membro interessato».

La previsione non elenca i casi di illiceità speciale, ma costituisce una clausola di atipicità che estende la responsabilizzazione dell'intermediario, onerandolo della valutazione di ogni caso di illegalità previsto da ogni norma sia dell'ordinamento dell'Unione, sia del diritto dello Stato membro interessato.

A tal proposito. non passa inosservata l'articolata portata oggettiva e soggettiva della previsione.

Infatti, quanto all'Unione, si fa riferimento solo alle «norme dell'ordinamento», così apparentemente limitando la conformità ad ogni norma rientrante nell'area del diritto positivo, senza distinzione tra norme di rango primario o secondario. In relazione alla sfera giuridica dello «Stato membro interessato», invece si fa riferimento al «diritto nazionale», così giustificando un obbligo di conformità ad un'area più estesa del sistema giuridico, che ricomprenderebbe ogni componente del diritto in senso lato, e non solo quanto previsto da norme di rango primario e secondario, ma anche quanto previsto da regole amministrative o paramministrative, o da accordi internazionali, decisioni e sentenze, tutti strumenti che, applicando le norme dell'ordinamento, rientrano a pieno titolo nel più ampio ambito del «diritto nazionale».

Una spia della coerenza sistematica di tale interpretazione estensiva, è fornita dalla stessa lettera dell'art. 31 DGA il quale, proprio in relazione all'«Accesso internazionale e trasferimento», al par. 1, nell'ambito dell'analoga, ma non simile, previsione di adozione di «ragionevoli misure», prevede una medesima valutazione di conformità, facendo salvi il «paragrafo 2 o 3» del medesimo articolo, e annove-

[22] Così recita l'art. 24 GDPR, «*Responsabilità del titolare del trattamento*»: «1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario. 2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento. 3. L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento».

rando «decisioni o sentenze di un'autorità giurisdizionale», «decisioni di un'autorità amministrativa», «accordi internazionali» [23].

Inoltre, quanto alla portata soggettiva dell'espressione «diritto nazionale dello Stato membro interessato» in relazione al quale l'intermediario dovrà svolgere la valutazione di conformità del trasferimento o accesso, la lettera della norma sembrerebbe limitare l'obbligo di conformità solo al diritto dello Stato membro interessato, così escludendo la valutazione del diritto di altri soggetti che, pur coinvolti nell'attività, non abbiano la qualità di Stato membro.

Invero, la ratio della condizione in commento sembrerebbe far riferimento al diritto di ciascun «soggetto» coinvolto nell'attività di trasferimento o accesso ai dati. Pertanto, l'onere di valutazione della conformità del trasferimento o accesso sembrerebbe esteso al diritto nazionale si ogni Stato membro interessato ove si tratti di

---

[23] Così recita l'art. 31 DGA, rubricato «*Accesso internazionale e trasferimento*»:

«1. L'ente pubblico, la persona fisica o giuridica cui è stato concesso il diritto di riutilizzo dei dati a norma del capo II, il fornitore di servizi di intermediazione dei dati, o l'organizzazione per l'altruismo dei dati riconosciuta, adotta tutte le ragionevoli misure tecniche, giuridiche e organizzative, compresi accordi contrattuali, per impedire il trasferimento internazionale di dati non personali detenuti nell'Unione o l'accesso a questi ultimi da parte delle autorità pubbliche qualora tale trasferimento o accesso confliggesse con il diritto dell'Unione o il diritto nazionale dello Stato membro pertinente, fatto salvo il paragrafo 2 o 3.

2. Le decisioni o le sentenze di un'autorità giurisdizionale di un paese terzo e le decisioni di un'autorità amministrativa di un paese terzo che dispongano che un ente pubblico, una persona fisica o giuridica cui è stato concesso il diritto di riutilizzo dei dati a norma del capo II, un fornitore di servizi di intermediazione dei dati o un'organizzazione per l'altruismo dei dati riconosciuta trasferiscano dati non personali detenuti nell'Unione o vi diano accesso nell'ambito di applicazione del presente regolamento sono riconosciute o assumono qualsivoglia carattere esecutivo soltanto se basate su un accordo internazionale in vigore tra il paese terzo richiedente e l'Unione, ad esempio un trattato di mutua assistenza giudiziaria, o su un accordo di questo tipo concluso tra il paese terzo richiedente e uno Stato membro.

3. In mancanza di un accordo internazionale di cui al paragrafo 2 del presente articolo, qualora un ente pubblico, una persona fisica o giuridica cui è stato concesso il diritto di riutilizzo dei dati a norma del capo II, un fornitore di servizi di intermediazione dei dati o un'organizzazione per l'altruismo dei dati riconosciuta siano destinatari di una decisione o di una sentenza di un'autorità giurisdizionale di un paese terzo o di una decisione di un'autorità amministrativa di un paese terzo che ordini il trasferimento di dati non personali detenuti nell'Unione o che vi sia dato accesso nell'ambito di applicazione del presente regolamento, e il rispetto di tale decisione rischi di mettere il destinatario in conflitto con il diritto dell'Unione o con il diritto nazionale dello Stato membro pertinente, il trasferimento di tali dati o l'accesso agli stessi da parte di tale autorità di un paese terzo ha luogo solo se: a) il sistema del paese terzo richiede che siano indicati i motivi e la proporzionalità della decisione o della sentenza, e richiede che tale decisione o sentenza abbia carattere specifico, ad esempio stabilendo un nesso sufficiente con determinate persone sospettate o determinate violazioni; b) l'obiezione motivata del destinatario è oggetto di esame da parte di un'autorità giurisdizionale competente del paese terzo; e c) l'autorità giurisdizionale competente del paese terzo che emette la decisione o la sentenza o esamina la decisione di un'autorità amministrativa ha il potere, in virtù del diritto di tale paese terzo, di tenere debitamente conto dei pertinenti interessi giuridici del fornitore dei dati tutelati a norma del diritto dell'Unione o dal diritto nazionale del pertinente Stato membro (...)».

un trasferimento interno all'UE, mentre sarebbe limitato al solo «diritto nazionale dello Stato membro interessato» ove si tratti di un trasferimento *extra* UE.

Come si è detto, il DGA è particolarmente attento a regolamentare le condizioni di tutte le tipologie di trasferimento di dati non personali, soprattutto quelli all'estero. Pertanto, l'analoga previsione di un obbligo di adozione di «(…) tutte le ragionevoli misure tecniche, giuridiche e organizzative, compresi accordi contrattuali, (…)» a carico dell'intermediario è prevista anche dall'art. 31 DGA [24] nel caso in cui oggetto di trasferimento internazionale dei dati personali detenuti nell'Unione siano i dati oggetto di riutilizzo o altruismo dei dati. In tal caso, limitandosi l'onere a «(…) tutte le ragionevoli misure (…)» sembra che la responsabilizzazione venga limitata ad un livello meno severo dell'adeguatezza.

Quanto infine al regime sanzionatorio previsto dall'art. 34 DGA nei casi di violazione da parte dell'intermediario delle condizioni di cui all'art. 12, e quindi anche della lett. *j*) in commento, si rinvia a quanto già esposto sopra, ed in particolare a come la previsione di sanzioni sia stata delegata ai Paesi membri.

Ma la violazione della condizione in commento rientra a duplice titolo nel regime sanzionatorio dell'art. 34: sia in quanto l'art. 12 è espressamente indicato tra i casi la cui violazione è soggetta a sanzione, sia perché il presupposto in esame è espressamente previsto dall'esordio della norma di delega del regime sanzionatorio stesso, che statuisce quanto segue: «Articolo 34 – *Sanzioni*. 1. Gli Stati membri stabiliscono le norme relative alle sanzioni da applicare in caso di violazione degli obblighi in materia di trasferimento di dati non personali a paesi terzi a norma dell'articolo 5 (…)».

Orbene, va notato come il divieto di trasferimento di dati non personali verso i paesi terzi previsto da diverse norme, sia rafforzato dalla doppia menzione e dalla delega del regime sanzionatorio. La ratio risiede nella natura particolarmente delicata e strategica del regime di trasferimento dei dati non personali, che costituisce uno dei capisaldi della DGA e che è rimesso al controllo e alla potestà sanzionatoria degli Stati membri.

Tuttavia, l'attuale formulazione della delega della potestà sanzionatoria a ciascun Stato membro avalla la prevedibilità di regimi sanzionatori differenti e soprattutto a diversa intensità afflittiva. Le differenze delle reazioni sanzionatorie, sino alla possibilità che in alcuni paesi non siano affatto previste e quindi comminate affatto sanzioni, potrebbero consentire la creazione di zone franche ed innescare situazioni di disparità di trattamento all'interno dell'Unione.

Tale discrepanza potrebbe quindi favorire lo sviluppo di aree che, essendo a minor rischio sanzionatorio, attrarrebbero lo stabilimento degli intermediari, così alterando l'equilibrio di un corretto rapporto concorrenziale.

---

[24] Per l'art. 31 DGA, vedi nota precedente.

5. Sull'art. 12, lett. *l*), DGA: le misure di sicurezza.

L'art. 12, lett. *l*), DGA, prevede che «il fornitore di servizi di intermediazione dei dati adotta le misure necessarie per garantire un adeguato livello di sicurezza per la conservazione, il trattamento e la trasmissione di dati non personali, e il fornitore di servizi di intermediazione dei dati assicura inoltre il massimo livello di sicurezza per la conservazione e la trasmissione di informazioni sensibili sotto il profilo della concorrenza».

La norma limita l'ambito oggettivo di applicazione dell'obbligo ai «dati non personali», a proposito dei quali si richiama quanto appena detto in proposito alla stessa limitazione di cui all'art. 12 lett. *j*).

Anche per tale previsione si deve preliminarmente notare come i termini utilizzati nel testo italiano presentino qualche incertezza, rispetto, ad esempio, alle corrispondenti versioni inglese e francese che potrebbero dar luogo a problemi sul piano esegetico e applicativo.

Difatti, in entrambe le parti della condizione si impone all'intermediario l'obiettivo della «(…) conservazione, (…) di dati non personali (…)».

Il termine «(…) conservazione (…)» usato nel testo italiano avrebbe dovuto tradurre il termine francese «(…) *stockage* (…)» o il termine inglese «(…) *storage* (…)». Invero, muovendo dal significato letterale e sistematico dei termini alloglotti europei, il termine «(…) conservazione (…)», che è già usato in contesti diversi e con accezione tanto diversa, quanto diffusa e consolidata[25], andrebbe sostituito dal diverso termine di «...archiviazione…», concetto tecnico ben diverso e che meglio si armonizza con l'obbligo di disponibilità e continuità dei dati e dei servizi che li riguardano.

Rimodulato il significato da attribuire al termine, la norma in commento articola due distinti oggetti di protezione, per ciascuno dei quali l'intermediario deve calibrare un proprio livello di protezione.

La prima parte della Condizione in esame impone all'intermediario «di adottare

[25] Nell'ambito della normativa relativa alla protezione dei dati personali, il termine «(…) conservazione (…)» normalmente traduce il diverso termine di «(…) *retention* (…)» nel senso di mantenimento, custodia, salvaguardia, come infatti si rinviene nell'art. 132 Codice *privacy* in tema di «Conservazione di dati di traffico per altre finalità» ed aventi ad oggetto i «Dati relativi al traffico» (1. I dati relativi al traffico riguardanti abbonati ed utenti trattati dal fornitore di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico» come previsto dall'art. 123 stesso Codice. Stessa accezione per l'uso del termine «conservare» lo si rinviene nell'art. 254 bis cpp in tema di «Sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni» per il quale» 1. L'autorità giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione, può stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi, che la loro acquisizione avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità. In questo caso è, comunque, ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali».

le misure necessarie per garantire un adeguato livello di sicurezza per la conservazione, il trattamento e la trasmissione di dati non personali».

Oggetto della protezione è costituito dai «dati non personali» come definiti dall'art. 2, n. 1, DGA, ovvero «(...) qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi raccolta di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva». A sua volta, l'art. 2, n. 4), DGA, definisce i «dati non personali» come «(…) i dati diversi dai dati personali», così distinti *per relationem* e *a contrariis* dai dati personali dall'art. 2, n. 3), per il quale vanno individuati ai sensi del GDPR in quelli «(...) definiti all'articolo 4, punto 1, del regolamento (UE) 2016/679».

L'obbligo di sicurezza previsto dalla prima parte dell'art. 12, lett. *l*), DGA è esteso indistintamente a tutti i dati non personali e alle attività di cui tali dati possono essere oggetto, sia staticamente che dinamicamente, quali sono quelle di archiviazione, trattamento e trasmissione.

In relazione alla delimitazione della portata del termine «trattamento», va ricordato l'ampio novero di azioni ricomprese nello spettro della definizione ormai tralaticia ed espressamente richiamata dall'art. 12, n. 12), come: «(...) il trattamento quale definito all'articolo 4, punto 2, del regolamento (UE) 2016/679 in materia di dati personali o all'articolo 3, punto (2), del Regolamento (UE) 2018/1807 in materia di dati non personali» [26].

Secondo la norma di rinvio di cui all'art. 4 n. 2, GDPR, si definisce come: «2) «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione».

Quanto al livello di sicurezza da garantire all'archiviazione, trattamento e trasmissione di dati non personali, la condizione in esame impone che sia assicurato mediante l'adozione di «misure necessarie». L'espressione è atipica e non solo non esclude nessuna misura – tecnica, organizzativa e giuridica – ma ancora una volta la modulazione è rimessa alla responsabilizzazione dell'intermediario, il quale dovrà garantire un adeguato livello di sicurezza in relazione alla valutazione del rischio.

Per definire cosa debba intendersi per «misure necessarie» da adottarsi in concreto per garantire il fine di un «adeguato livello di sicurezza», si può fare riferimento all'analogo art. 32 [27] del GDPR, il quale, essendo molto più ampio e detta-

---

[26] Reg. (UE) 2018/1807 del Parlamento Europeo e del Consiglio del 14 novembre 2018 relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea (Testo rilevante ai fini del SEE), GUUE L 303/59, 28.11.2018 IT, in https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32018R1807&from=IT.

[27] Così recita l'art. 32 GDPR: «Sicurezza del trattamento

1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto,

gliato, può costituire un criterio orientatore per la specificazione della portata della norma in commento.

A tal proposito, va sgomberato il campo dal rischio di confusione tra l'espressione «misure necessarie» usata nelle condizioni dell'art. 12 DGA e l'analoga rinvenibile anche nel Considerando n. 55 [28] e nell'art. 34 [29] dello stesso DGA. Si tratta di una mera assonanza che non deve trarre in inganno, atteso che in tali contesti l'espressione indica il diverso obbligo di adozione a carico dei Paesi membri delegati delle misure finalizzate a garantire l'applicazione delle sanzioni alle violazioni del Regolamento DGA.

---

del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) la pseudonimizzazione e la cifratura dei dati personali;

b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo.

4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri».

[28] Così recita il *considerando* n. 55: «Gli Stati membri dovrebbero stabilire norme in materia di sanzioni applicabili alle violazioni del presente regolamento e adottare tutte le misure necessarie per garantirne l'applicazione. Le sanzioni previste dovrebbero essere effettive, proporzionate e dissuasive. Discrepanze sostanziali tra le norme in materia di sanzioni potrebbero portare a una distorsione della concorrenza nel mercato unico digitale. L'armonizzazione di tali norme potrebbe essere utile a tal riguardo».

[29] Così recita l'art. 34 GDA: «Sanzioni 1. Gli Stati membri stabiliscono le norme relative alle sanzioni da applicare in caso di violazione degli obblighi in materia di trasferimento di dati non personali a paesi terzi a norma dell'articolo 5, paragrafo 14, e dell'articolo 31, dell'obbligo di notifica per i fornitori di servizi di intermediazione dei dati a norma dell'articolo 11, delle condizioni per la fornitura di servizi di intermediazione dei dati a norma dell'articolo 12, e delle condizioni per la registrazione come organizzazione per l'altruismo dei dati riconosciuta a norma degli articoli 18, 20, 21 e 22 e adottano tutte le misure necessarie per assicurarne l'applicazione. Le sanzioni previste devono essere effettive, proporzionate e dissuasive. Nelle loro norme in materia di sanzioni, gli Stati membri tengono conto delle raccomandazioni del comitato europeo per l'innovazione in materia di dati. Entro il 24 settembre 2023, gli Stati membri notificano tali norme e misure alla Commissione e notificano ad essa senza ritardo eventuali successive modifiche ad esse pertinenti».

La seconda parte della Condizione sub lett. *l*) dell'art. 12 DGA, invece, obbliga l'intermediario ad assicurare «il massimo livello di sicurezza per la conservazione e la trasmissione di informazioni sensibili sotto il profilo della concorrenza».

Dal punto di vista qualitativo, la norma focalizza la sua operatività sulle «informazioni sensibili» rientranti o attinenti al settore della concorrenza, circoscrivendo l'ambito di protezione alle informazioni relative ai diritti sui segreti commerciali e proprietà intellettuale con l'intento di assicurarlo da eventuali rischi di attività di concorrenza sleale o illecite e per evitare che la disponibilità di tali dati consenta vantaggi illeciti per i concorrenti di paesi extra UE [30].

Essendo costituito da ogni «informazione sensibile», l'oggetto della protezione risulta quinti molto più ampio di quello considerato dalla prima parte della norma, in quanto non è limitato ai «dati» (non personali) inteso come «rappresentazione digitale di informazioni» ex art. 2, n. 1, DGA.

Pertanto, la condizione impone di proteggere ogni informazione, a prescindere dalla tipologia o forma della sua rappresentazione, e quindi, anche l'informazione sensibile che sia rappresentata con strumenti o tecniche analogiche.

E a differenza di quanto previsto nella prima parte della norma in esame, nella seconda parte le azioni da proteggere sono limitate a quelle di «conservazione» (*rectius*: archiviazione) e di «trasmissione», pretermettendo il «trattamento», e quindi tutte le operazioni rientranti in tale *genus*.

Il Regolamento non consente di comprendere per quale motivo il legislatore abbia escluso le operazioni di «trattamento», per quanto sarebbe plausibile rinvenirlo nella più ampia estensione della seconda parte della Condizione alle «informazioni» che, come si è già detto, per quanto priva di definizione tipica, è da intendersi come termine più ampio di «dati».

Pertanto, poiché la seconda parte della norma riguarda le «informazioni», che non sono trattate solo in modalità automatizzata, ad esse non è pedissequamente applicabile né il concetto di «trattamento», né le operazioni rientranti nel suo spettro, né nella definizione dell'art. 12, n. 12), che viene specificato come: «(…) definito all'articolo 4, punto 2, del regolamento (UE) 2016/679 in materia di dati personali o all'articolo 3, punto (2), del Regolamento (UE) 2018/1807 in materia di dati non personali».

Il legislatore, ritenendo le informazioni oggetto solo di archiviazione e trasmissione ma estranee al concetto di «trattamento», potrebbe aver quindi escluso quest'ultimo dal novero delle azioni da proteggere.

Tornando ai rischi di utilizzi anticoncorrenziali delle informazioni, la preoccupazione del Legislatore europeo circa l'uso distorto se non illecito delle informazioni emerge evidente nel *considerando* n. 20, a tenore del quale: «È inoltre di estre-

[30] Altre norme a protezione delle informazioni commerciali sono previste dalla Direttive (UE) 2016/943 del Parlamento Europeo e del Consiglio dell'8 giugno 2016 sulla protezione del know-how riservato e delle informazioni commerciali riservate (segreti commerciali) contro l'acquisizione, l'utilizzo e la divulgazione illeciti (Testo rilevante ai fini del SEE).

ma importanza, al fine di preservare una concorrenza leale e l'economia di mercato aperta, salvaguardare i dati protetti di natura non personale, in particolare i segreti commerciali, ma anche i dati non personali che costituiscono un contenuto protetto da diritti di proprietà intellettuale da un accesso illecito che possa portare al furto della proprietà intellettuale o allo spionaggio industriale. Al fine di garantire la protezione dei diritti o degli interessi dei titolari dei dati, possono essere trasferiti a paesi terzi i dati non personali che devono essere protetti da accessi illeciti o non autorizzati in conformità del diritto dell'Unione o nazionale e che sono detenuti da enti pubblici, ma solo allorché sono previste tutele adeguate per l'utilizzo dei dati. (…)».

A tal fine, la seconda parte della Condizione impone al fornitore di servizi di intermediazione dei dati di assicurare «il massimo livello di sicurezza» per la conservazione (*rectius*: «*archiviazione*») e la trasmissione di informazioni sensibili sotto il profilo della concorrenza.

La norma non indica quali misure garantiscano e realizzino il livello massimo di sicurezza, ma può ritenersi che debbano essere adottate tutte le misure che la tecnologia mette a disposizione, in modo tale da assicurare il *non plus ultra* della protezione e risulti impossibile fare di più rispetto a quanto lo stato della tecnica metta a disposizione per la protezione dei dati. Nell'obbligo di assicurazione rientra altresì quello di verifica dell'efficacia delle misure massime, nonché il loro riesame e aggiornamento ove necessario, come ad esempio nel caso in cui il progresso tecnologico consenta l'adozione di nuove misure di innalzamento del livello massimo di sicurezza.

A tal fine esistono vari sistemi di misurazione dei livelli di sicurezza dei dati e delle informazioni, come ad esempio quelli implementati da istituti di standardizzazione statale, internazionale, quali ad es. gli Standard ISO, o da enti governativi, quali ad es. il NIST.

Tra le molteplici misure adottabili per limitare gli effetti di tale rischio, il Considerando appena citato indica espressamente come «adeguate», le misure volte ad implementare contratti aventi ad oggetto la protezione dei dati, l'assunzione del rispetto del Regolamento da parte di un riutilizzatore che intende trasferire i dati protetti a un tale paese terzo anche dopo il trasferimento e l'accettazione della giurisdizione dello Stato.

6. Considerazioni comuni alle norme esaminate.

6.1. Misure di sicurezza e livelli di protezione.

Nell'ambito del Regolamento, diverse norme menzionano previsioni o obblighi a carico di vari soggetti e a vario titolo, di adottare misure di protezione dei dati o delle informazioni, graduate in relazione al livello di protezione da garantire e con finalità di volta in volta diverse.

È un sistema che fissa un rapporto tra misure di sicurezza, da intendersi come strumento, e il livello di sicurezza da intendersi come fine da realizzare.

Quello delle misure di sicurezza dei dati in generale, è un tema affatto nuovo, che ha trovato costante ricorrenza nella normativa unionale, a partire dalla primissima disciplina sul trattamento dei dati personali, in particolare dal varo del GDPR [31], sino ai più recenti regolamenti dell'ambito digitale.

In linea di prima approssimazione, può ritenersi che l'ampia teorica [32] e prassi [33] basate sui principi del *Risk Management Approach* già sviluppatasi intorno alle misure di sicurezza per il trattamento dei dati personali trova un'ampia base comune con le esigenze del DGA, ed in particolare delle norme ripercorse, salvo alcuni necessari adattamenti imposti dallo specifico normativo in esame.

Tuttavia, nel Regolamento in esame si annovera una serie di previsioni alquanto eterogenee e difficilmente classificabili in uno schema pur approssimativo basato sul rapporto tra misure di sicurezza e livello di protezione da garantire.

L'analisi può portare al più ad una catalogazione basata sul criterio di graduazione qualitativa e quantitativa del rapporto tra misure di sicurezza e livello di protezione, che può costituire un sistema di primo orientamento tra le diverse previsioni.

Ponendo l'attenzione alle misure di sicurezza, ad un primo livello si richiede l'adozione di «adeguati requisiti tecnici e di sicurezza» per la conservazione e il trattamento dei dati, per garantire l'«opportuno livello» di sicurezza, così come ad esempio previsto dall'art. 22, par. 1, lett. *b*).

Un secondo livello, prevede l'adozione di «tutte le misure ragionevoli», come menzionato dal *considerando* n. 23 (per prevenire un accesso illecito a dati non personali) e dall'art. 31 per il quale i soggetti annoverati dalla norma sull'«Accesso internazionale e trasferimento», adottarono «(…) tutte le ragionevoli misure tecniche, giuridiche e organizzative, compresi accordi contrattuali, per impedire il trasferimento internazionale di dati non personali detenuti nell'Unione o l'accesso a questi ultimi da parte delle autorità pubbliche qualora tale trasferimento o accesso confliggesse con il diritto dell'Unione o il diritto nazionale dello Stato membro pertinente, fatto salvo il paragrafo 2 o 3.»

---

[31] Sul tema delle misure di sicurezza dei dati personali in ambito GDPR, con un *excursus* normativo, si veda il recente G.M. BILOTTA-D. SBORLINI-I. SCARPELLI, *Il principio di integrità e riservatezza (rectius, di sicurezza)*, in F. BRAVO (a cura di), *Dati personali. Protezione, libera circolazione e governance.* – Vol. 1. *Principi*, cit., p. 333 ss.

[32] Sul punto si richiamano le ampie trattazioni di F. BRAVO, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, in V. CUFFARO-R. D'ORAZIO-V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, pp. 775-854; nonché F. BRAVO, *Data Management Tools and Privacy by Design and by Default*, in R. SENIGAGLIA-C. IRTI-A. BERNES (eds.), *Privacy and Data Protection in Software Services*, Springer, 2022, pp. 85-95; P. PERRI, *Privacy, diritto e sicurezza informatica*, Milano, 2007; P. PERRI, *Protezione dei dati e nuove tecnologie. Aspetti nazionali, europei e statunitensi*, Milano, 2007.

[33] Cfr. ENISA, *Manuale sulla Sicurezza nel trattamento dei dati personali*, 2017.

Ad un ulteriore livello, operano le «misure adeguate» previste dall'art. 12 lett. *i*), per il quale il fornitore di servizi di intermediazione dei dati è tenuto ad adottarle per garantire l'interoperabilità con altri servizi di intermediazione dei dati, e dall'art. 12, lett. *j*), che prevede «adeguate misure tecniche, giuridiche e organizzative al fine di impedire il trasferimento di dati non personali o l'accesso a questi ultimi nel caso in cui ciò sia illegale a norma del diritto dell'Unione o del diritto nazionale dello Stato membro interessato».

Per «adeguate», non si intendono alcune misure tipizzate o ipotizzabili in «assoluto» e astrattamente, ma si fa riferimento a strumenti e attività che siano in concreto idonei a contrastare i rischi cui sono esposti i dati e/o le informazioni.

Nel testo dell'art. 21, par. 4, il requisito dell'adeguatezza slitta sul livello da garantire: «L'organizzazione per l'altruismo dei dati riconosciuta adotta misure intese a garantire un livello adeguato di sicurezza per la conservazione e il trattamento di dati non personali che ha raccolto sulla base dell'altruismo dei dati.)».

Al medesimo livello, operano le tutele adeguate, menzionate sia per le misure equivalenti per un livello di protezione analogo di cui al *considerando* n. 21 in tema di trasferimento di dati («Si dovrebbe inoltre prendere in considerazione l'applicazione di tutele adeguate se, nel paese terzo verso il quale vengono trasferiti i dati personali, sono in vigore misure equivalenti che garantiscono che i dati beneficino di un livello di protezione analogo a quello applicabile mediante il diritto dell'Unione)», sia all'art. 5, par. 9.

Ed ancora, un rafforzamento ulteriore del criterio di adeguatezza delle misure è da attribuirsi all'uso dell'aggettivo «necessario» nell'accezione di misure assolutamente «non derogabili», che viene utilizzato nella previsione di «misure necessarie per un livello adeguato» di cui all'art. 12 l) («il fornitore di servizi di intermediazione dei dati adotta le misure necessarie per garantire un adeguato livello di sicurezza per la conservazione, il trattamento e la trasmissione di dati non personali, e il fornitore di servizi di intermediazione dei dati assicura inoltre il massimo livello di sicurezza per la conservazione e la trasmissione di informazioni sensibili sotto il profilo della concorrenza»).

A tale previsione di assolutezza delle misure di sicurezza, si aggiunge l'assolutezza del fine da realizzare del «livello massimo» di sicurezza, previsto dall'art. 12, lett. *l*), DGA «(…) il fornitore di servizi di intermediazione dei dati assicura inoltre il massimo livello di sicurezza per la conservazione e la trasmissione di informazioni sensibili sotto il profilo della concorrenza».

Come si è appena visto, si tratta di obblighi di adozione di misure di sicurezza denotate da attributi modulati in rapporto alla finalità che richiedono livelli di crescente robustezza.

La scelta degli strumenti e delle azioni che in concreto perseguono e realizzano le finalità imposte dalla norma è, come si è già detto, rimessa all'obbligato, il quale non potrà che basarsi su procedure di analisi del rischio, adozione delle misure che ne mitigano l'impatto, e con azioni di costante verifica, revisione e aggiornamento.

6.2. Le sanzioni (cenni).

Come si è già accennato, e come sarà meglio trattato dall'Autore del commento delle norme sulle sanzioni, il Regolamento non prevede espressamente sanzioni conseguenti all'inosservanza delle condizioni, la cui previsione è invece rimessa agli stati membri.

Infatti, l'art. 12 fa altresì parte del novero delle norme previste dall'art. 34, per il quale il Regolamento rimanda agli Stati membri stabilire «...le norme relative alle sanzioni da applicare in caso di violazione (…) delle condizioni per la fornitura di servizi di intermediazione dei dati a norma dell'articolo 12 (…)».

Il Regolamento impone altresì che, ove i paesi membri adottino sanzioni, queste siano effettive, proporzionate e dissuasive e la loro imposizione segua i criteri previsti dall'art. 34, par. 2, DGA.

Ciò che rileva a proposito delle norme in commento, è che i legislatori dei singoli Stati membri potrebbero discrezionalmente optare per un rafforzamento della cogenza del Regolamento all'interno dell'ordinamento statale introducendo sanzioni da comminarsi nei casi di violazioni delle condizioni da parte degli intermediari.

Tuttavia, l'attuale formulazione della delega della potestà sanzionatoria a ciascun Stato membro avalla la prevedibilità di regimi sanzionatori differenti e soprattutto a diversa intensità afflittiva. Le differenze delle reazioni sanzionatorie, sino alla possibilità che in alcuni paesi non siano comminate affatto sanzioni, potrebbero consentire la creazione di zone franche e quindi innescare situazioni di disparità di trattamento all'interno dell'Unione.

Tale discrepanza potrebbe quindi favorire lo sviluppo di aree che essendo a minor rischio sanzionatorio, attraggono lo stabilimento degli intermediari, così alterando l'equilibrio di un corretto rapporto concorrenziale.

L'eventualità appena esposta non è peregrina, atteso che lo stesso legislatore nella seconda parte del *considerando* n. 55 fa espressa previsione di una possibile alterazione della correttezza concorrenziale: «Gli Stati membri dovrebbero stabilire norme in materia di sanzioni applicabili alle violazioni del presente regolamento e adottare tutte le misure necessarie per garantirne l'applicazione. Le sanzioni previste dovrebbero essere effettive, proporzionate e dissuasive. Discrepanze sostanziali tra le norme in materia di sanzioni potrebbero portare a una distorsione della concorrenza nel mercato unico digitale. L'armonizzazione di tali norme potrebbe essere utile a tal riguardo».

Solo l'esperienza applicativa del Regolamento potrà confermare o meno tali eventualità, ove tuttavia l'Unione, in coda al *considerando* n. 55 si è riservata la facoltà di implementare azioni correttive di eventuali effetti distorsivi della concorrenza.

Ma allo stato, il Considerando, pur prevedendo le potenziali disparità che verranno a crearsi tra i diversi trattamenti sanzionatori, auspica solo un'armonizzazione connotata anch'essa più dalle buone intenzioni che non da un'espressa e precisa previsione.

Pertanto, l'attuale ricomprensione delle condizioni dell'art. 12 nel novero delle norme sanzionate solo ove gli stati membri vi provvederanno (o meno), non costituisce un presupposto uniforme, cosicché la concreta attuazione di quanto previsto dalle norme appena commentate dipenderà molto dall'esito dell'evoluzione di tali aspetti.

6.3. Sulla prova della conformità alle disposizioni.

Le condizioni dell'art. 12 appena analizzate, rientrano anche nella previsione dell'art. 11, par. 9, DGA, a tenore del quale «Su richiesta del fornitore di servizi di intermediazione dei dati, l'autorità competente per i servizi di intermediazione dei dati conferma, che il fornitore di servizi di intermediazione dei dati è conforme alle disposizioni di cui al presente articolo e all'articolo 12 (...)».

Pertanto, la norma attribuisce all'Autorità per i servizi di intermediazione di rilasciare a richiesta dello stesso intermediario il risultato di una procedura di valutazione che esita in una dichiarazione di «conferma», ovvero una sorta di certificazione di conformità alle disposizioni dell'art. 12. L'intermediario potrà spendere tale riconoscimento formale e «fregiarsi» del titolo di «fornitore di servizi di intermediazione dei dati riconosciuto nell'Unione» che potrà comunicare ai terzi per iscritto o verbalmente, unitamente a un logo comune graficamente identificato, come previsto dallo stesso articolo. «(…) Una volta ricevuta detta conferma, il fornitore di servizi di intermediazione dei dati in questione può utilizzare il titolo "fornitore di servizi di intermediazione dei dati riconosciuto nell'Unione" nelle sue comunicazioni scritte e orali, nonché un logo comune.

Per garantire che i fornitori di servizi di intermediazione dei dati riconosciuti nell'Unione siano facilmente identificabili in tutta l'Unione, la Commissione stabilisce, mediante atti di esecuzione, un disegno per il logo comune. I fornitori di servizi di intermediazione dei dati riconosciuti nell'Unione espongono il logo comune in modo chiaro su ciascuna pubblicazione online e offline relativa alle loro attività di intermediazione dei dati (…)».

Tuttavia, l'Autorità per i servizi di intermediazione può in ogni momento monitorare e controllare la conformità ai requisiti del Capo III, tra i quali l'art. 12, come previsto dall'art. 14, par. 1, DGA: «Articolo 14 Monitoraggio della conformità 1. Le autorità competenti per i servizi di intermediazione dei dati monitorano e controllano la conformità dei fornitori dei servizi di intermediazione dei dati ai requisiti di cui al presente capo. Le autorità competenti per i servizi di intermediazione dei dati possono inoltre monitorare e controllare la conformità dei fornitori dei servizi di intermediazione dei dati sulla base di una richiesta da parte di persone fisiche o giuridiche. (…)».

Vieppiù che ai sensi dell'art. 14, c. 2, DGA, «(…) 2. Le autorità competenti per i servizi di intermediazione dei dati hanno il potere di chiedere ai fornitori di servizi di intermediazione dei dati o ai loro rappresentanti legali tutte le informazioni necessarie per verificare la conformità ai requisiti di cui al presente capo. Le richie-

ste di informazioni sono motivate e proporzionate rispetto all'assolvimento del compito. (…)».

Tale previsione attribuisce all'Autorità un potere di verifica e le consente di constatare il mancato rispetto di uno o più requisiti di conformità al III Capo e di comunicarlo all'intermediario, aprendo così una procedura in contraddittorio prevista dal comma 3 e soggetto al termine di 30 giorni per l'esercizio da parte dell'intermediario della facoltà di esprimere osservazioni.

All'esito della procedura, l'Autorità può imporre l'ordine di cessazione della violazione o, in caso di violazioni grave, di adottare misure adeguate e proporzionate con finalità ripristinatoria *ex* Capo III DGA.

In tal caso, l'Autorità ha diversi poteri: dall'imposizione di sanzioni pecuniarie, periodiche, con effetto retroattivo, all'avvio di procedimenti giudiziari per la comminatoria di ammende, o entrambe le misure (art. 14, par. 4, lett. *a*), o il rinvio dell'inizio o la sospensione del servizio di intermediazione (art. 14, par. 4, lett. *b*), o la sua cessazione nei casi di violazioni più gravi o ripetute (art. 14, par. 4, lett. *c*).

Inoltre, come già visto precedentemente, tra gli strumenti reattivi e coattivi vanno annoverate anche le sanzioni che gli Stati membri, ai sensi dell'art. 34 DGA, potranno prevedere nei rispettivi ordinamenti per i casi di violazione dei vari obblighi, a norma dell'art. 5, par. 14, e dell'art. 31, dell'art. 11, e ai fini della nostra disamina, delle condizioni per la fornitura di servizi di intermediazione dei dati a norma dell'art. 12.

Sia le previsioni dell'art. 14 che quelle dell'art. 34 DGA portano a forme diverse di procedimentalizzazione del contraddittorio, che quindi prevedono un onere della prova gravante sull'intermediario ed avente ad oggetto proprio l'avvenuto rispetto delle condizioni e obblighi posti dal DGA.

Pertanto, i soggetti obbligati che si conformano al Regolamento dovrebbero valutare come opportuna, l'adozione per tempo debito di quelle azioni che consentono di acquisire e mantenere gli elementi di prova delle azioni e procedure preventive messe in atto, al fine di poter dimostrare, ove richiesto o utile o necessario, quanto correttamente svolto.

A tal fine, l'intermediario dovrebbe ritenere opportuno e conveniente adottare quegli strumenti, tecniche e procedure di documentazione dell'attività di conformazione svolta, al fine di potere, in un momento successivo, adempiere al proprio onere della prova che, in tali contesti, e soprattutto in caso di coinvolgimento delle Autorità indipendenti e dell'Autorità giudiziaria, si presenta sempre alquanto arduo e comunque urgente.

Considerazioni solo parzialmente sovrapponibili possono farsi in relazione al fornitore di servizi di intermediazione dei dati che non è stabilito nell'Unione, ma che offre all'interno dell'Unione i servizi di intermediazione dei dati di cui all'art. 10.

Orbene, ai sensi dell'art. 11, par. 3, DGA, egli è tenuto a designare un rappresentante legale in uno degli Stati membri in cui offre tali servizi di intermediazione. A sua volta, il rappresentante legale, tra le altre cose, nel collaborare con le autorità competenti per i servizi di intermediazione dei dati e, «(…) su richiesta, dimostra

loro in modo esauriente le misure adottate e le disposizioni messe in atto dal fornitore di servizi di intermediazione dei dati per garantire la conformità al presente regolamento».

Anche in tal caso, è opportuno che l'intermediario si attrezzi in tempo debito con strumenti, tecniche e procedure di documentazione dell'attività svolta al fine di uniformarsi al Regolamento, che gli consentano di acquisire, mantenere e fornire gli elementi di prova delle procedure preventive messe in atto.

7. Conclusioni.

All'esito di questa prima disamina, necessariamente parziale e incompleta, delle condizioni di sicurezza di cui all'art. 12, lett. *g*), *l*) e *j*), DGA, sono emersi alcuni elementi ricorrenti nelle norme osservate.

Il primo luogo, alcuni termini del testo italiano del Regolamento si presentano incongruenti rispetto a quelli delle altre versioni ufficiali, ricorrenze che introducono incertezze che non agevolano l'esegesi e che darà luogo ad incertezze in sede applicativa interna rispetto a quelle di altri paesi membri.

Inoltre, le modalità con le quali la formulazione del regime sanzionatorio delle violazioni delle condizioni di cui all'art. 12 è stato delegato agli Stati membri, non potrà mancare di creare questioni di uniformità, uguaglianza e concorrenza che prima o poi emergeranno creando aree di insediamento degli operatori preferibili rispetto ad altre.

Infine, in relazione alle misure da attuare, la sola disamina di tre condizioni ha portato a graduare la conformità ad almeno tre livelli di misure, necessarie, ragionevoli e adeguate, attributi che non contribuiscono affatto ad incrementare la certezza degli obblighi.

In relazione a tali aspetti, sarebbe utile quantomeno un'azione di revisione o di integrazione di secondo livello.

I dubbi emersi dalla prima lettura delle norme appena ripercorse non potranno che trovare risposta nei primi orientamenti applicativi.

Capitolo XLIV

Le cooperative di dati e l'art. 12, lett. *l*), del *Data Governance Act* nel quadro delle disposizioni volte a soddisfare esigenze di sicurezza nella fornitura di servizi di intermediazione dei dati

Francesca Mollo

Abstract: This paper analyses the condition for the provision of data intermediation services dictated by art. 12, lett. l) of the Data Governance Act, highlighting its critical aspects, in comparison with European data protection law, with particular reference to articles 24 and 32 GDPR.

1. Introduzione.

Nella odierna «società dell'accesso» [1], in cui la persona è sempre più digitalizzata, profilata e trasparente, nel quadro della strategia europea dei dati e del progetto di mercato unico dei dati [2], con l'emanazione del *Data Governance Act* (*DGA*),

[1] J. RIFKIN, *L'era dell'accesso*, Milano, 2001, p. 17 ss.

[2] Tale progetto di mercato unico dei dati, presentato nel febbraio 2020, si inserisce in un quadro normativo già delineato dalle istituzioni europee negli anni precidenti con la direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche; con il regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (GDPR); con il Regolamento (UE) n. 2018/1807 del Parlamento europeo e del Consiglio, del 14 novembre 2018, relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea, GUUE 303 del 28 novembre 2018, p. 59; con la direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio del 20 giugno 2019 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico.

regolamento UE 2022/868 [3], si viene in qualche modo delineando un nuovo o quantomeno inedito paradigma di utilizzo e condivisione dei dati.

Nel quadro degli obiettivi della Commissione europea [4], intesi a percorrere scelte orientate sostenere gli spazi europei di dati [5], infatti, il mercato unico di dati deve rappresentare uno spazio «(...) aperto ai dati provenienti da tutto il mondo (...) nel quale sia i dati personali sia quelli non personali, compresi i dati commerciali sensibili, siano sicuri e le imprese abbiano facilmente accesso a una quantità pressoché infinita di dati industriali di elevata qualità, che stimolino la crescita e creino valore, riducendo nel contempo al minimo l'impronta di carbonio e ambientale».

Nell'ottica del legislatore europeo del *DGA*, ciò appare possibile stimolando una maggiore condivisione dei dati da parte dei cittadini europei [6], aumentando la loro fiducia nella neutralità [7] e nell'affidabilità dei servizi di intermediazione [8], ciò

---

[3] Su cui, diffusamente, F. BRAVO, *Le cooperative di dati*, in *Contr. e impr.*, 2023, 3, pp. 757-799; nonché ID., *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in *Contr. e impr. Europa*, 2021, 1, p. 199 ss.

[4] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni. Una Strategia europea per i dati, Bruxelles, COM (2020) 66 final, p. 5.

[5] In particolare, incoraggiandone il mercato, al fine di sostenere la competitività delle imprese europee di fronte alle logiche proprietarie che caratterizzano i mercati extraeuropei. Cfr. L. PETRONE, *Il mercato digitale europeo e le cooperative di dati*, in *Contr. e impr.*, 2023, 3, pp. 800-817; G. ALPA, *La Proprietà dei dati personali*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, 2019, p. 11 ss.; F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, cit., in part. p. 210.

[6] L. PETRONE, *op. cit.*, p. 808.

[7] Cfr. *considerando* 33 del Reg. (UE) n. 868/2022, ove si legge che «Un elemento essenziale attraverso il quale aumentare la fiducia e il controllo dei titolari dei dati, interessati e utenti dei dati nei servizi di intermediazione dei dati è la neutralità dei fornitori di servizi di intermediazione dei dati riguardo ai dati scambiati tra titolari dei dati o interessati e utenti dei dati. È pertanto necessario che i fornitori di servizi di intermediazione dei dati agiscano solo in qualità di intermediari nelle transazioni e non utilizzino per nessun altro fine i dati scambiati».

[8] Cfr. *considerando* 5 del Reg. (UE) n. 868/2022 che prevede: «L'azione a livello dell'Unione è necessaria per aumentare la fiducia nella condivisione dei dati istituendo adeguati meccanismi che garantiscano il controllo da parte degli interessati e dei titolari dei dati sui dati che li riguardano e al fine di affrontare altri ostacoli al buon funzionamento di un'economia competitiva basata sui dati. Tale azione non dovrebbe pregiudicare gli obblighi e gli impegni negli accordi commerciali internazionali conclusi dall'Unione. Un quadro di governance a livello dell'Unione dovrebbe avere l'obiettivo di creare fiducia tra gli individui e le imprese per quanto riguarda l'accesso ai dati, la loro condivisione e il loro controllo, utilizzo e riutilizzo, in particolare stabilendo adeguati meccanismi per gli interessati affinché conoscano ed esercitino fattivamente i propri diritti nonché per quanto riguarda il riutilizzo di alcune tipologie di dati detenuti dagli enti pubblici, la fornitura di servizi da parte dei fornitori di servizi di intermediazione dei dati agli interessati, ai titolari e agli utenti dei dati, nonché la raccolta e il trattamento dei dati messi a disposizione a fini altruistici da persone fisiche e giuridiche. In particolare, una maggiore trasparenza per quanto riguarda la finalità dell'utilizzo dei dati e le condizioni in cui i dati sono conservati dalle imprese può contribuire ad aumentare la fiducia».

che impone in qualche modo un bilanciamento tra interessi maggiormente inteso alla più ampia circolazione dei dati, personali e non personali. E proprio nella prospettiva di un migliore sviluppo del mercato europeo, nel *Data Governance Act*, le esigenze di protezione dei dati prese in considerazione e disciplinate dal Reg. UE 679/2016 (GDPR), vengono ad essere conciliate con quelle del diritto al libero accesso e riuso dei dati medesimi.

D'altra parte, «Nella costante tensione tra il perseguimento di interessi economici e il guadagno di competitività del mercato europeo, da un lato, e la tutela della persona, dall'altro lato, emerge una chiara presa d'atto della rilevanza, anche patrimoniale, dei dati personali» [9].

Ecco che i principi ispiratori del DGA sono costituiti proprio dalla necessità di rendere disponibili i dati del settore pubblico per il riutilizzo; condividere dati tra le imprese; nonché consentire l'utilizzo, per motivi altruistici [10], dei dati, sia personali che non personali.

E ancora, si veda il *considerando* 22, laddove prevede che «Alcuni paesi terzi adottano leggi, regolamenti e altri atti giuridici che mirano a trasferire direttamente i dati non personali o a fornire un accesso diretto agli stessi da parte delle autorità pubbliche nell'Unione, sotto il controllo di persone fisiche e giuridiche poste sotto la giurisdizione degli Stati membri. Le decisioni e le sentenze di autorità giurisdizionali o le decisioni di autorità amministrative di paesi terzi che dispongono un tale trasferimento di dati non personali o l'accesso agli stessi dovrebbero avere carattere esecutivo quando sono basate su un accordo internazionale in vigore tra il paese terzo richiedente e l'Unione o un suo Stato membro, ad esempio un trattato di mutua assistenza giudiziaria. Possono in alcuni casi presentarsi situazioni in cui l'obbligo di trasferire i dati non personali, o di fornirvi accesso, derivante dalla normativa di un paese terzo, sia in conflitto con un obbligo concorrente di proteggere tali dati a norma del diritto dell'Unione o nazionale, in particolare per quanto riguarda la protezione dei diritti fondamentali della persona o degli interessi fondamentali di uno Stato membro connessi alla sicurezza nazionale o alla difesa, nonché la protezione dei dati commerciali sensibili e dei diritti di proprietà intellettuale, compresi anche gli obblighi contrattuali in materia di riservatezza conformemente a tale normativa. In assenza di accordi internazionali atti a disciplinare simili questioni, il trasferimento o l'accesso a dati non personali dovrebbero essere consentiti solo previa verifica, in particolare, che il sistema giuridico del paese terzo imponga che siano indicati i motivi e la proporzionalità della decisione o della sentenza, che la decisione o la sentenza abbia carattere specifico e che l'obiezione motivata del destinatario sia sottoposta a riesame da parte di un'autorità giurisdizionale competente nel paese terzo, cui sia conferito il potere di tenere debitamente conto dei pertinenti interessi giuridici del fornitore di tali dati. Inoltre, gli enti pubblici, le persone fisiche o giuridiche cui è stato concesso il diritto di riutilizzo dei dati, i fornitori di servizi di intermediazione dei dati e le organizzazioni per l'altruismo dei dati riconosciute dovrebbero garantire, al momento della firma di accordi contrattuali con altre parti private, che i dati non personali detenuti nell'Unione siano accessibili da parte di paesi terzi o ad essi trasferiti solo in conformità del diritto dell'Unione o del diritto nazionale dello Stato membro interessato».

[9] F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, cit., in part. pp. 210-211.

[10] In questo modo le imprese potrebbero condividere i propri dati insieme al relativo know how (conoscenze, esperienza e strumenti operativi, ad esempio software, algoritmi ecc. ...). Si parla, in proposito, di "*corporate philantropy*", con il quale si indica anche la condivisione di competenze e risorse per condurre analisi e divulgare i risultati per un uso più ampio. Cfr. M. STEMPECK, *Sharing Data Is a Form of Corporate Philanthropy*, in *Harvard Business Review*, 24 July 2014; J. GEORGE-D.E.

Il *Data Governance Act* prende specificamente in considerazione anche dati non personali, al fine di aggiungere norme di protezione analoghe a quelle vigenti per i dati personali ai sensi del GDPR, anche se pare difficile definire un dato "permanentemente non personale" [11]. In linea di principio e nella maggior parte dei casi, i set di dati condivisi tramite un fornitore di servizi di condivisione dei dati o un'organizzazione di altruismo dei dati potrebbero contenere anche dati personali [12]. Secondo l'*European Data Protection Board* [13], la definizione dei dati non personali risulterebbe poco chiara nel *DGA*, mentre più chiaro al riguardo sarebbe il regolamento (UE) 2018/1807 sulla libera circolazione dei dati non personali [14], che all'art. 2, par. 2 prevede che «Nel caso di una serie di dati composta sia da dati personali che da dati non personali, il presente regolamento si applica alla parte relativa ai dati non personali della serie di dati. Se i dati personali e non personali in un set di dati sono collegati inestricabilmente, il presente regolamento non pregiudica l'applicazione del regolamento (UE) 2016/679» [15].

LEIDNER-J. YAN, *Data Philanthropy: Corporate Responsibility with Strategic Value?*, in *Information Systems Management*, November 2019; I. SUSHA-J.R. GIL GARCIA, *A Collaborative Governance Approach to Partnerships Addressing Public Problems with Private Data*, *Proceedings of the 52nd Hawaii International Conference on System Sciences, 24 January 2019*.

[11] Cfr. Communication from the Commission to the European Parliament and the Council "*Guideline on the Regulation framework for free flow of non personal data in the European Union*", COM(2019)250, par. 2.1. Sul punto, cfr. F. ROSSI DAL POZZO-L. ZOBOLI, *To protect or (not) to protect: definitional complexities concerning personal (and non-personal) data within the EU*, in *rivista.eurojus.it*, 2021, p. 315 ss; T. STREINZ, *The Evolution of European Data Law, forthcoming* in P. CRAIG-G. DE BÚRCA (eds.), *The Evolution of EU Law,* Oxford, 2021; M. FINCK-F. PALLAS, *They Who Must Not Be Identified – Distinguishing Personal from Non-Personal Data under the GDPR*, in *International Data Privacy Law*, 2020, p. 11 ss.

[12] Cfr. F. CALOPRISCO, *Data Governance Act. Condivisione e "altruismo" dei dati*, in *AISDUE*, 2021, III, *aisdue.eu, Focus "Servizi e piattaforme digitali"*, n. 3, 5 maggio 2021 Annali AISDUE p. 58-75, secondo cui «Al riguardo, si possono distinguere categorie di dati non personali che hanno meno probabilità di essere qualificati come dati personali ma date le capacità analitiche in continuo sviluppo, è probabile che quasi tutti i tipi di dati possono essere elaborati insieme ad altri dati ed essere qualificati come dati personali. Infatti, i dati personali possono essere resi anonimi, diventando così dati non personali; al contrario, i dati non personali possono essere integrati con altri set di dati più complessi, consentendo così l'identificazione indiretta delle persone».

[13] EDPB-EDPS, *Joint Opinion* 03/2021.

[14] Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio del 14 novembre 2018 relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea, che riconosce alcune peculiarità rispetto ai dati personali con la salvaguardia delle norme sull'organizzazione interna degli Stati membri. Sul punto, rilevanti appaiono le norme che attribuiscono poteri, e conseguenti responsabilità, ad autorità pubbliche e organismi di diritto pubblico in materia di trattamento dei dati di titolarità di soggetti privati. In materia di "apertura dei dati", la direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio, del 20 giugno 2019, relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico (direttiva *open data*) ha successivamente fissato norme minime in materia di riutilizzo dei documenti.

[15] Secondo la Commissione europea, i dati non personali possono essere classificati in due modi

2. L'art. 12, lett. *l*), DGA nel quadro delle disposizioni volte a soddisfare esigenze di sicurezza.

Tra le condizioni previste dall'art. 12 del regolamento, per la fornitura di servizi di intermediazione dei dati, la lett. *l*) prevede che «il fornitore di servizi di intermediazione dei dati adotta le misure necessarie per garantire un adeguato livello di sicurezza per la conservazione, il trattamento e la trasmissione di dati non personali, e il fornitore di servizi di intermediazione dei dati assicura inoltre il massimo livello di sicurezza per la conservazione e la trasmissione di informazioni sensibili sotto il profilo della concorrenza».

Tale disposizione si colloca nel quadro delle disposizioni che mirano a soddisfare esigenze di sicurezza, ed in particolare:

– la *business continuity*, che si traduce anche nella recuperabilità dei dati conferiti e trattati dal fornitore, nonché nell'accessibilità ai medesimi, in caso di eventi che possano compromettere il sistema di trattamento e gestione dei dati (lett. *h*);

– le procedure per la prevenzione di pratiche fraudolente o abusive a danno dei soggetti che richiedono l'accesso ai servizi di intermediazione (lett. *g*);

– l'adozione di procedure tecniche, giuridiche ed organizzative per impedire il trasferimento di dati non personali o l'accesso ad essi, nel caso in cui ciò contrasti con il diritto europeo o nazionale (lett. *j*);

– in una prospettiva *ex post*, infine, l'obbligo di informare senza ritardo il "titolare dei dati" qualora si verifichino ipotesi di *data breach* e, segnatamente, nei casi di trasferimento, accesso o utilizzo non autorizzati dei dati non personali che questi abbia condiviso tramite il servizio di intermediazione (ovvero, ai fini del nostro discorso, tramite la cooperativa di dati).

Il legislatore distingue due livelli di sicurezza esigibile in capo al fornitore di servizi di intermediazione di dati. Il primo, inteso ad assicurare un livello di sicurezza quantomeno «adeguato», che onera lo stesso fornitore di adottare le misure necessarie al fine di garantire tale adeguato livello di sicurezza in ordine alla conservazione, al trattamento e alla trasmissione di dati non personali, nell'accezione e nel senso già *supra* indicati.

Il secondo, invece, attinge a un livello «massimo» di sicurezza in relazione alla conservazione e la trasmissione di informazioni sensibili sotto il profilo della concorrenza.

Sotto il primo profilo, con formulazione perentoria, nel prevedere che il fornitore di servizi di intermediazione dei dati «adotta le misure necessarie, il legislatore

---

diversi a seconda dell'origine: dati che sin dall'inizio non riguardano una persona fisica identificata o identificabile (come i dati meteorologici); dati che inizialmente erano personali e solo successivamente sono diventati anonimi attraverso un processo di anonimizzazione. Tuttavia, il potenziale di reidentificazione è aumentato a causa dei progressi tecnologici, rendendolo "ragionevolmente più probabile". Si veda, sul punto, anche il *considerando* 26 del GDPR. Cfr. anche Corte di giustizia UE, sentenza del 19 ottobre 2016, causa C-582/14, Breyer, punto 38 ss. in tema di indirizzi IP "dinamici".

ha inteso, quindi, responsabilizzare lo stesso in ordine all'adozione di misure che rispondano a criteri di adeguatezza [16] tanto sotto il profilo tecnico, in considerazione dell'evoluzione tecnologica e dello stato dell'arte (con riferimento allo specifico settore di cui di volta in volta si tratta), quanto sotto il profilo organizzativo, presupponendo una sinergia tra competenze diverse e complementari, e costituendo una buona prova sul campo di quel dialogo ormai costante tra diritto e tecnica [17], intercettato dal legislatore europeo già quasi un decennio fa in sede di emanazione del GDPR, che abbraccia sul punto una visione integrata che combina fra loro competenze tecnico-informatiche e organizzative con competenze squisitamente giuridiche, in funzione di protezione a tutto tondo delle libertà e dei diritti delle persone fisiche coinvolte [18].

Sotto il profilo organizzativo, potrebbero venire in rilievo, misure organizzative, che attengano, ad esempio, alla ripartizione dei ruoli, alla governance, alle procedure e sistemi di audit e di controllo di cui si alimenta il circuito informativo che sta alla base dei meccanismi di protezione degli interessati; mentre sotto il profilo tecnologico, misure che attengano a *policy* di sicurezza logiche e fisiche, aggiornamenti di servizi e *software*, attività di *test* e *check*, nonché controllo accessi e tracciamento operazioni, nonché meccanismi che attengano alla minimizzazione dei dati, e più in generale che ineriscono alla qualità dei dati stessi e alla loro adeguata conservazione.

Con l'imporre misure «per garantire un livello di sicurezza adeguato» si chiede perciò di operare una prognosi *ex ante*, anche in ordine al verificarsi di rischi correlati al trattamento, conservazione o trasmissione dai dati, in relazione anche alla natura, oggetto, contesto e finalità del trattamento stesso, finanche dello stato dell'arte e dei costi di attuazione collegati.

Il termine «appropriate», poi, tradotto come «adeguato», declinato in relazione alle predette misure tecniche e organizzative e in relazione al livello di sicurezza da garantire, evoca in effetti proprio questa valutazione *ex ante*, peraltro calata nel caso concreto, in ragione delle sue caratteristiche peculiari.

Più in generale, il rischio può essere rappresentato in funzione della probabilità di una minaccia, della vulnerabilità (dei sistemi) e del danno (R = M x V x D), laddove per minaccia si intende qualsiasi incidente potenziale che metta in pericolo i

---

[16] Il giudizio di adeguatezza, in particolare deve essere parametrato in base a diversi criteri, quali le conoscenze acquisite in base al progresso tecnico, nonché la natura dei dati e le specifiche caratteristiche del trattamento. Si tratta pertanto di un'adeguatezza in concreto e non meramente in astratto, sulla base delle circostanze del caso concreto.

[17] In tema si veda G. FINOCCHIARO, *Introduzione al Regolamento europeo sulla protezione dei dati*, in *Nuove leggi civ. comm.*, 2017, 1, p. 1 ss.; nonché ID., *Riflessioni su diritto e tecnica*, in *Dir. inform*., 2012, pp. 831-841.

[18] In tema di obblighi previsti dal regolamento in funzione di protezione dei dati personali, sia consentito rinviare a F. MOLLO, *Gli obblighi previsti in funzione di protezione dei dati personali*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, cit., pp. 255-292.

dati e costituisca dunque un possibile *vulnus*, e che può essere di diversa origine (interna, esterna, ambientale ...) o causa (carenze organizzative, dolo o colpa *etc.*); e per vulnerabilità la capacità del sistema di sicurezza dell'impresa titolare del trattamento di contrastare tali minacce. Sono in astratto evocabili diverse dimensioni di sicurezza, da quella logica, che riguarda principalmente la protezione dell'informazione, delle applicazioni, sistemi e reti, sia in relazione al loro corretto funzionamento e utilizzo, che alla loro gestione e manutenzione nel tempo, a quella fisica (in termini di autenticazione, controllo degli accessi, tutela della confidenzialità e integrità dei dati), fino a quella di tipo organizzativo-comportamentale, riguardante principalmente la definizione di ruoli e responsabilità in tutta la filiera sicurezza, l'adozione di specifiche procedure intese a completare e rafforzare le contromisure tecnologiche adottate, nonché gli aspetti relativi al controllo sulla consistenza e affidabilità degli apparati.

Medesime misure intese a garantire un adeguato livello di sicurezza, in ordine alla conservazione e al trattamento dei dati non personali, si ritrovano anche nell'art. 21, par. 4, in tema di obblighi specifici di tutela dei diritti e degli interessi degli interessati e dei titolari dei dati per quanto riguarda i loro dati, laddove si prevede che «L'organizzazione per l'altruismo dei dati riconosciuta adotta misure intese a garantire un livello adeguato di sicurezza per la conservazione e il trattamento di dati non personali che ha raccolto sulla base dell'altruismo dei dati».

Sotto il secondo profilo, la lett. *l*) richiede inoltre che il fornitore di servizi di intermediazione dei dati assicura inoltre il massimo livello di sicurezza per la conservazione e la trasmissione di informazioni sensibili sotto il profilo della concorrenza. L'importanza tributata alla concorrenza, nella specie alle informazioni sensibili sotto tale profilo, rende quindi necessario attingere ad un livello di sicurezza «massimo», qui, in ordine ai profili della conservazione e della trasmissione delle stesse. In via generale, si tratta di informazioni suscettibili per loro natura idonee a condizionare il comportamento delle imprese sul mercato, la cui circolazione appare particolarmente rischiosa quando riguardi variabili competitive strategiche quali i prezzi, i costi, le quantità vendute, i rapporti commerciali, soprattutto se disaggregati e riferiti alle condizioni attuali e future del mercato. Così, un elenco meramente esemplificativo di informazioni sensibili sotto il profilo *antitrust* potrebbe comprendere prezzi, volumi e condizioni di vendita (ad esempio, sconti, termini di pagamento, ecc.); clienti e mercati geografici di vendita (*client/market sharing*); costi di acquisto o di produzione, ecc.) e capacità produttiva; strategie imprenditoriali e di *marketing* (ad esempio investimenti, il lancio di un nuovo prodotto, ecc.); strategie di partecipazione a procedure di gara.

D'altra parte, gli stessi obiettivi di crescita sottesi alla normativa, come sottolineato pure dalla Commissione nella già citata Comunicazione «*Una strategia europea per i dati*» [19], sono di per sé collegati anche ai profili di tutela della concor-

[19] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economi-

renza, per cui il mercato unico dei dati dovrà essere costruito sulla libera circolazione dei dati all'interno dell'UE e a livello intersettoriale, con la creazione di «(...) spazi comuni europei in settori economici strategici e ambiti di interesse pubblico», l'introduzione di norme e di maccanismi che facilitino e garantiscano l'accesso ai dati ed il loro utilizzo e l'applicazione di standard europei nel mercato unico in particolare sotto il profilo della protezione dei dati personali, della tutela dei consumatori e della concorrenza [20].

3. Il raccordo con le disposizioni contenute nel GDPR.

I soggetti presi in considerazione dal DGA dovrebbero operare garantendo il pieno rispetto della disciplina dettata dal Regolamento UE 2016/67928 gestendo per conto dei titolari dei dati tutti i diritti degli interessati che lo stesso accorda loro.

Sul punto, il *considerando* n. 35 dispone che «Il presente regolamento dovrebbe lasciare impregiudicati l'obbligo incombente ai fornitori di servizi di intermediazione dei dati di rispettare il regolamento (UE) 2016/679 e la responsabilità delle autorità di controllo di garantire il rispetto di tale regolamento. Qualora i fornitori di servizi di intermediazione dei dati trattino dati personali, il presente regolamento non dovrebbe pregiudicare la protezione degli stessi. Qualora siano titolari del trattamento o responsabili del trattamento dei dati quali definiti nel Reg. (UE) 2016/679, i

co e sociale europeo e al Comitato delle regioni. Una Strategia europea per i dati, Bruxelles, COM (2020) 66 final, p. 24.

[20] Ancora, le preoccupazioni per gli aspetti legati concorrenza, più in generale, si colgono tra le righe della stessa Comunicazione laddove si legge che «Nella partita dell'economia dei dati del futuro l'UE ha tutto da guadagnare. Un numero ridotto di grandi imprese tecnologiche (*Big Tech*) detiene attualmente buona parte dei dati disponibili a livello mondiale. Ciò potrebbe ridurre gli incentivi per le aziende basate sui dati che oggi vogliono emergere, crescere e innovare nell'UE, ma il futuro riserva numerose opportunità. Una gran parte dei dati del futuro proverrà da applicazioni industriali e professionali, ambiti di interesse pubblico o applicazioni dell'Internet delle cose di uso quotidiano, settori in cui l'UE è particolarmente competitiva. Altre opportunità scaturiranno dai cambiamenti tecnologici, con nuove prospettive per le imprese europee in settori quali il *cloud* ai margini della rete (*cloud at the edge*), dalle soluzioni digitali per le applicazioni critiche per la sicurezza e dal calcolo quantistico. Tali tendenze lasciano pensare che i vincitori di oggi non saranno necessariamente i vincitori di domani. Ma è oggi che sono determinate le fonti di competitività per i prossimi decenni nel settore dell'economia dei dati, ed è per questo che l'UE dovrebbe agire subito. L'UE ha tutte le potenzialità per avere successo nell'economia agile basata sui dati: ha a disposizione la tecnologia, le competenze e una forza lavoro altamente qualificata. Concorrenti quali Cina e Stati Uniti stanno tuttavia già innovando rapidamente e proiettando a livello mondiale i loro concetti di accesso ai dati e loro utilizzo. Negli Stati Uniti, l'organizzazione dello spazio di dati è affidata al settore privato, con ripercussioni significative in termini di concentrazione. In Cina si assiste a una combinazione tra sorveglianza governativa e forte controllo delle imprese *Big Tech* su massicce quantità di dati, senza sufficienti garanzie per i cittadini. Al fine di mettere a frutto il potenziale dell'Europa dobbiamo trovare una nostra strada europea, che consenta di equilibrare il flusso e l'ampio utilizzo dei dati mantenendo nel contempo alti livelli di privacy, sicurezza, protezione e norme etiche».

fornitori di servizi di intermediazione dei dati sono vincolati dalle norme di tale regolamento». Infatti, il fornitore del servizio di condivisione dei dati, qualora tale servizio abbia ad oggetto dati personali, è egli stesso "titolare del trattamento dei dati personali", ancorché in relazione a finalità di *data sharing*, sicché è comunque tenuto, ai sensi del Reg. UE 2016/679, all'adozione delle misure tecniche e organizzative *ex* art. 24, nonché quelle in tema di protezione dei dati *by design* e *by default ex* art. 25 GDPR, nonché quelle in tema di sicurezza *ex* art. 32 GDPR.

Ciò rende opportuno, se non necessario, in questa sede, operare quantomeno un riferimento alle relative previsioni contenute nel GDPR, al fine di cogliere i punti di contatto o di dissonanza in tema.

Il sistema delineato dal GDPR, in generale, è improntato ad un'analisi previa dei «rischi» – in una logica preventiva [21] e in ossequio al principio di precauzione [22] – potenzialmente sussistenti per i diritti e le libertà degli interessati.

In questo senso appare dunque centrale la nozione di rischio, inteso come uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità e che preliminarmente e a soli fini sistematici potrebbe distinguersi in: rischi correlati ai principi generali che presiedono al trattamento dei dati – particolarmente il principio di finalità – sotto il profilo del trattamento o della raccolta di dati non necessari in base alla finalità (in relazione agli artt. 5, par. 1, lett. *b*) e 13 GDPR), ovvero informativa e termini del trattamento non chiari o trasparenti (in relazione al consenso dell'interessato, di cui all'art. 4, par. 11 e art. 13 GDPR), ovvero mancato aggiornamento dei dati (in relazione agli artt. 15 e 16 GDPR); rischi correlati alla permanenza del dato stesso, sotto il profilo della inefficace o intempestiva cancellazione dei dati personali (in relazione al diritto alla cancellazione o c.d. «diritto all'oblio» di cui all'art. 17 GDPR), ovvero perdita dei dati lato operatore (in relazione alle misure di sicurezza da approntare *ex* art. 32 GDPR); i rischi insiti nella comunicazione dei dati, con particolare riferimento alla condivisione dei dati con terze parti (in relazione ai processi automatizzati di cui all'art. 22 GDPR, correlato all'art. 7 in tema di condizioni per il consenso e all'art. 21 concernente il di-

---

[21] Sul punto, cfr. EDPB, *Opinion* 12/2018 *on the draft list of the competent supervisory authority of Italy regarding the processing operations subject to the requirement of a data protection impact assessment* (*Article* 35.4 GDPR), adottato il 25 settembre 2018.

[22] Il principio di precauzione, espressamente previsto con riferimento alla materia ambientale dal Trattato sul funzionamento dell'Unione Europea all'art. 191, ha assunto portata generale a partire dalla comunicazione della commissione COM (2000), 1, del 2 febbraio 2000 sul principio di precauzione, in cui la Commissione Europea ha dichiarato applicabile detto principio «a qualunque misura di gestione dei rischi». Cfr. sul punto, F.D. BUSNELLI, *Il principio di precauzione e l'impiego di biotecnologie in agricoltura*, in M. GOLDONI-E. SIRSI (a cura di), *Regole dell'agricoltura e regole del cibo*, Pisa, 2005, p. 115 ss.; M.E. ARBOUR, *A proposito della nebulosa. Principio di precauzione – responsabilità civile*, in *Liber amicorum per Francesco D. Busnelli*, *Il diritto civile tra principi e regole*, Milano 2008, I, p. 513; nonché R. PARDOLESI, *Il principio di precauzione a confronto con lo strumento dell'analisi economica del diritto*, in G. COMANDÈ (a cura di), *Gli strumenti della precauzione: nuovi rischi, assicurazione e responsabilità*, Milano, 2006, p. 13.

ritto di opposizione) e al trasferimento dei dati che non rispetti le condizioni di sicurezza prescritte dalle misure di cui all'art. 32; finanche ai rischi correlati alle violazioni di dati, in relazione alla intempestiva notificazione di *data breach* di cui all'art. 33 (nonché di eventuale comunicazione all'interessato di cui all'art. 34), ovvero riconnesse alla vulnerabilità delle applicazioni (oggi prevalentemente *web*) utilizzate dal titolare del trattamento.

Nel contesto dell'obbligo generale, cui gli stessi sono soggetti, di gestire adeguatamente i rischi presentati dal trattamento di dati personali, secondo quanto previsto dal capo IV del regolamento, che nel suo complesso, istituisce un modello di gestione preventiva della protezione dei dati e si inserisce in una cornice più ampia, all'interno della quale, proprio in funzione di protezione di tali diritti e di gestione del potenziale rischio per i diritti e le libertà delle persone fisiche, si è inteso mettere in atto una vera e propria rivoluzione nell'approccio stesso al dato, sulla base dell'assunto della nozione dinamica e relazionale della sicurezza [23] e della non perfetta coincidenza tra protezione dei dati personali e sicurezza degli stessi, per cui il quadro complessivo restituisce una inedita centralità alla prospettiva del titolare del trattamento, in un'ottica di protezione dei dati personali, del quale «è opportuno stabilire la responsabilità generale (…) per qualsiasi trattamento di dati», come si legge nel *considerando* n. 74, avendo cura di effettuare una «valutazione oggettiva» circa la probabilità e la gravità del rischio per i diritti e le libertà dell'interessato, in relazione alla natura, al contesto e alle finalità del trattamento [24].

Sostanzialmente, a fronte dell'inadeguatezza mostrata dall'approccio essenzialmente riparatore adottato dal precedente sistema della Direttiva, la nuova disciplina accoglie un'impostazione fondata piuttosto su una tutela preventiva, che utilizza gli strumenti della valutazione di impatto sulla protezione dei dati personali e della *privacy by design* e della *privacy by default*, collocando la tutela del dato a monte del trattamento stesso.

Per questa via si finisce per orientare la produzione di beni e la prestazione di servizi nel senso della creazione di prodotti fin dall'origine *privacy oriented*, il cui vantaggio consiste nel fatto che lo strumento dovrebbe seguire l'intero ciclo di vita del prodotto o del servizio, agevolando l'adeguamento da parte delle imprese ai livelli di tutela previsti dalla norma e via via sempre più richiesti e attesi dagli utenti. Ne deriva un'impostazione al tempo stesso preventiva [25] e promozionale della nuo-

---

[23] G. FINOCCHIARO, *Il quadro d' insieme*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, p. 13, in cui si sottolinea che «la sicurezza è un concetto dinamico relazionale, da rapportarsi alle conoscenze in base al progresso tecnico, alla natura dei dati personali oggetto di trattamento ed alle specifiche caratteristiche delle operazioni di trattamento». Cfr. anche F. PIZZETTI, *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, p. 41.

[24] Cfr. *considerando* n. 75 e n. 76.

[25] Tale prospettiva si rinviene in particolare all'art. 25 reg., che introduce le due nozioni di *privacy by design* e *privacy by default*, quali strumenti volti ad attuare i principi posti alla base della materia, di cui all'art. 4, nati per gemmazione dal principio di necessità.

va disciplina che, segnando un ribaltamento rispetto al modello precedente, che permetteva di valutare l'adeguatezza delle misure adottate per evitare il danno soltanto *ex post* a pregiudizio verificatosi, trasla il baricentro di tutela in una prospettiva *ex ante*, mosso dall'esigenza di ridurre in via preventiva i rischi insiti nel trattamento dei dati personali [26].

Il nuovo approccio al rischio (*risk oriented approach*) appare quindi maggiormente incentrato nella sfera del titolare del trattamento, nelle declinazioni di una proceduralizzazione degli obblighi dello stesso – secondo un modello tipicamente anglo-americano approdato poi anche nell'Europa continentale – e del principio di *accountability* [27], tradizionalmente tradotto come principio di rendicontazione [28], o di responsabilità che si traduce in compliance dei trattamenti [29].

In particolare, tale architettura giuridica dei meccanismi di responsabilità prevede due livelli: il primo è costituito da un obbligo di base vincolante per tutti i titolari (o responsabili) del trattamento, consistente nell'attuazione di misure e procedure e nella conservazione delle relative prove; mentre il secondo livello include sistemi di responsabilità di natura volontaria eccedenti le norme di legge minima, in relazione ai principi fondamentali di protezione dei dati (tali da fornire garanzie più elevate di quelle prescritte dalla normativa vigente) e/o intermedi modalità di attuazione di garanzia dell'efficacia delle misure (norme di attuazione) e consistente nell'obbligo di conformarsi.

Sotto il primo profilo, vengono in rilievo, per tutti i tipi di trattamento, gli obblighi generali (previsti dall'art. 24 GDPR) in funzione di protezione dei dati personali, da un lato, nonché gli obblighi inerenti la sicurezza dei trattamenti di cui all'art. 32.

Nella disciplina degli obblighi generali viene attribuito centrale rilievo alla responsabilità del titolare del trattamento, che «mette in atto misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare che il tratta-

---

[26] Si veda la valorizzazione di *preventive policies, risk assessment* e *privacy by design* anche nelle *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, reperibile al sito *www.coe.int/data-protection*.

[27] G. FINOCCHIARO, *op. ult.cit*., p. 3 ravvisa nel modello dell'*accountability* un modello alternativo a quello incentrato sul consenso, «spesso vuoto di effettivo significato, perché prestato nell'inconsapevolezza o nell'assenza di alternative praticabili». Il termine si rinviene, tra le prime occasioni, nel corso della Conferenza Internazionale sui Garanti della *Privacy* e la Protezione dei Dati, tenutasi a Gerusalemme nel 2010, durante la quale *The Centre for Information Policy Leadership* ha presentato il documento «*Demonstrating and Measuring Accountability, Accountability Phase* II – *The Paris Project*», risultato della deliberazione del gruppo di lavoro internazionale che si è riunito in Irlanda nel 2009 e a Parigi nel 2010.

[28] È un termine che può essere tradotto in molti modi, fra cui responsabilità, affidabilità, assicurazione, obbligo di rendicontazione, attuazione dei principi concernenti il trattamento dei dati personali. Si vedano le precisazioni contenute nel parere 3/2010 (punti 21 e 22).

[29] Si veda F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016, p. 283.

mento viene effettuato» in maniera conforme alla disciplina [30].

L'adozione delle misure di cui all'art. 24 [31], che in un'ottica di *life-long adequacy* andrebbero riesaminate e aggiornata periodicamente (come del resto la valutazione di impatto), deve configurarsi come «appropriate» in una duplice ottica: da un lato quella di compliance, volta a garantire che il trattamento venga effettuato in conformità alla disciplina, in funzione di una più stringente protezione dei diritti che la stessa intende tutelare, dall'altro, nella prospettiva complementare e speculare della prova della compliance, di cui è onerato in primo luogo il titolare del trattamento, che deve essere in grado di dimostrare (di rendere conto o di dare conto) proprio questa circostanza nella prospettiva dell'*accountability* già richiamata, tenuto conto poi che tale onere della prova potrà essere reso più agevole (par. 3) dall'adozione di codici di condotta ed eventuale adesione a meccanismi di certificazione di cui agli artt. 40 [32] e 42 [33].

---

[30] Come osserva anche il WP29 nelle *Guidelines on data protection impact assessment*, la valutazione di impatto di cui all'art. 35 costituisce un *postquam* rispetto a quella prevista per tutti trattamenti dall'art. 24. La differenza tra le due norme è costituita dal fatto che mentre l'art. 24 prevede l'obbligo di una generale e generica valutazione del rischio, l'art. 35 definisce i casi in cui questa non è sufficiente ed occorre quindi la valutazione d'impatto.

[31] La nuova disciplina ha ampliato e razionalizzato il novero degli obblighi in capo al titolare e al responsabile del trattamento, rispetto alla disciplina previgente contenuta nella Direttiva, che si occupava soltanto degli obblighi in materia di sicurezza dei trattamenti all'art. 17, che prevedeva soltanto che gli Stati membri disponessero che il responsabile del trattamento attuasse «misure tecniche ed organizzative appropriate al fine di garantire la protezione dei dati personali» e solo in relazione a distruzione accidentale o illecita, ovvero perdita accidentale o alterazione, ovvero ancora diffusione o accesso non autorizzati – e quindi in una logica soltanto *ex post*, di modo da garantire «un livello di sicurezza appropriato rispetto ai rischi presentati dal trattamento e alla natura dei dati da proteggere», in relazione alle conoscenze allora attuali in materia e in ragione dei relativi costi di applicazione. La nuova disciplina adotta invece una visione più circolare e omnicomprensiva, disseminando lungo l'intero testo del regolamento le disposizioni di previsione di obblighi e adempimenti in funzione di tutela dei diritti e delle libertà delle persone fisiche i cui dati sono trattati, non confinando e circoscrivendo più la figura del titolare all'ambito della sicurezza dei trattamenti, ma coinvolgendolo in maniera più diretta e penetrante nell'intero ciclo di gestione del dato, comprensivo di tutte le sue fasi. Cfr., sul punto, L. GRECO, *I ruoli: titolare e responsabile*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, in part. p. 279.

[32] Si tenga presente che il Comitato Europeo per la Protezione dei Dati (EDPB) ha adottato il 12 febbraio 2019 le Linee-guida in materia di codici di condotta (*Guidelines* 1/2019 *on Codes of Conduct and Monitoring Bodies under Regulation 2016/679*), che mirano a fornire orientamenti pratici e supporto interpretativo rispetto all'applicazione degli artt. 40 e 41 del regolamento generale sulla protezione dei dati. Esse intendono contribuire a chiarire le procedure e le norme relative alla presentazione, all'approvazione e alla pubblicazione dei codici di condotta a livello sia nazionale che europeo; inoltre, e dovrebbero offrire un chiaro quadro di riferimento per tutte le autorità di controllo, il Comitato e la Commissione nel valutare i codici di condotta in modo coerente snellendo le relative procedure.

[33] La compliance sotto il profilo della protezione dei dati personali dovrebbe essere integrata nella *Corporate Governance* stessa dell'azienda, a monte delle strategie direzionali oltre che nella cultura aziendale, nonché a valle nei processi organizzativi, nella *policy* e nella comunicazione interna ed ester-

Nell'adottare e mettere in atto le misure previste dal GDPR, il titolare non deve tenere conto solo della natura del trattamento, nonché del suo ambito di applicazione, del contesto in cui si svolge e delle finalità per cui ha compiuto, ma deve tenere conto pure specificamente dei «rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche», per cui si impone che una valutazione in un'ottica protettiva per i diritti le libertà delle persone fisiche venga effettuata *prima facie* dello stesso soggetto che effettua il trattamento, nella misura in cui sia chiamato a tenere conto di tali rischi, vieppiù graduandone probabilità e gravità, in funzione tutoria dei diritti connessi alla protezione dei dati personali.

Più specificamente in punto agli obblighi *ex ante* concernenti la sicurezza, previsti in funzione di protezione dei dati personali in capo al titolare del trattamento – con formulazione sostanzialmente speculare rispetto a quella adottata dall'art. 24 in relazione agli obblighi generali e all'art. 25 con riferimento alla protezione dei dati personali fin dalla progettazione e per impostazione predefinita – l'art. 32 GDPR, impone al titolare o al responsabile del trattamento di mettere in atto misure tecnico-organizzative «adeguate per garantire un livello di sicurezza adeguato a rischio» [34], tenendo conto – e quindi operando, anche qui, una prognosi *ex ante* – «anche del rischio di varia probabilità e gravità per i diritti le libertà delle persone fisiche», in relazione anche alla natura, oggetto, contesto e finalità del trattamento stesso, nonché dello stato dell'arte e dei costi di attuazione [35] che quelle misure impongono a chi effettua il trattamento, secondo il modello della «massima sicurezza tecnologicamente fattibile».

Orbene, proprio in questo ambito in particolare emerge con forza il *risk based approach* abbracciato dalla nuova disciplina, e caratterizzato dalla tendenza incentivante l'adozione di procedure atte alla minimizzazione ovvero alla neutralizzazione del rischio, nel senso di rendere applicabile sin dall'inizio gli obblighi generali di protezione e trattamento conforme, come si legge fin dai *considerando* [36] del GDPR e come già emerso in sede di lavori preparatori [37].

---

na degli enti. In quest'ottica, sono individuabili molti punti di contatto tra gli adempimenti *privacy* previsti dal GDPR e i meccanismi che presiedono alle certificazioni ISO 27001.

[34] Cfr. *considerando* n. 39, che precisa, tra l'altro, che «(…) I dati personali dovrebbero essere trattati in modo da garantirne un'adeguata sicurezza e riservatezza, anche per impedire l'accesso o l'utilizzo non autorizzato dei dati personali e delle attrezzature impiegate per il trattamento».

[35] Incidentalmente si segnala che il riferimento ai costi, pur contenuto all'art. 17 della direttiva, non era stato raccolto dal legislatore nazionale nel recepimento in seno all'art. 17 del d.lgs. n. 196/2003, per cui «i dati personali oggetto di trattamento sono custoditi e controllati, anche relazione alle conoscenze acquisite in base al progresso tecnico, la natura dei dati alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, rischi di distruzione o perdita, anche accidentale, di dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta», articolo oggi abrogato dalle norme di coordinamento.

[36] Cfr. in particolare il *considerando* n. 78 GDPR.

[37] La necessità di vagliare i rischi sottesi allo svolgimento delle attività di trattamento dei dati per-

Da questo punto di vista, è proprio la prospettiva assunta dal regolamento a differenziarsi dall'approccio della direttiva precedente, che, peraltro dedicando poche disposizioni al tema, prevedeva all'art. 17, par. 1 solo l'attuazione di misure tecniche ed organizzative appropriate al fine di garantire la protezione dei dati dalla distruzione, dalla perdita, alterazione, diffusione, accessi non autorizzati ovvero da qualsiasi altra forma illecita di trattamento, precisando che tali misure dovessero garantire un livello di sicurezza appropriato rispetto ai rischi presentati dal trattamento e alla natura dei dati, tenuto conto delle conoscenze al momento disponibili e dei costi dell'applicazione; assumendo cioè una prospettiva di chi tratta i dati e guardando agli eventuali pregiudizi ai diritti dei singoli che possono derivare dalla gestione degli stessi, finendo con ciò per declinare il rischio secondo una visione incentrata sulla sicurezza informatica, e prendendo in esame i soli rischi attinenti alla qualità e alla sicurezza dell'informazione, senza attribuire rilievo a profili di rischio più generali in termini di impatto che possa derivarne, anche in considerazione della precipua natura delle posizioni soggettive coinvolte [38].

Ma a ben guardare, l'approccio è mutato in funzione di un cambiamento della stessa nozione di rischio, caratterizzato dal traghettamento da un rischio statico ad un rischio dinamico, nel contesto dell'attuale fenomeno di *datification* [39], governato dagli algoritmi [40] dei grandi detentori di dati, che fanno venire in rilievo, da un lato, il rischio sociale collettivo legato al controllo occulto e invasivo, reso possibile dagli odierni discendenti delle banche dati, dall'altro, un rischio individuale e disaggregato, riferibile all'utilizzo dei dati inerenti a persone specifiche, a fini di sfruttamento del loro profilo informativo ricavabile dalla ricostruzione degli aspetti caratterizzanti la persona [41].

---

sonali era ben presente già in seno ai lavori preparatori del regolamento. Si veda sul punto Commissione europea, *Salvaguardare la privacy in un mondo interconnesso. Un quadro della protezione dei dati per il XXI secolo*, COM (2012) 9 final del 25 gennaio 2012, p. 7, nonché Gruppo *ex* art. 29 WP, *Statement on the role of a risk-based approach in data protection legal frameworks*, WP 218 del 30 maggio 2014.

[38] Cfr. il *considerando* n. 46 della direttiva che poneva attenzione alle misure di protezione dei diritti del singolo in un'ottica orientata alle misure di sicurezza e alle misure volte a prevenire trattamenti non autorizzati, nonché i *considerando* n. 53 e n. 54.

[39] Cfr. A. MANTELERO, *La privacy all'epoca dei Big Data*, in V. CUFFARO-R. D'ORAZIO-V. RICCIUTO, *I dati personali nel diritto europeo. Il regolamento generale 2016/679 (e le direttive 2016/680 e 2016/681 sul trattamento dei dati in ambito penalistico)*, Torino, 2019.

[40] S. RODOTÀ, *Il mondo nella rete. Quali i diritti quali i vincoli*, Bari, 2014, p. 37 ss. Cfr. anche S. RODOTÁ, *Una Costituzione per Internet?*, in *Pol. dir.*, 2010, 3, p. 342, che sottolinea come proprio attraverso queste gigantesche raccolte di dati i nuovi «signori dell'informazione (...) governano la nostra vite», finendo per trasformarsi da strapotente società multinazionale in un «potere a sé, superiore a quello di un'infinità di Stati nazionali, con i quali negozia da potenza a potenza. (...) interlocutore quotidiano di centinaia di milioni di persone alle quali offre la possibilità di entrare e muoversi nell'universo digitale. Governa corpi conoscenza, relazioni sociali».

[41] Le esigenze di protezione dei dati personali ricollegate a tali profili sono certamente mutate ri-

Sul punto, il par. 2 dell'art. 32 si limita a sottolineare come il titolare debba tener conto «in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati», elencando cioè soltanto alcuni dei rischi prospettabili.

L'art. 32 esplicitamente distingue, all'interno del *genus* misure di sicurezza, tra misure organizzative e misure tecniche; richiamando così il disposto dell'art. 5 che espressamente prevede che «i dati personali sono trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita o distruzione o dal danno accidentali (integrità e riservatezza)» e quindi facendo specifico riferimento alle misure di sicurezza di tipo organizzativo, tra cui potrebbero rientrare misure per l'assegnazione di compiti e responsabilità, volte all'aumento della sensibilità aziendale alle tematiche privacy, nonché di protezione degli archivi cartacei e per evitare l'attuazione di trattamenti per finalità diverse.

Le misure tecniche (la cui elencazione è aperta e meramente esemplificativa) comprendono invece la pseudonimizzazione [42] e la cifratura dei dati personali; prendendo in considerazione i requisiti di sicurezza che attengono alla capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento, intendendosi in particolare per resilienza l'attitudine intrinseca di un sistema di adattarsi alle condizioni d'uso nonché di resistere all'usura al fine di assicurare la continuità dei servizi e la protezione dei dati trattati; nonché alla capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; nonché una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento*».*

La sicurezza intesa dal regolamento non attiene quindi soltanto all'aspetto informatico del trattamento [43], ma involge pure l'assetto organizzativo, che nel suo

---

spetto al quadro tenuto in conto dalla direttiva, come dimostra ad esempio la considerazione contenuta nel *considerando* n. 54 della stessa, allorché veniva riportato che «il numero di trattamenti che presentano tali rischi particolari (in quanto effettuati mediante l'utilizzo di nuove tecnologie, come si ricava dal *considerando* precedente) dovrebbe essere molto esiguo rispetto al totale dei trattamenti effettuati nella società».

[42] La pseudonomizzazione è una misura di sicurezza (e non di *privacy*) consistente nel sostituire un attributo, solitamente unico, di un dato con un altro, ugualmente univoco e solitamente non immediatamente intelligibile, al fine di rendere più complessa l'identificazione e la riferibilità del dato alla persona, ma mantenendo inalterato il quadro di certezze nella concatenazione di passaggi necessari per l'attribuzione del dato pseudonimo alla persona, al contrario della anonimizzazione, che tali elementi di incertezza introduce. All'esito di un processo di pseudonomizzazione la persona potrebbe ancora essere identificabile in maniera indiretta, per cui esso si pone come una misura volta a garantire la confidenzialità del dato, non più immediatamente intelligibile, ma anche a garantirne l'integrità contro manipolazioni accidentali, come nel caso dell'applicazione di tecniche crittografiche. Cfr. G. D'ACQUISTO-M. NALDI, *Big data e privacy by design*, Torino, 2018, p. 38 ss.

[43] Fermo restando che la protezione dei dati disegnata dal regolamento va inserita nel più ampio

complesso deve essere volto ad assicurare che i dati possano essere consultati, modificati, divulgati e cancellati solo dalle persone autorizzate, che siano accurati e completi in relazione alle specifiche finalità del trattamento, nonché recuperabili in caso di accidenti o eventi catastrofali mediante la predisposizione di un piano di continuità operativa.

Atteso quindi che le componenti maggiormente esposte a rischio risultano essere reti e apparati, elaboratori, *software* di sistema e software applicativi, supporti informatici di memorizzazione e archivi cartacei, infrastrutture e archivi di *backup*, può ritenersi in generale che le misure più adottate in quanto valutate «adeguate» saranno policies di *backup* dei dati, procedure interne di gestione dei codici di identificazione nonché di gestione, custodia e aggiornamento delle *password*, sistemi di assegnazione e controllo dei profili, misure a protezione delle categorie particolari di dati degli interessati [44], misure di prevenzione degli attacchi provenienti da programmi dannosi o da accessi abusivi, nonché misure di protezione delle aree [45] (secondo un criterio che richiama la dimensione fisica della sicurezza), misure di protezione delle architetture di rete, degli applicativi e delle banche dati (secondo un criterio che rimanda alla dimensione logica della sicurezza) [46], nonché misure di protezione per la trasmissione dei dati (in particolare su rete).

Il termine «appropriate», poi, tradotto come «adeguato», declinato in relazione alle predette misure tecniche e organizzative (così come in relazione al livello di sicurezza da garantire), evoca proprio questa valutazione *ex ante* [47] demandata al

---

contesto della *cybersecurity* aziendale, i cui moderni frameworks affrontano sistematicamente il problema sistematizzando il processo in diverse fasi, delle quali le prime tre proattive: individuare le possibili situazioni di rischio in termini di tipo di violazione, strutture organizzative e risorse coinvolte, nonché probabilità dell'evento e gravità del danno-conseguenza; proteggere, cioè adottare in via preventiva misure volte a evitare trattamenti non necessari e ridurre le probabilità di accadimento e le possibili conseguenze negative; rilevare, ovvero istituire un sistema di monitoraggio continuo in grado di segnalare tempestivamente eventi legati alla sicurezza informatica. Le ultime due fasi sono, piuttosto, reattive e consistono nel rispondere, predisponendo le azioni intese al contenimento delle conseguenze in caso di incidente (anche sotto il profilo informativo e dell'adozione di misure correttive che ne evitino la ripetizione) e ripristinare, garantendo la normale continuità operativa.

[44] Sul punto, cfr. Garante per la protezione dei dati personali, provvedimento in materia di rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali, adottato il 13 ottobre 2008.

[45] Tra di esse le misure anti-intrusione, i controlli degli accessi, misure per la protezione dei dati da eventi di origine naturale o dolosa, nonché da condizioni ambientali proibitive o da eventuali riduzioni dell'efficienza dei sistemi di supporto.

[46] Ad esempio, misure antivirus e misure necessarie finalizzate alla registrazione degli access log degli amministratori di sistema, su cui si veda il provvedimento del Garante per la protezione dei dati personali sulle «Misure e accorgimenti prescritti ai titolari di trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema», adottato il 27 novembre 2008.

[47] Se la valutazione di cui all'art. 32 par. 1 deve essere condotta *ex ante* sulla base delle precipue circostanze del caso concreto, su diverso versante si collocano invece le misure da adottarsi in caso di

titolare o al responsabile del trattamento, e peraltro calata nel caso concreto, in ragione delle caratteristiche peculiari del trattamento in questione, tanto sotto il profilo oggettivo che soggettivo, come suggerisce anche l'inciso «se del caso» contenuto nel paragrafo 1 dell'art. 32, allorché prevede quell' elencazione esemplificativa e non esaustiva di misure includibili tra le misure di sicurezza *de quibus* [48], con ciò consolidando più nello specifico, rispetto all'art. 17 della precedente direttiva, la regola di appropriatezza del livello di sicurezza rispetto ai rischi del trattamento, in un'ottica di adeguatezza in concreto delle stesse, indicando un modello basato sulla spersonalizzazione dei dati, ovvero sulla riservatezza, integrità, e resilienza dei servizi di trattamento, anche secondo le indicazioni del *Working group ex* art. 29.

Rimarrebbe a questo punto da interrogarsi sulla natura di tali obblighi di protezione, quali effetti giuridici che scaturiscono dall'esistenza materiale del trattamento, intesi come obblighi imposti dalla disciplina in materia di protezione dei dati personali al titolare del trattamento ricollegabili alla oggettiva sussistenza del trattamento medesimo [49].

L'obbligo di adozione delle misure di sicurezza potrebbe essere da questo punto

---

data breach, quindi *ex post*, quando la violazione si è già verificata con eventuale pregiudizio in atto o in potenza per i diritti e le libertà delle persone fisiche; in questi casi si prevede infatti all'art. 34 par. 3 un'esenzione dalla comunicazione all'interessato in caso di violazione laddove il titolare del trattamento abbia «successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati», in cui l'attitudine di siffatte misure a scongiurare detto rischio si atteggia quale idoneità in concreto allo scopo, intesa come vera e propria attitudine a neutralizzare le conseguenze pregiudizievoli che potrebbero prodursi in capo agli interessati.

[48] Le misure tecniche potrebbero comprendere, tra le altre, la pseudonimizzazione e la cifratura dei dati personali, nonché la capacità di assicurare che i sistemi servizi di trattamento garantiscano su base permanente riservatezza, integrità, disponibilità e resilienza, nonché l'attitudine a ripristinare in caso di incidente in modo tempestivo disponibilità all' accesso dei dati personali, nonché ancora procedure di *check* per testare e verificare periodicamente l'efficacia in termini di sicurezza di dette misure, in accordo con l'obbligo di aggiornamento e di revisione periodica previsto per gli obblighi generali all'art. 24 par. 1.

[49] Volendo in questo senso abbracciare l'impostazione che ravvisa nel trattamento un «fatto umano» (e non naturale), stando alla classificazione proposta da Galgano per il quale «Gli atti giuridici compongono una sottocategoria dei fatti umani: li si può definire come i fatti umani destinati a produrre effetti giuridici». Cfr. F. GALGANO, *Trattato di diritto civile*, 3ª ed. curata e aggiornata da N. ZORZI GALGANO, Milano, 2014, 1, p. 34. A partire da tale classificazione, in particolare, F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Milano, 2018, p. 98, evidenzia che «il trattamento andrebbe inquadrato come "fatto umano diverso dall'atto giuridico" e, dunque, andrebbe annoverato tra i fatti giuridici derivanti dall'attività umana per i quali è sufficiente la sola capacità naturale ai fini della produzione degli effetti previsti dalla disciplina in materia di protezione e di circolazione dei dati personali», e ancora «il trattamento, pur essendo prodotto dell'attività umana, non va inquadrato nella categoria dell'atto giuridico, ma in quella del fatto giuridico umano diverso dall'atto, e ciò perché l'ordinamento, quando lo prende in considerazione del suo aspetto causale, lo considera produttivo di effetti anche qualora gli stessi non siano voluti dal titolare del trattamento», cioè quand'anche il titolare non abbia voluto trattare dati riconducibili a soggetti determinati o determinabili ed il trattamento di dati personali abbia comunque avuto luogo.

di vista inquadrabile nella categoria delle obbligazioni di mezzi, per cui il titolare del trattamento è tenuto ad una determinata attività idonea a realizzare il risultato atteso con il dovuto grado di diligenza (cui la nozione di appropriatezza utilizzata dal legislatore europeo della *privacy* appare collegabile), fermo restando poi che il mancato raggiungimento di tale risultato può assumere rilievo proprio sotto il profilo della prova della diligenza (che nel caso specifico diviene prova della compliance al regolamento). Da questo punto di vista, sarà legittimo attendersi che si possa ragionare secondo un criterio di esigibilità secondo buona fede, anche in relazione all'assetto complessivo che presiede al trattamento da effettuarsi e alla concreta capacità organizzativo-aziendale, in relazione al criterio dimensionale degli interessi in gioco, che può comportare vari gradi e livelli di rischio diversi per i dati oggetto di trattamento, e quindi per i diritti e le libertà che vengono in gioco, in una logica che richiama in qualche modo il criterio di ragionevolezza [50].

In conclusione, il sistema che deriva dalla combinazione delle previsioni delle norme che fin qui si sono analizzate poggia su un modello di analisi del rischio fondato sui diritti impattati dal trattamento e sulla ponderazione in concreto fra loro, in ragione della loro rilevanza, che precede una qualsiasi valutazione in meri termini di rischi-costi/benefici, e che differenzia il settore della *data protection* dagli altri ambiti toccati dai principi e dalle soluzioni elaborate nel tempo dagli studi in materia di *risk management* [51], nonché uno schema di analisi di natura circolare [52] caratterizzato da una pluralità di fasi – costituenti nel loro complesso un processo di durata – e inerenti l'analisi specifica del contesto e la ricognizione delle

---

[50] Cfr. R. D'ORAZIO, *Protezione dei dati by default e by design*, cit., p. 96, che sottolinea come nell'ambito specifico *de quo* sia «la stessa vicenda concettuale della ragionevolezza nella sua più generale accezione a mostrare come essa (...), tenda a sostanziarsi nel quadro di riferimento e nel peso argomentativo di una regola di decisione del caso concreto, veicolandovi gli elementi valoriali sulla cui base devono bilanciarsi i contrapposti interessi», e che richiama le riflessioni dei civilisti sul punto, cfr. S. TROIANO, *La ragionevolezza nel diritto dei contratti*, Padova, 2005; PATTI, *Ragionevolezza e clausole generali*, Milano, 2013 e G. PERLINGIERI, *Profili applicativi della ragionevolezza nel diritto civile*, Napoli, 2015. Insiste sul criterio di ragionevolezza nel Regolamento pure G. FINOCCHIARO, *Introduzione al Regolamento europeo sulla protezione dei dati*, in *Nuove leggi civ. comm.*, 2017, 1, p. 1 ss. Pare interessante sottolineare il ruolo della ragionevolezza anche a livello europeo più in generale, sul punto si veda G. ALPA-U. PERFETTI-P. ZATTI-G. IUDICA (a cura di), *Il Draft Common Frame of Reference del diritto privato europeo*, Padova, 2009.

[51] In estrema sintesi, il *risk management*, di cui *gap analysis* e *risk analysis* costituiscono attività essenziali, configura la procedura aziendale avente ad oggetto l'identificazione, l'*assessment* e la prioritizzazione dei rischi, cui conseguono correlative applicazioni in termini di risorse organizzative ed economiche, volte a mitigare, monitorare e controllare la probabilità di impatto di eventi di danno. Interessante sotto questo profilo la ricostruzione delle criticità prodotte dalla «società del rischio» all'indomani dell'industrializzazione dei processi produttivi, compiuta da U. BECK, *Risk society: towards a new modernity*, London, 2010.

[52] A. MANTELERO, *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati. Valutazione d'impatto e consultazione preventiva* (*Artt. 32-39*), in G. FINOCCHIARO (a cura di), *Il nuovo regolamento*, cit., in part. p. 301.

fonti potenziali di rischio per i diritti, nonché la predisposizione e la successiva implementazione di misure volte a ridurre o neutralizzare tali rischi, il *check* in punto di efficacia ed efficienza delle stesse, che tenga conto tanto del mutamento del rischio in relazione ai diritti coinvolti quanto dell'obsolescenza tecnologica nel settore di riferimento e che pone capo ad una revisione periodica delle stesse.

Di tutti questi principi occorre tener conto per ricostruire un quadro quanto più completo delle disposizioni volte a soddisfare esigenze di sicurezza in relazione al tema che qui viene in rilievo.

Capitolo XLV

Tutela degli interessati e esercizio dei diritti: l'efficace intermediazione delle cooperative di dati

Isabella Cardinali

Abstract: This paper aims to analyse one of the conditions to which the provision of data intermediation services is subject under the Data Governance Act. Specifically, the analysis pertains to the provisions contained in Art. 12(m) of the DGA, which are of particular interest in terms of their implications for the protection of personal data especially in the prism of data cooperatives, which, by virtue of their specific vocation, represent a sure guarantee for the firm exercise of the rights of the data subject and therefore the privileged legal form for compliance with said condition.

1. Il DGA e la tutela rafforzata degli interessi dei *data subjects*.

Il Reg. UE n. 868/2022 [1], noto come *Data Governance Act* (in seguito anche so-

[1] Il riferimento è al Regolamento (UE) 2022/868 del Parlamento Europeo e del Consiglio del 30 maggio 2023 relativo alla *governance* europea dei dati e che modifica il Regolamento (UE) 2018/1724 (Regolamento sulla *governance* dei dati) (*Data Governance Act*).

Sull'uso del termine governance si rinvia a D. POLETTI, *A proposito di fonti nell' "ecosistema digitale*", in F. RICCI (a cura di), *Principi, clausole generali, argomentazione e fonti del diritto*, Milano, 2018, p. 345. Il citato Regolamento è stato pubblicato nella G.U.U.E. in data 3 giugno 2022 e venti giorni dopo è entrato in vigore. Ai sensi dell'art. 38 dello stesso, ha trovato applicazione a far data dal 24 settembre 2023. Il *Data Governance Act* rappresenta il pilastro della strategia digitale europea volta alla valorizzazione e al potenziamento del mercato basato sui dati.

Il *Data Governance Act* integra inoltre quanto previsto dalla Direttiva UE 2019/1024, afferente all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico.

lo DGA) ha inteso disciplinare i servizi di intermediazione di dati [2], personali [3] e non personali [4], tramite l'attività dei fornitori di servizi di intermediazione dei dati, che si pongono quindi al centro tra gli utenti e le società terze che acquisiscono e utilizzano tali informazioni [5].

La fornitura di servizi di intermediazione di dati è soggetta a quindici condizioni [6], specificatamente elencante nell'art. 12 del DGA. Tra queste spicca, in partico-

---

Sulla circolazione dei dati ed il loro sfruttamento economico si vedano, *ex multis*, F. BRAVO, *Il diritto a trattare dati personali nello svolgimento dell'attività economica*, Milano, 2018; N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Milano, 2019; Si rimanda altresì a M. TAMPIERI, *L'intelligenza artificiale e le sue evoluzioni*, che aggiunge: «Il Reg. (Ue) 679/2016 rappresenta sul punto un fondamentale passo avanti, enfatizzando maggiormente la dimensione della libera circolazione dei dati che affianca oggi quella indirizzata alla protezione della persona (art. 1, par. 1, GDPR). La tutela soggettiva viene quindi attuata a fronte del fenomeno (ammesse e promosso) della libera circolazione dei dati personali: si sottolinea così l'attenzione del legislatore europeo per le esigenze economiche e di mercato, pur sempre rimanendo sensibile alle istanze personalistiche di tutela della persona. I dati personali rivestono dunque un'importanza sempre crescente dal punto di vista economico: essi rappresentano infatti la nuova *most valuable resource* dell'economia dell'informazione, e vengono posti sullo stesso piano del petrolio che è stato fondamentale per lo sviluppo dell'economica industriale». Ed ancora: «In questo scenario, risulta opportuno (in particolare per il giurista) non limitarsi allo studio della materia unicamente in una prospettiva indirizzata alla assoluta intangibilità dei diritti della personalità, ma ricostruire la disciplina privacy anche con riguardo alla logica di base del rapporto obbligatorio e dei diritti relativi».

[2] La definizione di servizio di intermediazione dei dati è contenuta all'art. 2 del *Data Governance Act*. Trattasi, in particolare, di un servizio che mira a instaurare, attraverso strumenti tecnici, giuridici o di altro tipo, rapporti commerciali ai fini della condivisione dei dati tra un numero indeterminato di interessati e di titolari dei dati, da un lato, e gli utenti dei dati, dall'altro, anche al fine dell'esercizio dei diritti degli interessati in relazione ai dati personali, ad esclusione almeno di: a) servizi che ottengono dati dai titolari dei dati e li aggregano, arricchiscono o trasformano al fine di aggiungervi un valore sostanziale e concedono licenze per l'utilizzo dei dati risultanti agli utenti dei dati, senza instaurare un rapporto commerciale tra i titolari dei dati e gli utenti dei dati; b) servizi il cui obiettivo principale è l'intermediazione di contenuti protetti da diritto d'autore; c) servizi utilizzati esclusivamente da un titolare dei dati per consentire l'utilizzo dei dati detenuti da tale titolare dei dati, oppure utilizzati da varie persone giuridiche all'interno di un gruppo chiuso, anche nel quadro di rapporti con i fornitori o i clienti o di collaborazioni contrattualmente stabilite, in particolare quelli aventi come obiettivo principale quello di garantire la funzionalità di oggetti o dispositivi connessi all'internet delle cose; d) servizi di condivisione dei dati offerti da enti pubblici che non mirano a instaurare rapporti commerciali.

[3] I dati personali sono quelli definiti all'art. 4, n. 1, del Reg. (UE) 2016/679 (GDPR).

[4] Il Reg. (UE) 2018/1807 disciplina i dati non personali, cioè tutti quei dati diversi da quelli personali, e la loro libera circolazione.

[5] F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in *Contratto e impresa Europa*, 2021, 1, pp. 199-256. Per un'analisi puntuale relativa alle questioni giuridiche emergenti in materia di infomediazione cfr. F. BRAVO, *Il commercio elettronico di dati personali,* in T. PASQUINO-A. RIZZO-M. TESCARO (a cura di), *Questioni attuali in tema di commercio elettronico*, Napoli, 2020, pp. 83-130.

[6] Le condizioni a cui è sottoposta la fornitura di servizio di intermediazione di dati sono elencate dall'art. 12 DGA: il legislatore europeo, dopo aver specificato all'art. 10 quali siano i servizi di dati e

lare, la previsione di cui alla lett. *m*)[7], per le rilevanti implicazioni in materia di protezione dei dati personali.

Il legislatore, con la condizione testé richiamata, ha inteso infatti precisare che il fornitore di servizi di intermediazione di dati che offre tali servizi agli interessati[8] ha l'obbligo, prima che gli interessati diano loro il consenso[9], di agire nel superiore interesse di questi ultimi nel facilitare l'esercizio dei loro diritti in particolare informandoli e, se opportuno, fornendo loro consulenza in maniera coincisa, trasparente, intellegibile e facilmente accessibile[10] sugli utilizzi previsti dei dati da parte

---

dopo aver, all'art. 11, definito la procedura necessaria per poter avviare l'attività, ha inteso definire al successivo articolo, in maniera specifica, gli obiettivi e le misure di tutela.

[7] Sul punto si rimanda a F. BRAVO, *Le cooperative di dati*, in *Contratto e impresa*, 2023, 3, pp. 757-799: «Particolare attenzione merita poi di essere posta sulle condizioni di cui alle lett. *m*) ed *n*), per le implicazioni in materia di protezione dei dati personali. Nella prospettiva del legislatore europeo, i fornitori dei servizi di intermediazione di dati – incluse, in particolare, le cooperative di dati – sono tenuti a perseguire il "superiore interesse" dei *data subjects*, qualora fornisca servizi a questi ultimi. Sicché il loro interesse deve ritenersi prevalente rispetto a quello dei fornitori medesimi, che sono tenuti a "facilitare l'esercizio dei loro diritti, in particolare informandoli e, se opportuno, fornendo loro consulenza in maniera concisa, trasparente, intelligibile e facilmente accessibile sugli utilizzi dei dati da parte degli utenti dei dati e sui termini e le condizioni standard cui sono subordinati tali utilizzi, prima che gli interessati diano il loro consenso" (lett. m)».

E ancora: «(…) alla relativa lett. *m*) stabilisce uno specifico obbligo di natura fiduciaria per l'ipotesi in cui il servizio di intermediazione abbia ad oggetto dati personali, nell'intento di rafforzare ulteriormente la trasparenza e l'affidabilità del servizio». Così L. PETRONE, *Il mercato digitale europeo e le cooperative di dati*, in *Contratto e impresa*, 2023, 3, pp. 800-817.

[8] L'interessato è da intendersi, così come previsto dall'art. 4, n. 1, del Reg. (UE) n. 679/2016 (GDPR), come una persona fisica identificata o identificabile.

[9] Per un approfondimento più ampio sulla liceità del trattamento: cfr. F. BRAVO, *Le condizioni di liceità del trattamento dei dati personali*, in G. FINOCCHIARO (diretto da), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, 2019, p. 110 ss.; D. POLETTI, *Art. 6 Liceità del trattamento*, in R. D'ORAZIO-G. FINOCCHIARO-O. POLLICINO-G. RESTA (a cura di), *Codice della* privacy *e data protection*, Milano, 2021, p. 191 ss.; ID., *Le condizioni di liceità del trattamento dei dati personali*, in *Giur. it*., 2019, 12, p. 2783 ss.; con riferimento al ruolo delle condizioni di liceità del trattamento in relazione ai risvolti economici dello sfruttamento dei dati personali v. F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Milano, 2018, spec. p. 107 ss.; con particolare riguardo al consenso dell'interessato C. BASUNTI, *La (perduta) centralità del consenso nello specchio delle condizioni di liceità del trattamento dei dati personali*, in *Contr. e impr*., 2020, 2, p. 860 ss.

[10] Il *Data Governance Act*, nella suddetta previsione, richiama la tutela dell'interessato e il dovere di informazione in capo al titolare del trattamento contenuti nel principio di trasparenza enunciato nel GDPR. In particolare, a titolo esemplificativo ma non esaustivo, si rimanda al *considerando* n. 58 del GDPR «Il principio della trasparenza impone che le informazioni destinate al pubblico o all'interessato siano concise, facilmente accessibili e di facile comprensione e che sia usato un linguaggio semplice e chiaro, oltre che, se del caso, una visualizzazione. Tali informazioni potrebbero essere fornite in formato elettronico, ad esempio, se destinate al pubblico, attraverso un sito *web*. Ciò è particolarmente utile in situazioni in cui la molteplicità degli operatori coinvolti e la complessità tecnologica dell'operazione fanno sì che sia difficile per l'interessato comprendere se, da chi e per quali finalità

degli utenti dei dati e sui termini e le condizioni standard cui sono subordinati tali utilizzi [11].

Appare evidente come il legislatore europeo, in linea con lo spirito che permea l'impianto del Regolamento Generale sulla protezione dei dati n. 679/2016 (GDPR) [12], con detta previsione ha posto l'interessato, con i suoi interessi e diritti, al centro dell'attività di intermediazione di dati offrendo allo stesso una maggiore tutela.

---

sono raccolti dati personali che lo riguardano, quali la pubblicità online. Dato che i minori meritano una protezione specifica, quando il trattamento dati li riguarda, qualsiasi informazione e comunicazione dovrebbe utilizzare un linguaggio semplice e chiaro che un minore possa capire facilmente» ed al *considerando* n. 63 del GDPR «Un interessato dovrebbe avere il diritto di accedere ai dati personali raccolti che la riguardano e di esercitare tale diritto facilmente e a intervalli ragionevoli, per essere consapevole del trattamento e verificarne la liceità. Ciò include il diritto di accedere ai dati relativi alla salute, ad esempio le cartelle mediche contenenti informazioni quali diagnosi, risultati di esami, pareri di medici curanti o eventuali terapie o interventi praticati. Ogni interessato dovrebbe pertanto avere il diritto di conoscere e ottenere comunicazioni in particolare in relazione alla finalità per cui i dati personali sono trattati, ove possibile al periodo in cui i dati personali sono trattati, ai destinatari dei dati personali, alla logica cui risponde qualsiasi trattamento automatizzato dei dati e, almeno quando è basato sulla profilazione, alle possibili conseguenze di tale trattamento. Ove possibile, il titolare del trattamento dovrebbe poter fornire l'accesso remoto a un sistema sicuro che consenta all'interessato di consultare direttamente i propri dati personali. Tale diritto non dovrebbe ledere i diritti e le libertà altrui, compreso il segreto industriale e aziendale e la proprietà intellettuale, segnatamente i diritti d'autore che tutelano il software. Tuttavia, tali considerazioni non dovrebbero condurre a un diniego a fornire all'interessato tutte le informazioni. Se il titolare del trattamento tratta una notevole quantità d'informazioni riguardanti l'interessato, il titolare in questione dovrebbe poter richiedere che l'interessato precisi, prima che siano fornite le informazioni, l'informazione o le attività di trattamento cui la richiesta si riferisce».

[11] Nell'ottica dell'EDPB e dell'EDPS, «I "termini e le condizioni" per il trattamento di dati personali di fatto sono quelli contenuti nel GDPR e pertanto non possono essere modificati, né sostituiti, in virtù di un contratto o di un altro tipo di accordo privato, cfr. EDPB-EDPS, Parere congiunto n. 3/2021, cit., par. 3.4.2, p. 35. Di diverso avviso F. BRAVO in *Le cooperative di dati*, in *Contratto e impresa*, 2023, 3, che spiega: «pare tuttavia che la posizione esternata nella *joint-opinion* sia frutto di un equivoco di fondo, che si riflette su questioni di metodo, e non possa essere condivisa. I termini e le condizioni a cui fa riferimento la nuova disciplina europea sulla data governance – rimessi alla negoziazione delle data cooperatives – sono ben altra cosa rispetto alle condizioni di liceità del trattamento individuate nel GDPR quale base giuridica del trattamento».

[12] La letteratura in commento al Reg. (UE) n. 679/2016 è vastissima. In questa sede ci si limita a rinviare ad alcuni tra i contributi più autorevoli e quindi a V. CUFFARO-R. D'ORAZIO-V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, cit.; G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, 2019; N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, cit. Nella letteratura straniera, a titolo esemplificativo ma non esaustivo, a C. KUNER-L. A. BYGRAVE-C. DOCKSEY, *The EU general data protection regulation (GDPR): a commentary*, Oxford, 2020; MARIUSZ KRZYSZTOFEK, *GDPR: general data protection regulation (EU) 2016/679: Post-Reform Personal Data Protection in the European Union*, Alphen aan den Rijn, 2018. Per un'analisi approfondita dei principi che ispirano le norme del GDPR si veda F. BRAVO *(a cura di), Dati personali. Protezione, libera circolazione e governance. – Vol. 1. Principi*, Pisa, Pacini, 2023, pp. 601.

Il fornitore di servizi di intermediazione, infatti, ha il dovere di anteporre gli interessi dei *data subjects* ai propri facendosi parte diligente affinché questi ultimi possano esercitare i loro diritti. Inoltre, se necessario, gli intermediari di dati hanno l'onere di fornire un'*advice* relativa alle finalità di utilizzo dei dati da parte degli utenti di dati nonché su quelli che sono i termini e le condizioni che si applicano all'utilizzo. Nell'ottemperare a tale ultimo obbligo, il fornitore di servizi di intermediazione dei dati deve utilizzare una modalità che sia comprensibile, di facile accesso, nonché deve garantire sinteticità e trasparenza.

Il *considerando* n. 30 chiarisce ulteriormente la portata della lett. *m*) del già citato art. 12 del DGA.

In primo luogo, con detta premessa, il legislatore europeo ha inteso precisare che all'interno della categoria "fornitori di servizi di intermediazione dei dati" vanno senz'altro inclusi coloro che offrono i loro servizi agli interessati. Questa particolare categoria di intermediari ha la funzione di rafforzare la capacità di agire degli interessati e, in particolare, si legge nel *considerando* cit., «il controllo dei singoli individui in merito ai dati che li riguardano». Per tale ragione gli intermediari che offrono servizi agli interessati hanno lo scopo di assistere i singoli individui che ne beneficiano nell'esercizio dei loro diritti, così come previsti dal GDPR [13] e quindi in particolare per: il consenso (o la sua eventuale revoca), il diritto all'accesso ai propri dati, il diritto alla rettifica dei dati personali inesatti, il diritto alla cancellazione o «diritto all'oblio», il diritto alla limitazione del trattamento e il diritto alla portabilità dei dati, che consente agli interessati di trasferire i propri dati personali da un titolare del trattamento a un altro.

La descritta attività di intermediazione non deve però rappresentare uno strumento equivoco per gli interessati, tale da indurli in errore o persino idoneo a ledere i diritti degli stessi: il «superiore interesse» dei *data subjects* deve sempre per-

---

[13] Sulla natura dei diritti dell'interessato quali «situazioni soggettive» si rimanda a G. ALPA, *La normativa sui dati personali. Modelli di lettura e problemi esegetici*, in *Dir. inf.* 1997, 703 e ss. e CASTRONUOVO, *Situazioni soggettive e tutela nella legge sul trattamento dei dati personali* in *Europa e dir. priv*., 1998, p. 653 ss. Per un approfondimento relativo all'evoluzione della tutela dell'interessato e dei suoi diritti si rimanda, senza pretesa di esaustività, a S. RODOTÀ, *Intervista su privacy e libertà*, a cura di Paolo Conti, Roma-Bari, 2005,19: S. RODOTÀ, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Riv. critica dir. priv*. 1997, p. 583 ss.; G. FINOCCHIARO, voce «*Identità personale (diritto alla)»*, in *Digesto civ.* Agg., Torino, 2010, p. 721 ss.; D. SIMEOLI, *La tutela dell'interessato*, in R. ACCIAI (a cura di), *Il diritto alla protezione dei dati personali. La disciplina sulla privacy alla luce del nuovo codice*, Rimini, 2014; C. LO SURDO, *Dati personali e strumenti di tutela del soggetto interessato*, in *Danno e resp*. 2003; A. NERVI, *I diritti dell'interessato*, in V. CUFFARO-R. D'ORAZIO-V. RICCIUTO (a cura di), *Il codice del trattamento dei dati personali*; E. PELINO, *I diritti dell'interessato,* in L. BOLOGNINI-E. PELINO-C. BISTOLFI (a cura di), *Il regolamento privacy europeo. Commentario alla nuova disciplina sui dati personali*, Milano, 2016. Per una puntuale disamina sui diritti dell'interessato si rimanda, per tutti, a: A. RICCI, *I diritti dell'interessato*, in G. FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, 2019.

manere e prevalere e quindi, specifica il *considerando* cit., nell'attività di informazione e/o consulenza «è importante che il modello commerciale di tali fornitori garantisca che non vi siano incentivi disallineati che incoraggino i singoli individui a utilizzare tali servizi per mettere a disposizione più dati che li riguardano di quanto non sia nel loro stesso interesse. Ciò potrebbe comprendere l'offerta di consulenza ai singoli individui quanto ai possibili utilizzi dei loro dati e il controllo della dovuta diligenza degli utenti dei dati prima che sia consentito loro di contattare gli interessati, al fine di evitare pratiche fraudolente» [14].

Da tutto quanto sopra si evince come sia preminente e delicato il ruolo dell'intermediario dei dati e quanto sia decisiva l'attività dell'autorità competente [15]

---

[14] Il *considerando* n. 30 del *Data Governace Act* aggiunge inoltre che: «In alcune situazioni potrebbe essere auspicabile raccogliere dati reali in uno spazio di dati personali, affinché il trattamento possa aver luogo all'interno di tale spazio senza che i dati personali siano trasmessi a terzi, al fine di ottimizzare la protezione dei dati personali e della vita privata. Tali spazi di dati personali potrebbero contenere dati personali statici quali nome, indirizzo o data di nascita, nonché dati dinamici generati da una persona ad esempio con l'utilizzo di un servizio online o di un oggetto connesso all'internet delle cose. Potrebbero essere utilizzati anche per conservare informazioni verificate sull'identità quali i numeri di passaporto o informazioni sulla sicurezza sociale, nonché credenziali quali informazioni sulla patente di guida, diplomi o conti bancari».

[15] Si ricorda che, ai sensi dell'art. 11 del *Data Governance Act* i fornitori di servizi di intermediazione dei dati, oltre che rispettare requisiti rigorosi per garantire tale neutralità ed evitare conflitti di interesse, sono soggetti ad un obbligo di notifica alla competente autorità che verifica la conformità alle disposizioni di cui all'art. 12. Con l'entrata in vigore del d.lgs.144/2024 relativo alle «Norme di adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio, del 30 maggio 2022, relativo alla *governance* europea dei dati e che modifica il regolamento (UE) 2018/1724», in data 19 novembre 2024, l'Agenzia per l'Italia Digitale (AgID), ai sensi degli artt. 13, 23 e 26 del Reg. (UE) 2022/868 (*Data Governance Act*), è stata designata quale autorità competente allo svolgimento dei compiti relativi alla procedura di notifica per i servizi di intermediazione dei dati, nonché quale autorità competente alla registrazione di organizzazioni per l'altruismo dei dati. In particolare, secondo quanto disposto dall'art. 2 del citato decreto legislativo, l'AgID svolge la propria attività in maniera imparziale, trasparente, coerente, affidabile e tempestiva, salvaguardando, nell'esercizio della propria attività, la concorrenza leale e la non discriminazione e in conformità agli ulteriori requisiti di cui all'art. 26 del regolamento. È altresì previsto che l'AgID operi in stretta e leale cooperazione con l'Agenzia per la cybersicurezza nazionale (ACN), l'Autorità garante della concorrenza e del mercato (AGCM) e il Garante per la protezione dei dati personali (GPDP) e, a tal fine, può stipulare con gli stessi specifici accordi di collaborazione non onerosi. L'AgID, inoltre, sentite l'Agenzia per la cybersicurezza nazionale, l'Autorità garante della concorrenza e del mercato e il Garante per la protezione dei dati personali per gli aspetti di rispettiva competenza, stabilisce con proprio provvedimento ai sensi dell'art. 16 del regolamento le disposizioni tecniche e organizzative per facilitare l'altruismo dei dati nonché le informazioni necessarie che devono essere fornite agli interessati in merito al riutilizzo dei loro dati nell'interesse generale. L'AgID provvede anche, in applicazione e secondo le modalità di cui all'art. 14 del regolamento, al monitoraggio e al controllo della conformità dei fornitori dei servizi di intermediazione dei dati ai requisiti di cui al Capo III del regolamento medesimo. L'AgID, infine, provvede, in applicazione e secondo le modalità di cui all'art. 24 del regolamento, al monitoraggio e al controllo della conformità alle prescrizioni di cui al Capo IV del regolamento medesimo da parte delle organizzazioni riconosciute per l'altruismo dei dati.

rispetto alla verifica – anche – del rispetto del superiore interesse dei *data subjects*.

Il *Data Governance Act*, normando i servizi di intermediazione di dati e sottoponendoli a precise condizioni come quella oggetto del presente approfondimento, ha risposto, indubbiamente, ad una esigenza che fino alla sua introduzione non aveva trovato pieno compimento: il GDPR ha (aveva) infatti offerto una valida tutela per i dati personali dotando l'interessato di una corazza resistente ma lo ha (aveva) lasciato solo nel confronto con i giganti digitali. Il Reg. UE n. 868/2022 consente invece all'interessato di essere un *player* "parte di una squadra", non più da solo, quindi, "sul campo da gioco". La norma, attribuendo al fornitore del servizio di intermediazione di dati un ruolo attivo nella difesa degli interessi dei *data subjects*, introduce e afferma senza dubbio un nuovo modello di tutela rafforzata dei diritti degli interessati, contribuendo al loro effettivo esercizio.

2. L'efficace mediazione della cooperativa di dati per la tutela del superiore interesse dei *data subjects*.

Le cooperative di dati [16] rappresentano [17], probabilmente, la forma giuridica più

[16] Il *Data Governance Act* definisce i servizi di cooperative di dati come servizi di intermediazione dei dati offerti da una struttura organizzativa costituita da interessati, imprese individuali o da PMI, che sono membri di tale struttura, avente come obiettivi principali quelli di aiutare i propri membri nell'esercizio dei loro diritti in relazione a determinati dati, anche per quanto riguarda il compiere scelte informate prima di acconsentire al trattamento dei dati, di procedere a uno scambio di opinioni sulle finalità e sulle condizioni del trattamento dei dati che rappresenterebbero al meglio gli interessi dei propri membri in relazione ai loro dati, o di negoziare i termini e le condizioni per il trattamento dei dati per conto dei membri prima di concedere l'autorizzazione al trattamento dei dati non personali o prima che essi diano il loro consenso al trattamento dei dati personali»

[17] La cooperativa di dati non è definita nell'ambito del *Data Governance Act*. «Il concetto di "cooperativa di dati" non è rigidamente determinato nel DGA e apre la strada a forme soggettive diverse. Del resto il legislatore europeo, volutamente sintetico su tale aspetto, ha scelto di porre l'elemento oggettivo, la fornitura del "servizio", e non sulla natura oggettiva del fornitore: nel far ciò ha però definito i «servizi di cooperative di dati» senza mai menzionare la società cooperativa, facendo generico riferimento a una organizzazione strutturata costituita dai "membri" che la compongono, da individuarsi nelle persone fisiche cui i dati si riferiscono («interessati» ai sensi del Reg. UE 679/2016), alle imprese individuali o alle piccole e medie imprese (PMI), che abbia come «obiettivi principali» il supporto ai membri in relazione all'uso dei dati che verrà effettuato nella fornitura del servizio». Così F. BRAVO, *Le cooperative di dati,* in *Contratto e impresa*, 2023, 3, pp. 757-799. Sul punto, detto contributo, rappresenta senz'altro il principale approfondimento in materia così come, pioneristico, risulta essere il Progetto di Terza Missione dedicato alle cooperative di dati dell'Università di Bologna di cui è responsabile scientifico il citato autore. Per approfondire gli obiettivi ed il contesto del progetto, nonché le fasi e le attività, la rilevanza e l'impatto, si rimanda al sito dedicato https://site.unibo.it/cooperative-di-dati/it/progetto. Per offrire una ulteriore misura relativa all'importanza del progetto dell'Università di Bologna dedicato alle cooperative di

rispondente alla *ratio* dell'art. 12 del DGA ed in particolare la più efficace per rispondere compiutamente alla condizione prevista dalla lett. *m*).

Se da un lato il legislatore europeo non ha inteso fornire una definizione di cooperativa di dati [18] – né chiarire se il modello cooperativo sia l'unica forma giuridica

---

dati si evidenzia che le unità impegnate nella realizzazione sono sette, di cui due di estrazione accademica, facenti capo al Partner Proponente, e cinque di estrazione imprenditoriale o istituzionale, facenti capo ai Partner Aderenti: (1) Univ. Bologna – Dipartimento di Sociologia e Diritto dell'Economia (Referente Scientifico dell'unità capofila e Responsabile Scientifico del Progetto: Prof. Fabio Bravo), in qualità di Dipartimento Capofila Proponente; (2) Univ. Bologna – Dipartimento di Scienze Giuridiche (Referente Scientifico: Prof. Daniela Memmo), in qualità di Dipartimento Aggregato; (3) Legacoop Romagna (Referente: Dott. Emiliano Galanti); (4) Federcoop Romagna (Referente: Dott. Luca Petrone); (5) Fondazione PICO Innovazione Cooperativa (Referente: Dott. Piero Ingrosso); (6) Alma Vicoo (Referente: Dott. Piero Ingrosso); (7) Onit S.p.a. (Referente: Ing. Vladimiro Buda).

Si rimanda, sempre in tema di cooperative di dati, anche a F. BRAVO, *Il commercio elettronico dei dati personali,* in T. PASQUINO-A. RIZZO-M. TESCARO (a cura di), *Questioni attuali in tema di commercio elettronico*, Napoli, 2020, pp. 83-130; F. BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in *Contratto e impresa Europa*, 2021, 1, pp. 199-256, e, ivi, spt. par. 4.5; D. POLETTI, *Gli intermediari dei dati*, in *European Journal of Privacy Law & Technologies*, 2022, 1, p. 46 ss.; G. RESTA, *Pubblico, privato e collettivo nel sistema europeo di governo dei dati*, in *Riv. trim. dir. pubbl.*, 2022, 4, pp. 971-995, e, ivi, spt. par. 5, ripubblicato anche all'interno del volume seguente: G. RESTA-V. ZENO ZENCOVICH (a cura di), *Governance of/through data*, Roma, 2023, pp. 605-630 e, invi, spt. par. 5 (p. 622 ss.). Per quanto attiene invece a pubblicazioni interdisciplinari sempre afferenti alle cooperative di dati si rimanda a M. MICHELI-E. FARRELL-B. CARBALLA SMICHOWSKI-M. POSADA SANCHEZ-S. SIGNORELLI-M. VESPE, *Mapping the landscape of data intermediaries. Emerging models for more inclusive data governance*, Publications Office of the European Union, Luxembourg, 2023, pp. 47-52, S. GIRISH, *Exploring the value of adding a data layer to cooperatives: Megha farmer cooperative case study*, AAPTI Institute, 2022; A. PENTLAND-T. HARDJONO, *Data Cooperatives*, in A. PENTLAND-A. LIPTON-T. HARDJONO (eds.), *Building the New Economy*, MIT Press Work in Progress, 2020, Chapter 2; T. HARDJONO-A. PENTLAND, *Empowering Innovation through Data Cooperatives*, in A. PENTLAND-A. LIPTON-T. HARDJONO (eds.), *Building the New Economy*, MIT Press Work in Progress, 2020, Chapter 4; A. PENTLAND-T. HARDJONO-J. PENN-C. COLCLOUGH-B. DUCHARME-L. MANDEL, *Data Cooperatives: Digital Empowerment of Citizens and Workers*, Whitepaper, in *MIT Connerction Science*, 1 February 2019, J. Tait, *The Case for Data Cooperatives*, Whitepaper Series, *Open Data Manchester*, 6th September 2021, in *https://thedataeconomylab.com/2021/09/06/the-case-for-data-cooperatives*; S. MEHTA-M- DAWANDE-V. MOOKERJE, *Can data cooperatives sustain themselves?*, in *LSE Business Review*, 2021; E. BIETTI-A. ETXBERRIA-M. MANNAN-J. WONG, *Data Cooperatives in Europe: A Legal and Empirical Investigation*, White Paper created as part of *The New School's Platform Cooperativism Consortium and Harvard University's Berkman Klein Center for Internet & Society*, Research Sprint, December 2021, in *https://cyber.harvard.edu/sites/default/files/2022-02/Data_Cooperatives_Europe-group2.pdf*; T. HARDJONO-A. PENTLAND, *Data Cooperatives: Towards a Foundation for Decentralized Personal Data Management, in MIT Connection Science*, 15th May 2019; T. SCHOLTZ, *Platform Cooperativism. Challenging the Corporate Sharing Economy*, in *Rosa Luxemburg Stiftung*, New York, 2016; M.F. MORELL-R. ESPELT-M.R. CANO, *Cooperativismo de plataforma: Análisis de las cualidades democráticas del cooperativismo como alternativa económica en entornos digitales*, in *CIRIEC-España, revista de economía pública, social y cooperativa*, 2021.

[18] Le cooperative di dati hanno trovato nel *Data Governance Act* un riconoscimento normativo ma

attuabile per le cooperative di dati – dall'altro ha scelto di definirne dettagliatamente obiettivi e finalità. Ed è proprio nell'ambito degli obiettivi e delle finalità delle cooperative di dati (*rectius*, servizi di cooperative di dati) che la rispondenza all'esigenza di tutela – superiore – degli interessi dei *data subjects* e dell'esercizio rafforzato dei loro diritti emerge chiaramente.

Nel *considerando* n. 31 si legge infatti che «Le cooperative di dati mirano a raggiungere una serie di obiettivi, in particolare a rafforzare la posizione dei singoli individui, affinché compiano scelte informate prima di acconsentire all'utilizzo dei dati, influenzando i termini e le condizioni, stabiliti dalle organizzazioni di utenti dei dati, cui è subordinato l'utilizzo dei dati, in modo da offrire scelte migliori ai singoli membri del gruppo, o trovando possibili soluzioni alle posizioni contrastanti dei singoli membri di un gruppo in merito alle modalità di utilizzo dei dati laddove tali dati riguardino più interessati all'interno di tale gruppo. In tale contesto è importante riconoscere che i diritti a norma del regolamento (UE) 2016/679 sono diritti personali dell'interessato e che quest'ultimo non può rinunciarvi».

Appare quindi evidente come le cooperative di dati possano rappresentare la forma perfetta per sinterizzare al meglio le esigenze di perseguimento degli interessi superiori dei *data subjects*, tanto più quando questi ultimi rivestono la qualità di soci cooperatori.

Si osservi.

Il modello cooperativo [19] è in grado di incarnare, più di qualsiasi altro modello tradizionale capitalistico, il principio di solidarietà [20], di valenza costituzionale, e di

---

le *data cooperatives* erano una realtà già realizzata in ordinamenti europei e non: esempio, infatti, è *Driver's Seat* realtà americana operante nel settore dei trasporti (cfr. www.driversseat.co).

[19] Per una analisi approfondita del sistema cooperativo si rimanda, *ex multis*, a F. GALGANO, *Il ruolo dell'impresa cooperativa nel quadro delle istituzioni dell' economia*, in *Rivista del diritto commerciale e del diritto generale delle obbligazioni*, 1976, 11-12, 1, pp. 335-343; F. GALGANO, *La cooperazione nel sistema costituzionale*, in *Nuovo diritto agrario*, 1977, 3, 1, pp. 409-426; F. CASALE, *Scambio e mutualità nella società cooperativa*, in *Quaderni di Giurisprudenza Commerciale*, Milano, 2005; M. LAMANDINI-P. MORARA, *Cooperative a mutualità prevalente e quotazione di strumenti finanziari nei mercati regolamentati. Un primo approccio pratico mediante la presentazione di una bozza di statuto*, in *Rivista di diritto societario*, 2008, 3, p. 694 ss.; G. RIOLFO, *Il sistema monistico nelle società di capitali e cooperative*, Milano, 2010; M.C. TATARANO, *La nuova impresa cooperativa*, in *Trattato di diritto civile e commerciale*, diretto da Cicu-Messineo-Mengoni, Milano, 2011; G. BONFANTE (a cura di), *La società cooperativa*, in *Trattato di diritto commerciale*, Vol. V, Tomo III, Milano, 2014; L.F. PAOLUCCI, *Le società cooperative*, Milano, 2014; A. BASSI-S. FORTUNATO (a cura di), *Mutualità e capitale nelle cooperative*, in *Quaderni di giurisprudenza commerciale*, Milano, 2017 F. VELLA-R. GENCO-P.L. MORARA, *Diritto delle società cooperative*, Bologna, 2018; M.J. MORILLAS JARILLOS-M.I. FELIU REY, *Curso de cooperativas*, 3ª ed., Madrid, 2018.

[20] Sul principio di solidarietà, per tutti, si veda S. RODOTÀ, *Solidarietà. Un'utopia necessaria,* cit., p. 21 ss.; G. ALPA, *I principi generali*, cit., p. 393 ss., G. ALPA, *Solidarietà. Un principio normativo*, Bologna, 2022; G. ALPA, *Note sul principio di solidarietà come principio precettivo nel diritto interno e nel diritto dell'Unione europea*, in *Lo Stato*, 2022, 18, pp. 11-56. Si rimanda inoltre, per un ulteriore e più specifico approfondimento, a F. BRAVO *Il principio di solidarietà*, in: F. BRAVO (a cura

declinarlo nel suo quotidiano e concreto operare non però nella sola dimensione di obbligo/dovere e, soprattutto, nella sua accezione privatistica.

Il modello cooperativo è vocato, per sua natura, ad indirizzare l'esercizio dell'attività di impresa nell'interesse dei soci che sono, ciascuno, protagonisti indiscussi nelle interlocuzioni e nelle decisioni.

È quindi evidente come soprattutto attraverso le cooperative di dati sia possibile, dando seguito alla disposizione di cui alla lett. *m*), perseguire un potente effetto di *empowerment* per gli interessati così come per i *data holder*[21].

La forza del singolo (interessato) si amplifica grazie al modello cooperativo in

---

di), *Dati personali. Protezione, libera circolazione e governance. – Vol. 1. Principi*, Pisa, 2023, pp. 541-601; F. BRAVO, *Il principio di solidarietà in materia di protezione dei dati personali nelle decisioni del Garante e della Corte di Cassazione*, «*Contratto e impresa*», 2023, 2, pp. 405-441; F. BRAVO, *Il principio di solidarietà tra data protection e data governance*, in *Il diritto dell'informazione e dell'informatica*, 2023, 3, pp. 481-518. In detto contributo l'autore dà evidenza di come, il principio di solidarietà, ispiri l'interno *Data Governance Act*. In particolare, si legge: «L'altruismo dei dati ha punti di contatto evidenti con il principio di solidarietà, perché vengono delineati strumenti per l'uso non autoreferenziale del dato, che circola nella prospettiva del soddisfacimento di interessi altri rispetto a quelli propri del soggetto a cui i dati si riferiscono o appartengono. È un meccanismo di solidarietà, tuttavia, che qui opera in maniera diversa rispetto alle altre ipotesi di applicazione del principio in parola: non si configura più come "dovere" (nella sua dimensione privatistica, di tipo orizzontale, o nella sua dimensione pubblicistica, di tipo verticale), ma come "atto volontario", come esercizio di autonomia privata, come atto di autodeterminazione informativa orientato al raggiungimento di interessi altrui o collettivi. Qui la solidarietà non opera nella dimensione del dovere o dell'obbligo, a cui sembra essere confinata leggendo l'art. 2 Cost.: qui la solidarietà, personale e sociale, opera nella dimensione del diritto soggettivo, nella dimensione dei poteri e delle facoltà che sono rimesse al soggetto a cui i dati appartengono, in forza di un atto di autonomia privata che, come tale, è il frutto dell'autodeterminazione. È cioè espressione di libertà. Non siamo dunque al cospetto di una "solidarietà imposta", di una solidarietà che si fa "dovere", ma di una "solidarietà volontaria", che non solo ha i tratti della "spontaneità", ma è anche espressione della libera determinazione dell'individuo e che, quindi, si fa "diritto. Si rimanda inoltre a A. RICCI, *Sulla funzione sociale del diritto alla protezione dei dati personali*, in *Contratto e impresa*, 2017, 2, p. 587. Si veda anche P. MENGOZZI, *L'idea di solidarietà nel diritto dell'Unione europea*, Bologna, 2022. Infine, si legga M. TAMPIERI, *La riscoperta del principio di solidarietà*, in *Jus Civile*, 2020.

[21] Sul punto osserva F. Bravo nel contributo dedicato alle cooperative di dati già citato: «I rischi per gli interessati (e per i titolari dei dati), a cui la disciplina in materia di data governance ha inteso porre rimedio, appaiono leniti nel caso di intermediazione mediante cooperative di dati, che, strutturate con il modello mutualistico, possono ingenerare indubbi effetti di *empowerment* per i *data subject* (e per i *data holder*), nell'esercizio dei loro diritti. Infatti tale modello, meglio di altri, si adatta ad interpretare il principio normativo di solidarietà in quanto la cooperativa, strutturalmente, prevede un'operatività di impresa nell'interesse dei propri soci e una struttura democratica volta a favorire la discussione, il confronto e l'adozione delle decisioni da parte dei soci. Si tratta di un sistema particolarmente congeniale qualora la cooperativa è una data cooperative, i cui soci – data subjects o data holders – possono confrontarsi sulle scelte di utilizzo dei dati, adottare le relative decisioni e mantenere il controllo su di essi. Tra gli intermediari di dati, per vocazione le *data cooperatives* sono quelle che meglio dovrebbero riuscire ad agire perseguendo il prioritario e superiore interesse dei data subjects – ai sensi dell'art. 12, par. 1, lett. *m*), del DGA –, segnatamente qualora essi rivestano la qualità di soci» (F. BRAVO, *Le cooperative di dati*, cit.).

cui il socio (*data subjects*) nella *governance* collettiva trova condizioni di maggior favore – che da solo non avrebbe né sarebbe in grado di ottenere – e maggiori tutele.

Si pensi, restando nei limiti di quanto previsto dalla lett. *m*) dell'art. 12, all'esercizio dei diritti da parte dell'interessato che, secondo la previsione normativa in esame deve risultare facilitato dall'attività di intermediazione dei dati: è indubbio che una cooperativa di dati potrà offrire una informativa afferente al trattamento ed una successiva tutela ben più efficace rispetto non solo a quella di cui può godere il singolo interessato ai sensi del GDPR, chiamato da solo a confrontarsi nel complesso scenario digitale, ma anche rispetto a possibili diversi meccanismi di tutela offerti, nell'intermediazione dei dati di cui al *Data Governance Act*, con qualsiasi altro modello societario in cui non sia prevalente la mutualità bensì il profitto.

Si pensi anche alla possibilità per l'interessato-socio di ricevere una consulenza sull'utilizzo dei dati e sulle condizioni a cui è sottoposto il trattamento, prima che presti il proprio consenso: la cooperativa di dati, operando nell'interesse del proprio socio, avrà tutto l'interesse a rispettare i requisiti di chiarezza, immediatezza, accessibilità, comprensibilità, essenzialità così come la lett. *m*) richiede; il socio, peraltro, ricevendo direttamente consulenza dalla struttura organizzativa di cui è parte integrante, diviene il primo *tester* dell'efficacia dell'attività della cooperative, essendo in grado di comprendere se, davvero, i propri interessi siano primariamente tutelati, per poi decidere insieme agli altri soci, dall'interno, le modifiche da apportare per raggiungere gli obiettivi posti dal DGA. È quindi la stessa cooperativa di dati, nella sua attività di intermediazione rivolta nell'interesse del socio, a ricevere un importante *feedback* in termini di *compliance* alla normativa a cui è soggetta, con particolare riguardo alle condizioni di cui all'art. 12 GDA a cui è sottoposta nello svolgimento della propria attività.

Si tratta pertanto di un modello efficace anche nella direzione inversa, socio-cooperativa, con la cooperativa di dati che esce rafforzata dallo scambio, positivo e propositivo, con i suoi soci.

3. L'intermediazione "interessata" della cooperativa di dati, tra (in)neutralità e responsabilità.

La cooperativa di dati non è un intermediario neutrale.

La lett. *m*) di cui all'art. 12 del *Data Governance Act*, afferma, come detto, un principio non derogabile per coloro che intendono operare nell'ambito dell'intermediazione dei dati: il perseguimento dell'interesse superiore degli interessati.

Tale norma pone un vincolo inevitabile, imprescindibile, sulle scelte etiche ed economiche degli intermediari tanto è vero che, come pure evidenziato, il modello che meglio sembrerebbe corrispondere al rispetto di tale previsione – che è anche condizione necessaria per l'esercizio dell'attività di intermediazione – è la cooperativa di dati in ragione del principio mutualistico che ispira detta forma giuridica.

L'onere di informativa previsto dalla lett. *m*) e, ove necessario, la consulenza che l'intermediario deve fornire agli interessati, oltre a richiamare gli obblighi che incombono sul titolare del trattamento nell'ambito della protezione dei dati personali, rimandano, tra affinità e differenze, agli obblighi cui sono soggetti, ad esempio, gli intermediari finanziari e i mediatori (immobiliari, ad esempio).

Senza pretesa di esaustività, ma al solo fine di offrire ulteriori prospettive utili alla riflessione, si pensi, a titolo esemplificativo, all'obbligo informativo che incombe sull'intermediario finanziario [22]: le informazioni che l'intermediario deve fornire all'investitore devono essere specifiche, adeguate, complete e personalizzate [23]. È però vero che la posizione dell'intermediario finanziario non è del tutto affine a quella dell'intermediario di dati, nella specie la cooperativa di dati: l'informativa resa dall'intermediario finanziario assume i connotati di un limite alle logiche opportunistiche dell'attività prestata, mentre la cooperativa di dati, nell'esercizio della sua attività di intermediazione, è chiamata a finalizzare l'interesse superiore del *data subjects* a cui è tassativamente vincolata.

Volendo tracciare un ulteriore confronto con tutt'altri modelli, va rimarcato che l'obbligo informativo è esteso anche al mediatore mobiliare. Invero, ai sensi dell'art. 1759 c.c., «il mediatore è tenuto a riferire ai contraenti le circostanze afferenti alla valutazione e alla sicurezza dell'affare. L'obbligo di informativa riguardante il mediatore non concerne solo le circostanze note, ma anche quelle conoscibili con l'uso della diligenza da lui ordinariamente eseguibile; esso implica anche il divieto di fornire le informazioni sulle quali non abbia consapevolezza e che non abbia controllato» [24].

La *ratio* dell'art. 1759 c.c. va rinvenuta nella necessità di salvaguardare le parti contraenti che davanti ad una parziale o errata rappresentazione della realtà, potrebbero vedere i loro interessi compressi. Il mediatore quindi deve evitare che il proprio interesse personale prevalga su quello delle parti [25].

La cooperativa di dati invece è chiamata a perseguire l'interesse, definito «superiore», di una parte (l'interessato, probabilmente socio), proprio nell'esercizio dell'attività di intermediazione.

---

[22] Il primo riferimento è all'art. 21 del Testo Unico della Finanza che disciplina il comportamento dell'intermediario finanziario: questi deve essere ispirato ai principi di diligenza, correttezza e trasparenza nella fase di profilatura del cliente, in modo da pervenire ad un'assegnazione del profilo di rischio che sia esatta e non sovradimensionata. Un ulteriore riferimento normativa è all'art. 29 del Regolamento Intermediari del 1998 nel sistema pre-MiFID.

[23] «Gli obblighi informativi incombenti sugli intermediari finanziari non possono certo dirsi soddisfatti dalla sola consegna del prospetto generale dei rischi relativi agli investimenti (o di altre comunicazioni generiche e standardizzate) o dall'indicazione contrattuale del massimo rischio convenzionalmente previsto o ancora dalla dichiarazione con la quale il cliente investitore dà atto di aver ricevuto le informazioni necessarie ai fini della completa valutazione del grado di rischiosità». Così C. App. Palermo, sez. III, sent. n. 1705 del 5 ottobre 2023, in *DeJure*.

[24] Così C. App. Milano, sez. I, sent. n. 1201 dell'8 aprile 2022.

[25] C. App. Cagliari, sent. n. 336 del 3 novembre 2023.

La lett. *m*) dell'art. 12 del *Data Governance Act* offre spunti di riflessione anche per quel che attiene le eventuali responsabilità degli intermediari (nella specie, delle cooperative di dati) nel caso in cui manchino di osservare la previsione normativa.

Senz'altro, trattandosi di condizione necessaria ai fini della fornitura dei servizi di intermediazione di dati, va da sé che l'inosservanza comporterà l'eventuale intervento dell'autorità, su segnalazione o meno. Ma anche l'interessato potrebbe, in ragione della lesione del proprio superiore interesse, invocare l'intervento dell'autorità di settore (Autorità per l'intermediazione dei dati), ai fine di assicurare che l'intermediario rispetti le condizioni per la fornitura del servizio, incluso l'obbligo di agire nel superiore interesse dei *data subjects*, e (se del caso) di far valere la responsabilità della cooperativa di dati, in caso di violazione.

Lo stesso dicasi qualora l'interessato venga fornita una informativa parziale e/o una consulenza non adeguata: il *data subject* potrebbe richiedere l'intervento dell'Autorità di settore per ottenere il rispetto degli obblighi sorti a carico dell'intermediario e, se del caso, far valere le responsabilità della cooperativa di dati verso l'interessato.

Da esplorare, in tal senso, i profili di responsabilità emergenti, per il fornitore dei servizi di intermediazione di dati, anche sul piano civilistico, con rimedi di tipo risarcitorio [26].

4. Brevi riflessioni conclusive.

Il modello cooperativo per i servizi di intermediazione dei dati rappresenta senz'altro, come detto, una delle forme giuridiche privilegiate per quel che attiene l'esercizio dell'attività di intermediazione dei dati, ma non l'unica.

Invero, la struttura organizzativa del servizio di cooperativa di dati potrebbe assumere forme soggettive diverse (quella di consorzio e/o di una rete d'imprese e/o di associazione temporanea d'imprese ad esempio) e quindi differenti modelli di *business*. Senz'altro, come detto, la finalità mutualistica rappresenta la principale solida colonna su cui poggia la tutela rafforzata dell'interessato anche nell'esercizio dei propri diritti [27].

---

[26] Per quanto attiene la responsabilità dell'intermediario finanziario si rileva che dall'inosservanza dell'obbligo informativo gravante sull'intermediario deriva la sua responsabilità per inadempimento (così Trib. Nuoro, sez. II, sent. n. 449 del 3 agosto 2023) financo pre contrattuale (Trib. Terni, sez. I, sent. n. 636 del 20 settembre 2023). Sulla responsabilità del mediatore si richiamano, *ex multis*, Cass. Civ. sez. II, sent. n. 11371 del 2 maggio 2023; Cass. Civ., sez. II, sent. n. 17385 del 16 giugno 2023; Cass. Civ., sez. III, sent. n. 34503 dell'11 dicembre 2023.

[27] Sul "neomutualismo" e sul "neomutualismo digitale" si rimanda a P. VENTURI-F. ZANDONAI, *Neomutualismo. Ridisegnare dal basso competitività e welfare*, Milano, 2022; AA.VV., *Le cooperative e la sfida all'innovazione digitale: il neo mutualismo in 10 tesi*, a cura di Legacoop e Fondazione PICO ("Manifesto" sul neomutualismo digitale di Legacoop e Fondazione PICO).

Le attività previste dalla lett. *m*) dell'art. 12 (quindi informazione e assistenza) aprono inoltre molteplici scenari.

In primo luogo, occorrerà verificare nel concreto in che modo il modello cooperativo intende garantire il rispetto del superiore interesse dei *data subjets*, quanto alle modalità attraverso cui rendere l'informativa agli interessati. Qualsiasi sarà la forma scelta (anche tecnologica) l'intermediario dovrà comunque considerare – essendo la previsione oggetto di condizione controllata e monitorata dall'autorità – che le modalità con cui intende rendere l'informativa dovranno essere in qualche modo tracciate per assicurarsi, lato suo, una valida prova (in termini di *accountability*) rispetto alla *compliance* all'adempimento anche nel caso in cui si tratti di un socio/interessato, sia con riguardo alla fonte normativa di cui agli art. 13 e 24 GDPR, sia con riguardo alle condizioni per lo svolgimento dell'attività di intermediazione di dati previste dall'art. 12 DGA.

Analoghe considerazioni valgono anche per l'attività di consulenza che, secondo quanto previsto dalla lett. *m*) cit., deve essere concisa, trasparente, intellegibile e facilmente accessibile: se sotto il profilo dell'accessibilità il rispetto, o meno, della previsione appare sufficientemente verificabile nell'immediato altrettanto non può dirsi per gli ulteriori requisiti relativi alle altre caratteristiche poco sopra elencate.

Per l'intermediario di servizi, che sia esso una cooperativa o meno, risulterà probabilmente utile effettuare una preventiva verifica del rispetto della disciplina in esame, per evitare di incorrere in provvedimenti correttivi o, peggio in provvedimenti di sospensione o cessazione dell'attività di intermediazione di dati imposti dalle autorità di settore.

Anche lo statuto, nelle cooperative di dati di neo costituzione in particolare, così come le procedure che regolano le attività interne alla struttura organizzato, possono essere utili strumenti per rendere *compliant* l'attività al regime normativo ora considerato. Altresì, possono assumere un ruolo di rilievo anche gli *audit* diretti a verificare preventivamente il rispetto delle singole condizioni di cui all'art. 12 del DGA.

Al di là delle specifiche soluzioni che nel concreto le cooperative di dati adotteranno – che in termini di costi/benefici implicano anche la possibilità di accedere a eventuali significativi vantaggi fiscali [28] – quel che più di tutti appare in grado di

[28] «Ai fini delle agevolazioni previste per le Cooperative/Onlus, debbono essere accuratamente distinte le cooperative che realmente perseguono una finalità mutualistica, ovvero quello che operano nell'interesse economico dei loro soci e intrattengono con questi ultimi una relazione non puramente commerciale, bensì personale particolare, in cui essi siano attivamente partecipi ed abbiano diritto ad un'equa ripartizione dei risultati economici, da quelle che tali effettivamente non sia, le quali non possono beneficiare di un trattamento fiscale di favore rispetto alle società con scopo di lucro (nella specie, il giudice non riteneva condivisibile il disconoscimento, alla cooperativa ricorrente caratterizzata dalla concorrente finalità di assicurare ai soci migliori condizioni di lavoro, dei benefici fiscali di legge sulla scorta dell'erogazione di maggior retribuzioni ai soci lavoratori, effettuata in ragione di maggiori prestazione effettivamente rese)», Comm. Trib. Prov., sez. I, Isernia, 2 ottobre 2019, n. 168.

fare la differenza sul mercato digitale, anche rispetto ad altri fornitori di servizi di intermediazione, sarà la capacità del modello mutualistico di affermare, quotidianamente, la preminenza degli interessi dei *data subjects*: le cooperative di dati non dovranno limitarsi ad una mera e vacua enunciazione ma occorrerà che realizzino, nel concreto, lo spirito cooperativistico attraverso un saldo ancoraggio al principio di solidarietà utile soprattutto quando il mercato in cui operano muove verso direzioni contrarie.

Allegato

Modello di Statuto di Cooperativa di dati*

S T A T U T O

TITOLO I
DENOMINAZIONE – SEDE – DURATA

Art. 1

È costituita la Società Cooperativa denominata «_____ Società Cooperativa di Dati» (…) [1], in sigla «_____ Soc. Coop.».

La società è costituita ai sensi e per gli effetti di cui al Reg. UE 2022/868. Una volta ottenuta la conferma di cui all'art. 11, comma 9, Reg. UE 2022/868, la cooperativa utilizzerà, nella denominazione, anche la dicitura «*fornitore di servizi di intermediazione dei dati riconosciuto nell'Unione*» nelle sue comunicazioni scritte e orali, nonché un logo comune [se ed in quanto realizzato dalle competenti autorità].

Art. 2

La Cooperativa ha sede nel Comune di _____.

Su deliberazione del Consiglio di Amministrazione, essa può trasferire la sede sociale nel territorio nazionale nonché istituire e sopprimere sedi secondarie, succursali, agenzie e filiali fuori della propria sede sociale.

Art. 3

La Cooperativa ha durata fino al 31/12/….; tale durata potrà essere prorogata e la Cooperativa anticipatamente sciolta con deliberazione dell'Assemblea straordinaria dei soci.

---

* *Modello di Statuto di Cooperativa di dati, elaborato da Gianluca Riolfo nell'ambito del Progetto di Terza Missione dell'Università di Bologna in tema di Cooperative di dati (P.I. Fabio Bravo), sulla base di un modello di statuto di società cooperativa che rinvia alla struttura organizzativa delle società per azioni elaborato e prodotto da Federcoop Romagna Soc. Coop, società di servizi e consulenza alle imprese di Legacoop Romagna, partner di progetto, in accordo con la Lega Nazionale delle Cooperative e Mutue (Legacoop Nazionale). Federcoop Romagna, dunque, è autore del modello di statuto di società cooperativa che rinvia alla struttura organizzative delle società per azioni, mentre Gianluca Riolfo è autore delle modifiche, degli adattamenti e delle annotazioni apportate per giungere all'elaborazione del modello di Statuto di Cooperativa di dati.*

[1] Il presente modello di statuto di cooperativa di dati rinvia primariamente al modello organizzativo delle società per azioni. Rimane ferma la possibilità di utilizzare il modello organizzativo della società a responsabilità limitata, con i necessari adeguamenti.

TITOLO II
SCOPO – OGGETTO

Art. 4

La Cooperativa è retta e disciplinata dai principi della mutualità senza fini di speculazione privata.

Lo scopo che la Cooperativa intende perseguire è quello di offrire servizi per mettere in collegamento i soci e contribuire alla messa in comune efficiente dei loro dati, nonché agevolare gli stessi nella condivisione bilaterale o multilaterale dei dati, anche attraverso la creazione di piattaforme o banche dati che consentano la condivisione o l'utilizzo congiunto dei dati, o l'istituzione di un'infrastruttura specifica per l'interconnessione di interessati e titolari dei dati con gli utenti dei dati.

Per il raggiungimento del suddetto scopo mutualistico, i soci instaurano con la Cooperativa, oltre al rapporto associativo, un ulteriore rapporto mutualistico (…)[2] finalizzato alla costituzione – attraverso l'attività della cooperativa – di rapporti commerciali volti alla condivisione dei dati degli stessi soci (interessati o titolari dei dati) con i potenziali utenti di dati, nonché a consentire ai medesimi soci l'esercizio dei loro diritti in relazione ai propri dati personali.

I criteri e le regole inerenti alla disciplina dei rapporti mutualistici tra la Cooperativa ed i soci, distinti ed autonomi rispetto al rapporto sociale, sono stabiliti da apposito Regolamento interno predisposto, nel rispetto del principio di parità di trattamento di cui all'art. 2516 c.c., dagli amministratori ed approvato dall'Assemblea ordinaria dei soci stessi con le maggioranze previste per l'Assemblea straordinaria.

Per il raggiungimento dei propri scopi la cooperativa opera e agisce nel superiore interesse dei soci.

I soci concorrono alla gestione dell'impresa, partecipando alla formazione degli organi sociali e alla definizione della struttura di direzione e conduzione dell'impresa; partecipano alla elaborazione di programmi di sviluppo e alle decisioni concernenti le scelte strategiche, nonché alla realizzazione dei processi produttivi dell'azienda; contribuiscono alla formazione del capitale sociale e partecipano al rischio d'impresa, ai risultati economici ed alle decisioni sulla loro destinazione; mettono a disposizione, al fine del raggiungimento delle finalità proprie della cooperativa, i propri dati (di natura personale o non personale) che saranno tratti nel rispetto delle normative interne ed europee vigenti.

In considerazione di quanto sopra, lo Statuto assume pertanto valore di "patto societario", di cui i soci possono avvalersi ed a cui debbono sottostare.

La rappresentanza e la tutela dei soci, come tali, viene esercitata dalla Cooperativa, nell'ambito della legge in materia, dello Statuto sociale e dei regolamenti interni.

Art. 5

La Cooperativa ha per oggetto, con riferimento ai requisiti ed agli interessi dei soci, l'esercizio delle seguenti attività:

a) supportare i soci nell'esercizio dei loro diritti in relazione a determinati propri dati, espressamente identificati dal socio nel rapporto mutualistico, all'atto della propria entrata nella società;

b) supportare i soci per consentire agli stessi di operare consapevolmente scelte informate prima di acconsentire al trattamento dei dati da parte di soggetti terzi;

c) agevolare e supportare lo scambio di opinioni da parte dei soci sulle finalità e sulle condizioni del trattamento dei dati che rappresentino al meglio gli interessi degli stessi in relazione ai loro dati;

d) negoziare termini e condizioni commerciali – compresa la fissazione del prezzo – per il trattamento dei dati da parte di soggetti terzi e per conto dei soci/membri prima di concedere l'autorizzazione al trattamento dei dati non personali o prima che i membri stessi diano il loro consenso al trattamento dei dati personali;

---

[2] Di mandato, anche con rappresentanza, o similare. Va specificato nel Regolamento e poi tradotto nel singolo accordo.

e) fornire un servizio di analisi dei dati resi disponibili dai soci, sia a beneficio dei soci tessi sia a beneficio di soggetti terzi, in quest'ultimo caso a fronte del pagamento del servizio sulla base di tariffe predefinite.

(…) [3]

Per la realizzazione di tale oggetto sociale, essa opera attraverso procedure di accesso al servizio eque, trasparenti e non discriminatorie e provvede, fra l'altro, a:

– raccogliere e gestire i dati apportati da ciascuno socio alla cooperativa;

– agevolare lo scambio dei dati nel formato in cui vengono ricevuti da parte di un socio (interessato o titolare dei dati), convertirli in formati specifici solo allo scopo di migliorare l'interoperabilità a livello intrasettoriale e intersettoriale, se richiesto dall'utente dei dati, se prescritto dal diritto dell'Unione o per garantire l'armonizzazione con le norme internazionali o europee in materia di dati, offrendo ai soci (interessati o titolari dei dati) la possibilità di non partecipare a tali conversioni;

– offrire strumenti e servizi supplementari specifici ai soci (titolari dei dati o interessati), anche forniti da soggetti terzi rispetto alla cooperativa di dati, allo scopo di facilitare lo scambio dei dati, come la conservazione temporanea, la cura, la conversione, l'anonimizzazione e la pseudonimizzazione, nonché – e più in generale – servizi di *data-based* nelle logiche dell'uso e del riuso consapevole dei dati personali, secondo la disciplina europea della *data governance*. Tali strumenti e servizi sono utilizzati solo su richiesta o approvazione esplicita del titolare dei dati o dell'interessato e gli eventuali strumenti di terzi offerti in tale contesto non utilizzano i dati per altri e diversi scopi;

– promuovere la formazione tecnica specifica e l'assistenza mutualistica in genere a favore dei soci cooperatori, con riferimento alle tematiche del consenso informato, della portabilità dei dati e di ogni altra tematica ad esse legate, al fine di consentire un uso consapevole ed informato dei dati da parte dei soci.

La Cooperativa, inoltre, potrà svolgere, in modo non prevalente, qualunque altra attività connessa od affine a quelle sopra elencate, compiere tutti gli atti e concludere tutte le operazioni contrattuali di natura mobiliare, immobiliare, industriale, commerciale e finanziaria, necessarie od utili alla realizzazione degli scopi sociali e comunque sia direttamente che indirettamente attinenti ai medesimi; pertanto, essa potrà, fra l'altro e per indicazione meramente esemplificativa:

a) assumere interessenze e partecipazioni, sotto qualsiasi forma, in altre cooperative di dati, consorzi o enti che svolgano attività analoghe, accessorie, complementari o strumentali all'attività sociale, non a scopo di alienazione e comunque senza che si configuri operatività nei confronti del pubblico, nonché partecipare sia come capo-gruppo sia come semplice aderente a gruppi cooperativi paritetici ai sensi dell'art. 2545-*septies* c.c., operanti nell'intermediazione dei dati, sia a contratti di rete o altre forme di aggregazione con soggetti che svolgano attività analoghe o funzionali al raggiungimento degli scopi sociali;

b) concedere avalli cambiari, fideiussioni ed ogni altra garanzia sotto qualsiasi forma per facilitare l'ottenimento del credito agli enti e società, cui la Cooperativa aderisce.

Infine, la Cooperativa può effettuare, esclusivamente per il conseguimento dell'oggetto sociale, la raccolta del risparmio presso i soli soci, conformemente a quanto previsto dall'art. 11 D.Lgs. n. 385/93 («Testo unico delle leggi in materia bancaria e creditizia») e dalle relative disposizioni di attuazione vigenti; le modalità di esercizio di tale attività saranno disciplinate da apposito regolamento interno approvato dall'Assemblea ordinaria dei soci. Pertanto, è vietata alla cooperativa la raccolta di risparmio tra il pubblico, se non nei limiti e nelle forme consentite dalla legge.

La Cooperativa potrà emettere gli strumenti finanziari previsti dal Titolo IV del presente statuto.

---

[3] Può essere utile declinare più nello specifico e dettagliare meglio i contorni delle singole attività che la società decide di svolgere nel caso concreto.

Art. 5-bis

L'Assemblea dei soci, nella prima riunione utile, su proposta del Consiglio di Amministrazione, dovrà approvare uno specifico Regolamento volto a disciplinare il rapporto mutualistico per la gestione/conservazione/messa disposizione, da parte della cooperativa, dei dati dei singoli soci e la cui titolarità resta in capo agli stessi. In esso andranno stabilite, tra le altre cose, la struttura del rapporto mutualistico con riferimento all'individuazione dei dati da conferire, l'ambito di circolazione, l'eventuale durata temporale del servizio, le finalità e per quali trattamenti, e così via.

Nel Regolamento saranno regolate anche le modalità di manifestazione del consenso per il trattamento dei dati di natura personale, se il trattamento avviene da parte della cooperativa, la forma giuridica dell'incarico conferito alla cooperativa per la gestione dei dati apportati dai soci, le modalità di partecipazione individuale del singolo socio alle scelte della cooperativa laddove sia richiesto il suo consenso esplicito per l'utilizzo di determinati dati.

L'adesione alla cooperativa di dati, oltre che al conferimento e alla sottoscrizione dello statuto, è condizionata all'espressa accettazione del Regolamento di cui al presente articolo nonché alla stipula dell'apposito rapporto mutualistico.

L'Assemblea dei Soci approva altresì un Codice di Condotta per la Gestione dei Dati volto a regolamentare i comportamenti dei componenti degli organi sociali e dei dipendenti e collaboratori della cooperativa e funzionale a garantire correttezza, trasparenza, assenza di conflitti d'interesse ed eticità nella prestazione dei servizi offerti dalla cooperativa.

TITOLO III
SOCI COOPERATORI

Art. 6

I soci cooperatori sono coloro che stabiliscono, con la propria adesione alla Cooperativa un ulteriore rapporto mutualistico con la Cooperativa medesima, con cui attribuiscono alla cooperativa il potere di agire, a seconda dei casi, in sostituzione di essi o in nome e per loro conto per la realizzazione degli obiettivi e delle finalità proprie della cooperativa di dati di cui fanno parte e che caratterizza la partecipazione sociale.

I rapporti mutualistici instaurabili fra la Cooperativa ed i soci cooperatori saranno definiti e disciplinati dal regolamento interno di cui al precedente art. 5-bis.

I soci cooperatori hanno diritto a concludere rapporti mutualistici con la società, secondo le regole stabilite dal presente statuto e dal regolamento mutualistico, nei limiti della effettiva e concreta capacità della cooperativa di instaurare i suddetti rapporti e di soddisfare gli interessi dei soci medesimi.

Correlativamente, la cooperativa ha il dovere di contrarre con i soci cooperatori che ne facciano richiesta, compatibilmente, con le esigenze della gestione sociale e la necessità di rispettare il principio di parità di trattamento.

Il numero dei soci cooperatori è variabile ed illimitato, ma non potrà essere inferiore al minimo stabilito dalla legge.

Possono essere ammessi a soci cooperatori le persone fisiche che abbiano compiuto il 18° anno di età, nonché le persone giuridiche che siano qualificabili come PMI, che mettano a disposizione della cooperativa, al fine del perseguimento dello scopo sociale da parte di quest'ultima, i propri dati (personali o non personali) in qualità di titolari o di interessati.

Per dati deve intendersi "qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi raccolta di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva" (secondo la definizione di cui all'art. 2, p.to 1, Reg. UE 2022/868).

Non possono essere ammessi a soci cooperatori coloro che esercitino, in proprio o avendovi interessenza diretta, imprese in concorrenza con quella esercitata dalla Cooperativa.

Art. 7

Chi intende essere ammesso come socio cooperatore dovrà presentare al Consiglio di Amministrazione domanda scritta, che dovrà contenere:

a) indicazione del nome, cognome, residenza e data di nascita, codice fiscale;

b) indicazione della tipologia e della natura di dati che intende rendere disponibili alla cooperativa, in conformità al presente statuto e all'apposito regolamento, dei quali dichiara di aver preso visione, nonché dell'attività sociale di cui intende usufruire;

c) la quota sociale che intende sottoscrivere, in misura non inferiore a quanto stabilito dall'Assemblea ordinaria dei soci e comunque non inferiore ad euro _____,00 (_____/00), né superiore al limite massimo fissato dalla legge, nonché l'impegno a versare l'eventuale sovrapprezzo stabilito dall'Assemblea in sede di approvazione del bilancio, su proposta del Consiglio di Amministrazione;

d) dichiarazione di attenersi al presente statuto, ai regolamenti interni ed alle deliberazioni legalmente adottate dagli organi sociali, nonché di approvare specificamente la clausola compromissoria di cui ai successivi artt. 43 e 44.

Il Consiglio di Amministrazione, accertata la esistenza dei requisiti di cui all'art. 6 e l'inesistenza delle cause di incompatibilità in detto articolo indicate, delibera sulla domanda.

L'ammissione è finalizzata allo svolgimento effettivo dello scambio mutualistico e all'effettiva partecipazione del socio all'attività economica della Cooperativa; in ogni caso, l'ammissione deve essere coerente con la capacità economica della Cooperativa di soddisfare gli interessi dei soci, anche in relazione alle strategie imprenditoriali di medio e lungo periodo; inoltre, l'ammissione di nuovi soci non deve compromettere l'erogazione del miglior servizio mutualistico in favore dei soci preesistenti ed il perseguimento dei possibili vantaggi mutualistici.

La deliberazione di ammissione dovrà essere comunicata all'interessato ed annotata, a cura degli amministratori, nel libro dei soci cooperatori, solo dopo che da parte del nuovo ammesso sia stata sottoscritta la quota sociale e sia stato versato l'eventuale sovrapprezzo.

In caso di rigetto della domanda di ammissione, il Consiglio di Amministrazione dovrà, entro sessanta giorni, motivare la relativa deliberazione e comunicarla agli interessati, i quali potranno, entro sessanta giorni dal ricevimento di tale comunicazione, chiedere che sull'istanza si pronunci l'Assemblea; quest'ultima delibera sulle domande non accolte, se non appositamente convocata, in occasione della sua prossima, successiva convocazione.

In caso di deliberazione assembleare difforme da quella del Consiglio di Amministrazione, quest'ultimo provvederà ad assumere, entro trenta giorni dalla data dell'Assemblea, la deliberazione di sua competenza conformemente a quanto stabilito dall'Assemblea medesima.

Il Consiglio di Amministrazione, nella relazione al bilancio, illustra le ragioni delle determinazioni assunte con riguardo all'ammissione di nuovi soci.

A seguito della deliberazione di ammissione del nuovo socio cooperatore, con la quale si stabilisce il tipo di rapporto che sarà instaurato fra la Cooperativa ed il nuovo socio cooperatore, quest'ultimo aderisce in forma scritta alla relativa disciplina contenuta nel regolamento di cui al precedente art. 5-bis.

Art. 8

I soci cooperatori sono obbligati:

a) a versare la quota sociale sottoscritta, con le modalità e nei termini previsti dal successivo art. 20;

b) a versare l'eventuale sovrapprezzo deliberato dall'Assemblea in sede di approvazione del bilancio su proposta degli amministratori;

c) a rendere disponibili alla cooperativa i propri dati, come definiti nell'art. 6, nelle modalità e nei termini definiti dal Regolamento di cui all'art. 5-bis nonché dello specifico rapporto mutualistico instaurato con la cooperativa [4];

[4] Possibile la configurabilità di un conferimento del dato, quale conferimento in natura ed in godimento

d) ad osservare il presente statuto, i regolamenti interni e le deliberazioni legalmente adottate dagli organi sociali;

e) a contribuire al raggiungimento degli scopi sociali, comunque conformemente alle condizioni previste dal Regolamento interno e/o dal rapporto mutualistico.

Art. 9

È fatto divieto ai soci cooperatori di aderire contemporaneamente ad altre cooperative che perseguano identici scopi sociali od esercitino un'attività concorrente.

Art. 10

La qualità di socio cooperatore si perde per recesso, esclusione o per causa di morte.

I rapporti mutualistici si estinguono a seguito di scioglimento del rapporto sociale conseguente a recesso, morte, esclusione del socio cooperatore, ovvero alla cessione della partecipazione sociale, secondo le regole stabilite nel presente statuto.

Art. 11

Oltre che nei casi previsti dalla legge, può recedere dalla Cooperativa il socio cooperatore se la società violi gli impegni assunti verso il socio cooperatore stesso, contenuti nell'accordo che regolamenta il rapporto mutualistico sottoscritto dalla società con il socio cooperatore all'atto della sottoscrizione della quota e disciplinati altresì dal Regolamento di cui all'art. 5-*bis*.

Il recesso non può essere parziale.

La dichiarazione di recesso deve essere comunicata alla Cooperativa per iscritto, tramite lettera raccomandata. Il Consiglio di Amministrazione deve esaminarla entro sessanta giorni dalla ricezione. Se non sussistono i presupposti del recesso, il Consiglio di Amministrazione deve darne immediata comunicazione al socio, che, entro sessanta giorni dal ricevimento della comunicazione, può proporre opposizione innanzi al Collegio Arbitrale.

Riguardo al rapporto sociale, il recesso ha effetto dal ricevimento della comunicazione del provvedimento di accoglimento della domanda.

Di regola, lo scioglimento del rapporto sociale per recesso determina la risoluzione, con la stessa decorrenza, anche dell'accordo tra socio e cooperativa volto a regolare il rapporto mutualistico [5].

Art. 12

L'esclusione è pronunciata dal Consiglio di Amministrazione, oltre che nei casi previsti dalla legge, nei confronti del socio cooperatore:

a) che abbia perso i requisiti di ammissibilità;

b) che venga a trovarsi in una situazione di incompatibilità prevista dall'art. 6;

c) che, senza giustificato motivo e pur dopo formale sollecitazione e diffida, si renda moroso, oltre che nel versamento della quota sociale, altresì nel pagamento dei debiti eventualmente contratti verso la Cooperativa per qualsiasi titolo;

d) che non ottemperi alle obbligazioni derivanti dal presente statuto, dai regolamenti interni, dalle deliberazioni legalmente adottate dagli organi sociali o dal rapporto mutualistico, con gravi inadempienze, che non consentano la prosecuzione del rapporto sociale;

---

conseguenze in termini di valutazione/perizia e iscrizione a bilancio del valore del dato come capitale sociale; preferibile la configurabilità di un accordo separato di utilizzo e gestione dei dati per periodo predeterminato, rinnovabile e sino a revoca sulla base del rapporto mutualistico. L'impostazione dello statuto è basata su questa seconda opzione.

[5] Va tenuta presente la possibile criticità dovuta alla gestione dei dati del socio, apportati alla cooperativa, e il cui utilizzo/gestione potrebbe avere effetti che si protraggono in un periodo temporale anche successivo all'uscita del socio dalla cooperativa. La questione può porsi anche in caso di esclusione.

e) che, senza giustificato motivo, si rifiuti od ometta di rendere disponibili tutti o parte dei propri dati, secondo le modalità concordate – all'atto di sottoscrizione della quota sociale – nell'accordo con cui si realizza il rapporto mutualistico, o non rilasci il consenso alla gestione e utilizzo degli stessi dati per le finalità dell'attività cooperativa;

f) che, in violazione degli accordi assunti, revochi anzitempo l'autorizzazione alla cooperativa per la gestione e l'utilizzo dei dati resi disponibili e non abbia presentato domanda di recesso;

g) che violi uno o più dei divieti di cui al precedente art. 9;

h) che svolga, o tenti di svolgere, attività in concorrenza o contraria agli interessi sociali;

i) che, con suoi atti, comportamenti o dichiarazioni, leda gravemente l'immagine e il buon nome della Cooperativa nonché l'onorabilità degli amministratori, dei soci e/o dei dipendenti della Cooperativa medesima o fomenti dissidi tra i soci;

j) che in qualunque modo arrechi danni alla Cooperativa;

k) che venga condannato con sentenza penale irrevocabile per reati non colposi contro la persona, il patrimonio o la pubblica amministrazione.

Prima di deliberare l'esclusione del socio cooperatore inadempiente, il Consiglio di Amministrazione dovrà contestare le inadempienze commesse al socio medesimo, assegnandogli un termine non inferiore a 5 (cinque) giorni per presentare giustificazioni verbali o scritte.

L'esclusione ha effetto con il ricevimento della comunicazione del relativo provvedimento.

Lo scioglimento del rapporto sociale per esclusione determina la risoluzione, con la stessa decorrenza, anche del rapporto mutualistico instaurato con il socio.

Contro la deliberazione di esclusione il socio può proporre opposizione innanzi al Collegio Arbitrale nel termine di sessanta giorni dal ricevimento della comunicazione.

Art. 13

Le deliberazioni prese in materia di recesso ed esclusione debbono essere comunicate ai soci cooperatori che ne sono oggetto mediante raccomandata con ricevuta di ritorno.

Le controversie che insorgessero tra i soci cooperatori e la Cooperativa in merito ai provvedimenti adottati dal Consiglio di Amministrazione su tali materie saranno demandate alla decisione del Collegio Arbitrale, regolato dagli artt. 43 e 44 del presente statuto.

I soci cooperatori, che intendessero reclamare contro i menzionati provvedimenti del Consiglio di Amministrazione, dovranno proporre la procedura arbitrale con atto comunicato alla Cooperativa, tramite raccomandata, a pena di decadenza, entro sessanta giorni dalla ricevuta comunicazione dei provvedimenti stessi.

Art. 14

I soci cooperatori receduti od esclusi hanno il diritto alla liquidazione della quota sociale effettivamente versata eventualmente aumentata per rivalutazione gratuita e/o per ristorno.

La liquidazione della partecipazione sociale avrà luogo sulla base del bilancio dell'esercizio, nel quale lo scioglimento del rapporto sociale fra la Cooperativa ed il socio cooperatore diventa operativo, eventualmente ridotta in proporzione alle perdite imputabili al capitale e, comunque, in misura mai superiore all'importo di cui al comma precedente.

La liquidazione della partecipazione sociale non comprende il rimborso del sovrapprezzo eventualmente versato [oppure: *... comprende anche il rimborso dell'eventuale sovrapprezzo versato, alle condizioni previste dall'art. 2535, secondo comma c.c.*].

Il pagamento deve essere effettuato entro 180 (centottanta) giorni dall'approvazione del bilancio, salvo il diritto di ritenzione spettante alla Cooperativa fino a concorrenza di ogni proprio eventuale credito liquido.

La frazione di capitale assegnata al socio cooperatore ai sensi dell'art. 2545-sexies c.c., unitamente agli interessi legali, può essere liquidata in più rate entro il termine di cinque anni.

Art. 15

In caso di morte del socio cooperatore, gli eredi hanno diritto alla liquidazione della quota sociale, nella misura e con le modalità previste dal precedente articolo, nonché al pagamento dei dividendi maturati, con riferimento all'esercizio nel corso del quale si sia verificata la morte. Cessa in ogni caso il rapporto mutualistico e, di conseguenza, ogni attività di gestione/utilizzo dei dati apportati dal socio defunto.

Art. 16

I soci cooperatori receduti od esclusi e gli eredi del socio cooperatore defunto dovranno richiedere per iscritto la liquidazione della quota sociale loro spettante entro cinque anni dalla data di approvazione del bilancio dell'esercizio nel quale lo scioglimento del rapporto sociale è divenuto operativo.

TITOLO IV
SOCI SOVVENTORI E SOTTOSCRITTORI DI TITOLI DI DEBITO

CAPO I
SOCI SOVVENTORI[6]

Art. 17

Qualora vengano costituiti dalla Cooperativa, con deliberazione dell'Assemblea, i fondi per lo sviluppo tecnologico o per la ristrutturazione od il potenziamento aziendale di cui all'art. 4 L. n. 59/92, al fine di agevolare il conseguimento degli scopi sociali e la realizzazione dell'oggetto, possono essere ammessi soci sovventori, sia persone fisiche che persone giuridiche, nei limiti previsti dalle leggi vigenti.

Chi intende diventare socio sovventore dovrà presentare al Consiglio di Amministrazione apposita domanda scritta contenente: nome, cognome, luogo e data di nascita, residenza, ovvero, qualora si tratti di persona giuridica, denominazione sociale e sede legale; numero delle azioni che intende sottoscrivere; impegno ad osservare il presente statuto e le deliberazioni legalmente adottate dagli organi sociali della Cooperativa; ogni altra ed eventuale indicazione stabilita dall'Assemblea che delibera l'emissione delle azioni di sovvenzione.

Sull'accettazione della domanda è competente a deliberare il Consiglio di Amministrazione, che provvede all'annotazione nel libro.

I soci sovventori sono obbligati: al versamento delle azioni sottoscritte con le modalità e nei termini previsti dal successivo art. 20; all'osservanza dello statuto e delle deliberazioni legalmente adottate dagli organi sociali.

Il socio sovventore ha il diritto di recedere dalla Cooperativa, oltre che nei casi previsti dall'art. 2437 c.c., in qualsiasi momento, dandone comunicazione scritta al Consiglio di Amministrazione, alla condizione che sia decorso il periodo minimo di durata del suo conferimento eventualmente stabilito dall'Assemblea che delibera l'emissione delle azioni di sovvenzione. In tal caso, il recesso avrà effetto negli stessi termini stabiliti per il recesso del socio cooperatore. Al socio sovventore receduto spetterà il rimborso delle azioni, da liquidarsi con le stesse modalità previste per la liquidazione della quota sociale del socio cooperatore, in misura comunque non superiore a quanto effettivamente versato per liberare le azioni sottoscritte, eventualmente aumentato per rivalutazione.

Le somme eventualmente versate a titolo di sovrapprezzo non sono comunque rimborsabili [oppure: *... sono rimborsabili, alle condizioni previste dall'art. 2535, secondo comma, c.c.*].

---

[6] Si può facoltativamente eliminare o mantenere. Se ne suggerisce il mantenimento.

Per quanto non espressamente previsto dal presente statuto, la disciplina delle azioni di sovvenzione è disposta, in conformità alla normativa vigente in materia, da apposito regolamento approvato dall'Assemblea dei soci, che potrà stabilire, tra l'altro: l'ammontare complessivo del fondo; l'eventuale periodo minimo di durata del rapporto sociale del socio sovventore; l'eventuale ed ulteriore contenuto della domanda di ammissione a socio sovventore; il valore nominale di ciascuna azione di sovvenzione e l'ammontare dell'eventuale sovrapprezzo; le modalità ed i termini di esecuzione dei conferimenti; i diritti patrimoniali e di voto, nonché i privilegi attribuiti alle azioni di sovvenzione; le eventuali condizioni che ne limitano la trasferibilità ed ogni altra caratteristica delle azioni medesime.

CAPO II
STRUMENTI FINANZIARI NON PARTECIPATIVI [7]

Art. 18

Con deliberazione dell'Assemblea straordinaria, la Cooperativa può emettere obbligazioni nonché strumenti finanziari di debito, diversi dalle obbligazioni, ai sensi degli artt. 2410 e seguenti, c.c.

In tal caso, con regolamento approvato dalla stessa Assemblea straordinaria, sono stabiliti:

– l'importo complessivo dell'emissione, il numero dei titoli emessi ed il relativo valore nominale unitario;

– le modalità di circolazione;

– i criteri di determinazione del rendimento e le modalità di corresponsione degli interessi;

– il termine di scadenza e le modalità di rimborso.

La deliberazione dell'Assemblea stabilisce altresì i compiti che vengono attribuiti al Consiglio di Amministrazione ai fini del collocamento dei titoli.

All'assemblea speciale degli obbligazionisti ed al relativo rappresentante comune si applica quanto previsto dalle norme di legge.

TITOLO V
PATRIMONIO SOCIALE

Art. 19

Il patrimonio sociale è costituito:

a) dal capitale sociale, che è variabile ed è formato:

a.1) dalle quote sociali, ciascuna del valore nominale non inferiore ad euro _____,00 (_____/00), sottoscritte dai soci cooperatori;

a.2) dalle azioni sottoscritte dai soci sovventori, destinate ai fondi per lo sviluppo tecnologico o per la ristrutturazione od il potenziamento aziendale, di cui all'art. 4 L. n. 59/92;

b) dal fondo di riserva legale;

c) da eventuali fondi di riserva straordinaria;

d) dall'eventuale fondo di riserva per sovrapprezzo;

e) da ogni altro fondo di riserva costituito o previsto per legge.

Sono ammessi conferimenti, oltre che di denaro, di beni in natura e di crediti, ai sensi degli articoli 2342-2343 c.c., da parte dei soci sia cooperatori che sovventori.

---

[7] Nel caso in cui si rinviasse al modello organizzativo della società a responsabilità limitata resta ferma la possibilità per la società cooperativa di offrire in sottoscrizione, esclusivamente ad investitori qualificati e ad investitori professionali soggetti a vigilanza prudenziale, strumenti finanziari partecipativi privi di diritti di amministrazione nonché titoli di debito, ai sensi degli artt. 2526, comma 4, 2483 c.c. e 111-*octies* delle norme di attuazione e transitorie.

Per le obbligazioni sociali risponde soltanto la Cooperativa con il suo patrimonio e, conseguentemente, i soci nei limiti delle quote sociali sottoscritte ed eventualmente aumentate per rivalutazione e/o per ristorno.

Le riserve comunque costituite non possono essere distribuite fra i soci [*ad eccezione di quella per sovrapprezzo, esclusivamente per il rimborso ai soci receduti ed esclusi di quanto da ciascuno di loro effettivamente versato a tale titolo al momento dell'ammissione, alle condizioni di cui all'art. 2535, comma 2, c.c.*].

Art. 20

Le quote dei soci cooperatori sono nominative.

Le quote s'intendono sottoscritte con la ricevuta comunicazione della delibera di ammissione e i relativi importi devono essere interamente versati dai soci cooperatori entro ____ (_____) giorni dalla sottoscrizione medesima.

Nessun socio cooperatore può avere una quota sociale, il cui valore nominale superi il limite massimo consentito dalla legge.

Le azioni sottoscritte dai soci sovventori sono nominative; il valore nominale, le modalità ed i termini di conferimento, l'ammontare dell'eventuale sovrapprezzo ed i privilegi nella ripartizione degli utili di tali azioni, saranno stabiliti dall'Assemblea al momento della loro emissione. In ogni caso, i versamenti sulle azioni di sovvenzione di cui al Titolo IV, da liberarsi in denaro, dovranno essere effettuati, per almeno il 25 % (venticinque per cento), all'atto della sottoscrizione e, per la parte restante, nei termini stabiliti dagli Amministratori.

La riduzione del capitale sociale della Cooperativa in conseguenza di perdite comporterà la riduzione del valore nominale delle azioni sottoscritte dai soci sovventori esclusivamente per la parte delle perdite stesse eccedente il valore nominale complessivo delle quote sottoscritte dai soci cooperatori.

Con riferimento agli strumenti finanziari di cui al Titolo IV, la Cooperativa avrà la facoltà di non emettere i relativi titoli, ai sensi dell'art. 2346, comma 1, c.c.

Art. 21

Le quote sottoscritte dai soci cooperatori non possono essere sottoposte a pegno o a vincoli e neppure essere cedute con effetto verso la Cooperativa senza la preventiva autorizzazione scritta del Consiglio di Amministrazione.

In ogni caso, la cessione della quota sociale non può essere parziale.

Il socio cooperatore che intende trasferire la propria quota deve darne comunicazione al Consiglio di Amministrazione mediante lettera raccomandata.

Il provvedimento che concede o nega l'autorizzazione deve essere comunicato al socio entro sessanta giorni dal ricevimento della richiesta; decorso tale termine, il socio è libero di trasferire la propria partecipazione e la Cooperativa deve iscrivere nel libro dei soci l'acquirente che abbia i requisiti per divenire socio cooperatore.

Il provvedimento che nega al socio cooperatore l'autorizzazione deve essere motivato; contro il diniego il socio, entro sessanta giorni dal ricevimento della comunicazione, può proporre opposizione al Collegio Arbitrale.

In caso di cessione della quota cessa, oltre al rapporto sociale, anche il rapporto mutualistico in essere tra socio e società. Colui che acquista la quota è tenuto a sottoscrivere l'accordo per instaurare il nuovo rapporto mutualistico nei termini e alle condizioni previste nel presente Statuto e nel Regolamento di cui all'art. 5-bis.

Art. 22

Le azioni di sovvenzione sono trasferibili per atto tra vivi; tuttavia, l'Assemblea potrà stabilire le condizioni, alle quali sarà subordinata eventualmente la loro trasferibilità, al momento dell'emissione.

TITOLO VI
GESTIONE SOCIALE – BILANCIO

Art. 23

L'esercizio sociale va dal 1° gennaio al 31 dicembre di ogni anno.

Alla fine di ogni esercizio sociale il Consiglio di Amministrazione provvede alla redazione del bilancio secondo le disposizioni di legge in materia e con criteri di prudenza.

Nel bilancio devono essere riportati separatamente i dati dell'attività svolta con i soci, distinguendo eventualmente le diverse gestioni mutualistiche.

Il Consiglio di Amministrazione ed il Collegio Sindacale, se nominato, documentano nella nota integrativa la condizione di prevalenza, ai sensi dell'art. 2513 c.c.

Il Consiglio di Amministrazione deve indicare, nella relazione di cui all'art. 2428 c.c., i criteri seguiti nella gestione sociale per il conseguimento degli scopi statutari in conformità con il carattere cooperativo della società; nella stessa relazione il Consiglio di Amministrazione deve altresì illustrare le ragioni delle determinazioni adottate con riguardo all'ammissione di nuovi soci.

Il bilancio deve essere presentato all'Assemblea per l'approvazione entro centoventi giorni dalla fine dell'esercizio sociale ovvero entro centottanta giorni, nel caso in cui la Cooperativa sia tenuta alla redazione del bilancio consolidato ovvero quando lo richiedano particolari esigenze relative alla struttura e all'oggetto della Cooperativa medesima; in caso di dilazione del termine, il Consiglio di Amministrazione ne segnala le ragioni nella relazione di cui all'art. 2428 c.c.

Art. 24

L'Assemblea, che approva il bilancio, può deliberare il riconoscimento ai soci cooperatori di somme da erogarsi a titolo di ristorno, ai sensi dell'art. 2545-*sexies* c.c. e del successivo art. 25.

Allo stesso modo la suddetta delibera assembleare può operare ratifica dello stanziamento delle somme di cui al precedente periodo effettuato dagli amministratori.

La stessa Assemblea delibera sulla distribuzione degli utili annuali, tenuto conto di quanto espressamente stabilito dal presente statuto e dall'eventuale regolamento interno destinandoli come segue:

a) non meno del 30% al fondo di riserva legale;

b) al fondo mutualistico per la promozione e lo sviluppo della cooperazione di cui all'art. 11 L. n. 59/92 e successive modificazioni, nella misura di legge;

c) all'eventuale aumento gratuito del capitale sottoscritto e versato nei limiti consentiti dalla legge in materia per il mantenimento dei requisiti mutualistici ai fini fiscali;

d) un dividendo ai soci cooperatori, in misura non superiore all'interesse massimo dei buoni postali fruttiferi, aumentato di due punti e mezzo rispetto al capitale effettivamente versato, qualora sussistano le condizioni di cui all'art. 2545-*quinquies*, secondo comma, c.c.;

e) un dividendo ai soci sovventori, previsti dal Capo I del Titolo IV, nella misura stabilita dal presente statuto ovvero dalla deliberazione assembleare di emissione, ma comunque in misura non superiore a due punti in più rispetto al limite massimo di cui alla precedente lettera d);

f) l'eventuale residuo a fondo di riserva straordinaria o ad altro fondo comunque costituito;

g) ad eventuale ripartizione dei ristorni nel rispetto dei limiti e delle modalità previste dal successivo art. 25.

In deroga a quanto sopra stabilito, l'Assemblea potrà deliberare di destinare tutti gli utili di esercizio al fondo di riserva legale, ad accezione di quelli da destinarsi conformemente alle disposizioni di legge per il mantenimento dei requisiti mutualistici ai fini fiscali.

Art. 25

La ripartizione di ristorni ai soci cooperatori avviene in proporzione alla quantità [*eventualmente in aggiunta od in alternativa*: *ed alla qualità*] degli scambi mutualistici effettivamente realizzati. Si tiene conto, a tal fine, del volume degli scambi mutualistici risultanti dal bilancio di

esercizio approvato, del valore della prestazione mutualistica offerta a ciascun socio cooperatore, e dell'eventuale vantaggio mutualistico attribuito al medesimo socio cooperatore contestualmente all'effettuazione dello scambio mutualistico.

In nessun caso l'ammontare del ristorno potrà essere superiore al valore della prestazione mutualistica usufruita dal socio cooperatore; in generale, l'ammontare complessivo dei ristorni non può eccedere il valore dell'avanzo di gestione che la cooperativa ha conseguito nell'esercizio dell'attività svolta con i soci cooperatori [8].

TITOLO VII
ORGANI SOCIALI

Art. 26

Sono Organi Sociali della Cooperativa:
A) l'Assemblea;
B) il Consiglio di Amministrazione;
C) il Collegio Sindacale, se nominato.

SEZIONE I
ASSEMBLEA

Art. 27

Le Assemblee sono ordinarie e straordinarie.

L'Assemblea è convocata dal Consiglio di Amministrazione mediante avviso contenente l'elenco delle materie da trattare e l'indicazione del luogo, della data e dell'ora della prima e della seconda convocazione, che non può aver luogo nello stesso giorno fissato per la prima.

L'avviso di convocazione dovrà essere, alternativamente:

A) comunicato ai soci, mediante lettera raccomandata, fax, posta elettronica, rispettivamente al domicilio risultante dal libro dei soci o al numero di fax o all'indirizzo di posta elettronica comunicati dai soci medesimi, o mediante altro mezzo che garantisca la prova dell'avvenuto ricevimento da parte dei soci medesimi, almeno otto giorni prima dell'Assemblea;

B) affisso presso la sede sociale ed i luoghi di lavoro, nonché comunicato ai soci mediante lettera semplice, almeno quindici giorni prima di quello fissato per l'Assemblea.

Il Consiglio di Amministrazione potrà, a sua discrezione ed in aggiunta a quelle previste dal comma precedente, usare qualunque altra forma di pubblicità diretta a meglio diffondere fra i soci l'avviso di convocazione delle Assemblee.

In mancanza dell'adempimento della suddetta formalità, l'Assemblea si reputa validamente costituita quando siano presenti o rappresentati tutti i soci con diritto di voto e partecipi la maggioranza degli amministratori e dei sindaci. Tuttavia, in tale ipotesi, ciascuno dei partecipanti può opporsi alla discussione degli argomenti, sui quali non si ritenga sufficientemente informato, e dovrà essere data tempestiva comunicazione delle deliberazioni assunte agli amministratori e sindaci non presenti.

In deroga all'art. 2363 c.c., l'Assemblea può essere convocata in luogo diverso dalla sede sociale, purché nel territorio ____(*regionale/nazionale*)___.

Nell'avviso di convocazione può inoltre essere prevista la possibilità di intervento a distanza mediante l'utilizzo di sistemi di collegamento audio/video, a condizione che siano rispettati il metodo collegiale ed i principi di buona fede e di parità di trattamento.

In particolare, è necessario che:

---

[8] Ritengo non in contrasto con il modello della cooperativa di dati la previsione dei ristorni. Si tratta però di scelta da operare caso per caso.

– sia consentito al presidente dell'assemblea, anche a mezzo del proprio ufficio di presidenza, di accertare l'identità e la legittimazione degli intervenuti, regolare lo svolgimento dell'adunanza, constatare e proclamare i risultati della votazione;

– sia consentito al soggetto verbalizzante di percepire adeguatamente gli eventi assembleari oggetto di verbalizzazione;

– sia consentito agli intervenuti di partecipare alla discussione e alla votazione simultanea sugli argomenti all'ordine del giorno;

– vengano indicati nell'avviso di convocazione i luoghi audio/video collegati a cura della società, nei quali gli intervenuti potranno affluire, dovendosi ritenere svolta la riunione nel luogo ove saranno presenti il presidente e il soggetto verbalizzante, fatta salva l'ipotesi nella quale l'Assemblea sia stata convocata prevedendo esclusivamente la partecipazione mediante mezzi di telecomunicazione, senza indicare un luogo fisico predeterminato di svolgimento della riunione. In tal caso non è necessaria la presenza di alcun soggetto in alcun determinato luogo ed il soggetto verbalizzante assiste alla riunione assembleare solo mediante mezzi di telecomunicazione e dà atto dell'intero procedimento decisionale sulla base di quanto percepito tramite gli stessi.

Al fine della determinazione dell'organo giudiziario competente a prendere cognizione delle eventuali azioni scaturenti dall'Assemblea, quando questa si sia tenuta esclusivamente virtuale, si considera la sede legale della società risultante dalla Camera di Commercio.

L'Assemblea ha luogo almeno una volta all'anno, entro i termini di cui al precedente art. 24.

L'Assemblea si riunisce inoltre quante volte il Consiglio di Amministrazione lo creda necessario o ne sia fatta richiesta per iscritto, con indicazione delle materie da trattare, dal Collegio Sindacale, se nominato, o da tanti soci che rappresentino almeno un decimo dei voti spettanti a tutti i soci; in questi ultimi casi, la convocazione deve avere luogo entro venti giorni dalla data della richiesta.

Art. 28

L'Assemblea Ordinaria:

1) approva il bilancio consuntivo con la relazione del Consiglio di Amministrazione;

2) delibera l'eventuale distribuzione di ristorni ai soci cooperatori;

3) provvede alla nomina degli amministratori, previa determinazione del loro numero e della durata del loro mandato, ed eventualmente del Presidente e del Vice Presidente del Consiglio di Amministrazione nonché alla loro revoca;

4) determina la misura dei compensi da corrispondersi agli amministratori per la loro attività collegiale;

5) provvede alla nomina, obbligatoria per legge o facoltativa, ed alla revoca del Collegio Sindacale, eleggendone il Presidente, e fissa i compensi spettanti ai sindaci;

6) conferisce, su proposta motivata del Collegio Sindacale, se nominato, e revoca, sentito lo stesso Collegio, l'incarico di revisione legale dei conti e determina il corrispettivo spettante al soggetto incaricato relativo all'intera durata dell'incarico;

7) delibera sulla responsabilità degli amministratori, dei sindaci e del soggetto incaricato della revisione legale dei conti;

8) approva tutti i regolamenti interni e, con le maggioranze previste per l'Assemblea straordinaria, quello sulla disciplina dei rapporti mutualistici; approva altresì un Codice di Condotta per la Gestione dei Dati;

9) delibera, su istanza dell'aspirante socio cooperatore, sul mancato accoglimento della domanda di ammissione di quest'ultimo da parte del Consiglio di Amministrazione;

10) delibera, secondo le previsioni dell'apposito regolamento interno, piani di crisi aziendale, stabilendo forme di apporto anche economico da parte dei soci cooperatori per la soluzione della crisi stessa, nonché l'eventuale distribuzione di somme a titolo di ristorni, ai sensi del precedente art. 24;

11) delibera sulla misura della partecipazione che dovrà essere sottoscritta dai nuovi soci cooperatori.

L'azione sociale di responsabilità contro gli amministratori, di cui al precedente punto n. 7, può essere esercitata anche dai soci aventi diritto ad almeno un terzo dei voti spettanti a tutti i soci.

L'Assemblea ordinaria delibera su ogni altra materia riservata alla sua competenza dalla legge e dal presente statuto nonché sottoposta alla sua preventiva autorizzazione dagli amministratori, ferma restando la responsabilità di questi per gli atti compiuti [9].

Art. 29

L'Assemblea, a norma di legge, è considerata straordinaria, quando si riunisce per deliberare sulle modificazioni dell'atto costitutivo, sulla proroga della durata e sullo scioglimento anticipato della Cooperativa, sulla nomina, sulla sostituzione e sui poteri dei liquidatori nonché su ogni altra materia espressamente attribuita dalla legge alla sua competenza, ad eccezione delle seguenti materie riservate dal presente statuto, ai sensi dell'art. 2365, secondo comma, c.c., alla competenza del Consiglio di Amministrazione: la fusione, nei casi previsti dagli articoli 2505 e 2505-bis c.c.; l'istituzione e la soppressione di sedi secondarie; l'indicazione di quali tra gli amministratori hanno la rappresentanza della società; gli adeguamenti dello statuto alle disposizioni normative; il trasferimento della sede sociale nel territorio nazionale [10].

Art. 30

In prima convocazione, l'assemblea, sia ordinaria che straordinaria, è regolarmente costituita quando siano presenti o rappresentati tanti soci che siano titolari della metà più uno dei voti spettanti a tutti i soci della Cooperativa aventi diritto al voto e delibera validamente con la maggioranza favorevole dei voti spettanti ai soci presenti e/o rappresentati.

In seconda convocazione, l'Assemblea ordinaria è regolarmente costituita qualunque sia il numero dei voti spettanti ai soci presenti o rappresentati e delibera validamente con la maggioranza favorevole dei voti spettanti ai soci presenti e/o rappresentati, mentre l'Assemblea straordinaria è regolarmente costituita quando siano presenti e/o rappresentati tanti soci che siano titolari di almeno ___ [es.: *un terzo*] ___ dei voti spettanti a tutti i soci della Cooperativa aventi diritto di voto e delibera validamente con la maggioranza favorevole dei voti spettanti ai soci presenti e/o rappresentati.

Qualora si tratti di deliberare sullo scioglimento e sulla liquidazione della Cooperativa, l'Assemblea straordinaria, sia in prima che in seconda convocazione è regolarmente costituita quando siano presenti o rappresentati tanti soci che siano titolari della metà più uno dei voti spettanti a tutti i soci aventi diritto al voto e delibera validamente con la maggioranza favorevole dei tre quinti dei voti spettanti ai soci presenti e/o rappresentati.

In deroga a quanto sopra, per la nomina delle cariche, risulteranno eletti amministratori e sindaci coloro che avranno ottenuto il maggior numero di voti di preferenza, fra quelli espressi dai soci presenti e/o rappresentati in Assemblea, secondo quanto precisato eventualmente in apposito regolamento interno.

Art. 31

Per le votazioni si procederà con il sistema dell'alzata di mano; esclusivamente per le elezioni delle cariche sociali si procederà, salvo diversa deliberazione dell'Assemblea, con il sistema della votazione a scrutinio segreto.

---

[9] Questa previsione potrebbe essere valorizzata per attribuire all'assemblea il potere di condizionare l'organo amministrativo nell'assunzione di decisioni che possano coinvolgere i diritti dei soci, tenendo però conto che la gestione spetta comunque in esclusiva all'organo gestorio. Il potere autorizzatorio dell'assemblea potrebbe però svolgere un ruolo importante nel rapporto fiduciario che lega amministratori e soci.

[10] Laddove si scelga il tipo di cooperativa a responsabilità limitata la distinzione tra assemblee ordinarie e straordinarie non è più contemplata nel codice civile. Si tratterà allora di indicare materie su cui deliberare con maggioranze rafforzate (come avviene per le assemblee straordinarie) e maggioranze ordinarie.

È in facoltà del Consiglio di Amministrazione ammettere, con l'avviso di convocazione dell'Assemblea, il voto per corrispondenza, ai sensi dell'art. 2538, ultimo comma, c.c. In tal caso, qualora fossero poste in votazione proposte diverse da quelle indicate nell'avviso di convocazione, i voti espressi per corrispondenza non si computeranno ai fini della regolare costituzione dell'Assemblea.

Art. 32

Nelle Assemblee hanno diritto al voto i soci cooperatori che risultino iscritti nel libro dei soci da almeno novanta giorni e che non siano in mora con i versamenti delle quote sottoscritte.

Ogni socio cooperatore ha diritto ad un solo voto, qualunque sia la partecipazione posseduta.

Hanno altresì diritto di voto i soci sovventori iscritti nell'apposito libro da almeno _____ giorni; essi possono avere diritto ciascuno a più voti, ma non oltre tre [11], in relazione all'ammontare dei loro conferimenti, secondo quanto meglio precisato dall'Assemblea al momento dell'emissione delle azioni. In ogni caso, ai soci sovventori non può essere attribuito complessivamente più di un terzo dei voti spettanti all'insieme dei soci presenti ovvero rappresentati in ciascuna Assemblea generale. Qualora, per qualunque motivo, si superi tale limite, i voti di tutti i soci sovventori saranno ricondotti automaticamente entro la misura consentita, applicando un coefficiente correttivo determinato dal rapporto tra il numero massimo dei voti ad essi attribuibili per legge e il numero di voti da essi portato.

Ai soci cooperatori non possono essere attribuiti voti in qualità di soci sovventori.

Ogni socio avente diritto di voto può farsi rappresentare nell'Assemblea da un altro socio appartenente alla stessa categoria, purché non amministratore né sindaco, che abbia diritto al voto, mediante delega scritta; ciascun socio delegato può rappresentare fino ad un massimo di ___ [*max: dieci*] ___ soci [12].

Le deleghe debbono essere conferite per iscritto, menzionate nel verbale dell'Assemblea e conservate fra gli atti sociali.

Le Associazioni di rappresentanza, assistenza e tutela del movimento cooperativo e gli organismi periferici delle medesime, cui la Cooperativa aderisce, potranno partecipare coi propri rappresentanti ai lavori dell'Assemblea, senza diritto di voto.

Art. 33

L'Assemblea, tanto in sede ordinaria che straordinaria, è presieduta dal Presidente del Consiglio di Amministrazione o, in caso di sua assenza o rinuncia, dal Vice Presidente; in caso di assenza di entrambi, essa sarà presieduta da un socio eletto dall'Assemblea stessa con il voto favorevole della maggioranza dei presenti e/o rappresentati.

Il Presidente dell'Assemblea verifica la regolarità della costituzione, accerta l'identità e la legittimazione dei presenti, regola il suo svolgimento ed accerta i risultati delle votazioni; degli esiti di tali accertamenti deve essere dato conto nel verbale.

L'Assemblea nomina, con la stessa maggioranza, un segretario, e, quando occorreranno, due scrutatori.

Le deliberazioni devono constare da verbale sottoscritto dal Presidente dell'Assemblea e dal Segretario.

---

[11] Ritengo che in relazione all'attività e ai fini delle cooperative di dati il peso dei soci sovventori debba essere minimo nell'ambito delle decisioni assembleari.

[12] Pare opportuno evidenziare che l'art. 2539 c.c. nulla dispone in merito alle deleghe attribuibili ad un singolo socio in assemblea nel caso la cooperativa adottasse il modello organizzativo delle società a responsabilità limitata. In tal caso si ritiene opportuno evidenziare la necessità di valutare attentamente, caso per caso, il numero di deleghe conferibili, tenuto conto che le coop a r.l. sono in genere formate da una base sociale ristretta e, conseguentemente, potrebbe concretizzarsi una concentrazione eccessiva di potere in capo al delegato/i tale da porre la scelta statutaria in contrasto con i principi generali cooperativi di partecipazione personale del socio e di democrazia.

Il verbale deve indicare la data dell'Assemblea e, anche in allegato, l'identità dei partecipanti; esso deve altresì indicare le modalità ed il risultato delle votazioni e deve consentire, anche per allegato, l'identificazione dei soci favorevoli, astenuti o dissenzienti. Nel verbale devono essere riassunte, su richiesta dei soci, le loro dichiarazioni pertinenti all'ordine del giorno.

Il verbale delle Assemblee in sede straordinaria deve essere redatto dal notaio.

I soci hanno diritto di esaminare il libro delle adunanze e delle deliberazioni dell'assemblea e di ottenerne estratti a proprie spese.

SEZIONE II
CONSIGLIO DI AMMINISTRAZIONE

Art. 34

Il Consiglio di Amministrazione si compone di un numero di consiglieri, variabile da un minimo di 3 fino ad un massimo di _____, eletti dall'Assemblea.

Gli amministratori possono essere scelti solamente tra i soci cooperatori o tra soggetti individuati e proposti dai soci cooperatori [13].

Gli amministratori restano in carica da uno a tre esercizi, secondo quanto stabilito di volta in volta dall'Assemblea, e scadono alla data dell'Assemblea convocata per l'approvazione del bilancio relativo all'ultimo esercizio della loro carica.

Essi sono rieleggibili.

Spetta al Consiglio di Amministrazione, sentito il parere del Collegio Sindacale, se nominato, determinare il compenso dovuto a quelli dei suoi membri, che siano investiti di particolari cariche in conformità del presente statuto.

Qualora non vi abbia provveduto l'Assemblea, il Consiglio elegge nel suo seno il Presidente ed il Vice Presidente.

Il Consiglio può delegare proprie attribuzioni ad uno o più amministratori, oppure ad un Comitato Esecutivo, determinando il contenuto, i limiti e le eventuali modalità di esercizio della delega conferita; tuttavia, non potranno essere oggetto di delega, oltre alle materie previste dall'art. 2381 C.C., i poteri in materia di ammissione, di recesso e di esclusione dei soci e le decisioni che incidono sui rapporti mutualistici con i soci.

Gli organi delegati dovranno riferire al Consiglio di Amministrazione ed al Collegio Sindacale, se nominato, almeno ogni ___ (*max: sei*) ___ mesi, sul generale andamento della gestione e sulla sua prevedibile evoluzione nonché sulle operazioni di maggior rilievo, per le loro dimensioni o caratteristiche, effettuate dalla Cooperativa e dalle sue controllate.

Gli amministratori sono tenuti ad agire in modo informato; ciascuno di essi può chiedere agli organi delegati che in Consiglio siano fornite informazioni relative alla gestione della società.

(…) [14].

Art. 35

Il Consiglio di Amministrazione è convocato dal Presidente tutte le volte in cui vi sia materia su cui deliberare, oppure quando ne sia fatta domanda scritta da un consigliere o dal Collegio Sindacale, se nominato, con indicazione delle materie da discutere.

---

[13] Possibile previsione: per essere eletti come amministratori i candidati devono possedere particolari requisiti di professionalità e onorabilità eventualmente da indicare con attenzione nello statuto. Si dovrebbe trattare di requisiti legati alle particolari attività poste in essere dalla cooperativa di dati.

[14] È possibile prevedere la presenza in consiglio di una percentuale (ad es. 1/3) di amministratori indipendenti, con funzioni di controllo e vigilanza sull'operato degli eventuali delegati e del consiglio nel suo insieme a garanzia della liceità, legalità, eticità e coerenza con le finalità statutarie della cooperativa dell'operato dell'organo gestorio.

La convocazione è fatta a mezzo di lettera da spedirsi non meno di cinque giorni prima dell'adunanza e, nei casi urgenti, anche tramite telegramma, fax o posta elettronica, in modo che i consiglieri ed i sindaci ne siano informati almeno un giorno prima della riunione.

Le adunanze sono valide quando vi intervenga la maggioranza degli amministratori in carica.

Le votazioni sono palesi.

Le deliberazioni sono validamente prese con il voto favorevole della maggioranza assoluta dei presenti; la parità di voti comporta la reiezione della proposta.

È ammessa, anche per il Consiglio di Amministrazione, la possibilità di intervento a distanza mediante l'utilizzo di sistemi di collegamento audio/video, a condizione che siano rispettati il metodo collegiale ed i principi di buona fede e di parità di trattamento.

In particolare, è necessario che:

sia consentito al presidente del Consiglio di Amministrazione di accertare l'identità e la legittimazione degli intervenuti, regolare lo svolgimento dell'adunanza, constatare e proclamare i risultati della votazione;

sia consentito al soggetto verbalizzante di percepire adeguatamente gli eventi gestori oggetto di verbalizzazione;

sia consentito agli intervenuti di partecipare alla discussione e alla votazione simultanea sugli argomenti all'ordine del giorno;

vengano indicati nell'avviso di convocazione i luoghi audio/video collegati a cura della società, nei quali gli intervenuti potranno affluire, dovendosi ritenere svolta la riunione nel luogo ove saranno presenti il presidente e il soggetto verbalizzante, fatta salva l'ipotesi nella quale il Consiglio di Amministrazione sia stato convocato prevedendo esclusivamente la partecipazione mediante mezzi di telecomunicazione, senza indicare un luogo fisico predeterminato di svolgimento della riunione. In tal caso non è necessaria la presenza di alcun soggetto in alcun determinato luogo ed il soggetto verbalizzante assiste alla riunione assembleare solo mediante mezzi di telecomunicazione e dà atto dell'intero procedimento decisionale sulla base di quanto percepito tramite gli stessi.

Al fine della determinazione dell'organo giudiziario competente a prendere cognizione delle eventuali azioni scaturenti dal Consiglio di Amministrazione, quando questo si sia tenuto esclusivamente virtuale, si considera la sede legale della società risultante dalla Camera di Commercio.

Ciascun amministratore deve dare notizia agli altri amministratori ed al Collegio Sindacale, se nominato, di ogni interesse che, per conto proprio o di terzi, abbia in una determinata operazione della Cooperativa, precisandone la natura, i termini, l'origine e la portata; se si tratta di amministratore delegato, deve altresì astenersi dal compiere l'operazione, investendo della stessa il Consiglio di Amministrazione. In tali casi, la deliberazione del Consiglio di Amministrazione deve adeguatamente motivare le ragioni e la convenienza per la Cooperativa dell'operazione.

Art. 36

Il Consiglio di Amministrazione è investito, in via esclusiva, di tutti i poteri per la gestione ordinaria e straordinaria della Cooperativa.

Esso ha il dovere di istituire un assetto organizzativo, amministrativo e contabile adeguato alla natura e alle dimensioni dell'impresa, anche in funzione della rilevazione tempestiva della crisi dell'impresa e della perdita della continuità aziendale, nonché di attivarsi senza indugio per l'adozione e l'attuazione di uno degli strumenti previsti dall'ordinamento per il superamento della crisi e il recupero della continuità aziendale.

In particolare il Consiglio di Amministrazione dovrà istituire una procedura di verifica e controllo del rischio tecnologico, adottando gli strumenti ed i meccanismi ritenuti idonei al fine di impedire il trasferimento di dati non personali o l'accesso a questi ultimi nel caso in cui ciò sia illegale, nonché adeguate procedure per prevenire pratiche fraudolente o abusive in relazione a soggetti che richiedono l'accesso tramite i suoi servizi.

Inoltre spetta al Consiglio di Amministrazione il compito di adottare le misure necessarie per garantire un adeguato livello di sicurezza per la conservazione, il trattamento e la trasmissione di dati non personali, nonché assicurare il massimo livello di sicurezza per la conservazione e la trasmissione di eventuali informazioni sensibili.

Compete al Consiglio di Amministrazione, fra l'altro e a titolo meramente esemplificativo:

A) curare l'esecuzione delle deliberazioni dell'Assemblea;

B) redigere il bilancio consuntivo e la relazione ad esso, conformemente alle norme di legge in materia ed a quanto previsto del presente statuto;

C) gestire il collocamento delle azioni di sovvenzione e degli altri strumenti finanziari affidato alla sua competenza dalla legge o dal presente statuto;

D) compilare i regolamenti interni;

E) stipulare tutti gli atti e contratti di ogni genere inerenti all'attività sociale;

F) deliberare e concedere avalli cambiari, fideiussioni ed ogni altra garanzia sotto qualsiasi forma per facilitare l'ottenimento del credito agli enti o società, cui la Cooperativa aderisce;

G) deliberare su tutte le altre materie, di cui all'art. 5, che non siano riservate all'Assemblea dei soci;

H) conferire procure, sia generali che speciali, ferma la facoltà attribuita al Presidente;

I) nominare un direttore, determinandone le funzioni e la retribuzione;

J) deliberare circa l'ammissione, il recesso e l'esclusione dei soci;

K) promuovere la costituzione di Consorzi o aderire a quelli promossi da altre cooperative, compilando od approvando i progetti di statuto relativi, determinando le quote di capitale da sottoscrivere e nominando i delegati;

L) deliberare e compiere tutti gli atti e tutte le operazioni di ordinaria e straordinaria amministrazione inerenti all'oggetto sociale, fatta eccezione soltanto di quelli, che, per disposizioni di legge o del presente statuto, siano riservati all'Assemblea generale.

Il Consiglio di Amministrazione, inoltre, sarà competente a deliberare sulle materie ad esso delegate dal precedente art. 29, ferma restando l'applicazione dell'art. 2436 c.c. («Deposito, iscrizione e pubblicazione delle modificazioni»).

Art. 37

In caso vengano a mancare uno o più amministratori, il Consiglio provvede a sostituirli nei modi previsti dall'art. 2386 c.c., scegliendo i nuovi amministratori fra i soci cooperatori [15].

Art. 38

I soci, che non siano in mora per la mancata esecuzione dei conferimenti o inadempienti rispetto alle obbligazioni contratte con la Cooperativa, quando almeno un decimo del numero complessivo lo richieda, hanno diritto ad esaminare, attraverso un rappresentante eventualmente assistito da un professionista di sua fiducia, il libro delle adunanze e delle deliberazioni del Consiglio di Amministrazione e il libro delle deliberazioni del comitato esecutivo, se esiste.

Art. 39

Il Presidente del Consiglio di Amministrazione ha la rappresentanza e la firma sociale.

Egli è perciò autorizzato a riscuotere, da pubbliche amministrazioni e da privati, pagamenti di ogni natura ed a qualsiasi titolo, rilasciandone liberatorie quietanze.

Egli ha anche facoltà di nominare avvocati e procuratori nelle liti attive e passive riguardanti la Cooperativa davanti a qualsiasi autorità giudiziaria od amministrativa ed in qualunque grado di giurisdizione.

Previa autorizzazione del Consiglio di Amministrazione, può delegare i propri poteri, in tutto

[15] In presenza di amministratori indipendenti è necessaria una previsione *ad hoc*.

o in parte, al Vice Presidente o ad un membro del Consiglio nonché, con speciale procura, a dipendenti della Cooperativa o a terzi.

Il Presidente convoca il Consiglio di Amministrazione, ne fissa l'ordine del giorno, ne coordina i lavori e provvede affinché adeguate informazioni sulle materie iscritte all'ordine del giorno vengano fornite a tutti i consiglieri.

In caso di assenza o di impedimento del Presidente, tutte le di lui mansioni spettano al Vice Presidente.

SEZIONE III
COLLEGIO SINDACALE E REVISIONE LEGALE DEI CONTI

Art. 40

La Cooperativa ha l'obbligo di nominare un Collegio Sindacale, mediante deliberazione dell'Assemblea, nei casi previsti dagli artt. 2543 e 2477 c.c. e successive modificazioni [16].

L'Assemblea avrà comunque la facoltà di provvedere alla nomina di un Collegio Sindacale anche al di fuori dei suddetti casi.

Qualora nominato, il Collegio Sindacale si compone di tre membri effettivi e di due supplenti tutti in possesso dei requisiti di legge; esso è regolarmente costituito con la presenza della maggioranza dei sindaci e delibera a maggioranza assoluta dei presenti. Il Presidente del Collegio è nominato dalla stessa Assemblea.

Le riunioni del collegio sindacale potranno essere tenute anche con il metodo della audio o videoconferenza a condizione che risulti garantita l'identificazione dei partecipanti e la possibilità degli stessi di intervenire attivamente nel dibattito e purché siano assicurati i diritti di partecipazione costituiti dalla scelta di un luogo di riunione, nel quale sarà presente almeno il presidente, dalla esatta identificazione delle persone legittimate a partecipare ai lavori, dalla possibilità di intervenire oralmente su tutti gli argomenti e di poter esaminare, ricevere e trasmettere documenti.

I Sindaci restano in carica per tre esercizi e scadono alla data dell'Assemblea convocata per l'approvazione del bilancio relativo al terzo esercizio della carica.

La cessazione dei Sindaci per scadenza del termine ha effetto dal momento in cui il Collegio è stato ricostituito.

Art. 41

Il Collegio Sindacale vigila sull'osservanza della legge e dello statuto, sul rispetto dei principi di corretta amministrazione ed in particolare sull'adeguatezza dell'assetto organizzativo, amministrativo e contabile adottato dalla società e sul suo concreto funzionamento.

Esso ha l'obbligo di verificare che l'organo amministrativo valuti costantemente, assumendo le conseguenti idonee iniziative, se l'assetto organizzativo dell'impresa è adeguato, se sussiste l'equilibrio economico finanziario e quale è il prevedibile andamento della gestione, nonché di segnalare immediatamente allo stesso organo amministrativo l'esistenza di fondati indizi della crisi.

I Sindaci devono assistere alle adunanze del Consiglio di Amministrazione, alle Assemblee e alle riunioni del Comitato Esecutivo.

In occasione della approvazione del bilancio di esercizio, i Sindaci devono indicare specificamente nella relazione prevista dall'art. 2429 c.c. i criteri seguiti nella gestione sociale per il perseguimento dello scopo mutualistico.

I Sindaci possono in ogni momento procedere, anche individualmente, ad atti di ispezione e

[16] Nelle cooperative che rinviano al modello organizzativo delle S.r.l. è possibile procedere, laddove ricorressero le condizioni di cui al combinato disposto degli agli artt. 2543 e 2477 c.c., alla nomina di un organo di controllo caratterizzato dalla presenza di un sindaco unico, che eserciti anche la revisione legale dei conti, o di un revisore.

controllo, oltre ad effettuare gli accertamenti periodici di legge. Di ogni ispezione, anche individuale, dovrà compilarsi verbale da inserirsi nell'apposito libro.

Il Collegio Sindacale può esercitare inoltre la revisione legale dei conti nei casi previsti dalla legge.

I Sindaci hanno ogni altro potere e dovere, nonché le responsabilità di cui alle norme di legge in materia.

Art. 42

La revisione legale dei conti è esercitata da un revisore legale o da una società di revisione legale iscritti nell'apposito registro.

L'Assemblea, su proposta motivata del Collegio Sindacale, se nominato, conferisce l'incarico di revisione legale dei conti della Cooperativa e determina il corrispettivo spettante al soggetto incaricato per l'intera durata dell'incarico e gli eventuali criteri per l'adeguamento di tale corrispettivo durante l'incarico.

L'incarico ha durata di tre esercizi, con scadenza alla data dell'assemblea convocata per l'approvazione del bilancio relativo al terzo esercizio dell'incarico.

Il revisore e la società di revisione, che effettuano la revisione legale dei conti della Cooperativa, devono essere indipendenti da questa e non devono essere in alcun modo coinvolti nel suo processo decisionale.

Il soggetto incaricato della revisione legale dei conti:

1) verifica, nel corso dell'esercizio, la regolare tenuta della contabilità sociale e la corretta rilevazione nelle scritture contabili dei fatti di gestione;

2) esprime con apposita relazione un giudizio sul bilancio di esercizio e sul bilancio consolidato, ove redatto.

Ricorrendo i presupposti di legge, l'Assemblea potrà affidare la revisione legale dei conti al Collegio Sindacale, che, in tal caso, dovrà essere interamente costituito da revisori legali iscritti nell'apposito registro.

TITOLO IX
CLAUSOLA COMPROMISSORIA

Art. 43

Le controversie derivanti dal presente statuto, comprese quelle insorte in materia di recesso, esclusione e tutte le altre relative all'interpretazione ed all'applicazione delle disposizioni statutarie, regolamentari o delle deliberazioni legalmente prese dagli organi sociali competenti, che dovessero insorgere tra la Cooperativa ed i soci o tra i soci stessi, aventi per oggetto diritti disponibili relativi al rapporto sociale, devono essere rimesse alla decisione di un Collegio Arbitrale.

La presente clausola compromissoria ha per oggetto anche le controversie promosse da amministratori, liquidatori e sindaci ovvero promosse nei loro confronti e, pertanto, è per essi vincolante, a seguito dell'accettazione dell'incarico.

Restano, in ogni caso, escluse dalla presente clausola compromissoria le controversie nelle quali sia obbligatorio per legge l'intervento del pubblico ministero.

Il ricorso al Collegio Arbitrale deve essere comunicato con lettera raccomandata entro il termine di decadenza di sessanta giorni dalla data dei provvedimenti che si intendono impugnare o dal momento dell'insorgere della controversia, con la precisazione dell'oggetto della controversia.

Art. 44

Il Collegio Arbitrale si compone di tre arbitri nominati a cura del Presidente della CCIAA di _____, che provvederà anche alla designazione del Presidente del Collegio.

Qualora il soggetto sopra designato non provvedesse, la nomina degli arbitri sarà effettuata, su istanza della parte più diligente, dal Presidente del Tribunale di _____.

L'arbitrato sarà rituale e gli arbitri decideranno secondo diritto.

Il collegio provvederà ad emettere la propria decisione nel termine di 90 (novanta) giorni dal ricevimento del ricorso, salvo proroga motivata da parte del collegio stesso per un periodo di ulteriori 30 (trenta) giorni.

Di tutte le riunioni del collegio dovrà essere redatto un processo verbale e la decisione, da adottarsi a maggioranza, dovrà essere motivata.

L'arbitrato avrà sede a _____.

TITOLO X
REQUISITI DELLE COOPERATIVE A MUTUALITÀ PREVALENTE

Art. 45

È fatto divieto di:

A) distribuire dividendi in misura superiore all'interesse massimo dei buoni postali fruttiferi, aumentato di due punti e mezzo rispetto al capitale effettivamente versato;

B) remunerare gli strumenti finanziari offerti in sottoscrizione ai soci cooperatori in misura superiore a due punti rispetto al limite massimo previsto per i dividendi;

C) distribuire le riserve fra i soci cooperatori.

Art. 46

In caso di scioglimento della Cooperativa, l'intero patrimonio sociale, dedotto soltanto il capitale sociale ed i dividendi eventualmente maturati, deve essere devoluto al fondo mutualistico per la promozione e lo sviluppo della cooperazione.

Al momento dello scioglimento, i soci della Cooperativa saranno privilegiati nel rimborso delle rispettive partecipazioni nel seguente ordine: soci sovventori; soci cooperatori.

Art. 47

Le clausole di cui agli artt. 45 e 46, primo comma non possono essere derogate e devono essere di fatto osservate.

TITOLO XI
SCIOGLIMENTO E LIQUIDAZIONE

Art. 48

L'Assemblea che dichiara lo scioglimento della Cooperativa nominerà uno o più liquidatori e ne stabilirà i poteri.

TITOLO XII
DISPOSIZIONI GENERALI

Art. 49

Per quanto non previsto dal presente statuto, si applicano le norme contenute nel Titolo VI del Libro V del Codice Civile, le leggi speciali in materia di società cooperative nonché, in quanto compatibili, le disposizioni sulle società per azioni.

Finito di stampare nel mese di dicembre 2024
nella LegoDigit s.r.l. – Via Galileo Galilei, 15/1
38015 Lavis (TN)

L'opera raccoglie i contributi del Progetto di Terza Missione dell'Università di Bologna sulle Cooperative di dati, disciplinate per la prima volta con il Data Governance Act (Reg. UE 2022/868) ed ivi inquadrate quali fornitori di servizi di intermediazione di dati. Il volume, in una prospettiva interdisciplinare, analizza tale nuovo *framework* giuridico, per giungere – attraverso l'interazione tra mondo accademico ed imprenditoriale – alla realizzazione di un modello fattibile, sostenibile ed efficiente di «cooperativa di dati», all'interno della cornice teorica del neomutualismo digitale. Il volume include anche un modello di statuto di cooperativa di dati.

This publication collects the contributions of the Third Mission Project of the University of Bologna on Data Cooperatives, which are, for the first time, regulated by the Data Governance Act (EU Reg. 2022/868) and framed therein as data intermediation services providers. From an interdisciplinary perspective, this volume analyses the aforementioned new legal regime, in order to achieve – through the interaction between academia and business – the development of a feasible, sustainable and efficient model of a 'data cooperative', within the theoretical framework of digital neo-mutualism. The volume also includes a model statute of a data cooperative.

FABIO BRAVO

Avvocato e Professore Ordinario di Diritto Privato all'Università di Bologna, ove è Direttore del Corso di Alta Formazione in Privacy e Data Protection Officer. Responsabile Scientifico del Progetto di Terza Missione dell'Università di Bologna sulle "Cooperative di dati".

Lawyer and Full Professor of Private Law at the University of Bologna, where he is Director of the Postgraduate Advanced Course in Privacy and Data Protection Officer. Principal Investigator of the Third Mission Project of the University of Bologna on 'Data Cooperatives'.

ISBN/EAN

9 791221 111460

€ 116,00