RIVISTA TRIMESTRALE DI DIRITTO DELL'ECONOMIA

RASSEGNA
DI
DOTTRINA
E
GIURISPRUDENZA

Supplemento al n. 1/2024

ISSN: 2036 - 4873

RIVISTA TRIMESTRALE
DI DIRITTO DELL'ECONOMIA

WWW.RTDE.LUISS.IT

La sede della Rivista è presso
la Fondazione G. Capriglione Onlus,
Università Luiss G. Carli,
Viale Romania 32, 00197 Roma.

Autorizzazione n. 136/2009, rilasciata dal Tribunale di Roma in data 10 aprile 2009.

COMITATO SCIENTIFICO

REGOLE DI AUTODISCIPLINA PER LA VALUTAZIONE DEI CONTRIBUTI

Al fine di assicurare uno standard elevato della qualità scientifica dei contributi pubblicati, nel rispetto dei principi di integrità della ricerca scientifica, la Rivista adotta un modello di revisione dei manoscritti proposti per la pubblicazione che contempla il referaggio tra pari a doppio cieco (double blind peer review). I contributi inviati alla Rivista sono oggetto di esame da parte di due valutatori individuati all'interno di un elenco, periodicamente aggiornato, di Professori ordinari, associati e ricercatori in materie giuridiche. L'assegnazione è effettuata dal Comitato di Direzione in accordo con il Direttore Responsabile tenendo conto delle aree di competenza di ciascun revisore e in assenza di conflitti di interessi con l'autore/l'autrice del contributo. Il contributo è trasmesso dal Comitato editoriale ai referees in forma anonima, unitamente ad una scheda di valutazione.

A seguito del referaggio, attraverso comunicazione telematica da parte del Comitato editoriale, l'Autore riceve la scheda contenente il parere anonimo reso dai valutatori. Se i valutatori si esprimono a favore della pubblicazione senza modifiche, il contributo è avviato alla pubblicazione. Se anche uno solo dei valutatori si esprime a favore della pubblicazione subordinandola a modifiche, i rilievi così formulati sono trasmessi all'Autore (sempre in forma anonima). Nel caso in cui l'Autore decida di uniformarvisi, egli trasmette il contributo modificato al Comitato editoriale che, su indicazione del Comitato di Direzione, può inoltrarlo di nuovo al valutatore oppure procedere direttamente alla pubblicazione. In caso di valutazione finale positiva, il contributo è avviato alla pubblicazione; in caso contrario, il Comitato di Direzione valuta se rifiutare il contributo o procedere a un'ulteriore fase di revisione. In ogni caso, in presenza di pareri dissenzienti tra i valutatori, il Comitato di direzione si assume la responsabilità di procedere alla pubblicazione, previo parere di un componente del Comitato scientifico scelto ratione materiae. Qualora entrambi i valutatori esprimano parere negativo alla pubblicazione, il contributo viene rifiutato a meno che il Direttore non ne autorizzi la pubblicazione se ritiene che esso soddisfi gli standard scientifici della Rivista. Per ogni ulteriore chiarimento si rinvia al Codice Etico pubblicato sul sito internet della Rivista.

TEMI E PROBLEMI

DI

DIRITTO DELL'ECONOMIA

Liber amicorum Laura Ammannati

A cura di Allegra Canepa e Gian Luca Greco*

* I curatori del *Liber Amicorum* ringraziano il Prof. Diego Rossano per la preziosa collaborazione prestata nella raccolta dei contributi e la Fondazione G. Capriglione onlus per aver ospitato la pubblicazione degli scritti nella prestigiosa 'Rivista Trimestrale di Diritto dell'Economia'.

INDICE

PARTE III. SERVIZI FINANZIARI TRA TRADIZIONE E INNOVAZIONE

MERCATO DIGITALE ED *EMPOWERMENT* DEL CONSUMATORE: VERSO LA NECESSITÀ DI UNA NUOVA INTERPRETAZIONE DEL CONSUMATORE 'MEDIO'. IMPLICAZIONI PER LA REGOLAMENTAZIONE DEL MERCATO INTERNO DELL'UNIONE EUROPEA*

(Digital market and consumer empowerment: towards a new interpretation of the 'average' consumer. Implications for the regulation of the internal market of the European Union)

ABSTRACT: *Il presente contributo rivisita il concetto di consumatore nell'ambito del diritto dell'UE alla luce del consolidamento e dell'espansione dei mercati digitali. Evidenzia l'inadeguatezza delle politiche di empowerment dei consumatori e il conseguente paradigma dell'informazione che ha dominato il diritto dei consumatori dell'UE. In particolare, l'articolo affronta i concetti giuridici di consumatore medio e vulnerabile che finora hanno permeato la regolamentazione dei mercati. Rileva che la nuova ondata di sforzi normativi per regolare i mercati digitali non si discosta dalla visione tradizionale della protezione dei consumatori. Al contrario, essi tendono a rafforzare ulteriormente i consumatori. È dunque necessaria una reinterpretazione della nozione di consumatore medio. In definitiva, questo contributo sostiene che nei mercati digitali una nuova e più ampia forma di vulnerabilità è la norma, e il consumatore medio è vulnerabile. Ciò implica che il legislatore dovrebbe affrontare le fonti di questa nuova vulnerabilità e cambiare radicalmente il modo in cui protegge i*

*Contributo approvato dai revisori.

Questa ricerca è stata condotta nell'ambito della Jean Monnet Chair in Digital Market Law (E-DSM), rif. E-DSM - 101047038 - GAP-101047038 e del Jean Monnet Network European Network on Digitalization and E-governance (ENDE), rif. ENDE - 101127038 - GAP-101127038. Il sostegno della Commissione europea alla ricerca non costituisce un'approvazione dei contenuti, che riflettono esclusivamente il punto di vista dell'autore. La Commissione non può essere ritenuta responsabile per l'uso che può essere fatto delle informazioni in essa contenute.

consumatori. In definitiva, l'articolo suggerisce che questa protezione dovrebbe avvenire attraverso disposizioni sostanziali ex ante che includano l'equità architettonica by default e by design.

This paper revisits the concept of the consumer under EU law in light of the consolidation and expansion of digital markets. It highlights the inadequacy of consumer empowerment policies and the ensuing information paradigm that has dominated under EU consumer law. In particular, it contrasts the legal concepts of both the average and the vulnerable consumer that so far have permeated the regulation of markets. It notes that the new wave of normative efforts to regulate digital markets does not depart from traditional views of consumer protection. On the contrary, they tend to empower consumers further. A reinterpretation of the notion of the average consumer is necessary. Eventually, this contribution puts forward that in digital markets a new broader form of vulnerability is the norm, and the average consumer is vulnerable. This implies that the legislator should tackle the sources of this new vulnerability and radically change the way it protects consumers. Ultimately, it suggests that this protection should occur by way of ex ante substantive provisions that include architectural fairness by default and by design.

1. Non è certo una novità che la creazione e il consolidamento del mercato unico digitale siano una dichiarata priorità per il legislatore europeo.[1]

[1] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale europeo e al Comitato delle regioni, Strategia per il mercato unico digitale in Europa,

Il percorso per realizzare la trasformazione digitale dell'UE entro il 2030 è volto a conseguire gli obiettivi del decennio nei settori delle competenze digitali, delle infrastrutture digitali e della digitalizzazione delle imprese e dei servizi pubblici.[2] Sorprendentemente, i consumatori non fanno parte direttamente e specificamente di questa ambiziosa agenda europea. Eppure, essi dovranno sempre più confrontarsi con questa nuova frontiera – se non addirittura diventarne dipendenti - man mano che i servizi si spostano sempre più verso il digitale e la vita privata e quella digitale divengono progressivamente intrecciate.

Allo stesso tempo, nella retorica e narrativa dell'Unione Europea la tecnologia dovrebbe dare più potere agli individui, mettendoli al centro dei mercati digitali come arbitri.[3]

Di pari passo, è da riconoscere come negli ultimi tempi il legislatore europeo sia stato particolarmente impegnato nell'attuazione di un programma di modernizzazione che, in una qualche misura, ha preso in considerazione la protezione dei consumatori, con la creazione di molteplici iniziative normative volte ad allineare le esigenze degli stessi alla spinta della digitalizzazione. Tra queste, il Regolamento sui mercati digitali (*Digital Markets Act -DMA*),[4] il Regolamento sui servizi digitali (*Digital Services Act -DSA*),[5] la proposta di Regolamento sull'intelligenza artificiale (*Artificial*

COM/2015/0192 final. Presidente della Commissione europea Ursula von der Leyen, A Union that strives for more - My agenda for Europe. Political guidelines for the next European Commission 2019-2024, 16 luglio 2019.

[2] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale europeo e al Comitato delle regioni, Bussola per il digitale 2030: il modello europeo per il decennio digitale, COM/2021/118 final; Commissione europea, Un percorso per il decennio digitale: governance comune e coordinamento degli investimenti per la trasformazione digitale dell'UE entro il 2030 (15 settembre 2021);

[3] Comunicazione della Commissione al Parlamento europeo e al Consiglio, Nuova agenda dei consumatori - Rafforzare la resilienza dei consumatori per una ripresa sostenibile, COM/2020/696 final.

[4] 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), GU L 265 del 12.10.2022, 1–66.

[5] 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), GU L 277 del 27.10.2022, 1–102.

Intelligence Act - AIA),[6] la proposta di Regolamento sull'accesso equo ai dati e sul loro utilizzo (*Data Act*)[7] - oltre a normative chiave per il dominio digitale quale il Regolamento sulla protezione dei dati personali (GDPR)[8] e a normative settoriali quali la revisione della direttiva sul credito al consumo[9] e la direttiva sui sistemi di pagamento (PSD2),[10] solo per nominarne alcune.

Affrontare le esigenze di specifici gruppi di consumatori, ivi inclusi alcuni aspetti della vulnerabilità degli stessi, è uno degli obiettivi più critici della Nuova Agenda dei Consumatori (*New Consumer Agenda*).[11] Ad esempio, si sottolineano in modo specifico le esigenze di consumatori sovra-indebitati, minori di età e disabili. Tuttavia, seppure apprezzabile negli intenti, il difetto principale di queste politiche e dei risultanti atti normativi è che rimangono permeati di vecchi concetti e paradigmi che già faticavano a proteggere i consumatori nel c.d. mondo analogico.

In una certa misura, a causa dell'asimmetria informativa, della differenza di potere negoziale e della relativa mancanza di trasparenza spesso insita nei rapporti di diritto privato tra i singoli consumatori e le imprese fornitrici di beni e servizi, nonché a causa del rischio sempre presente di cadere vittima di pratiche commerciali scorrette, tutti i consumatori possono essere considerati come parte 'debole' o

[6] 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.
[7] Proposta di Regolamento del Parlamento europeo e del Consiglio riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (normativa sui dati), COM/2022/68 final.
[8] 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), GU L 119 del 4.5.2016, 1–88.
[9] Direttiva (UE) 2023/2225 del Parlamento europeo e del Consiglio, del 18 ottobre 2023, relativa ai contratti di credito ai consumatori e che abroga la direttiva 2008/48/CE, GU L, 2023/2225, 30.10.2023.
[10] Direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE, GU L 337 del 23.12.2015, 35–127 – la cui revisione è al momento al vaglio della Commissione europea.
[11] Cit. nota 3.

'vulnerabile'.[12] Ciò è specialmente vero nel caso di mercati caratterizzati da transazioni particolarmente complesse, in cui i consumatori sono spesso poco preparati a prendere decisioni oculate. Esempi tradizionali sono rappresentati dal mercato finanziario e dal mercato dei servizi di interesse generale, non solo a causa di asimmetrie informative tra le parti o di un limitato livello educativo dei consumatori, ma anche a causa di complessità o altri fattori inerenti ai mercati che spingono gli individui verso scelte incoerenti con le proprie esigenze nel lungo termine.[13]

L'Unione Europea, pur riconoscendo le insidie di questi mercati problematici, sembra in gran parte non volersi discostare dal suo tradizionale e inflessibile standard di comportamento dei consumatori, basato sull'ideale del c.d. consumatore 'medio' come agente del mercato ragionevolmente ben informato e attento, al quale è sufficiente fornire adeguate informazioni per riequilibrare il rapporto commerciale con le imprese. Tuttavia, le carenze del paradigma informativo tradizionale diventano particolarmente evidenti nei casi in cui la quantità e la complessità delle informazioni disponibili, nonché la complessità dei prodotti e servizi stessi e sottostanti tecnologie, rendono paradossalmente più difficile per il consumatore non specializzato prendere decisioni informate.

Alla luce di questi problemi, il presente saggio si propone di contrastare questo standard di consumo del legislatore, specialmente alla luce delle complessità dei mercati digitali e sofisticazione delle sottostanti tecnologie.

2. Storicamente, il diritto dei consumatori si è sviluppato in continuità con l'economia neoclassica. Quest'ultima parte dalla premessa che gli individui cercano di

[12] In questa sede non è possibile dar conto in modo esaustivo della abbondante letteratura scientifica in merito. Sia consentito a titolo meramente esemplificativo rinviare all'autorevole ALPA, CATRICALA', *Diritto dei Consumatori*, Bologna, 2016; Fra i più recenti, PAGLIANTINI, *Il consumatore "frastagliato"*, Pisa, 2021; BARENGHI, *Diritto dei consumatori*, Milano, 2020.
[13] CORRIAS, *I soggetti vulnerabili nella disciplina comune e nei mercati regolamentati*, Napoli, 2022; CARTWRIGHT, *Understanding and Protecting Vulnerable Financial Consumers*, in 38(2) *Journal of Consumer Policy*, 2015, 119.

massimizzare l'utilità del consumo e sono in grado di compiere scelte oculate una volta ottenute tutte le informazioni rilevanti su un prodotto. Pertanto, l'utilizzo del modello economico neoclassico tradizionale implica la comprensione del consumatore come un *homo oeconomicus*, vale a dire un soggetto che agisce in modo sempre razionale, capace di prendere in considerazione tutte le informazioni disponibili, comprendendole appieno ed elaborandole, nonché in grado di soppesare tutte le opzioni a propria disposizione prima di giungere a una decisione perfettamente informata e logica. Questa visione, a sua volta, implica che i consumatori vengano considerati come agenti attivi arbitri dei mercati, poiché la capacità di ottimizzare le proprie scelte costringerebbe i mercati ad autoregolarsi.[14]

In questo quadro, il diritto dei consumatori si è evoluto sulla premessa che nel mercato esiste uno squilibrio tra consumatori e imprese, laddove sono soprattutto le asimmetrie informative a causare una sostanziale differenza nel potere contrattuale delle parti in grado di portare a un'importante inefficienza del mercato (*market failure*). Pertanto, a fronte di agenti economici contrattualmente deboli e in una condizione di intrinseca vulnerabilità, il diritto dei consumatori è stato concepito come mezzo per riequilibrare il mercato, proteggendo il contraente debole nel rapporto con le imprese.[15]

Nella narrativa economica neoclassica c'è sempre stata, e per molti versi c'è ancora, una forte convinzione che l'efficienza allocativa delle risorse debba essere lasciata al mercato più che alla regolamentazione,[16] anche in quelle giurisdizioni dove il diritto dei consumatori viene concepito nel contesto di un'attenzione di più ampio respiro sociale, come avviene ad esempio nella maggior parte dei paesi membri

[14] Per tutti, ALPA, CATRICALA', *Diritto dei Consumatori*, cit.; MICKLITZ, REICH, ROTT, TONNER, *European Consumer Law*, Cambridge, 2014; HOWELLS, WEATHERILL, *Consumer Protection Law*, Aldershot, 2005; WEATHERILL, *EU consumer law and policy*, Cheltenham, 2013; ZORZI GALGANO, *Il consumatore medio ed il consumatore vulnerabile nel diritto comunitario*, in *Contratto E Impresa Europa*, 2010, 442.
[15] Ibid.
[16] CSERES, *Competition Law and Consumer Protection*, The Hague, 2005, 178.

dell'Unione Europea.[17]

Pertanto, il diritto dei consumatori dell'UE si è rapidamente orientato verso l'utilizzo dell'informazione come strumento primario di regolamentazione. Più o meno fin dagli albori, si è riconosciuto che la concorrenza nei mercati può funzionare solo se i consumatori dispongono di tutte le informazioni necessarie per prendere decisioni economiche efficienti. Di conseguenza, i rimedi informativi offerti dalla regolamentazione sono diventati rapidamente una scorciatoia largamente adottata per la correzione dei mercati.[18] Tale tendenza e tecnica normativa si è protratta fino ai tempi recenti. Anzi, vale la pena notare come nel tempo l'interpretazione del paradigma dell'informazione da parte dell'UE si sia estesa e divenuta sempre più pervasiva, se non invasiva. Si veda, per esempio, come la direttiva sul credito al consumo[19] non solo abbia imposto ai creditori di fornire ai consumatori informazioni esaurienti, ma anche di renderle accessibili in forma standardizzata.[20] La direttiva sulle pratiche commerciali sleali[21] ha fatto un ulteriore passo avanti: la sua formulazione mostra un tentativo di conciliare i due obiettivi della libertà del mercato interno e di un'adeguata protezione dei consumatori, passando dall'approccio di armonizzazione minima delle direttive precedenti a quello di massima armonizzazione. Con questo approccio, il diritto europeo del consumatore diviene in grado di limitare la discrezionalità degli Stati Membri per quanto riguarda la possibilità di introdurre elementi di carattere sociale nella recezione delle norme sulla

[17] RUTGERS, *European Contract Law and the Welfare State*, Zutphen, 2012; DOMURATH, *Consumer Vulnerability and Welfare in Mortgage Contracts*, Oxford, 2017.
[18] SICILIANI, RIEFA, GAMPER, *Consumer Theories of Harm, an Economic Approach to Consumer Law Enforcement and Policy Making*, Oxford, 2019, 19.
[19] Cit. nota 9.
[20] DOMURATH., *The Case for Vulnerability as the Normative Standard in European Consumer Credit and Mortgage Law – An Inquiry into the Paradigms of Consumer Law*, in (2018) 2 *EuCML* (2018), 124.
[21] Direttiva 2005/29/CE del Parlamento europeo e del Consiglio, dell'11 maggio 2005, relativa alle pratiche commerciali sleali tra imprese e consumatori nel mercato interno e che modifica la direttiva 84/450/CEE del Consiglio e le direttive 97/7/CE, 98/27/CE e 2002/65/CE del Parlamento europeo e del Consiglio e il regolamento (CE) n. 2006/2004 del Parlamento europeo e del Consiglio («direttiva sulle pratiche commerciali sleali»), GU L 149 dell'11.6.2005, 22–39.

protezione dei consumatori, pur mantenendo il criticato elemento di responsabilizzazione degli stessi.[22]

D'altra parte, l'uso di uno standard elevato di consumatore sembra essere in linea con la considerazione che il regime di protezione dei consumatori dell'UE viene generalmente governato da considerazioni economiche e non sociali. Come scrive Norbert Reich, infatti, la protezione dei consumatori intesa come forma di protezione sociale è generalmente di competenza della legislazione nazionale degli Stati membri, non certo della UE.[23]

L'impostazione adottata dal legislatore europeo - e a cascata dai legislatori nazionali - è pertanto stata quella di obbligare i mercati a fornire il maggior numero di informazioni possibili, senza curarsi troppo dell'efficienza di tale strumento, nella convinzione che il consumatore 'razionale e responsabile' sarebbe stato in grado di fare il resto.

In una tale ottica, nel quadro del diritto europeo, l'informazione è stata elevata da 'metodo' a 'diritto' ed è considerata, a torto o a ragione, il più fondamentale diritto specifico del consumatore.[24]

Quando l'informazione è sovrana, al consumatore viene data la responsabilità di prestare attenzione, utilizzare gli strumenti messi a disposizione per difendersi dagli eccessi del mercato e valutare l'adeguatezza o meno dell'offerta alle proprie esigenze. Non sorprende, pertanto, che la posizione di default delle Corti di giustizia nell'UE sia stata, e continui a essere, quella per cui i consumatori siano dotati di elevate facoltà cognitive in grado di digerire le informazioni ad essi fornite. Parallelamente al paradigma dell'informazione, così, la giurisprudenza ha sviluppato

[22] REICH, *Vulnerable Consumers in EU Law*, in LECZYKIEWICZ e WEATHERILL, *The Images of the Consumer in EU Law: Legislation, Free Movement and Competition Law*, Oxford, 2018, 139.
[23] Ibid.
[24] Nella causa *GB- INNO- BM contro Confédération du Commerce Luxembourgeois* del 7 marzo 1990, ECLI: ECLI:EU:C:1990:102, la Corte di giustizia europea ha confermato come l'informazione ai consumatori sia 'sovrana'. In letteratura, STUYCK, *European consumer law after the Treaty of Amsterdam: Consumer policy in or beyond the internal market*' in 37 *Common Market Law Review*, 2000, 367.

la nozione di consumatore 'medio' come punto di riferimento. Nell'interpretare il termine giuridico 'consumatore' come "persona fisica che (…) agisce per fini che non rientrano nel quadro della sua attività professionale",[25] la Corte di giustizia ha dovuto determinare l'entità della protezione da accordare a chiunque rientri nell'ambito di applicazione del termine. In linea con casi precedenti in cui la questione si poneva in via incidentale,[26] la Corte ha costruito la sua decisione sulle aspettative di un 'consumatore medio ragionevolmente informato e ragionevolmente attento e avveduto'.[27]

La giurisprudenza della Corte di giustizia europea ha continuato a utilizzare la formula *Gut Springenheide* per interpretare il comportamento del consumatore medio stabilendo un chiaro precedente giuridico,[28] peraltro introdotto anche nella legislazione europea in materia di tutela dei consumatori con la direttiva sulle pratiche commerciali sleali,[29] la quale nell'articolo 2 fa esplicito riferimento al

[25] Definito per esempio dalla Direttiva 93/13/CEE del Consiglio, del 5 aprile 1993, concernente le clausole abusive nei contratti stipulati con i consumatori GU L 95 del 21.4.1993, 29–34 e dalla Direttiva 2008/48/CE del Parlamento europeo e del Consiglio, del 23 aprile 2008, relativa ai contratti di credito ai consumatori e che abroga la direttiva 87/102/CEE, GU L 133 del 22.5.2008, 66–92.
[26] Si vedano, ad esempio, le cause C-238/89 *Pall Corp. contro P.J. Dahlhausen & Co.* del 13 dicembre 1990, ECLI:EU:C:1990:473; C-126/91 *Schutzverband gegen Unwesen in der Wirtschaft e.V. contro Yves Rocher GmbH* del 18 maggio 1993 ECLI:EU:C:1993:191; C-315/92 *Verband Sozialer Wettbewerb eV contro Clinique Laboratoires SNC e Estée Lauder Cosmetics GmbH* del 2 febbraio 1994, ECLI:EU:C:1994:34; C-456/93 *Zentrale zur Bekämpfung unlauteren Wettbewerbs eV contro Privatkellerei Franz Wilhelm Langguth Erben GmbH & Co. KG* del 25 giugno 1995, ECLI:EU:C:1995:206. Di particolare interesse è la causa C-470/93 *Verein gegen Unwesen in Handel und Gewerbe Köln eV contro Mars GmbH* del 6 luglio 1995, ECLI:EU:C:1995:224, in quanto segna il primo riferimento esplicito alla categoria dei "consumatori ragionevolmente avveduti".
[27] Causa C-210/96 *Gut Springenheide GmbH e Rudolf Tusky contro Oberkreisdirektor des Kreises Steinfurt - Amt für Lebensmittelüberwachung* del 16 luglio 1998, ECLI:EU:C:1998:369.
[28] Si vedano, per esempio, le cause C-342/97 *Lloyd Schuhfabrik Meyer & Co. GmbH contro Klijsen Handel BV* del 22 giugno 1999, ECLI:EU:C:1999:323; C-465/98 *Verein gegen Unwesen in Handel und Gewerbe Köln eV contro Adolf Darbo AG* del 4 aprile 2000, ECLI:EU:C:2000:184; C-239/02 *Douwe Egberts NV v Westrom Pharma NV and Christophe Souranis, carrying on business under the commerical name of "Etablissements FICS' and Douwe Egberts NV contro FICS-World BVBA* del 15 luglio 2004, ECLI:EU:C:2004:445. In letteratura, si vedano in particolare DE GIULI, *Sul concetto di "vulnerabilità" secondo la Corte di Giustizia UE*, in *Diritto Penale e Uomo*, 2020, 1; PONCIBO', *Il consumatore medio*, in *Contratto Impresa Europa*, 2007, 756-757; INCARDONA, PONCIBO', *The average consumer, the unfair commercial practices directive and the cognitive revolution* in 30 *Journal of Consumer Policy*, 2007, 21.
[29] Cit. nota 21.

comportamento economico del consumatore medio di un determinato prodotto nella definizione di 'pratica commerciale sleale'.[30]

L'assunto, pertanto, diventa che il consumatore medio non possa essere facilmente ingannato, stabilendosi uno standard elevato che pone l'accento sull'responsabilizzazione, autosufficienza e trasferimento di potere al consumatore agente economico attivo (*consumer empowerment*).

Un tale standard di consumatore è stato già ampiamente criticato dal mondo accademico come irrealisticamente esigente, eccessivamente semplificato e, più in generale, come una finzione giuridica lontana dal comportamento effettivo del singolo consumatore, sia in termini di informazione che di ragionevolezza.[31]

L'idea dell'*empowerment* del consumatore come 'Sacro Graal' della strategia dell'UE, spesso combinata con politiche di deregolamentazione del mercato, diviene di difficile accettazione se rapportata al sovraccarico di informazioni, alla crescente complessità (a volte artificiale) dei mercati e alle modalità eccessivamente (spesso artificialmente) complesse con cui vengono fornite le informazioni essenziali. In un tale contesto di mercato, nella realtà i consumatori finiscono spesso per essere esautorati, agendo così in modo meno informato e meno avveduto, in netto

[30] Si noti altresì come il Considerando 18 del preambolo chiarisca che la direttiva "prende come riferimento il consumatore medio, ragionevolmente informato e ragionevolmente attento e avveduto, tenendo conto dei fattori sociali, culturali e linguistici, secondo l'interpretazione della Corte di giustizia".

[31] Si veda, senza pretesa di completezza, HOWELLS, *The potential and limits of consumer empowerment by information*, in *Journal of law and Society*, 2005, 349; BEN SAHAR, SCHNEIDER, *More than you wanted to know – the failure of mandated disclosure*, Princeton, 2016; RABITTI, *Il consumatore vulnerabile e la fragilità del diritto. Brevi considerazioni*, in *Dialoghi di Diritto dell'Economia*, 2023; PAGLIANTINI, *Il consumatore "frastagliato"*, cit.; MICKLITZ, *The consumer: marketised, fragmentised, constitutionalised*, in LECZYKIEWICZ, WEATHERILL, *The Images of the Consumer in EU Law: Legislation, Free Movement and Competition Law*, Oxford, 2018, 21; MEZZASOMA, *Consumatore e Costituzione*, in *Rass. Dir. Civ.*, 2015, 311; NATOLI, *L'abuso di dipendenza economica. Il contratto e il mercato*, Napoli, 2004; PERLINGERI, *Il diritto privato europeo tra riduzionismo economico e dignità della persona*, in *Eur. dir. priv.*, 2010, 345-360; CORRIAS, *I soggetti vulnerabili nella disciplina comune e nei mercati regolamentati*, cit.; RUBINO, *L'evoluzione della nozione di "consumatore" fra tutela dei diritti della persona, economia collaborativa e futuro del mercato interno dell'Unione Europea*, in AA.VV. *Dialoghi con Ugo Villani*, Bari, 2017, 363; GENTILI, *La nullità di protezione*, in *Eur. Dir. priv.*, 2011, 79.

contrasto con gli obiettivi stessi dall'UE.[32] Non ci si può certo aspettare che un consumatore reale sia sempre in grado di comprendere e/o disposto a valutare in modo approfondito la quantità di informazioni a sua disposizione prima di prendere una decisione di consumo; né ci si può aspettare che compia scelte perfettamente razionali, non offuscate da emozioni e influenze sociali di vario tipo.[33]

All'opposto, in questa sede si sostiene perfino che per i consumatori sia razionale essere passivi o disimpegnati, un meccanismo attraverso il quale essi diventano vulnerabili o che amplifica una vulnerabilità già esistente. In questo senso, peraltro, si può arguire che i settori di mercato più problematici siano proprio i settori più essenziali per il benessere dei consumatori, tra cui alcuni servizi di interesse generale come l'energia e le telecomunicazioni, nonché il settore dei servizi finanziari, spesso tacciato di essere caratterizzato da un'inutile complessità dei prodotti, mancanza di trasparenza all'interno delle imprese e mancanza di fiducia nelle imprese stesse, cattiva o insufficiente consulenza e/o commissioni nascoste per gli intermediari con conseguenti vendite inadatte di prodotti, o costi e rischi elevati rispetto ai ricavi degli investimenti.[34]

Come si vedrà oltre, lo stesso dicasi per un mercato digitale che permea sempre più in modo essenziale la società contemporanea.

3. Il benchmark del consumatore 'medio' può essere utilizzato per prendere in

[32] Cfr. BEUC, *EU Consumers' 2020 Vision* (2012) https://www.beuc.eu/publications/2012-00316-01-e.pdf.
[33] INCARDONA, PONCIBO', *The average consumer, the unfair commercial practices directive and the cognitive revolution*, cit.
[34] BERTI DE MARINIS, *La tutela del cliente vulnerabile*, in *Banca borsa titoli di credito*, 2018, 651; CARTWRIGHT, *Banks, Consumers and Regulation*, Oxford, 2004; CARTWRIGHT, *Understanding and Protecting Vulnerable Financial Consumers*, cit.; JOHNSTON, *Seeking the EU 'Consumer' in Services of General Economic Interest* in LECZYKIEWICZ, WEATHERILL, *The Images of the Consumer in EU Law: Legislation, Free Movement and Competition Law*, Oxford, 2018, 93; MICKLITZ, DOMURATH, Consumer debt and social exclusion in Europe, Farnham, 2015; MICKLITZ, *Access to, and exclusion of, European consumers from financial markets after the global financial crisis*, in WILSON, *International responses to issues of credit and over-indebtedness in the wake of the crisis*, Farnham ; 2013, 47.

esame i concetti di 'debolezza del consumatore' e 'vulnerabilità'. Questo in quanto la nozione di consumatore 'vulnerabile' è stata sviluppata per distinguere il consumatore meno abile rispetto ai suoi pari c.d. 'medi'.

Il concetto di vulnerabilità è problematico, in primo luogo perché non in linea con gli obiettivi economici originari del diritto dei consumatori sopra esaminati. In secondo luogo, la difficoltà concettuale, e giuridica, derivano dalla stigmatizzazione di alcuni consumatori nei confronti di altri. Attraverso questa lente, i consumatori vulnerabili sono visti come consumatori di rango inferiore, non capaci come le controparti 'medie'. Così, il concetto di 'vulnerabilità' viene classificato come 'inferiorità rispetto alla media', non da ultimo nella direttiva sulle pratiche commerciali sleali, dove i consumatori vulnerabili vengono presentati come di rango inferiore rispetto alla media per via della loro infermità mentale o fisica, età o credulità.[35]

Un più ampio concetto di 'vulnerabilità' è per molti versi legato all'influenza dell'economia comportamentale (*behavioural economics*), la disciplina che incorpora lo studio della psicologia nell'analisi economica per riconoscere i limiti che i consumatori hanno nel valutare le informazioni e nel compiere scelte razionali. Riconoscendo che in realtà i consumatori non prendono spesso decisioni razionali o logiche, e che le imprese possono sfruttarne i pregiudizi comportamentali per indirizzare a proprio vantaggio il comportamento dei consumatori, l'economia comportamentale cerca di comprendere come tali meccanismi si sviluppino e se ne possano superare i pregiudizi.[36]

---

[35] Cfr. Articolo 5(3) della direttiva sulle pratiche commerciali sleali, cit. Nella dottrina italiana, per tutti si vedano i contributi in CORRIAS, PIRAS, *I soggetti vulnerabili nell'economia, nel diritto e nelle istituzioni*, Napoli, 2021.

[36] Questa disciplina è stata introdotta da KHANEMAN, TVERSKY, *Prospect theory: An analysis of decision under risk*, in 47 *Econometrica*, 1979, 263. KHANEMAN, TVERSKY, *Loss aversion in riskless choice: A reference dependent model*, in 106 *Quarterly Journal of Economics*, 1991, 1039; KHANEMAN, TVERSKY, *Judgment under uncertainty: Heuristics and biases*, in 185 *Science*, 1974, 1124. Tale disciplina é stata ulteriormente sviluppata da THALER e SUNSTEIN, *Nudge: Improving Decisions about Health, Wealth, and Happiness*, New Haven, 2008, i quali hanno portato aspetti

Così, la dottrina è andata oltre alla valutazione delle caratteristiche strettamente personali (età, genere, localizzazione geografica, istruzione e lingua) per prendere in considerazione una gamma sempre più ampia di fattori socio-economici, oltre a osservare come elementi esterni possano creare, influenzare o rafforzare le vulnerabilità. Precursore di questo mutamento dottrinale lo si deve al lavoro di David Caplovitz, che già negli anni sessanta ha evidenziato la situazione di fattiva vulnerabilità dei consumatori a basso reddito.[37] Più recentemente, Martha Fineman ha sviluppato una teoria della vulnerabilità che serve sempre più come punto di riferimento per lo studio del diritto dei consumatori.[38] Fineman concepisce la vulnerabilità come un'esperienza universale e sempre presente, che può emergere in qualsiasi momento per via di circostanze individuali o da quella che l'autore definisce *embeddedness* (cioè il rapporto o l'integrazione di un individuo con le istituzioni, la società e la cultura che lo circondano). L'approccio di Fineman si concentra così sulla struttura della società e adotta una visione più sostanziale del concetto di uguaglianza. Tale teoria è utile in un contesto consumeristico perché elimina la necessità di categorizzare gli individui e, nel caso dei consumatori, evita di stigmatizzare i consumatori vulnerabili, troppo spesso percepiti come coloro che non possono, o non possono più, far fronte alle esigenze della moderna società dei consumi.[39]

Riflettendo sul diritto europeo, si sarebbe potuto pensare che il lavoro della Commissione europea potesse mostrare un'apertura normativa verso le più recenti teorie comportamentali e il riconoscimento dei consumatori vulnerabili. Il Rapporto

---

dell'economia comportamentale, come la teoria dei *nudge*, nelle politiche legislative dominanti. La teoria dei *nudge* sostiene che i processi decisionali e i comportamenti possono essere influenzati attraverso suggerimenti e rinforzi indiretti con un'efficacia pari o superiore a quella che può essere ottenuta attraverso l'imposizione di regole, leggi o istruzioni dirette.

[37] CAPLOVITZ, *The Poor pay more*, New York, 1967.

[38] FINEMAN, *The Vulnerable Subject: Anchoring Equality in the Human Condition*, in 20 *Yale Journal of Law and Feminism*, 2008, 1; FINEMAN, *Vulnerability and Inevitable Inequality*, in 4 *Oslo Law Review*, 2017, 133.

[39] Ibid.

sulla vulnerabilità dei consumatori nei mercati chiave dell'unione europea ha infatti proposto l'adozione di una definizione più esaustiva di consumatore vulnerabile, sottolineando come le caratteristiche socio-demografiche, le caratteristiche comportamentali, la situazione personale o l'ambiente di mercato possano avere un effetto decisivo sul consumo. La Commissione evidenzia come a causa di una combinazione di questi fattori, i consumatori siano più a rischio di subire esiti negativi sul mercato, abbiano una capacità limitata nel massimizzare il proprio benessere, abbiano difficoltà a ottenere o assimilare informazioni, siano meno in grado di scegliere o accedere a prodotti adeguati, o siano più suscettibili a subire determinate pratiche di marketing.[40]

Questo modesto spiraglio non trova tuttavia eco nel diritto dell'UE e, a cascata, nel diritto nazionale degli Stati Membri, dove permane una concettualizzazione limitata della vulnerabilità dei consumatori.

Vale comunque la pena ricordare che, nonostante la maggior parte della giurisprudenza della Corte di giustizia europea continui a perseguire fedelmente il paradigma dell'informazione al consumatore medio,[41] in rari casi la Corte stessa ha adottato un approccio più protettivo.[42] Tale orientamento ha tuttavia avuto una portata molto limitata, applicabile solo in contesti specifici, rimanendo un'eccezione alla regola generale dell'interpretazione del consumatore come ragionevolmente avveduto, applicabile solo nei casi in cui la Corte ha esaminato la legislazione

[40] Commissione Europea, *Consumer vulnerability across key markets in the European Union* (Gennaio 2016), https://op.europa.eu/en/publication-detail/-/publication/79b42553-de14-11e6-ad7c-01aa75ed71a1

[41] Da ultimo, si vedano le cause C-139/22 *AM and PM contro mBank S.A.* del 21 settembre 2023, ECLI:EU:C:2023:692; C-265/22 *ZR e PI contro Banco Santander, SA.* del 13 luglio 2023, ECLI:EU:C:2023:578.

[42] La prima e più significativa di queste decisioni è stata la sentenza della Corte nella causa C-382/87 *R. Buet e Educational Business Services (EBS) SARL contro Pubblico Ministero* del 16 maggio 1989, ECLI:EU:C:1989:198, dove ha ritenuto che un regolamento francese che vietava la vendita porta a porta di materiale didattico non costituisse una restrizione sproporzionata alle disposizioni del Trattato UE sulla libera circolazione delle merci, dato che il potenziale acquirente solitamente appartiene a una categoria di persone che, per un motivo o per l'altro, sono poco istruite e cercano di colmare una tale mancanza, rendendoli particolarmente vulnerabili di fronte ai venditori di materiale didattico.

nazionale che fornisce una protezione aggiuntiva a un gruppo ristretto e specifico di consumatori.[43]

Tuttavia, con la più recente legislazione dell'UE in materia di tutela dei consumatori che propende per un approccio di armonizzazione totale - sia in generale che nel contesto specifico delle vendite fuori dai locali commerciali - è dubbio che si possano verificare eccezioni nazionali che possano portare al medesimo risultato.33

4. Procedendo con una disamina verso il mercato digitale, occorre sin da subito rilevare come la percezione del consumatore non sia cambiata.
Al contrario, le politiche e la regolamentazione UE puntano sempre più sul c.d. *empowerment* dei consumatori, rafforzandone il ruolo e mirando a garantire loro modalità più immediate per ottenere informazioni, confrontare prodotti e condividere esperienze, oltre che ad avere il controllo sui propri dati.

È interessante rimarcare come la Nuova Agenda dei Consumatori osservi come questi ultimi siano la parte più debole di una transazione e che necessitino di protezione per la salute, sicurezza e interessi economici. Si sottolinea che alcuni gruppi possono essere particolarmente vulnerabili, per cause legate alla situazione sociale o a particolari caratteristiche (età, genere, salute, alfabetizzazione digitale, capacità di calcolo o situazione finanziaria, mancanza di accessibilità).[44]

Tuttavia, una rapida carrellata della regolamentazione in essere, o prospettata, dal legislatore europeo evidenzia una mancanza di discostamento dalla visione del consumatore medio tradizionalmente inteso, all'opposto rinforzandone la responsabilizzazione in talune fattispecie nell'aspirare a porre i consumatori al centro

[43] Un ridotto numero di decisioni successive presentano argomentazioni simili. Si veda, per esempio, la causa C-441/04 *A-Punkt Schmuckhandel contro Claudia Schmidt* del 23 febbraio 2006, ECLI:EU:C:2006:141.
[44] Nuova Agenda dei Consumatori, cit. nota 3.

del progetto digitale e in pieno controllo dei propri dati.[45]

Il *DMA*, considerata un'iniziativa a tutela dei consumatori, cerca di promuovere la concorrenza nei mercati digitali tenendo sotto controllo le grandi piattaforme online e imponendo obblighi per favorire la libera scelta, ad esempio attraverso la portabilità.[46] Tuttavia, la normativa non menziona affatto situazioni di vulnerabilità.

Allo stesso modo, il *DSA*, incentrato sulla protezione dei consumatori, cerca di garantire fiducia nell'economia digitale con una sezione dettagliata sui mercati online e norme ritenute complementari all'*acquis* in materia di protezione dei consumatori[47] - in particolare la direttiva (UE) 2019/2161 che stabilisce norme specifiche per aumentare la trasparenza di alcune caratteristiche offerte da determinati servizi della società dell'informazione.[48] Tuttavia, nel *DSA* la vulnerabilità dei consumatori viene appena menzionata. Nelle rare occasioni in cui questo avviene, la concettualizzazione della vulnerabilità è ancora molto limitata. In piena continuità con il passato, il *DSA* si concentra sul genere, razza o origine etnica, religione o convinzioni personali, disabilità, età o orientamento sessuale come fattori che rendono gruppi o persone vulnerabili o svantaggiate nell'uso dei servizi digitali. La visione della vulnerabilità rimane ancora molto ancorata a fattori personali, così come avviene nel caso della

[45] Si veda, ad esempio, la strategia UE sull'Open Finance, con dichiarata intenzione del legislatore di porre i consumatori al centro del progetto, conferendo loro pieno controllo sui propri dati, consapevolezza sul relativo utilizzo e protezione da usi impropri. Cfr. Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni relativa a una strategia in materia di finanza digitale per l'UE, COM/2020/591 final; Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni relativa a una strategia in materia di pagamenti al dettaglio per l'UE, COM/2020/592 final; Commissione europea, Targeted consultation on open finance framework and data sharing in the financial sector, https://finance.ec.europa .eu/regulation-and-supervision/consultations/finance-2022-open-finance_en.

[46] Cit. nota 4.

[47] Cit. nota 5.

[48] Direttiva (UE) 2019/2161 del Parlamento europeo e del Consiglio del 27 novembre 2019 che modifica la direttiva 93/13/CEE del Consiglio e le direttive 98/6/CE, 2005/29/CE e 2011/83/UE del Parlamento europeo e del Consiglio per una migliore applicazione e una modernizzazione delle norme dell'Unione relative alla protezione dei consumatori, GU L 328 del 18.12.2019, 7–28.

normativa in materia di protezione dei dati personali (GDPR), che considera come sensibili i dati inerenti a tali categorie.[49]

Parimenti, l'AIA[50] si concentra principalmente su attributi personali. La proposta di regolamento vieta alcune pratiche di intelligenza artificiale che abbiano un potenziale significativo di manipolare le persone attraverso tecniche subliminali al di là della loro coscienza o di sfruttare le vulnerabilità di specifici gruppi vulnerabili, come i bambini o le persone con disabilità, al fine di distorcere materialmente il loro comportamento in modo tale da causare a loro o a un'altra persona danni psicologici o fisici. Altre pratiche manipolative o di sfruttamento nei confronti degli adulti che potrebbero essere facilitate dai sistemi di intelligenza artificiale potrebbero essere coperte dalla legislazione esistente in materia di protezione dei dati, protezione dei consumatori e servizi digitali, che garantisce che le persone fisiche siano adeguatamente informate e abbiano la possibilità di scegliere liberamente di non essere soggette alla profilazione o ad altre pratiche che potrebbero influenzare il loro comportamento.[51] Nel dettaglio, l'articolo 5(1)(b) della proposta vieta:

"l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA che sfrutta le vulnerabilità di uno specifico gruppo di persone, dovute all'età o alla disabilità fisica o mentale, al fine di distorcere materialmente il comportamento di una persona che appartiene a tale gruppo in un modo che provochi o possa provocare a tale persona o a un'altra persona un danno fisico o psicologico;"

Il danno economico sembra quindi escluso dall'ambito di protezione, lasciando la possibilità dell'uso dell'intelligenza artificiale nello sfruttamento e nella loro manipolazione dei consumatori in contesto economico. Tuttavia, la definizione di intelligenza artificiale ad alto rischio contenuta nell'articolo 7, che consente alla Commissione di adottare atti delegati, tiene conto della vulnerabilità in modo

[49] MALGIERI, *Vulnerability and Data Protection Law*, Oxford, 2023.
[50] Cit. nota 6.
[51] Relazione, para. 5.2.3

leggermente più ampio. L'articolo 7(2)(f) della proposta tiene conto della misura in cui le persone potenzialmente danneggiate o con un impatto negativo si trovino in una posizione vulnerabile rispetto all'utente di un sistema di intelligenza artificiale, in particolare a causa di uno squilibrio di potere, di conoscenze, di circostanze economiche o sociali o di età. Questa è di gran lunga la concezione più ampia di vulnerabilità, ma può essere presa in considerazione solo in presenza di un rischio elevato per la salute e la sicurezza o per i diritti fondamentali, limitandone così drasticamente la possibilità di applicazione.

Ancora, sempre nell'ottica di favorire l'innovazione e la concorrenza, la Commissione europea ha recentemente presentato una proposta di Regolamento sull'accesso equo ai dati e sul loro utilizzo (*Data Act*).[52] La proposta affronta il tema della concentrazione dei dati nel mercato e ha l'obiettivo di garantire equità nell'allocazione del valore dei dati stessi e promuoverne l'accesso e l'uso, creando un quadro di *governance* orizzontale e intersettoriale. Per raggiungere l'obiettivo, il Data Act mira a garantire che una più ampia gamma di soggetti interessati abbia accesso a un maggior numero di dati per usi innovativi. Di rilievo in questa sede è l'isolata menzione alla vulnerabilità del consumatore e la conseguente ininterrotta visione del consumatore medio da parte del legislatore. La proposta normativa mira a evitare che gli operatori digitali ricorrano a mezzi coercitivi, ingannevoli o manipolatori nei confronti degli utenti, sovvertendone o pregiudicandone l'autonomia, il processo decisionale o le scelte, anche mediante l'uso di interfaccie digitali. In tale contesto, non dovrebbero fare affidamento sui cosiddetti *dark patterns*, vale a dire tecniche di progettazione che ingannano i consumatori spingendoli verso decisioni che hanno conseguenze per loro negative. Ebbene, il Considerando 34 del Data Act si limita a riconoscere che queste tecniche di manipolazione possano essere utilizzate per persuadere gli utenti, in particolare i consumatori vulnerabili, ad adottare

[52] Cit. nota 7.

comportamenti indesiderati, per indurli con l'inganno a prendere decisioni in favore di operazioni di divulgazione dei dati, o per distorcere indebitamente il processo decisionale degli utenti del servizio, in modo da sovvertirne e pregiudicarne l'autonomia, il processo decisionale e la scelta.

Passando alla disamina di legislazione settoriale, la proposta di direttiva sul credito al consumo[53] menzionava i consumatori vulnerabili solo due volte nella relazione esplicativa. Dapprima, riconosce come la crisi del COVID-19 e le conseguenti misure di confinamento abbiano accelerato la trasformazione digitale e abbia altresì avuto un impatto significativo sul mercato del credito e sui consumatori, in particolare quelli vulnerabili, rendendo molte famiglie finanziariamente più vulnerabili.[54] Inoltre, limita l'intervento ai servizi di consulenza in materia di debito (*debt advice*), all'informazione e ad alcuni miglioramenti delle norme relative al merito creditizio, sebbene possa ritenersi che l'allargamento del proprio ambito di applicazione a una serie di prestiti precedentemente esclusi e a nuove misure di tolleranza dovrebbero rivelarsi utili ad assistere i consumatori più vulnerabili.[55] Il testo della risultante Direttiva 2023/2225[56] appena emanato si limita all'enunciato del Considerando 76, secondo cui:

"*Il quadro dell'Unione applicabile dovrebbe dare ai consumatori fiducia nel fatto che i creditori e gli intermediari del credito tengono conto degli interessi del consumatore, compresi la sua eventuale vulnerabilità e le sue difficoltà a comprendere il prodotto, sulla base delle informazioni a disposizione del creditore o dell'intermediario del credito nel momento considerato e di ipotesi ragionevoli circa i rischi cui è esposta la situazione del consumatore per tutta la durata del contratto di credito proposto*."

[53] Proposta di direttiva del Parlamento europeo e del consiglio relativa ai crediti al consumo, COM/2021/347 final.
[54] Relazione esplicativa alla proposta di direttiva relativa ai crediti al consumo, cit. nota 53, punto 1.
[55] Ibid., punto 3.
[56] Cit. nota 9.

Nell'ambito delle priorità della *Digital Financial Strategy*[57] – la politica della Commissione volta a promuovere l'innovazione guidata dai dati nel settore finanziario - l'UE mira a creare uno spazio comune di dati finanziari attraverso una serie di misure più specifiche. Di rilievo è la priorità di creare una maggiore condivisione e accesso ai dati per il loro riutilizzo nel settore finanziario, aprendo così la strada alla cd. 'finanza aperta' (*Open Finance*). L'*Open Finance* intende essere un'iniziativa incentrata sul cliente, il cui cardine si fonda sul controllo dei dati da parte dello stesso. Tra le possibili questioni giuridiche da analizzare, diviene essenziale determinare quale sia la condizione giuridica per il trattamento dei dati, nonché gli strumenti giuridici affinché i consumatori vengano responsabilizzati e mantengano un effettivo controllo, sempre che queste siano le soluzioni idonee a una effettiva tutela nel mercato digitale.[58]

5. La ricerca di equità per i consumatori nei mercati digitali richiede la messa in discussione dello *status quo* e delle basi consolidate del diritto dei consumatori dell'UE. La Nuova Agenda dei Consumatori si limita ad aggiornare la direttiva sulla tutela dei consumatori e gli orientamenti della direttiva sui diritti dei consumatori per garantire che i consumatori beneficino di un livello di protezione e di equità online paragonabile a quello di cui godono offline.[59] Questa posizione appare miope in quanto presuppone che i mercati offline funzionino in modo ottimale per i consumatori. In tutti questi anni si è pensato che l'equità sarebbe stata raggiunta affidandosi all'informazione come rimedio, aspettandosi che il consumatore medio garantisse che le imprese fossero tenute sotto controllo.

[57] Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni relativa a una strategia in materia di finanza digitale per l'UE, COM/2020/591 final.
[58] Sull'Open Finance si veda FERRETTI, *L'Open Finance: Quali prospettive regolatorie per una strategia UE in materia di protezione dei consumatori nella finanza digitale?*, in *Banca Impresa Società*, 2023, 277; PARACAMPO, *Trasformazione digitale del settore finanziario e open finance: quali prospettive per un credito "sostenibile"? Prime riflessioni*, in *Media Laws*, 2023, 1.
[59] Nuova Agenda dei Consumatori, cit. nota 3.

Nel momento in cui l'UE cerca di muoversi verso un'Europa digitale, la realizzazione della protezione dei consumatori nel mercato unico digitale richiede diversi cambiamenti radicali nei concetti e nei metodi utilizzati finora per proteggere i consumatori, andando ben oltre rispetto a quanto lasci intendere la nuova agenda dei consumatori.

I mercati digitali sono un terreno fertile per la vulnerabilità. In linea di principio, tutti i consumatori sono coinvolti. Di conseguenza, questa realtà contrasta con il culto del consumatore medio. Nell'ambiente digitale, più che nel mercato tradizionale, il consumatore medio si scontra con una realtà dove è lecito aspettarsi che fatichi maggiormente a comportarsi come idealizzato.

La tecnologia stessa è un fattore trainante della vulnerabilità, intesa non in senso prettamente giuridico ma di fatto. Come già notato da altri, le fonti di vulnerabilità possono essere individuate non solo nelle vulnerabilità attuali (quelle che esistono e si sono già concretizzate) ma anche in quelle disposizionali (quelle latenti e non ancora concretizzate). Così, la raccolta di dati può non danneggiare i consumatori al momento e in ogni istante in cui essi vengono raccolti. Ma la raccolta di grandi quantità di dati da fonti diverse e non correlate, unitamente alla loro fusione in un profilo, potrebbero rendere i consumatori 'disposizionalmente' vulnerabili. Per prevenire abusi o usi imprevedibili, la protezione dovrebbe quindi pensare all'uso futuro dei dati e non solo a quello effettivo.[60]

La vulnerabilità deriva anche dal fatto che, nei mercati digitali, i consumatori spesso si disimpegnano. Lasciano che sia l'algoritmo a guidarli. È quanto mai raro che tentino di disattivare gli avvisi sulla privacy o di cercare un'offerta migliore, pur sapendo che i prezzi possono essere personalizzati. Non leggono i termini e le condizioni che consentono all'operatore di raccogliere dati e utilizzarli a proprio vantaggio, e così via. A questo proposito, viene evidenziato come i consumatori

[60] HELBERGER, LYNSKEY, MICKLITZ, ROTT, SAX, STRYCHARZ, *EU Consumer Protection 2.0, Structured Asymetries in digital consumer markets*, Bruxelles, 2021.

'disimpegnati' si trovino in situazioni di acquisto vulnerabili, non per particolari carenze cognitive o caratteristiche socio-demografiche, ma perché la struttura stessa dei mercati di consumo su cui si evolvono porta all'apatia attraverso l'offuscamento. In questi casi, infatti, diviene del tutto razionale che i consumatori si disimpegnino. In generale, i consumatori sono vittime della manipolazione online, ovvero dell'uso delle tecnologie per influenzare in modo occulto il processo decisionale di una persona, sfruttandone le vulnerabilità decisionali. Il disimpegno è il risultato del funzionamento di un mercato che si ostina a trattare i consumatori in modo iniquo, creando così una vulnerabilità, oltre a creare malfunzionamenti nel mercato stesso. I consumatori fanno solo la cosa più razionale possibile: non perdono tempo a leggere le note sulla privacy o i termini e le condizioni.[61]

Torna utile, quindi, considerare anche il ruolo delle strutture nel profilo di vulnerabilità dei consumatori. Come sostenuto da Helberger et al., nella società digitale la vulnerabilità risiede nelle architetture di scelta digitale in cui i consumatori si muovono quotidianamente, in quanto progettate per indurre o creare vulnerabilità. Tali vulnerabilità - siano esse disposizionali o contingenti - non sarebbero uno sfortunato sottoprodotto dei mercati digitali, ma il prodotto stesso dei mercati digitali. Così, nelle pratiche digitali la configurazione commerciale diviene solo una parte di un approccio più ampio e sistemico per influenzare il comportamento dei consumatori.[62]

Pertanto, se da un lato si riconosce che la vulnerabilità sia più variegata di quanto previsto dal diritto, dall'altro le cause strutturali della creazione o aggravamento della vulnerabilità risultano meno documentate.

Come prospettato da Fineman, un crescente riconoscimento del fatto che gli elementi esterni creino, influenzino o rafforzino le vulnerabilità producono un

[61] SICILIANI, RIEFA, GAMPER, *Consumer Theories of Harm, An economic approach to consumer law enforcement and policy making*, cit.
[62] Ibid.

fenomeno che può essere identificato come 'vulnerabilità sistemica', cioè una vulnerabilità creata dal sistema stesso, una vulnerabilità della persona che deriva dal modo in cui un sistema è concepito - in altre parole, dalla sua architettura.[63]

Tuttavia, la vulnerabilità sistemica del mercato digitale non sarebbe limitata esclusivamente alla sua architettura, ma sarebbe anche il risultato di sistemi che non riescono ad assisterli, come una regolamentazione mal concepita o inefficiente. Trattasi, ad esempio, di regole di concorrenza obsolete o di una scarsa protezione dei dati o di un eccessivo affidamento alle informazioni - fragilità normative tutte ben documentate in letteratura.[64]

Piuttosto che regolamentare facendo una distinzione tra sistemi o tra gruppi di consumatori e la loro capacità come avviene oggi, pertanto, sembrerebbe più opportuno puntare sulle asimmetrie digitali riconoscendo il concetto di 'vulnerabilità digitale' caro a Helberger et al., al fine di poter descrivere uno stato universale di incapacità di difendersi e suscettibilità a squilibri di potere economico, in aggiunta al potenziale sfruttamento tipico della crescente automazione commerciale, delle relazioni dati-consumatore-venditore e dell'architettura stessa dei mercati digitali.

6. Come ampiamente notato sopra, nonostante i limiti ben documentati e le numerose critiche, l'informazione rimane a tutt'oggi il principale strumento giuridico di tutela dei consumatori.

In questa sede, si sostiene che con il mercato digitale il paradigma dell'informazione sia sempre meno appropriato e, di pari passo, vi sia la necessità di rivalutare le principali nozioni del diritto del consumo a cominciare dal concetto giuridico di

[63] FINEMAN, *Vulnerability and Inevitable Inequality*, cit.

[64] HELBERGH et al., *EU Consumer Protection 2.0, Structured Asymetries in digital consumer markets*, cit.; RIEFA, SAINTIER, *The way forward: For an inclusive access to justice to protect vulnerable consumers* in RIEFA, SANTIER *Vulnerable Consumers and the Law: Consumer Protection and Access to Justice*, Oxford, 2021, 248; CREUTZFELDT, GILL, CORNELIS, MCPHERSON, *Access to justice for vulnerable and energy-poor consumers, Just Energy?* Oxford, 2021.

consumatore 'medio'.

A quest'ultimo proposito, si riscontra una modesta prospettiva con una domanda di pronuncia pregiudiziale alla Corte di giustizia UE da parte del Consiglio di Stato, laddove si chiede se la nozione di consumatore 'medio', inteso come consumatore normalmente informato e ragionevolmente attento ed avveduto, non debba essere formulata con riferimento alla miglior scienza ed esperienza delle più recenti teorie sulla 'razionalità limitata'. Queste, infatti, hanno dimostrato come le persone agiscono spesso riducendo le informazioni necessarie con decisioni irragionevoli se parametrate a quelle che sarebbero prese da un soggetto ipoteticamente attento ed avveduto, acquisizioni che impongono una esigenza protettiva maggiore dei consumatori nel caso, sempre più ricorrente nelle moderne dinamiche di mercato, di pericolo di condizionamenti cognitivi.[65]

Seppure una tale interpretazione possa già rappresentare un passo in avanti nella protezione del consumatore, specialmente nei mercati digitali, come notato sopra gli attuali dibattiti dottrinali sulla psicologia dei consumi e nelle scienze sociali sembrano essere già andati ben oltre l'idea di 'razionalità limitata', per tenere conto non solo dei limiti cognitivi ma anche di vincoli sociali, abitudini, motivazioni, etc.
Spingendosi oltre alle predette teorie dottrinali, qui si sostiene che occorrerebbe, piuttosto, riconoscere che nelle dinamiche dei mercati digitali il consumatore medio è vulnerabile di default– o, in altre parole, la vulnerabilità rappresenta lo standard del consumatore 'medio'.
Riconoscendo che la vulnerabilità dei consumatori nei mercati digitali è di ampia concezione, disancorata dalla sua limitata nozione giuridica e che, anzi, rappresenta la norma nella misura in cui ogni consumatore è vulnerabile, implica che verrebbe a

[65] Causa C-646/22, Domanda di pronuncia pregiudiziale proposta dal Consiglio di Stato (Italia) il 13 ottobre 2022 — *Compass Banca SpA / Autorità Garante della Concorrenza e del Mercato*, OJ C 24, 23.1.2023, 28–29. Sulla nozione economica di razionalità limitata, si veda in particolare BANCA D'ITALIA, *Bounded rationality and expectations in economics*, in *Questioni di economia e finanza*, luglio 2020.

cambiare il modo in cui viene immaginato il diritto e la sua applicazione. L'attenzione normativa dovrebbe così spostarsi dalla definizione di vulnerabilità o dall'individuazione di particolari gruppi verso un concetto di vulnerabilità rivolto alla gestione delle fonti di vulnerabilità, che ricomprendono *in primis* l'asimmetria digitale come fonte primaria. A tal fine, è auspicabile un approccio che preveda un quadro normativo costituito da obblighi positivi e sostanziali piuttosto che affidarsi, come guida, all'equità procedurale. Si tratterebbe di sviluppare standard di condotta più prescrittivi tali da introdurre regole volte a garantire un dovere positivo di correttezza da parte dei prestatori di servizi digitali.

La promozione di un siffatto approccio alla regolamentazione non eliminerebbe del tutto i doveri informativi, che in una certa misura rimarrebbero comunque necessari, ma cesserebbe di affidarsi alle informazioni come proxy di protezione.

L'attuale ondata normativa dei mercati digitali rappresentata dal GDPR, DMA, DSA, Data Act, AIA etc. prosegue con un approccio frammentario che affronta vari aspetti, ma non affronta il tema della vulnerabilità intesa come asimmetria digitale. A tal uopo, occorrerebbe un dovere positivo in capo ai prestatori di servizi di operare in modo equo, invitando il legislatore a ripensare le operazioni digitali in termini di correttezza progettuale proprio allo scopo di ridurre quella asimmetria digitale causa della nuova vulnerabilità.

Come recentemente sostenuto in modo convincente da Gianclaudio Malgieri e Frank Pasquale, con la richiesta di misure di controllo di qualità prima dell'impiego delle nuove tecnologie digitali, un approccio *ex ante* spesso attenuerebbe e talvolta impedirebbe del tutto i danni che esse provocano o contribuiscono a provocare. Ad esempio, un sistema di concessione di licenze sarebbe un importante strumento di regolamentazione *ex ante* da utilizzarsi in diversi mercati digitali, specialmente quelli ad alto rischio. Le agenzie di autorizzazione dovrebbero richiedere ai prestatori di servizio di dimostrare che le loro tecnologie digitali soddisfano chiari requisiti di sicurezza, non discriminazione, accuratezza, adeguatezza e correggibilità prima di

essere impiegate. Secondo questo modello di regolamentazione *ex ante*, gli sviluppatori di nuove tecnologie avrebbero l'onere di dimostrare che il loro utilizzo non è discriminatorio, manipolativo, ingiusto, impreciso o illegittimo.[66] Malgeri e Pasquale riconoscono altresì che, a differenza delle normative sin qui in essere applicabili al dominio digitale, un modello del genere trova già riscontro nel AIA come primo timido tentativo di regolamentazione verso un regime di licenze *ex ante* in aree ad alto rischio. Questo avviene attraverso la procedura di valutazione di conformità che i fornitori di sistemi di IA ad alto rischio devono eseguire per dimostrare la conformità a diversi principi e garanzie di progettazione, tra cui la *governance* dei dati, l'integrità e la supervisione umana.[67] Tuttavia, un siffatto impianto normativo dovrebbe essere rafforzato attraverso un ampliamento del suo ambito di applicazione e del suo contenuto sostanziale a causa della portata limitata del modello di autorizzazione, della mancanza di trasparenza del processo di giustificazione ex ante e del contenuto limitato della giustificazione dell'AIA.[68]

Un tale invito a riconsiderare il diritto dei consumatori, specialmente nei mercati digitali, trova giustificazione dal fatto che, in difetto, i danni subiti dai consumatori non solo persisterebbero, ma rischierebbero altresì di peggiorare laddove si affermasse la sfiducia dei consumatori nei mercati, oltre a rappresentare un limite per un sano sviluppo dell'economia digitale. Ripensare al diritto in termini di obblighi di correttezza *by default* e *by design* condurrebbe a garantire che i consumatori possano essere trattati in modo equo, giusto o comunque ragionevole *ex ante*, riflettendone la reale natura comportamentale. Allo stesso tempo, responsabilizzerebbe i prestatori di servizi facilitando la supervisione e l'applicazione del diritto stesso.

[66] MALGERI, PASQUALE, *Licensing high-risk artificial intelligence: Toward ex ante justification for a disruptive technology*, in 52 *Computer Law & Security Review*, 2024.
[67] Articoli 9-15 AIA.
[68] MALGERI, PASQUALE, *Licensing high-risk artificial intelligence: Toward ex ante justification for a disruptive technology*, cit.

In definitiva, la correttezza nei mercati digitali diverrebbe essere di natura architetturale e non qualcosa da offrire ai consumatori come rimedio dopo che il danno si è già verificato.

Per concludere, una reinterpretazione giuridica del concetto di consumatore 'medio' in termini di vulnerabilità *lato sensu* appare quanto mai necessaria. Di pari passo, sarebbe desiderabile una regolamentazione che, riconoscendo una tale vulnerabilità, non si concentri su tentativi di darne una definizione ma si rivolga a contrastarne le fonti *ex ante*, con obblighi di correttezza architetturale *by design e by default*. Questo risponderebbe non solo a esigenze di equità nella protezione della parte debole nel sinallagma contrattuale in un momento storico particolarmente critico sul piano socio-economico, ma favorirebbe anche quella fiducia nei mercati essenziale per l'espansione degli stessi.

Federico Ferretti

Associato di Diritto dell'economia

nelll'Alma Mater Studiorum Università di Bologna

Volume 11 – Part 2 – 2022 ISSN 2050-9014

LAW AND ECONOMICS YEARLY REVIEW

ISSUES ON FINANCIAL MARKET REGULATION, BUSINESS DEVELOPMENT AND GOVERNMENT'S POLICIES ON GLOBALIZATION

Editors

F. CAPRIGLIONE – R. M. LASTRA – R. MCCORMICK
C. PAULUS – L. REICHLIN – M. SAKURAMOTO

in association with

Queen Mary University of London

LAW AND ECONOMICS YEARLY REVIEW

www.laweconomicsyearlyreview.org.uk

Mission

The "Law and Economics Yearly Review" is an academic journal to promote a legal and economic debate. It is published twice annually (Part I and Part II), by the Fondazione Gerardo Capriglione Onlus (an organization aimed to promote and develop the research activity on financial regulation) in association with Queen Mary University of London. The journal faces questions about development issues and other several matters related to the international context, originated by globalization. Delays in political actions, limits of certain Government's policies, business development constraints and the "sovereign debt crisis" are some aims of our studies. The global financial and economic crisis is analysed in its controversial perspectives; the same approach qualifies the research of possible remedies to override this period of progressive capitalism's turbulences and to promote a sustainable retrieval.

Address

Fondazione Gerardo Capriglione Onlus

c/o Centre for Commercial Law

Studies Queen Mary, University of

London 67-69 Lincoln's Inn Fields

London, WC2A 3JB

United Kingdom

Main Contact

Fondazione G. Capriglione Onlus - fondazionecapriglione@luiss.it

ISSN 2050-9014

Review Process

1. Articles and case notes submitted to the Review will be reviewed by at least two reviewers (chosen among the Editorial Board members) and, where necessary, by an external advisor.

2. Any paper will be submitted by the Editorial Board – anonymously, together with an evaluation form – to the reviewers for an overall assessment.

3. In case of a single negative evaluation by one of the reviewers, the Editor-in-chief may assume the responsibility to publish the paper having regard to highlight this circumstance.

4. In any case, the submission of the paper or its positive evaluation does not provide any right to the author to ask for the publication of the paper. Fondazione Gerardo Capriglione Onlus may reproduce articles published in this Review in any form and in any other publications.

CONTENTS

OPEN FINANCE AND CONSUMER PROTECTION: UNEASY BEDFELLOWS

Federico Ferretti [*] - Peter Petkoff [**]

ABSTRACT: *This article examines Open Finance and the risks that it poses for consumer protection. To exist, Open Finance needs enabling legislation. EU policy, as well as actual and proposed legislation, point to empowering consumers and give them control over their data. The traditional role of data in financial services markets is examined, as well as the transformative role of new data technologies to deliver new market structures. Drawing from the experience of Open Banking, the GDPR and the proposal for a Data Act this article questions to what extent the EU legal instruments are capable of delivering the goal, and consumers are factually empowered, remain in control of their data and are protected against the main risks of data-driven finance and the digital domain, where vulnerability is likely to be the norm. It shows how other jurisdictions such as the United Kingdom engage in a different approach to suggest a paradigm shift in the EU regulatory approach.*

---

[*] Jean Monnet Chair in Digital Market Law and Associate Professor at *Alma Mater Studiorum* University of Bologna.

[**] Research Fellow at the University of Oxford and Senior Lecturer in Law at Brunel University London (UK).

This research has been carried out within the Jean Monnet Chair in Digital Market Law (E-DSM) E-DSM - 101047038 - GAP-101047038. The European Commission's support for the research does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. Sections 1, 2, 3, 4.1, 4.2, 5, and 6 are attributed to Federico Ferretti, and Section 4.3 to Peter Petkoff.

– 4.3. – The approach in the United Kingdom. – 5. Open Risks. – 5.1. Legal uncertainty and the lack of effective control. – 5.1.1. Contractual necessity ex Article 6(1)(b) GDPR. – 5.1.2. Consent ex Article 6(1)(a) GDPR. - 5.2. Black boxes and dark patterns. – 6. Conclusions.

1. This paper investigates the challenges posed by Open Finance in its quest to place consumers at its centre by empowering and protecting them. It questions the extent to which the envisaged legal framework is capable of offering the tools to achieve such goals.

Information to financial service markets has been crucial for long time. However, its function is undergoing a deep transformation. As the financial services industry embraces digitalisation, financial service providers use increasing data analysis and profiling to target customers, offer them customised products with personalised pricing, and create new products or services. Technological innovation has become the key aspect for new models in the provision of finance.[1]

Open Finance is the late frontier of the financial services' industry. Upon enabling legislation, it will refer to the obligation for traditional financial service providers to open access to their customers' financial data to third-party providers ('TPP') and share the data with them for the provision of a wider range of the same financial products or services, or the creation of new ones. It aims to expand TPP access to, and sharing of, the whole spectrum of financial data sources taken from a variety of financial providers and product lines such as savings, mortgages, consumer credits, investments, pensions, insurance, advice, etc. So devised, Open Finance advances significantly the transition to data-driven finance and may reshape the EU financial services industry.

So far, digital innovation and competition have been the thrust for the enactment of the late rich body of EU law which is currently being developed in

[1] CAPRIGLIONE, *The financial system towards a sustainable transition*, Law and Economics Yearly Review, 10(1), 2021, p 1.

response to the digital age.[2] At the same time, under EU policy, for Open Finance to exist customers need to factually control their data and be protected from abuses or misuses.[3]

However, data control, consumer empowerment and protection, and the processing of large amounts of diverse data in finance raise policy and legal issues. Regulation plays a pivotal role in the shaping of a EU single market fit for a sustainable digital economy, ensuring an optimal economic and social balance. The aim of this work is to analyse the extent to which the intersection of current and envisaged legal instruments may offer suitable solutions to achieve the envisaged policy goals and tackle the risks likely to be opened by Open Finance.

To reach its goal, this work is construed as follows.

Section 2 sets the theoretical foundations of data sharing in the financial services domain to show the transformative type and use of data to the changing economic cycle. It provides the necessary context of the new market structures in the transition towards open innovation and data-driven finance. Section 3 explores the role of regulation as enabler of innovation. It shows how the provisions of the Payment Services Directive 2 have instituted the new market model of Open Banking, presenting to the reader the mingling between banking and the data business as the

[2] E.g. Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, OJ L 337, 23.12.2015, p. 35–127; Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016, p. 89–131; Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, OJ L 172, 26.6.2019, p. 56–83; Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, OJ L 303, 28.11.2018, p. 59–68.

[3] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Digital Finance Strategy for the EU, COM(2020) 591 final; Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on a Retail Payments Strategy for the EU, COM/2020/592 final; European Commission, Targeted consultation on open finance framework and data sharing in the financial sector, available at https://finance.ec.europa.eu/regulation-and-supervision/consultations/finance-2022-open-finance_en.

forerunner of Open Finance, where the whole financial service sector becomes involved. Like Open Banking, Open Finance is a concept enabled by legislation. Thus, drawing from the experience of Open Banking, Section 4 examines the difficult intersection between the legislative model of the PSD2 and data protection law. Equally, it studies the proposal for a Data Act as a regulatory initiative on fair access and use of data of general application with whom Open Finance specific regulation will need to coexist. The approach taken in the neighbouring jurisdiction of the United Kingdom ('UK') is also presented to show the feasibility of a functional alternative policy debate. Section 5 sets forth the risks identified from the legal analysis, advancing that the resulting legal uncertainty, coupled with weak legal instruments may pose great risks for consumers, especially in a complex environment susceptible to opacity and dark patterns, where vulnerabilities thrive. Section 6 concludes.

2.

2.1. Finance has long been an information industry. It is a common feature that financial institutions process and exchange a growing amount of personal financial data about their customers as part of their business models. For example, lenders and insurers access databases managed by sectoral associations or third-party providers (e.g. Credit Bureaus) in order to evaluate a consumer's application, the risks involved in a transaction and their management, or the prospective customer's creditworthiness or trustworthiness.[4]

Traditionally, the type of data exchanged are those of the concerned product line for the benefit of the concerned market players. For example, in credit relationships, traditional data are personal data relating to debt payments and financial accounts with lenders. But the level of product coverage in the databases

[4] *SCIARRONE ALIBRANDI and MATTASSOGLIO, Le centrali dei rischi: problemi e prospettive, Diritto della Banca e del Mercato Finanziario, 2017, 4, p 764;* FERRETTI, *The law and consumer credit information in the European community: the regulation of credit information systems*, 2008, Routledge.

differs from country to country.[5]

Likewise, in the insurance sector traditional data are those relating to the insured risk, e.g. the behaviuor of a customer that is likely to cause the event.

In financial circles, the virtues of data sharing are usually portrayed in terms of more efficient processes and decision-making, or for a better management of financial risks or fraud situations. Most of the times, the benefits for consumers have been highlighted in terms of products/services better tailored to their needs, better quality, or cost-efficiency.[6] Moreover, the extensive use of financial data has been promoted to achieve a number of policy objectives. These include the facilitation of the access to more affordable and better-quality financial services for consumers,[7] the prevention of consumer over-indebtedness by limiting irresponsible/predatory lending,[8] and the contribution to financial stability by limiting financial institutions' loss risks.[9]

Under certain national systems, financial data can even be part of a broader information centralisation system managed by national central banks for the purpose of oversight of the financial system as a whole, i.e. they are an instrument for the prudential supervision of the financial system.[10]

Supported by classical economic and financial literature, dominant justifications for data sharing have started with the reduction of the information

---

[5] ACCIS, *ACCIS 2020 Survey of Members – An Analysis of Credit Reporting in Europe*, 2020.

[6] E.g. BANK OF ENGLAND, *Should the availability of UK credit data be improved?*, Discussion Paper, May 2014; HM TREASURY, *Improving access to SME credit data: summary of responses*, June 2014, at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/323318/PU1681_final.pdf; TURNER and VARGHESE, *The Economic Consequences of Consumer Credit Information Sharing: Efficiency, Inclusion, and Privacy*, 2010, OECD; JENTZSCH, *Financial Privacy - An International Comparison of Credit Reporting Systems*, 2007, Springer.

[7] OECD, *Facilitating access to finance - Discussion Paper on Credit Information Sharing*, at https://www1.oecd.org/globalrelations/45370071.pdf

[8] ACCIS, *ACCIS Response to Financial Services User Group (FSUG) Position Paper on the London Economics Study on Means to Protect Consumers in Financial Difficulty*, October 2013, at http://www.accis.eu/uploads/media/ACCIS_Response_to_FSUG_Position_Paper_October_2013.pdf.

[9] WORLD BANK, *General principles for credit reporting*, 2011, at http://documents.worldbank.org/curated/en/662161468147557554/General-principles-for-credit-reporting.

[10] JAPPELLI and PAGANO, *Public Credit Information: A European Perspective*. In *Reporting systems and the international economy*, 2003, MIT Press, p 81.

asymmetry between financial providers and borrowers for a better risk analysis, including problems of bad selection of customers, and the risk which arises from the characteristics of prospective customers that may increases the possibility of an economic loss.[11]

It is from this classic economic theory that the first correlations or associations have started to emerge, in particular the one that past behaviour is predictive of future behaviours.[12] Contrary to causation, under these assumptions the observation of human past through the data has been deemed to statically or repeatedly predict the likelihood of the future.

Such correlations also explain how economic theory has then moved to advance the proposition that data exchanges among financial service providers could play a major role as a customer's discipline device. Customers would know that the causation of an event, change in circumstances, or a delay or a default in re-payment compromise their reputation with all the other providers on the market, resulting in credit or insurance with more costly terms or by cutting them off from the market entirely.[13] Therefore, data sharing has been seen as reducing moral hazard. A customer's 'good name', i.e. their reputation collateral, contributes to provide an incentive to maintain certain behaviours or meet commitments much the same way as does a physical collateral.[14]

From another angle, the sharing of data on customer relationships has been also promoted to reduce the information monopoly of individual providers and the

[11] STIGLITZ and WEISS, *Credit Rationing in Markets with Imperfect Information*, American Economic Review 71(3), 1981, p 393; BERGER and UDELL, *Relationship Lending and Lines of Credit in Small Firm Finance*, Journal of Business, 68, 1995, p 351; AKELOF, *The market for 'Lemons': Quality uncertainty and the market mechanism*, Quarterly Journal of Economics, 28(3), 1970, p 523; DIAMOND, *Monitoring and Reputation: The Choice between Bank Loans and Directly Placed Debt*, *Journal of Political Economy*, 99(4), 1991, 689; ADMATI and PFLEIDERER, *Forcing Firms to Talk: Financial Disclosure Regulation and Externalities*, Review of Financial Studies, 13, 2000, p 479.

[12] MILLER, *Introduction*. In *Reporting Systems and the International Economy*, 2003, MIT Press, pp 1.

[13] JAPPELLI and PAGANO, *Information Sharing, Lending and Defaults: Cross-Country Evidence*, *Journal of Banking and Finance*, 2002, p 2017.

[14] MILLER, *Introduction*, cit., p 1.

competitive advantage of large financial institutions, thus promoting market competition.[15] The problem of asymmetric information and adverse selection becomes greater for new market entrants, particularly providers from other Member States. This is particularly the case in the context of the EU single market and cross-border entry or cross-border provision of financial services. In addition to competitive disadvantages in relation to incurring greater risks of incorrectly estimating a customer's risk, without relevant information on customers new market entrants would be likely to attract precisely those who were rejected or overpriced by existing providers in the market.[16] This circumstance has induced recent literature to conclude that personal data exchanges, market structure, and competitive conduct are intrinsically intertwined in the financial services market. From the standpoint of industrial organisation, the availability of data shared by the sector can affect firms' choice not only of whether to entry another jurisdiction but also the mode of doing it, i.e. whether through the cross-border provision of services, the setting-up of branches or subsidiaries, or through mergers and acquisitions.[17]

One of the most apparent limitations of the above theoretical foundations lies in the neo-classical understanding or bias of the consumer as purely a *homo economicus* where they are seen as rational, informed, narrowly self-interested, vigilant and alert economic agents. In short, consumers who have the ability to make judgments towards their subjectively defined ends and who maximise their own utility and make intelligent and conscious choices, free of external events biasing or forcing their behaviour.[18] Such an economic interpretation appears inconsistent with

[15] European Commission, *Report of the Expert Group on Credit Histories*, May 2009.
[16] GIANNETTI, JENTZSCH, SPAGNOLO, *Information-Sharing and Cross-Border Entry in European Banking*, ECRI Research Report N. 11, February 2010.
[17] *Ibid.*
[18] STATEN and CATE, *Does the Fair Credit Reporting Act Promote Accurate Credit Reporting?*, Working Paper Series BABC 04-14, 2004, Joint Center for Housing Studies, Harvard University; BECKER, *The economic approach to human behavior*, 1976, University of Chicago Press; OSOVSKY, *The misconception of the consumer as a homo economicus: a behavioral-economic approach to consumer protection in the credit-reporting system*, 46(3) Suffolk University Law Review, 46(3), 2013, p 881.

the findings and increasing acceptance of the behavioural literature which attempts to explain relevant features of human behaviour and the consumers' cognitive limitations that cannot be explained under standard economic assumptions. It challenges economic assumptions by using a number of alternative social sciences or disciplines such as psychology, sociology, neurosciences to explore the real behaviour of human beings and how economic decisions are taken or dictated in the economic, cultural, and social context where they live.[19] Under this perspective, traditional financial data may only give a partial or fragmented picture of a customer's story or situation. They may present a distorted impression of individuals, not because the data are incorrect but for presenting a piecemeal picture making it seem incomplete and incorrect. In simple language, it is like taking a few silvers of a person and presenting that as the whole her/him.

Many other questions arise on the viability and assessment of those who are not in the databases. Arguably, those who are not in the databases or lack information for not having incurred into any financing operation are not negligible in numbers. Such a data sharing seems to penalise those segments of the population with a weaker financial history notwithstanding their personal circumstances, or ignoring behavioural biases or unstandardised conducts. From this point of view, the resulting theories appear to some extent artificial. The inability of these systems to detect atypical behaviours raises questions and problems because they also make

[19] The literature on behavioural economics is copious. Examples are JOLLS, SUSTAIN, THALER, *A behavioral approach to law and economics*, Stanford Law Review, 50, 1998, p 1471; DIAMOND and VARTIAINEN (edited by), *Introduction to behavioural economics and its applications* , 2007, Princeton University Press; CAMERER, ISSACHAROFF, LOEWENSTEIN, O'DONOGHUE, RABIN, *Regulation for conservatives: behavioral economics and the case for asymmetric paternalism*, University of Pennsylvania Law Review 151, 2003, p 1211; HANSEN and KYSAR, *Taking behaviouralism seriously: the problem of market manipulation*, New York University Law Review, 74, 1999, p 630. For literature specifically addressing borrowers' behavior see AGARWAL and ZHANG, *A review of credit card literature: perspectives from consumers*, 19 October 2015, at https://www.fca.org.uk/publication/market-studies/review-credit-card-literature.pdf; LEA, *Behaviour Change: Personal Debt*, no date, The British Psychological Society, at www.bps.org.uk/ behaviourchange; XIAO, *Consumer Economic Wellbeing*, 2015, Springer; WRIGHT, *Behavioral law and economics, paternalism, and consumer contracts: an empirical perspective*, NYU Journal of Law and Liberty, 2, 2007, p 470.

assumptions about what 'normal' behaviour is, where deviation from the established pattern is seen as undesirable or questionable, with all the following implications.

The use of personal data in the same financial product line - combined with the limitations or errors in the data and in the analytic tools – could also raise questions around the relationship between the data and pricing practices, for example making use of analytical data showing a consumer's degree of willingness to pay more, liaising higher prices to higher perceived risks of a consumer, or demonstrating their inertia to switch products or services. In this respect, the biases behind the classic economic theories go against the foundations of human behaviours as heterogeneous and unpredictable.

2.2. As the underwriting of financial services and technologies evolve, and finance adapts to changing economic cycles and demographics, new business models recognise the limits of traditional data.

A limit of traditional data is that they are largely of historical nature. As they make use of a limited number of categories of data, they do not provide a reliable picture.

Technological innovation thus becomes the key to develop new models in the provision of personal finance.[20]

Technologically enabled financial innovation in consumer financial services ('fintech') capable of making use of large datasets from various unrelated sources ('big data') are one important facet of late innovations that is generating significant interest in financial markets for its possible disruptive effects in the sector.[21] Many Fintech developments are based on proprietary artificial intelligence systems (AI) and

[20] BASKERVILLE, CAPRIGLIONE and CASALINO, *Impacts, challenges and trends of digital transformation in the banking sector*, Law and Economics Yearly Review, 9(2), 2020, 341.
[21] EUROPEAN BANKING AUTHORITY, *Discussion Paper on innovative uses of consumer data by financial institutions*, London, 4 May 2016; EUROPEAN BANKING AUTHORITY, *EBA Guidelines on creditworthiness assessment", Final Report on Guidelines on Creditworthiness Assessment*, London, 19 August 2015; THE FINANCIAL INCLUSION CENTRE, *FinTech – Beware of the "Geeks' Bearing Gifts?*, A Financial Inclusion Centre Discussion Paper, January 2018.

associated innovative uses of data. AI embraces different forms of computer systems that are able to learn from the data and their own experiences to solve complex problems or uncover patterns to predict future data or perform decision-making tasks (also known as machine-learning powered by mathematical algorithms able to create further algorithms based on accumulated data).[22]

As technologies evolve, and standards and appetite for financial services adapt to changing economic cycles and shifting demographics, a wider array of new data become available for analysis. These other data are those data gathered from diverse sources outside the standard product lines that financial institutions used to evaluate their clients. Their volume is greater than that of the traditional sources as they are usually taken from several data points mined from consumers' digital or offline activities. Even if such big data are not intuitively related to the product line and specific transactional risk, all data become financially relevant data with an open nature as to their sources. This also enables the leverage of a large volume of data from diverse sources and generated from various transactions to create new products or business models. The analysis of big data, increasingly in real time, drives knowledge and value creation across society in the fashion of a so-called 'open innovation', that is an innovation ecosystem where ideas and knowledge flow across firm boundaries sourced from both internal and external sources by means of sharing knowledge and information.[23]

These innovative techniques are capable of reshaping business models, underwriting criteria, and customer experiences. Their innovations associate the commoditization of big data analytics with an understanding of demographic changes, borrower needs, and how to connect to customers through new

[22] CAPRIGLIONE, *Law and economics. The challenge of artificial intelligence*, Law and Economics Yearly Review, 10(2), 2021, p 189. See also MURPHY, *Machine Learning: A Probabilistic Perspective*, 2012, MIT Press, 2012; LANDAU, *Artificial Intelligence and Machine Learning: How Computers Learn*, 17 August 2016, Tech Innovation, at https://iq.intel.com/artificial-intelligence-and-machine-learning/

[23] CHESBROUGH, *Open Innovation: The new imperative for creating and profiting from technology*, 2003, Harvard Business School Press.

technological channels.[24] Reportedly, the 2008 financial crisis first, and the COVID-19 pandemic next, also have played an accelerating role marking the impetus and arrival of new market players pushing for competition over innovation to lower costs and gain market share.[25]

The fundamental drawback of the resulting market physiognomy is that data holders could legitimately refuse access to their data infrastructures on grounds of intellectual property protection, data protection concerns, security risks, or the permanence of unclear rules over liabilities towards the customers.[26]

The fintech ecosystem thus risks displaying low competition characterised by low elasticity of demand, lock-in problems, and exclusivity of services of mainstream providers,[27] as well as a legal vacuum of an alternative market operating outside the relationship between the traditional incumbents and their customers.[28]

3. Regulation can take a key role in enabling innovation in financial services and opening financial markets.

So far, in the EU this targeted regulation has been limited to the banking payments sector.

---

[24] PricewaterhouseCoopers, *Is it time for consumer lending to go social?*, February 2015, at https://www.pwc.lu/en/fintech/docs/pwc-fintech-time-for-consumer-lending-to-go-social.pdf

[25] ZETZSCHE, BUCKLEY, ARNER and BARBERIS, *From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance*, 2017, EBI Working Paper Series n. 6; MALVAGNA and SCIARRONE ALIBRANDI A (edited by), *Sistema Produttivo e Finanziario Post COVID-19: dall'Efficienza alla Sostenibilità*, 2011, Pacini Giuridica.

[26] EUROPEAN COMMISSION, *Towards an integrated European market for card, Internet and mobile payments*, COM (2011) 941 final. See also COLANGELO and BORGOGNO, *Data, Innovation and Transatlantic Competition in Finance: The Case of the Access to Account Rule*', European Business Law Review, 31, 2020, p 573.

[27] EUROPEAN COMMISSION, *Commission staff working document Impact Assessment accompanying the Proposal for a directive on payment service in the internal market*, SWD (2013) 288 final; EUROPEAN CENTRAL BANK, Financial Stability Review – Special Feature, 2016, at https://www.ecb.europa.eu/pub/pdf/fsr/financialstabilityreview201611.en.pdf; UK COMPETITION AND MARKET AUTHORITY, *The Retail Banking Market Investigation Order 2017*, 2017, at https://www.gov.uk/government/publications/retail-banking-market-investigation-order-2017; THE NETHERLANDS AUTHORITY FOR CONSUMERS AND MARKETS, *Barriers to entry into the Dutch retail banking sector*, 2014, at https://www.acm.nl/sites/default/files/old_ publication/ publicaties/13257_barriers-to-entry-into-the-dutch-retail-banking-sector.pdf.

[28] EUROPEAN BANKING AUTHORITY, *Discussion Paper on the EBA's approach to financial technology (FinTech), EBA/DP/2017/02*, 4 August 2017.

As the data business permeates the global economy, banking and electronic payment services represent a frontier very exposed to competitive pressures from the infant fintech industry. For some time, payments have been characterised by electronic fund transfer systems having gone through the transition from paper payment services (e.g. cash, bank cheques, traveller's cheques, etc.) to electronic means. In the digital economy, payment accounts and data have become an essential source from which services can be provided, not only by banks but also by new market players capable of extracting value from them competitively.[29]

The thrust towards innovation and competition in a market traditionally dominated by the banking sector has motivated the substantial revision and reordering of the regime formerly established by the foregoing Payment Services Directive ('PSD1').[30] The late legislative intervention of the Payment Services Directive 2 ('PSD2')[31] has modernised the regulation of payment transactions and consumer protection to the changing needs brought by digitalisation.[32] It intervenes in the single payments market enabling a new banking model called 'Open Banking'.

Open Banking is not a technology-based concept but one of legal derivation. This model refers to the obligation under the PSD2 for banks to open access to their customers' payment accounts, banking transactions, and other financial data using interoperable interfaces ('Application Programming Interfaces') to third-party service providers ('TPP'). The PSD2 lays down the normative terms for the achievement of

[29] MAVROMATI, *The Law of Payment Services in the EU: The EC Directive on Payment Services in the Internal Market*, 2008, Alphen aan den Rijn: Kluwer Law International; JANCZUK-GORYWODA, *Evolution of EU Retail Payments Law*, European Law Review, 40, 2015, p 858; GRIMIGLIANO, *The Lights and Shadows of the EU law on Payment Transactions*. In *Money, Payment Systems and the European Union*, 2016, Cambridge: Cambridge Scholars Publishing, p 25; VARDI, *Regulation of Payments after the PSD: Is there still a Role for Domestic Law*. In G *Money, Payment Systems and the European Union*, 2016, Cambridge: Cambridge Scholars Publishing, p 39.

[30] Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC, OJ L 319, 5.12.2007, 1–36.

[31] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, OJ L 337, 23.12.2015, 35–127.

[32] See, in particular, Recital 95 PSD2.

integrated retail payments in the EU that are inclusive of existing and new payment services delivered by new market players. Its ambitious goal is to take advantage of innovative technology-enabled solutions (fintech) to generate efficiencies and reach a broader market with more choice and integrated services. At the same time, it aims to pursue transparency and consumer protection.[33]

Thus, regulation has not just allowed, but it has mandated data access and sharing to develop a novel market model in the area of payments, in which traditional banking meets and is transformed by the data economy and the competition of innovative fintech firms. Mandating data access and sharing through regulation, the EU shifts the single market approach towards digitalisation and competition. Customers are required to grant consent to let the bank allow such access. Third-party providers can then use the customer's shared data. So doing, this model breaks the concentration of information in traditional banks, and allows the networking of accounts and data across a novel sector made of traditional and new service providers. Fresh competition is created for a more efficient provision of existing services, as well as the development of new ones.[34]

Examples are new methods of mobile payments or the delivery of complimentary personalised financial services such as financial advice, loans, insurance products. New uses may include comparing the customer's accounts and transaction history to a range of financial service options, aggregating data to create marketing profiles, or making new transactions and account changes on the customer's behalf. Shared data can facilitate the process of switching from using one bank's account to another bank's account. Financial service providers can look at

[33] Recital 6, PSD2.

[34] On Open Banking see e.g. COLANGELO and BORGOGNO, *Data, Innovation and Transatlantic Competition in Finance: The Case of the Access to Account Rule*', cit.; EUROPEAN BANKING AUTHORITY, *Discussion Paper on innovative uses of consumer data by financial institutions*, *EBA/DP/2016/01* (4 May 2016); RABITTI and SCIARRONE ALIBRANDI, *I servizi di pagamento tra PSD2 e GDPR: Open Banking e conseguenze per la clientela*, in *Liber Amicorum Guido Alpa*, 2019, CEDAM, p 711; CIRAOLO, *Open Banking, Open Problems. Aspetti controversi del nuovo modello dei "sistemi bancari aperti"*, Rivista di Diritto Bancario, IV, 2020, p 611.

consumers' transaction data to identify the best financial products and services for them, such as new accounts that would earn a higher interest rate than the current account or different credit cards with a lower interest rate. Providers may get a more accurate picture of a consumer's financial situation and risk level to offer more profitable financial terms. New services may help consumers get a more accurate picture of their own finances before taking on debt or other financial services.

Broadly, the PSD2 operates on two interrelated levels.

At first, it intervenes in the establishment, authorisation, and supervision of payment firms and the regulation of payment transactions. Adjusting to the digital market, it enlarges the scope of coverage of the law, it clarifies the extent of consumer rights and service provider obligations, and it reinforces security and authentication requirements.[35]

Next, it recognises and regulates those TPP emerging from new fintech realties in payment services, bringing them under the same harmonised standards, requirements, and obligations on an equal footing with the traditional payment providers regardless of the business model they apply.[36] Introducing the so-called 'access to account rule', it opens the market to new services by granting TPP access to the customers' payment accounts held in the banks. The latter must allow TPP authorised by the competent authority in their home Member State[37] access to the data contained in payment accounts in real time on a non-discriminatory basis.[38] By accessing and exploiting the large quantity of real-time data of the banking realm, technology firms have started disrupting retail financial markets.[39]

[35] See the various provisions of Titles II, III and IV of the PSD2.
[36] Recitals 27-33 PSD2.
[37] Art. 36 PSD2.
[38] Art. 64 to 68 PSD2.
[39] BORGOGNO and COLANGELO, *The data sharing paradox: BigTechs in Finance*, European Competition Journal, 16, 2020, p 492; BORGOGNO and COLANGELO, *Consumer Inertia and Competition-sensitive Data Governance: The Case of Open Banking*', Journal of European Consumer and Market Law 4, 2020, 143; DI PORTO and GHIDINI, *I access your data, you access mine. Requiring data reciprocity in payment services*, IIC - International Review of Intellectual Property and Competition Law, 51, 2020, p 307.

The 'access to account rule' has therefore become the tool to unlock the data power of banks over innovative fintech firms. Access by TPP is to 'payment accounts' only, defined as accounts "held in the name of one or more payment service users *(…)* used for the execution of payment transactions".[40] Savings accounts and other non-payment accounts seem therefore excluded from the application of the PSD2.[41]. Access to payment accounts shall take place in a secure way under the guidelines laid down by the European Banking Authority.[42] Any access may occur only upon conclusion of a contractual relationship between the account holder and a TPP, unusually framed as 'explicit consent' by the PSD2, precisely for the purpose of providing those kinds of services that need the data contained in the account.[43] Under the PSD2, TPP are subject to conduct of business restrictions and requirements that do not allow them to hold the payer's funds in connection with the service, store sensitive payment data of the service user, or process data beyond that necessary to provide the service.[44]

These provisions have given rise to a market model that shifts from the money business to the data business and vice versa, where account data are shared with new market players of the fintech industry capable of capturing or creating value

[40] Art. 4(12) PSD2.

[41] This circumstance also finds support in Case C-191/17, *Bundeskammer für Arbeiter und Angestellte v ING-DiBa Direktbank Austria Niederlassung der ING-DiBa AG* [2018] EU:C:2018:809 where the Court confirmed that accounts which allow for sums deposited without notice and from which payment and withdrawal transactions may be made solely by means of a current account do not come within the concept of payment account.

[42] Art.95 PSD2, followed by European Banking Authority, *Final draft RTS on SCA and CSC under PSD2 (EBA-RTS-2017-02)* (23 February 2017); Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication C/2017/7782, OJ L 69, 13.3.2018, p. 23–43; EUROPEAN BANKING AUTHORITY, *Opinion of the European Banking Authority on the implementation of the RTS on SCA and CSC (EBA-Op-2018-04)*, 13 June 2018.

[43] For Payment Initiation Services, see Art. 66 PSD2, stating that "when the payer gives its explicit consent for a payment to be executed and (*omissis*)"; for Account Information Services, see Art. 67 PSD2 providing that "the account information service provider shall: (a) provide services only where based on the payment service user's explicit consent; (*omissis*)".

[44] Art. 66(3) PSD2.

around existing un- or under-exploited assets.[45]

In the Open Banking model, therefore, the new paradigm reflects the unbundling of the provision of financial services in more market segments, and the disintermediation of the banking industry. The latter, however, becomes key in the Open Banking ecosystem, assuming a new form of forced intermediation between the service user (the account holder) and the fintech TPP. The services can only exist via the traditional providers, creating a new market structure where the latter become digital platforms for the distribution of financial services. They facilitate and create a dependency for the contractual interactions of two or more market agents, but without having any contractual relationship with one of them (the TPP), at the same time allowing the other one (the customers) to continue the fruition of their own services.

The Open Banking environment thus generates indirect network effects, making possible bilateral ventures otherwise not attainable with other means,[46] at the same time producing new dependencies.

In this way, the Open Banking market structure moves towards a confluence between traditional financial service providers becoming technological firms (but still on the money business) and technological firms entering the financial services market, where the latter may be infant fintech businesses or established technological giants already dominating the data service market (the so-called 'Tech-Fin' or 'Big-Tech').[47]

---

[45] CHESBROUGH, *Business Model Innovation: Opportunities and Barriers*, Long Range Planning, 43, 2010, p 354.

[46] ZACHARIADIS and OZCAN, *The API economy and digital transformation in financial services: the case of Open Banking*, SWIFT Institute Working Paper No. 2016-001, at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2975199; MILANESI, *A new banking paradigm: the state of Open Banking in Europe, the United Kingdom and the United States*, TTLF Working Papers No. 29, Stanford-Vienna Transatlantic Technology Law Forum, 2017, from https://law.stanford.edu/publications/a-new-banking-paradigm-the-state-of-open-banking-in-europe-the-united-kingdom-and-the-united-states/

[47] ZETZSCHE D ET AL, *EBI Working Paper Series n. 6*, 2017; DI PORTO and GHIDINI, *I access your data, you access mine. Requiring data reciprocity in payment services*, cit.; STULZ, *FinTech, BigTech, and the future of banks*', NBER Working Paper No. 26312, 2019, at https://www.

From this angle, the PSD2 is the law that encourages an expanding use of personal data and enables a vast array of newcomers to access increasingly more data sources for novel purposes.

True, payment accounts contain a vast amount of data for analysis, from financial data relating to incoming and outgoing transactions, balances, preferences, patterns, dependencies, behaviours, aspects of the social life, etc. They can be an exceptional tool for consumer profiling and predictive purposes. At the same time, however, they can also reveal behavioural biases and vulnerabilities in all aspects of consumers' life, especially if integrated with data from other unrelated sources and processed by algorithms powered by artificial intelligence technologies.

4. Following the opportunity provided by the PSD2 of opening-up bank account data for TPP access, the EU legislator plans to extend the Open Banking model gradually in a transition to data-driven finance to a broader range of financial services. As part of the priorities of the Digital Finance Strategy to promote data-driven innovation in finance, the EU aims to establish a common financial data space through a number of more specific measures.[48] Of relevance here is the priority to create enhanced data sharing and access to, and reuse of, data in the financial sector paving the way to 'Open Finance'.

Upon enabling legislation, Open Finance will be the next step in the evolution of Open Banking, whose reach becomes expanded by empowering consumers with further control over their data and granting TPP access to more data sources for a wider range of financial services such as savings, mortgages, consumer credit,

---

nber.org/papers/w26312. For example, note that Google has secured an e-money license after Lithuania granted authorisation. The license enables the company to process payments, issue e-money, and handle electronic money wallets. It gives permission to operate across the EU via the passporting rights system. Likewise, Facebook and Amazon obtained licenses in Ireland and Luxembourg. See SEPUTYTE and KAHN, *Google Payment Expands With E-Money License From Lithuania*, Bloomberg, 21 December 2018, at https://www.bloomberg.com/news/articles/2018-12-21/google-payment-expands-with-e-money-license-from-lithuania.

[48] Digital Finance Strategy, cit.

investments, pensions, insurance, financial advice, etc. It extends the delivery of digital financial services via interoperable interfaces, creating new fintech industries, and developing further service disintermediation and new forms of data intermediation. With Open Finance it is created a networked system that is no longer limited to payment services but that relies on the ability to leverage a broad range of financial institutions' infrastructures to provide a financial service that the provider does not offer to consumers outside of its existing footprint.

As for Open Banking, the key element to enable Open Finance is the regulation to be implemented.

4.1.The starting point about the nature of a legislative framework for Open Finance is rooted in the consolidation and extension of Open Banking-like legislation, as well as overlapping legislation relating to data.

As a consumer-centric business model, from the angle of consumer protection the most important building block of Open Finance is that of consumers' control of the data pertaining to them.

Consumer financial data processing triggers the application of the GDPR, thus overlapping with a PSD2-like and creating a legal environment where financial regulation and data regulation blend. Therefore, the question of whether this blended regulation is robust enough to foster a transition to Open Finance becomes essential.

As a EU Regulation, the GDPR has direct effect designed to eliminate risks of national particularities and diversity of practices, which would frustrate the goal of achieving uniformity.

Prima facie the principal purposes of the PSD2 model and the GDPR are in contrast one another, with the former endorsing the stimulus for expansive data sharing, whilst the latter protecting and restricting the freedom to share them.

In the absence of derogations, it is in light of the significance of data

protection legislation that one should read the processing of big data in financial services, including data in Open Finance.[49]

The GDPR formulates the conditions under which data processing is legitimate.

Among the many aspects regulated by the GDPR, some require attention for their overlap with the PSD2 model.

Within the respect of the key principles of purpose limitation and data minimisation,[50] the GDPR sets the legal requirements for a valid basis for legitimate data processing. A data controller must be able to provide a base for the processing activity only if it can claim that the processing relies on one of the criteria established by the law.[51] The set of criteria is exhaustive, so that if a data controller is unable to rely on one of them the processing is unlawful. Financial data are considered of non-sensitive nature.[52]

For Open Finance, the relevant legal bases for a legitimate processing under Article 6 GDPR are in principle that the data subject has unambiguously given consent or that the data processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering a contract. The complications surrounding the choice between the two legal bases will be discussed in the next Section.

Moreover, in the case at study fintech solutions make an extensive use of profiling techniques which constitute the business model. Where profiling occurs, the GDPR requires for an additional layer of control. It postulates that individuals have the right not to be subject to a decision based solely on automated processing to

[49] See also Recital 90 PSD2.
[50] See Art. 5 GDPR, in particular where it states "personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes" (purpose limitation) and "personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" (data minimisation).
[51] Art. 6 GDPR.
[52] This is so as they are not included in the exhaustive list of sensitive data of Art. 9(1) GDPR.

evaluate certain personal aspects of a person.[53] Profiling can be used if it is necessary for contractual necessity, it is authorised by EU or national law, or it is based on the data subject's 'explicit consent'. In the case of automated decisions based on 'explicit consent' or contractual fulfilment, controllers must respect a right for data subjects to obtain human intervention, express their point of view, and contest decisions.[54]

Another important provision of the GDPR to empower data subjects is the right to data portability, i.e. their right to transmit or have the data transmitted to another controller where the processing is based on the legal bases of 'consent' or on a contract.[55] Consent and contract necessity are only two of the grounds for lawful data processing as per Article 6 GDPR. The processing grounds of compliance with a legal obligation, protection of vital interests, the performance of a task carried out in the public interest, and the pursuit of legitimate interests of data controllers or third parties are therefore excluded from the data portability right. This narrow scope of the right is further restricted to data which data subjects have provided themselves to the data controller—so-called volunteered data. The scope of the provision includes active observation of the data but excludes derived or inferred data, or anything resulting from the analysis of the data.[56]

From these norms of the GDPR related to the PSD2 model, it emerges that in principle the two laws are not necessarily in conflict - as it may have *prima facie* appeared – since they both aim to grant transparency and user control.

However, inconsistencies arise from their cohabitation and coordination, starting from the legal basis legitimising the use of relevant financial data and the ensuing rights and obligations of the parties.

The leitmotiv of 'consent' in the two laws has already triggered discussions and uncertainties within Member States and stakeholders regarding the correct

[53] Art. 4(4) GDPR.
[54] Art. 22 GDPR.
[55] Art. 20 GDPR.
[56] ARTICLE 29 WORKING PARTY, *Guidelines on the right to data portability*, Adopted on 13 December 2016, last Revised and adopted on 5 April 2017.

implementation of the PSD2, especially in relation to measures concerning the protection of personal data.[57]

As far as data protection is concerned, Article 94(2) PSD2 stipulates that "payment service providers shall only *access*, *process and retain* personal data necessary for the provision of their payment services, with the *explicit consent* of the payment service user" (emphasis added). Moreover, other provisions of the PSD2 refer to 'consent' as regards authorisation of a payment transaction. Under Article 64 PSD2 "a payment transaction is considered to be authorised only if the payer has given *consent to execute the payment transaction*" (emphasis added). This 'consent' to authorise a payment is later referred as 'explicit consent' in Articles 65 and 66 PSD2 when specifying the actions that banks need to perform to ensure the payer's right to use a Payment Initiation Service[58] or an Account Information Service.[59] Arguably, the 'consent' referred in these provisions do not relate to access or processing of data but to the authorisation of a service. It signifies contractual agreement albeit equivocally normed as 'explicit consent' in the realm of contract law.

4.2. In the thrust towards innovation and competition, the European Commission has recently unveiled a proposal for a Regulation on fair access to and use of data, the so-called 'Data Act' (or 'Proposal')[60] pursuant to the European strategy for data.[61]

The Proposal addresses market concentration and it has the aim of ensuring

[57] See e.g. EUROPEAN DATA PROTECTION BOARD, *Letter to Sophie in 't Veld, Member of the European Parliament*, 5 July 2018; BEUC, *Consumer-Friendly Open Banking*, 20 September 2018; EUROPEAN BANKING FEDERATION, *European Banking Federation's comments on the Article 29 Working Party guidelines on consent* (wp259), 23 January 2018.
[58] Art. 66 PSD2.
[59] Art. 67 PSD2.
[60] European Commission, Proposal for a Regulation of the European Parliament and of the Council on Harmonised Rules on Fair Access to and Use of Data (Data Act), COM/2022/68 final.
[61] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European Strategy for Data, COM/2020/66 final.

fairness in the allocation of value from data and foster access to and use of data, creating a horizontal cross-sectoral governance framework. To achieve its goal, it ensures that a wider range of stakeholders gain availability of more data for innovative uses.

Of relevance here are the generalised rules on making data generated using a product or service mandatorily available to their users.[62] Products shall be created, and services provided, in such a manner that by default data generated by their use are easily, securely and directly accessible to the users.[63] When users wish to transfer these data to other providers, the data holders need to ensure that the data are shared transparently in fair, reasonable and non-discriminatory conditions.[64] To do so, the Proposal prohibits unfair contracts relating to data-related obligations and introduces a new unfairness test to protect weaker commercial parties such as SMEs.[65] The sharing may occur only upon request by users.[66] This requirement accords to them a portability right, extending the portability right already conferred to data subjects by Article 20 GDPR (above). This new extended portability right grants users the right to access and make available to third parties to any data irrespective of their nature as personal or non-personal, of the distinction between 'actually provided' or 'passively observed' data, and of the limited legal basis of the processing under Article 20 GDPR. Moreover, unlike the GDPR that reduces the reach of the right by providing that controllers may transfer data where it is 'technically feasible', the Proposal mandates such a technical feasibility.[67]

As a horizontal proposal, the Data Act envisages the above basic rules for all sectors as regards the rights to use data, but it leaves to vertical legislation the establishment of more detailed rules for the achievement of sector-specific

[62] Art 1 Data Act.
[63] Art 3 Data Act.
[64] Art 8 Data Act.
[65] Art 13 Data Act.
[66] Art 5 Data Act.
[67] Art.5 See also Recital 31 Data Act.

regulatory objectives. For Open Finance, therefore, it will not yet introduce new data access rights in the financial sector, but it hints at a subsequent legislative vertical initiative aligned with the horizontal principles provided by the Data Act.[68] The anticipated review of the PSD2[69] and future framework for Open Finance would need to converge with the horizontal rules of the Data Act, provided that the latter will be confirmed through the EU legislative process.

In any event, the provisions of the Data Act on the binding nature of data transfer clearly generalise the mandatory data sharing already adopted by the PSD2 upon consent of the customer.

As a consumer-centric initiative focusing on consumer empowerment, therefore, the key questions remain whether the PSD2 model and the Data Act are robust enough for consumer protection beyond the alleged benefits of Open Finance, and what the risks for consumers are.

4.3. While in the EU the PSD2 enabled Open Banking contemplating both retail and corporate banks, in the UK the Competition and Market Authority ('CMA') launched it by first mandating to the country's nine largest banks only to open to TPP regulated by the Financial Conduct Authority ('FCA'), and providing standardised rules subject to the consent of their customers.[70] Through this experience it has led the public debate on Open Finance and the set-up of an advisory group to drive forward the strategy for its implementation.[71]

The UK approach is grounded on principles and conduct of business rules,

[68] Data Act, explanatory memorandum p. 5.
[69] European Commission, Consultation Document Targeted Consultation on the Review of the Revised Payment Services Directive PSD2,(2022), available at https://finance.ec.europa.eu/regulation-and-supervision/consultations/finance-2022-psd2-review_en.
[70] COMPETITION AND MARKET AUTHORITY, Retail Banking Market Investigation Order 2017, at https://assets.publishing.service.gov.uk/media/5893063bed915d06e1000000/retail-banking-market-investigation-order-2017.pdf.
[71] FINANCIAL CONDUCT AUTHORITY, *Business Plan 2019/20*, 2019, at https://www.fca.org.uk/publication/business-plans/business-plan-2019-20.pdf;
FINANCIAL CONDUCT AUTHORITY, *Advisory Group on open finance*, at https://www.fca.org.uk/firms/adv isory-group-open-finance.

where the latter are best seen to adapt to the specific mechanisms of Open Finance.

In the draft principles of Open Finance, it has been set out that regulation would be needed to ensure that consumers are protected, data is used ethically and in a way that they have consented to and expect, and that liability is clear and effective redress ensured when problems occur.

To achieve the goals, the debate focuses on TPPs being authorised and held to appropriate standards. They should be subject to appropriate threshold conditions on financial resources, appropriate systems and controls, operational resilience requirements and security architecture. Regulation of TPPs and their activities emerges in the public debate to ensure consumers do not face a patchwork of regulated and unregulated activities, which could also help ensure that consumers have access to the Financial Ombudsman Service when needed. Concerns are express with regard to the UK data protection legislation. Accordingly, the UK GDPR is not considered to be designed and adequate to support a full Open Finance framework. Therefore, any new regulation needs to work with UK GDPR.[72] The Information Commissioner's Office (ICO) itself agrees that the UK GDPR applies to the general process of personal data rather than providing for any specific sector. To the extent that the UK GDPR proves insufficient, therefore, the approach is that any additional regulation should be focused on the specific mechanisms of Open Finance.[73]

Hence, the general theme in the UK differs from the EU debate in that the experience of Open Banking should be the starting point in terms of liability, data rights, standards and ethics. At the same time, however, the specific risks in each financial sector should be considered and integrated in the regulation of Open Finance. From this perspective, additional layers of consumer protection are needed in the form of conduct of business rules.

---

[72] FINANCIAL CONDUCT AUTHORITY, *Open Finance*, *Feedback Statement FS21/7*, March 2021, at https://www.fca.org.uk/publication/feedback/fs21-7.pdf

[73] INFORMATION COMMISSIONER'S OFFICE, *The Information Commissioner's response to the Financial Conduct Authority's call for input on open finance*, 2020, at https://ico.org.uk/media/about-the-ico/consultation-responses/2617565/ico-response-fca-open-finance-20200313.pdf

5.

5.1. As noted, Open Finance is meant to be customer-centric and rest on consumers' control of the data.

It is therefore essential to determine what is the legal basis for data processing, and how consumers are empowered and remain effectively in control.

Under the PSD2 it is already unclear whether the processing of account data finds its legal basis in the contractual necessity under Article 6(1)(b) GDPR or though the consent of the customer under Article 6(1)(a) GDPR.

Article 94(2) PSD2, under Chapter 4 titled "data protection", stipulates that "payment service providers shall only *access*, *process and retain* personal data necessary for the provision of their payment services, with the *explicit consent* of the payment service user" (emphasis added). In so doing, the PSD2 seems to qualify the basis for processing account data with 'explicit consent'. However, the EDPB in a letter addressed to a European Member of Parliament (i.e. not laid down in the form of official guidelines) considers the 'explicit consent' of Article 94(2) PSD2 as contractual consent, thus not interfering with contractual necessity. According to the Authority,

"article 94(2) of PSD2 should be interpreted in the sense that when entering a contract with a payment service provider under PSD2, data subjects must be made fully aware of the purposes for which their personal data will be processed and have to explicitly agree to these clauses. *Such clauses should be clearly distinguishable from the other matters dealt with in the contract* and would need to be *explicitly accepted by the data subject*. The concept of explicit consent under Article 94(2) of PSD2 is therefore *an additional requirement of a contractual nature and is therefore not the same as (explicit) consent under the GDPR*"[74] (emphasis added).

Arguably, holding the 'explicit consent' as contractual would not explain why it

[74] EUROPEAN DATA PROTECTION BOARD, *Letter to Sophie in 't Veld, Member of the European Parliament*, cit.

has been expressed in the norm addressing data protection under a separate dedicated heading of the PSD2. In addition, this interpretation not only would dispute the letter of the norm where it affirms that 'explicit consent' is required for the access, processing and retention only to the extent necessary for the provision of the services, but it would also overlap with the contractual meaning of 'consent' used in Articles 64-67 PSD2. These other provisions of the PSD2 refer to 'consent' as regards authorisation of a payment transaction. Under Article 64 PSD2 "a payment transaction is considered to be authorised only if the payer has given *consent to execute the payment transaction*" (emphasis added). This simple 'consent' to authorise a payment is later referred as 'explicit consent' in Articles 65 and 66 PSD2 when specifying the actions that banks need to perform to ensure the payer's right to use a PIS.[75] Equally, AIS "shall provide services only where based on the payment service user's *explicit consent*".[76] (emphasis added). The 'consent' and 'explicit consent' referred in these provisions do not relate to access or processing of data but to the authorisation of a PIS or AIS service. It signifies contractual agreement albeit equivocally normed in the 'simple' versus 'explicit' dichotomy in the realm of contract law.

Likewise, the Data Act is silent on the legal basis for data processing, referring to a "request" by the user.[77] Where such user is not a data subject, the Data Act makes express reference to "a valid legal basis under Article 6(1)" of the GDPR.[78] True, the Data Act is meant to complement and be without prejudice to the GDPR,[79] although it would be clearer and desirable if it explicitly and unequivocally specified that in case of conflict between the two the provisions of the GDPR should prevail.[80]

[75] Art. 66 PSD2.
[76] Art. 67 PSD2.
[77] Articles 4 and 5 Data Act; Recital 31 Data Act.
[78] Article 4 Data Act.
[79] Article 1(3) Data Act; Recital 7 Data Act.
[80] This is to avoid risks of interpretation regarding e.g. the special law vs general law or posterior vs anterior law relationship between the two. See also EDPB-EDPS, *Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on Harmonised Rules on Fair Access to and Use of Data (Data Act)*, 4 May 2022, p 10.

At any rate, the legal uncertainty over the use of 'consent' or 'contractual necessity' remains. Either way, moreover, both legal bases for data processing could be problematic to ensure consumer control in an Open Finance ecosystem.

5.1.1. The legal basis of contractual necessity needs to be considered in the context of the obligations of purpose limitation and data minimisation laid down by the GDPR. Data needs to be as little as possible and they must be collected for specified, explicit and legitimate purposes. They should not be further processed in a manner that is incompatible with the initial purposes.[81] These requirements already pose some problems as to their suitability with Open Finance, since the data were originally collected under a different set of contracts in different product lines.

At any rate, data processing must be objectively "necessary" for the performance of the contract or for taking steps prior to entering into a contract. It is established case-law that the requirement of 'necessity' does not equates to what is permitted by or written into the terms of a contract, especially consumer contracts that typically are not negotiated on an individual basis.[82] Instead, the assessment needs to be fact-based vis-à-vis the objective pursued. If there are other realistic less intrusive alternatives the processing is not necessary. Therefore, it does not include processing which is useful but not objectively necessary.[83]

Contractual necessity must be interpreted strictly with particular regard to the aim, purpose or objective of the product or service. A controller needs to be able to demonstrate how the main subject-matter of the specific contract with the data subject cannot, as a matter of fact, be performed without the processing.[84] Moreover, where contracts consist of separate services or options that can be

[81] Article 5(1)(b) and (c).
[82] Case *Heinz Huber v Bundesrepublik Deutschland* (C-524/06) ECLI:EU:C:2008:724.
[83] Joined cases *Volker und Markus Schecke GbR* (C-92/09) and *Hartmut Eifert* (C-93/09) *v Land Hessen* ECLI:EU:C:2010:662.
[84] EUROPEAN DATA PROTECTION BOARD, *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*, 16 October 2019.

performed independently of one another, the applicability of contractual necessity needs to be assessed in the context of each of those services or options separately.[85] Crucially, if a processing is necessary for the controller's business model but not for the strict provision of the service, the requirement of contractual necessity cannot be satisfied but other legal bases must be used.[86]

Within the Open Finance ecosystem in particular, and with big data generally, all data would become 'necessary' but it is doubtful the extent to which such a necessity is for the objective delivery of the service rather than the providers' business models. Arguably, the boundaries are blurred but the suspicion is that in many cases the processing leans more towards the satisfaction of the needs of new business models. In most instances, the primary roles and functions of financial services remain the same, but the way they are undertaken is changing —payments still need to be made, loans granted, savings and investments made, etc. Those specific activities still need to be undertaken as ever and do not change. What changes is how these activities are carried out and the roles undertaken by the providers. Moreover, it has to be reminded that most of the data processing for the provision of Open Finance services rests on correlations, not on causation.

Arguably, in conclusion, contractual necessity may be a lawful basis for processing on occasions to be verified case-by-case but hardly as the one of general applicability.

5.1.2. Consent under the GDPR is probably one of the most complicated lawful bases to implement,[87] and the addition of Article 94(2) PSD2 does not help.

[85] *Ibid* p. 11.
[86] *Ibid*.
[87] Exemplified by the many interpretative interventions of the supervisory authority for data protection, the European Data Protection Board – 'EDPB' (formerly, Article 29 Working Party): ARTICLE 29 WORKING PARTY, *Opinion 15/2011 on the Definition of Consent*, 01197/11/ENWP187, July 13, 2011; ARTICLE 29 WORKING PARTY, *Article 29 Working Party Guidelines on consent under Regulation 2016/679* , Adopted on 28 November 2017, and last Revised and adopted on 10 April 2018; EUROPEAN DATA PROTECTION BOARD, *Guidelines 05/2020 on consent under Regulation 2016/679*, 4 May 2020.

As conceived by data protection law, it is a key element that permits the processing of personal data by data controllers that would otherwise be forbidden. When a data subject gives valid consent, data controllers are released from the restrictions provided by law. The processing becomes lawful from the moment consent is unambiguously expressed.

By law, consent shall be granular and distinguished from declarations concerning other matters (Article 7[2] GDPR). It must be "freely given, specific, informed and unambiguous" (Article 4[11] GDPR). Correspondingly, the law mandates 'affirmative consent' requiring the data subject to signal agreement by "a statement or a clear affirmative action" (Article 4[11] GDPR). At the same time, it continues to distinguish between 'explicit consent' if the data in question is sensitive personal data, and 'unambiguous' consent for all the other personal data (Article 6 GDPR combined with Article 4 GDPR).

The issue of what standard of consent should apply under the GDPR was the subject-matter of intense debates and negotiations at the lengthy proposal stage of the GDPR. The legislative history of the GDPR demonstrates that the final drafting was intentional in maintaining different qualifiers of consent and making the express distinction between 'unambiguous' and 'explicit' consent depending on the ordinary or sensitive nature of the data. To the extent that the GDPR makes clear that 'explicit' and 'unambiguous' consent are not the same, the boundaries of what is 'unambiguous' remain unclear, with the additional complication that the law states that it must be given by an 'affirmative action'. For example, it is unclear to what extent implied consent remains possible.[88] While the GDPR provides that "silence, pre-ticked boxes or inactivity should not *(omissis)* constitute consent" (Recital 32 GDPR), it also states that consent can be given through "another statement or conduct which clearly indicates in this context the data subject's acceptance of the

[88] In this regard, the latest 2020 opinion of the EDPB does not help much, limiting their interpretation to "all presumed consents that were based on a more implied form of action by the data subject (e.g. a pre-ticked opt-in box) will also not be apt to the GDPR standard of consent". See EUROPEAN DATA PROTECTION BOARD, *Guidelines 05/2020 on consent under Regulation 2016/679*, cit., p 20.

proposed processing of his or her personal data" (Recital 32 GDPR). In any event, controllers must be able to demonstrate that data subjects have consented (Article 7 GDPR).

The distinction between 'explicit' and 'unambiguous' consent matters in practice as long as different models of consent translate into very different engineered solutions within financial products and services, especially online. In the 'explicit' consent model an opt-in tick box or declaratory consent statement will be necessary. However, in the 'unambiguous' consent model that dominates commercial services a prominent notice together with an 'affirmative action' may suffice to obtain an implied consent without the need for an opt-in box or declaratory consent.

In the consumer protection realm, this can make a substantial difference in terms of the way consent is collected from consumers or the interface presented to them, and the way in which they interact with the product or service provider.

Ultimately, this also makes a difference as to the real knowledge and control that consumers may have on the processing of their personal data, and the uses that can be made with the data. Consent must rely on transparency and an 'affirmative action' (whether explicitly given or inferred through conduct) but how this translates in practice remains vague, especially in the context of Open Finance and within the complexities of financial transactions.

It needs to be added that the GDPR establishes explicitly that data subjects have a subsequent right of withdrawal of consent. The data subject may withdraw consent at any time and this must be as practical as granting consent. Clearly, however, the withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal (Art. 7(3) GDPR).

The complexities of the Fintech business models, data-collection practices, vendor-customer relationships, or technological applications may make it impossible for consumers to understand what they are consenting. Equally, these complexities

may in practice render consumers unable to freely and actively decide to accept the consequences of consenting to data processing, particularly when faced with a perceived immediate economic benefit.

Despite the apparently robust legal protection afforded to data subjects, consent may be obtained by a number of methods and has proved problematic as a basis for data processing because it can be easily abused, confused, or conflated.[89]

Treating consent as a transactional moment using standard form agreements may constitute a mechanical or perfunctory means of obtaining overarching consent for data processing.[90]

For instance, the condition of consent in the provision of financial services is a common yet elusive method of obtaining consumer consent. Consent becomes associated with the legal paradigm of contract. At the same time, the contractual relationship is a situation with a typical imbalance between the consumer and the business counterpart. Consumers are presented with no much choice but to abide by the lenders' terms if they wish to receive a service. In practice, the consumer's consent becomes either mandatory or assumed. Open Finance is based on data exploitation. As seen above, the PSD2 names contractual consent and data processing consent in the same way ('explicit consent'), albeit in two different Articles and contexts.[91]

The legal mechanism of consent becomes more confused where the GDPR further intends to protect data subjects stating that 'consent' should not be regarded as freely given if they are "unable to refuse or withdraw consent without detriment"

[89] In theory, consent that does not meet the requirements of the law or is vitiated should be regarded as void, and should invalidate all data processing *ex tunc*—from the outset. See ARTICLE 29 WORKING PARTY, *Article 29 Working Party Guidelines on consent under Regulation 2016/679*, Adopted on 28 November 2017, and last Revised and adopted on 10 April 2018. For specific literature see e.g. MANTELERO, *The future of consumer data protection in the EU. Re-thinking the 'notice and consent' paradigm in the new era of predictive analytics*, Computer Law and Security Review, 30, 2014, p 643; KOSTA, *Consent in European Data Protection Law*, 2013, Martinus Nijhoff.

[90] BROWNSWORD, *Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality*. In *Reinventing Data Protection?*, 2009, Springer, p 83.

[91] Articles 64-67 PSD2 and Article 94 PSD2.

(Recital 42 GDPR) or "where there is a clear imbalance between the data subject and the controller" (Recital 43 GDPR). Recent studies show that in order to gain specific transactional and personal advantages most consumers willingly consent or disclose information about themselves and their social activities without thinking about the effects of their disclosures, thus making consent *de facto* ineffective. Yet very few consumers understand the significant consequences of this trade-off, including how data controllers use their personal data. Not only data processing can be very complex and non-transparent, but most consumers lack both the information and the skills to properly evaluate their own decision to consent.[92]

In the end, under the discussed legal uncertainties it remains unclear how the aspirations of placing consumers in control can be effectively reconciled with the reality of Open Finance.

5.2. It has to be reminded that the expanded data processing is mostly done in the interest of the financial services industry to enlarge the customer base, minimise risks, and increase profitability. True, these elements may coincide with product innovation. At the same time, these interests may not necessarily coincide with the provision of suitable products in the interest of consumers in terms of provision of financial services at affordable costs to those who really need and qualify for them.

Open Finance relies on enhanced data sharing for personalisation and profiling purposes. Personalisation relies on profiling. The latter is about prediction, which is not the same as knowledge. Unlike knowledge, it is not neutral and it is used to determine the future. Therefore, the risk is that Open Finance will create a more

[92] PASQUALE, *The Black Box Society*, 2015 Harvard University Press; PEPPET, *Unraveling Privacy: The Personal Prospectus and the Threat of a Full Disclosure Future*, Northwestern University Law Review, 105(3), 2011, p 1153; BORGHI, FERRETTI and KARAPAPA, *Online Data Processing Consent Under EU Law: A Theoretical Framework and Empirical Evidence from the UK*, International Journal of Law and Information Technology, 21, 2013, p 109; EDGAR, WHITLEY and PUJADAS, *Report on a study of how consumers currently consent to share their financial data with a third party*, Report provided for the Financial Services Consumer Panel, London, 19 April 2018, at https://www.fs-cp.org.uk/sites/default/files/fscp_report_on_how_consumers_currently_consent_to_share_their_data.pdf.

complex and fragmented financial environment where data analytics may exploit or manipulate consumer behaviour or biases.

The problem is that these systems are overly complex, not transparent and there are no mechanisms to safeguard against abuses and mistakes – generally known as the 'black box' problem.[93]

Most of the time not only the logics/biases of the algorithms remain undisclosed and guarded as trade secrets, but also the data sources used by the individual lenders are undisclosed. Arguably, it is very difficult to determine how the data are correlated and whether the variety of unrelated data operate as proxies for personal features – also of sensitive nature – targeting vulnerable individuals or behavioural biases. The issue of selecting qualitative in addition to quantitative data can pose the risk of unintentional or even intentional discrimination (e.g. by cherry-picking certain customers to increase profitability), especially since their choice reflect biased human decisions in the design of the algorithm, and thus of the product or service. Algorithms work on the basis of predetermined features or variables. Therefore, they are in a sense inherently biased or discriminatory. They assess the features of a person – thus his/her viability - according to the behaviour of others. In this way, the most appropriately designed algorithm is the one that can select, or discriminate, most effectively or better than others. This is a fundamental feature of algorithms that cannot be avoided. Obviously, the resulting products or services do not overtly discriminate on the basis of factors such as race, gender or age that are caught by anti-discrimination laws.[94] Nevertheless, they may instead use correlated information to build an in-depth profile of a particular customer and make

[93] PASQUALE, *The Black Box Society*, cit.

[94] E.g. see Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin, OJ L 180/22; Council Directive 2004/113/EC of 13 December 2004 implementing the principle of equal treatment between men and women in the access to and supply of goods and services, OJ L 373/37. See also *Association Belge des Consommateurs Test-Achats ASBL and Others v Conseil des ministers* (Case C-236/09), ECLI:EU:C:2011:100, where the CJEU ruled that insurers can no longer take gender into account when calculating insurance premiums.

indirect or other discriminations not explicitly covered by the law, e.g. discriminations based on behaviours, culture or wealth. Some instances of these discriminations can be re-conduced to traits of race, gender, or age but they will be very hard - if not impossible - to prove. Big data may dig-up protected information.

An indiscriminate use of data may easily lead to increased stereotypical decisions. They may respond to schemes selecting certain groups of the population posing issues of access to financial services to those groups of consumers.

In this environment, the risk of dark patterns is concrete. Dark patterns are "business practices employing elements of digital choice architecture, in particular in online user interfaces, that subvert or impair consumer autonomy, decision-making or choice. They *(…)* are likely to cause direct or indirect consumer detriment in various ways, though it may be difficult or impossible to measure such detriment in many instances".[95]

The subversion or impairment of consumer autonomy is the contrary of a consumer-centric environment and effective control. A critical point is that of attempting to empower consumers in an environment of vulnerability to dark patterns and other online perils.[96]

The Data Act attempts to fix the problem. It provides that third parties shall not "coerce, deceive or manipulate the user in any way" by subverting or impairing their autonomy, decision-making or choices, including by means of a digital interface.[97] However, it does not explicitly rule the prohibition of any form of coercion, deception or manipulation of data subjects, regardless of whether the user is also a data subject.[98] Under the Data Act, 'users' are natural or legal persons that

[95] OECD, *Dark commercial patterns*, OECD Digital Economy Papers, No. 336, 2022, OECD Publishing, at https://doi.org/10.1787/44f5e846-en

[96] *Ibid.* See also SEIZOV, WULF and LUZAK, *The Transparent Trap: A Multidisciplinary Perspective on the Design of Transparent Online Disclosures in the EU*, Journal of Consumer Policy, 42, 2019, p 149.

[97] Article 6(2)(a) Data Act.

[98] EDPB-EDPS, *Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on Harmonised Rules on Fair Access to and Use of Data (Data Act)*, cit.

own, rent or lease a product or receive a service.[99] The factors that may affect decision-making - hence real control of the data - may be different depending on whether or not the 'user' is also the data subject.[100]

The above difficulties could have additional counterproductive effects if a number of consumers become untrustworthy of their data being processed properly. Sections of the population may become averse to share information for fear of having their personal integrity violated. This, in a vicious circle, poses challenges to the commercial use of the data that will leave them behind or excluded.

On a related line, there are risks for those segments of the population who are un-networked or have no or limited digital presence. With Fintech development, increasing concerns are expressed by groups of consumers who face difficulties to access information, or buy and pay for goods/services in the digital domain. These include elderly persons who for various reasons do not use technologies, persons with disabilities, or persons in poverty. The causes for these difficulties may be diverse and range from a lack of digital literacy, lack of accessibility to the digital devices supporting the financial services, as well as lack of trust in digitalised services (e.g. fear around fraudulent use of identity, difficulty to identify misuse and claim redress, etc.).[101] The problems of consumer vulnerability in the digital sphere are well documented in the literature,[102] with the addition of the other layer of vulnerability in the realm of financial services.[103] As a result, significant numbers of consumers could be denied access to financial services.

---

[99] Article 2(5) Data Act.

[100] EDPB-EDPS, *Joint Opinion 2/2022 on the Proposal of the European Parliament and of the Council on Harmonised Rules on Fair Access to and Use of Data (Data Act)*, cit.

[101] OECD, *G20/OECD INFE Report on Ensuring Financial Education and Consumer Protection in the Digital Age*, 2017; CENTRAL BANK OF IRELAND, *Discussion Paper: Consumer Protection Code and the Digitalisation of Financial Services*, June 2017.

[102] For all, see HELBERGER, SAX, STRYCHARZ, MICKLITZ, *Choice Architectures in the Digital Economy: Towards a New Understanding of Digital Vulnerability*, Journal of Consumer Policy, 45, 2022, p 175, and the literature there cited. See also ALPA and CARTICALA', *Diritto dei Consumatori*, 2016, Il Mulino.

[103] PAGLIETTI and RABITTI, *A Matter of Time. Digital-Financial Consumers' Vulnerability in the Retail Payments Market*, European Business Law Review, 33(4), 2022, p 581.

In any event, the concern may not be limited to those who are not digitalised. The broader question, affecting everyone, is the extent to which people remain with the liberty of being un-networked or offline, with the safeguard of not attracting negative consequences in case personal data are not available digitally or refusal to share data.[104]

All in all, these risks raise debates and concerns over the commodification of personal data, the financialisation of people's lives, and the shaping and conforming of behaviours beyond the provision of financial services. These issues have not been discussed sufficiently in the making of the PSD2 or the Data Act.

6. This work was concerned with Open Finance and the challenges facing EU regulation to adequately protect consumers. Following the opportunities provided by Open Banking via the PSD2, the EU aims to extend this data-driven financial model to the entire financial services sector.

To enable Open Finance, regulation is needed. The question is what kind of regulation. The EU places consumer empowerment and data control as the tools to achieve a consumer-centric data-driven financial market led by innovation. How factual consumer empowerment, data control and protection can be reconciled with the regulatory approach currently envisaged by the EU legislator is an open matter that raises doubts and needs to be carefully addressed.

The regulatory framework for Open Finance rests in the consolidation and extension of a sectoral PSD2-like legislation that will have to integrate the general framework provided by the proposed Data Act. Moreover, as personal data are involved, it overlaps and needs coordination with the GDPR.

An analysis of the current and proposed EU legal instruments to enable Open Finance reveals that the latter may rather open risks for consumer protection for providing legal uncertainty and failing to grant an environment where consumers are

[104] PACKIN and ARETZ, *On Social Credit and the Right to Be Unnetworked*", Columbia Business Law Review, 2, 2016, p 339.

indeed in control and find adequate protection. Black boxes and dark patterns may flourish in such an environment. In a financial services market that is mainly supply-driven and governed by the supply-side, there are conduct of business risks. Aggressive business models may expand via the digital development. Innovation and competition are welcome, but data-driven business models are complex and take new unconventional forms where data feed new scenarios and create new markets. This can result in an environment favourable for targeted individual marketing, exploitation of consumers' behavioural biases, mis-selling of financial services, or financial discrimination. Freeriding wallows in legal uncertainty and may flourish.

The identified risks stemming from Open Finance may derive from the failure of the approach taken by present and proposed regulation to deliver the goal of realistically placing consumers at the centre and put them in control. Such a goal could not happen with the usual legal instruments of consumer consent or reliance on contractual necessity for data processing. This is particularly the case already in a context of legal uncertainty over their use in the PSD2 as the proper legal basis under the GDPR.

More than in any other market, in the digital environment vulnerability is likely to be the norm rather than the exception.[105] In Open Finance, consumers face the combination of both digital and financial vulnerability. Arguably, there is a need for a paradigm shift reversing the expectations placed on consumers to be self-governing and the arbiters of markets, particularly the digital financial one. In vulnerability-sensitive markets data control should be by regulatory and technological design, and not left to the autonomy of consumers. The use of principles integrated by conduct of business rules is the leading debate taking place in neighbouring jurisdictions such as the UK.

Consumer protection concerns intensify if regulation aims to achieve autonomy through the instrument of consent. Digitalisation exacerbates the

[105] RIEFA, *Protecting Vulnerable Consumers in the Digital Single Market*, European Business Law Review, 33(4), 2022, p 607.

weaknesses of this legal technique designed to empower consumers. In addition, consumers are likely to consent too easily when faced with perceived immediate financial gains.

Thus, the overarching question is the extent to which the current regulatory approach taken by the EU is prone to sufficiently protect consumers from the fundamental problems likely to be opened by Open Finance.

All the above considerations need to go along with ever-existing problems of lack of effective supervision and enforcement in the digital domain – this is a theme that this paper has not addressed but that needs equal in-depth attention by complementing research.

A Single European Data Space and Data Act for the Digital Single Market: on Datafication and the Viability of a PSD2-like Access Regime for the Platform Economy

Federico Ferretti*

In its new digital strategy for Europe, the EU highlights the need for better data-access and sharing. In line with this priority, it is working on a proposal for a Data Act that aims to provide the underlying legal framework. This paper seeks to disentangle key legal concepts and issues related to datafication that affect the envisaged European Data Space. It reveals that the EU already has a suitable regulatory model under the Payment Services Directive 2 ('PSD2'). The strategy focuses on market imbalances of the platform economy and challenges the legitimacy of large technological companies ('Big-Techs'). The latter act as gatekeepers to maintain a key role in data-access and monetise their data dominance. The paper casts into question the existence of a data market, suggesting that the EU already has a viable legislative model provided by the 'PSD2' sectoral legislation. Its data-access model could be applied horizontally across data-driven markets and the platform economy without engineering new rules or adding regulatory layers.

Keywords: Digital Single Market; Data Act; data; data rights and control; data access; data sharing; platform economy; PSD2

* Associate Professor of Law, Alma Mater Studiorum University of Bologna; Director of the Jean Monnet Centre of Excellence 'Consumers and SMEs in the Digital Single Market (Digi-ConSME)'; Jean Monnet Chair of EU Digital Market Law (E-DSM). Co-funded by the Erasmus+ Programme of the European Union. The author is grateful to the three anonymous reviewers for their insightful and helpful comments. The usual disclaimer applies.

TABLE OF CONTENTS

I. INTRODUCTION

The EU strives to attain a leading role in the data economy by exploiting an expanding amount of data to create innovative products and services in the Single Market. It views digitalisation as a tool for relaunching economic growth and social welfare.

This paper focuses on the key issue of data-access and sharing in the current market imbalances of the platform economy, where dominant undertakings act as gatekeepers. First, it explores the limits of existing EU laws addressing different aspects of data-access and sharing such as proprietary rights, data protection and competition that prevent the creation of a genuine market for data-driven products and services. Next, it investigates the extent to which the objectives set forth by proposed EU legislation can be met through the model of cognate regulatory instruments like the one governing the payment sector. Ultimately, this study claims that the latter provides a feasible regulatory model capable of creating the envisaged market in conjunction with current data laws. This model could be replicated for the entire digital market.

As part of the Digital Single Market Strategy,[1] the European Commission's latest policy goal is to create a single European Data Space, conceived as a 'genuine single market for data (…) where personal as well as non-personal data (…) are secure and businesses also have easy access to an almost infinite amount of high-quality data'.[2]

The digital expansion has placed data at the centre of major economic and social transformations. To the extent that data are the lifeblood of innovation, they have become an essential resource in economic terms. Data are no longer seen as mere outputs generated by the use of technology.

---

1 Commission, 'A Digital Single Market Strategy for Europe' (Communication) COM (2015) 192 final.

2 Commission, 'A European strategy for data' (Communication) COM (2020) 66 final.

Instead, they are increasingly regarded as inputs for the creation or improvement of products and services such as information services, processes, or decision-making tools.[3]

To achieve its policy objectives, the EU has committed to combining fit-for-purpose cross-sectoral (horizontal) legislation and governance to ensure the free flow, access and sharing of data within the Union.[4] The legislation will integrate existing data laws such as the GDPR[5] and few others[6] to support the viability and sustainability of an alternative model for the data economy that is at once open yet fair, transparent, and accountable.[7] In addition to furnishing a legislative framework for the governance of a common data space and the reuse of public sector data, data sharing among market players has a preeminent role to be achieved by means of a Data Act.[8] Two major problems for the achievement of policy goals are the intense

---

3 Ikujiro Nonaka, 'A Dynamic Theory of Organizational Knowledge Creation' (1994) 5 Organization Science 14; Francesco Mezzanotte, 'Access to Data: the Role of Consent and the Licensing Scheme' in Sebastian Lohsse, Reiner Schulze and Dirk Staudenmayer (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools* (Nomos 2017) 159.

4 Commission, 'A European strategy for data' (n 2).

5 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1 (GDPR).

6 See Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union [2018] OJ L303/59; Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) [2019] OJ L151/15; Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information [2019] OJ L172/56.

7 European Data Protection Supervisor, 'Opinion 3/2020 on the European Strategy for Data' (16 June 2020) <https://edps.europa.eu/sites/edp/files/publication/20-06-16_opinion_data_strategy_en.pdf>.

8 Commission, 'A European strategy for data' (n 2).

concentration of data in the hands of limited large online platforms (also known as 'Big-Techs') and market imbalances in the access and (re)use of data.[9] Big-Techs raise a number of different problems, some of which have already been addressed in legislative proposals.[10] Of concern here is that they are large multinational corporations that dominate the digital business. Within such a vast industry, Big-Techs dominate their respective niche market using the data to expand subsequently into other markets. Big-Techs may have very different business models, levels of maturity and financialisation, or corporate governance. They share in common the capacity to act as intermediary infrastructure and become gatekeepers of the indispensable facility represented by the data. They also become market gatekeepers in this way.[11] Their models build on creating, maximising, and monetising network effects and economies of scale to dominate the market, reduce competition and consumer welfare, and stifle innovation driven by others. Due to their distinctive features, Big-Techs have given rise to the so-called 'platform economy' which, overall, enjoys largely unchecked power in a regulatory vacuum.[12]

---

9 Ibid.

10 See e.g. Commission 'Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)' COM (2020) 842 final, which proposes new ex-ante rules for gatekeeper platforms as well as a new supervisory framework at EU level to address conduct and competition harm risks.

11 The European Commission defines a gatekeepers as 'a provider of core platform services', where core platform services are any online intermediation services, online search engines, online social networking services; video-sharing platform services; number-independent interpersonal communication services; operating systems; cloud computing services; advertising services, including any advertising networks, advertising exchanges and any other advertising intermediation services, provided by a provider of any of the core platform services. See ibid art 2.

12 Anne Helmond, 'The Platformization of the Web: Making Web Data Platform Ready' (2015) 1 Social Media + Society 1; Rodrigo Fernandez and others, *The Financialisation of Big Tech* (SOMO 2020).

This paper disentangles key legal aspects of datafication in the policy and market context discussed above that impact the envisaged European Data Space and a prospective data-access regime under the Data Act. These aspects include proprietary data rights, data protection and competition law. Particular attention is granted to the market imbalances in the platform economy created by Big-Techs and the extent to which such organisations should be allowed to monetise data acting as gatekeepers. This analysis ultimately suggests that the objectives of the proposed EU Data Act are already met by the model of cognate regulatory instruments governing the payments sector. The model could be applied horizontally as a norm of general application for all data without adding regulatory layers to current standards.

The study employs a doctrinal approach, analysis, and analogy to sustain its claims. Its contribution to the literature is to propose the extension of an existing regulatory framework for the novel purpose of data-access and sharing in the digital single market as a whole.

Section 2 explores the concept of data and their features to identify the extent and reach of data ownership or control rights and how these influence the idea of a 'single market for data'.[13] The analysis of the existence of a single market for data-driven products and services, rather than a 'data market', serves to highlight the relationship among players in the digital market. In turn, market characteristics shape the horizontal data-access regime needed for a Data Act that could correct the problems created by the imbalances of the platform economy. Section 3 demonstrates the limits of competition law enforcement to offer solutions for the creation of a genuine market for data-driven products and services. Designing an adequate data-access regime for the European data strategy and Data Act requires an understanding of the inherent limitations of available legal tools. The essential question is what form the Data Act should take. This is examined in Section 4, which studies

[13] As framed by Commission, 'A European strategy for data' (n 2).

the sectoral EU legislation on payment services to explore its viability as a model of horizontal general application for the entire digital market.

The EU does not have to reinvent any measures, nor would it need to engineer new rules.

II. The Limits of Competition Law Enforcement: A Single Market for Data-Driven Products and Services, Not a Single market for Data

The strategy for creating a single European Data Space presupposes maximum data availability. These are considered an essential component—or raw material—for the development of a competitive digital market, especially in terms of data-access and (re)usability. The policy vision and debate centre around the creation of a 'single market for data' and the rebalancing of market power in relation to data-access and sharing.[14]

Inevitably, the idea of a 'data market' prompts questions about its nature and reintroduces the long-debated issue of data ownership or titles to data, i.e. the extent of exclusive right to use, exploit, and disclose data, subject only to the rights of persons with a superior interest or legal or contractual restrictions.

One fundamental reservation is the extent to which recognition of a title in rem to data, and therefore the resultant market type, can be justified. Claims to proprietary rights are linked to commercial exploitation and the delineation of the market. Simply put, the allocation of a title in rem to data, in whatever form this may be recognised, would give rise to important consequences. These lead in turn to the question of how to strike a balance between the rights, obligations, and limits of those claiming title and a general interest in access to - and reuse of - data for the innovation and development of the digital market.

---

14 Ibid.

Moreover, if rights in rem are recognised and allocated, they must have limits and exceptions that serve the public interest.[15]

Therefore, defining the nature of data is key to informing public policy and establishing the legal basis for claims of title, including the very existence of a 'data market'.[16] It is also instrumental in defining the boundaries of the public interest in access to, and (re)usability of, data as an essential resource.[17]

As previous scholarship suggests, delineating the concept of data and their economic properties is a challenging exercise.[18] Yet it is a necessary one if data are to be treated as a commodity in the market.

1. The Nature of Data

The first difficulty is one of terminology and derives from the misleading interchangeability, in everyday jargon, of terms like 'data' and 'information'. However, the distinction between the two matters for policy and legal discourse. In information science, data is conceptualised in two ways: as signals, i.e. unprocessed reinterpretable digital representations, and as measurable and discrete observations of facts or acts in a formalised manner (such that there is a clear separation between the different possible values). However they are conceptualised, data must be suitable for communication,

---

15 Also argued by Teresa Scassa, 'Data Ownership' (2018) CIGI Paper No 187 <https://www.cigionline.org/publications/data-ownership/#:~:text=Teresa%20Scassa%20is%20a%20CIGI,of%20data%20ownership%20and%20control> accessed 10 June 2022.

16 See also Vincenzo Zeno-Zencovich, 'Do "Data Markets" Exist?' (2019) 2 Media Laws 22.

17 Josef Drexl, 'Data Access and Control in the Era of Connected Devices' (BEUC, The European Consumer Organisation, 15 January 2019) <https://www.beuc.eu/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdf> accessed 12 April 2021.

18 See e.g. Nestor Duch-Brown, Bertin Martens and Frank Mueller-Langer, 'The Economics of Ownership, Access and Trade in Digital Data' (2017) JRC Digital Economy Working Paper 2017-01 <https://joint-research-centre.ec.europa.eu/system/files/2017-03/jrc104756.pdf> accessed 10 June 2022.

interpretation or processing.[19] The definition of data is often supplemented with the requirement that signals be readable, generated or observable by a machine.[20] Data are often viewed as a by-product of other activities.[21] Yet they are also a resource in their own right when converted into information - that is the number of discernible signals or data points necessary to transmit a message.[22]

Other characterisations distinguish between a syntactic level (signs and their relationship with each other) and a semantic level (the meaning of data), which leads to a distinction between the content and code layers.[23] Information is instead a broader concept than data that depends on context and usage to convey meaning.

In the end, data are most appropriately defined in relation to the other parameters in their lifecycle, which can be illustrated in sequential order: data

---

19 Russel Ackoff defines data as 'symbols that represent the properties of objects and events. Information consists of processed data, the processing directed at increasing its usefulness'. 'From Data to Wisdom' in Russel Ackoff (ed), *Ackoff's Best* (John Wiley and Sons 1999) 170. See also Chaim Zins, 'Conceptual Approaches for Defining Data, Information, and Knowledge' (2007) 58 Journal of the Association for Information Science and Technology 479; Commission, 'Towards a thriving data-driven economy' (Communication) COM (2014) 442 final; Commission, 'Proposal for a Regulation on European data governance (Data Governance Act)' COM (2020) 767 final, art 2(1).

20 Herbert Zech, 'Data as a Tradable Commodity' in Alberto De Franceschi (ed), *European Contract Law and the Digital Single Market* (Intersentia 2017) 51.

21 Wolfgang Kerber, 'A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis' (2016) 65 Gewerblicher Rechtsschutz und Urheberrecht, Internationaler Teil (GRUR Int) 989.

22 Max Boisot and Agustì Canals, 'Data, Information and Knowledge: Have We Got It Right?' (2004) 14 Journal of Evolutionary Economics 43; Ronaldo Vigo, 'Complexity over Uncertainty in Generalized Representational Information Theory (GRIT): A Structure-Sensitive General Theory of Information' (2013) 4 Information 1. See also Robert M Losee, 'A Discipline Independent Definition of Information' (1997) 48 Journal of the American Society for Information Science 254.

23 Zech (n 20).

(any representation of something in digital form) are the raw material for information, information (structured data with a discernible meaning) is the raw material for knowledge, and knowledge (information whose validity has been established through tests of proof or intellectual virtue) is the raw material for wisdom (the ability to use knowledge to achieve and establish desired goals).[24]

This multichotomy implies a linear flow and hierarchy that do not remain on a purely theoretical level but have important economic and legal consequences.

2. The Data Value Chain

From an economic perspective, data represent a primary material. A sequential process of transformation adds value to the data, especially when combined with the resourcefulness, capability and experience of the agents who utilise the outcomes at each stage.[25] This is the value extraction process. The extensive availability of large volumes of diverse datasets from various unrelated sources (big data) is decisive to extracting maximum value.[26] The

---

24 Paul Bierly, Eric Kessler and Edward Christensen, 'Organisational Learning, Knowledge and Wisdom' (2000) 13 Journal of Organisational Change Management 595; Yochai Benkler, 'From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access' (2000) 52 Federal Communications Law Journal 561. According to Rob Kitchin, data are not neutral. They reflect choices about which data to collect or exclude and cannot exist independently of the ideas, instruments, practices, contexts and knowledges used to generate, process and analyse them. *The Data Revolution: Big Data, Open Data, Data Infrastructure and their Consequences* (Sage 2014) 1.

25 Antti Aine, Tom Bjorkroth and Aki Koponen, 'Horizontal Information Exchange and Innovation in the Platform Economy – A Need to Rethink?' (2019) 15 European Competition Journal 347.

26 Kitchin (n 24).

value of data grows progressively through the information, knowledge and wisdom conveyed by the data on the semantic level.[27]

In practical terms, the value chain distinguishes between data production, processing, collection, organisation and analysis and the achievement of set goals, including innovations based on the insights gained in the previous steps. As a raw material, data are an infinite resource generated at an insignificant cost. Moreover, they are immaterial and non-consumable (non-rival), which means usage does not exhaust the supply and they may be used simultaneously by more than one agent. These features are a novelty in economic theory, which considers limited or restricted resources, as well as production costs.[28]

Consequently, the economic value of data in their essential form is trivial and irrelevant.[29]

The paradox of the debate over titles to data is precisely that where there is no value, one would conclude that ownership or other rights of economic exploitation are not an issue. This deduction is reinforced by the unique nature of data as limitless and non-rivalrous, which fits uneasily with the

---

27 Zech (n 20); Drexl, 'Data Access and Control in the Era of Connected Devices' (n 17).

28 Jean-Sylvestre Bergé, Stephane Grumbach and Vincenzo Zeno-Zenchovic, 'The "Datasphere", Data Flows beyond Control, and the Challenges for Law and Governance' (2018) 5 European Journal of Comparative Law 144.

29 See Commission, 'Decision of 27.6.2017 relating to the proceedings under Article 102 of the Treaty on the Functioning of the European Union and Article 54 of the Agreement on the European Economic Area (AT.39740 – Google Search (Shopping))' C (2017) 4444 final (Google Search case). See also Edouard Bruc, 'Data as an Essential Facility in European Law: How to Define the "Target" Market and Divert the Data Pipeline?' (2019) 15 European Competition Journal 177.

legal concept of a title in rem. As in the case of ideas, these features are the foundations for the classification of data as public goods.[30]

If property rights are difficult to extend to data, this, in turn, creates challenges in establishing usage rights.[31] Instead, the issue arises as soon as value is provided, i.e. at the later stage when data provide information, knowledge and wisdom.

Another complication that surfaces is the contribution of multiple actors to the datafication process and the relationship between them. Different persons (natural and/or legal) may contribute to generating data through human activities or technologies (e.g. data created or observed by a sensor, search engine, or website), or may add value during the processing, observation, aggregation, storage, selection, verification and analysis stages. Data can be directly generated by the person or by that person's use of services.[32] Value may also reside in the immediacy and instant availability of data.[33]

---

30 Harold Demsetz, 'Toward a Theory of Property Rights' (1967) 57 The American Economic Review 347; Priscilla Regan, 'Privacy as a Common Good in the Digital World' (2010) 5 Information, Communication and Society 382. See also Drexl, 'Data Access and Control in the Era of Connected Devices' (n 17), which also makes reference to constitutional principles of freedom of information and the EU Charter of Fundamental Rights (Article 11(1)).

31 Some scholarship, forcing the established economic and legal notion of property, debates whether its concept should be flexible enough to extend to new immaterial goods and eventually allow the commodification of data. See Nadezhda Purtova, 'The Illusion of Personal Data as No One's Property' (2015) 7 Law, Innovation and Technology 83; Alberto De Franceschi and Michael Lehmann, 'Data as Tradable Commodity and New Measures for their Protection' (2015) 1 Italian Law Journal 51.

32 Inge Graef, 'Market Definition and Market Power in Data: The Case of Online Platforms' (2015) 38 World Competition 473; Josef Drexl, 'Legal Challenges of the Changing Role of Personal and Non-Personal Data in the Data Economy' (2018) Max Planck Institute for Innovation & Competition Research Paper No 18-23 <https://ssrn.com/abstract=3274519> accessed 12 April 2021.

33 Duch-Brown, Martens and Mueller-Langer (n 18).

From this perspective, the distinction between personal and non-personal data—which has thus far remained indistinct—assumes relevance. Data may be non-personal or personal in nature, where the latter are broadly defined in relation to an identified or identifiable natural person.[34]

Natural persons would intuitively assert that they own data about themselves, as these comprise personal attributes. However, individuals do not own information about themselves. Personal data do not pre-exist prior to their expression or disclosure. They are always to some extent constructed or created by more than one agent.[35] They pertain to a person yet do not belong in a proprietary sense to him/her. Those who process personal data (data controllers) have the right to process data pertaining to data subjects as long as such processing is lawful, i.e. they abide by procedural rules established by law (in the EU, the GDPR - infra) with the objective of protecting individual citizens not against data processing per se but against unjustified collection, storage, use and dissemination of the data pertaining to them.[36] Moreover, personal data may be turned into anonymous data, but

---

34 Descriptive definition based on GDPR, art 4(1). See also the earlier Article 29 Data Protection Working Party, 'Opinion 4/2007 on the Concept of Personal Data' (European Commission, 20 June 2007) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf> accessed 12 April 2022.

35 Federico Ferretti, *Competition, the Consumer Interest, and Data Protection* (Springer 2014). See also Annette Rouvroy and Yves Poullet, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer 2009).

36 E.g. individuals do not own their criminal records or credit history. Ferretti, *Competition, the Consumer Interest, and Data Protection* (n 35). See also the discussions about individuals not owning information about themselves in Jerry Kang and Benedikt Bunter, 'Privacy in Atlantis' (2004) 18 Harvard Journal of Law and Technology 230; Rouvroy and Poullet (n 35).

they are still data (of a non-personal nature) that remain in existence without allocation to data subjects.[37]

In the end, the value chain and the role of different stakeholders are crucial from the legal perspective. Each transformation, creation of value, and interaction of different subjects at different levels epitomises a separate legal construction and allocation of rights. For this reason, it is crucial to determine whether and at what stage data may become a commodity giving rise to transferable rights, and whether legal protections should intervene.[38]

3. Data-related Rights

The value chain determines when legal rights should be allocated, who is entitled to claim a title over the data, and how to exercise such rights.

The fluid nature of data and their unsuitability to being defined and regulated in the same way as other tangible or intangible goods has generated debates about the potential creation of a new right in rem specific to data.[39] Under existing laws, however, no data property right can exist. Nor do there seem to be legal grounds for recognising rights of economic

---

37 Gintare Surblyte, 'Data Mobility at the Intersection of Data, Trade Secret Protection and the Mobility of Employees in the Digital Economy' (2016) 65 Gewerblicher Rechtsschutz und Urheberrecht, Internationaler Teil (GRUR Int) 1121.

38 Barbara Evans, 'Much Ado About Data Ownership' (2011) 25 Harvard Journal of Law and Technology 70; Viktor Mayer-Schonberger and Kenneth Cukier, *Big Data – A Revolution that Will Transform How We Live, Work and Think* (John Murray 2013).

39 For all, see Zech (n 20).

exploitation over data per se.[40] Likewise, no EU jurisprudence satisfactorily deals with the matter.[41]

Instead, rights over data usability and allocation can be constructed as a bundle of other rights. These originate from a patchwork of existing laws, protecting other goods or values, that affect interested parties in data use without allocating property rights. Not surprisingly, these rights shift from a sales or transfer paradigm to a licence model based on access.[42]

Access requires a subject to hold the data, which presupposes control. In the debate over data accessibility, the point is to define the precise extent of control rights and entitlements, as well as the legal mechanisms to deal with access restrictions in a framework that does not presuppose a comprehensive data regime.

---

40 Zech (n 20); Mezzanotte (n 3); Sjef van Erp, 'Ownership of Digital Assets and the Numerus Clausus of Legal Objects' (2017) Maastricht European Private Law Institute Working Paper No 2017/6 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3046402> accessed 12 April 2021; Francesco Banterle, 'Data Ownership in the Data Economy: A European Dilemma' in Tatiana-Eleni Synodinou and others (eds), *EU Internet Law in the Digital Era* (Springer 2020) 199.

41 See Ivan Stepanov, 'Introducing a Property Right Over Data in the EU: The Data Producer's Right – An Evaluation' (2020) 34 International Review of Law, Computers & Technology 65. According to the author, however, although no property rights as such over data exist, when faced with gaps some national Courts seem to adapt and in certain aspects treat data as property offering points of divergence. German Courts ruled on the proprietary aspects of data on matters of mishandling by company employees, albeit in criminal and labour law cases. The Courts concluded that for the purposes of those fields of law, data can be owned, thus exhibiting traits associated with property. In the Netherlands, the Supreme Court stated that from the perspective of criminal law data could be the object of theft. Finally, Luxembourgian law gives the right to reclaim ownership in data from the cloud in bankruptcy proceedings if the circumstances provide for such an opportunity. Ibid 73-74.

42 Aaron Perzanowski and Jason Schultz, *The End of Ownership. Personal Property in the Digital Economy* (MIT Press 2016).

The assortment of laws that assign rights and obligations over data are discussed below.

A. Intellectual Property Laws

Intellectual property is the traditional form of protection of intangible assets. Its normative frameworks, including related rights, are often used to provide some form of protection for rights over data.

-*Copyright Law*

Copyright protects the original expression of ideas or facts, but there is no protection for ideas or facts in the abstract. What is protected is originality in the form, not in the contents.[43] To enjoy protection, data must therefore result from creative choices, not merely technical ones, and cannot be the straightforward result of investments. Accordingly, raw data aggregations or compilations do not satisfy the requirement of originality.[44] Human authorship is moreover essential. This element excludes generations, aggregations or compilations of data performed by software or automated processes (the latter, by contrast, are protected as intellectual property).[45]

Considering that the utilitarian value of data in the big data context does not derive from creativity or originality, copyright protection offers very limited rights, if any, over data control and access restrictions.

---

43 Commission, 'Towards a thriving data-driven economy' (n 19); Commission, 'A Digital Single Market Strategy for Europe' (n 1).

44 Case C-145/10 *Eva-Maria Painer v Standard VerlagsGmbH and Others* EU:C:2011:798; Joined Cases C-403/08 and C-429/08 *Football Association Premier League Ltd and Others v QC Leisure and Others* and *Karen Murphy v Media Protection Services Ltd* EU:C:2011:631; Case C-604/10 *Football Dataco Ltd and Others v Yahoo! UK Ltd and Others* EU:C:2012:115.

45 *Football Dataco* (n 44).

-Trade Secrets and Confidentiality

In a business setting, anything may be confidential or secret in nature. Typically, the values protected by law are confidentiality and secrecy rather than the good itself. For example, ideas that cannot be protected under copyright law may find protection when shared under the private law setting of a confidentiality agreement. Likewise, information about customers and suppliers, business plans, market research and strategies can be used as business competitiveness or research innovation management tools.[46]

Thus, data may constitute the subject matter of confidential information or a trade secret, whether collected automatically or not and without any requirement of originality or creativity.

The Trade Secrets Directive sets forth a liability regime in tort against the unlawful acquisition, use and disclosure of trade secrets.[47] A trade secret is defined as information at the semantic level (i.e. it is different from data).[48] To enjoy protection, the information must be secret, i.e. it is not generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question.[49] Its commercial value derives from secrecy, and should be subject to adequate security measures to keep it secret.[50] Trivial information is excluded.[51] Here, the right holder controls the secret rather than the data that turn into information.[52]

As the scope of such protection is confidentiality and secrecy, both contracts and trade secrecy law confer rights in personam, applying only to the

---

46 Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure [2016] OJ L157/1 (Trade Secrets Directive).

47 Ibid recital 2.

48 Zech (n 20).

49 Trade Secrets Directive, art 1.

50 Ibid art 2(1).

51 Ibid recital 14.

52 Ibid art 2(2).

contractual parties or persons who have unlawfully acquired, used or disclosed a trade secret.[53] Third parties are not bound by access restrictions and further dissemination. Equally, the law offers remedies only if parties knew or should have known of their secret nature.

Moreover, contracts or secrets presuppose a party holding the data. Questions remain regarding the legal title of control over data. This can be a de facto situation when data are generated internally by one agent only, with no other agent claiming rights over them.[54] This is already a substantial limit on value in the data economy.

As regards commercial value, the doubtful or trivial value of raw data has already been noted above. This is especially the case for data generated by multiple agents and/or interconnected machines.[55] The causal link between the secrecy of individual data and the commercial value of information or knowledge can be challenged too.[56] Some scholars use this point to argue that in a big data environment, trivial information may also have economic value when compiled in sufficient quantities, showing false premises in the law.[57] Nevertheless, whether their prospective value derives from their secrecy remains uncertain. Allocating value in a network environment may be unattainable.[58] By contrast, it is the secrecy of algorithms that holds value.

In light of the above considerations, some authors conclude that trade secrets legislation can nonetheless be better suited to serving the purposes of the

---

53 Ibid art 2(3).

54 See e.g. Andreas Wiebe, 'Protection of Industrial Data – A New Property Right for the Digital Economy?' (2017) 12 Journal of Intellectual Property Law & Practice 62.

55 E.g. in the Internet of Things, which describes the network of physical objects owned by one or more parties that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the Internet.

56 Drexl, 'Data Access and Control in the Era of Connected Devices' (n 17); Banterle (n 40).

57 Zech (n 20).

58 Wiebe (n 54); Stepanov (n 41).

data economy by focussing on the specific way someone has unlawfully gained access to the data, allowing a more flexible regime than erga omnes rights over the data.[59]

Overall, it appears clear that trade secrecy law grants relative protection over data control.

-*Database Rights*

At first sight, the legal protection of databases may appear the simplest model for data rights. The growing importance of data over time has given rise to support for and protection of investments in databases, without which early EU policymakers believed the database industry could not emerge.[60]

With the creation in the Database Directive[61] of a sui generis right akin to copyright, EU legislature has provided a right for database creators able to demonstrate that 'there has been qualitatively and/or quantitatively a substantial investment in either the obtaining, verification or presentation of the contents to prevent extraction and/or re-utilization of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database'.[62] No originality obligation is required.[63]

---

59 Banterle (n 40).

60 It can be questioned whether any backing law was needed and the scope of its success, especially if the experience of other non-EU jurisdictions is compared. See Bernt Hugenholtz, 'Something Completely Different: Europe's Sui Generis Database Right Book' in Susy Frankel and Daniel Gervais (eds), *The Internet and the Emerging Importance of New Forms of Intellectual Property* (Wolters Kluwer 2016) 205; Scassa (n 15), comparing EU law with the experience of the US and Canada that have no specific database protection law.

61 Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases [1996] OJ L77/20 (Database Directive).

62 Ibid art 7.

63 Bernt Hugenholtz, 'Intellectual Property and Information Law' in Jan Kabel and Gerard Mom (eds), *Intellectual Property and Information Law: Essays in Honour of Herman Cohen Jehoram* (Kluwer Law International 1998).

The subject of the right is the substantial investment in the creation of a database, not the data themselves.[64] Under established jurisprudence, the investment should be in data that have been obtained, verified or presented. By contrast, investment in data created or generated by the person is excluded.[65] This is a limit of protection in the context of big data and artificial intelligence.

In addition, the protection is circumscribed to extraction and/or reutilisation of the 'whole' or a 'substantial part' of the contents of a database, not individual datasets. Unauthorised insubstantial extractions or reutilisations do not qualify as infringement.

Another difficulty that emerges is that big data, given their volume and diversity, are incongruent with traditional databases as conceived by the law. The Directive defines databases as collections of 'data or other materials which are systematically or methodically arranged and can be individually accessed'.[66] With big data, new technologies produce non-relational databases; that is, software associated with databases provide a mechanism for data storage and retrieval that is modelled using different means than the tabular schemas of relational databases. The 'systemic or methodical arrangement' elements are lacking and data are not compiled in a way that

---

64 Commission, 'Building a European Data Economy' (Communication) COM (2017) 9 final. See also Case C-46/02 *Fixtures Marketing Ltd v Oy Veikkaus Ab* EU:C:2004:694; Case C-338/02 *Fixtures Marketing Ltd v Svenska Spel AB* EU:C:2004:696; Case C-444/02 *Fixtures Marketing Ltd v Organismos prognostikon agonon podosfairou AE (OPAP)* EU:C:2004:697.

65 Case C-203/02 *The British Horseracing Board Ltd and Others v William Hill Organization Ltd* EU:C:2004:695.

66 Database Directive, recitals 17, 21 (emphasis added). See also Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [2015] OJ L337/35, art 1(2) (PSD2).

preserves the semantic value of data. These circumstances have induced scholars to conclude that protection does not apply.[67]

Although it pertains to the field of data protection law, the recent *Schrems*[68] case confirms in a novel way that the data in a database, regardless of their substantiality, do not automatically belong to the database owner. Invalidating the agreement between the EU and the US on the international transfer of personal data, the CJEU prevented the database owner from moving the data to a different jurisdiction that did not offer adequate protection under EU standards. The case imposed new limits on the proprietary rights to databases composed of personal data.

As the above analysis suggests, database protection legislation prevents the simple extension of real rights or legal control over individual or raw data.

B. Personal Data Protection Law

Data protection law dictates important rights and obligations in data usability and allocation relating to an identified or identifiable natural person.

The GDPR details the conditions under which data processing is legitimate. It forces processing to be transparent, enabling data subjects to control it where the processing is not authorised by the law itself as necessary for social reasons. In short, data protection law focuses on the activities of processors and enforces their accountability, thus regulating an accepted exercise of power.[69] The law is rooted in the idea that democratic societies should not

---

67 Daniel Gervais, 'Exploring the Interfaces Between Big Data and Intellectual Property Law' (2019) 10 Journal of Intellectual Property, Information Technology and E-Commerce Law 22.

68 Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* EU:C:2020:559.

69 Paul De Hert and Serge Gutwirth, 'Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalization in Action' in Serge Gutwirth and others (eds) (n 35). On a critical view that data protection acts are seldom

be turned into societies based on control, surveillance, actual or predictive profiling, classification, social sorting, and discrimination. It is not only a question of individual liberty, privacy, integrity and dignity, but a wider personal right aimed at fostering the social identity of individuals as citizens and consumers alike. Accordingly, the data protection regime provides legal protection to pursue the common goal of a free and democratic society where citizens develop their personalities freely and autonomously through individual, reflexive self-determination. It provides for collective deliberative decision-making about the rules of social cooperation.[70] Granting individuals control over their personal data is more than a mere tool allowing them to control the persona they project in society, free from unreasonable or unjustified associations, manipulations, distortions, misrepresentations, alterations or constraints on their true identity. It is the fundamental value of humans developing their personality in a way that allows them full participation in society without having to make thoughts, beliefs, behaviours, or preferences conform to those of the majority or those dictated from above by commercial interests.[71]

The conceptual principles outlined above are reflected in the provisions of the GDPR, the scope of which is to ensure those who determine the purposes and methods of personal data processing (the 'data controllers') engage in good data management practices. The GDPR incorporates a series of general rules on the lawfulness of personal data processing.[72] Data subjects must be informed of the processing, which has to be performed for legitimate, explicit and precise purposes. Processing is limited to the necessary time

---

privacy laws but rather information laws, protecting data before people, see Simon Davis, 'Re-engineering the right to privacy: How privacy has been transformed from a right to a commodity' in Philip Agre and Marc Rotenberg (eds), *Technology and Privacy: The New Landscape* (MIT Press 1997) 143.

70 Federico Ferretti, 'Data Protection and the Legitimate Interest of Data Controllers: Much Ado About Nothing or the Winter of Rights?' (2014) 51 Common Market Law Review 843 (citing Rouvroy and Poullet (n 35)).

71 Ibid.

72 GDPR, art 13-14.

frame (principles of purpose specification and data minimization).[73] Finally, data subjects are granted the right to access their data[74] and non-absolute data portability rights.[75]

A data controller can claim a valid basis for processing only if it meets one of the exhaustive criteria established by the law. If the data controller's processing does not satisfy one of them, it is unlawful.[76]

4. De Facto Control

What emerges from the previous Sections is that the existing framework is not resolutive in allocating data rights.

Intellectual property protections or related regimes are unsuitable to grant legal recognition of exclusive powers of control over datasets.[77]

When data are personal, the law grants stronger control. Even here, however, legal control is not absolute but relative. The speciality is that the debate on data control and allocation is enriched with the respect of fundamental rights. Nonetheless, data protection does not provide economic rights.

If there are no legal rights in rem or title transfer of data, in principle the latter should be freely available and access to them unrestricted. The 'data market' should not exist. The conception of data as a collective good is not an unfamiliar one (res communis)[78], with the caveat of the control conferred by the GDPR.

---

73 Ibid art 5.

74 Ibid art 15.

75 Ibid art 20.

76 Ibid art 6.

77 This conclusion is in line with those of Zech (n 20); Wiebe (n 54); Gervais (n 67).

78 Demsetz (n 30); Yoram Barzel, *Economic Analysis of Property Rights* (Cambridge University Press 1997). Collective goods (technically, things that are common to humankind) are not appropriable but the public may acquire certain usufructuary

Yet this scenario does not reflect reality. Data are regarded as a valuable economic asset, characterised by data gatekeeping, access restrictions, entry barriers, and lock-ins.

The question of how such power materialises conclusively leads to de facto control. This control allocates economic exploitation and allows sole use or access contracts. It transforms data from a non-rival good into a rival one. De facto control—which can also be termed 'possession'—is typically ensured by technical means and the ability of platforms to mine data from users. Simply put, de facto controllers are incentivised to invest in data collection because they appropriate the gains.

This finding could lead EU lawyers toward a nest of wasps regarding the law of possession in the absence of a legal title. Sharp divergences persist between civil and common law. Countries and doctrinal debates differ over the existence or nature of possessors' titles and the extent of protection.79 These fascinating discussions would deviate from this study. Here, it is sufficient to acknowledge that the law of possession would lead to weak non-resolutive protection.[80] In any event, it would not fall within the competence of EU law, but follow an impassable path for EU intervention that would frustrate from the outset any idea of harmonisation and a Single Digital Market.

---

rights (a limited real right of *usus*), directly and without altering them, and their fruits (*fructus*, the right to derive profit from them). They should be kept separate from no one's good (*res nullius*), in that the latter derives from private Roman law whereby they are considered ownerless property appropriable by means of occupation or possession if not regulated otherwise (e.g. wild animals). See Paul Du Plessis, *Borkowski's Textbook on Roman Law* (Oxford University Press 2020).

79 For a comprehensive account of comparative doctrines on the law of possession, see James Gordley and Ugo Mattei, 'Protecting Possession' (1996) 44 The American Journal of Comparative Law 293.

80 Ibid.

Rather than a market for data, factual control defines a market for access to data holding. Due to regulatory gaps, the gatekeepers are dominant technological companies.

Big data are a game-changer. They have been exploited by new technologies for the collection, storage, mining, synthesis, pattern recognition, and analysis of large volumes of wide-scoped, varied, and accurate data almost in real-time.[81] The value lies in the cumulative features of the 4 Vs: volume, velocity, variety, and veracity.[82] The maximum value of data is created by mining and analytical tools of artificial intelligence and machine-learning technologies. Competitiveness is a function of the sophistication of technologies and analyses they can perform. Arguably, data analysis is the real commodity rather than the data themselves.

As discussed above, 'data markets' should have no reason to exist, at least in conventional economic and legal terms. Rather, data are an essential, non-rivalrous, and infinite component of novel product or service markets best represented as 'data-driven markets', with different markets employing different types of big data as inputs for different outcomes.

As things stand, it seems that 'data markets' exist as the de facto result of unsuitable regulation over a fluid res that is collective in nature.[83]

To the extent that this conclusion is plausible, de facto control negatively impacts the ensuing data-driven markets. Hence, it is not only conceivable but also desirable that data-access should become unrestricted.

---

81 Mark Lycett, 'Datafication: Making Sense of (Big) Data in a Complex World' (2013) 22 European Journal of Information Systems 381.

82 Ibid. See also Maurice Stucke and Allen Grunes, *Big Data and Competition Policy* (Oxford University Press 2016); Daniel Rubinfeld and Michal Gal, 'Access Barriers to Big Data' (2017) 59 Arizona Law Review 339.

83 But see Inge Graef, *EU Competition Law, Data Protection and Online Platforms: Data as Essential Facility* (Kluwer 2016), according to which competition authorities and courts should define and analyse a potential market for data in addition to relevant product markets.

In principle, the enforcement of competition law should overcome abuses of market power and anticompetitive practices such as barriers to the access of essential facilities and market development.

III. The Limits of Competition Law Enforcement

1. The Unsuitability of Data as an Essential Facility

In principle, the importance ascribed to data as an indispensable input for the Digital Single Market could trigger the application of competition law. In its traditional application to dominant firms,[84] the question is the extent to which the de facto control of gatekeeping platforms over data qualifies as anticompetitive conduct harming the competitive process, innovation and entrepreneurship. A market where a data-dominant firm may restrict or impose unfair conditions on access can create a bottleneck. Provided there is abuse, the natural suggestion would be to use competition law as a tool for creating a level playing field of unrestricted data-access through a duty to share.

Competition law provides two legal grounds to remedy gatekeeping: the prohibition of anticompetitive agreements under Article 101 TFEU if the gatekeeper's refusal is based on an agreement with other firms, or in the absence of such an agreement, the prohibition of the abuse of dominant position under Article 102 TFEU.

To the extent that data constitute the essential input in the hands of monopolists, the most appropriate enforcement instrument is offered by the 'essential facility doctrine' under Article 102 TFEU. The doctrine may require a dominant firm to share its assets with others if those assets are indispensable to competing in the market and refusing access would eliminate effective competition. The market failure arising because control

---

[84] Giorgio Monti, 'Abuse of Dominant Position: A Post-Intel Calm?' (2019) 3 CPI Antitrust Chronicle <https://www.competitionpolicyinternational.com/abuse-of-a-dominant-position-a-post-intel-calm/> accessed 12 April 2021.

of data infrastructure and network effects (direct or indirect) force competing firms to depend on platforms, which become indispensable in the same fashion as physical infrastructures like railroads or ports.

The imposition of dealing with a dominant undertaking interferes with fundamental principles of freedom of contract and party autonomy. This is a controversial point that demands a limited application of the doctrine.[85] Moreover, it should be borne in mind that this is a measure meant to stimulate competition in the market and not for the market.[86] In the context of data and the European strategy, it may emerge as an important factor since competition in the market and for the market each lead to a different form of innovation: sustaining innovation that improves existing products/services in the former case, and disruptive innovation that discontinues products or services in the latter. The scholarly literature highlights how competition authorities need to balance the two in determining whether or not to intervene.[87] In this scenario, competition law enforcement may be only partially useful to the goals of the European Data Strategy.

Given this caveat, there is no general approach for applying the essential facility doctrine. It is a test based on the analysis of the specific circumstances of each case: the specific characteristics of the relevant facility, the conduct under scrutiny, and its economic context. To apply the essential facility

---

85 Inge Graef, 'Rethinking the Essential Facilities Doctrine for the EU Digital Economy' (2019) 53 Revue Juridique Thémis de l'Université de Montréal 33; Jaques Crémer, Yves-Alexandre de Montjoye and Heike Schweitzer, *Competition Policy for the Digital Era – Final Report* (European Commission 2019). See also Case C-7/97 *Oscar Bronner GmbH & Co. KG v Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co KG, Mediaprint Zeitungsvertriebsgesellschaft mbH & Co KG and Mediaprint Anzeigengesellschaft mbH & Co KG* EU:C:1998:264, Opinion of AG Jacobs; Case T-41/96 *Bayer AG v Commission of the European Communities* EU:T:2000:242.

86 Ibid. See also Drexl, 'Data Access and Control in the Era of Connected Devices' (n 17).

87 Ibid.

doctrine, the facility (data) must be defined as a distinct relevant market from derivative markets. However, there is no market for (big) data as such. Moreover, platforms act as gatekeepers in different service markets. Therefore, one would need to examine the competitive reality of the markets in which each platform operates and to which the data content relates.[88] Next, robust evidence of likely anticompetitive effects should be provided.

The application of the doctrine is notoriously narrow and cumbersome.

The first step in establishing dominance is to define the relevant market. However, a digital market per se cannot be identified. Instead, platforms are heterogeneous with different business models. Relevant markets must be defined anew each time. Moreover, the potential harm to competition posed by platforms' dominance may not be always recognised if measured in terms of price and output.[89] Instead, the economic feature of platforms is their multi-sidedness; they interconnect and operate in two or more markets with network economy effects and economies of scale, where the basis for deriving income may be very diverse. In so operating, the benefits that one market (one side) derives from the platform depends on the participants of one or more other markets (other sides).[90] Data obtained in one market offer

---

88 Joined Cases 6 and 7/73 *Istituto Chemioterapico Italiano S.p.A. and Commercial Solvents Corporation v Commission of the European Communities* EU:C:1974:18.

89 Lina Khan, 'Amazon's Antitrust Paradox' (2017) 126 The Yale Law Journal 710; Inge Graef and Francisco Costa-Cabral, 'To Regulate or Not to Regulate Big Tech' (2020) 1 Concurrences 24. See also Google Search case (n 29), according to which, even if users do not pay a monetary consideration for the use of search services on the internet, they contribute by providing data with each query.

90 For example, a search engine provider offers its services to users for free, at the same time providing advertising services or tools to other companies for profit. Likewise, a retailer may offer its intermediation services to buyers for free, at the same time operating as retailer in competition with other retailers but with the advantage of having more complete profiles of users. On the two or multi-sidedness of platforms, see Inge Graef, *EU Competition Law, Data Protection and Online Platforms* (n 83); Geoffrey Parker, Marshall van Alstyne and Sangeet Choudary, *Platform Revolution* (Norton 2017); Crémer, de Montjoye and Schweitzer (n 85).

a competitive advantage in the other(s). Therefore, the definition of the relevant market depends not only on diverse data-driven markets to which undertakings may require access but also on the markets for the several types of information that can be extracted from the data.[91] In the big data age, defining relevant markets for the essentiality of data may prove highly complex if not impossible.[92]

Second, the degree of dependence needs to be established. A successful claim must demonstrate the indispensability of the facility to business activity and that there are no other actual or potential substitutes for the facility. Moreover, there should be technical, legal, or economic obstacles that make it impossible, or unreasonably difficult, for competitors to obtain the facility.[93] Accordingly, exclusivity does not necessarily imply either essentiality or monopolistic power. Resources are not essential as such, but relative to something or in comparison with other available inputs. With big data, it is impossible to recognise a certain set of data that could identify a product/service market. In principle, all data may be useful and they can be replaceable or interchangeable in connection with the purpose for which they are needed.[94] The very notion of big data suggests that they are an extremely heterogeneous resource, whose applications cannot be known in advance. However, to be essential, a facility should serve a defined product/service in a cause-and-effect relationship.[95] Therefore, data should be divided into different categories and access granted only to the truly

---

91 Giuseppe Colangelo and Maria Teresa Maggiolino, 'Big Data as Misleading Facilities' (2017) 13 European Competition Journal 249; Mark Patterson, *Antitrust Law in the New Economy* (Harvard University Press 2017).

92 Patterson (n 91).

93 *Oscar Bronner* (n 85); Case C-418/01 *IMS Health GmbH & Co OHG v NDC Health GmbH & Co KG* EU:C:2004:257; Case T-201/04 *Microsoft Corp v Commission of the European Communities* EU:T:2007:289.

94 Niels-Peter Schepp and Achim Wambach, 'On Big Data and its Relevance for Market Power Assessment' (2016) 7 *Journal of European Competition Law and Practice* 120; Colangelo and Maggiolino (n 91).

95 Ibid.

indispensable ones. From this perspective, the solution offered by the application of the doctrine appears far removed from the reality of big data and the goals of the European data policy.

Third, the refusal to provide access to the facility should exclude all effective competition on the market.[96] Mutatis mutandis, the features of platform business models and those of the facility (data) could impede the realisation of such a condition.

Finally, the refusal to provide access should not be justified by objective reasons.[97] When data are personal, data protection rules may be used as a defence against data-access requests based on competition law.

All the above illustrates that the already cumbersome enforcement of the essential facility doctrine finds additional obstacles when platforms and data are involved, making competition law enforcement an inadequate tool for the goals of unrestricted data-access and innovation.

2. Data Portability

When data are personal, Art. 20 of the GDPR recognises the right of data portability. Data subjects have the right to have their data transmitted to another controller in a structured, commonly used and machine-readable format, as long as the processing is based on consent or a contract.

Consent and contract necessity are only two of the grounds for lawful data processing as per Article 6 GDPR. The processing grounds of compliance with a legal obligation, protection of vital interests, the performance of a task carried out in the public interest, and the pursuit of legitimate interests of data controllers or third parties are therefore excluded from the data portability right.

---

96 *Microsoft* (n 93).

97 Ibid.

Under the circumscribed range of situations in which the right is applicable, data subjects continue to have their data processed by the original controller after a data portability operation, since this operation does not trigger the erasure of the data from the former controller but simply a transfer to another controller for the provisions of services from the latter.[98] The decision of consumers to switch service providers becomes consent to pass their data to another provider, but the possibility of erasing their data from the former provider remains subject to a separate request and conditions as per Article 17 GDPR.

The absence of a general right to data portability in the GDPR already portrays a narrow scope. This is further restricted to data which data subjects have provided themselves to the data controller—so-called volunteered data. The scope of the provision includes observation of the data but excludes derived or inferred data, or anything resulting from the analysis of the data.[99]

The norm also reduces the reach of the right by adding that controllers may transfer data where it is 'technically feasible'[100] without providing any indication about its meaning. This vagueness allows significant leeway to data controllers unwilling to make a transfer.[101]

Data protection rights of third parties provide an additional constraint when the request involves data of other individuals. This situation is not infrequent in social media where individuals share activities and intertwine their data.[102]

---

98 Article 29 Data Protection Working Party, 'Guidelines on the Right to Data Portability' (European Commission, 5 April 2017) <https://ec.europa.eu/newsroom/article29/items/611233/en> accessed 12 April 2022.

99 Ibid. see also GDPR, recital 68.

100 GDPR, art 20(2).

101 Aysem Vanberg and Mehmet Unver, 'The Right to Data Portability in the GDPR and EU Competition Law: Odd Couple or Dynamic Duo?' (2017) 8 European Journal of Law and Technology 1.

102 Barbara Engels, 'Data portability amongst online platforms' (2016) 5 Internet Policy Review <https://policyreview.info/articles/analysis/data-portability-among -online-platforms> accessed 12 April 2021.

Last but not least, true individual control over personal data – hence effective portability - has proven difficult to achieve due to the disproportionate costs or efforts borne by data subjects, especially with the advent of technologies utilising big data and the ability to turn anything into personal data without individuals' knowledge or communication.[103]

Keeping the above limitations in mind, legal scholars have already analysed the control mechanism of horizontal application of the right and its relationship with competition law.[104] The right is analogous to the control approach of data protection and its limited application (see above, Section 2.3.2). The GDPR addresses the issue from the perspective of data subjects' rights. The main policy objective is to ensure that individuals are in control of their data and trust the digital domain. However, the perspective of competition remains outside the remit of the GDPR, which must be complemented by the limited applicability of competition law (above).[105] The primary aim of data portability is data subjects' control, not competition concerns. It enables access and transferability to or via individuals without creating an access system at the disposal of competitors for product development. Thus, even if data portability impacts on competition for the prevention of service lock-ins alongside the equally limited Regulation

103 Nadezhda Purtova, 'Do Property Rights in Personal Data Make Sense after the Big Data Turn: Individual Control and Transparency' (2017) 10 Journal of Law and Economic Regulation 64.

104 Peter Swire and Yianni Lagos, 'Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique' (2013) 72 Maryland Law Review 335; Inge Graef, Martin Husovec and Nadezhda Purtova, 'Data Portability and Data Control: Lessons for an Emerging Concept in EU Law' (2018) 19 German Law Journal 1359; Inge Graef, 'The Opportunities and Limits of Data Portability for Stimulating Competition and Innovation' (2020) 2 CPI Antitrust Chronicle 1.

105 Ira Rubinstein, 'Big Data: The End of Privacy or a New Beginning?' (2013) 3 International Data Privacy Law 74; Paul De Hert and others, 'The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services' (2018) 34 Computer Law and Security Review 193.

2018/1807 on the free flow of non-personal data,[106] its applicability is narrow. The measure is very far from providing an appropriate data-access regime to satisfy the sharing obligation of European policy goals.[107]

IV. THE CASE FOR PSD2-LIKE REGULATION OF THE PLATFORM ECONOMY

1. Ex-ante Regulation and the PSD2 Model[108]

The Sections above aimed to demonstrate the shortcomings of property, competition, and data protection law enforcement to offer a regulatory framework hospitable to a data-access and sharing regime for the European Data Strategy. A major drawback in digital markets is that they move too fast and are too varied and complex to be supervised ex-post and comprehensively. Moreover, the amorphous nature of big data complicates their 'essentiality' in legal terms. This does not mean that competition law is

---

106 Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union [2018] OJ L303/59. The Regulation operates on two specific obstacles to data mobility, i.e. data localization requirements imposed by Member States and contractual vendor lock-in practices in the private sector (situations where customers are dependent on a single provider and cannot easily switch to a different vendor without substantial costs, legal constraints or technical incompatibilities). On the latter aspect, it facilitates and encourages EU companies to develop self-regulatory codes of conduct to improve the competitive data economy based on the principles of transparency, interoperability and open standards. Companies that provide data processing services should introduce some self-regulatory codes of conduct to ensure the provision of clear and transparent information and thereby avoiding vendor lock-ins. In the case of a dataset composed of both personal and non-personal data, the Regulation applies to the non-personal data part of the dataset.

107 See also the Commission recognition that 'as a result of its design to enable switching of service providers rather than enabling data reuse in digital ecosystems the right [to data portability] has practical limitations'. Commission, 'A European strategy for data' (n 2) 10.

108 PSD2.

generally unfit to preserve the contestability of markets or other structural aspects not covered in this contribution.[109] However, legal intervention could give regulators the power to require or prohibit behaviours to reach desired economic and social outcomes without having to engage in proving unfit competition rules on a case-by-case basis.

Unsurprisingly, ex-ante regulation of the platform economy is gaining popularity in EU policy circles. In preventing a level playing field and obstructing innovation, the bottlenecks created by data are a difficult issue that could be better addressed by the regulatory realm.[110]

On the one hand, regulation ensures higher technical specialisation and can be more effective in addressing the structural problems of markets like the digital ones that cannot be tackled under EU competition rules. On the other hand, it is also capable of more effectively addressing the unfair allocation of resources, welfare, and social harms.[111]

The EU already has sector-specific legislative instruments enabling data-access in place.[112] Before engineering a new one, the question is whether any

---

109 Nicolas Petit, *Big Tech and the Digital Economy: The Moligopoly Scenario* (Oxford University Press 2020).

110 Commission, 'A European strategy for data' (n 2) especially 8, 14.

111 Niamh Dunne, *Competition Law and Economic Regulation, Making and Managing Markets* (Cambridge University Press 2015); Jean Tirole, *Economics for the Common Good* (Princeton University Press 2017); Crémer, de Montjoye and Schweitzer (n 85).

112 See e.g., in the payment services sector, PSD2; in the motor vehicles sector, Regulation (EU) 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles, amending Regulations (EC) No 715/2007 and (EC) No 595/2009 and repealing Directive 2007/46/EC [2018] OJ L151/1; in the digital content sector, Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services [2019] OJ L136/1; in the energy sector, Directive (EU) 2019/944 of the European Parliament and of the Council of 5 June 2019 on

of these could be suitable as a horizontal regulatory model of general applicability. The financial sector is an interesting case to investigate due to the precursory and more mature role it has traditionally played as a data-driven market.[113]

The PSD2 is the EU sector-specific legislation providing a normative data-access framework for payment services within the Internal Market.

Its objective is to lay down the terms for achieving integrated retail payments in the EU that are inclusive not only of existing but also new payment services and market players. Its ambitious goal is to take advantage of innovative technology-enabled solutions (fintech) to generate efficiencies and reach a broader market with more choice and integrated services, at the same time pursuing transparency and consumer protection.[114]

The Payment Services Directive ('PSD1')[115] was the first attempt to comprehensively regulate the sector and provide the necessary infrastructure for the perfection of the internal market. It specified the allocation of risk among service providers and customers, regulated a vast array of payment instruments, enhanced market transparency, and strengthened competition

---

common rules for the internal market for electricity and amending Directive 2012/27/EU [2019] OJ L158/125.

113 George Akelof, 'The Market for "Lemons": Quality Uncertainty and the Market Mechanism' (1970) 84 Quarterly Journal of Economics 488; Joseph Stiglitz and Andrew Weiss, 'Credit Rationing in Markets with Imperfect Information' (1981) 71(3) American Economic Review 393; Douglas Diamond, 'Monitoring and Reputation: The Choice between Bank Loans and Directly Placed Debt' (1991) 99 Journal of Political Economy 689; Allen Berger and Gregory Udell, 'Relationship Lending and Lines of Credit in Small Firm Finance' (1995) 68 Journal of Business 351; More recently, see Dirk Zetzsche and others, 'The Evolution and Future of Data-Driven Finance in the EU' (2020) 57 Common Market Law Review 331.

114 PSD2, recital 6.

115 Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC [2007] OJ L319/1 (PSD1).

by harmonising market access requirements, licencing and access to technical infrastructures.[116] Taking a pro-competition attitude, the PSD1 also enabled the operations of new end-to-end providers, i.e. new firms, in the form of closed platforms that digitally intermediate between the payer and the payee, arranging the payment transaction within their closed system with no dependence on other providers such as the firm where the payment account is held.[117]

At the same time, the market witnessed the emergence of infant front-end providers, i.e. third-party providers (TPP) of digital services based on the customer's payment account held by banks. These services could include payment initiation (Payment Initiation Services or 'PIS')[118] or account information (Account Information Services or 'AIS'),[119] either requiring direct and continuous access to the customer's account and the data therein contained. However, the banks where the payment account are held could legitimately refuse access to their infrastructure on grounds of intellectual

---

116 See e.g. ibid recitals 10, 16-17, 42 and arts 10, 28. In the literature, see Despina Mavromati, *The Law of Payment Services in the EU: The EC Directive on Payment Services in the Internal Market* (Kluwer Law International 2008).

117 A typical example of end-to-end are e-money schemes such as the one provided by PayPal, a well-known firm operating as a payment processor and online payments system that supports instant online money transfers and serves as an electronic alternative to traditional methods like checks or money orders. Other end-to-end examples are virtual currencies/crypto-assets, or electronic money providers.

118 PIS operate as a bridging software between a trader's website and a payer's bank account. Examples of PIS are internet payment gateway providers or mobile wallets that position themselves as interfaces between the payers or the payees and the bank of the payment account.

119 AIS provide a single source of information on the current state of the aggregated finances of payment service users. Examples of AIS are services consolidating in one all the accounts of a person, money management, credit-risk analysis and scoring, financial advice, comparisons, access to targeted offers of other financial services such as credit or insurance, etc. They all analyse a person's transactions on their accounts to provide services based on information.

property protection, security risks, or persistent unclear rules regarding liabilities towards customers.[120]

Whilst applying in principle to online payment services, the PSD1 ignored both the specific issues and new developments of the fast-growing digital market. As a regulatory instrument conceived for payment services offered by traditional incumbents, the legal framework of the PSD1 displayed essentially two limits: i) the de facto low competition in the retail-banking sector characterised by low elasticity of demand, lock-in problems, and exclusivity of payments services linked to the holding of bank accounts;[121] ii) obsolescence in the face of fintech acceleration, with new unregulated market players and services operating outside the relationship between the banks and their account-holding customers.[122]

---

120 Giuseppe Colangelo and Oscar Borgogno, 'Data, Innovation and Transatlantic Competition in Finance: The Case of the Access to Account Rule' (2020) 31 European Business Law Review 573.

121 The Netherlands Authority for Consumers and Markets, 'Barriers to Entry Into the Dutch *Retail* Banking Sector' (June 2014) <https://www.acm.nl/sites/default/files/old_publication/publicaties/13257_barriers-to-entry-into-the-dutch-retail-banking-sector.pdf> accessed 12 April 2021; Commission, 'Impact Assessment Accompanying the document Proposal for a directive of the European parliament and of the Council on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/UE and 2009/110/EC and repealing Directive 2007/64/EC and Proposal for a Regulation of the European Parliament and of the Council on interchange fees for card-based payment transactions' SWD (2013) 288 final; European Central Bank, 'Financial Stability Review' (November 2016) <https://www.ecb.europa.eu/pub/pdf/fsr/financialstability review201611.en.pdf> accessed 12 April 2021; UK Competition and Market Authority, 'The Retail Banking Market Investigation Order 2017' (gov.uk, 2 February 2017) <https://www.gov.uk/government/publications/retail -banking-market-investigation-order-2017> accessed 12 April 2021.

122 European Banking Authority, 'Discussion Paper on Innovative Uses of Consumer Data by Financial Institutions' (2016) EBA/DP/2016/01 <https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1455508/68e9f120-8200-4973-aabc-c147e9121180/EBA-DP-2016-01%20DP%20on%20innovative%20uses%20of%20consumer%20data%20by%20financial%

The fundamental drawbacks of this market physiognomy were the high profit margins of the traditional banking industry to the detriment of consumer welfare and the weak protection of consumers exposed to the legal vacuum of the alternative market of emerging, highly demanded fintech.[123] These trends occurred in a legal environment unfavourable to innovation, where the growth of the digital market played almost no role in policy decisions.[124]

This historical primer on EU payments law suggests similarities with the platform economy in terms of the rationale and extent of the changes heralded by the PSD2. The directive launched the banking industry into uncharted territory, to the extent that many observers have branded the resulting EU payments market a 'revolution'.[125]

20institutions.pdf?retry=1>; European Banking Authority, 'Discussion Paper on the EBA's Approach to Financial Technology (FinTech)' (2017) EBA/DP/2017/02 <https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1919160/7a1b9cda-10ad-4315-91ce-d798230ebd84/EBA%20Discussion%20Paper%20on%20Fintech%20%28EBA-DP-2017-02%29.pdf?retry=1>. In the literature, see Dirk A Zetzsche and others, 'From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance' (2017) EBI Working Paper Series no 6 < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2959925> accessed 12 April 2022; Federico Ferretti, 'Consumer Access to Capital in the Age of FinTech and Big Data: The Limits of EU Law' (2018) 25 Maastricht Journal of European and Comparative Law 476.

123 E.g. consumer protection concerns related to data protection, money laundering and fraud risks, and the difficulties of proof in establishing authorisation in cases of unauthorised payments. See Commission, 'Towards an integrated European market for card, internet and mobile payments' (Communication) COM (2011) 941 final.

124 Mary Donelly, 'Payments in the Digital Market: Evaluating the Contribution of Payment Services Directive II' (2016) 32 Computer Law and Security Review 827.

125 Inna Oliinyk and William Echikson, 'Europe's Payment Revolution' (2018) CEPS Research Report No 2018/06 <https://www.ceps.eu/ceps-publications/europes-payments-revolution/> accessed 12 April 2022, recalling industry trade and consumer groups.

2. The Access to Account Rule as a Game-changer: Open Banking and the Data Economy

With the PSD2, the EU legislature shifted its policy approach to digitalisation and undertook a significant intervention in the single payments market.[126]

Broadly, the law operates on two interrelated levels. Like the PSD1, it intervenes in the establishment, authorisation, and supervision of payment firms and the regulation of payment transactions. Adjusting to the digital market, the directive enlarges the scope of coverage of the law, clarifies the extent of consumer rights and service provider obligations, and reinforces security and authentication requirements.[127] In addition, the PSD2 recognises and incorporates into the regulation those TPPs emerging from new fintech endeavours in payment services. It brings TPPs under the same harmonised standards, requirements, and obligations as traditional payment providers and on an equal footing with them, regardless of the business model they apply.[128] Introducing the so-called 'access to account rule', it opens the market to new services by granting TPPs access to the customer payment accounts held by banks. The latter must allow TPPs authorised by the competent authority in their home Member State[129] access to the data contained in payment accounts in real-time and on a non-discriminatory basis.[130] By accessing and exploiting the large quantity of real-time data of the banking realm, technology firms have started disrupting retail financial markets.[131]

---

126 See, in particular, PSD2, recital 95.

127 See the various provisions of ibid, titles II-IV.

128 Ibid, recitals 27-33.

129 Ibid art 36.

130 Ibid arts 64-68.

131 Oscar Borgogno and Giuseppe Colangelo, 'The Data Sharing Paradox: BigTechs in Finance' (2020) 16 European Competition Journal 492; Oscar Borgogno and Giuseppe Colangelo, 'Consumer Inertia and Competition-sensitive Data

The 'access to account rule' has therefore become the tool to unlock the data power of dominant banks over innovative fintech firms.

The TPPs access payment accounts. Such access must occur securely, under the guidelines laid down by the European Banking Authority ('EBA'),[132] and does not require any payment to the holding banks. The access is only carried out upon the conclusion of a contractual relationship between the account holder and a TPP for the provision of PIS or AIS and is instrumental to providing those kinds of services that require the data contained in the account.[133]

Governance: The Case of Open Banking' (2020) 4 Journal of European Consumer and Market Law 143; Fabiana Di Porto and Gustavo Ghidini, 'I Access Your Data, You Access Mine. Requiring Reciprocity in Payment Services' (2020) 51 IIC - International Review of Intellectual Property and Competition Law 307.

132 PSD2, art.95, followed by European Banking Authority, 'Final Report: Draft Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Communication under Article 98 of Directive 2015/2366 (PSD2)' (2017) EBA-RTS-2017-02 <https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1761863/314bd4d5-ccad-47f8-bb11-84933e863944/Final%20draft%20RTS%20on%20SCA%20and%20CSC%20under%20PSD2%20%28EBA-RTS-2017-02%29.pdf> accessed 12 April 2022; Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication C/2017/7782 [2018] OJ L69/23; European Banking Authority, 'Opinion of the European Banking Authority on the Implementation of the RTS on SCA and CSC' (2018) EBA-Op-2018-04 <https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2137845/0f525dc7-0f97-4be7-9ad7-800723365b8e/Opinion%20on%20the%20implementation%20of%20the%20RTS%20on%20SCA%20and%20CSC%20%28EBA-2018-Op-04%29.pdf?retry=1> accessed 12 April 2022.

133 For PIS, see PSD2, art 66, stating that 'when the payer gives its explicit consent for a payment to be executed and (…)'. For AIS, see PSD2, art 67, providing that 'the account information service provider shall: (a) provide services only where based on the payment service user's explicit consent; (…)'.

These provisions have given rise to the novel concept of 'Open Banking', a market model that shifts from the money business to the data business and vice versa. Account data are shared with new market players of the fintech industry capable of capturing or creating value around existing un- or under-exploited assets.[134] By law, banks must share the data they control for the benefit of fintech firms for the creation of new products or the provision of new services.

Payment accounts contain a vast amount of data for analysis: financial data relating to incoming and outgoing transactions, balances, preferences, patterns, dependencies, behaviours, aspects of social life, etc. They are an exceptional tool for product development, especially when integrated with data from other unrelated sources ('big data') and processed by algorithms powered by artificial intelligence technologies.

The new paradigm of the Open Banking model thus reflects the unbundling of the provision of financial services in multiple market segments and the disintermediation of the banking industry.

Under the PSD2, TPPs are subject to business conduct restrictions and requirements that do not allow them to hold the payer's funds in connection with the service, store sensitive payment data of the service user, or process data beyond that necessary to provide the service.[135] The services can only exist via the traditional providers, creating a new market structure where the latter become digital platforms for the distribution of financial services. They facilitate and create a dependency for the contractual interactions of two or more market agents, but without having any contractual relationship with one of them (the TPP) and at the same time allowing the other one (the customers) to continue the fruition of their own services. The consent of customers is sufficient to allow TPPs to access account data.

---

134 Henry Chesbrough, 'Business Model Innovation: Opportunities and Barriers' (2010) 43 Long Range Planning 354.

135 PSD2, art 66(3).

Thus, the Open Banking environment generates indirect network effects, enabling bilateral ventures not otherwise attainable with other means.[136]

The Open Banking market structure is moving towards a confluence of traditional financial service providers transforming into technological firms (while still engaging in their core business) and technological firms entering the financial services market, where the latter may be infant fintech businesses or established Big-Techs.[137]

From this point of view, the PSD2 is a law that encourages the expanding use of personal data. By forcing data sharing, it enables a vast array of newcomers to access an increasing amount of data sources for novel purposes.

Moreover, the 'access to account rule' does not entail access to an essential facility. It escapes the precise definition of the relevant market, which is a highly discretional exercise.[138] The rule permits the exploitation of a facility controlled by others and at the same time, reinforces the control requirements of data protection law.

The PSD2 also grants stronger bargaining power to consumers in the digital market. Unlike the one-off transfer upheld by the right to data portability, data-access under the PSD2 allows for continuous access to real-time data.

---

136 Markos Zachariadis and Pinar Ozcan, 'The API Economy and Digital Transformation in Financial Services: The Case of Open Banking' (2016) SWIFT Institute Working Paper No 2016-001 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2975199> accessed 12 April 2021; Diana Milanesi, 'A New Banking Paradigm: The State of Open Banking in Europe, the United Kingdom and the United States' (2017) Stanford Law School TTLF Working Papers Series No 29 <https://law.stanford.edu/publications/a-new-banking-paradigm-the-state-of-open-banking-in-europe-the-united-kingdom-and-the-united-states/> accessed 12 April 2021.

137 René Stulz, 'FinTech, BigTech, and the future of banks' (2019) NBER Working Paper No 26312 <https://www.nber.org/papers/w26312> accessed 12 April 2021; Dirk Zetzsche and others, 'The Evolution and Future of Data-Driven Finance in the EU' (n 113); Di Porto and Ghidini (n 131).

138 Di Porto and Ghidini (n 131).

Adopting a pro-competitive perspective, the directive arguably strengthens subjects' control over their data by complementing the data protection right of portability. This way, it addresses the opening-up of retail financial markets. Together, the PSD2 and the GDPR may be regarded as a building block targeting the difficult relationship between competition and consumer protection.

Even as the PSD2 has broken the gatekeeping position of banks in the payment financial services sector, by analogy its regulatory model may well interrupt the gatekeeping role of Big-Techs in the platform economy. The PSD2 has disrupted the financial services sector traditionally dominated by large banks. Likewise, it can unlock the data power of Big-Techs and disrupt the digital market.

In short, it can be argued that the PSD2 attains for a single sector the same goals that the EU aims to achieve more generally with its recent data-access and sharing policies - that is, to ensure competition and consumer protection in the Digital Single Market. It already provides a regulatory model that would not require the reinvention of rules. A fragmented legislative strategy with a diverging data act could have the undesirable result of creating an uneven playing field among sectors, where technological firms enjoy unjustified advantages over traditional market players without reciprocity. Asymmetrical regulatory measures are prone to tilt the market in favour of platforms to the detriment of new market players. This is already the case in the Open Banking market structure, where the Big-Techs are entering the financial services market without reciprocity.[139]

---

[139] Borgogno and Colangelo, 'Consumer Inertia and Competition-sensitive Data Governance' (n 131). For example, note that Google has secured an e-money license after Lithuania granted authorisation. The license enables the company to process payments, issue e-money, and handle electronic money wallets. It gives permission to operate across the EU via the passporting rights system. Likewise, Facebook and Amazon obtained licenses in Ireland and Luxembourg. See Milda Seputyte and Jeremy Kahn, 'Google Payment Expands With E-Money License

A one-size-fits-all Data Act built on the model of the PSD2 may set a fairer playing field, leaving room for competition law enforcement to challenge other anticompetitive practices in the market.

V. Conclusion

The EU has launched an ambitious policy for a Single Data Space. It seeks to combine legislation and governance across business sectors to ensure the free flow, access and sharing of data for competition and innovation. This paper analysed the legal aspects of the datafication process in the context of the market imbalances created by Big-Techs and how they influence the prospective Data Act for the establishment of a data-access and sharing regime for digital market players. It contributes to the field by assessing a recent policy and legislative announcement and advancing a novel suggestion for an alternative and simplified approach. It aimed to show that to build a genuine data-driven market for products and services and accomplish the latest policy goals, the EU should take stock of its legislation in the payments sector. The access to account rule of the PSD2 could be reproduced to grant free access to and sharing of data for innovation, at the same time breaking the gatekeeping role of Big-Techs in the same fashion as it did for banks in the financial services sector.

Many Big-Techs have built their business models on monetising data and acting as gatekeepers. Because data are so important for the digital economy, it is rational to assess the extent to which 'data markets' exist or take shape. No matter how tempting it may be, in legal terms, data cannot be qualified as tradable goods. Their fluid nature finds no parallel with existing concepts and traditional legal doctrines deriving from property and contracts. Likewise, competition principles cannot be directly applied.

From Lithuania' (Bloomberg, 21 December 2018) <https://www.bloomberg.com/news/articles/2018-12-21/google-payment-expands-with-e-money-license-from-lithuania> accessed 12 April 2021.

Therefore, a market for data cannot exist without further complications or elaboration. Instead, digital markets can be considered 'markets for data-driven products and services', where competition and innovation lie in the ability to exploit the data, e.g. through the use of software algorithms, digital infrastructures, or product/service engineering and design. This distinction matters as it hardly justifies gatekeeping practices, where data are controlled de facto without proper legal title except in those established circumscribed situations where intellectual property rights or data protection law intervene.

However, the controls granted by intellectual property escape individual data. Likewise, when data are personal, data protection law addresses data subjects' control as a relative right that does not necessarily exclude the possibility of others accessing or using the data. Moreover, third parties may well access personal data upon data subjects' consent.

De facto control and gatekeeping negatively impact data-driven markets. Yet competition law enforcement is limited in application and does not offer a regulatory framework capable of challenging them. Not only are data amorphous and challenging to traditional legal constructs, but digital markets move too fast and are too varied and complex to be supervised ex-post by the competent authorities. Moreover, competition law does not provide a general approach for applying the essential facility doctrine to dominant platforms; enforcement would depend on the specific circumstances of each case, in terms of the specific conduct in question and its economic context. Competition law may continue to serve the purpose of limiting anticompetitive practices but appears unsuitable to tackle data concentration and bottlenecking.

It seems inevitable that ex-ante regulation, as expressed in the Data Act, will eliminate the limits or uncertainties of competition law enforcement. Yet the question remains of how it can achieve the expected results established in the policy goals.

Arguably, an analysis of the existing sectoral legislation advanced by the PSD2 reveals that the EU does not have to reinvent the wheel. The directive already enacts, in the financial services market, the results envisioned by the EU for the entire digital market. The PSD2 has set a precedent of user-driven data-access, enabling the real-time sharing of data, favouring interconnectedness, and facilitating innovation. By providing for the 'access to account rule', the PSD2 breaks the data monopoly of the traditional banking sector. It has given rise to the Open Banking model that is disrupting the sector, allowing for a free data-access regime where fintech companies (including Big-Techs) enter the market, design new products and provide new services. In such a renewed market, consumers continue to enjoy the usual protections afforded by data protection law. At the same time, the expanded applicability of data portability and reinforced ability to consent to data-access enables consumers to drive the process. More transparent control over data-access further empowers them.

The PSD2 has disrupted the retail financial market and unlocked the data and service power of dominant banks in favour of innovative firms. By analogy, its regulatory model could disrupt the digital market and unlock the data power of Big-Techs.

To the extent that the market failure of the platform economy mirrors the one that existed in the banking sector, the 'access to account rule' could be a replicable legislative model that addresses the market imbalances caused by the Big-Techs. If it works for banks, why shouldn't it be suitable for gatekeeping platforms?