ISSN 1826-3534

federalismi.it
RIVISTA DI DIRITTO PUBBLICO ITALIANO, COMPARATO, EUROPEO

7 APRILE 2021

L'*open banking* e le troppe zone grigie del conflitto tra la legislazione europea sui pagamenti e la tutela dei dati personali

di Federico Ferretti
Professore associato di Diritto dell'Economia
Alma Mater Studiorum – Università di Bologna

L'*open banking* e le troppe zone grigie del conflitto tra la legislazione europea sui pagamenti e la tutela dei dati personali *

di Federico Ferretti
Professore associato di Diritto dell'Economia
Alma Mater Studiorum – Università di Bologna

Abstract [It]: Questo lavoro analizza rilevanti problemi del quadro giuridico dell'*Open Banking* attivato dalla legislazione europea sui servizi di pagamento. La confluenza tra il settore bancario e la *data economy* rivela un mercato nuovo in cui i diritti individuali sono a rischio. L'intersezione normativa tra la legge sui servizi di pagamento (PSD2) e la legge sulla protezione dei dati personali (GDPR) espone non solo uno scarso coordinamento, ma anche un crescente intreccio di nodi giuridici. Le incongruenze giuridiche, le lacune e le difficoltà interpretative vengono esaminate per esporre i rischi operativi che vanno oltre il tecnicismo. In gioco ci sono i diritti fondamentali dei cittadini dell'UE. Un ripensamento, o almeno una correzione, del regime europeo dell'*Open Banking* è necessario per conciliare le esigenze di un mercato emergente e la tutela dei suoi utenti.

Abstract [En]: This work analyses problems in the legal framework of Open Banking enabled by the European legislation on payment services. The conflation between banking and the data economy reveal a brand-new market where individual rights are at stake. The normative intersection between the law on payment services (PSD2) and data protection law (GDPR) expose not only poor coordination but also a growing entanglement of legal knots. The legal inconsistencies, loopholes, and interpretative difficulties are examined to expose operational risks beyond difficulties of legal technicism. Fundamental rights of EU citizens are at stake. A rethinking, or at least a correction, of the European regime of Open Banking is necessary to reconcile the needs of an emerging market and the protection of its users.

Parole chiave: Open Banking, GDPR, consenso, servizi di pagamento, diritti fondamentali
Keywords: Open Banking, GDPR, consent, payment services, fundamental rights

1. Introduzione

Questo contributo identifica ed esamina una serie di problematiche relative al quadro giuridico dell'Open Banking nell'ambito dell'Unione Europea (UE).

Fino a poco tempo fa, il termine <open (aperto)> associato a <banking (operazione bancaria)> poteva suonare come un ossimoro, l'espediente retorico che usa un'apparente contraddizione per rivelare un paradosso. In effetti, la <chiusura> dei rapporti bancari si è tradizionalmente manifestata nell' aspettativa

* Articolo sottoposto a referaggio. Co-funded by the Erasmus+ Programme of the European Union.

di segretezza e obbligo di riservatezza sugli affari finanziari privati delle persone, scontrandosi con l'idea che i loro rapporti e transazioni potessero essere <aperti>.[1] Allo stesso modo, la prospettiva che l'attività bancaria possa essere <aperta> può facilmente fare inarcare le sopracciglia se si considera la crescente enfasi dell'UE sulla protezione dei dati personali che è culminata nell'adozione del regolamento generale sulla protezione dei dati (GDPR).[2]

Tuttavia, con la digitalizzazione dei servizi finanziari, le banche tradizionali e altre nuove tipologie di soggetti finanziari utilizzano sempre più analisi dei dati e tecniche di profilazione per rivolgersi ai clienti e offrire loro prodotti e prezzi personalizzati. Sotto questo profilo, l'innovazione tecnologica sta diventando l'aspetto chiave e dominante per nuovi modelli di businesses nella fornitura di servizi finanziari. La cosiddetta innovazione finanziaria tecnologicamente finalizzata alla fornitura di servizi finanziari ai consumatori (Fintech), in grado di utilizzare grandi set di dati provenienti da varie fonti non correlate (big data) attraverso l'intelligenza artificiale, rappresenta oggi l'aspetto più importante delle ultime accelerazioni della digitalizzazione e sta generando un significativo impatto sui mercati finanziari al dettaglio, con effetti dirompenti sul settore.[3]

---

[1] Tali aspettative e obblighi hanno una lunga tradizione giuridica. Per esempio, si veda Guex, S, "The Origins of the Swiss Banking Secrecy Law and Its Repercussions for Swiss Federal Policy", 74 *Business History Review* (2000), 237-266. Il segreto bancario solleva complesse questioni giuridiche che esulano dallo scopo di questo lavoro. Inoltre, la tutela giuridica della riservatezza, sui clienti bancari, presenta differenze a seconda della giurisdizione e della tradizione giuridica. Per semplificare, nei paesi di *common law* il dovere di riservatezza è un termine implicito nel rapporto contrattuale tra una banca e il suo cliente. L'obbligo non nasce da disposizioni normative ma da precedenti. Il caso seminale è rappresentato da *Tournier v National Provincial and Union Bank of England* [1924] 1 KB 461 (UK), dove è stato stabilito che la banca è tenuta, per tutelare i clienti, a un dovere di riservatezza giuridica, e non meramente morale. Ciò implica che essa non possa legalmente divulgare a terzi le informazioni riguardanti il proprio cliente a meno che la divulgazione non sia imposta dalla legge, vi sia un obbligo di divulgazione nei confronti del pubblico, gli interessi della banca richiedano la divulgazione o la divulgazione venga effettuata con il consenso espresso o implicito del cliente. Nei paesi di diritto civile, per contro, il segreto bancario non si limita a un obbligo contrattuale della banca nei confronti dei propri clienti, ma l'obbligo può anche derivare dalla legislazione, generalmente contenuta nel diritto bancario o nel codice civile, o derivante da usi e consuetudini. Tale obbligo, tuttavia, può decadere in presenza di altre disposizioni che introducano delle eccezioni. In alcuni casi, una violazione del segreto bancario può costituire un reato penale, a differenza delle giurisdizioni di *common law* in cui dà luogo a una richiesta civile di risarcimento danni e/o un diritto a un'ingiunzione per impedire ulteriori divulgazioni. Sul tema, si veda generalmente Campbell D, *International Bank Secrecy* (Sweet & Maxwell, 1992). A livello dell'UE, si veda la causa *C-594/16 Enzo Bucioni / Banca d'Italia [2018] ECLI: EU: C: 2018: 717*, dove la Corte di Giustizia dell'Unione Europea ha confermato che "spetta alle autorità competenti e ai tribunali valutare gli interessi del richiedente nell'avere le informazioni in questione e gli interessi connessi al mantenimento della riservatezza delle informazioni coperte dall'obbligo del segreto professionale, prima di divulgare ogni informazione riservata richiesta".

[2] 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.

[3] Si veda Autorità Bancaria Europea, Documento di discussione sugli usi innovativi dei dati dei consumatori da parte delle istituzioni finanziarie (Londra, 4 maggio 2016); The Financial Inclusion Center, "FinTech - Beware of the Geeks' Bearing Gifts? ", *A Financial Inclusion Center Discussion Paper* (gennaio 2018). Nuovi servizi fintech ai consumatori si stanno sviluppando ed espandendo in modo significativo nell'UE. Secondo Zhang B, Wardrop R, Ziegler T, Lui A, Burton J, James A e Garvey K, *Sustaining Momentum - the 2nd European Alternative Finance Industry Report* (Cambridge University,

Con il business dei dati, che ormai permea l'economia globale, i servizi bancari e quelli di pagamento elettronico rappresentano una frontiera molto esposta alle pressioni competitive del nascente settore Fintech. Da tempo ormai i pagamenti sono caratterizzati da sistemi di trasferimento elettronico di fondi, che sono passati dai servizi di pagamento cartaceo (es. contanti, assegni bancari, traveller's cheques, ecc.) a mezzi elettronici. Nell'economia digitale, conti e dati di pagamento sono diventati una risorsa essenziale grazie alla quale possono essere forniti servizi, non solo dalle banche ma anche da nuovi operatori del mercato in grado di estrarne valore in modo competitivo.

È bene ricordare come la regolamentazione UE dei servizi di pagamento non rappresenti una novità. Nel tempo, essa si è tuttavia trasformata per adeguarsi agli sviluppi del mercato e della moneta, al fine di promuovere la concorrenza e creare condizioni di parità in un ambiente economico in cui i consumatori devono essere prima di tutto protetti da condotte abusive.

Da ultimo, l'innovazione digitale e la concorrenza sono state tra le cause determinanti che hanno indotto il legislatore UE ad adottare la seconda Direttiva sui Servizi di Pagamento entrata in vigore nell'Unione Europea il 13 gennaio 2016 (PSD2).[4] Da un lato, tale legislazione ha modernizzato la regolamentazione esistente in materia di transazioni di pagamento e protezione dei consumatori, in virtù delle mutevoli esigenze portate dalla digitalizzazione. Dall'altra, la PSD2 ha aperto il mercato a nuovi servizi e forze competitive emerse dal settore Fintech. In particolare, essa ha consentito lo sviluppo del c.d. Open Banking, un nuovo modello bancario che garantisce a terze parti, fornitrici di servizi finanziari (TPP), un accesso aperto/libero a servizi bancari, transazioni e altri dati finanziari dei clienti tramite l'uso di interfacce tecnologiche interoperabili (API, dall'inglese Application Programming Interface). L'Open Banking elimina così la concentrazione di informazioni finanziarie in capo alle banche tradizionali e consente la condivisione di conti e dati, al fine di instaurare un nuovo mercato in cui vengono offerti sia servizi tradizionali, sia innovativi. In questo contesto, si instaurano altresì nuove dinamiche concorrenziali che non solo spingono verso una fornitura più efficiente di servizi già esistenti, ma anche per lo sviluppo di nuovi. I nuovi metodi di pagamento mobile o la fornitura di servizi finanziari personalizzati di consulenza finanziaria, prestiti, prodotti assicurativi ne sono un esempio emblematico.

In tal modo, l'Open Banking rimodella il settore bancario dell'UE.

Allo stesso tempo, l'Open Banking pone una serie di problematiche relative alla sua regolamentazione. Questa è un'area in cui la legislazione settoriale della PSD2 si interseca con la legislazione di carattere

2015), il mercato europeo della finanza alternativa online è cresciuto del 92% per raggiungere i 5.431 milioni di euro nel solo 2015.

[4] Direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio, del 25 novembre 2015, sui 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 che abroga la direttiva 2007/64/CE, GU L 337 del 23.12.2015, 35–127.

generale e omnicomprensiva del GDPR, richiedendone un'interpretazione integrata. Tuttavia, proprio un'attenta lettura dei due testi normativi solleva notevoli perplessità non solo circa la necessità di un corretto recepimento della PSD2 da parte degli Stati Membri, ma anche sia per quanto concerne l'applicazione degli operatori del mercato, sia per le garanzie poste a tutela degli utenti dei servizi finanziari.

In siffatto contesto, questo articolo si focalizza sull'analisi dei problemi e delle difficoltà interpretative del quadro giuridico posto dall'Open Banking, al fine di delinearne i profili di incertezza giuridica e i connessi rischi.

Il saggio è impostato come segue.

La Sezione 2 ripercorre il diritto dell'UE nel settore dei servizi di pagamento per mostrarne la transizione verso la digitalizzazione e il Fintech, nonché l'ampiezza dei cambiamenti portati dalla PSD2, conducendo allo stesso tempo gli operatori bancari tradizionali in un territorio nuovo e sconosciuto.

La Sezione 3 prende in esame le disposizioni della PSD2 che istituiscono il nuovo modello di mercato dell'Open Banking, soffermandosi sull'attuale commistione tra attività bancaria classica e quella innovativa che poggia sul business dei dati. La Sezione si chiude con un'analisi che prende in considerazione i punti di contatto e di intersezione tra la disciplina della PSD2 e il GDPR.

Nella successiva Sezione 4, vengono analizzati alcuni aspetti particolarmente problematici che si configurano quando gli obblighi imposti dal GDPR devono trovare applicazione nell'ambito dell'Open Banking. In proposito, si pensi ad esempio ai presupposti giuridici che consentono l'accesso e il trattamento dei dati dei conti bancari, ma che allo stesso tempo dimostrano lo scarso coordinamento con la PSD2.

Nella Sezione 5, viene analizzato il problema relativo alla diversa terminologia giuridica utilizzata rispettivamente dalla PSD2 e dal GDPR. Come verrà messo in luce, infatti, le due disposizioni spesso utilizzano i medesimi termini con significati diversi l'una dall'altra, anche con riferimento alla questione nodale relativa alle condizioni di legittimità per un accesso aperto ai dati. Tale analisi risulta necessaria come base per la successiva analisi circa le incoerenze e le difficoltà interpretative, poste dai due testi normativi, che sarà condotta invece nella Sezione 6.

Il lavoro si chiude infine con una Sezione 7, che evidenzia le conseguenze pratiche e i rischi legati a questo incerto quadro giuridico relativo all'Open Banking.

2. Il percorso della regolamentazione UE fino alla PSD2

La PSD2 definisce il quadro giuridico del mercato unico dei pagamenti dell'UE. Il suo obiettivo è stabilire il quadro normativo finalizzato a instaurare un sistema dei pagamenti al dettaglio integrati nel mercato

unico, che includano non solo i servizi di pagamento esistenti, ma anche nuove tipologie di servizi di pagamento rese possibili grazie allo sviluppo tecnologico. La normativa si propone altresì di regolamentare gli operatori di questo mercato, sfruttando soluzioni tecnologiche innovative (Fintech) capaci di generare efficienze impensabili fino a pochi anni fa. Così facendo, il regolatore cerca di promuovere un mercato caratterizzato da maggiori possibilità di scelta e da servizi più integrati, perseguendo, allo stesso tempo, trasparenza e tutela del consumatore.[5]

Infatti, è stata proprio la spinta verso l'innovazione e la concorrenza, in un mercato tradizionalmente dominato dal settore bancario, che ha determinato la revisione sostanziale e il riordino del regime precedentemente stabilito dalla prima direttiva sui servizi di pagamento (PSD1).[6]

La disciplina europea dei servizi di pagamento trova le proprie radici nell'era precedente all'introduzione della moneta unica, dove la regolamentazione dei pagamenti era principalmente finalizzata a regolare le transazioni transfrontaliere attraverso meccanismi di *soft law* ed integrazione negativa.[7] Solo la successiva introduzione della moneta unica e la creazione dell'area unica dei pagamenti in euro (SEPA)[8] hanno cominciato a costituire i primi tasselli per un modello normativo ibrido pubblico-privato di integrazione positiva. Questo modello, nato grazie alla collaborazione tra il settore bancario privato e le istituzioni dell'UE, era finalizzato a garantire i diritti e gli obblighi nell'ambito interbancario, poggiando sull'interoperabilità di ordini privati. In seguito, la regolazione europea è stata introdotta principalmente per supportare questo sistema di autoregolamentazione del settore bancario, che inevitabilmente si trovava a dover operare in un contesto caratterizzato da una moltitudine di legislazioni nazionali[9]. È stato proprio grazie all'impulso di questa iniziativa del settore privato che il legislatore UE ha adottato la PSD1,

[5] Considerando 6, PSD2.

[6] Direttiva 2007/64/CE del Parlamento europeo e del Consiglio, del 13 novembre 2007, sui servizi di pagamento nel mercato interno, che modifica le direttive 97/7/CE, 2002/65/CE, 2005/60/CE e 2006/48/CE e che abroga la direttiva 97/5/CE, GU L 319 del 5.12.2007, 1–36.

[7] Janczuk-Gorywoda A, "Evolution of EU Retail Payments Law", 40 (6) *European Law Review*, 858-876; Grimigliano G, "The Lights and Shadows of the EU law on Payment Transactions", in Grimigliano G (Ed.) *Money, Payment Systems and the European Union* (Cambridge Scholars Publishing, 2016), 25-38; Vardi N, "Regulation of Payments after the PSD: Is there still a Role for Domestic Law", in Grimigliano G (Ed.) *Money, Payment Systems and the European Union* (Cambridge Scholars Publishing, 2016), 39-56.

[8] European Payments Council, About SEPA, disponibile sul sito https://www.europeanpaymentscouncil.eu/about-sepa

[9] Per esempio, cfr. Direttiva 97/5 / CE del Parlamento europeo e del Consiglio, del 27 gennaio 1997, sui bonifici transfrontalieri, GU L 43 del 14.2.1997, pag. 25-30; Direttiva 2000/46 / CE del Parlamento europeo e del Consiglio, del 18 settembre 2000, concernente l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica, GU L 275 del 27.10.2000, pag. 39–43. In dottrina, Janczuk-Gorywoda, cit. *supra* nota 7; Rabitti M e Sciarrone Alibrandi A, "I servizi di pagamento tra PSD2 e GDPR: Open Banking e conseguenze per la clientela", in F Capriglione (a cura di), *Liber Amicorum Guido Alpa* (CEDAM, 2019), 711-735.

vale a dire una normativa che ha inteso rispondere all'esigenza di creare un quadro giuridico uniforme per i pagamenti in tutta l'UE e fornire, nella eurozona, il supporto legislativo per il SEPA.[10]

Come primo tentativo di regolamentazione completa del settore, atta a fornire l'infrastruttura necessaria per il funzionamento del mercato interno, la PSD1 si è prima di tutto soffermata sulla ripartizione dei rischi tra fornitori di servizi e clienti; ha regolato una vasta gamma di strumenti di pagamento; ha rafforzato la trasparenza del mercato e, infine, ha rafforzato la concorrenza armonizzando i requisiti di accesso al mercato, le licenze e l'accesso alle infrastrutture tecniche.[11]

Assumendo un atteggiamento pro-concorrenziale, la PSD1 ha anche consentito l'operatività di nuovi fornitori c.d. *end-to-end*, ovvero nuove imprese sotto forma di piattaforme (chiuse) che interagivano digitalmente con il pagatore e il beneficiario, organizzando l'operazione di pagamento all'interno del loro sistema chiuso, senza alcun collegamento con gli enti in cui è radicato il conto di pagamento.[12]

Allo stesso tempo, il mercato ha assistito all'emergere di nuovi fornitori c.d. *front-end*, vale a dire terze parti fornitrici di servizi digitali basati sul conto di pagamento del cliente detenuto dalle banche (i c.d. *Third Party Providers* o TPP). Questi servizi possono includere l'iniziazione di pagamenti ovvero servizi di avvio del pagamento (i c.d. *Payment Initiation Services* o PIS),[13] o servizi di informazioni sul conto di pagamento (i c.d. *Account Information Services* o AIS),[14] che possono essere svolti grazie all'accesso diretto e continuo al conto del cliente e ai dati in esso contenuti. Tuttavia, le banche presso le quali è detenuto il conto di pagamento (note anche con la terminologia alternativa di <Fornitori di servizi di pagamento per la manutenzione del conto> – dall'inglese *Account-Servicing Payment Service Providers* o ASPSP) potevano legittimamente rifiutare l'accesso alle proprie infrastrutture per motivi legati alla protezione della proprietà intellettuale, ai rischi per la sicurezza o al permanere di regole poco chiare sulle responsabilità nei

[10] Considerando 1, PSD1.

[11] Per esempio, si vedano gli Art. 10 e 28, PSD1 ed i considerando 10, 16, 17 e 42, PSD1. In dottrina v., Mavromati D, *The Law of Payment Services in the EU: The EC Directive on Payment Services in the Internal Market* (Kluwer Law International, 2008).

[12] Un tipico esempio di *end-to-end* sono gli schemi di moneta elettronica come quello fornito da *PayPal*, una nota azienda che opera come processore e sistema di pagamenti online, supporta trasferimenti di denaro online istantanei e funge da alternativa elettronica a metodi di pagamento tradizionali come assegni o vaglia postali. Altri esempi *end-to-end* sono le valute virtuali/cripto-asset o fornitori di moneta elettronica. Su questo tema v., Colangelo G e Borgogno O, "Open Banking, portabilità dei dati e regime di accesso ai conti di pagamento", in Finocchiaro G e Falce V (a cura di) *Fintech: diritti, concorrenza, regole* (Zanichelli Editore, 2019), 117-132.

[13] I PIS funzionano come software di collegamento tra il sito internet di un trader e il conto bancario di un pagatore. Esempi di PIS sono fornitori di *gateway* di pagamento Internet o portafogli mobili che si posizionano come interfacce tra i pagatori o i beneficiari e la banca del conto di pagamento.

[14] Gli AIS forniscono un'unica fonte di informazioni sullo stato delle finanze aggregate degli utenti dei servizi di pagamento. Esempi di AIS sono i servizi che consolidano, in uno unico, tutti i conti di una persona, servizi per la gestione del denaro, l'analisi e lo *score* del rischio di credito, la consulenza finanziaria, i confronti e l'accesso ad offerte mirate di altri servizi finanziari come credito o assicurazioni, ecc. Questi servizi analizzano le transazioni della persona sui propri conti per fornire servizi integrati costruiti sulle informazioni risultanti.

confronti dei clienti.[15] In breve, la legge consentiva loro di avanzare tutta una serie di obiezioni che hanno di fatto impedito l'operatività di nuovi o concorrenti servizi.

Pertanto, pur applicandosi in linea di principio ai servizi di pagamento online, la PSD1 ha avuto il difetto di ignorare sia le esigenze di dettaglio che i nuovi sviluppi di un mercato digitale in rapida crescita.

In quanto strumento normativo concepito per i servizi di pagamento offerti dagli operatori bancari tradizionali, il quadro giuridico della PSD1 ha mostrato essenzialmente due limiti: i) la scarsa concorrenza, di fatto, nell'ambito del mercato dei servizi bancari rivolti al consumatore, caratterizzato da bassa elasticità della domanda, problemi di *lock-in* ed esclusività dei servizi di pagamento legati alla detenzione di conti bancari;[16] ii) l'obsolescenza nei confronti delle nuove realtà Fintech e del loro ruolo di nuovi operatori di mercato, lasciandoli sostanzialmente privi di regolazione e al di fuori del rapporto tra le banche e la loro clientela.[17]

Gli svantaggi fondamentali di questa fisionomia di mercato erano rappresentati essenzialmente dagli alti margini di profitto del settore bancario tradizionale a scapito dei consumatori, nonché dalla scarsa protezione dei consumatori stessi, esposti al vuoto giuridico del mercato alternativo emergente del Fintech[18] - il tutto in un contesto giuridico sfavorevole all'innovazione, dove la crescita del mercato digitale non ha avuto quasi alcun ruolo nel sottostante contesto politico.[19]

Questo excursus storico sulla normativa UE inerente ai pagamenti si rivela funzionale a segnalare, fin dall'inizio, che il settore bancario tradizionale ha sempre potuto operare, nell'ambito della PSD1, con

---

[15] Colangelo G e Borgogno O, "Data, Innovation and Transatlantic Competition in Finance: The Case of the Access to Account Rule", 31 *European Business Law Review* (2020), 573-610.

[16] 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 November 2016 – Special Feature" (2016), disponibile sul sito https://www.ecb.europa.eu/pub/pdf/fsr/financialstabilityreview201611.en.pdf; UK Competition and Market Authority, "The Retail Banking Market Investigation Order 2017" (2017), disponibile sul sito 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), disponibile sul sito https://www.acm.nl/sites/default/files/old_publication/publicaties/13257_barriers-to-entry-into-the-dutch-retail-banking-sector.pdf.

[17] European Banking Authority, "Discussion Paper on the EBA's approach to financial technology (FinTech)", *EBA/DP/2017/02* (4 August 2017); European Banking Authority, "Discussion Paper on innovative uses of consumer data by financial institutions", *EBA/DP/2016/01* (4 May 2016). In dottrina, Ferretti F, "Consumer Access to Capital in the Age of FinTech and Big Data: the Limits of EU Law", 25 *Maastricht Journal of European and Comparative Law* (2018), 476-499; Zetzsche DA, Buckley RP, Arner DW and Barberis JN, "From FinTech to TechFin: The Regulatory Challenges of Data-Driven Finance", *EBI Working Paper Series n. 6* (2017).

[18] Per esempio, preoccupazioni inerenti alla protezione dei consumatori relative alla protezione dei dati, al riciclaggio di denaro, ai rischi di frode ed alle difficoltà di fornire la prova nello stabilire l'autorizzazione in caso di pagamenti non autorizzati. Cfr. Commissione Europea, Libro Verde Verso un mercato europeo integrato dei pagamenti tramite carte, internet e telefono mobile, COM (2011) 941 definitivo.

[19] Donelly M, "Payments in the digital market: evaluating the contribution of Payment Services Directive II", 32(6) *Computer Law & Security Review* (2016), 827-839.

procedure, strutture tecnologiche e standard operativi con cui aveva grande famigliarità. Malgrado le nuove pressioni competitive, la PSD1 ha così finito per plasmare un mercato ancora più a misura del settore bancario tradizionale. Allo stesso tempo, la storia normativa dei servizi di pagamento si rivela utile per comprendere ed apprezzare la logica e la portata dei cambiamenti apportati dalla PSD2 in un territorio inesplorato per il settore bancario tradizionale, al punto che molti hanno etichettato la PSD2 come <dirompente> ed il risultante mercato dei pagamenti UE come una <rivoluzione>.[20]

3. La PSD2 come punto di svolta: l'Open Banking e la *data economy*

Con la PSD2 il legislatore UE rivoluziona il proprio approccio politico verso la digitalizzazione e interviene in modo sostanziale nel mercato unico dei pagamenti.[21]

In generale, la legge agisce su due livelli correlati.

Da un lato - come la PSD1 - interviene nella costituzione, autorizzazione e vigilanza delle società di pagamento e nella regolamentazione delle operazioni di pagamento. Adattandosi al mercato digitale, la PSDD2 amplia l'ambito di copertura della normativa, chiarisce la portata dei diritti dei consumatori e degli obblighi dei fornitori di servizi, e rafforza i requisiti di sicurezza e autenticazione.[22]

Dall'altro lato, essa riconosce e include nel regolamento quei TPP emergenti dalle nuove realtà Fintech nell'ambito dei servizi di pagamento, applicandogli gli stessi standard, requisiti e obblighi dei fornitori di servizi di pagamento tradizionali, indipendentemente dal modello di business.[23] In tal modo, la PSD2 apre il mercato a nuovi servizi, concedendo ai TPP l'accesso ai conti di pagamento dei clienti radicati presso le banche. Quest'ultime devono consentire, ai TPP autorizzati dall'autorità competente nello Stato Membro di origine[24], l'accesso ai dati contenuti nei conti di pagamento in tempo reale e su base non discriminatoria.[25]

I TPP possono accedere ai conti di pagamento, definiti come <conti detenuti a nome di uno o più utilizzatori di servizi di pagamento utilizzati per l'esecuzione di operazioni di pagamento>.[26] I conti di risparmio e altri conti non qualificabili come <di pagamento> sembrano pertanto esclusi dall'applicazione della PSD2. Questa circostanza sembra convalidata dal caso *Bundeskammer für Arbeiter und Angestellte*, dove la Corte ha confermato che nella nozione di <conto di pagamento> non rientra il conto di risparmio,

[20] Oliinyk I and Echikson W, "Europe's Payment Revolution", *CEPS Research Report No. 2018/06* (September 2018), richiamando i commenti delle associazioni bancarie e dei consumatori in Europa.
[21] Si veda, in particolare, il Considerando 95 della PSD2.
[22] Si vedano le varie disposizioni dei Titoli II, III e IV della PSD2.
[23] Considerando 27-33 della PSD2.
[24] Art. 36 PSD2.
[25] Art. 64-68 PSD2.
[26] Art. 4(12) PSD2.

che consente di esigere, a vista, somme depositate e a partire dal quale le operazioni di versamento e di prelievo possono essere effettuate soltanto attraverso un conto corrente.[27]

Innanzitutto, l'accesso ai conti di pagamento deve avvenire in modo sicuro secondo gli orientamenti stabiliti dall'Autorità Bancaria Europea (ABE).[28]

Inoltre, l'accesso deve avvenire solo previa conclusione di un rapporto contrattuale tra il titolare del conto e un TPP per la fornitura di PIS o AIS. Tale rapporto contrattuale viene insolitamente inquadrato dalla PSD2 come <consenso esplicito>, proprio allo scopo di fornire quei servizi che necessitano dei dati contenuti nel conto stesso.[29]

Queste disposizioni hanno dato origine al nuovo concetto di Open Banking, un modello di mercato che si sposta dal business del denaro a quello dei dati e viceversa, dove i dati dei conti sono condivisi con nuovi operatori di mercato del settore Fintech in grado di cogliere e creare valore intorno a beni esistenti ma fino a quel momento non sfruttati o sottoutilizzati.[30] In virtù di un obbligo imposto dalla legge, le banche devono quindi condividere i dati che controllano con le imprese Fintech, al fine di consentire la creazione di nuovi prodotti e la fornitura di nuovi servizi.

I conti di pagamento contengono una grande quantità di dati da analizzare: dati finanziari relativi a transazioni in entrata e in uscita, saldo e relative date, preferenze, modelli, dipendenze, comportamenti, aspetti della vita sociale, ecc. Essi sono uno strumento eccezionale per la profilazione dei consumatori a scopi predittivi, rivelando allo stesso tempo pregiudizi comportamentali e vulnerabilità in tutti gli aspetti della vita, soprattutto se integrati con dati provenienti da altre fonti non correlate (qui si inserisce il concetto di <big data>) ed elaborati da algoritmi alimentati da tecnologie di intelligenza artificiale.

Nel modello dell'Open Banking, quindi, il nuovo paradigma riflette la disaggregazione (il c.d. *unbundling*) della fornitura di servizi finanziari in più segmenti di mercato, e la disintermediazione del settore bancario. Quest'ultimo, però, diventa fondamentale nell'ecosistema Fintech, assumendo una nuova forma di forzata ma necessaria intermediazione tra l'utente del servizio (il titolare del conto) e il TTP. Ai sensi della

[27] Causa C-191/17, *Bundeskammer für Arbeiter und Angestellte v ING-DiBa Direktbank Austria Niederlassung der ING-DiBa AG* [2018] EU:C:2018:809.

[28] Art. 95 PSD2, seguito da European Banking Authority, *Final draft RTS on SCA and CSC under PSD2 (EBA-RTS-2017-02)* (23 febbraio 2017); Regolamento delegato (UE) 2018/389 della Commissione, del 27 novembre 2017, che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e standard di comunicazione aperti comuni e sicuri C/2017/7782, GU L 69 del 13.3.2018, pag. 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).

[29] Per i PIS, si veda l'Art. 66 PSD2 laddove prevede che "se il pagatore presta il consenso esplicito all'esecuzione di un pagamento (omissis)"; per gli AIS, si veda l'Art. 67 PSD2 in base al quale il prestatore di servizi di informazione sui conti "presta servizi unicamente sulla base del consenso esplicito dell'utente dei servizi di pagamento; (omissis)".

[30] Chesbrough H, "Business Model Innovation: Opportunities and Barriers", 43 *Long Range Planning* (2010), 354-363.

PSD2, i TPP sono soggetti a regole di condotta e restrizioni che non consentono loro di trattenere i fondi del soggetto pagatore in relazione al servizio prestato, memorizzare dati di pagamento sensibili dell'utente del servizio o elaborare dati oltre a quelli necessari per fornire il servizio stesso.[31] I servizi possono esistere solo tramite i fornitori tradizionali presso cui sono radicati i conti, creando una nuova struttura di mercato dove questi ultimi si trasformano da banche in piattaforme digitali per la distribuzione dei servizi finanziari.

Le banche facilitano e creano nuove dipendenze per le interazioni contrattuali di due o più agenti di mercato, ma senza avere alcun rapporto contrattuale con uno di loro (il TPP), consentendo allo stesso tempo all'altro (il cliente) di continuare la fruizione dei propri servizi. Schematizzando, la Parte A (il cliente) può stipulare un contratto con la Parte B (TPP) solo tramite l'intermediazione della Parte C (banca), dove la Parte A e la Parte C hanno un contratto per il conto di pagamento (e possono ancora avere contratti futuri per altri servizi), ma dove la Parte B e la Parte C non hanno alcun rapporto contrattuale (al contrario, possono competere).

Il modello dell'Open Banking genera quindi effetti di rete indiretti, rendendo possibili iniziative bilaterali altrimenti non realizzabili con altri mezzi, e producendo allo stesso tempo nuove dipendenze.[32]

In questo modo, la struttura del mercato dell'Open Banking si muove verso una confluenza tra i fornitori di servizi finanziari tradizionali - che diventano imprese tecnologiche (ma sempre operanti nel business del denaro) - e le imprese tecnologiche che entrano nel mercato dei servizi finanziari. Queste ultime possono essere imprese Fintech start-up o giganti tecnologici affermati che già dominano il mercato dei servizi dati (c.d. <Tech-Fin> o <Big-Tech>).[33]

---

[31] Art. 66(3) PSD2.

[32] Zachariadis M and Ozcan P, "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 D, "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/; Colangelo e Borgonovo, cit. *supra* nota 12.

[33] Zetzsche et al, cit. *supra* nota 17; Di Porto F and Ghidini G, "I access your data, you access mine. Requiring data reciprocity in payment services", 51 *IIC - International Review of Intellectual Property and Competition Law* (2020), 307-329; Stulz RM, "FinTech, BigTech, and the future of banks", *NBER Working Paper No. 26312* (2019), at https://www.nber.org/papers/w26312. Ad esempio, si consideri che Google si è assicurata una licenza per la moneta elettronica dopo che la Lituania le ha concesso l'autorizzazione. La licenza consente all'azienda di elaborare pagamenti, emettere moneta elettronica e gestire portafogli di moneta elettronica. Una tale licenza permette al licenziatario di operare in tutta l'UE tramite I diritti garantiti dal Sistema del passaporto europeo. Allo stesso modo, Facebook e Amazon hanno ottenuto analoghe licenze in Irlanda e Lussemburgo. In tal senso si veda Seputyte M and Kahn J, "Google Payment Expands With E-Money License From Lithuania", *Bloomberg* (21 December 2018), disponibile sul sito https://www.bloomberg.com/news/articles/2018-12-21/google-payment-expands-with-e-money-license-from-lithuania.

Da questo punto di vista, la PSD2 è una normativa che stimola un uso crescente dei dati personali e consente, a una vasta gamma di nuovi operatori, di accedere a un numero sempre maggiore di dati per nuove finalità.

Tuttavia, un tale crescente uso di dati personali, da parte di un sempre maggior numero di operatori, per finalità in continua espansione, genera in automatico più rischi e dubbi per la tutela dei dati stessi, soprattutto alla luce della natura dei dati di conto e le conclusioni che possono essere tratte dal loro trattamento. Usi impropri o abusi possono avere gravi conseguenze per le persone. A questo proposito, la PSD2 non contiene controlli diretti per proteggere i consumatori. Diversamente, essa rimanda all'applicazione della normativa sulla protezione dei dati (il GDPR),[34] con l'avvertenza che i TPP possono accedere e trattare i dati necessari per la fornitura dei propri servizi solo previo "consenso esplicito" dell'utente del servizio di pagamento.[35]

4. L'Open banking e il GDPR

Il trattamento dei dati di conto comporta la necessaria applicazione del GDPR, che in tal modo si sovrappone alla PSD2.

In quanto Regolamento UE, il GDPR è immediatamente applicabile, proprio per eliminare i rischi di particolarità nazionali e diversità applicative, che vanificherebbero l'obiettivo di raggiungere uniformità giuridica nell'Unione.

A prima vista, gli obiettivi della PSD2, in relazione all'Open Banking, e quelli del GDPR appaiono in contrasto tra loro. La prima normativa, infatti, è proiettata verso una maggiore condivisione dei dati con una tendenza espansiva, laddove la seconda si prefigge di proteggerne il trattamento per finalità nuove o diverse rispetto a quelle originarie e limitarne, altresì, la possibilità di libera condivisione.

In assenza di deroghe legislative nella normativa concorrente, è pertanto alla luce dell'importanza della legislazione sulla protezione dei dati che si deve leggere il trattamento dei big data nei servizi finanziari, compresi i dati dei conti trattati nell'Open Banking.[36]

A tal fine, è utile ricordare che la tutela dei dati personali e la privacy sono qualificati dal nostro ordinamento come diritti fondamentali. Il presupposto giuridico della protezione dei dati risiede nell'Articolo 16 TFUE, che lo eleva a disposizione di applicazione generale, ai sensi del titolo II insieme

[34] Art. 94(1) PSD2.
[35] Art. 94(2) PSD2.
[36] In tal senso, si veda anche il Considerando 90 della PSD2, ai sensi del quale la PSD2 "rispetta i diritti fondamentali e osserva i principi riconosciuti dalla Carta dei diritti fondamentali dell'Unione europea, incluso il diritto al rispetto della vita privata e familiare, il diritto alla protezione dei dati personali, la libertà d'impresa, il diritto a un ricorso effettivo e il diritto di non essere giudicati o puniti due volte per lo stesso reato. La presente direttiva deve essere applicata conformemente a tali diritti e principi".

ad altri principi fondamentali dell'UE. Allo stesso modo, l'Articolo 8 della Carta dei diritti fondamentali dell'Unione Europea riconosce la protezione dei dati personali come un diritto fondamentale autonomo e distinto da quello della <privacy> sancito dall'Articolo 7 della Carta stessa. La protezione dei dati è un concetto complesso e dalle molteplici sfaccettature sia dal punto di vista sociale sia giuridico. Tradizionalmente, il suo obiettivo primario è stato identificato con la protezione della privacy o riservatezza della persona nell'ambito delle operazioni di trattamento dei dati personali. I molti dibattiti dottrinali sulla privacy testimoniano non solo la difficoltà nel decifrare un concetto ampio e talvolta ambiguo, ma aiutano altresì a gettare le basi per distinguere la <protezione dei dati> dalla <privacy>.[37] Almeno secondo il diritto dell'UE - e pertanto il diritto nazionale - i due sono diventati diritti fondamentali distinti, ma complementari, che derivano la loro forza normativa da valori che, sebbene a volte coincidenti, possono essere concettualizzati indipendentemente. Mentre le leggi sulla privacy derivano dalla necessità di proteggere una legittima opacità dell'individuo attraverso misure inibitorie, la legge sulla protezione dei dati sancisce le condizioni alle quali il trattamento delle informazioni è legittimo, imponendo la trasparenza del trattamento dei dati, consentendo così il loro pieno controllo da parte dei soggetti interessati il cui trattamento non sia già autorizzato dalla legge stessa in quanto necessario per motivi di un più ampio interesse economico o sociale. In breve, la legge sulla protezione dei dati si concentra sulle attività dei responsabili del trattamento (i c.d. titolari del trattamento) e sulla loro responsabilità, regolando così un esercizio di potere accettato.[38] Sia i regimi di privacy sia quelli di protezione dei dati (ovvero isolamento e legittima riservatezza da una parte, inclusione e partecipazione dall'altra) rappresentano un insieme di tutele legali per perseguire l'obiettivo comune di una società libera e democratica in cui i suoi membri sviluppano la loro personalità liberamente e autonomamente

[37] Si vedano, ad esempio, gli scritti seminali di Warren S and Brandeis L, "The Right to Privacy", 4 *Harvard Law Review* (1890), 193-220; Bloustein EJ, "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser", 39 *New York University Law Review* (1964), 962-1007; Stromholm S, *Right of Privacy and Rights of the Personality* (Norstedt, 1967); Westin A, *Privacy and Freedom* (Atheneum, 1967); Fried C, *An Anatomy of Values* (Harvard University Press, 1970); Rachels J, "Why Privacy is Important", 4 *Philosophy and Public Affairs* (1975), 323-333; Thomson J, "The Right to Privacy", 4 *Philosophy and Public Affairs* (1975), 295-314; Scanlon T, "Thomson on Privacy", 4 *Philosophy and Public Affairs* (1975), 323-333; Gerstein R, "Intimacy and Privacy", 89 *Ethics* (1978), 76-81; Gavison R, "Privacy and the Limits of the Law", 89 *Yale Law Journal* (1980), 421-471; Posner R, *The Economics of Justice* (Harvard University Press, 1981); Parent W, "Privacy, Morality and the Law", 12 *Philosophy and Public Affairs* (1983), 269-288; Inness J, *Privacy, Intimacy, and Isolation* (Oxford University Press, 1992); Johnson J, "Constitutional Privacy", 13 *Law and Philosophy* (1994),161-193; DeCew J, *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology* (Cornell University Press, 1997); Moore A, "Intangible Property: Privacy, Power, and Information Control", 35 *American Philosophical Quarterly* (1998), 365-378.

[38] Davis SG, "Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity", in Agre PE and Rotenberg M (eds.), *Technology and Privacy: The New Landscape* (The MIT Press, 1997), 143-165; De Hert P and Gutwirth S, "Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalisation in Action", in Gutwirth S et al (eds.), *Reinventing Data Protection?* (Springer, 2009), 3-44; Rouvroy A and Poullet Y, "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy", in Gutwirth S et al (eds.), *Reinventing Data Protection?* (Springer, 2009), 45-76.

attraverso l'autodeterminazione individuale. Concedere agli individui il controllo sui propri dati non è solo uno strumento per consentire loro di avere il controllo sulla *persona* che manifestano o esprimono nel contesto sociale - senza il rischio di manipolazioni, distorsioni, false dichiarazioni, semplificazioni, stereotipizzazioni, discriminazioni, classificazioni, alterazioni o vincoli irragionevoli o ingiustificati – ma diventa anche un valore fondamentale. Gli esseri umani hanno, infatti, il diritto di mantenere e sviluppare la propria personalità in un modo che consenta loro di partecipare pienamente alla società senza dover conformare pensieri, convinzioni, comportamenti o preferenze a quelli della maggioranza o a quelli impostati dall'alto dagli operatori economici per interessi commerciali.[39]

In questo contesto, i diritti conferiti dalla legge sulla protezione dei dati diventano diritti partecipativi di autodeterminazione. Il GDPR, pertanto, formula le condizioni alle quali il trattamento dei dati è legittimo.[40]

Tra i tanti aspetti regolamentati dal GDPR, alcune norme richiedono attenzione per la loro attinenza o sovrapposizione con quelle della PSD2.

Nel rispetto dei principi chiave della limitazione delle finalità di trattamento e della minimizzazione dei dati,[41] il GDPR stabilisce i requisiti inerenti a un legittimo trattamento dei dati. Un titolare del trattamento, per poter porre in essere legittimamente l'attività, deve soddisfare i criteri stabiliti dalla legge. L'insieme dei criteri è esaustivo, per cui se un titolare del trattamento non può fare affidamento su uno di essi il trattamento è considerato illecito. A tal fine, la legge distingue tra dati di natura sensibile e non sensibile. Le categorie speciali di dati sensibili sono quelle che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale e il trattamento dei dati relativi alla salute o alla vita sessuale.[42]

Per i dati di natura non sensibile, un trattamento legittimo deve svolgersi in conformità con quanto sancito dall'Art.6 comma 1 GDPR:

a) l'interessato ha prestato il consenso (in modo inequivocabile);

(b) il trattamento dei dati è necessario per l'esecuzione di un contratto di cui l'interessato è parte o per prendere provvedimenti su richiesta dell'interessato prima della conclusione di un contratto;

(c) il trattamento dei dati è necessario per adempiere un obbligo legale del titolare del trattamento;

(d) il trattamento dei dati è necessario per proteggere gli interessi vitali dell'interessato;

---

[39] Rouvroy and Poullet, cit. supra *nota* 38.

[40] In tal senso, De Hert and Gutwirth, cit. *supra* nota 38.

[41] Si veda l'Art. 5 GDPR, in particolare laddove si afferma che "i dati personali devono essere raccolti per scopi determinati, espliciti e legittimi e non ulteriormente trattati in modo incompatibile con tali scopi" (limitazione della finalità) e "i dati personali devono essere adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità per le quali sono trattati" (minimizzazione dei dati).

[42] Art. 9(1) GDPR.

e) il trattamento dei dati è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri;

(f) il trattamento è necessario ai fini degli interessi legittimi perseguiti dal titolare del trattamento o da terzi.

Laddove invece il trattamento riguardi dati personali di natura sensibile, la legge prevede una regolazione più rigorosa.

Ai sensi dell'Articolo 9 paragrafo 2 del GDPR, infatti, il trattamento di questi dati è consentito solo:

a) se gli interessati hanno dato il loro <consenso esplicito>;

(b) il trattamento è necessario ai fini dell'adempimento degli obblighi ed esercizio di specifici diritti del titolare o dell'interessato in materia di diritto del lavoro, previdenziale e di protezione sociale;

(c) il trattamento è necessario per proteggere gli interessi vitali dell'interessato o di un'altra persona se l'interessato è fisicamente o legalmente incapace di fornire il consenso;

(d) il trattamento è svolto nel corso di attività legittime con garanzie adeguate da una fondazione, associazione o altro ente senza scopo di lucro con finalità politiche, filosofiche, religiose o sindacali;

(e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;

f) il trattamento è necessario per l'accertamento, l'esercizio o la difesa di rivendicazioni legali o ogniqualvolta i tribunali agiscano nella loro capacità giudiziaria;

(g) il trattamento è necessario per motivi di interesse pubblico sostanziale;

(h) il trattamento è necessario ai fini della medicina preventiva o del lavoro, per la valutazione della capacità lavorativa del dipendente, la diagnosi medica, l'erogazione di cure o cure sanitarie o sociali o la gestione di sistemi e servizi sanitari o sociali;

i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica;

(j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, per scopi di ricerca scientifica o storica o per scopi statistici.

Nel caso in esame, soprattutto per la fornitura di AIS, le soluzioni Fintech fanno un ampio uso delle tecniche di profilazione, che costituiscono l'elemento caratterizzante del proprio modello di business. Laddove viene effettuata la profilazione, il GDPR richiede un ulteriore livello di controllo. Esso postula che gli individui abbiano il diritto di non essere soggetti a una decisione basata esclusivamente sul trattamento automatizzato per valutare determinati aspetti personali.[43] La profilazione può essere utilizzata, qualora sia necessaria per esigenze contrattuali; previa autorizzazione da parte della normativa comunitaria o nazionale, oppure sia basata sul <consenso esplicito> dell'interessato.

[43] Art. 4(4) GDPR.

Nel caso di decisioni automatizzate basate sul <consenso esplicito> o sull'adempimento contrattuale, i titolari del trattamento devono rispettare il diritto degli interessati di ottenere l'intervento umano, esprimere il proprio punto di vista e contestare le decisioni. In ogni caso, le decisioni automatizzate non possono essere basate sui dati sensibili di cui all'Articolo 9, paragrafo 1 del GDPR.[44]

Un ultimo istituto introdotto dal GDPR - ma non per questo meno importante per responsabilizzare gli interessati - è il diritto alla portabilità dei dati, ovvero il diritto di trasmettere o far trasmettere i dati a un altro titolare del trattamento laddove il trattamento sia fondato sul <consenso> o su un contratto.[45]

Da un primo esame di queste norme del GDPR, che si collegano all'Open Banking regolato dalla PSD2, si può quindi affermare che, in linea di principio, le due normative non sono necessariamente in conflitto - come potrebbe apparire a una prima lettura - poiché entrambe mirano in realtà a garantire trasparenza e controllo dell'utente.

Tuttavia, si deve segnalare come alcune incongruenze derivino dalla necessaria convivenza e coordinamento tra i due plessi normativi, soprattutto ai fini dell'operatività dell'Open Banking. In particolare, un primo ambito problematico riguarda proprio la base giuridica che legittima l'utilizzo dei dati di conto e dai conseguenti diritti e obblighi delle parti.

Il leitmotiv del <consenso> nelle due leggi, sotto forma di <non qualificato> o <esplicito>, ha innescato discussioni all'interno degli Stati Membri e tra le parti interessate in merito alla corretta attuazione della PSD2, con riferimento alle misure relative alla protezione dei dati personali.[46] A sua volta, tale tema innesca, a cascata, una serie di questioni di rilevanza pratica per le imprese, per i soggetti interessati e per gli interpreti del diritto.

5. La questione del "consenso": significati giuridici sovrapposti

5.1. Il <Consenso> nella PSD2

Il Capitolo 4 della PSD2 si intitola <protezione dei dati>, sebbene esso sia composto da un solo articolo suddiviso in due parti (art. 94 PSD2). La prima fa espresso rinvio all'applicazione della Direttiva 95/46/CE,[47] la disciplina previgente, limitandosi a sancire che qualsiasi riferimento all'abrogata direttiva 95/46/CE debba essere interpretato come riferimento al GDPR.

[44] Art. 22 GDPR.

[45] Art. 20 GDPR.

[46] Si veda, ad esempio, European Data Protection Board, *Letter to Sophie in 't Veld, Member of the European Parliament* (Brussels, 5 July 2018); BEUC, *Consumer-Friendly Open Banking* (Brussels, 20 September 2018); European Banking Federation, *European Banking Federation's comments on the Article 29 Working Party guidelines on consent* (wp259), (Brussels, 23 January 2018).

[47] Direttiva 95/46 / CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, GU L 281 del 23.11.1995, 31– 50.

Allo stesso tempo, l'Articolo 94 (2) PSD2 stabilisce che <i prestatori di servizi di pagamento hanno accesso, trattano e conservano i dati personali necessari alla prestazione dei rispettivi servizi di pagamento, *solo dietro consenso esplicito dell'utente dei servizi di pagamento*> (corsivo aggiunto).

In tal modo, la PSD2 sembra specificare che, per il trattamento dei dati di conto, il consenso debba essere <esplicito>.

Il requisito della PSD2 di <consenso esplicito> si contrappone ai termini <consenso> e <consenso esplicito> delle già esaminate disposizioni del GDPR,[48] facendo sorgere il dubbio se tali espressioni abbiano dunque lo stesso significato, nel contesto delle due normative. Sorge anche incertezza sulla necessità della PSD2 di dover qualificare, riproducendolo, un termine già rilevabile nel GDPR, qualificando il requisito di un <consenso esplicito>.

Occorre precisare che altre disposizioni della PSD2 fanno riferimento al <consenso> per quanto riguarda l'autorizzazione di un'operazione di pagamento. Ai sensi dell'Articolo 64 PSD2, un'operazione di pagamento può essere autorizzata <solo se il pagatore ha prestato il suo consenso ad eseguire l'operazione di pagamento>. Questo semplice <consenso> per autorizzare un pagamento viene successivamente denominato <consenso esplicito> negli articoli 65 e 66 PSD2, quando vengono specificate le azioni che le banche devono eseguire per garantire il diritto del pagatore di utilizzare un PIS.[49] Allo stesso modo, gli AIS possono prestare servizi <unicamente sulla base del *consenso esplicito* dell'utente dei servizi di pagamento>.[50] (enfasi aggiunta)

A parere di chi scrive, il <consenso> e il <consenso esplicito>, richiamati in queste disposizioni, non si riferiscono all'accesso o al trattamento dei dati, ma all'autorizzazione di un servizio PIS o AIS. Trattasi pertanto di un accordo contrattuale, anche se equivocamente normato nella dicotomia terminologica di <semplice o non qualificato> ovvero <esplicito> nel campo del diritto contrattuale privato. A causa di tale equivoco, la PSD2 sembra gettare ombre sulla forma e attuazione contrattuale ricevuta nei sistemi giuridici degli Stati Membri, nonché sulla compatibilità di un tale requisito con il diritto contrattuale nazionale dei diversi sistemi giuridici. Per quanto interessante, non si ritiene opportuno indulgere, in questa sede, su una simile questione, che esula dall'ambito di analisi di questo lavoro.

Per ciò che qui rileva, il problema interpretativo si pone per l'uso degli stessi termini all'interno della PSD2, che sembrano non avere lo stesso significato. Infatti, le norme in esame non operano sullo stesso livello: gli Articoli 64-67 PSD2 fanno riferimento all'accordo contrattuale, mentre l'Articolo 94, paragrafo 2 PSD2 si riferisce al trattamento dei dati.

[48] Si vedano, rispettivamente, gli Art. 6(1)(a) GDPR and Art. 9(1) GDPR.
[49] Art. 66 PSD2.
[50] Art. 67 PSD2.

Resta da capire, pertanto, se il "consenso esplicito" inerente al trattamento dei dati ai sensi della PSD2 abbia lo stesso significato e debba essere interpretato alla stessa stregua di quello sancito dal GDPR.

5.2. Il 'Consenso' ai sensi del GDPR

Il consenso dell'interessato ai sensi del GDPR rappresenta probabilmente uno degli istituti più complessi da applicare nell'ambito del trattamento dei dati personali.[51] L'aggiunta qualificata della PSD2, pertanto, non facilita il compito dell'interprete.

Nell'ambito della legge sulla protezione dei dati, il consenso è un elemento chiave che permette il trattamento dei dati personali da parte dei titolari del trattamento, altrimenti vietato. Quando un soggetto interessato presta un valido consenso, i titolari del trattamento vengono liberati dalle restrizioni previste dalla legge. Il trattamento diventa lecito dal momento in cui il consenso viene espresso in modo univoco. Per legge, il consenso deve essere granulare e distinto dalle dichiarazioni riguardanti altre questioni (Articolo 7 [2] GDPR). Deve trattarsi di <manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato> (Articolo 4 [11] GDPR). Di conseguenza, la legge impone il <consenso affermativo>, che richiede alla persona interessata di manifestare il proprio assenso <mediante dichiarazione o azione positiva inequivocabile> (Articolo 4 [11] GDPR). Allo stesso tempo, come si è visto, il GDPR continua a distinguere tra <consenso esplicito> - se i dati in questione sono dati personali sensibili e consenso <inequivocabile> per tutti gli altri dati personali (Articolo 6 GDPR combinato con Articolo 4 GDPR).

La questione di quale standard di consenso debba essere applicato ai sensi del GDPR è stata oggetto di intensi dibattiti e negoziati, nella lunga fase di proposta del GDPR. La storia legislativa del GDPR dimostra che la versione finale ha volutamente mantenuto diverse qualificazioni del consenso e la distinzione tra consenso <non ambiguo> ed <esplicito>, a seconda della natura ordinaria o sensibile dei dati. In particolare, non si comprende, nell'ambito del GDPR, quale sia la differenza tra la nozione di consenso <esplicito> e <non ambiguo> che debba trovare manifestazione <con un'azione positiva>. Ad esempio, non è chiaro fino a che punto il consenso implicito possa rimanere valido.[52] Sebbene il

[51] Così come esemplificato dai numerosi interventi interpretativi del Comitato Europeo per la Protezione dei Dati (in precedenza denominato "Gruppo di Lavoro Articolo 29"), l'organo europeo competente per l'applicazione delle norme sulla protezione dei dati nell'Unione e promuove la cooperazione tra le autorità nazionali competenti per la protezione dei dati dell'UE. Si vedano 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* (Brussels, 4 May 2020).

[52] A questo proposito, l'ultimo parere del 2020 del Comitato Europeo per la Protezione dei Dati non è di particolare aiuto, limitando la propria interpretazione all'affermazione che "tutte le presunte forme di consenso fondate su una più

GDPR stabilisca che <non dovrebbe pertanto configurare consenso il silenzio, l'inattività o la preselezione di caselle> (Considerando 32 GDPR), allo stesso tempo afferma anche che il consenso può essere prestato tramite <qualsiasi altra dichiarazione o qualsiasi altro comportamento che indichi chiaramente in tale contesto che l'interessato accetta il trattamento proposto> (Considerando 32 GDPR). In ogni caso, i titolari del trattamento devono essere in grado di dimostrare che gli interessati hanno acconsentito (Articolo 7 GDPR).

La distinzione tra consenso <esplicito> e <inequivocabile> risulta importante all'atto pratico, dal momento che diversi modelli di prestazione del consenso possono tradursi in soluzioni ingegneristiche di prodotti e servizi molto diverse tra loro, soprattutto nel dominio digitale. Nel modello di consenso <esplicito>, sarà necessaria una casella di selezione o una dichiarazione di consenso. Tuttavia, nel modello di consenso <inequivocabile>, che rileva nell'ambito dei servizi commerciali, un'informativa evidente insieme a un '<azione affermativa> possono essere sufficienti per ottenere un consenso implicito, senza la necessità di crociare un'apposita casella o di una dichiarazione di consenso.

Nel campo della protezione dei consumatori, ciò può fare una differenza sostanziale in termini di modalità di raccolta del consenso dei consumatori, del tipo di interfaccia presentata loro, nonché delle modalità con cui essi interagiscono con il fornitore del prodotto o del servizio. In definitiva, questo impatta sulla reale conoscenza e sul controllo che i consumatori possono avere sia sul trattamento dei loro dati personali, sia sugli usi che possono esserne fatti.

Il consenso deve fare affidamento sulla trasparenza e su un '<azione affermativa> (sia esplicitamente data o dedotta attraverso la condotta), ma il modo in cui questo si traduce nella pratica può rimanere vago, soprattutto nella complessità delle transazioni finanziarie.

Per completezza, va aggiunto che il GDPR stabilisce esplicitamente che gli interessati abbiano un successivo diritto di revoca del consenso eventualmente prestato. L'interessato può revocare il consenso in qualsiasi momento e ciò deve essere semplice quanto la concessione del consenso stesso. Tuttavia, è opportuno ricordare come la revoca del consenso non pregiudichi la liceità del trattamento occorso antecedentemente alla revoca stessa (Art. 7 (3) GDPR).

La complessità dei modelli di business del Fintech, le pratiche di raccolta dati, le relazioni fornitore-cliente o le applicazioni tecnologiche possono rendere impossibile, per i consumatori, capire a cosa stiano acconsentendo. Allo stesso modo, queste complessità possono in pratica rendere i consumatori incapaci di decidere liberamente e accettare consapevolmente le conseguenze del consenso al trattamento dei dati, in particolare di fronte alla prospettazione di un vantaggio economico immediato.

implicita forma di azione dell'interessato (ad esempio, una casella di consenso preselezionata) non possano essere conformi allo standard di consenso del GDPR". Si veda European Data Protection Board, cit. *supra* nota 51, 20.

Nonostante l'apparentemente solida protezione giuridica offerta agli interessati, il consenso può essere ottenuto con diverse metodologie che possono giungere ad abusarne, ad ampliarlo indebitamente o, talora, a confonderlo, rendendolo un requisito poco efficace ai fini del trattamento dei dati.[53]

Un mezzo meccanico e automatizzato, per ottenere un generale consenso al trattamento dei dati, può essere costituito dal trattare il consenso come un momento transazionale, tramite l'utilizzo di accordi standard.[54] Ad esempio, nel campo dei servizi finanziari, prevedere come condizione la prestazione del consenso può essere un metodo comune ma elusivo per ottenere il consenso dei consumatori. Spesso, il consenso rischia di venire associato al paradigma giuridico del contratto. Allo stesso tempo, il rapporto contrattuale impresa-consumatore rappresenta una tipica situazione di squilibrio tra le parti. Al consumatore (la parte debole) non viene offerta molta scelta se non quella di accettare i termini dei prestatori del servizio se desiderano ottenerlo. In pratica, il consenso del consumatore diventa obbligatorio o presunto.

In un tale contesto, i modelli Fintech si fondano sullo sfruttamento dei dati. Come visto sopra, tuttavia, la PSD2 nomina il consenso contrattuale e il consenso al trattamento dei dati nello stesso modo (<consenso esplicito>), sebbene in due articoli e contesti diversi.[55]

Il meccanismo giuridico del consenso diventa ancora più problematico laddove il GDPR intende ulteriormente proteggere i soggetti interessati affermando che il consenso non dovrebbe essere considerato liberamente prestato se questi ultimi sono <nell'impossibilità di rifiutare o revocare il consenso senza subire pregiudizio> (Considerando 42 GDPR) o <qualora esista un evidente squilibrio tra l'interessato e il titolare del trattamento> (Considerando 43 GDPR). Studi recenti dimostrano che, al fine di ottenere specifici vantaggi transazionali e personali, la maggior parte dei consumatori acconsente o divulga volontariamente informazioni personali e sulle proprie attività sociali senza pensare agli effetti della loro divulgazione, rendendo così il consenso inefficace di fatto. Tuttavia, un numero limitato di consumatori comprende le conseguenze di un tale compromesso, incluso il modo in cui i titolari del trattamento utilizzano i loro dati personali. Non solo il trattamento dei dati può essere molto complesso e non trasparente, ma alla maggior parte dei consumatori mancano sia le informazioni sia la capacità di valutare adeguatamente la propria decisione di prestare il consenso.[56]

---

[53] A rigore, un consenso che non rispetta i requisiti di legge o che è viziato dovrebbe essere considerate nullo e dovrebbe invalidare ogni trattamento dei dati *ex tunc*. Si veda Mantelero A, "The future of consumer data protection in the EU. Re-thinking the 'notice and consent' paradigm in the new era of predictive analytics" 30 *Computer Law and Security Review* (2014), 643-660; Kosta E, *Consent in European Data Protection Law* (Martinus Nijhoff, 2013).

[54] Brownsword R, "Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality", in Gutwirth S et al. (eds.) *Reinventing Data Protection?* (Springer, 2009), 83-110.

[55] Articoli 64-67 PSD2 e Articlo 94 PSD2.

[56] Pasquale F, *The Black Box Society* (Harvard University Press, 2015); Peppet SR, "Unraveling Privacy: The Personal Prospectus and the Threat of a Full Disclosure Future", 105(3) *Northwestern University Law Review* (2011), 1153-1204;

Alla fine, pertanto, risulta poco chiaro come poter conciliare le ambizioni del legislatore con la realtà del Fintech.

6. Molteplici complicazioni giuridiche

6.1. La base giuridica per il trattamento dei dati di conto

Il quadro giuridico finora evidenziato si complica nel momento in cui l'interprete è chiamato a stabilire la base giuridica appropriata per il trattamento dei dati di conto.

Prima facie, il trattamento dei dati di conto sembra trovare fondamento nella necessità contrattuale di cui all'Articolo 6, paragrafo 1, lettera b) GDPR. Ai sensi di tale norma, i TPP non avrebbe nemmeno bisogno del consenso del cliente.

Di per sé, i dati finanziari non vengono considerati dati sensibili dalla normativa. La situazione finanziaria di una persona non viene contemplata come categoria speciale ai sensi dell'Articolo 9, paragrafo 1 GDPR. In linea di principio e in tale ottica, si aggiunga che i PIS o gli AIS non sono servizi che fanno uso di dati sensibili o forniscono un servizio di natura sensibile.

Questo, per lo meno, è il punto di vista sostenuto dal Comitato Europeo per la Protezione dei Dati (EDPB) - l'Autorità europea responsabile della supervisione e della coerente applicazione del GDPR nell'UE - in una lettera indirizzata a un membro del Parlamento europeo (ossia un orientamento non espresso in forma di linee guida ufficiali). Allo stesso tempo, l'EDPB considera il "consenso esplicito" dell'Articolo 94, paragrafo 2 PSD2 come un consenso contrattuale, senza così interferire con la legittimazione al trattamento dei dati, che poggia sulla necessità contrattuale. Secondo l'Autorità, l'Articolo 94 (2) PSD2 dovrebbe essere interpretato nel senso che quando si stipula un contratto con un prestatore di servizi di pagamento ai sensi della PSD2, gli interessati devono essere pienamente consapevoli delle finalità per le quali i loro dati personali saranno trattati e devono concordare tali clausole esplicitamente. Queste ultime dovrebbero essere chiaramente distinguibili dalle altre questioni presenti nel contratto e dovrebbero essere esplicitamente accettate dall'interessato. Sempre secondo l'EDPB, pertanto, il concetto di <consenso esplicito> ai sensi dell'Articolo 94, paragrafo 2 PSD2 diviene quindi

Borghi M, Ferretti F, and Karapapa S, "Online Data Processing Consent Under EU Law: A Theoretical Framework and Empirical Evidence from the UK", 21 *International Journal of Law and Information Technology* (2013), 109 – 153; Edgar A, Whitley A, and Pujadas R, "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), disponibile sul sito https://www.fs-cp.org.uk/sites/default/files/fscp_report_on_how_consumers_currently_consent_to_share_their_data.pdf

un requisito aggiuntivo di natura contrattuale. Di conseguenza, si tratta di un consenso esplicito diverso da quello del GDPR.[57]

A parere di chi scrive, però, l'interpretazione di cui sopra non è convincente e deve essere respinta.

Il considerare il <consenso esplicito> come contrattuale non spiegherebbe perché sia stato previsto dal legislatore proprio nella norma della PSD2 relativa alla protezione dei dati in una separata sezione a tal uopo esplicitamente dedicata. Inoltre, questa interpretazione non solo metterebbe in discussione la lettera della norma, laddove afferma che per l'accesso, il trattamento e la conservazione è richiesto un <consenso esplicito> solo nella misura necessaria per la fornitura dei servizi, ma sarebbe altresì in contraddizione con il significato contrattuale di "consenso" utilizzato negli Articoli 64-67 PSD2. Come si è visto sopra (si veda la Sezione 5.1), infatti, trattasi di norme che non operano sullo stesso terreno dell'Articolo 94 PSD2.

Probabilmente più grave, tuttavia, appare la considerazione che, con una tale interpretazione, l'EDPB sembra operare al di fuori del suo mandato. La lettura dell'EDPB fornisce un'interpretazione originale in materia di diritto privato dei contratti, non in materia di protezione dei dati. L'influenza del diritto dell'UE nell'area della teoria del diritto privato contrattuale è già di per sé materia complessa e non priva di controversie dottrinali.[58] Pertanto, l'introduzione da parte del EDPB di un ulteriore livello di consenso contrattuale rafforzato, separato ed <esplicito> (vale a dire in puro ambito contrattuale) nei sistemi giuridici di diversi Stati Membri non avverrebbe certo senza problemi di conformità con tali ordinamenti e non sarebbe esente da contrasti. Esso metterebbe altresì in dubbio la legittimità del diritto dell'UE in una sfera di competenza nazionale.

Inoltre, è tutt'altro che chiaro cosa si intenda per <requisito aggiuntivo di natura contrattuale>. Si tratterebbe, probabilmente, di una nozione affine a quella delle clausole vessatorie proprie del diritto italiano, ma aliena ad altri ordinamenti nazionali dei paesi dell'UE. Sicuramente, non può essere né l'ambizione né la competenza dell'EDPB quella di armonizzare una siffatta nozione contrattuale estranea a un vasto numero di sistemi di diritto privato degli Stati Membri. Inoltre, si tratterebbe di una nozione contrattuale incapace di condurre ad un'attuazione, interpretazione o applicazione uniforme del diritto UE negli Stati Membri, compito peraltro non di competenza dell'EDPB ma della Corte di Giustizia dell'UE.

Vale inoltre la pena insistere sul difetto di competenza dell'EDPB. Una tale questione pone un'ulteriore problematica relativa alle competenze di vigilanza sulla PSD2 – a rigore, proprie dell'ABE - e sul

[57] European Data Protection Board, cit. *supra* nota 46. Sul punto, si veda anche Rabitti e Sciarrone Alibrandi, cit. *supra* nota 9.

[58] Per tutti, si veda per esempio Rutgers J and Sirena P (eds.), *Rules and Principles in European Contract Law* (Intersentia, 2015); Miller L, *The Emergence of EU Contract Law – Exploring Europeanization* (Oxford University Press, 2011).

coordinamento tra l'ABE e l'EDPB, soprattutto perché l'EDPB non qualifica la questione come una nozione di protezione dei dati propria del GDPR. Al contrario, una simile costruzione giuridica rischia di creare un'ulteriore area di sovrapposizione e conflitto tra le due normative.

Come considerazione complessiva dell'analisi di cui sopra, pertanto, si potrebbe concludere che l'intervento dell'EDPB, volto a chiudere una falla, ha l'effetto indesiderato di causare, altrove, un allagamento.

6.2. Dati sensibili e non sensibili

Nel tentativo di stabilire la base giuridica del trattamento dei dati di conto, è necessario notare che in determinate situazioni i dati sui pagamenti possono rivelare aspetti di natura razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza a sindacati, salute, vita sessuale o orientamento sessuale di una persona. Ne siano un esempio i pagamenti effettuati ad associazioni sindacali, politiche o religiose. I pagamenti possono rivelare preferenze o orientamenti sessuali. Le spese mediche rivelano molti ambiti personali e sensibili. Simili esempi potrebbero continuare.

Pertanto, in quest'ottica, i dati di conto potrebbero essere considerati sensibili.

Nel trattamento dei dati sensibili, tuttavia, l'Articolo 9, paragrafo 2 GDPR non riconosce la necessità contrattuale come eccezione al divieto generale di trattare categorie speciali di dati ai sensi del precedente Articolo 9, paragrafo 1 GDPR. Al contrario, richiede che si applichi il "consenso esplicito".

Questa osservazione mette in discussione la base giuridica che dovrebbe essere realmente utilizzata per elaborare i dati di un conto di pagamento. A seconda delle circostanze, tale trattamento può essere considerato non sensibile o sensibile. Cosi, in determinate situazioni, i dati possono essere trattati per motivi contrattuali, senza il consenso dell'interessato, laddove in altre situazioni dovrebbe venire richiesto il <consenso esplicito> dell'interessato.

Per contro, la PSD2 indica il <consenso esplicito> indipendentemente da qualsivoglia distinzione, sollevando la questione se l'Articolo 94, paragrafo 2 PSD2 costituisca *lex specialis* rispetto al GDPR. Una risposta in senso positivo significherebbe che il "consenso esplicito" dovrebbe sempre costituire la base giuridica per il trattamento dei dati di conto indipendentemente dalla natura dei dati trattati. Al contrario, un'interpretazione in senso negativo comporterebbe che i TPP dovrebbero conformarsi sia ai requisiti della PSD2 sia a quelli del GDPR; oppure, in alternativa, si potrebbe ipotizzare di utilizzare la PSD2 come prevalente sul GDPR *ad abundantiam*.

Ad ogni buon conto, in assenza di un'interpretazione ufficiale sulla questione, il rinvio del Considerando 90 PSD2 alla necessaria attuazione degli articoli della PSD2 in conformità - *inter alia* - alla legge sulla protezione dei dati[59], sembra potere escludere il rapporto *lex specialis* - *lex generalis* tra le due disposizioni.[60] Mantenendo pertanto che la PSD2 non sia *lex specialis* e nell'impossibilità di separare in pratica il trattamento dei dati sensibili da quelli non sensibili, probabilmente il requisito del "consenso esplicito" dovrebbe costituire la base giuridica più sicura per il trattamento dei dati di conto ai sensi del GDPR. Pertanto, il requisito *ad abundantiam* del "consenso esplicito" della PSD2 verrebbe considerato dello stesso livello o standard di quello GDPR.

Questa interpretazione sarebbe anche conforme al requisito del "consenso esplicito" richiesto ai fini della profilazione, ai sensi dell'Articolo 22 del GDPR.

Dopo una tale analisi, tuttavia, questa interpretazione risulterebbe in contrasto con gli standard tecnici di regolamentazione emanati della Commissione Europea sull'Autenticazione dei Clienti e sui Requisiti per la Comunicazione Comune e Sicura (RTS, dall'inglese *Regulatory Technical Standards*),[61] secondo cui le banche devono fornire agli AIP informazioni a condizione che i dati di pagamento sensibili non siano inclusi,[62] indicando così che non possono essere trattati neanche con il "consenso esplicito" del titolare del conto. Detto questo, non è altresì chiaro come gli RTS possano mai essere in discontinuità con il GDPR.

Alla luce di tutto quanto sopra, pertanto, ai fini della certezza del diritto, non rimane che richiedere l'intervento ufficiale della CGUE o del legislatore dell'UE, vale a dire le uniche istituzioni competenti a tal fine.

---

[59] Ai sensi del Considerando 90 PSD2, "la presente direttiva rispetta i diritti fondamentali e osserva i principi riconosciuti dalla Carta dei diritti fondamentali dell'Unione europea, incluso il diritto al rispetto della vita privata e familiare, il diritto alla protezione dei dati personali, la libertà d'impresa, il diritto a un ricorso effettivo e il diritto di non essere giudicati o puniti due volte per lo stesso reato. La presente direttiva deve essere applicata conformemente a tali diritti e principi".

[60] Questa problematica ha lasciato nell'incertezza anche l'Autorità olandese per la protezione dei dati. Inizialmente, in una lettera indirizzata al Ministro delle Finanze olandese, l'Autorità ha ritenuto che la PSD2 fosse *lex specialis* rispetto al GDPR. In tal senso, si veda la lettera del Garante per la protezione dei dati personali indirizzata al Ministero delle Finanze del 20 dicembre 2017, disponibile al sito internet https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/20171220_advies_aan_min_fin_implementatiebesluit_psd2.pdf. Successivamente, la stessa Autorità si è orientata in senso opposto, ritenendo che la PSD2 non costituisca *lex specialis* rispetto al GDPR. Cfr. l'Autorità olandese per la protezione dei dati sull'interazione tra PSD2 e GDPR del 18 ottobre 2018, disponibile al sito internet https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-geeft-betaaldienstverleners-uitleg-over-uitdrukkelijke-toestemming-psd2#subtopic-6852.

[61] Regolamento Delegato (UE) 2018/289, cit. *supra* nota 28.

[62] Si veda Art. 36(1)(a) RTS, ai sensi del quale le banche devono fornire agli AIS "le stesse informazioni relative ai conti di pagamento designati e alle operazioni di pagamento associate rese disponibili all'utente dei servizi di pagamento in caso di richiesta diretta di accesso alle informazioni sui conti, *purché tali informazioni non comprendano dati sensibili relativi ai pagamenti*" (enfasi aggiunta).

6.3. Portabilità dei dati e conti "non di pagamento"

Nel contestualizzare le problematiche finora individuate con il diritto alla portabilità dei dati previsto dal GDPR, il titolare di un conto di pagamento dovrebbe avere il diritto di far trasmettere i propri dati a un altro titolare del trattamento. Un tale diritto è sancito dal GDPR purché il trattamento sia fondato sul 'consenso' dell'interessato oppure su un 'contratto'. In tale situazione, l'interessato potrebbe continuare a fruire dei servizi offertigli dalla banca anche in seguito ad un'operazione di portabilità dei dati, poiché tale circostanza non innesca l'obbligo giuridico di cancellazione dei dati da parte della banca stessa.[63] Ai sensi dell'Articolo 20, paragrafo 1 GDPR la portabilità dei dati è limitata ai dati che l'interessato ha fornito al titolare del trattamento. La portabilità dei dati include l'osservazione delle attività degli utenti, ma ne esclude l'analisi.

Anche in una siffatta situazione, pertanto, configurare o meno il rapporto tra la PSD2 e il GDPR come *lex specialis* rispetto a *lex generalis*, ovvero stabilire la natura dei dati del conto di pagamento come sensibili o non-sensibili, comporta importanti differenze dal punto di vista pratico. Interpretazioni in un senso o nell'altro, infatti, decreterebbero la linea di demarcazione tra l'applicabilità o meno dell'Articolo 20 GDPR.

Coerentemente con il punto di vista sopra espresso, unitamente all'impossibilità pratica di determinare la natura sensibile dei dati di conto a seconda delle circostanze, è opinione di chi scrive che tali dati non dovrebbero essere trattati ai sensi del diritto alla portabilità dei dati del GDPR.

Una simile deduzione potrebbe a prima vista sembrare di poca importanza, dal momento che una tale distinzione non comporterebbe conseguenze pratiche per il trattamento dei dati di conto. A rigore, infatti, per accedere ai dati i TPP non dovrebbero basarsi sull'Articolo 20 GDPR ma sugli Articoli 64-67 PSD2. Tuttavia, una tale distinzione potrebbe diventare rilevante per un trattamento supplementare di dati di conto non qualificabili come <di pagamento>. Come visto, infatti, la PSD2 non concede alcun diritto di accesso a questa tipologia di conti.[64] Facendo uso dell'Articolo 20 GDPR e del conseguente requisito del <consenso> o della <necessità contrattuale>, probabilmente una richiesta di accesso a conti non di pagamento potrebbe in linea di principio essere inquadrata come un diritto alla portabilità dei dati fintanto che il titolare del conto lo richiede formalmente. Questo punto di vista sembra avallato dal predecessore del EDPB, dove proprio nelle sue linee guida sulla portabilità dei dati include il seguente esempio:

Se la richiesta dell'interessato mira specificamente a fornire l'accesso alla cronologia del suo conto bancario a un fornitore di servizi di informazioni sul conto, per gli scopi indicati nella Direttiva sui Servizi

[63] Article 29 Working Party, Guidelines on the right to data portability (Adopted on 13 December 2016, last Revised and adopted on 5 April 2017).

[64] Si veda la Sezione 3 di questo lavoro, *supra*.

di Pagamento 2 (PSD2), tale accesso dovrebbe essere concesso in base alle disposizioni della presente direttiva.[65]

Tuttavia, come notato, il ragionamento sulla possibile natura sensibile dei dati di conto di pagamento può creare un ostacolo. Allo stesso tempo, si deve considerare che i conti di risparmio o altri conti non di pagamento non contengono dati di pagamento, facendo così luce sulla possibilità di consentire l'accesso ai TPP a questi conti, non ai sensi della PSD2, bensì ai sensi della portabilità dei dati del GDPR.

In ogni caso, l'esigenza di certezza del diritto sarebbe auspicabile anche in questa ulteriore circostanza di sovrapposizione tra le due normative in esame.

6.4. Dati di conto, big data e riutilizzo dei dati

Il trattamento dei dati di conto da parte dei TPP si complica con l'utilizzo aggiuntivo di big data per la fornitura dei propri servizi. Questo è particolarmente vero per gli AIS che fanno della profilazione il proprio modello di business.

In questo caso, l'interessato dovrà fornire il <consenso> per l'utilizzo di dati estratti da altre fonti, ad esempio i social media o altri dati riferibili alla navigazione di siti internet. Poiché ai sensi di legge il 'consenso' deve essere granulare[66], questo requisito pone la questione pratica di quanti livelli e forme di consenso i TPP devono richiedere per la fornitura dei servizi. In primo luogo, ci sarebbe il <consenso esplicito> di natura contrattuale degli Articoli 64-67 PSD2; quindi, il <consenso esplicito> (o nessun consenso, se si accetta il parere dell'EDPB) per il trattamento dei dati di conto; infine, il <consenso inequivocabile> per il trattamento e l'aggregazione di dati da altre fonti. Con ogni probabilità, l'attuazione pratica dei suddetti requisiti risulterebbe eccessivamente onerosa per i prestatori di servizi. Allo stesso tempo, la protezione dei consumatori non può essere sacrificata o ridotta.

Il problema è che, anche in caso di trattamento dei dati di conto non sensibili, la loro combinazione con i big data può rivelare aree sensibili della vita personale. Il confine tra il trattamento dei dati che rivela o meno informazioni sensibili diventa sfocato.

In linea di principio, inoltre, ai sensi del GDPR, i TPP potrebbero riutilizzare o riciclare i dati personali per altri servizi oltre a quello originale, purché gli interessati diano il loro consenso, sia esso espresso in modo inequivocabile o esplicito.

Tuttavia, l'Articolo 66, paragrafo 3, lettera g) PSD2 vieta categoricamente qualsiasi utilizzo ulteriore dei dati per fini diversi dalla prestazione del servizio di disposizione di ordine di pagamento. A sua volta, l'Articolo 67 paragrafo 2, lettera f) PSD2 prevede un divieto simile per gli AIS, ma aggiungendo che

[65] Article 29 Working Party, cit. *supra* nota 63, 8 (n 15).
[66] Ex Art. 7(2) GDPR.

questo dovrebbe avvenire <conformemente alle norme sulla protezione dei dati>. Il significato di queste parole aggiuntive per gli AIS non è chiaro. Interpretato alla lettera, sembrerebbe ammettere che, previo <consenso> dell'interessato, gli AIS (ma non i PIS) possano riutilizzare o riciclare i dati di conto per fornire altri servizi agli stessi titolari del conto.

Ancora una volta, la collisione tra la PSD2 e il GDPR comporta problemi di implementazione e applicazione pratica, nonché conseguenze per la protezione dei consumatori.

In assenza di una posizione ufficiale, pertanto, l'intero contesto imprenditoriale circostante rimane nell'ombra dell'incertezza giuridica.

6.5. Le c.d. terze parti silenti

I dati del conto di pagamento contengono inevitabilmente dati personali di altri soggetti terzi, ovvero i cosiddetti soggetti silenti i cui dati si trovano nel conto in oggetto in quanto beneficiari di un pagamento o cointestatari.

Da questa osservazione nasce il dubbio relativo al fatto se il trattamento dei dati di parti silenti sia legittimo o meno quando il <consenso esplicito> per il trattamento di tali dati venga prestato da un diverso soggetto (l'utente del servizio di pagamento o il titolare del conto), ovvero se altre basi giuridiche per il trattamento dei dati debbano essere prese in considerazione.

Questo elemento mette nuovamente alla prova la coerenza della PSD2 con il GDPR.

In questo caso, la difficoltà è duplice. Da un lato, vi è l'accesso concesso dalle banche ai TPP di dati delle parti silenti. La concessione dell'accesso ai dati personali da parte di un titolare del trattamento è essa stessa un'operazione di trattamento dei dati ai sensi dell'Articolo 4, paragrafo 2 GDPR.[67] Dall'altro lato, c'è il successivo trattamento di tali dati personali da parte dei TPP, che non si fonda né sul consenso in nessuna delle sue espressioni, né su un obbligo contrattuale con l'interessato silente.

Così, per individuare la base giuridica ci si domanda se sia ipotizzabile configurare il trattamento dei dati come necessario per adempiere a un obbligo giuridico del titolare del trattamento ai sensi dell'Articolo 6, paragrafo 1, lettera c) GDPR. In questo caso, l'obbligo giuridico ipotizzabile sarebbe quello prospettato dalla PSD2, ovvero l'obbligo contrattuale tra le parti del contratto.

La contro argomentazione confuterebbe una siffatta costruzione giuridica sulla base del fatto che un tale trattamento non viene effettuato per perseguire un obbligo di legge. La PSD2, infatti, non impone un

[67] Ai sensi dell'Articolo 4(2) GDPR, per <trattamento> si intende qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

obbligo giuridico al trattamento dei dati delle persone che non sono parti di un contratto. Al contrario, la PSD2 impone l'accesso ai dati del conto nell'ambito di un rapporto contrattuale nell'interesse delle parti del contratto. Dal punto di vista delle banche, esse sono obbligate per legge a concedere l'accesso ai dati dell'utente del servizio, che può essere considerato un obbligo legale ai sensi dell'Articolo 6 (1) (c) GDPR, ma solo nei confronti della parte contraente. Per le parti silenti, un tale obbligo giuridico non sussiste.

Allo stesso modo, è discutibile prospettare rapporti contrattuali alieni ad una persona che possano costituire un obbligo giuridico fungibile da base per il trattamento dei dati di terzi. Se così fosse, la legge sulla protezione dei dati sarebbe generalmente frustrata, consentendo un trattamento indiscriminato di dati di un numero indeterminato di interessati, solo per soddisfare gli interessi privati di contratti estranei agli interessati stessi.

Per contro, l'interesse legittimo perseguito dal responsabile del trattamento o da una terza parte ai sensi dell'Articolo 6, paragrafo 1, lettera f) GDPR potrebbe coprire in modo più appropriato la situazione in questione e fornire la base giuridica per il trattamento. Almeno, questa è l'opinione espressa dall'EDPB nella citata lettera indirizzata a un membro del Parlamento europeo, in cui afferma che una base giuridica per il trattamento di dati di parti silenti, da parte dei PIP e degli AIS ai sensi della PSD2, potrebbe essere rappresentato dal legittimo interesse di un titolare del trattamento o di una terza parte ex Articolo 6 (1) (f) per l'esecuzione del contratto con l'utente del servizio.[68]

Se il consenso rappresenta una delle basi giuridiche più complicate da attuare ai sensi della legge sulla protezione dei dati, l'interesse legittimo è probabilmente quella più controversa e di difficile applicazione.[69] Si afferma che i titolari del trattamento, che determinano le finalità e i mezzi del trattamento dei dati personali, possono farlo lecitamente, senza soddisfare le altre strette condizioni di legge, se ciò è necessario per le finalità del loro legittimo interesse o di quello di terzi, a meno che tali interessi siano superati dagli interessi per i diritti e le libertà fondamentali degli interessati. Trattasi di un criterio che amplia l'ambito del trattamento consentito sulla base delle altre basi giuridiche, in particolare il trattamento fondato sul consenso. La disposizione è formulata in modo sufficientemente ampio anche per comprendere situazioni di conflitto di legittimi interessi privati nei confronti di titolari del trattamento o di terzi rispetto ai diritti degli interessati, conflitti che richiedono l'esercizio di un bilanciamento. Questo test fornisce flessibilità al sistema, consentendo la legittimità del trattamento con una determinazione caso per caso. Tuttavia, se da un lato la flessibilità è accolta favorevolmente dai titolari di trattamento, dall'altro lato essa ha il difetto di compromettere la certezza del diritto. Il test di bilanciamento richiede

[68] European Data Protection Board, cit. supra nota 46.
[69] Ferretti F, "Data protection and the legitimate interest of data controllers: Much ado about nothing or the winter of rights?", 51 *Common Market Law Review* (2014), 843-868.

l'interpretazione da parte di soggetti legalmente non qualificati che hanno lo scopo di applicare i risultati beneficiandone. I titolari del trattamento hanno la facoltà di determinare se essi stessi hanno un interesse legittimo che giustifichi il trattamento e se il loro interesse abbia la precedenza sui diritti e le libertà degli interessati. Non è esente da controversia il fatto che le persone, che effettuano il bilanciamento e che determinano quali interessi o diritti prevalgono per il trattamento dei dati, siano anche gli stessi titolari del trattamento, passibili di controlli giudiziari, per giunta di difficile applicazione pratica, solo *ex post*.[70]

Tenendo conto della specificazione di cui sopra, ciò significa, nel caso in esame, che le banche e i TTP non possono applicare automaticamente l'interesse legittimo come base per il trattamento ma devono effettuare un test di bilanciamento, dovendo prendere in considerazione tra l'altro il tipo e la natura dei dati raccolti, il contesto, le circostanze e i rischi per gli individui.

Tuttavia, il legittimo interesse del titolare del trattamento deve essere limitato e determinato dalle ragionevoli aspettative degli interessati,[71] in questo caso le parti silenti. Così, in contrapposizione al parere dell'EDPB, appare dubbio in quale misura siano soddisfatte le ragionevoli aspettative delle parti silenti. Questo requisito potrebbe al limite essere soddisfatto nel caso della fornitura di PIS, ma appare senz'altro discutibile per la fornitura di AIS.

Resta comunque incontestabile che, ai sensi degli Artt.13 e 14 GDPR, i titolari del trattamento debbano darne comunicazione agli interessati del trattamento e debbano trovare una modalità tecnica adeguata anche per i soggetti silenti.

Come notato nelle sezioni precedenti, tuttavia, il problema è che i dati di conto possono facilmente contenere informazioni sensibili. Altresì, il trattamento di big data può facilmente rivelare informazioni di tale natura. *Mutatis mutandis*, questa circostanza vale anche per le parti silenti. L'ostacolo è che, ai sensi dell'Articolo 9, paragrafo 1 GDPR, l'interesse legittimo non può essere utilizzato come base giuridica per il trattamento dei dati sensibili. Pertanto, posta l'impraticabilità da parte delle banche di implementare misure tecniche idonee a separare i dati del conto che potrebbero rivelare informazioni che rientrano nell'Articolo 9, paragrafo 1 GDPR da altri dati del conto medesimo, è discutibile la misura in cui i dati delle terze parti silenti possano essere trattati sulla base giuridica dell'interesse legittimo ai sensi del GDPR.

Il problema di fondo è che un tale diniego potrebbe mettere a repentaglio l'operatività dell'Open Banking e frustrare le norme della PSD2. Per contro, chiudere gli occhi sul problema comporterebbe un inaccettabile indebolimento delle tutele offerte agli interessati dal GDPR. Ci si troverebbe inoltre di fronte ad una lettura della normativa priva di senso.

[70] Ibid.
[71] Considerando 47 GDPR.

Inutile insistere che, anche in questa circostanza, si verifica una collisione tra la PSD2 e il GDPR a scapito della necessaria coerenza e certezza del diritto.

7. Conclusioni: la necessità di certezza giuridica e adeguata tutela dei diritti

Tirando le somme al numero di questioni giuridiche risultanti dalla complessità del rapporto tra la PSD2 e il GDPR, quanto emerge è un intricato nodo gordiano.

Questo scritto ha esaminato l'Open Banking, vale a dire il nuovo modello di mercato nell'area dei pagamenti reso possibile dalla PSD2, in cui l'attività bancaria tradizionale si incontra e viene trasformata dalla *data economy* e dalla nuova concorrenza di imprese Fintech. Con la PSD2, l'UE ha cambiato il suo approccio nei confronti del mercato unico, prediligendo la digitalizzazione e la concorrenza. Allo stesso tempo, digitalizzazione e concorrenza sono sinonimo di crescente trattamento di dati personali da parte di un numero crescente di nuovi operatori di mercato. Inevitabilmente, quindi, l'Open Banking non solo è regolato dalla PSD2, ma rientra anche nell'ambito di applicazione del GDPR.

Tuttavia, l'interazione di queste due normative crea una serie di difficoltà giuridiche e domande sulla loro relazione e compatibilità.

In questa sede, sono state identificate una serie di problematiche di coordinamento, a partire dai diversi significati giuridici di "consenso", utilizzati rispettivamente sia dalla PSD2 sia dal GDPR, nonché l'ambiguità circa il loro grado di applicabilità per il trattamento dei dati di conto. A sua volta, lo scarso coordinamento delle due leggi rende incerta l'applicazione della base giuridica o legittimazione appropriata per l'accesso e il trattamento dei dati di conto. Allo stesso modo, la portata e la misura in cui il diritto alla portabilità dei dati concesso dal GDPR trova efficacia sono dubbie. Di conseguenza, non è chiaro come i fornitori di servizi debbano condurre la propria attività e i titolari dei conti siano salvaguardati, ovvero se il legittimo accesso e il trattamento dei dati avvengano sulla base di un obbligo contrattuale, un consenso semplice ma non ambiguo, o un consenso esplicito.

La natura sensibile delle informazioni contenute nei conti di pagamento e l'impossibilità di tenerle separate dagli altri dati di pagamento rappresentano una particolare fonte di preoccupazione, soprattutto se non trovano applicazione i più elevati standard di protezione propri del GDPR. Anche la possibile aggregazione dei big data e la portata del possibile riutilizzo dei dati rimangono questioni oscure, soprattutto nel dominio digitale dove le Fintech hanno il potenziale di estrarre valore per la fornitura di nuovi servizi competitivi.

Ultimo ma non meno importante, il trattamento dei dati di conto implica il necessario accesso a dati di terze parti silenti. Tuttavia, la legittimità di tale trattamento è controversa.

Tutte le questioni giuridiche identificate culminano in tentativi insoddisfacenti di ricostruzioni, forzature o interpretazioni giuridiche.

L'impressione è che nel rapporto tra la PSD2 e il GDPR ci siano troppi nodi giuridici, creando in tal modo una matassa così aggrovigliata da non poter essere sciolta trattando i nodi uno a uno.

È pertanto auspicabile un taglio netto con l'urgente interpretazione autentica della CGUE o una revisione da parte del legislatore competente. In mancanza di ciò, l'operatività dell'Open Banking in un quadro giuridico certo e rispettoso dei diritti sarebbe compromessa.

A parere di chi scrive, un primo passo importante verso una risoluzione ordinata della questione sarebbe costituito dall'inclusione dei dati finanziari nella categoria dei dati sensibili del GDPR. Tuttavia, ciò non sarebbe risolutivo per facilitare il coordinamento della PSD2 e del GDPR, ma sarebbe necessaria ulteriore certezza del diritto.

Innanzitutto, data l'attuale struttura del mercato dell'UE, permane il rischio che i diversi Stati Membri continuino a fornire risposte diverse ai problemi, così come hanno fatto in sede di recepimento della PSD2.[72]

Non meno importante, gli operatori finanziari e i consumatori necessitano di certezza giuridica e di un ambiente dell'Open Banking che consenta un'adeguata protezione dei consumatori per prevenire il fenomeno del free-riding del mercato. Nello sviluppo di un nuovo mercato, è sia nell'interesse generale che in quello particolare delle parti gestire modelli innovativi che funzionino per l'economia reale e la società.

Presi singolarmente, si potrebbe affermare che il quadro giuridico della PSD2 e quello del GDPR non siano perfetti. Tuttavia, le incertezze giuridiche derivanti dallo scarso coordinamento delle due normative possono comportare rischi che vanno al di là dei tecnicismi giuridici.

In un mercato dei servizi finanziari, che è principalmente guidato e governato dall'offerta, vi sono non pochi rischi legati alla condotta degli operatori. Modelli di business aggressivi possono facilmente espandersi tramite lo sviluppo digitale. L'innovazione e la concorrenza sono certamente benvenute, ma le complessità dei modelli di business del Fintech assumono nuove forme non convenzionali in cui i dati personali alimentano nuovi scenari e creano nuovi mercati. Ciò può portare a un ambiente favorevole al marketing individuale mirato, allo sfruttamento dei pregiudizi comportamentali dei consumatori, alla vendita di servizi finanziari inadeguati o alla discriminazione finanziaria. Il free-riding trova il proprio ambiente ideale nell'incertezza giuridica e potrebbe facilmente prosperare.

[72] Ad esempio, si vedano le legislazioni nazionali di Francia, Germania, Danimarca e Svezia che nella trasposizione dell'Articolo 67(2)(f) non includono la dicitura "conformemente alle norme sulla protezione dei dati" A tal proposito, si veda European Commission, National transpositions by Member States, Document 32015L2366, disponibile al sito web https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32015L2366.

La tempestiva comprensione da parte del legislatore dei diversi modelli di business è fondamentale per riconoscere lo sviluppo del mercato e le inadeguatezze dell'attuale quadro giuridico. Pertanto, sarebbe necessario ripensare a un regime dell'Open Banking libero da incertezze per conciliare le esigenze di un nuovo mercato, dove gli operatori operano in un quadro chiaro e gli utenti sono adeguatamente tutelati.