**Elisabetta Bani e Eugenia Macchiavello** *

# Il diritto alla portabilità dei dati nell'ambito della nuova economia dei dati

SOMMARIO: 1. Introduzione. Il nuovo "diritto alla portabilità dei dati personali": *ratio* ed implicazioni generali. – 2. Una breve analisi del diritto alla portabilità dei dati (art. 20 *GDPR*). – 2.1. Aspetti principali: formato dei dati, tipologie di trasferimento e soggetti. – 2.2. Dati oggetto del diritto. – 2.3. Limitazioni del diritto alla portabilità. – 3. *PSD* 2 e *open banking*. – 3.1. *Open banking*: caratteristiche principali e *ratio*. – 3.2. Gli obblighi dei soggetti coinvolti ed il difficile rapporto tra *PSD2* e *GDPR*. – 4. Libero flusso di dati e altre forme di portabilità: dati non personali e dati pubblici. – 5. Aspetti problematici di tale architettura e conclusioni.

## 1. Introduzione. Il nuovo "diritto alla portabilità dei dati personali": *ratio* ed implicazioni generali

Il «diritto alla portabilità dei dati personali» è stato introdotto dall'art. 20 del Regolamento generale sulla protezione dei dati [1] ed è non solo una delle novità più significative introdotte dal *GPDR*, ma anche un'epifania del modello europeo di regolazione dell'economia digitale. Già nella Comunicazione sull'economia dei dati del 2014, la Commissione ha iniziato a sottolineare l'importanza della portabilità dei dati per la costruzione di un mercato interno dei dati [2] ma è negli ultimi anni che la Commissione ha

* Eugenia Macchiavello è Ricercatrice in diritto commerciale e titolare del corso di diritto bancario presso l'Università degli studi di Genova. Elisabetta Bani è Professore Ordinario di diritto dell'economia. I capitoli del presente contributo sono da attribuirsi agli autori come segue: Elisabetta Bani: 1 e 5.2; Eugenia Macchiavello: 2, 3, 4, 5.1 e 5.3.

[1] Regolamento 2016/679 del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

[2] COMMISSIONE EUROPEA, *Verso una florida economia basata sui dati*, (2 luglio 2014), COM(2014) 442 final, p. 13; COMMISSION, *A Digital Single Market Strategy for Europe* (Communication) COM(2015) 192 final 6. Cfr. anche, S. COLLINS *et al.*, *Turning fair into reality* –

meglio definito e tradotto in iniziative strettamente interconnesse e complementari la strategia europea dei dati e la libera circolazione dei dati come quinta libertà europea [3].

L'idea di fondo è semplice: si vuole consentire a ciascun individuo che utilizzi servizi *on-line* di «portare» i propri dati personali da un servizio/-fornitore all'altro, in modo da poterli riutilizzare in piena autonomia senza perdere il patrimonio di informazioni creato in precedenza. Il precedente logico e storico, in ambito europeo, è dato dalla portabilità del numero telefonico da un operatore all'altro [4] e la portabilità dei mutui [5].

In tutti tali casi, una delle ragioni alla base del diritto di portabilità è favorire la concorrenza tra operatori anche a beneficio degli utenti [6], con effetti regolativi sui mercati digitali [7].

---

*Final Report of the European Commission Expert Group on FAIR Data*, EU, Brussels, 2018, https://ec.europa.eu/info/sites/info/files/turning_fair_into_reality_1.pdf (a favore di un sistema di dati *findable*, *accessible*, *interoperable*, *reusable* - *FAIR*).

[3] COMMISSION, *A European strategy for data* (Communication) COM(2020) 66 final.

[4] Cfr. art. 30 e consideranda 40-42 della direttiva 2002/22/EC (*Universal Service and users' rights relating to electronic communications networks and services Directive*). Cfr. anche considerando 31 della direttiva 2002/21/EC (*Framework for electronic communication networks and services Directive*). Sulle origini del diritto di portabilità, cfr. EUROPEAN DATA PROTECTION SUPERVISOR, *Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy – Preliminary Opinion* (March 2014), p. 15; I. GRAEF, *Mandating Portability and Interoperability in Online Social Networks: Regulatory and Competition Law Issues in the European Union*, in *Telecommunications Policy* 2015, 39, 6, 502.

[5] Cfr. S. TROIANO, *Il diritto alla portabilità dei dati*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, p. 195 ss., pp. 196, 203; E. BATTELLI, G. D'IPPOLITO, *Il diritto alla portabilità dei dati personali*, in E. TOSI (a cura di), *Riservatezza e protezione dei dati tra GDPR e nuovo Codice Privacy*, Giuffrè, Milano, p. 185, in particolare, pp. 187 ss. e 193 ss.; R.H. WEBER, *Data portability and big data analytics. New competition policy challenges*, in *Concorrenza e mercato*, 2016, p. 59; I. GRAEF, J. VERSCHAKELEN, P. VALCKE, *Putting the right to data portability into a competition law perspective*, in *Law: The Journal of the Higher School of Economics*, in *Annual Review*, 2013, p. 53.

[6] In comune tra i casi citati vi è purtroppo anche l'illusione che la mobilità tra operatori non presenti differenze tra i mercati, così come ci si è illusi per anni che la divisione tra rete e servizio potesse assicurare la concorrenza allo stesso modo sia nel settore dell'energia elettrica, che delle reti telefoniche e dei treni, salvo poi constatare che mentre gli elettroni sono fungibili e facilmente scambiabili e le infrastrutture telefoniche – a un costo – scalabili, le reti ferroviarie e i treni sono oggetti ingombranti e infungibili.

[7] Sul ruolo della disciplina sulla protezione dei dati in ottica di norme di comportamento e normativa antitrust: G. COLANGELO, M. MAGGIOLINO, *Data Protection in Attention Markets: Protecting Privacy Through Competition?*, in *Journal of European Competition Law & Practice* 2017, 1; M. BORGHI, *Portabilità dei dati e regolazione dei mercati digitali*, in *Mercato conc. reg.* 2018, 2, p. 223, in particolare p. 224; J. DREXL, *Designing Competitive Markets for Industrial Data – Between Propertisation and Access*, in *JIPITEC* 2017, 8, p. 257, in particolare p. 286.

La mobilità ed interoperabilità dei dati abbassa infatti i *transaction cost*, in particolare quelli di passaggio da un fornitore di servizio all'altro (*switching*) [8], visti sia in termini monetari che di adempimenti e "seccature", e di conseguenza i fenomeni di *lock-in* (in cui cioè il cliente rimanga "intrappolato" nonostante la presenza altrove sul mercato di opportunità migliori) [9], così rafforzando la facoltà di scegliere tra servizi concorrenti o, più esattamente, tra fornitori che forniscono almeno un servizio percepito come succedaneo a ciò che il cliente usa già (ad esempio, carta di credito e ApplePay). Tale diritto rende quindi più difficile per gli operatori del mercato digitale "bloccare" gli utenti all'interno del proprio servizio, dal momento che questi ultimi possono chiedere di riutilizzare i propri dati con altro operatore e usufruire di servizi analoghi o comunque per cui servano i medesimi dati forniti da tale altro operatore e percepiti come migliori o comunque interessanti.

Si rende inoltre teoricamente possibile il *multi-housing*, ovvero l'impiego simultaneo dei propri dati su piattaforme che forniscono servizi diversi (o diverse piattaforme che forniscono lo stesso servizio: ad esempio, ApplePay e GooglePay), così offrendo ai *new entrant* la possibilità di offrire un servizio innovativo e competere almeno in quella nicchia, invece che dover competere (invano) con gli *incumbents* in tutti i segmenti di mercato e quindi per tutti i servizi degli stessi [10]. Allo stesso tempo, i consumatori dovrebbero anche essere più propensi a fornire i loro dati (sapendo di poterli poi trasferire altrove e comunque di poterli proteggere) e quindi a contribuire al miglioramento e maggior personalizzazione dei servizi [11].

L'art. 20 si presenta perciò come un rimedio concorrenziale *a priori*, impedendo a monte l'insorgere di situazioni di *lock-in* e riducendo le barriere all'entrata, non richiedendo investimenti spropositati al *challenger*.

Tuttavia, il diritto alla portabilità dei dati, anche in considerazione della collocazione sistematica (*GDPR*), è prima di tutto un diritto personale dell'individuo teso a realizzare l'identità in senso digitale dell'individuo [12] e segna in tal senso la strada europea nel settore.

---

[8] EUROPEAN COMMISSION, *Building A European Data Economy*, cit. Cfr. anche W. KERBER, H. SCHWEITZER, *Interoperability in the digital economy*, Joint Discussion Paper Series in Economics, *MAGKS*, 2017, 12, 20; L. SOMAINI, *The right to data portability and user control: ambitions and limitations*, in *Riv. dir. media*, 2018, 3, 164, in particolare p. 173.

[9] TROIANO, *Il diritto alla portabilità dei dati*, cit., p. 203.

[10] Cfr. J. CRÉMER, Y.-A. DE MONTJOYE, H. SCHWEITZER, *Competition Policy for the Digital Area*, (EU, Luxembourg, 2019), p. 37.

[11] EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 8/2016 on coherent enforcement of fundamental rights in the age of big data*, (23 September 2016), p. 14.

[12] G. ZANFIR, *The right to Data portability in the context of the EU data protection reform*, in

In materia di dati, infatti, Stati Uniti e Cina hanno puntato su cospicui investimenti e sulla *deregulation*, prestando tuttavia scarsa attenzione finora in merito a questioni di *privacy*, di tutela dei dati personali ed etiche, impostando la tutela dei dati personali in temi di diritti di proprietà e non di tutela della personalità [13]. L'Unione europea, invece, ha deciso di seguire una strada distinta ed originale, pur partendo con ritardo e senza il supporto di giganti tecnologici comparabili a quelli delle due superpotenze commerciali, puntando a massimizzare i benefici dei dati e dell'intelligenza artificiale (di seguito, IA, che rappresenta il principale strumento di impiego e applicazione dei dati) e ridurre al minimo i rischi, sempre ponendo al centro l'uomo e l'etica [14]. Letti in questa chiave, lo sviluppo e l'utilizzo dell'IA e dei dati non sono da considerarsi come obiettivi di per sé, ma come mezzi che possono migliorare la vita dei cittadini e aumentare il benessere sociale e ciò sarà possibile solo se gli esseri umani potranno fidarsi di questa tecnologia e si potrà assicurare affidabilità e sicurezza della stessa [15]. Più in particolare, attraverso la strategia europea dei dati (che si coordina con quella in materia di IA) [16], l'UE si propone di far beneficiare i cittadini europei dei benefici scaturenti dai dati, e non solo in termini di produttività (incrementando la domanda e consumo di beni e servizi basati sui dati) e concorrenza ma anche "*improvements in health and well-being, environment, transparent governance and convenient public services*", inclusi servizi più personalizzati ed efficienti [17].

In questa prospettiva, l'accesso e la condivisione dei dati rivestono un ruolo centrale nel potenziale di crescita dell'economia dei dati europea ed è essenziale per mantenere la competitività sul mercato, per incrementare

---

*International Data Privacy Law*, 2(3), 2012, 3; O. LYNSKEY, *Aligning Data Protection Rights with Competition Law Remedies? The GDPR Right to Data Portability*, in *European Law Review* 2017, 42, 793; SOMAINI, *op. cit.*, p. 171; L. SCUDIERO, *Bringing Your Data Everywhere: A Legal Reading of the Right to Portability*, in *ECPL* 2017, 3(1), 119.

[13] G. ALPA, *La proprietà dei dati personali*, in N. ZORZI GALGANO (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Cedam, Padova, 2019, p. 25 ss.; A. PRETA, L. ZOBOLI, *Intelligenza artificiale ed economia dei dati. Profili regolatori e concorrenziali in tema di accesso e condivisione dei dati*, in *AGE* 2019, 1, p. 213; M. GIORGIANNI, *Il «nuovo» diritto alla portabilità dei dati personali. Profili di diritto comparato*, in *Contr. e impr.*, 2019, 4, p. 1387. A. BEATTIE, *Technology: how the US, EU and China compete to set industry standards*, in *Financial Times* (23 July 2019).

[14] Cfr. Commissione, *Libro bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia*, COM(2020) 65 final.

[15] PRETA, ZOBOLI, *op. cit.*, pp. 215-216.

[16] Cfr. COMMISSION, *Libro Bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia*, (19 febbraio 2020) COM(2020) 65 final.

[17] COMMISSION, *A European Strategy for Data*, cit., pp. 1-2.

le opportunità di innovazione delle imprese e, in particolare, per sviluppare le applicazioni di IA. La Commissione si propone di ribilanciare l'equilibrio del mercato dei dati (attualmente dominato in particolare dai grandi *players* Statunitensi), riconoscendo un nuovo ruolo all'Europea e a tal fine auspica di incrementare i dati disponibili per il riuso benefico degli stessi e quindi, attraverso una varietà di azioni ed iniziative proposte, favorire il libero movimento di qualunque tipo di dati. In tale contesto si collocano altre forme di portabilità, quali ad esempio la portabilità nei servizi di pagamento, il riuso dei dati, anche non personali, in possesso delle autorità pubbliche o ottenuti attraverso risorse pubbliche, il trasferimento di dati da imprese ad autorità (*business-to-government*) e tra imprese (*business-to-business* specialmente in caso di collaborazione nel generare i dati) (cfr. §§ 3 e 4) [18].

Tuttavia, la tutela dell'individuo non deve essere messa da parte e, attraverso le disposizioni del *GDPR*, si intende bilanciare due esigenze potenzialmente in conflitto: favorire la libera circolazione dei dati personali e assicurare contestualmente la protezione di tali dati. È da sottolineare l'aspetto che il principale obiettivo del nuovo diritto consiste nel rafforzare il controllo sui propri dati personali quando siano detenuti da altri (*considerandа* 7 e 68 *GDPR*) [19], e ciò in base al principio – largamente accettato nella dottrina europea – che la protezione dei dati personali serve interessi che eccedono la tutela della *privacy* e si estendono all'"autodeterminazione informativa" [20]. Con il *GDPR* si è passati infatti da un concetto di diritto fondamentale dell'individuo limitato a custodire gelosamente i propri dati personali in un cassetto, ad essere lasciato solo escludendo gli altri dalla propria "fortezza" (diritto alla riservatezza, diritto alla protezione dei dati in senso "negativo"), al diritto di seguire e controllare proattivamente i dati che lo stesso ha fornito per limitare le interferenze e correggerne o cancellare eventuali errori (diritto alla protezione dei dati in senso "positivo") [21],

---

[18] COMMISSION, *A European strategy for data*, cit., pp. 13-14.

[19] Cfr. anche EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 7/2015 Meeting the Challenges of Big Data: A Call for Transparency, User Control, Data Protection by Design and Accountability* (19 November 2015), p. 13.

[20] ZANFIR, *op. cit.*; E. FIALOVA, *Data Portability and Informational Self-Determination*, in *Masaryk University Journal of Law and Technology*, 2014, 8(1), pp. 47-48; G. FINOCCHIARO (diretto da), *Il nuovo Regolamento europeo sulla* privacy e sulla protezione dei dati personali, collana *Le riforme del diritto italiano*, Zanichelli, Bologna, 2017, p. 6; SOMAINI, *op. cit.*, pp. 171-172.

[21] S. RODOTÀ, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Laterza, Roma-Bari, 2014, pp. 28-29; G. DE MINICO, *Big Data e la debole resistenza delle categorie giuridiche. Privacy e lex mercatoria*, in *Dir. pubbl.*, 2019, 1, 89, p. 91; M. GIORGIANNI, *Il «nuovo» diritto alla portabilità dei dati personali. Profili di diritto comparato*, in *Contr. e impr.*, 2019, 4, p. 1387.

comprensivo del diritto di deviare il flusso di tali dati per indirizzarlo dove più conveniente per l'individuo stesso [22].

La norma reagisce quindi ad un contesto di diffuso sfruttamento commerciale dei dati personali forniti in cambio di servizi fittiziamente gratuiti, puntando su un rafforzamento dei diritti dell'individuo, inteso anche come rappresentazione sociale della persona in rete, formata da dati sparsi in diverse banche dati e i diversi profili costruiti sulla base di questi [23]. È all'individuo che appartengono i dati che le/gli si riferiscono e che può decidere autonomamente l'uso da farsi, anche qualora tali dati siano raccolti e in possesso di terzi [24]. Si tenta perciò di riportare al centro del mondo digitale l'individuo, invece dei dati stessi o dei suoi sfruttatori [25], e di porre in posizione di preminenza i suoi diritti fondamentali sugli eventuali interessi economici dei terzi, permettendogli di beneficiare dei servizi aggiuntivi dei terzi e condividere anche il valore aggiunto e ricchezza dei grandi *players* del settore [26], potenzialmente anche riducendo il rischio di uso dei dati discriminatorio o incorretto [27]. È quindi un diritto personale ma dai rilevanti

[22] Il diritto alla protezione dei dati è riconosciuto come diritto fondamentale dall'art. 8, par. 1, della Carta dei diritti fondamentali dell'Unione europea (che fa espresso riferimento al solo diritto di accesso) e dall'art. 16, par. 1, del Trattato sul funzionamento dell'Unione europea ed il diritto alla portabilità dei dati è un'esplicazione del diritto alla protezione dei dati in senso dinamico, come diritto a controllare il trattamento e circolazione dei propri dati. Cfr. GIORGIANNI, *op. cit.*; L. BIANCHI, *Il diritto alla portabilità dei dati*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. n. 196/2003 (Codice Privacy)*, *Scritti in memoria di Stefano Rodotà*, Giuffrè, Milano, 2019, 223, p. 224 ss.; E. PELINO, *I diritti dell'interessato*, in E. BOLOGNINI, L. PELINO, C. BISTOLFI (a cura di), *Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Giuffrè, Milano, 2016, p. 250; TROIANO, *Il diritto alla portabilità*, cit., p. 201; SOMAINI, *op. cit.*, p. 8; M. RABITTI, A. SCIARRONE ALIBRANDI, *Dalla PSD alla PSD2: open banking e servizi di pagamento*, in A. BAGLIONI (a cura di), *Le attuali sfide del sistema bancario. Congiuntura e tecnologia – Osservatorio Monetario* 1/2019, (marzo 2019), 47, p. 55: «*Il GDPR tutela il diritto alla protezione dei dati personali come diritto fondamentale – il cui principio cardine è l'autodeterminazione informativa, ossia il diritto del singolo a decidere in prima persona sulla cessione e l'uso dei dati che lo riguardano – e ragiona nell'ottica del bilanciamento tra circolazione e protezione del dato personale a garanzia della dignità degli individui (basandosi sulla nota triade* consent/ownership/portability*)*».

[23] S. RODOTÀ, *Il mondo nella rete*, cit., p. 30; ID., *Il diritto di avere diritti*, Laterza, Roma-Bari, 2012, pp. 396-397.

[24] BORGHI, *op. cit.*, p. 224.

[25] SOMAINI, *op. cit.*, p. 171.

[26] Article 29 Working Party (WP29), *Opinion 3/2013 on purpose limitation*, (2 April 2013), WP203, 47. Cfr. anche P. DE HERT *et al.*, *Reinventing Data Protection*, Springer, Dordrecht/Heidelberg/London/New York, 2009, p. 11.

[27] WP29, *Opinion 3/2013 on purpose limitation*, cit., pp. 46-47; P. DE HERT *et al.*, *Reinvent-*

risvolti economici e si pone all'intersezione di molti segmenti del diritto (della personalità, della concorrenza, industriale, protezione del consumatore, ecc.), assumendo dunque contorni polifunzionali [28] e talvolta portando i commentatori a temere una "mercificazione" dei dati personali [29].

Data l'ampiezza della sua portata, il *GDPR* è destinato ad avere, nei prossimi anni, un impatto significativo in tutti i settori in cui ha luogo un trattamento di dati personali.

Il presente contributo intende analizzare il diritto alla portabilità dei dati di cui all'art. 20 *GDPR*, nel contesto della più ampia strategia europea dell'economia dei dati, e individuarne alcuni aspetti problematici.

## 2. Una breve analisi del diritto alla portabilità dei dati (art. 20 *GDPR*)

### 2.1. Aspetti principali: formato dei dati, tipologie di trasferimento e soggetti

Il diritto alla portabilità dei dati personali permette all'utente di ottenere una copia dei propri dati personali e conservarli (su supporto personale o *cloud*) per un uso personale futuro (art. 20, par. 1, prima parte *GDPR*), come forma complementare al diritto di accesso [30]. Tuttavia, il diritto alla portabilità dei dati presenta anche nuovi profili, potendo pure consistere nel diritto di trasmettere i dati ricevuti a terzi (art. 20, par. 1, seconda parte) [31] e obbligando il titolare del trattamento di dotarsi di certe infrastruttu-

*ing*, cit., 2; DE HERT *et al.*, *The Right to Data Portability in the GDPR: Towards User-centric Interoperability of Digital Services*, in *Computer Law & Security Review* 2018, 193; SOMAINI, *op. cit.*, p. 174.

[28] DE HERT *et al.*, *The Right to Data Portability*, cit., p. 195; TROIANO, *Il diritto alla portabilità dei dati*, cit., p. 202.

[29] TROIANO, *Il diritto alla portabilità dei dati*, cit., p. 216; F. PIRAINO, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *NLCC* 2017, 2, 369, pp. 382, 399.

[30] WP29, *Guidelines on the right to data portability*, (revised 5 April 2017), pp. 3-5, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233. Cfr. anche P. HUSTINX, *EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection regulation* (EDPS, 15 September 2014), https://edps.europa.eu/sites/edp/files/publication/14-09-15_article_eui_en.pdf.

[31] Il diritto alla portabilità dei dati si distingue dal diritto di accesso per la possibilità di ottenere copia su un supporto personale e con certe caratteristiche (ad esempio, strutturato) e di trasferire a terzi tali dati, anche richiedendo il trasferimento diretto tra titolari del trattamento. Cfr. TROIANO, *Il diritto alla portabilità*, cit., p. 198.

re tecniche per soddisfare le specifiche di formato (cfr. subito *infra*)[32]. In particolare, assumeranno un ruolo centrale le *Application Programming Interface* (API), cioè software che permettono la comunicazione tra due applicazioni.

Anche per motivi connessi a tale "ampiezza", il diritto alla portabilità è più circoscritto rispetto al diritto di accesso per quanto riguarda la tipologia di dati (ad esempio, solo quelli forniti dal cliente e trattati sulla base del consenso o per l'esecuzione di un contratto: cfr. § 2.2.) Non si tratta però di un vero e proprio trasferimento, per cui, qualora la finalità non sia stata ancora raggiunta e il trattamento presso il primo titolare sia ancora legittima, la trasmissione non comporta di per sé la cancellazione dei dati presso il primo titolare[33], benché questa possa comunque essere richiesta dall'interessato ai sensi dell'art. 17 *GDPR*, esercitando separatamente ma contestualmente il suo diritto all'oblio (cfr. § 2.3)[34]. Tale profilo appare in linea con l'obiettivo di favorire la condivisione – più che il trasferimento esclusivo – dei dati, al fine di offrire servizi migliori ed interconnessi a beneficio dell'utente, incluso attraverso piattaforme multicanale (v. *supra*, § 1)[35] e sembra escludere la natura "proprietaria" del diritto in questione[36].

La normativa precisa che i dati di cui si chiede il trasferimento debbano essere forniti dal titolare del trattamento "in un formato strutturato, di uso comune e leggibile da dispositivo automatico" ("*machine readable*", cioè con limitato intervento umano), senza ulteriori indicazioni tecniche a causa della varietà di formati impiegati nei diversi settori (il *GDPR* resta un regolamento "generale", applicabile "*across sectors*")[37]. Il consideran-

---

[32] Sulle differenze tra diritto di accesso e diritto alla portabilità, cfr.: W. LI, *A tale of two rights: exploring the potential conflict between right to data portability and right to be forgotten under the General Data Protection Regulation*, in *International Data Privacy Law*, 2018, 8, 4, 309, p. 315; R. STOYKOVAR, *The Right to Data Portability. Data protection scope and technical feasibility*, in *Computer Law Review International*, 2018, 3, 65, pp. 66-67.

[33] Sotto tale aspetto, il diritto alla portabilità dei dati si distingue dal diritto alla portabilità del numero telefonico: cfr. S. ELFERING, *Unlocking the Right to Data Portability An Analysis of the Interface with the Sui Generis Database Right*, Nomos, Monaco, 2019, p. 20.

[34] G. MALGIERI, *Il diritto alla portabilità dei dati personali*, in G. COMANDÉ, G. MALGIERI (a cura di), *Manuale per il trattamento dei dati personali*, Gruppo24ore, Milano, 2018, p. 56; GIORGIANNI, *op. cit*.

[35] DE HERT *et al*., *The right*, cit., p. 203.

[36] I. GRAEF, M. HUSOVEC, N. PURTOVA, *Data Portability and Data Control: Lessons for an Emerging Concept in EU Law*, in *German Law Journal* 2018, 19, 1359.

[37] Il considerando 21 della direttiva 2013/37/EU sull'informazione nel settore pubblico definisce il termine "*machine readable*" come "*a file format that is structured in such a way that software applications can easily identify, recognise and extract specific data from it*". Il WP29

do 68 incoraggia i titolari dei trattamenti a sviluppare formati interoperabili (e quindi in grado di comunicare e trasferire correttamente i dati tra loro) in modo da assicurare l'utilizzabilità dei dati trasferiti, senza che ciò si traduca in un obbligo di adottare sistemi compatibili (cioè che funzionino allo stesso tempo insieme condividendo lo stesso contesto)[38]. L'assenza di un vero e proprio obbligo di interoperabilità o tantomeno compatibilità è reputato un fattore che inevitabilmente indebolisce il diritto in questione[39].

Il trasferimento deve poi avvenire gratuitamente, speditamente (entro un mese, quindi non istantaneamente) e senza impedimenti. In particolare, non potranno essere frapposti ostacoli di tipo finanziario, tecnico o legale: perciò non si potrà applicare alcun costo, richiedere l'adozione di un certo formato o l'impiego di una certa API o il superamento da parte degli utenti di altri ostacoli, quali complessità tecnica, ritardi o formalità eccessive, benché non sia facile la valutazione del carattere eccessivo o sproporzionato di tali ostacoli[40].

L'utente può anche chiedere la trasmissione dei dati, anziché a sé, direttamente ad altro titolare del trattamento (art. 20, par. 2) affinché questi siano riutilizzati e valorizzati presso quest'ultimo. Tale ultima forma di diritto alla portabilità dei dati è stata aggiunta nella versione finale del *GDPR* ed è particolarmente rilevante dal momento che il trasferimento diretto di dati tra il vecchio ed il nuovo titolare del trattamento facilita l'esercizio del diritto dell'individuo che potrebbe altrimenti essere ostacolato dalla complessità tecnica e difficoltà di comprensione dei passaggi. Esso è però subordinato, al contrario delle prime due forme di portabilità, alla circostan-

---

(*Guidelines*, cit., p. 18) lo riferisce, qualora in un dato settore non siano di uso commune certi formati, ai "*commonly used open formats (e.g. XML, JSON, CSV, etc.) along with useful metadata at the best possible level of granularity*". Cfr. anche DE HERT *et al.*, *The right to data portability*, cit., p. 197. Per aspetti tecnici sui formati, cfr. J. Krämer, P. Senellart, A. de Streel, *Making Data Portability More Effective for the Digital Economy - Report*, CERRE (June 2020), pp. 37, https://cerre.eu/wp-content/uploads/2020/07/cerre_making_data_portability_more_effective_for_the_digital_economy_june2020.pdf.

[38] Cfr. WP29, *op. cit.*, p. 17. Sulla differenza tra interoperabilità (dei dati, dei sistemi, ecc.) e compatibilità cfr. anche http://www.testingstandards.co.uk/interop_et_al.htm e CRÉMER *et al.*, *Competition Policy for the Digital Area*, cit.; E. CERVONE, *Strumenti di pagamento innovativi, interoperabilità e neutralità tecnologica: quali regole e quale governance per un mercato sicuro, efficiente ed innovativo*, in *Riv. trim. dir. econ.*, 2016, 41.

[39] P. PRZEMYSŁAW POLAŃSKI, *Some thoughts on data portability in the aftermath of the Cambridge Analytica scandal*, in *EuCML* 2018, 4, 141, pp. 142-143; O. BORGOGNO, G. COLANGELO, *Data sharing and interoperability: Fostering innovation and competition through APIs*, in *Computer Law & Security Review* 2019, 35, 5, p. 6.

[40] SOMAINI, *op. cit.*, p. 180; BORGHI, *op. cit.*, pp. 232-233.

za che l'operazione sia "tecnicamente possibile" in punto di interoperabilità [41] ed in particolare, come chiarito dal WP29, che la comunicazione tra i due sistemi sia possibile, sicura ed il sistema ricevente sia tecnicamente in posizione di ricevere i dati [42]. Stante l'incoraggiamento del considerando 68 all'interoperabilità ed il divieto per il titolare del trattamento di frapporre ostacoli (v. subito *supra*), le ipotesi in cui tale impossibilità tecnica si realizzi dovrebbero essere ridotte ma potrebbero concretizzarsi in casi in cui i costi di adeguamento per i piccoli operatori risultino eccessivi. Nel valutare l'impossibilità tecnica, infatti, sarà necessario tenere conto anche del tipo e del potere economico del titolare del trattamento [43].

La portabilità dei dati è un diritto che spetta solo alle persone fisiche (con esclusione quindi di persone giuridiche, associazioni, ecc. che non sono titolari del diritto alla tutela dei dati personali sulla base della CEDU, Carta dei diritti fondamentali e TFEU) ed è esercitabile unicamente dall'interessato.

Il novero dei soggetti obbligati (cioè dei titolari del trattamento tenuti a dare soddisfazione al diritto di portabilità) è particolarmente ampio, ricomprendendo tutti i soggetti che trattano elettronicamente dati personali, indipendentemente dal tipo di servizio offerto, dalle dimensioni dell'impresa e dal supporto. Per questo motivo, alcuni commentatori ritengono che lo stesso possa avere effetti anti-competitivi, non tenendo conto delle diversità esistenti tra imprese ed imponendo costi significativi (in termini di *compliance* o sanzioni in caso di violazione) in particolare per le piccole e medie imprese (che sarebbero quindi spinte a non investire in sistemi innovativi) [44] e che non sono ammesse ad addurre i costi come giustificazione

---

[41] La precisazione che l'espressione "tecnicamente possibile" si riferisca solo all'interoperabilità (che resta opzionale) e non al formato (che è invece obbligatoriamente per legge "strutturato, di uso comune e leggibile da dispositivo automatico") è suggerita dal WP29 che precisa anche il dovere del titolare del trattamento di fornire spiegazioni in merito all'impossibilità tecnica (*Guidelines*, p. 16). Cfr. anche DE HERT *et al.*, *Right to Data Portability*, cit., p. 197.

[42] WP29, *Guidelines*, cit., p. 16.

[43] J. SCHREY, *General conditions for data processing in companies under the GDPR*, in D. RUCKER, T. KUGLER (a cura di), *New European Data Protection Regulation: A Practitioner's Guide. Ensuring Compliant Corporate Practice* Hart Nomos, 2018, p. 145; PRZEMYSŁAW POLAŃSKI, *op. cit.*, p. 141.

[44] P. SWIRE, Y. LAGOS, *Why the right to data portability likely reduces customer welfare: antitrust and privacy critique*, in *MLR*, 2013, 72, 335, p. 339; A. DIKER VANBERG, M.B. ÜNVER, *The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?*, in *European Journal of Law and Technology*, 2017, 8, 1; A. DIKER VANBERG, *The right to data portability in the GDPR: what lessons can be learned from the EU experience?*, in *Journal of Internet*

per il mancato rispetto della normativa [45] (salvo quanto detto *supra* nel caso di portabilità diretta).

## 2.2. Dati oggetto del diritto

I dati oggetto del diritto alla potabilità sono esclusivamente dati personali cioè «qualsiasi informazione riguardante una persona fisica identificata o identificabile» (art. 4, par. 1 *GDPR*), con tale intendendosi non solo informazioni sensibili ma qualunque informazione sia soggettiva che oggettiva, anche in forma di pareri e valutazioni, purché concernenti il soggetto interessato [46]. Tale concetto è ormai amplissimo a seguito dell'interpretazione estensiva della Corte di Giustizia e della Corte CEDU, ricomprendendosi non solo nomi, dati riguardanti localizzazione, identità fisica, psicologica, genetica, mentale, culturale, economica e sociale ma addirittura anche una prova d'esame e le correzioni ad esso apportate, i valori di beni immobili, la velocità di veicoli e informazioni metereologiche qualora riferibili ad un soggetto [47].

Tali dati devono infatti riguardare uno specifico interessato, con esclusione quindi di dati riguardanti soggetti terzi o anonimi. Tuttavia, sono invece ricompresi i dati pseudo-anonimizzati, cioè per i quali sia possibile l'identificazione dell'interessato *ex post* attraverso l'ausilio della tecnologia, anche se in possesso di terzi e disponibili solo in un prossimo futuro [48].

---

*Law*, 2018, 21, 7, 11, p. 13; R. JANAL, *Data Portability – A Tale of Two Concepts*, in *JIPITEC*, 2017, 8, 1, 59, 5. Per una stima dei costi di adeguamento che il *GDPR* impone alle imprese europee, cfr. L.R. CHRISTENSEN, A. COLCIAGO, F. ETRO, G. RAFAERT, *The Impact of the Data Protection Regulation in the EU*, in *European Financial Review* 2013, 72.

[45] Cfr. WP29, *Guidelines*, cit., p. 15.

[46] M. MONTAGNANI, *La libera circolazione dei dati al bivio. Tra tutela dei dati personali e promozione dell'intelligenza artificiale europea*, in *Mercato, concorrenza e regole*, 2019, 2, 293, p. 306.

[47] Anche dati biometrici, valori dei beni immobili, indirizzi IP dinamici, informazioni meteorologiche, velocita di un veicolo: Case C-70/10 *Scarlet Extended* (2011) ECLI:EU:C:2011:771 para 51; Case C-582/14 *Breyer* (2016) ECLI:EU:C:2016:779 paras 44-49; Case C-434/16 *Nowak* (2017) ECLI:EU:C:2017:994 para 62. Cfr. BORGHI, *op. cit.*, p. 229 ss.; N. PURTOVA, *The Law of Everything. Broad Concept of Personal Data and Future of Eu Data Protection Law*, in *Journal Law, Innovation and Technology*, 10, 1, 2018, pp. 40, 43-44.

[48] Nella valutazione della personalità del dato deve tenersi conto dei costi, tempi necessari e tecnologie disponibili anche in un prossimo futuro. Cfr. considerando 26 *GDPR*; Sentenza CGCE (Seconda sezione), caso C-582/14, *Patrick Breyer vs Bundesrepublik Deutschland*, Ecli:Eu:C:2016:779; MONTAGNANI, *op. cit.*, pp. 306-307; SOMANI, *op. cit.*, p. 184; BORGHI, *op. cit.*; S. STALLA-BOURDILLON, A. KNIGHT, *Anonymous Data v Personal Data – A False Debate: An EU Perspective on Anonymization, Pseudonymization and Personal Data*, in *Wisconsin International Law Journal*, 34, 2017, p. 285.

Ad ogni modo, i dati personali coperti dal diritto alla portabilità costituiscono un gruppo più ristretto rispetto a quelli ricompresi nel diritto di accesso, anche a causa della maggior ampiezza del primo diritto in termini di azioni permesse. La portabilità, infatti, riguarda solo i dati precedentemente "forniti" dall'interessato ad un titolare del trattamento e che siano stati trattati in forma automatizzata (non, ad esempio, cartacea [49]), sulla base del consenso [50] o per la necessità oggettiva di eseguire un contratto o misure precontrattuali su richiesta dell'interessato [51] (art. 20, par. 1 *GDPR*). Sono quindi esclusi i dati raccolti con base giuridica diversa, quali quelli trattati dalle banche in adempimento degli obblighi in materia di antiriciclaggio [52]. Il WP29 ha interpretato estensivamente il concetto di "dati forniti" ricomprendendovi non solo i dati forniti dall'interessato attivamente ma anche quelli forniti passivamente, cioè le informazioni personali che possono essere "osservate" nel corso dell'erogazione del servizio (ad esempio, cronologia di ricerca, dati su traffico e localizzazione ottenuti attraverso *cookies*, *GPS*, metadata, numero di click su certi prodotti, precedenti acquisti) [53]. Ciò potrebbe comportare un significativo aggravio economico

[49] Alcuni commentatori ritengono coperti dal diritto in questione, in linea con l'ambito generale di applicazione del *GDPR*, anche i dati oggetto solo parzialmente di automazione ma in tal caso si richiederebbe al titolare del trattamento l'onere aggiuntivo di convertire tali dati nel formato "*machine readable*" prima della trasmissione: ELFERING, *op. cit.*, p. 25. *Contra*, limitando la copertura del diritto alla portabilità ai soli dati processati in modo completamente automatico: SCUDIERO, *op. cit.*, p. 123.

[50] Cfr. all'art. 6, par. 1, lett. a), e, in caso di dati sensibili, art. 9, par. 2, lett. a), *GDPR*. In materia di consenso, cfr. anche recentemente EUROPEAN DATA PROTECTION BOARD (EDPB), *Guidelines 05/2020 on consent under Regulation 2016/679*, (May 2020), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

[51] Cfr. considerando 68 e art. 6, par. 1, lett. b), *GDPR*. La Commissione non ha dunque accolto il consiglio dello *European Data Protection Supervisor* di far coincidere l'ambito di copertura del diritto di accesso e quello di portabilità, stabilendo dunque di limitare quest'ultimo ai soli casi di consenso e contratto: EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 3/2015 (with addendum) Europe's big opportunity – EDPS recommendations on the EU's options for data protection reform*, (9 October 2015), p. 12 (nota 34); cfr. anche SOMAINI, *op. cit.*, p. 166, nota 7. In materia, cfr. anche EUROPEAN DATA PROTECTION BOARD (EDPB), *Linea guida 2/2019 sul trattamento di dati personali ai sensi dell'articolo 6, paragrafo 1, lettera b), del regolamento generale sulla protezione dei dati nel contesto della fornitura di servizi online agli interessati*, (8 ottobre 2019), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_it.pdf.

[52] KRÄMER, SENELLART, DE STREEL, *Making Data Portability More Effective*, cit., pp. 19 ss.

[53] WP29, *Guidelines on the right to data portability*, cit., pp. 9-10 (sarebbero anche coperti i dati grezzi, quali sul battito cardiaco, raccolti attraverso *wearable devices*, storico di operazioni e accessi); European Data Protection Supervisor, *Opinion 3/2015*, cit., p. 12, nota 34. KRÄMER, SENELLART, DE STREEL, *Making Data Portability,* p. 51. *Contra*, a favore quindi di un'inter-

per i titolari del trattamento, salvo l'impiego, nei casi più gravi (in cui sia a rischio la prosecuzione dell'attività economica), della clausola di bilanciamento di cui all'art. 20, par. 4, la quale permette la limitazione del diritto alla portabilità qualora ciò comporti la lesione di diritti e libertà altrui. Conseguentemente, risulterebbero ricompresi nel diritto alla portabilità anche i dati osservati dal titolare del trattamento senza ulteriore lavoro e sforzi (di tipo intellettuale, economico e scientifico)[54], mentre resterebbero esclusi i dati "derivati" (ad esempio, dati computazionali) e "rielaborati" ("*inferred*") a partire dai dati forniti o osservati e quindi "creati" dal titolare del trattamento attraverso la *data analytics*, (quali calcoli, predizioni, profili, *ranking*, ecc.), così da favorire la concorrenza e l'innovazione nella fase di rielaborazione dei dati (invece che nell'osservazione)[55]. Con riferimento a queste tipologie di dati, si potrebbero solo usare gli strumenti riconosciuti dal Regolamento in materia di processo decisionale automatizzato e profilazione (art. 22 *GDPR*), cioè il diritto di accesso con riferimento alle informazioni "[sul]*l'esistenza di un processo decisionale automatizzato, compresa la profilazione […] e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato*" (art. 15, par. 1, lett. h, *GDPR*), diritto di opposizione (art. 21 *GDPR*), diritti di rettifica, cancellazione e limitazione del trattamento (artt. 16-18 *GDPR;* cfr. anche *infra*, §3.2)[56].

---

pretazione restrittiva e più letterale che escluda pure i dati osservati: CENTRE FOR INFORMATION POLICY LEADERSHIP, *Comments on the Article 29 Data Protection Working Party's "Guidelines on the right to data portability"*, cit., p. 8 (i dati non forniti attivamente ma "osservati" rientrerebbero nell'ambito del diritto alla portabilità solo qualora inestricabilmente legati ai primi). Cfr. anche G. MALGIERI, *Property and (Intellectual) Ownership of Consumers' Information: A New Taxonomy for Personal Data, Privacy*, in *Germany – PinG,* 2016, 4, 133, p. 143; G. MALGIERI, *User-provided personal content' in the EU: digital currency between data protection and intellectual property* in *IRLCT* 2018, 32, 1, 118, p. 130; B. VAN DER AUWERMEULEN, *How to attribute the right to data portability in Europe: A comparative analysis of legislations*, in *Computer Law & Security Review* 2017, 33, 57, p. 61; DE HERT *et al.*, *The right*, cit., pp. 199-200; SOMAINI, *op. cit.*, p. 185 ss.; BORGHI, *op. cit.*, p. 230 ss.

[54] WP29, *Guidelines*, cit., p. 10; WP29, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, (revised 6 February 2018), p. 17, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053; DE HERT *et al.*, *The right*, cit., p. 199.

[55] Cfr. KRÄMER, SENELLART, DE STREEL, *Making Data Portability More Effective*, cit., pp. 8-9, 51 ss.

[56] WP29, *Guidelines*, cit., p. 10 (nota 20); WP29, *Guidelines on Automated individual decision-making*, cit., p. 17 ss.; GRAEF *et al.*, *Data Portability*, cit.; SCUDIERO, *op. cit.*, p. 123; BORGHI, *op. cit.*, p. 230; SOMAINI, *op. cit.*, p. 186; GIORGIANNI, *op. cit.*; F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali – Il Regolamento europeo 2016/679*, in F. PIZZETTI (a cura di), *I diritti nella "rete" della rete*, Giappichelli, Torino, 2016; cfr. anche STOYKOVAR,

Un capitolo a parte è rappresentato dalle recensioni che gli utenti lasciano sulle piattaforme online, che gli studi attestano come capaci, ad esempio, di orientare significativamente le scelte di chi acquista online e, conseguentemente, anche alla scelta in merito piattaforma, spingendo verso quella con un maggior numero di *reviews*, con conseguenti eventuali significativi effetti di *lock-in*[57]. Tali recensioni, infatti, possono considerarsi dati personali pubblici forniti dagli utenti compratori (che sarebbero titolari del diritto alla portabilità delle proprie recensioni salvo il limite dei diritti dei titolari di database di recensioni che abbiano compiuto rilevanti investimenti per la creazione del detto database: v. *infra* § 2.3) ma i veri interessati al trasferimento sarebbero soprattutto gli utenti venditori che trarrebbero beneficio nel trasferire anche su altre piattaforme i *feedback* (se positivi) che li riguardano: le recensioni potrebbero forse essere considerate anche dati personali dei venditori (visto che li riguardano, anche se sono primariamente dati personali degli autori delle recensioni) e "forniti" sulla base del consenso (acconsentendo alla pubblicazione degli stessi)[58] e quindi coperti dal diritto alla portabilità, sempre che non siano frutto di rielaborazioni della piattaforma (perciò le singole recensioni sì, non i *ranking/score* elaborati dalla piattaforma) e sempre senza compromissione dei diritti dei terzi (autori delle recensioni o la piattaforma che abbia investito nel database: v. *infra*, § 2.3) ma il punto è dibattuto anche in dottrina e si propende per una risposta negativa.

Con riferimento invece all'inciso "sulla base del consenso", sarebbero esclusi i dati, ad esempio, sulla visualizzazione del profilo dell'interessato o ricerche effettuate sullo stesso, proprio perché su tali dati "osservati" non sarebbe stato dato uno specifico consenso da parte dell'interessato ma gli stessi sarebbero trattati comunque legittimamente a causa della presenza di un legittimo interesse del titolare *ex* art. 6, par. 1, lett. f), *GDPR*[59]. Allo stesso modo restano esclusi i dati processati nell'ambito degli obblighi conseguenti all'applicazione della normativa in materia di anti-riciclaggio,

---

*The Right to Data Portability*, cit., p. 67. A proposito della tassonomia dei dati, cfr. OECD, *Summary of the OECD Privacy Expert Roundtable on 21 March 2014 – Protecting Privacy in a Data-driven Economy Taking Stock of Current Thinking* (2014), pp. 3, 5.

[57] V. KATHURIA, J.C. LAI, *User review portability: Why and how?*, in *Computer Law & Security Review*, 2018, 34, p. 1291; VANBERG, *The right to data portability in the GDPR*, cit., pp. 11-12.

[58] Probabilmente *contra* Elfering (cit., pp. 26-27) che esclude la portabilità di eventuali foto ritraenti il soggetto interessato ma postate da terzi (ad esempio, un amico), in quanto non fornite dall'interessato ma, appunto, da terzi.

[59] BORGHI, *op. cit.*, p. 232; F. FERRETTI, *Data protection and the legitimate interest of data controllers: much ado about nothing or the winter of rights?*, in *Common Market Law Review*» 2014, 51(3), 843.

avvenendo il trattamento sulla base degli obblighi di legge (art. 6, par. 1, lett. c, *GDPR*) o legittimo interesse (art. 6, par. 1, lett. f, *GDPR*) e non del consenso o dell'esecuzione di un contratto [60].

## 2.3. Limitazioni del diritto alla portabilità

Date la *ratio* del diritto alla portabilità e la lata interpretazione della Corte e del *WP29*, sono limitati i casi in cui la richiesta di portabilità può essere rigettata o accettata solo in parte.

In primo luogo, il titolare del trattamento non è tenuto a (anzi, in forza dell'art. 5 *GDPR*, ha il divieto di) conservare i dati una volta esaurita la finalità per cui era stato iniziato il trattamento, per cui l'interessato può esercitare il diritto solo prima che sia stata raggiunta la finalità o esaurito il tempo utile per il perseguimento della stessa (cfr. § 2.1) [61]. Tuttavia, perché il dovere di cancellazione dei dati da parte del titolare del trattamento non si traduca in una frustrazione del diritto alla portabilità, il principio di correttezza richiede al titolare del trattamento d'informare l'interessato dell'eventuale prossima cancellazione dei dati [62].

In secondo luogo, può essere opposto un rifiuto alla richiesta di portabilità qualora il trattamento avvenga sulla base dell'espletazione di un compito nel pubblico interesse o nella veste di autorità (considerando 68; art. 20, par. 3, *GDPR*) [63]. Il WP29 raccomanda comunque agli Stati di sviluppare *best practices* per rispondere automaticamente alle richieste di portabilità nei confronti di tali soggetti espletanti una funzione pubblica [64].

In terzo luogo, può essere rifiutata la richiesta di portabilità nel caso particolare già menzionato di trasferimento diretto tra titolari del trattamento (non quindi in caso di trasferimento tra un titolare e l'interessato) qualora il trasferimento sopra descritto non sia "tecnicamente fattibile" (v. *supra* § 2.1). In tal caso, però, l'interessato potrebbe comunque chiedere il trasferimento a sé e poi ritrasferire al nuovo titolare, così da disincentivare

---

[60] WP29, *Guidelines*, cit., p. 8.

[61] GIORGIANNI, *op. cit*.

[62] A. RICCI, *I diritti dell'interessato*, in G. FINOCCHIARO (diretto da), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, cit., p. 179 ss., p. 224; PELINO, *I diritti dell'interessato*, cit., p. 171 ss., p. 252; GIORGIANNI, *op. cit.*

[63] Cfr. anche artt. 6, par. 1, lett. e), artt. 9, par. 2, e 23 *GDPR*.

[64] WP29, *Guidelines*, cit., p. 8 (anche nota 16).

eventuali rifiuti ingiustificati[65]. Si è sollevata la questione se, tra i casi di impossibilità tecnica, si possano far rientrare quelli in cui il secondo titolare non garantisca un'adeguata tutela dei dati trasmessi: tale ipotesi rappresenta un pericolo concreto nonché effetto indesiderato della concorrenza (il nuovo operatore offre un prezzo più basso sacrificando la sicurezza dei dati, aspetto non percepibile, almeno immediatamente, dal cliente) ma che potrebbe anche essere strumentalizzato a suo vantaggio dal primo titolare del trattamento[66]. Inoltre, il *GDPR* non si occupa di regolare il riparto di responsabilità anche in caso di perdita o danneggiamento dei dati durante l'operazione di trasferimento, fattore che certo non agevola il diritto alla portabilità[67].

Ancora, la richiesta di portabilità può essere disattesa qualora ciò comporti la lesione di diritti e libertà altrui (art. 20, par. 4, *GDPR*) quali, ad esempio, la compromissione dei diritti (anche di accesso e opponibilità) di altri soggetti i cui dati non siano separabili da quelli dell'interessato (v. in caso di e-mail, discussioni su forum o blogs o foto su *social network* ritraenti più soggetti). La "*non-prevalence clause*" (il diritto alla portabilità "*non deve ledere* i diritti e le libertà altrui") impone un bilanciamento quindi tra diritti di soggetti diversi[68] e il WP29 ha individuato come principi guida la personalità della disponibilità del dato e della finalità del trattamento, nel senso che i dati trasferiti, per non ledere i diritti dei terzi, devono restare nell'esclusiva disponibilità del richiedente e per finalità personali e domestiche di questi. Sono fatti però salvi i casi in cui la finalità del trattamento sia la stessa per cui è stato dato originariamente il consenso da parte degli altri soggetti al primo titolare (ad esempio, trasferimento della rubrica di indirizzi e-mail o dello storico sui pagamenti dove la finalità di trattamento sia sempre la stessa invece che diventare finalità di *marketing* presso i terzi o profilazione dei medesimi) oppure sia concesso un nuovo consenso da parte dei terzi o il trattamento dei dati degli stessi sia legittimo su altra base legale (ad esempio, il legittimo interesse del titolare del trattamento *ex* art. 6, par. 1, lett. f, *GDPR*)[69]. Ad ogni modo, il WP29 raccomanda che i titolari del trattamento mettano a disposizione strumenti

---

[65] ELFERING, *op. cit.*, p. 23.

[66] SCUDIERO, *op. cit.*, p. 124.

[67] KRÄMER, SENELLART, DE STREEL, *Making Data Portability*, cit., p. 76. Cfr. anche E. EGAN, *Charting a way forward: Data portability and privacy – Facebook White Paper*, https://about.fb.com/wp-content/uploads/2020/02/data-portability-privacy-white-paper.pdf.

[68] Cfr. STOYKOVAR, *op. cit.*, p. 70.

[69] WP29, *Guidelines*, cit., pp. 11-12. Cfr. anche TROIANO, *op. cit.*, p. 215.

che permettano la scelta dei dati da trasferire da parte del richiedente e, quando possibile, di escludere i dai personali di altri così come di sistemi per ottenere il consenso dei terzi coinvolti. La valutazione dovrà avvenire inevitabilmente caso per caso, tenendo in considerazione molteplici fattori (come i dati sono usati, aspettative ragionevoli sull'uso, relazioni tra il titolare del trattamento e i soggetti, ulteriori tutele predisposte dal titolare del trattamento, ecc.) [70].

Il WP29, in analogia col diritto di accesso (cfr. considerando 63 e art. 15 *GDPR*), ritiene che possano rientrare nei diritti e libertà altrui, anche i diritti di proprietà industriale di soggetti terzi così come dello stesso titolare del trattamento, senza però che si possa negare in tal caso il diritto alla portabilità sulla base di ciò ma realizzando invece un bilanciamento e potendosi quindi solo escludere dalla portabilità i dati che comprometterebbe i diritti in questione. Il WP29 precisa però ovviamente che l'interessato non debba far uso dei dati ricevuti in modo che ciò possa qualificarsi come pratiche commerciali sleali e che il titolare del trattamento debba mettersi nella condizione di essere in grado di trasferire solo i dati non coperti dai suoi diritti di proprietà industriale (quindi potendo solo limitare, non escludere, il diritto alla portabilità) [71]. Tale posizione viene comunque contestata da diversi commentatori per la distinta fruizione dei dati in caso di accesso e di portabilità (solo in tale secondo caso, infatti, i dati possono essere anche trasferiti a terzi) e si suggerisce di lasciare ai giudici il compito di valutare caso per caso [72].

Come anticipato, possono venirsi a creare conflitti di compatibilità anche con i diritti di titolari di banche dati riconosciuti dalla direttiva 96/9 sulla tutela giuridica delle banche dati [73]. Per banca dati deve intendersi "una raccolta di opere, dati o altri elementi indipendenti" (per cui la separazione degli stessi non influisce sul valore del singolo elemento nella prospettiva dell'utente) [74], "sistematicamente o metodicamente disposti" (an-

---

[70] Cfr. WP29, *Guidelines*, p. 12; SOMAINI, *op. cit.*, p. 21; TROIANO, *op. cit.*, p. 215.

[71] WP29, *Guidelines on the right to data portability*, cit., 12; P. VOIGT, A. VON DEM BUSSCHE, *The EU General Data Protection Regulation (GDPR). A practical Guide*, Springer, London/New York, 2017, p. 173; DIKER VANBERG, ÜNVER, *The right to data portability in the GDPR and EU competition law*, cit., p. 5; ELFERIN, *op. cit.*, p. 30.

[72] BORGHI, *op. cit.*, p. 235; SOMAINI, *op. cit.*, pp. 183-184.

[73] Directive 96/9/EC of 11 March 1996 on the legal protection of databases [1996] OJ L 77/20 (Database Directive). Cfr. in questo *Volume* il contributo di V. Falce, *Tech-fin databases in the open banking system. An out-of-the-box competition law perspective*.

[74] Case C-444/02 *Fixtures Marketing v OPAP* (2004) ECLI:EU:C:2004:697 para 24; Case C-490/14 *Verlag Esterbauer* (2015) ECLI:EU:C:2015:735 para 37.

che semplicemente attraverso un indice o organizzati secondo un certo metodo)[75] ed individualmente accessibili grazie a mezzi elettronici o in altro modo". Perché il diritto di esclusiva dei creatori dei *database* (di impedire l'estrazione ed il riutilizzo dell'intero database o di una parte sostanziale dei relativi contenuti) trovino protezione, è necessario che essi abbiano effettuato significativi investimenti, non necessariamente in termini monetari ma anche di risorse umane e tecniche, nella creazione del database cioè nella raccolta, verifica e presentazione dei dati contenuti. In considerazione perciò dell'ampia definizione di banca dati, anche i dati personali raccolti ed organizzati sistematicamente o metodologicamente da un titolare del trattamento potrebbero costituire una banca dati e, conseguentemente, sempre in presenza di investimento consistente in tale raccolta ed organizzazione, un'eventuale estrazione e trasferimento sostanziale oppure frequente di dati degli utenti a seguito di richieste di portabilità (specialmente se dirette e incentivate dal secondo titolare) potrebbe costituire una compromissione dei diritti del titolare del trattamento in quanto creatore della banca dati e quindi giustificare una limitazione dei diritti di portabilità, con compromissione dell'obiettivi del *GDPR* in materia di portabilità[76]. Tale ostacolo potrebbe essere probabilmente risolto a livello interpretativo ma un miglior coordinamento tra le due normative sarebbe opportuno[77] e nell'ambito della Strategia Europea dei dati si propongono appunto modifiche sia alla *Database Directive* che alla direttiva *Trade Secrets Protection* (96/9/CE) per portare maggior chiarezza su tale punto[78].

Infine, l'art. 20, par. 3 (primo periodo), *GDPR* stabilisce una prevalenza del diritto all'oblio sul diritto alla portabilità (il secondo deve lasciare "*impregiudicato*" il primo), per cui quest'ultimo potrebbe trovarsi legittimamente impedito dalla richiesta di cancellazione di terzi i cui dati siano inseparabili da quelli del primo interessato (v. anche *supra*)[79].

Ad ogni modo, una richiesta di portabilità può essere rifiutata qualora sia manifestatamente infondata, eccessiva, anche in quanto ripetitiva (oppure giustificare l'applicazione di spese: art. 12, par. 5, *GDPR*). Tuttavia, il WP29 ha chiarito, in parte togliendo efficacia alla norma in discorso, che

---

[75] Case *Fixtures Marketing*, cit., para 30.

[76] ELFERING, *op. cit.*, p. 36 ss., in particolare, p. 43 ss.

[77] Per un'analisi approfondita del problema e proposta di soluzione, cfr. ELFERING, *op. cit.*

[78] COMMISSION, A *European Strategy for Data*, cit., p. 14.

[79] WP29, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*. Cfr. anche DE HERT *et al.*, *The right to data portability*, cit., p. 198; LI, *op. cit.*

l'uso di sistemi automatici e API dovrebbe ridurre il peso collegato a richieste ripetitive e quindi non giustificare il rifiuto su tali basi, non potendosi comunque addurre gli elevati costi come ragione del rifiuto [80].

## 3. *PSD* 2 e *open banking*

### 3.1. *Open banking*: caratteristiche principali e *ratio*

Prima che il *GDPR* introducesse un diritto alla portabilità dei dati personali in via generale, il legislatore europeo aveva già creato una speciale forma di portabilità dei dati nel settore dei servizi di pagamento.

Questo perché la raccolta e l'impiego dei dati ha da sempre rivestito una rilevanza particolare nel settore dei pagamenti. Gli operatori bancari e finanziari, infatti, nel normale svolgimento della propria attività, vengono in possesso di un'enorme quantità di dati, specialmente di pagamento (personali, sensibili, e non) e li hanno tradizionalmente utilizzati per una varietà di funzioni, non solo per adempiere a taluni obblighi di legge (v. in materia di antiriciclaggio e lotta al terrorismo e classificazione *MiFID II*) ma anche per svolgere in maniera più efficiente la propria attività (si pensi alle informazioni necessarie per concedere un mutuo o un'apertura di credito) ed offrire ulteriori servizi parametrati al conseguente profilo del cliente. Sempre tradizionalmente, le banche sono state le uniche depositarie di una massa così consistente di dati dei clienti, a causa della natura di operatore universale (l'unico a poter offrire qualunque tipo di servizio finanziario) e dello stretto rapporto diretto con la clientela, avendo, d'altra parte, come contraltare investimenti di tempo e risorse così come regole molto stringenti da rispettare.

Tuttavia, non solo questa attività di raccolta e profilazione deve sottostare alle relative norme del *GDPR* (*in primis*, art. 22; cfr. *infra* § 3.2) ma la riserva di dati in questione è stata aperta anche altri operatori, sia in virtù dell'art. 20 *GDPR* sulla portabilità dei dati personali (e trasmissione diretta degli stessi ad altri operatori), sia ancora di più a seguito dell'entrata in vigore della *Payments Services Directive n. 2* (*PSD2*) – direttiva 2015/2366 sui servizi di pagamento nel mercato interno, recepita nell'ordinamento nazionale con d.lgs. 15 dicembre 2017, n. 218 [81]. Questa direttiva specifica

[80] WP29, *Guidelines*, cit., p. 15.

[81] D.lgs. 15 dicembre 2017, n. 218 "Recepimento della direttiva (UE) 2015/2366 relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e

ed estende la tendenza a rendere i dati dei clienti delle banche maggiormente accessibili ai soggetti terzi, dietro autorizzazione dei clienti stessi, secondo il modello del c.d. "*open banking*" [82].

In particolare, l'art. 36 *PSD2* stabilisce l'obbligo per le banche e altri operatori presso cui sono radicati i conti (istituti di pagamento, ad esempio) di dare accesso, in tempo reale e in maniera non discriminatoria (anche in termini di costi, quindi non applicando commissioni superiori a quelle normalmente applicate per ordini di pagamento o accesso al conto provenienti da operatori diversi), ai dati sull'informazione sui conti di pagamento online dei loro clienti (in questo caso, anche persone giuridiche), con consenso esplicito di questi ultimi. Beneficiari di tale accesso sono *provider* terzi che forniscano certi servizi di pagamento o di informazione sui conti (v. *infra*) e anche in assenza di accordi contrattuali con questi operatori (*access to account – XS2A – rule*). Ciò sarà reso possibile anche dall'impiego di *API*, cioè, si è visto, interfaccia che permettano a *provider* e programmi diversi di interagire in maniera sicura e predefinita, secondo le indicazioni tecniche fornite dall'European Banking Authority (EBA).

La logica è quindi quella di permettere a tali emergenti *third party providers – TPP* – di accedere al mercato grazie all'accesso ai dati delle banche. Tali operatori, infatti, offrendo servizi di tipo *front-end*, non sarebbero in grado di svolgere la propria attività in assenza di collaborazione da parte delle banche e di conseguente accesso ai dati sui clienti e di collaborazione. D'altra parte, le banche non vedono di buon occhio operatori in grado di operare come interfacce dirette con i propri clienti e di sostituirsi alle stesse nel rapporto privilegiato con i medesimi e potevano, ai sensi della precedente normativa *PSD*, negare l'accesso ai dati dei clienti adducendo ragioni non solo di sicurezza ma anche di tutela della proprietà intellettuale e di rischi di responsabilità. In tal modo, invece, la nuova normativa riduce il rischio di pratiche anti-competitive delle banche e migliora perciò la con-

2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE, nonché adeguamento delle disposizioni interne al regolamento (UE) n. 751/2015 relativo alle commissioni interbancarie sulle operazioni di pagamento basate su carta". Per un'analisi della nuova normativa: F. PORTA, *Obiettivi e strumenti della PSD2*, in F. MAIMERI, M. MANCINI, *Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, criptovalute e rivoluzione digitale*, Quaderni di ricerca giuridica della Banca d'Italia n. 87/2019, Banca d'Italia, Roma, 2019, p. 21 ss. Con riguardo ai conti di pagamento, cfr. S. MEZZACAPO, *La nuova disciplina nazionale dei conti di pagamento alla luce dell'armonizzazione attuata con la Payments Accounts Directive*, in *Banca Borsa e titoli di credito*, 2017, I, 787.

[82] In materia, BASEL COMMITTEE ON BANKING SUPERVISION (BCBS), *Report on open banking and application programming interfaces*, (November 2019), https://www.bis.org/bcbs/publ/d486.pdf.

correnza nel settore dei pagamenti, favorendo il fenomeno dell'*un-bundling* dei servizi e la frammentazione delle catene di valore degli stessi, con, potenzialmente, l'offerta di servizi migliori ai clienti [83].

La *PSD2* apre infatti contestualmente il mercato a due nuovi servizi e due nuove categorie di operatori: i prestatori di servizi di disposizione di ordini di pagamento (o *Payment Initiation Service Providers – PISP*) e i prestatori di servizi di informazione sui conti (*Account Information Services Providers – AISP*) [84].

I *PISP* consentono al cliente di disporre un ordine di pagamento a valere direttamente su un conto di pagamento che lo stesso abbia presso altro operatore (il prestatore di servizi di radicamento del conto o *Account Servicing Payment Service Provider*, *ASPSP*). In tal modo, nell'ambito ad esempio dell'*e-commerce*, si crea un collegamento agevole tra il sito del commerciante ed il sito della propria banca e si può rassicurare il beneficiario dell'avvenuta disposizione di pagamento (in modo che proceda immediatamente alla spedizione del bene) ma, allo stesso tempo, eliminare la necessità di usare una carta di credito e sopportare i relativi costi e oneri (ad esempio, digitazione del numero della carta e PIN di sicurezza) o, comunque, avere la comodità di usare la semplice impronta digitale o dati precompilati su importo e beneficiario [85].

Gli *AISP* invece offrono un servizio *on line* che permette di consolidare

---

[83] COMMISSION, *Impact Assessment accompanying the Proposal for a directive on payment service in the internal market*, SWD(2013) 288 final; G. COLANGELO, O. BORGOGNO, *Open banking, portabilità dei dati e regime di accesso ai conti di pagamento*, in G. FINOCCHIARO, V. FALCE (a cura di), *Fintech: diritti, concorrenza, regole. Le operazioni di finanziamento tecnologico*, Zanichelli, Milano, 2019, p. 117 ss., pp. 220-21. La *PSD2* è stata definita come "il fronte più avanzato del processo di destrutturazione in atto nella filiera dell'attività finanziaria" (A. SCIARRONE ALIBRANDI, *Impostazione sistematica della direttiva 20152366*, relazione presentata al convegno "*Innovazione e regole: il bilanciamento degli interessi nella PSD2*, svoltosi presso l'Università degli studi Roma Tre il 18 ottobre 2018, i cui atti sono stati raccolti nell'omonimo volume a cura di MARIA CECILIA PAGLIETTI, MARIA IRIDE VANGELISTI, Romatre-press, marzo 2020, reperibile al link http://romatrepress.uniroma3.it/wp-content/uploads/2020/03/Innovazione-e-regole-nei-pagamenti-digitali.pdf) e "la punta normativamente più avanzata del processo di *un-bundling* in atto nel settore" (A. ARGENTATI, *Le banche nel nuovo scenario competitivo. Fin-Tech, il paradigma Open banking e la minaccia delle big tech companies*, in *Mercato Concorrenza Regole* 2018, 3, p. 441, in particolare p. 443).

[84] In materia *di third party providers*: COLANGELO, BORGOGNO, *Open banking,* cit., p. 117 ss.; C. SERTORI, *PSD2, sicurezza e privacy*, in MAIMERI, MANCINI, *op. cit.*, pp. 161-63.

[85] Cfr. considerando 27 *PDS2*; P.T.J. WOLTERS, B.P.F. JACOBSB, *The security of access to accounts under the PSD2*, in *Computer Law & Security Review*, 2019, 35, 29; F. CIRAOLO, *I servizi di pagamento nell'era FinTech*, in M.T. PARACAMPO (a cura di), *Fintech. Introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari*, 2ª ed., Giappichelli, Torino, 2019, volume II, p. 217, in particolare p. 227.

le informazioni relative ai diversi conti di cui uno stesso utente dispone (presso lo stesso o diversi intermediari), così fornendogli un quadro complessivo della propria situazione finanziaria e movimenti, eventualmente anche organizzati secondo categorie di preferenza (ad esempio, lavoro, tempo libero, famiglia, ecc.), e, conseguentemente, anche l'opportunità di gestire meglio le proprie risorse. L'ampiezza definitoria di tale servizio sembrerebbe permettere anche la prestazione di servizi personalizzati di vario tipo (monitoraggio delle spese, *budget planning*, consulenza sulla situazione debitoria o sulla presentazione di domande di prestito o assistenza) [86] o la trasmissione di dati a terzi per la stessa finalità (ad esempio, consulenti finanziari o agenzie di informazione creditizia) [87].

Tuttavia, esso non copre altri servizi finanziari che richiedono una separata autorizzazione (servizi di investimento) o l'accesso a dati di conti diversi da quelli di pagamento (quali conti di risparmio e investimenti): in tal caso, non troverebbe applicazione l'*open banking* ed il trattamento dei dati regolato dalla *PSD* 2 ma solo il diritto alla portabilità e il trattamento dei dati del *GDPR* [88].

A seguito di tale fenomeno dell'*open banking* e delle prescrizioni della *PSD2*, le banche sono chiamate a dotarsi di infrastrutture tecnologiche adeguate a consentire un'efficace e sicura interazione con i sistemi *TPP* attraverso modifiche all'interfaccia del cliente o, più probabilmente, la predisposizione di API (art. 31 *PSD2*), sostenendo costi per lo sviluppo e la manutenzione delle reti e dei sistemi informativi [89]. A causa dell'assenza d'imposizione di specifici requisiti tecnologici da parte della *PSD2* e del suo regolamento tecnico [90] in forza del principio di neutralità tecnologica, anche i *TPP* sarebbero potenzialmente esposti a costi considerevoli: le banche potrebbero infatti stabilire diverse API tra loro, così imponendo ai

[86] FINANCIAL CONDUCT AUTHORITY (FCA), *Call for Input: Open finance*, (dicembre 2019), p. 8, https://www.fca.org.uk/publication/call-for-input/call-for-input-open-finance.pdf.

[87] WOLTERS, JACOBSB, *op. cit.*, p. 32.

[88] EUROPEAN DATA PROTECTION BOARD (EDPB), *Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR (version 1.0) - Consultation*, (22 luglio 2020), p. 6, https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202006_interplay psd2andgdpr.pdf (secondo il quale neppure il servizio di valutazione del merito creditizio potrebbe ritenersi ricompreso nell'ambito del servizio dell'informazione sui conti della *PSD2*).

[89] CIRAOLO, *I servizi di pagamento*, cit., p. 235 ss.; D. GAMMALDI, C. IACOMINI, *Mutamenti del mercato dopo la PSD2*, in F. MAIMERI, M. MANCINI, *Le nuove frontiere dei servizi bancari e di pagamento fra PSD2, criptovalute e rivoluzione digitale 2019*, Quaderni di ricerca giuridica della Banca d'Italia n. 87/2019 (Banca d'Italia, Roma, 2019), p. 139.

[90] Regolamento delegato UE 2018/389 della Commissione del 27 novembre 2017 che va ad integrare la *PSD2* con norme tecniche di regolamentazione (*RTS*).

*TPP* di attrezzarsi per interagire con tali differenti ed innumerevoli tipi di API [91]. Oltre agli sforzi di coordinamento e fissazione di standard tecnici dell'EBA [92], nel nostro paese tale rischio è stato scongiurato da un'iniziativa di settore (attraverso un consorzio di banche e *TPP*), così come sembra avvenire più in generale in Europa (v. Gruppo di Berlino), mentre nel Regno Unito si è ricorsi alla definizione di parametri comuni a livello normativo [93].

Ad ogni modo, si ripete, la *ratio* dell'art. 36 è stata quella di completare l'apertura alla concorrenza nel settore dei pagamenti iniziata con la *PSD* attraverso l'apertura del patrimonio informativo delle banche ai *new entrants*, in particolare, le piccole imprese *fintech*, così anche da spingere le banche a migliorare i propri servizi e abbassare i costi attraverso la tecnologia [94]. Un effetto sul settore potrebbe anche consistere in una spinta verso l'*unbundling* anche da parte delle banche ("*bank-as-platform*") [95].

Tuttavia, la normativa è risultata desueta ancora prima della sua entrata in vigore. Infatti, nel frattempo è mutato il mercato dei pagamenti e nel settore si è assistito all'ingresso dei colossi tecnologici (*Big Tech*) i quali

---

[91] L'art. 32, par. 3, *PSD2* proibisce alle banche che predispongano specifici API per interagire con i *TPP* di creare ostacoli alla fornitura dei servizi da parte di questi. L'EBA ha recentemente specificato quali tra le pratiche attuate dalle banche e istituti di pagamento europei possa considerarsi ostacolo (v. su re-indirizzamento per l'autenticazione, verifica del consenso, pre-registrazione e altre condizioni che vadano oltre le condizioni richieste dai *RTS* per garantire la sicurezza e tutela dei dati): EBA, *Opinion on obstacles under Article 32(3) of the RTS on SCA and CSC*, (4 giugno 2020) EBA/OP/2020/10.

[92] EBA, *Opinion on the implementation of the RTS on SCA and CSC,* (13 June 2018) EBA-Op-2018-04. Si veda anche l'istituzione dell'*EBA working group on APIs under PSD2*, che pubblica periodicamente chiarimenti: https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/eba-working-group-on-apis-under-psd2.

[93] O. BORGOGNO, G. COLANGELO, *Data, Innovation and Competition in Finance: The Case of the Access to Account Rule*, in corso di pubblicazione in *European Business Law Review* 2020, disponibile su SSRN, https://ssrn.com/abstract=3251584; GRAEF *et al.*, *Spill-overs*, cit., 12; RABITTI, SCIARRONE ALIBRANDI, *op. cit*., pp. 52-53.

[94] V. DOMBROVSKIS, *Payment services: Consumers to benefit from cheaper, safer and more innovative electronic payments*, (2018), http://europa.eu/rapid/press-release_IP-18-141_en.htm; A. BRENER, *Payment Service Directive II and Its Implications*, in T. LYNN *et al.*, *Disrupting Finance. FinTech and Strategy in the 21st Century*, Springer, Cham, 2019, p. 104.

[95] D. GAMMALDI, C. IACOMINI, *Mutamenti del mercato dopo la PSD2*, in MAIMERI, MANCINI, *op. cit.*, p. 140; cfr. anche EUROPEAN FINANCIAL MANAGEMENT & MARKETING ASSOCIATION (EFMA), *Building the bank of the future* (maggio 2019): "'*Bank as a Platform': the bank maintains the privileged relationship it has with its customers and enriches its value proposition by using services from other players"; "'Bank as a Service': the bank offers its value-added services to other players with the aim of increasing the flows and amortizing its IT investments at the risk of losing the relationship with its customers*".

hanno finito per avere il monopolio su nuovi dati di carattere disparato (quali informazioni tratte dai *social media,* dati di acquisto per l'*e-commerce*, invece che solo dati sui conti), oltre che spiccate capacità tecnologiche di elaborare tale mole di dati non strutturati, *customer base* estesa e risorse finanziarie considerevoli [96], ed essere allo stesso tempo invece liberi dagli stringenti obblighi normativi delle banche. Le *Big tech* hanno inoltre sviluppato la strategia del "*one stop shop*", fornendo perciò ai propri clienti la possibilità di accedere attraverso la medesima piattaforma a più servizi *across-industries* anche forniti da operatori diversi e perciò un servizio completo (disincentivando la ricerca degli stessi servizi altrove) [97]. Un effetto indesiderato dell'*open banking* potrebbe quindi essere quello di portare ulteriore concentrazione nel settore a favore delle *big tech* e a discapito delle banche, le quali devono aprire il proprio patrimonio informativo in maniera unilaterale, senza poter beneficiare dell'accesso alla mole di dati dei *competitor*, con inevitabili effetti anche dal punto di vista del rischio sistemico [98]. Il mercato si sta per la verità orientando verso varie forme di collaborazione tra banche e *Big tech* in forza della necessità delle prime di puntare maggiormente sulla tecnologia nell'offerta dei propri servizi e, dall'al-

---

[96] European Securities and Markets Authority (ESMA), *Report on Trends, Risks and Vulnerabilities*, n. 1/2020 (19 febbraio 2020), p. 48 ss., https://www.esma.europa.eu/sites/default/files/library/esma_50-165-1040_trv_no.1_2020.pdf. Cfr. D.A. ZETZSCHE, R. BUCKLEY, D. ARNER, J. BARBERIS, *From FinTech to TechFin: the regulatory challenges of data-driven finance*, in *NYU Journal of Law and Business* 2018, 14, 101; J. FROST, L. GAMBACORTA, Y. HUANG, H.S. SHIN, *Big tech and the changing structure of financial intermediation*, BIS Working Paper 779/2019, https://www.bis.org/publ/work779.pdf; D. BEAU, *Financial regulation and supervision issues raised by the impact of Tech firms on financial services*, Speech at the ESSEC – Centre d'excellence, Paris, 30 January 2019, https://www.bis.org/review/r190130a.pdf; A. CARSTENS, *Big tech in finance and new challenges for public policy*, speech at the FT Banking Summit (London, 4 December 2018), https://www.bis.org/speeches/sp181205.pdf; A. TANDA e C. SCHENA, C., *FinTech, BigTech and Banks: Digitalisation and its impact on banking business models*, (Palgrave MacMillan, 2019); F. BASSAN, *Potere dell'algoritmo e resistenza dei mercati,* (Rubettino, 2019).

[97] M. MAGGIOLINO, M. SCOPSI, *La prospettiva antitrust sulle big data companies e i servizi finanziari*, in FINOCCHIARO, FALCE, *op. cit.*, pp. 187-192.

[98] Expert Group on Regulatory Obstacles to Financial Innovation (ROFIEG), *30 Recommendations on Regulation, Innovation and Finance – Final Report to the European Commission*, (December 2019), p. 47 ss., 84 ss., https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/191113-report-expert-group-regulatory-obstacles-financial-innovation_en.pdf; Financial Stability Board (FSB), *FinTech and market structure in financial services. Market developments and potential financial stability implications*, (14 February 2019), https://www.fsb.org/wp-content/uploads/P140219.pdf; F. DI PORTO, G. GHIDINI, *"I Access Your Data, You Access Mine": Requiring Data Reciprocity in Payment Services*, in *IIC*, 2020, 51, 307, p. 323 ss.; D.A. ZETZSCHE, D. ARNER, R. BUCKLEY, R. WEBER, *The EU's Future of Data-driven Finance*, in *Comm. Market L. Rev.*, 2020, 57, 2, p. 331.

tra parte, dell'esperienza e posizionamento sul mercato delle seconde. Tuttavia, in tali *business partnership*, si registra un ribaltamento del potere contrattuale e di controllo a favore delle società tecnologiche che forniscono servizi di supporto alle prime (infrastrutture tecnologiche, *cloud*, ecc.) anche a causa della forte concentrazione del settore tecnologico, per cui anche i principi in materia di *outsourcing* elaborati anche recentemente nel settore bancario risultano desueti [99].

## 3.2. Gli obblighi dei soggetti coinvolti ed il difficile rapporto tra *PSD2* e *GDPR*

I dati personali dei clienti acquisiti nell'ambito dei servizi di pagamento devono essere trattati nel rispetto della normativa sui dati personali (ora *GDPR*), e quindi dei relativi obblighi di sicurezza informatica, base legale e principi di minimizzazione, proporzionalità, ecc. (consideranda 89 e 93; art. 94, par. 1, *PSD2*), la PSD2 specifica che il *PISP* (oltre a non poter detenere fondi dei clienti – fattore che giustifica una normativa più "leggera" rispetto agli istituti di pagamento) deve assicurare che le credenziali personali del pagatore non siano accessibili ad altri al di fuori del pagatore stesso e che comunque ogni altra informazione sul pagatore è fornita solo al beneficiario dell'operazione e col consenso esplicito del pagatore stesso. Il *PISP* non deve richiedere dati diversi da quelli necessari per eseguire il servizio in questione, non può accedere a, usare o conservare i dati per finalità diverse dalla prestazione del servizio in questione (secondo un modello più restrittivo dunque rispetto portabilità *ex* art. 20 *GDPR*) e comunque non può conservare dati sensibili (quali credenziali di accesso o altri suscettibili di permettere frodi accessi non autorizzati) relativi ai pagamenti del pagatore (art. 5-*ter*, comma 2, lett. e, d.lgs.

[99] ROFIEG, cit., p. 45 ss. (dove si parla di "*reverse outsourcing*"); FSB, *Third-party dependencies in cloud services. Considerations on financial stability implications*, (dicembre 2019), https://www.fsb.org/wp-content/uploads/P091219-2.pdf. Cfr. EBA, *Guidelines on outsourcing arrangements* (2019), https://eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf; BCBS, *Report on open banking*, cit., p. 7; High Level Forum on the Capital Markets Union (HLFCMU), *A New Vision for Europe's Capital Market Union – Final Report*, (giugno 2020), pp. 82 ss. https://ec.europa.eu/info/sites/info/files/business_economy_euro/growth_and_investment/documents/200610-cmu-high-level-forum-final-report_en.pdf; H.S. Scott, J. Gulliver, H. Nadler, *Cloud Computing in the Financial Sector: A Global Perspective*, (2019), https://www.pifsinternational.org/wp-content/uploads/2019/07/Cloud-Computing-in-the-Financial-Sector_Global-Perspective-Final_July-2019.pdf.

n. 11/2010 come modificato dal d.lgs. n. 218/2017; cfr. anche art. 66 *PSD2*). Similmente, l'*AISP* deve proteggere le credenziali dell'utente, accedere soltanto alle informazioni sui conti di pagamento designati e sulle operazioni di pagamento effettuate a valere su tali conti, senza neppure richiedere dati sensibili relativi ai pagamenti (a differenza del *PISP*), e non accedere a, usare o conservare dati per fini diversi dalla prestazione del servizio di informazione sui conti, sempre nel rispetto delle norme sulla protezione dei dati (art. 5-*quater* d.lgs. 11/2010 e art. 67 *PSD2*). Come si è visto, la nozione di tale servizio è piuttosto ampia e l'*European Data Protection Board* (istituito dall'art. 70 *GDPR* e che ha sostituito il WP29 a partire dall'entrata in vigore del *GDPR*) propone ragionevolmente di interpretare tale norma come un obbligo dell'*AISP* di esplicitare in sede contrattuale le tipologie di servizi che verranno offerti sulla base di quei dati, così come di quali dati si renda necessario il trattamento per l'espletamento del servizio e, conseguentemente, ottenere il consenso informato, libero ed esplicito dall'utente [100] e impiegare filtri e altre misure tecniche per limitare l'acquisizione dei soli dati necessari [101]. L'uso successivo dei dati personali raccolti da parte di *PISP/AISP* per fini diversi è quindi vietato salvo che non possa trovare giustificazione nel *GDPR* e quindi sia legittimo perché fondato sul consenso libero dell'utente (non forzato dal timore di subire un danno; art. 6, par.4 *GDPR*) o sul diritto nazionale (ad esempio, derivi dall'obbligo di rispettare la disciplina antiriciclaggio) [102]. Qualora, inoltre, i servizi offerti dai *TTP* prevedessero forme di decisione automatica e profilazione [103] (anche con riferimento alle speciali categorie di dati, salve certe condizioni quali in consenso espresso), dovrebbero rispettarsi le condizioni fissate in via generale dagli artt. 12-22 *GDPR* e, quindi, gli utenti dovranno essere informati, in maniera concisa, chiara e facilmente accessibile, dell'esistenza di un processo di profilazione ed in merito alla logica utilizzata (senza compromissione dei diritti industriali o simili dell'operatore), all'importanza e alle conseguenze derivanti da tale trattamento per l'interessato e ai diritti degli utenti stessi di accesso ai dati utilizzati, di opporsi, e, in caso di decisione com-

[100] EDPB, *Guidelines 06/2020*, cit., p. 7-9 e (anche sul coordinamento con l'art. 94, par. 2, a proposito del consenso esplicito) 12-14.

[101] Ibidem, p. 19-20.

[102] Ibidem, p. 10

[103] Intesa come la valutazione di "determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica» (art. 4, par. 4, *GDPR*).

pletamente automatizzata che abbia conseguenze significative per il soggetto, di richiedere un intervento umano, di esporre le proprie ragioni e di rifiutare la decisione finale, ecc. [104].

Da parte loro, invece, i prestatori di servizi di radicamento del conto devono comunicare con i *TPP* in maniera sicura, fornire ai *PISP* tutte le informazioni disponibili sull'ordine di pagamento ed eseguire l'ordine senza discriminazione così come trattare le richieste di dati degli *AISP* senza discriminazioni. Inoltre, il prestatore di radicamento del conto può rifiutare l'accesso ai *TPP* solo ove abbia giustificate e comprovate ragioni connesse all'accesso fraudolento o non autorizzato al conto di pagamento da parte di tali soggetti (dovendo in tal caso informare l'utente, specificando i motivi del rifiuto, e darne immediata comunicazione alla Banca d'Italia) mentre deve sempre rifiutare senza indugio l'accesso qualora riceva dall'utente la re-voca del consenso alla prestazione di tali servizi (art. 6-*bis,* d.lgs. 11/2010) [105]. I rapporti tra *TPP* e prestatori di radicamento del conto non sembrano comunque destinati ad essere semplici, dal momento che possono instaurarsi anche in assenza di precedente rapporto contrattuale e la *PSD2* fissa solo alcuni principi generali in materia di riparto di responsabilità tra gli stessi a tutela dell'utente (cfr. art. 25-*bis*, d.lgs. n. 11/2010) [106].

La *PSD2*, perciò, ha reso possibile, anche in un momento antecedente al

---

[104] Cfr. WP29, *Guidelines on Automated individual decision-making*, cit.; EDPB, *Guidelines 06/2020*, cit. Su *GDPR* e profilazione nei servizi finanziari: F. FERRETTI, *Consumer access to capital in the age of Fintech and big data: The limits of EU law, in Maastricht Journal of European and Comparative Law,* 2018, 25, 476; F. MATTASSOGLIO, *Big data: impatto sui servizi finanziari e sulla tutela dei dati personali*, in M.T. PARACAMPO (a cura di), *Fintech: introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari,* (Giappichelli, 2017), pp. 65 ss.; ID., *Innovazione tecnologica e valutazione del merito creditizio. Verso un social credit system?,* (EDUCatt, 2018).

[105] L'EDPB specifica che il prestatore di radicamento del conto può usare un "*privacy dashboard*", cioè un sistema che permetta agevolmente al cliente di visualizzare a quali *TPP* ha concesso il consenso al trattamento dei dati e di revocarlo, pur non creando ostacoli ai servizi dei *TPP* e quindi permettendo ai *TPP*, ad esempio, di ri-ottenere il consenso dall'utente in un secondo momento: *Guidelines 06/2020*, cit., p. 22.

[106] Qualora l'ordine di pagamento sia stato disposto mediante *PISP*, il prestatore di radicamento del conto è tenuto a rimborsare l'utente in caso di operazione non eseguita o non correttamente eseguita e poi a rivalersi immediatamente (senza costituzione in mora) sul *PISP*; ad ogni modo, il *PISP*, una volta rimborsato il prestatore di radicamento del conto, qualora dimostri che l'ordine di pagamento «è stato ricevuto dal prestatore di servizi di pagamento di radicamento del conto del pagatore conformemente all'articolo 15 e che, nell'ambito delle competenze del medesimo prestatore di servizi di disposizione di ordine di pagamento, l'operazione di pagamento è stata autenticata, correttamente registrata e non ha subito le conseguenze di guasti tecnici o altri inconvenienti correlati alla mancata, inesatta o tardiva esecuzione dell'operazione di pagamento», avrà diritto alla restituzione delle somme.

*GDPR*, il passaggio di certi dati dalle banche a nuovi soggetti ma gli elementi di differenziazione tra l'*open banking* e l'art. 20 *GDPR* sono numerosi (e, conseguentemente, il coordinamento difficile). Solo per menzionare i più rilevanti e partendo dalla *ratio*, la *PSD2* ha una spiccata finalità di abbattimento dei tradizionali monopoli e di promozione del mercato interno (cfr. considerando 33) pur nel rispetto dei dati dei clienti, mentre il *GDPR* mira *in primis* a tutelare l'individuo con i suoi dati, benché, in via secondaria risponda all'esigenza di favorire la concorrenza. Il diverso ordine di prevalenza degli obbiettivi si riflette nella distinta base giuridica dei due strumenti: il primo art. 16 TFEU e art. 8 Carta dei diritti fondamentali dell'UE (in materia di diritto alla protezione dei dati personali), mentre il secondo art. 14 TFEU (misure di armonizzazione per l'integrazione del mercato interno) [107].

Ancora, a livello di ambito di applicazione, la *PSD2* copre i dati di pagamento, sia personali che non, e di qualunque tipo di utente, mentre il *GDPR* solo i dati personali e solo di persone fisiche. Inoltre, la *PSD2* comporta una trasmissione sempre diretta (tra operatori) dei dati e, più propriamente un accesso e condivisione continui ed in tempo reale degli stessi benché limitata alla finalità di fornire certi servizi complementari, mentre il *GDPR* riguarda la realizzazione di una copia dei dati e relativo trasferimento tra operatore e cliente o direttamente tra operatori, solo in un certo momento, ma senza particolari restrizioni sull'uso dei dati e finalità di trattamento. In particolare, il titolare del trattamento potrebbe anche rifiutare *ex* art. 12, par. 5, una richiesta così frequente da assurgere ad accesso continuo in quanto richiesta eccessiva e ripetitiva, salvo che non prevalga l'interpretazione estremamente restrittiva del WP29 (cfr. *supra*). La differenza tra le due discipline in commento a tal riguardo influisce anche sulle potenzialità ed effetto di tali diversi diritti sul mercato: mentre l'*open banking* della *PSD2* facilita l'offerta dei soli servizi complementari elencati e per far ciò fornisce un accesso continuo, il *GDPR* aumenta la concorrenza per vari servizi sia complementari che sostitutivi ma che non richiedano un flusso continuo di dati tra il primo operatore ed in secondo [108].

Inoltre, le due normative sembrano usare in modo diverso alcuni termi-

---

[107] Cfr. I. GRAEF, M. HUSOVEC, J. VAN DEN BOOM, *Spill-Overs in Data Governance: Uncovering the Uneasy Relationship. Between the GDPR's Right to Data Portability and EU Sector-Specific Data Access Regimes*, in *EuCML* 2020, 1, 3, in particolare p. 5. Cfr. anche WOLTERS, JACOBSB, *The security*, cit. (che ritengono che la *PSD2* affidi ai singoli operatori l'equilibrio tra concorrenza e sicurezza e privacy, facendo sì che, a seconda delle dinamiche di mercato, i diritti degli utenti possano trovarsi sacrificati per far prevalere le logiche della concorrenza).

[108] Cfr. EDPB, *Guidelines 06/2020*, cit., pp. 12-14.

ni rilevanti: ad esempio, la prima sembra riferirsi con "dati sensibili" solo a quei dati di pagamento suscettibili di provocare frodi, mentre, la seconda, alle informazioni su caratteristiche etniche, opinioni politiche, orientamento sessuale, ecc.; disarmonie esistono similmente anche con riferimento al significato del termine "consenso esplicito" [109].

A proposito del difficile raccordo tra il *GDPR* e la *PSD2*, il WP29 ha ritenuto che l'art. 36 *PSD2* costituisca *lex specialis* rispetto all'art. 20 *GDPR* e quindi, quando l'utente avanzi una richiesta di portabilità, si debba interpretare come presentata ai sensi della *PSD2* qualora i dati riguardino l'*history payment account* del cliente [110]. Più recentemente, l'*European Data Protection Board* ha chiarito alcuni elementi di raccordo tra le due normative [111]: in particolare, ha specificato che il *TPP* può legittimamente trattare i dati personali di chi non abbia espressamente dato il suo consenso ("parte silente"), in forza del legittimo interesse del titolare del trattamento di eseguire un contratto (art. 6, par. 1, f) *GDPR*), sempre che tale trattamento sia strettamente necessario al fornitura del servizio e siano rispettati i principi di minimizzazione dei dati (con filtri per escludere dati non necessari), proporzionalità e rispetto della finalità per cui i dati sono stati raccolti e che non vengano lesi diritti o libertà fondamentali di terzi soggetti. A tal fine, si richiede ai tutti i titolari del trattamento coinvolti di predisporre misure tecniche per impedire che siano trattati dati delle silent party per fini diversi da quelli per i quali erano stati raccolti (quindi è escluso il "further processing" non potendosi peraltro ottenere il consenso dei terzi) o encryption o simili per minimizzare i dati dei terzi e garantire la sicurezza degli stessi (ad esempio, escludendo l'identità e IBAN di questi) [112].

Indicazioni vengono date anche in merito al trattamento di dati appartenenti alle categorie speciali di dati "sensibili" *ex* art. 9, par. 1 *GDPR* (cioè riguardanti l'etnia, orientamenti politici, religiosi, sessuali, salute, ecc.) nell'ambito della prestazione dei servizi di pagamento offerti dai *TPP* (ad

---

[109] Ibidem, pp. 12 ss.; EUROPEAN DATA PROTECTION BOARD (EDPB), *Letter of the 5th July 2018*, https://edpb.europa.eu/sites/edpb/files/files/news/psd2_letter_en.pdf; WP29, *Guidelines*, cit., p. 8 (nota 15); Rabitti, Sciarrone Alibrandi, cit., p. 59;.

[110] WP29, *Guidelines*, 8-9. Cfr. anche DI PORTO, GHIDINI, *op. cit.*, p. 311 ss. Sulla difficoltà di conciliare *GDPR* e *PSD2*: C. Sertoli, *PSD2, sicurezza e privacy*, in FINOCCHIARO, FALCE, *Fintech*, cit., p. 160, in particolare p. 169 ss. (che sottolinea come la *PSD2* richieda il consenso esplicito del cliente sempre mentre il *GDPR* ammette altre basi legali e richiede il consenso esplicito solo in presenza di dati sensibili).

[111] EDPB, *Letter of the 5th July 2018*, cit.; EDPB, *Guidelines 06/2020*, cit.

[112] Anche in considerazione dei limiti al trattamento dei dati da parte dei TPP contenuti nel considerando 87 e artt. 66, par. 3, lett. *g*) e 67, par. 2, lett. *f*) *PSD2*; EDPB, *Guidelines 06/2020*, cit., pp. 15-16, 19-20.

esempio, derivanti da informazioni su donazioni a certe organizzazioni o certi acquisti): se non si può giustificare suddetto trattamento sulla base del consenso esplicito o interesse pubblico, dovranno essere adottate soluzioni tecniche per impedire il trattamento di certe informazioni e quindi selezionare i dati.

## 4. Libero flusso di dati e altre forme di portabilità: dati non personali e dati pubblici

Come anticipato, la strategia europea dei dati mira a creare uno spazio unico dei dati e completare, insieme alle suesposte discipline della *GDPR* e *PSD2*, la nuova quinta libertà europea: la libera circolazione dei dati.

A tal fine, la Commissione ha adottato o intende adottare (v. il *Data Act* entro il 2021) una serie di normative, settoriali e non, che mirano, al contrario del *GDPR*, primariamente a formare un mercato europeo dei dati, benché ovviamente assicurando il rispetto della tutela dei dati personali [113], incentivando la circolazione e riuso (piuttosto che il trasferimento degli stessi) dei dati (quali sul traffico, ritardo dei treni, foreste, ecc.) raccolti dal settore privato (attraverso sistemi di intelligenza artificiale, *Internet of Things*, ecc.) con il settore pubblico [114] e tra privati (*business-to-business*) [115], anche al fine

[113] Benché appartengano a settori diversi (non finanziari), si segnalano anche la direttiva del 5 giugno 2019, 2019/944 relativa a norme comuni per il mercato interno dell'energia elettrica e che modifica la direttiva 2012/27/UE (che, in caso di installazione di sistemi di misurazione intelligenti, all'art. 20 riconosce il diritto dei consumatori di accedere a e visualizzare facilmente, in modo sicuro e gratuitamente, i dati – anche personali – sui consumi storici convalidati e quelli in tempo reale attraverso un'interfaccia standardizzata o accesso a distanza, così come di comunicarli a terzi per ricevere offerte comparabili) e regolamento (UE) del 30 maggio 2018, 2018/858 relativo all'omologazione e alla vigilanza del mercato dei veicoli a motore e dei loro rimorchi, nonché dei sistemi, dei componenti e delle entità tecniche indipendenti destinati a tali veicoli, che modifica i regolamenti (CE) n. 715/2007 e (CE) n. 595/2009 e abroga la direttiva 2007/46/CE (che copre i dati non personali richiesti per effettuare servizi di riparazione e manutenzione).

[114] HIGH-LEVEL EXPERT GROUP ON BUSINESS-TO-GOVERNMENT DATA SHARING, *Towards a European strategy on business-to-government data sharing for the public interest – Final Report*, (2020), https://ec.europa.eu/digital-single-market/en/news/experts-say-privately-held-data-available-european-union-should-be-used-better-and-more.

[115] COMMISSIONE EUROPEA, *Verso uno spazio comune europeo dei dati,* (Comunicazione) COM(2018) 232 final; ID., *Documento di lavoro dei servizi della Commissione – Orientamenti sulla condivisione dei dati del settore privato nell'economia europea dei dati che accompagna il documento Comunicazione della Commissione "Verso uno spazio comune europeo dei dati"*, SWD(2018) 125 final. Cfr. anche https://ec.europa.eu/digital-single-market/en/guidance-private-sector-data-sharing#Business-to-business.

di migliorare, rispettivamente, la risposta dei governi a diverse problematiche (anche alle pandemie) e la concorrenza e qualità dei servizi [116].

Il nuovo Regolamento in materia di dati non personali [117] introduce la portabilità dei dati non personali *business-to-business* (art. 6) *cross-sectoral* (come il *GDPR* per i dati personali), area prima non coperta da alcuna normativa e che possono risultare utili anche nel settore finanziario per finalità statistiche e analisi di mercato. Tuttavia, in questo caso il Regolamento, per facilitare il trasferimento dei dati, si affida a codici volontari di condotta di settore invece che all'imposizione di diritti/obblighi [118]. Inoltre, anche stante l'ampiezza del concetto di dato personale sopra esposta, non è facile identificare a quali dati si applicherebbe (dati anonimizzati, aggregati) [119] e, in caso di dati anonimi (tra i pochi sicuramente non personali), il soggetto da considerare titolare dei dati. Inoltre, la portabilità dei dati è affidata a codici di autodisciplina da adottarsi fatto che rende più difficile l'esercizio del diritto (insieme all'assenza di standardizzazione e di API, ecc.) [120]. Inoltre, spesso i dati sono misti e, se divisibili, risulterebbe difficile l'applicazione di due regimi separati o, se indivisibili, l'applicazione del solo *GDPR* (come invece richiesto dall'art. 2, par. 2) [121].

---

[116] Per uno studio sugli ostacoli alla libera circolazione dei dati in Europa: M. BARBERO et al., *Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability – Final Report*, (2018), European Commission – DG COONECT, https://ec.europa.eu/digital-single-market/en/news/study-emerging-issues-data-ownership-interoperability-re-usability-and-access-data-and.

[117] Regolamento relativo alla libera circolazione dei dati non personali nell'Unione europea n. 2018/1807/UE. Per un raffronto puntuale e critico di questi diritti rispetto a quelli trattati in questo lavoro, cfr. GRAEF *et al.*, *Spill-overs*, cit.

[118] Uno dei *Digital Single Market Cloud Stakeholders Working Group* (*Switching cloud service providers and Porting Data - SWIPO*) ha adottato a novembre 2019 la bozza di due codici di Condotta (uno per il mercato "*Infrastructure as a Service*" e uno per quello "*Software as a Service*") che la Commissione valuterà entro la fine del 2022: cfr. KRÄMER, SENELLART, DE STREEL, *Making Data Portability More Effective*, cit., p. 26.

[119] La Commissione ha recentemente esemplificato i dati non personali con i dati anonimizzati, inclusi i dati che sono aggregati sino a che i singoli eventi non siano più identificabili, i "dati del trading ad alta frequenza nel settore finanziario o i dati sull'agricoltura di precisione che aiutano a monitorare e a ottimizzare l'uso di pesticidi, nutrienti e acqua" e i dati di persone giuridiche (sempre che, ad esempio, il nome della persona giuridica non corrisponda a quello della persona fisica o le informazioni non si riferiscano ad una persona fisica): COMMISSION, *Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, (Communication) COM(2019) 250 final, pp. 7-8.

[120] In senso critico cfr. M.L. MONTAGNANI, *La libera circolazione dei dati al bivio. Tra tutela dei dati personali e promozione dell'intelligenza artificiale europea*, in *Mercato Concorrenza Regole*, 2019, 2, 293; BORGOGNI, COLANGELO, *Data sharing*, cit., p. 7.

[121] MONTAGNANI, *La libera circolazione*, cit. La Commissione ha elaborato, ai sensi dell'art.

La recente direttiva EU 2019/770 sulla fornitura di contenuti e servizi digitali [122], al fine di migliorare il mercato interno e la protezione dei consumatori, oltre ad imporre ai fornitori certi obblighi in materia di conformità al contratto (con conseguenti rimedi a favore dei consumatori in caso di inadempimento) e recesso nei contratti a tempo indeterminato, include una norma sulla condivisione di dati tra fornitore del servizio e il consumatore (non quindi direttamente tra fornitori). In particolare, l'art. 16, par. 4, riconosce ai consumatori (quindi solo alle persone fisiche che agiscano per scopi estranei all'eventuale attività professionale o imprenditoriale) il diritto, solo al termine del rapporto contrattuale, di richiedere ed ottenere dal fornitore entro un tempo ragionevole, senza impedimenti ed in un formato di uso comune e leggibile da dispositivo automatico «*contenuti diversi dai dati personali, che sono stati forniti o creati dal consumatore durante l'utilizzo del contenuto digitale o del servizio digitale fornito dall'operatore economico*». Quest'ultimo, al contrario di quanto avviene in base al *GDPR* per i dati personali, deve da quel momento astenersi dall'utilizzare tali dati e contenuti forniti o creati dal consumatore nell'ambito dell'utilizzo del contenuto o servizio digitale (art. 16, par. 3), traducendosi quindi il diritto del consumatore in questione in un potere di esclusiva sui dati, che è stato quindi paragonato al diritto di proprietà [123]. Tuttavia, tale diritto non è assoluto in quanto il fornitore può continuare ad usare i dati/contenuti in questione qualora «*a) sia privo di utilità al di fuori del contesto del contenuto digitale o del servizio digitale fornito dall'operatore; b) si riferisca solamente all'attività del consumatore nell'utilizzo del contenuto digitale o del servizio digitale fornito dall'operatore; c) sia stato aggregato dall'operatore economico ad altri dati e non possa essere disaggregato o comunque non senza uno sforzo sproporzionato; d) sia stato generato congiuntamente dal consumatore e altre persone, e altri consumatori possano continuare a utilizzare il contenuto*». Tutto ciò deve inoltre avvenire nel rispetto delle norme del *GDPR* (cfr. art. 3, par. 8, che contiene una norma di prevalenza del *GDPR*,

8(3) del regolamento, una guida proprio sull'applicazione della direttiva in questione in rapporto con il *GDPR* e in presenza di dati personali e non personali insieme ma con indicazioni abbastanza intuitive e quindi non particolarmente illuminanti: COMMISSION, *Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union*, cit.

[122] Direttiva (UE) del 20 maggio 2019 n. 2019/770 relativa a determinati aspetti dei contratti di fornitura di contenuto digitale e di servizi digitali. Ai sensi dell'art. 2, per "contenuto digitale" s'intendono "i dati prodotti e forniti in formato digitale" e per "servizio digitale" "un servizio che consente al consumatore di creare, trasformare, archiviare i dati o di accedervi in formato digitale" oppure "un servizio che consente la condivisione di dati in formato digitale caricati o creati dal consumatore e da altri utenti di tale servizio o qualsiasi altra interazione con tali dati".

[123] GRAEF *et al.*, *Spill-overs*, cit., p. 8.

e art. 16, par. 2). Ad ogni modo, l'opinione degli interpreti è che tale normativa (perlomeno nella versione inizialmente proposta) presenti una logica distante dal *GDPR*, presupponendo che i dati possano considerarsi beni e siano concessi in cambio di contenuti o servizi digitali [124]. Inoltre, tale diritto, potendo attivarsi solo al termine del contratto, non facilita il *multihousing* né le prove con i nuovi operatori prima di interrompere il contratto con il precedente [125].

Infine, la direttiva "*Open data*" sul riuso (commerciale e non) dei dati nel settore pubblico (direttiva UE 2019/1024) favorisce il riuso e la condivisione, anche continua e *real time*, di dati e documenti (in formato scritto, audio, video, banche dati) in possesso di enti pubblici, oltre che di musei, biblioteche, enti di ricerca e organizzazioni finanziate con fondi pubblici (per esempio, centri metereologici). Nell'accogliere le richieste, che non potranno compromettere i diritti alla protezione dei dati personali e i diritti di *copyright* e privativa industriale di terzi, gli enti non potranno porre a carico dei richiedenti spese salvo i costi marginali per la riproduzione, messa a disposizione, divulgazione e anonimizzazione dei documenti. La direttiva rimette inoltre alla Commissione il compito di stilare una lista di *dataset* di elevato valore (ad esempio, dati geospaziali, metereologici, statistici, ecc.) da mettere a disposizione gratuitamente, in formato *machine readable* e da fornire attraverso API (art. 13). La finalità è ancora quella di favorire la concorrenza e l'accesso anche da parte di PMI di tali dati, evitando lo sfruttamento monopolistico degli stessi da parte di *first mover* più vicini alle amministrazioni pubbliche [126], e avrà potenzialmente effetti benefici su diversi settori, incluso quello finanziario [127].

---

[124] EUROPEAN DATA PROTECTION SUPERVISOR, *Opinion 4/2017 on the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content'* (14 March 2017) (che si opponeva alla precedente versione della direttiva la quale si riferiva alla concessione di dati, anche personali, come "controprestazione"); ID., European Data Protection Supervisor, *Opinion 8/2016*, cit., p. 6; GRAEF *et al.*, *Spill-overs*, cit., p. 5. La direttiva ora si applica, ai sensi dell'art. 3, par. 1, «a qualsiasi contratto in cui l'operatore economico fornisce, o si impegna a fornire, contenuto digitale o un servizio digitale al consumatore e il consumatore corrisponde un prezzo o si impegna a corrispondere un prezzo», e «nel caso in cui l'operatore economico fornisce o si impegna a fornire contenuto digitale o un servizio digitale al consumatore e il consumatore fornisce o si impegna a fornire dati personali all'operatore economico […]».

[125] Cfr. KRÄMER, SENELLART, DE STREEL, *Making Data Portability*, cit., p. 77.

[126] COMMISSIONE EUROPEA, *Verso uno spazio comune europeo dei dati,* (cit., pp. 5-6; BORGOGNI, COLANGELO, *Data sharing*, cit., p. 9.

[127] Per un'analisi degli effetti positivi in materia di finanza sostenibile: E. MACCHIAVELLO, M. SIRI, *Sustainable Finance and Fintech: Can Technology Contribute to Achieving Environmen-*

La strategia europea dei dati è perciò composta da una molteplicità di diritti e strumenti diversi, tra l'altro, per tipo (accesso *real time versus* portabilità *una tantum*), ampiezza (*cross-sectoral* o settoriale), tipologia di dati (personali o non; su pagamenti, dati in possesso di soggetti pubblici), finalità (libera o per solo certi servizi), condizioni (gratuità o spese ragionevoli; tempistiche) e soggetti coinvolti (trasferimenti diretti tra operatori o tra operatore e utente). È ancora presto per constatare le difficoltà applicative e sovrapposizioni problematiche di tali diversi diritti ma al momento gli strumenti offerti per coordinare le discipline in questioni sono scarsi, dandosi espressamente prevalenza solo alla tutela dei dati personali ai sensi del *GDPR*. Il WP29 ha semplicemente indicato la necessità, qualora il diritto europeo o nazionale prevedano altri diritti di portabilità o simili per specifici settori, di tenere in considerazione le condizioni fissate in tali normative specifiche anche nella soddisfazione della richiesta di portabilità presentata ai sensi del *GDPR*, valutando eventuali effetti sulla stessa. Qualora poi sia evidente che la richiesta sia stata presentata ai sensi della disciplina specifica, essa deve essere soddisfatta seguendo la relativa disciplina e non il *GDPR* [128].

Infine, la presenza di molteplici *framework* e la diversità tra gli stessi contribuisce anche ad indebolire l'effettività del diritto alla portabilità dell'utente, rendendo difficile per lo stesso comprendere come esercitarlo in concreto e rendersi vero detentore del potere sui propri dati, anche a beneficio della qualità dei prodotti conseguentemente offerti allo stesso.

## 5. Aspetti problematici di tale architettura e conclusioni

### 5.1. Nuova economia dei dati: questioni rimaste aperte

La nuova economia dei dati, in conclusione, mette a dura prova le tradizionali forme di regolazione. Inoltre, alcune difficoltà tecnico-pratiche rendono ancora non realizzato un vero e proprio controllo dell'individuo sui propri dati e lo scarso utilizzo del diritto alla portabilità dei dati contribuisce ad attestarlo. Ancora, il perseguimento di obiettivi, quali quelli di favorire la concorrenza e l'innovazione a beneficio degli utenti, perseguiti attraverso disposizioni normative che facilitano il flusso dei dati (esemplare

*tal Goals? A Preliminary Assessment of 'Green FinTech'*, European Banking Institute Working Paper Series 71/2020, https://ssrn.com/abstract=3672989.

[128] WP29, *Guidelines*, cit., pp. 7-8.

la disciplina sulla portabilità), finiscono in realtà per creare nuovi, apparentemente insanabili, conflitti tra i due interessi in gioco (concorrenza/innovazione).

Il primo dato che emerge è la presenza di molte diverse normative, non ben coordinate fra loro, che sicuramente attesta la difficoltà iniziale di regolare la nuova economia ed indubbiamente rende più difficoltoso raggiungere effettivamente gli obiettivi perseguiti (§4).

Inoltre, il diritto alla portabilità dei dati, pur essendo un elemento cardine ed emblematico della strategia europea dei dati, solleva anche alcuni rischi: ad esempio, esso contribuisce ad aumentare anche il *cyber-risk*, particolarmente in combinazione con l'impiego di API (che facilita l'identificazione di *bugs* e altri difetti) [129], come dimostrato dal caso *Cambridge Analytics*, dove il *data breach* è stato reso possibile da un sistema di API mal congegnato [130]. Inoltre, potrebbe portare ad instaurare una *race to the bottom* tra operatori su tale profilo (minore livello di *data security* ma a prezzo inferiore: cfr. *supra* § 2.3) [131]. Il WP29 ha raccomandato al *data controller* di identificare i rischi collegati alla portabilità e prendere misure adeguate ma senza che ciò possa limitare il diritto dell'utente, pur rimanendo quindi il dover del primo titolare del trattamento di rifiutare il trasferimento in presenza di comprovate inadempienza al *GDPR* da parte del nuovo titolare (cfr. ancora § 2.3). Ad ogni modo, negli ultimi anni si sta dando un peso sempre maggiore alla *cyber-security*, specialmente nei settori rilevanti quali quello finanziario [132] e questo sforzo su più fronti potrebbe migliorare la situazione anche in ambito di diritto alla portabilità, sempre muovendolo verso forme di accesso *real time*.

Ancora, benché questa non sia la sede per approfondire il discorso, il diritto alla portabilità, sganciato com'è dai tipici presidi del diritto *anti-*

---

[129] Cfr. BCBS, *Report on open banking*, cit., p. 6; SCUDIERO, cit., p. 124 ss.; TROIANO, *Il diritto alla portabilità dei dati*, cit., p. 210-211; SWIRE, LAGOS, cit., p. 373; F. PIZZETTI, *Privacy e il diritto EUROPEO alla protezione dei dati personali*, cit., p. 289; BORGOGNO, COLANGELO, *Data sharing*, cit., p. 6; CIRAOLO, *I servizi di pagamento*, cit., pp. 230 ss.

[130] PRZEMYSŁAW POLAŃSKI, cit.

[131] SOMAINI, cit., p 177.

[132] OECD, *Digital security and resilience in critical infrastructure and essential services*, OECD Digital Economy Papers, No. 281 (April 2019), https://www.oecd-ilibrary.org/docserver/a7097901-en.pdf?expires=1604476535&id=id&accname=guest&checksum=6B1F99170C6E6A05CAA0FF75A87D8020; G. MUSCOLO, A. MASSOLO, *Data Driven Economy. Trade-off Between Competition and Cybersecurity*, in AGE 2019, 1, 189. Cfr. anche il recente Regolamento (EU) 2019/881 relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento *cybersecurity*»).

*trust*, potrebbe comunque avere effetti anti-competitivi non voluti [133]: applicandosi a tutti i titolari dei trattamenti indipendentemente dalla presenza di una posizione dominante e abuso o delle dimensioni dei titolari, comporta un peso comparativamente maggiore e quindi sproporzionato sulle imprese di piccole dimensioni, salvo che non si utilizzi il limite della fattibilità tecnica per smorzare tale peso (ancora § 2.3) [134].

Alcune scelte, inoltre, quale quella del *GDPR* e Regolamento sui dati non personali, di lasciare al mercato la ricerca di soluzioni in materia di interoperabilità e API, benché giustificata dalla volontà di non frenare l'innovazione e dalla difficoltà di fornire indicazioni che valgono per tutti i settori, potrebbe nella pratica ostacolare l'esercizio del diritto alla portabilità (§2). Anche recenti iniziative del mercato nella giusta direzione potrebbero non essere sufficienti: ad esempio, la piattaforma *open source* "*Data Transfer Project*" promossa da Apple, Facebook, Google, Microsoft e Twitter dal 2018 per facilitare la trasmissione fluida e frequente di dati da un operatore all'altro in alcuni casi non ha ancora realizzato gli adattamenti tecnici necessari per la fase di importazione dei dati dopo l'esportazione [135], lasciando quindi sospesa l'effettività dell'operazione e la realizzazione del diritto di portabilità. Non a caso in ambito settoriale (come avviene con la *PSD2*) si va verso l'interoperabilità [136] e potrebbe essere proprio l'azione combinata delle normative settoriali e dello sviluppo tecnologico a spingere il mercato verso soluzioni tecniche condivise, anche nell'ambito del generale diritto di portabilità, che potrebbe ve-

---

[133] In materia di diritto alla portabilità ed anti-trust: DIKER VANBERG, ÜNVER, *The right to data portability in the GDPR and EU competition law*, cit.; LYNSKEY, 'Aligning', cit.; BORGOGNO, COLANGELO, *Data sharing*, pp. 11 ss.; F. DIVETTA, Fintech fra dati e concentrazioni, in FINOCCHIARO, FALCE, cit., pp. 133 ss.; MAGGIOLINO, SCOPSI, cit.; M.R. PATTERSON, *Antitrust Law in the New Economy: Google, Yelp, LIBOR, and the Control of Information* (Harvard University Press, 2017); DI PORTO, GHIDINI cit.; B. VAN DER AUWERMEULEN, *How to attribute the right to data portability in Europe: A comparative analysis of legislations*, in *Computer Law & Security Review* 2017, 33, 57; MUSCOLO, MASSOLO, *Data Driven Economy, cit.*; CRÉMER et al., cit; S. VEZZOSO, *Fintech, Access to Data, and the Role of Competition Policy*, (January 22, 2018), in V. Bagnoli (ed.), *Competition and Innovation*, (Scortecci, São Paulo, 2018), disponibile su SSRN, https://ssrn.com/abstract=3106594.

[134] TROIANO, *Il diritto alla portabilità dei dati*, cit., pp. 207-208.

[135] KRÄMER, SENELLART, DE STREEL, *Making Data Portability More Effective*, cit., pp. 8, 47, 77.

[136] BORGOGNI, COLANGELO, *Data sharing*, cit., pp. 10-11, 13. Nell'ambito del settore della pubblica amministrazione, la Commissione da tempo promuove l'interoperabilità e neutralità tecnologica per favorire la portabilità: Commission, *New European Interoperability Framework Promoting seamless services and data flows for European public administrations*, (EU, Brussels, 2017), https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf.

nire influenzato (ed in parte esteso) proprio da tali discipline settoriali [137]. Recentemente, infatti, la Commissione sembra aver realizzato, nell'ambito della sua nuova strategia dei dati, l'importanza dell'interoperabilità anche fra settori, spingendo verso maggior omogeneità, almeno in alcuni settori strategici [138].

In secondo luogo, la mole di dati in possesso delle *big tech* e la pluralità di servizi offerti attraverso un'unica piattaforma producono un nuovo effetto di *lock-in* (cfr. anche § 1): i costi di *switching* rimangono o vengono percepiti come alti quanto maggiore è il volume di dati immessi, il numero di servizi connessi (e spesso gratuiti) forniti dalla prima piattaforma e grande il *network* (ad esempio, numero di contatti e *follower*), risultando improbabile ricreare la medesima situazione con il nuovo titolare del trattamento nel breve periodo [139]. Peraltro, è proprio il diritto alla portabilità ad incentivare i soggetti a fornire maggiori dati, nella consapevolezza di poterli agevolmente spostare ("*demand expansion effect*") [140]. Inoltre, non essendo portabili i dati rielaborati dalla piattaforma (cfr. § 2.2), un soggetto potrebbe essere disincentivato a cambiare operatore dal fatto di non voler perdere e ricostruire la propria "reputazione digitale" [141]. Similmente, nell'ambito dei *social network* ad esempio, non potendosi trasferire la propria "*social identity*" comprensiva di precedenti messaggi, contenuti condivisi e altre interazioni passate, così come continuare a comunicare con chi rimane nel precedente network (il che richiederebbe un'interoperabilità di protocollo e quindi standardizzazione massima), un utente ha scarsi incentivi a cambiare piattaforma se i suoi contatti non fanno altrettanto in blocco [142].

Strettamente connessa ai precedenti aspetti è anche la constatazione che, per rendere effettivamente possibile il *multi-housing*, non serve tanto un accesso *una tantum* ai dati e realizzabile nell'arco di un mese (come invece, si è visto, avviene ai sensi dell'art. 20 *GDPR*) ma un flusso continuo

---

[137] GRAEF *et al.*, *Spill-overs*, cit.

[138] COMMISSION, *A European strategy for data*, cit., pp. 8 ss.; Id., *The 2018 Rolling Plan For Ict Standardisation*, (2018), https://ec.europa.eu/digital-single-market/en/news/rolling-plan-ict-standardisation.

[139] BORGHI, cit., p. 241.

[140] WING MAN WYNNE LAM, XINGYI LIU, *Does data portability facilitate entry?*, in *International Journal of Industrial Organization* 2020, 69, 1.

[141] Ibidem.

[142] J. GANS, *Enhancing Competition with Data and Identity Portability*, (giugno 2018) Brookings Institute, https://www.brookings.edu/wp-content/uploads/2018/06/ES_THP_20180611_Gans.pdf. Cfr. anche KRÄMER, SENELLART, DE STREEL, *Making Data Portability More Effective*, cit., pp. 58-59.

di dati reso possibile da un eventuale futuro obbligo o incentivo all'interoperabilità sopra suggerito (*real time access* e *data interoperability*) [143].

Ad ogni modo, per bilanciare il peso economico e tecnico derivante dallo stesso, alcuni commentatori limiterebbero l'obbligo in questione alle imprese dominanti [144], così, appunto, anche da ridurre almeno in parte la suesposta nuova forma di *lock-in*. D'altra parte, l'obbligo di portabilità di per sé, ma in particolare se affiancato da più stringenti obblighi in termini di interoperabilità, potrebbe avere la capacità di ridurre gli incentivi all'innovazione, in un settore (mercati digitali) nel quale le imprese hanno tipicamente bisogno di esercitare un controllo esclusivo sui dati forniti dai propri consumatori e di mantenerli per sviluppare servizi innovativi con consistenti investimenti e raggiungere dimensioni di scala. Tuttavia, importante incentivo all'innovazione, si ripete, consisterebbe ancora nella concorrenza in ambito di rielaborazione dei dati (non coperta dal diritto alla portabilità che si limita ai dati forniti e osservati).

Ulteriori soluzioni tecniche potrebbero infine conferire realmente il potere agli utenti di decidere sui propri dati al di là delle dichiarazioni di principio, rendendo più agevole l'esercizio consapevole del diritto di portabilità da parte degli utenti ed incentivandone l'impiego (finora, appunto, scarso). Ad esempio, la creazione di *dashboard* che sintetizzino i dati "portabili" e le autorizzazioni concesse, semplificando a dei click l'espressione della volontà di condivisione, di selezione dei dati e le relative condizioni, potrebbe risultare fondamentali [145].

## 5.2. La problematica di fondo: il *level-playing field*

Il nuovo assetto normativo, letto in combinazione con le previsioni della *PSD2*, sembra ad ogni modo porre gli operatori bancari in condizioni più sfavorevoli rispetto ai nuovi concorrenti e realizza quindi un *un-level playing field* (cfr. § 3.1).

Al di là, infatti, della finalità espressa di promuovere la concorrenza nel

---

[143] Cfr. anche KRÄMER, SENELLART, DE STREEL, *Making Data Portability More Effective*, cit., p. 79.

[144] CRÉMER, DE MONTJOYE E SCHWEITZER, *Competition Policy for the Digital Area*, cit., pp. 8-9, 81-82, 102. Cfr. anche J. FURMAN et al., *Unlocking digital competition - Report of the Digital Competition Expert Panel*, (March 2019), p. 68.

[145] Cfr. le soluzioni tecniche proposte da KRÄMER, SENELLART, DE STREEL, *Making Data Portability*, cit., p. 76.

settore dei pagamenti, una ragione inespressa (o una *unintended* eterogenesi dei fini) dell'*open banking* della *PSD2* potrebbe consistere nel contenere il peso del potere economico concentrato nelle banche. E rispondere al problema, ampiamente discusso in relazione alla crisi del decennio scorso, delle banche *too big to fail*. Curiosamente, però, invece che abbracciare la cultura del *break-up* (che ha caratterizzato parecchie svolte negli Stati Uniti) [146], la soluzione europea al problema è passata attraverso fusioni tra banche (con un aumento delle dimensioni di numerose banche e, quindi, andando in senso opposto) e, appunto, la sottrazione alle banche di un'attività riservata, al fine di alleggerirne il peso sull'economia. Il punto è che l'attività – la prestazione di servizi di pagamento –, non risulta particolarmente pericolosa, non essendo noto alcun dissesto bancario (perlomeno in Italia) derivato da falle nell'attività di pagamento, e che, sottraendo l'attività a basso rischio dalle banche, a queste ultime restano in dotazione quelle a più alto rischio.

La *PSD2*, quindi, al fine di assicurare una maggior concorrenza tra vecchi e nuovi operatori nei servizi di pagamento e ridurre il peso delle banche nel settore, erode la posizione di supremazia conoscitiva degli istituti di credito nei confronti della propria clientela, favorendo l'interoperabilità e consentendo la circolazione dei dati. Allo stesso tempo, in base al principio di minimizzazione e consenso per specifiche finalità, il *GDPR* riduce le possibilità per le istituzioni finanziarie di usare i dati raccolti dai clienti in altri settori, per altri servizi o prodotti. Inoltre, a causa della complessità tecnica della normativa (analisi di impatto, misure tecnologiche per la minimizzazione, ecc.), essa ha spinto le istituzioni a ricorrere alle *big tech* con conseguente concentrazione di potere nelle mani di queste che sono anche le potenziali beneficiarie e in senso univoco del diritto alla portabilità (cfr. § 3.1) [147]. I grandi operatori del digitale possono quindi acquisire in proprio i pagamenti (anziché triangolarli con carte di credito e, quindi, banche), emettere *e-money* con carte di debito e prepagate, gestire i loro sistemi di pagamento, oltre che arricchire il loro patrimonio già inestimabile di dati (che, a differenza delle banche, non devono condividere con nessuno) da vendere sul mercato e potranno diventare i nuovi, più temibili concorrenti delle banche tradizionali. L'aspetto paradossale è infatti che in

[146] Si pensi alla Standard Oil o a Ma Bell, in epoche differenti e sotto Presidenti di diverso segno politico. L'unico esempio italiano che viene alla mente è l'apertura del mercato elettrico con la costituzione delle Genco scorporate dall'Enel e cedute ma si trattava di proprietà pubblica e non privata, al contrario dei casi Statunitensi indicati.

[147] ZETZSCHE *et al.*, *Data drive*, cit.

questo caso l'*incumbent* non è il detentore del vero potere di mercato ma è anzi il soggetto apparentemente destinato a soccombere.

La posizione di debolezza degli operatori bancari è acuita dal ritardo innovativo rispetto ai nuovi *player* a causa di retaggi storico-tecnologici e rigidità dei *business model*[148]. Per operatori – come le banche – che hanno visto nel tempo ridurre sempre più l'area di attività oggetto di riserva a loro favore (quindi riduzione delle barriere all'entrata di origine regolatoria) e che non possono ampliare la propria gamma di servizi oltre certi limiti, questa disciplina può rappresentare un vero problema. Esse, infatti, svolgono un'attività riservata (e di contro hanno oggetto sociale a quella limitato), sono sottoposte a regole prudenziali che impongono precisi limiti al loro operare, non pochi costi di *compliance* e a costante vigilanza. La situazione si è poi aggravata dopo la crisi, che ha quasi azzerato la profittabilità di alcuni segmenti della tradizionale attività bancaria, e, appunto, con l'avvento delle piattaforme che consentono la disintermediazione bancaria. D'altra parte, una volta che il sistema bancario non svolge più da solo la funzione che giustificava il monopolio delle informazioni sulla clientela e condivide tali informazioni con gli oligopolisti dei *big data*, si rende necessario un ripensamento del sistema.

Tuttavia, non è d'altra parte agevole, come si è cercato di rappresentare in questo lavoro, trovare un equilibrio tra i diversi obiettivi in gioco, quali concorrenza, protezione dell'innovazione e dei diritti altrui (si pensi alla questione della non portabilità dei dati *inferred* e reputazione "*social*"; i diritti dei titolari di *database*, ecc.), così come dei diversi tipi di *competitor* (banche, operatori *fintech*, *big tech*).

Senza potersi addentrare sull'adeguatezza dei tradizionali meccanismi antitrust per sorvegliare questo fenomeno, sembra che si possa dire, in un certo senso, che uno dei pilastri tradizionali della regolazione antitrust (e cioè livellare il terreno di gioco) stia venendo meno: quantomeno perché non esiste una reciproca condivisione di informazioni da parte dei nuovi entranti nei confronti delle banche e soprattutto in considerazione del fatto che le banche non potrebbero utilizzare le eventuali informazioni fornite in quanto limitate nella loro attività allo svolgimento di attività finanziarie (o connesse o strumentali all'attività bancaria). Un ritorno perciò alle radici dell'antitrust in funzione di democrazia economica e non solo di efficienza dei mercati – che quindi ammette anche deroghe a tutela dei più

[148] Cfr. G. PITRUZZELLA, *Fintech e i nuovi scenari competitivi nel settore finanziario-creditizio assicurativo*, intervento al Convegno ABI (10 maggio 2018, Roma), https://www.startmag.it/wp-content/uploads/Relazione-Pitruzzella-su-Fintech-ABI-10-maggio.pdf.

deboli – e qualche contemperamento alla spinta verso l'innovazione aperta (peraltro meritoria in linea di principio verso la quale orienta la portabilità dei dati e l'obbligo di interoperabilità), potrebbe essere un utile spunto di riflessione, insieme ad un miglior coordinamento, come anticipato, con le normative in materia di banche dati e diritti industriali.

Alcune proposte avanzate dalla dottrina nel settore, quindi, per rispondere al nuovo monopolio e concentrazione nelle mani delle *big tech*, mirano a limitare l'accesso ai dati delle banche solo in presenza di posizione dominante di queste [149]. Altre subordinano l'accesso a dati in possesso delle banche a condizioni di reciprocità quando il richiedente sia una *big tech* o comunque un conglomerato tecnologico e, ovviamente, sempre in presenza del consenso cliente [150].

## 5.3. Ultimi sviluppi

In chiusura, è ancora opportuno notare come i regolatori europei abbiano recentemente iniziato a muovere i primi passi verso adeguate risposte a tali problematiche e, in particolare, ai nuovi rischi creati dall'ingresso delle *Big Tech* nel settore finanziario e dalla fornitura da parte di questi e delle piattaforme di servizi diversi '*across different economic sectors*' così come della necessità di garantire una tutela adeguata dei consumatori. Si è infatti di recente anche sottolineata la portata in termini di rischio prudenziale e sistemico delle *Big tech* nel settore finanziario: il rischio operativo in una linea di *business* (*data analytics*, *cloud service*, etc.) di questi colossi tecnologici può avere rilevanti riflessi su tutte le altre, compresa quella dei servizi finanziari [151].

---

[149] ZETZSCHE *et al.*, *op. cit.*

[150] DI PORTO, GHIDINI, *op. cit.*, p. 323 ss.

[151] COMMISSION, *Consultation on new digital finance strategy for Europe - FinTech action plan*, (2020), p. 15, https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/2020-digital-finance-strategy-consultation-document_en.pdf; ESMA, *Response to the European Commission's Consultation on a New Digital Finance Strategy for Europe*, (29 giugno 2020), 12 ss., https://www.esma.europa.eu/press-news/esma-news/esma-responds-european-commission-consultation-digital-finance-stragtegy; EBA, *Response to EC consultation on the digital finance strategy/action plan*, (26 giugno 2020), 14 ss., https://eba.europa.eu/sites/default/documents/files/document_library/About%20Us/Missions%20and%20tasks/Correspondence%20with%20EU%20institutions/2020/886668/EBA%20Response%20to%20EC%20DFS%20consultation%20260620.pdf (dove peraltro si sottolinea che la concorrenza nel settore finanziario è minacciata dal monopolio sui dati da parte di alcune grosse imprese).

Nell'ambito del *Digital Finance Package* (adottato a fine settembre 2020, quando il presente lavoro era stato già chiuso) [152], la Commissione ha annunciato una serie di misure che potrebbero avere un impatto significativo sulle problematiche descritte nel presente lavoro.

In primo luogo, si sta pensando di trasformare l'*open banking* in "*open finance*", estendendo cioè i servizi coperti da tale particolare forma di portabilità di dati anche ai servizi diversi da quelli di pagamento (quindi di deposito, investimento, assicurazione, ecc.), introducendo un nuovo *framework* normativo (entro metà 2022), in collegamento con la revisione della *PSD2* (entro il 2021), l'adozione dei *Digital Services and markets Acts* (entro fine 2020) [153] con revisione della Direttiva sul commercio elettronico e atti collegati e la Strategia Europea sui dati. Benché le caratteristiche di tale programma non siano ancora state specificate dalle istituzioni europee, se la Commissione seguisse le indicazioni dell'*High Level Forum on the Capital Markets Union* (HLFCMU) [154], esso dovrebbe estendersi ad informazioni anche non finanziarie (ad esempio, con rifermento a metadati sui *social network* e utenze) e garantire un *level-playing field* tra banche ed altri operatori, *big tech* incluse, così come tenere in considerazione i costi, eventuali diritti industriali e, ovviamente, la protezione dei dati personali. In caso contrario, l'*open finance* potrebbe ulteriormente peggiorare le problematiche da noi sopra descritte. Altre indicazioni provenienti dall'HLFCMU riguardano, per facilitare la portabilità e condivisione dei dati, l'adozione di standard comuni per il formato con cui trasmettere i dati e di un'unica API a livello europeo, livelli minimi di sicurezza informatica, insieme a chiari criteri di ripartizione della responsabilità tra diversi operatori coinvolti.

In secondo luogo, la Commissione intende rispondere ai suesposti rischi creati dalla frammentazione delle catene di valore dei servizi finanziari e dalle *Big tech* e società tecnologiche nel settore finanziario attraverso la revisione della normativa sui conglomerati finanziari, anche introducendo l'obbligo di *supervisory colleges* per certe catene di valore, la creazione di un *framework* autorizzativo e di vigilanza per i fornitori di servizi tecnici

---

[152] Per il *Digital Finance Package* cfr. https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en; per la *Comunicazione relativa a una strategia in materia di finanza digitale per l'UE*, COM(2020) 591 final (24 settembre 2020): https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52020DC0591&from=EN.

[153] Cfr. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12417-Digital-Services-Act-deepening-the-Internal-Market-and-clarifying-responsibilities-for-digital-services. In materia di *open finance* cfr. anche FCA, *Call for Input: Open finance*, cit.

[154] HLFCMU, *A New Vision for Europe*, cit., pp. 109-111.

(*ICT*) critici (v. *cloud service*) ed una normativa *cross-sectoral* per i servizi finanziari al fine di assicurare la resilienza operativa in tutto il settore finanziario e con riferimento a tutti gli operatori, anche *fintech* e *big tech* ("*DORA Proposal*") [155].

L'Unione Europea sembra quindi intenzionata a tenere il passo con i fulminei cambiamenti del mercato e le problematiche emergenti: solo nel corso di questo difficile 2020 e successivo 2021 saremo in grado di vedere se le risposte assunte saranno in grado di trovare un corretto (e complesso) bilanciamento tra le diverse esigenze coinvolte.

[155] Cfr. COMMISSION, *Proposal for a Regulation on digital operational resilience for the financial sector*, COM(2020) 595 final (24 settembre 2020), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0595. In materia di problematiche e regolazione *cross-sectoral* del settore finanziario, cfr. in questo volume, A. Sciarrone Alibrandi; V. COLAERT et al., *European Financial Regulation. Levelling the Cross-Sectoral Playing Field*, (Hart, 2019) e, in particolare, con riferimento al *fintech*, il contributo di E. MACCHIAVELLO, *FinTech Regulation from a Cross-Sectoral Perspective,* pp. 63 ss. Cfr. anche E. MACCHIAVELLO, *FinTech. Problematiche e spunti per una regolazione ottimale*, in *Mercato concorrenza e regole*, 2019, 3, 435.