Gatti S, 'Dalla portabilità alle "portabilità": l'evoluzione al plurale di un diritto (e concetto) chiave nella disciplina europea dei dati' (2025) special issue 2 EJPLT, 157-177.
DOI: https://doi.org/10.57230/ejplt25SIBSG

EJPLT
ISSN 2704-8012



Dalla portabilità alle "portabilità": l'evoluzione al plurale di un diritto (e concetto) chiave nella disciplina europea dei dati

From portability to "portabilities": the evolution in the plural of a key right (and concept) in European data law

STEFANO GATTI
Ricercatore (RTD-B) di Diritto privato
Università di Verona

Abstract
Il diritto alla portabilità dei dati personali è una delle principali novità del Reg. UE 2016/679, c.d. GDPR, dove è espressione di un punto di incontro tra una concezione evoluta della protezione dei dati, che mira a rafforzare il controllo dell'interessato, e l'esigenza di agevolarne la libera circolazione, anche allo scopo di incentivare la concorrenza e aumentare la tutela dei consumatori. La successiva legislazione europea, animata dall'obiettivo di costruire un efficiente mercato unico dei dati, trasforma il concetto che si cela dietro questo diritto in un pilastro fondamentale. Ne risulta, per un verso, che questo diritto viene potenziato o integrato, almeno in determinati ambiti e, per altro verso, che allo stesso si affiancano nuove situazioni soggettive che si sovrappongono alla portabilità, e che possono essere nella titolarità di soggetti diversi da coloro che rivestono la qualifica di "interessati" ai sensi del GDPR.

© The author(s) 2024, published by Suor Orsola Benincasa Università Editrice.
This contribution is licensed under a Creative Common Attribution 4.0 International Licence CC-BY-NC-ND, all the details on the license are available at: https://creativecommons.org/licenses/by-nc-nd/4.0/

Abstract
The right to personal data portability is one of the main novelties of the EU Reg. 2016/679, so called GDPR. In this Regulation, data portability acts as a meeting point between an advanced conception of data protection, which aims to strengthen the data subject's control over his or her own data, and the need to facilitate the free movement of data, also with the aim of boosting competition and increasing consumer protection. In subsequent European legislation aimed at creating an efficient single market for data, the concept underpinning the right to data portability becomes a key pillar. As a result, on the one hand, this right is strengthened or complemented, at least in certain areas; on the other hand, the right to data portability is joined by new overlapping subjective rights, which may be in the hands of parties other than GDPR "data subjects".

Keywords: portabilità dei dati; diritto alla portabilità; dati personali e non personali; protezione e circolazione dei dati personali.

Sommario: 1. Premessa. Le varie forme della portabilità e l'art. 20 GDPR come punto di osservazione della ricerca. – 2. Il diritto alla portabilità dei dati personali nel GDPR: un innovativo strumento di autodeterminazione dell'interessato… – 3. … il cui potenziale è frenato da numerose limitazioni di compromesso. – 4. La progressiva affermazione della portabilità come propellente della circolazione dei dati: il Regolamento europeo relativo ai dati non personali (c.d. Regolamento Free-flow), la Legge europea sulla governance dei dati (Data Governance Act) e la Legge europea sulla governance dei dati (Data Governance Act) e la Legge europea sui mercati digitali (Digital Markets Act). – 5. L'ulteriore evoluzione della portabilità nell'architettura dei più recenti interventi normativi dell'UE: la compiuta rottura degli argini soggettivi del diritto dell'interessato nella Legge europea sui dati (Data Act). – 6. La duplice veste della portabilità nel Regolamento sullo spazio europeo dei dati sanitari (European Health Data Space Act). – 7. Osservazioni conclusive. La declinazione al plurale della portabilità e la sua rilevanza al di fuori della disciplina dei dati.

1. Premessa. Le varie forme della portabilità e l'art. 20 GDPR come punto di osservazione della ricerca.

Questo lavoro riflette sullo sviluppo del concetto di portabilità dei dati nella magmatica disciplina europea ad essi dedicata, in tumultuosa espansione dall'emanazione del Regolamento europeo sulla protezione dei dati personali (Reg. UE 2016/679, d'ora in avanti abbreviato con l'acronimo inglese, invalso nella prassi, GDPR). Il dirompente diritto dell'interessato codificato nell'art. 20 GDPR offre un punto di osservazione privilegiato per seguire le traiettorie evolutive della portabilità anche negli atti normativi successivi, consentendo di misurare i traguardi di volta in volta raggiunti nel garantire il controllo e l'effettiva circolazione delle informazioni a chi, avendone la legittimazione, vi dà impulso. Lo stesso legislatore europeo suggerisce questa prospettiva allorché compara espressamente le disposizioni più recenti alla versione "base" della portabilità, che viene, al pari di altri diritti dell'interessato, "rafforzata" o "integrata". Allo stesso tempo, l'insistenza sull'obiettivo della circolazione dei

dati ha reso presto stretta, per la portabilità, la veste esclusiva di un diritto del data subject: il concetto corre infatti più veloce di questa forma, con l'emersione nella normativa di ulteriori strumenti che si sganciano dalla disciplina della protezione dei dati in senso stretto – presupponendo, allo stesso tempo, un non semplice coordinamento con essa Alla portabilità, come si vedrà, si collegano ora non solo il diritto previsto dall'art. 20 del Regolamento, ma anche prerogative che possono venire esercitate da soggetti diversi dai data subjects, e, più in generale, una condizione dei dati che li rende pronti alla circolazione[1].

2. Il diritto alla portabilità dei dati personali nel GDPR: un innovativo strumento di autodeterminazione dell'interessato…

Fin dalle prime indagini sulle novità introdotte dal GDPR, è stato messo in luce il carattere innovativo e polivalente del diritto dell'interessato alla portabilità dei dati personali[2]. Emancipandosi dal già noto diritto all'accesso (art. 15 GDPR), ancora inserito in una prospettiva che guarda con una certa cautela il trattamento dei dati, la portabilità (art. 20 GDPR) è espressione di una prospettiva dinamica, finalizzata a garantire all'interessato la gestione attiva e il riuso dei propri dati[3].

La polivalenza della portabilità è sottolineata dalla moltitudine delle *rationes* collegate a questo diritto: accanto a quella, basilare, di riequilibrare il rapporto tra titolare del trattamento ed interessato[4], rafforzando il controllo di quest'ultimo sui propri dati[5], anche per consentirgliene uno sfruttamento

[1] Sul carattere «*multi-faceted*» del concetto di portabilità, v. già R. JANAL, *Data Portability – A tale of Two Concepts*, in *Journal of Intellectual Property, Information Technology, and Electronic Commerce Law*, 2017, Vol. 8, 59 - 69. Segnala l'emersione e il consolidamento, nelle relazioni di mercato, del nuovo paradigma della 'condivisione dei dati' G. MARINO, *Accesso, portabilità e condivisione nella disciplina europea del mercato dei dati*, in AA. VV., *Persona e mercato nella società digitale*, a cura di G. GUZZARDI, Napoli, 2024, 53 ss.

[2] Per tutti, v. S. TROIANO, *Il diritto alla portabilità dei dati personali*, in AA. VV., *Persona e mercato dei dati. Riflessioni sul GDPR*, a cura di N. ZORZI GALGANO, Milano-Padova, 2019, 199 ss.; A. RICCI, *I diritti dell'interessato*, in AA. VV., *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018*, n. 101, a cura di G. FINOCCHIARO, Bologna, 2019, 219.

[3] E. BATTELLI, G. D'IPPOLITO, *Il diritto alla portabilità dei dati personali*, in AA. VV., *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice della Privacy*, a cura di E. TOSI, Milano, 2019, 193.

[4] GRUPPO DI LAVORO ARTICOLO 29 (WP29), *Linee guida sul diritto alla portabilità*, adottate il 13 dicembre 2016 e da ultimo riviste e adottate il 5 aprile 2017, 4. Consultabili online: https://ec.europa.eu/newsroom/article29/items/611233.

[5] Considerando 68 GDPR. Va comunque sottolineato che, nel quadro giuridico previgente, il complesso di diritti dell'interessato sui propri dati personali (artt. 12 ss. dir. 95/46/CE, attuati in Italia prima nell'art. 13 legge 31 dicembre 1996, n. 675, e infine trasfusi nell'art. 7 d.lgs. 196/2003, c.d. codice della *privacy*, oggi abrogato) già suggeriva un'impostazione non limitata alla tradizionale prospettiva difensiva nei confronti di ingerenze esterne, ma aperta all'idea di un controllo dell'interessato sulle informazioni personali e, di conseguenza, sull'identità rivelata al pubblico: v. E. BARGELLI, sub art. 7, in AA. VV., *La protezione dei dati personali. Commentario al D.Lgs. 30 giugno 2003, n. 196 («Codice della* privacy*»)*, a cura di C.M. BIANCA e F.D. BUSNELLI, I, Padova, 2007,134 ss., la quale ha evidenziato che tale controllo non sfociava in una logica proprietaria sui dati, quanto, piuttosto, nell'enfasi dell'autodeterminazione informativa della persona (che risponde pur sempre ad una logica di bilanciamento). Il diritto alla portabilità, rispetto a questo quadro, esalta «la *dimensione dinamica* del controllo, proiettando la protezione nella sfera della disponibilità dei dati da parte dello stesso interessato»: S. TROIANO, *op. cit.*, 199.

economico[6], sono state evidenziate le conseguenze positive sulla platea dei consumatori e, più in generale, degli utenti di servizi online. La portabilità elimina infatti un ostacolo di natura tecnica, che rende più difficoltoso cambiare fornitore di tali servizi, anche se l'offerta del concorrente è più conveniente (c.d. effetto lock-in) [7] . Al rafforzamento del consumatore (consumer empowering)[8] segue l'incentivo ad una competizione positiva tra imprese, in una duplice direzione: per un verso e in termini generali, la maggiore libertà di movimento degli utenti spinge i fornitori ad elevare gli standard qualitativi e la convenienza economica della propria offerta; per altro verso, e in termini più specifici, l'aspettativa maturata di godere di questa libertà induce le imprese a sviluppare o a reperire sul mercato tecnologie innovative per assicurare ai consumatori l'effettività di questo diritto[9].

Oltre ai vantaggi di natura economica, di immediata percezione, merita altresì sottolineare l'intimo collegamento con la sfera della personalità dell'interessato: il diritto alla portabilità, permettendo una circolazione fluida delle informazioni personali sotto il controllo dell'interessato, costituisce un potente mezzo nelle mani degli individui per costruire ed affermare la propria identità nell'ambiente digitale, superando le barriere fisiche dello spazio e del tempo[10]; essa contribuisce, inoltre, alla creazione di sistemi più efficienti di gestione dei propri dati personali, ciò che incrementa le possibilità di esercizio

[6] GARANTE EUROPEO DEI DATI PERSONALI (EDPS), *Meeting the challenges of big data. A call for transparency, user control, data protection by design and accountability*, Opinion 7/2015, 13. Consultabile online: https://www.edps.europa.eu/sites/default/files/publication/15-11-19_big_data_en.pdf.

[7] In merito all'effetto positivo della portabilità sui cc.dd. *switching costs* e, in particolare, di quelli «*data-induced*», v. J. KRÄMER, P. SENELLART, A. DE STREEL, *Making Data Portability more effective for the Digital Economy. Economic Implications and regulatory Challenges*, *Report*, Centre on Regulation in Europe (CERRE), 2020, 55 ss., nonché 272 ss., i quali sottolineano la limitata efficacia del diritto, per come congegnato nel GDPR, nei confronti delle situazioni di *lock-in* generate dal c.d. effetto network (ivi, 57: «Network effects arise whenever a consumer's value of a good or service depends on how many other consumers are using the same good or service»): per contrastare un tale effetto, la portabilità dovrebbe avere ad oggetto, più che singoli set di dati, l'identità dell'interessato *(identity portability*), che comprende i collegamenti (come "amici" o "follwers") che, attraverso il primo servizio, sono stati instaurati con altre persone.

[8] V. G. COLANGELO, M. MAGGIOLINO, *From fragile to smart consumers: shifting paradigm for the digital era*, in *Computer Law & Security Review*, 2019, Vol. 35, 173 - 181.

[9] Sulla valenza concorrenziale del diritto alla portabilità, v., tra i molti, E. BATTELLI, G. D'IPPOLITO, *op. cit.*, 187 ss., i quali (ivi, 217 ss.), sulla scorta di quanto già osservato dal WP 29, in esordio delle linee guida citate sopra alla nota 4 (ivi, 4), sottolineano che rimane ferma la natura del diritto, che appartiene non già alle logiche della concorrenza ma, specificamente, al diritto della protezione dei dati personali: l'impatto che, indiscutibilmente, questo nuovo strumento dell'interessato ha sul mercato disvelerebbe piuttosto un obiettivo di orientarne lo sviluppo (tecnologico) verso una dimensione «aperta e inclusiva del ruolo dell'utente/interessato».

[10] V. M. FENWICK, M. FERTIK, P. JURCYS, T. MINSSEN, *Data Portability Revisited. Toward the Human-Centric, AI-Driven Data Ecosystems of Tomorrow*, in *Vanderbilt Journal of Entertainment and Technology Law*, 2025, 373 ss. La portabilità si candida a divenire strumento di controllo dei propri dati anche in funzione di costruire e governare la propria identità digitale (sul cui dinamismo v. i riferimenti di M. TESCARO, *L'identità digitale e la profilazione dell'utente*, in AA. VV., *Manuale di diritto privato dell'informatica*, a cura di R. BOCCHINI, Napoli, 2023, 79 ss.; S. SICA, V. D'ANTONIO, I *diritti della personalità in rete*, ivi, 91 ss.). Per una riflessione sull'intima connessione tra la portabilità e la personalità dell'individuo, anche in un sistema, quello argentino, dove il corrispondente diritto non è stato codificato, v. A. LAJE, *El derecho a la portabilidad de datos como derecho personalìsimo*, in AA. VV., *Diritto privato e nuove tecnologie. Riflessioni incrociate tra esperienze giuridiche a confronto*, a cura di S. TROIANO, Napoli, 2022, 9 ss.

e di tutela dei propri diritti della personalità[11], ad esempio del diritto alla salute[12].

La portabilità concepita dal GDPR è, in sostanza, lo strumento congegnato per permettere alle persone fisiche di autodeterminarsi con riguardo ai propri dati[13] (e grazie ai propri dati[14]), sia sul piano patrimoniale sia su quello personale.

Secondo una logica di flessibilità che mira ad adeguarne l'attuazione a seconda del grado di avanzamento tecnologico dei vari settori di mercato, il diritto dell'interessato si snoda in due versioni. La prima, più elementare, consiste in due poteri che possono essere esercitati anche disgiuntamente dall'interessato: a) richiedere al titolare del trattamento di trasmettergli i dati a lui previamente «forniti» (purché trattati con mezzi automatizzati[15] sulla base del consenso oppure dell'esecuzione di un contratto di cui l'interessato è parte), in un formato con requisiti minimi di interoperabilità («formato strutturato, di uso comune e leggibile da dispositivo automatico»); b) trasmettere i dati ricevuti dal titolare del trattamento ad un diverso titolare del trattamento senza impedimenti da parte del primo (art. 20, par. 1, GDPR). La seconda forma di portabilità, più avanzata, riguarda le medesime categorie di dati e legittima l'interessato a richiedere il trasferimento diretto degli stessi da un titolare del trattamento ad un altro, ma è limitato a quei casi in cui una tale attività risulti «tecnicamente fattibile» (art. 20, par. 2, GDPR).

3. … il cui potenziale è frenato da numerose limitazioni di compromesso.

Nonostante la centralità di questo diritto nella costruzione di una dimensione antropocentrica dell'ambiente digitale[16], spiccano, già ad una piana lettura dell'attuale formulazione dell'art. 20 GDPR, specie se confrontata con

[11] Sulla portabilità si basano i Personal Information Management Systems (PIMSs), i quali, offrendo agli interessati un servizio di raccolta dei dati personali detenuti dai vari titolari del trattamento e di gestione degli stessi in una interfaccia unica, rappresentano un'occasione di (modesto) guadagno per gli interessati e agevolano l'esercizio dei diritti su quei dati (revoca del consenso, cancellazione, rettifica, e la stessa portabilità). L'attività di questi intermediari di dati è ora regolata dal Reg. UE 2022/868, relativo alla governance europea dei dati (su cui, per cenni, v. *infra*, par. 4).

[12] *Infra*, par. 6.

[13] Il diritto alla portabilità può essere dunque concepito come strumento che fissa uno standard ancora più elevato del diritto alla protezione dei dati personali (sulla cui autonomia come diritto della personalità, anche sul piano dei contenuti e della disciplina, nonostante l'indubbia valenza strumentale alla realizzazione di altri diritti e l'ottica di bilanciamento che lo stesso sovente impone, v. C.M. BIANCA, *Note introduttive*, in AA. VV., *La protezione dei dati personali*, cit., XX ss., nonché ID., *Diritto civile*, 1, *La norma giuridica. I soggetti*, Milano, 2002, 180). Come osserva S. TROIANO, *op. cit.*, 199ss., tuttavia, l'evoluzione della «proiezione positiva» della protezione dei dati personali impressa dalla portabilità svela la logica polifunzionale di tale strumento, tesa non solo ad enfatizzare l'autodeterminazione dell'individuo, ma anche a rafforzare «una visione patrimonialistica e obiettivizzata dei dati personali» e a concorrere alla «regolamentazione del mercato dei dati».

[14] V. D. COPETTI CRAVO, *How to Make Data Portability Right More Meaningful for Data Subjects*, in *European Data Protection Law Review*, 2022, Vol. 8, 53.

[15] Ancorché vi sia intervento umano: L.R. BIANCHI, *Il diritto alla portabilità dei dati*, in AA. VV., *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, a cura di R. PANETTA, Milano, 2019, 224.

[16] Sottolineano la dimensione *user-centric* della portabilità già P. DE HERT, V. PAPAKONSTANTINOU, G. MALGIERI, L. BESLAY, I. SANCHEZ, *The right to data portability in the GDPR: Towards user-centric interoperability of digital services*, in *Computer Law & Security Review*, 2018, Vol. 34, 193 - 203; v. anche considerando 3 del Reg. UE 2022/868 (DGA).

quella degli altri diritti dell'interessato, numerose limitazioni, frutto della soluzione di compromesso adottata, nel percorso legislativo, dalle istituzioni dell'Unione[17]. Queste limitazioni trovano in larga parte spiegazione, per un verso, in ostacoli di natura tecnica[18] e, per altro, nei possibili rischi nei quali possono incorrere, per effetto di questo diritto, i soggetti del trattamento. Senza perdere di vista la prospettiva dell'interessato[19], occorre prendere in considerazione anche quelle del titolare del trattamento e dei terzi. Il primo, oltre a sopportare l'onere economico della richiesta, corre principalmente il rischio di essere costretto a svelare informazioni, deducibili dai dati personali trasmessi, che si traducano in vantaggi competitivi per i concorrenti (dati lavorati e, grazie a questi, strategie di trattamento e di mercato)[20]. Gli altri vedono la propria posizione minacciata principalmente allorché i dati oggetto della richiesta dell'interessato comprendano informazioni che riguardano anche loro[21]. Tenendo conto di questo, l'art. 20 GDPR non solo indugia in alcune

[17] Come è noto, il diritto alla portabilità è, almeno nel campo della tutela dei dati personali, una novità introdotta dal GDPR: v. L. SCUDIERO, *Bringing Your Data Everywhere: A Legal Reading of The Right to Portability*, in *European Data Protection Law Review*, 2017, Vol. 3, 119. L'idea di fondo era però già nota: nel diritto europeo, almeno dalla dir. 2002/22/CE (c.d. direttiva servizio universale), che ha introdotto la portabilità del numero telefonico (cfr. S. TROIANO, *op. cit.*, 196 ss.; ma v. anche l'obbligo alla portabilità transfrontaliera di servizi di contenuti online di cui al Reg. UE 2017/1128); nelle prassi di alcune delle principali imprese del settore digitale, ad iniziare dai primi progetti di Google, descritti sinteticamente da F. CATALANO, *Il diritto alla portabilità dei dati tra interessi individuali e prospettiva concorrenziale*, in *Europa dir. priv.*, 2019, III, 837 ss. Suggerito da numerosi atti preparatori, il diritto alla portabilità era già previsto, seppure embrionalmente, nell'art. 18 della Proposta di GDPR della Commissione, COM (2012) 11 *final*. Nella formulazione finale, dopo il fallimento del tentativo di accorparla al diritto all'accesso, la portabilità è affermata come diritto autonomo ma è d'altra parte connotata dalle limitazioni che si esamineranno *infra*, nel testo. Scompare infine il ruolo della Commissione di specificare norme tecniche in relazione al formato in cui l'interessato ha diritto di ricevere i dati e neppure vi è più riferimento ai formati che devono essere accettati dal titolare del trattamento ricevente.

[18] Ciò non solo sul piano dell'interoperabilità (v. *infra*), ma anche dei costi che può implicare soddisfare le richieste di portabilità (ragione per cui, ad esempio, è previsto che il diritto si applichi solo allorché i dati siano trattati con mezzi automatizzati), in modo sicuro: v. E. BATTELLI, G. D'IPPOLITO, *op. cit.*, 199.

[19] Ad es., l'art. 20, par. 3, GDPR prevede esplicitamente che l'interessato non perde il diritto alla cancellazione dei dati: da questa previsione si è ricavato che l'esercizio di un diritto è indipendente dall'altro e si è altresì escluso che la portabilità abbia ripercussioni sul piano del rapporto contrattuale tra interessato e titolare del trattamento (considerando 68 GDPR).

[20] Con riguardo a questa seconda tipologia di rischio, si spiega la limitazione della portabilità ai dati «forniti» dall'interessato, dati grezzi (raw data), escludendo le ulteriori informazioni ricavate (dati inferiti o inferenziali, e dati previsti). Ancora, la portabilità non può pregiudicare i segreti industriali e la proprietà intellettuale del titolare del trattamento, a cui spetta la possibilità di valutare di non dare seguito alla richiesta dell'interessato che rechi pregiudizio ai propri diritti, fermo che – come precisato dal considerando 63 GDPR, in relazione al diritto all'accesso, ma con un discorso senz'altro estensibile alla portabilità – «tali considerazioni non dovrebbero condurre a un diniego a fornire all'interessato tutte le informazioni».

[21] Poiché i dati personali sono spesso caratterizzati da una «intrinseca complessità e relazionalità», la portabilità può riguardare informazioni che concernono più soggetti contemporaneamente e non sempre è possibile o ragionevole, rispetto alla finalità dell'interessato, epurare tali dati da ciò che riguarda persone diverse dal richiedente. Per questa ragione, la disposizione secondo cui il diritto alla portabilità «non deve ledere i diritti e le libertà altrui» (art. 20, par. 4, GDPR), pur perentoria nel contenuto, deve essere debitamente interpretata, se non si vuole svuotare completamente di significato la disposizione normativa. Il punto è stato approfondito dal WP29, secondo cui la trasmissione di dati può riguardare anche informazioni di terzi (ad esempio, contatti, fotografie e messaggi) nella misura in cui questa serva all'interessato per realizzare una finalità di natura personale (in sostanza, rispetto a questi dati l'interessato ha una posizione assimilabile a quella di un titolare del trattamento, per il quale tuttavia le regole dello stesso Regolamento non vengono in rilievo alla luce dell'eccezione di cui all'art. 2, par. 2, lett. c, c.d. household exception) e tali dati non siano utilizzati per finalità ulteriori dal titolare del trattamento a cui essi vengano trasmessi, per il quale, invece, la base giuridica utile all'impiego di tali dati può essere rinvenuta nel legittimo interesse (art. 6, lett. f], GDPR) di prestare l'attività in favore dell'interessato (WP29, *Linee guida sul diritto alla portabilità*, cit., 11 s.).

precisazioni in relazione ad eventuali conflitti tra la portabilità e gli altri diritti dell'interessato o di altri soggetti (art. 20, par. 3 e 4, GDPR), ma circoscrive, a monte, l'ambito di applicazione di questo diritto[22]. In particolare, come già si è accennato, l'interessato può esercitare le prerogative della portabilità esclusivamente con riguardo ai dati da lui «forniti» al titolare del trattamento e che questo tratta sulla base del consenso o dell'esecuzione di un contratto (ovvero di misure precontrattuali), ricorrendo a mezzi automatizzati. La palpabile tensione tra le finalità sottese a questo innovativo strumento e il quadro dei principi di fondo del regolamento (e del diritto della concorrenza), si traduce in alcune rilevanti insicurezze nell'interpretare l'articolato normativo e le soluzioni adottate nel tentativo di bilanciare le diverse istanze[23].

Dal punto di vista dell'effettività del diritto alla portabilità, il principale limite[24] è quello, di natura tecnica, consistente nella mancanza di una garanzia di interoperabilità dei dati tra i titolari del trattamento[25], elemento che, confrontato con l'attuale realtà tecnologica, non solo relega la dimensione più avanzata del diritto ad una dimensione eventuale (come si è detto, la

[22] L'inapplicabilità del diritto alla portabilità non esclude poi la possibilità di esercitare il diritto all'accesso: E. BATTELLI, G. IPPOLITO, *op. cit.*, 193.

[23] Come è noto e come risulta pianamente dal suo primo articolo, il GDPR intende proteggere i diritti delle persone fisiche (ad iniziare da quello alla protezione dei dati personali), ad un tempo incoraggiando una più fluida circolazione dei dati personali, condizione fondamentale per la creazione e lo sviluppo del mercato digitale. Questa duplice dimensione (o «anima»: N. ZORZI GALGANO, *Le due anime del GDPR e la tutela del diritto alla privacy*, in AA. VV, *Persona e mercato dei dati*, cit., 36 ss.) implica un bilanciamento tra esigenze difficilmente conciliabili, al punto che la portabilità, esprimendole entrambe, è congenitamente affetta da un inevitabile 'strabismo': così, efficacemente, S. TROIANO, *op cit.*, 207 ss. Emblematico è l'esempio dell'ampiezza della portabilità in base al significato del concetto di dati «forniti» dall'interessato: esclusi, come detto (*supra*, nota 20) i dati inferenziali (inferred data), rimane il problema se siano invece compresi i dati semplicemente 'osservati' grazie ad un dispositivo (ad es., lo smartwatch: observed data), o se vadano considerati oggetto della portabilità i soli dati attivamente forniti dall'interessato (volunteered data). L'interpretazione estensiva del WP29 (invero non accolta unanimemente, come osserva F. CATALANO, *op. cit.*, 844; in termini dubitativi anche S. TROIANO, *op. cit.*, 19 s.; in senso favorevole, si è però assestato l'orientamento dominante: E. BATTELLI, G. D'IPPOLITO, *op. cit.*, 195, che invero raccomandano sul punto una valutazione caso per caso; J. KRÄMER, *Personal data portability in the platform economy: economic implications and policy recommendations*, in *Journal of Competition Law & Technologies*, 2020, Vol. 17, 290, nelle conclusioni; A. DIX, *Sub art. 20*, in AA. VV., *General Data Protection Regulation. Article-by-Article Commentary*, a cura di I. SPIECKER GEN. DÖHMANN, V. PAPAKONSTANTINOU, G. HORNUNG, P. DE HERT, Baden-Baden-München-Oxford, 2023, 513) si giustifica certamente con l'intento di estendere la portata del diritto, ma un tale obiettivo non deve essere assolutizzato, se si tiene conto che ogni passo in quella direzione accentua una contraddizione col principio della minimizzazione dei dati (art. 5, par. 1, lett. c, GDPR) e eleva lo standard di mercato ad un livello che rischia di escludere piccole e medie imprese dal mercato digitale, concentrandolo, ancora di più, nelle mani delle grandi piattaforme digitali: cfr. R.H. WEBER, *Data Portability and Big Data Analitycs. New Competition Policy Challenges*, in *Concorrenza e Mercato*, 2016, 70; v. pure F. BRAVO, *Intermediazione di dati personali e servizi di* data sharing *dal GDPR al* Data Governance Act, in *Contratto e impresa Europa*, 2021, I, 225 ss.

[24] Frequentemente sottolineata è, per il vero, la scarsa dimestichezza degli interessati rispetto ad uno strumento non ancora noto e diffuso, e le cui potenzialità non sono immediatamente percepibili dai singoli: v., anche sull'importanza di sviluppare strumenti *user-friendly*, S. KUEBLER-WACHENDORFF *et al., The Right to Data Portability: conception, status quo, and future directions*, in *Informatik Spektrum*, Vol. 44, 2021, 266 ss.

[25] Come confermato dal considerando 68, il Regolamento non intende porre in capo ai titolari del trattamento un obbligo di adottare formati interoperabili (né, tantomeno, impone il risultato della perfetta compatibilità), limitandosi solamente a fissare criteri generali e di base (ossequiosi del principio di neutralità tecnologica: A. DIX, *op. cit.*, 514; v. considerando 15 GDPR) che, si auspica, consentano di rendere le informazioni trasmesse realmente utilizzabili dall'interessato e dal nuovo titolare del trattamento. Oltre a queste indicazioni di carattere generale, il GDPR non va oltre al semplice 'incoraggiamento' a che i titolari del trattamento sviluppino «formati interoperabili che consentano la portabilità dei dati».

trasmissione diretta può essere richiesta solo «se tecnicamente fattibile»)[26], ma getta altresì una pesante ombra sulla realizzazione degli obiettivi sottesi alla 'versione di base' del diritto (riutilizzare i dati già forniti ad un primo titolare trasmettendoli ad un secondo titolare), giacché, se il titolare del trattamento è obbligato a trasmettere all'interessato i dati che lo riguardano «in un formato strutturato, di uso comune e leggibile da dispositivo automatico»[27], l'ulteriore titolare del trattamento che riceve tali dati non è obbligato ad adottare misure tecniche che ne consentano l'immediata fruizione[28].

4. La progressiva affermazione della portabilità come propellente della circolazione dei dati: il Regolamento europeo relativo ai dati non personali (c.d. Regolamento Free-flow), la Legge europea sulla governance dei dati (Data Governance Act) e la Legge europea sui mercati digitali (Digital Markets Act).

Rispetto al quadro di partenza, sopra descritto per sommi capi, i successivi interventi del legislatore europeo si sono mossi, su più fronti, nella direzione del consolidamento[29] e di un deciso potenziamento della portabilità dei dati[30].

---

[26] Seppure si rinvenga l'opinione, segnalata da F. CATALANO, *op. cit.*, 862, che la norma avrebbe l'effetto di addossare al titolare del trattamento l'onere della prova della non fattibilità tecnica.

[27] Sullo spostamento del focus normativo dall'interoperabilità dei servizi a quello dei formati dei dati trasmessi, v. E. BATTELLI, G. D'IPPOLITO, *op. cit.*, 202 ss., che ne sottolineano i punti di forza, oltre che la evidente finalizzazione alla circolazione dei dati. Simmetriche preoccupazioni si sono affacciate nel dibattito: cfr. S. TROIANO, *op. cit.*, 209 ss., che porta alla luce come la predeterminazione dei formati e la facilitazione della circolazione dei dati attraverso la rimozione delle barriere tecniche aumentino le occasioni di violazione da parte di terzi e agevolino altresì comportamenti poco prudenti degli stessi interessati.

[28] L'interoperabilità è un pilastro tecnico senza il quale l'effettività del diritto non può essere garantita: v. F. CATALANO, *op. cit.*, 847 ss.; D. COPETTI CRAVO, *op. cit.*, 56 s. e, per una sintesi di alcune soluzioni tecniche, v. JOHANN KRANZ *et al.*, *Data portability*, in *Business & Information Systems Engineering*, Vol. 65, 2023, 601 ss. Per una recente analisi empirica sulla distanza tra l'auspicio del legislatore europeo e la realtà del mercato, v. S. KUEBLER-WACHENDORFF *et al., op. cit.*, 268 s., i quali, anche sulla base di questa ragione, discorrono di una «blunt sword».

[29] Il concetto di portabilità ha fatto il suo ingresso anche nella disciplina consumeristica. Nella dir. 770/2019/UE sui contratti di fornitura di contenuti e servizi digitali, in particolare, si prevede il diritto dei consumatori, che recedono dal contratto, alla portabilità, non solo dei dati personali (che, nel testo finale della direttiva, si risolve nel richiamo generale al GDPR, all'art. 16, par. 2, attuato dall'art. 135-*noviesdecies*, co. 3, cod. cons.: v. A. METZGER, Z. EFRONI, L. MISCHAU, J. METZGER, *Data-Related Aspects of the Digital Content Directive*, in *Journal of Intellectual Property, Information Technology, and Electronic Commerce Law*, 2018, Vol. 9, 102 s.; K. SEIN, G. SPLINDER, *The New Directive on Contracts for the Supply of Digital Content and Digital Services – Conformity Criteria, Remedies and Modifications – Part 2*, in *European Review of Contract Law*, 2019, Vol. 15, 381 ss.) ma anche dei 'contenuti digitali', ossia dati diversi da quelli personali generati dal consumatore nell'utilizzo del contenuto o del servizio digitale oggetto del contratto risolto (art. 16, parr. 4, dir., attuato dall'art. 135-*noviesdecies*, co. 5, c. cons.). Disposizioni simili sono contenute nella disciplina del recesso nei contratti a distanza e conclusi al di fuori dei locali commerciali, in base alla dir. 2011/83/UE, come emendata dalla dir. 2019/2161/UE, c.d. *omnibus* (art. 13, parr. 4 e 6, attuati dall'art. 56, co. 3-*bis* e 3-*quater*, c. cons.). Come è stato puntualmente osservato, però, da G. COLANGELO, M. MAGGIOLINO, *op. cit.*, 177, il diritto contemplato dalle direttive, almeno con riguardo ai dati non personali, non si estende sino a comprendere la portabilità diretta.

[30] Conformemente al chiaro indirizzo espresso nella Comunicazione della Commissione del 19 febbraio 2020, COM(2020) 66 final, *Una strategia europea per i dati*, 22. Il deciso cambio di passo dell'Unione, teso a favorire la circolazione, condivisione e riuso dei dati è sottolineato, tra gli altri, da D. POLETTI, *Il controllo dell'interessato e la strategia europea sui dati*, in *Osservatorio delle fonti*, 2023, 368 ss., consultabile al sito https://www.osservatoriosullefonti.it; A. METZGER, H. SCHWEITZER, *Shaping Markets, A Critical Evaluation of the Draft Data Act*, in *Zeitschrift für Europäisches Privatrecht*, 2023, I, 43 ss. In questo si sostanzia il progressivo e inesorabile 'scivolamento' della prospettiva europea da una logica unipolare e difensiva (ancora prevalente, seppure con l'emersione ben più decisa dell'incentivo della circolazione, nel GDPR) ad una tesa a considerare

Finendo per trascendere i confini di una situazione giuridica soggettiva, la portabilità è divenuta la pietra d'angolo su cui si reggono molti dei pilastri dell'economia europea dei dati: per un verso, questo concetto è scelto dal Reg. UE 2018/1807 (relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea, c.d. Regolamento Free-flow) come cifra distintiva della circolazione dei dati non personali[31]; per altro verso, lo stesso è alla base dell'attività di condivisione delle informazioni, personali e non, (c.d. data sharing), incentivata quale condizione imprescindibile per la costruzione di un mercato dei dati equo e contendibile[32]. Non sorprende dunque che il Reg. UE 2022/868, c.d. Data Governance Act (DA)[33], nel disciplinare l'attività degli intermediari dei dati (in particolare, agli artt. 10-15)[34], presti attenzione a quello che, nei fatti, si è rivelato essere il principale limite all'effettività del diritto alla portabilità dei dati personali, vale a dire l'interoperabilità degli stessi: così, si prevede che gli intermediari debbano «agevola[re] lo scambio dei dati nel formato in cui li ricev[ono] da un interessato o da un titolare dei dati» per «convertir[li] in formati specifici solo allo scopo di migliorare l'interoperabilità a livello intrasettoriale e intersettoriale, se richiesto dall'utente dei dati, se prescritto dal diritto dell'Unione o per garantire l'armonizzazione con le norme internazionali o europee in materia di dati», salva la necessità di «offr[ire] agli interessati o ai titolari dei dati la possibilità di non partecipare a tali conversioni, a meno che la conversione non sia prescritta dal diritto dell'Unione» (art. 12, lett. d, DGA)[35].

L'effettività del diritto alla portabilità dei dati, personali e non, è al cuore anche del Reg. UE 2022/1925, relativo a mercati equi e contendibili nel settore digitale (legge sui mercati digitali o Digital Markets Act, d'ora in avanti abbreviato con l'acronimo DMA)[36]. Questa disciplina, che ha lo scopo di rivitalizzare la concorrenza nel mercato dei «servizi di piattaforma di base»[37] e, per l'effetto, limitare il potere delle grandi piattaforme digitali anche negli altri

---

i dati come risorsa economica e di sviluppo sociale, riutilizzabile a costo zero: cf. G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, in *Riv. trim. dir. pubbl.*, 2022, IV, 973 ss.

[31] V., in particolare, art. 6 e considerando 29 dello stesso Regolamento.

[32] V. considerando 2 DGA.

[33] L. VON DITFURTH, G. LIENEMANN, *The Data Governance Act: – Promoting or Restricting Data Intermediaries?*, in *Journal of Competition and Regulation in Network Industries*, 2022, Vol. 23, 274; A. OWUSU, *Data sharing in the personal data economy. Does sharing mean caring?*, in *EJPLT*, 2023, II, 6 ss. V. anche F. BRAVO, *Intermediazione di dati*, cit., 251 s.

[34] La centralità di questi nuovi attori del mercato è riconosciuta dallo stesso DGA (cfr. considerando 27). Come già osservato *supra*, alla nota 11, l'attività di alcuni di questi soggetti (specialmente le PIMSs, ma anche le Cooperative di dati) ha il merito di rafforzare la posizione di controllo dell'interessato sui propri dati: v. D. POLETTI, *op. cit.*, 370 ss.

Il Regolamento disciplina altresì la condivisione volontaria e gratuita di dati per obiettivi di interesse generale (c.d. data altruism): Artt. 15 e 16-25 DGA.

[35] Lo osserva F. BRAVO, *Le cooperative dei dati*, in *Contratto e impresa*, 2023, III, 777 s.; v. già ID., *Intermediazione di dati*, cit., 251 s.

[36] Per una panoramica generale, v. S. FORASASSI, *Il nuovo Regolamento europeo sui mercati digitali (Digital Markets Act). Inquadramento generale e criticità*, in *Contratto e Impresa Europa*, 2023, I, 145 – 176.

[37] Definiti in un elenco contenuto dall'art. 2, n. 2, DMA, che comprende il servizio di intermediazione online, motori di ricerca, social network, condivisione di video, servizi di comunicazione interpersonali indipendenti dal numero, sistemi operativi, browser web, assistenti virtuali, servizi di cloud computing, servizi pubblicitari online.

settori[38], impone una serie di stringenti obblighi in capo ad alcuni soggetti del mercato che, alla luce di indicatori quantitativi e qualitativi previsti dallo stesso Regolamento, sono qualificati (e designati dalla Commissione) come gatekeepers[39]. In questa cornice, visto il rilievo della disponibilità dei dati nell'espansione trasversale di queste grandi realtà, la portabilità rappresenta uno strumento che le altre imprese possono stimolare (trattandosi di un diritto dell'interessato) per ottenere l'accesso ad una grande quantità di informazioni, rendendosi così competitive sul mercato digitale. In questo si spiega, rispetto all'art. 20 GDPR[40], la notevole estensione del campo di applicazione del diritto[41] e, in generale, il considerevole rafforzamento dello stesso allorché sia esercitato nei confronti dei gatekeepers, sotto la forma di un obbligo loro imposto (art. 6, par. 9, DMA)[42].

Nel più recente testo normativo, scompare ogni limitazione concernente la base giuridica del trattamento; oggetto del diritto, inoltre, non sono solo i dati «forniti», ma anche quelli «generati mediante l'attività dell'utente finale nel contesto dell'utilizzo del pertinente servizio di piattaforma di base».

L'effettività della portabilità è qui parte integrante dell'obbligo imposto ai gatekeepers (al punto che la norma discorre di «effettiva portabilità» e, poco dopo, di «effettivo esercizio di tale portabilità»), traducendosi nella previsione non più solo di standard minimi per favorire l'interoperabilità, ma anche della garanzia di questo risultato («fornendo a titolo gratuito strumenti per agevolar[lo]»)[43]. È altresì prevista la possibilità che la Commissione, per concretizzare quest'obbligo, adotti atti di esecuzione (art. 46, par. 1, lett. b, DMA) oppure si avvalga, allo stesso scopo, delle organizzazioni europee di normazione (art. 48 DMA). L'interoperabilità deve essere assicurata – come precisa il considerando 59 – con «misure tecniche adeguate e di elevata qualità». Andando ancora oltre, e mutuando un risultato già raggiunto settorialmente nel diritto dell'Unione, si prevede segnatamente una portabilità immediata e continua, ossia con accesso «continuo e in tempo reale»[44].

---

[38] Come osservano S. KUEBLER-WACHENDORFF *et al., op. cit.*, 265 s., «As a consequence, these platforms grow ever more powerful in their primary markets and leverage their data silos, market power and installed user base to enter other markets».

[39] Il procedimento di designazione dei gatekeeper è stabilito all'art. 3 DMA. Come riportato dal Comunicato stampa del 6 settembre 2023, i primi sei gatekeeper designati dalla Commissione sono Alphabet, Amazon, Apple, ByteDance, Meta e Microsoft (https://ec.europa.eu/commission/presscorner/detail/en/IP_23_4328).

[40] Fermo che, come normalmente accade nella normativa europea in materia di dati, si ritrova anche nel DMA l'affermazione che il regolamento lascia 'impregiudicate' le norme del GDPR (considerando 12), è significativa la precisazione secondo cui «l'obbligo per il gatekeeper di garantire l'effettiva portabilità dei dati a norma del presente regolamento integra il diritto alla portabilità dei dati a norma del regolamento (UE) 2016/679».

[41] J. KRANZ *et al.*, *op. cit.*, 598.

[42] L'art. 5 DMA proibisce la combinazione di dati personali provenienti dal servizio di piattaforma di base offerto «con dati personali provenienti da altri servizi di piattaforma di base o da eventuali ulteriori servizi forniti dal gatekeeper o con dati personali provenienti da servizi di terzi» (par. 2, lett. b) e l'uso incrociato di tali dati «in altri servizi forniti separatamente dal gatekeeper, compresi altri servizi di piattaforma di base, e viceversa» (par. 2, lett. c).

[43] In base al considerando 59 DMA, infatti, «[i] dati dovrebbero essere ricevuti in un formato immediatamente ed effettivamente accessibile e utilizzabile da parte dell'utente finale o dei pertinenti terzi autorizzati dall'utente finale a cui i dati sono trasferiti».

[44] Sono citate direttamente, come esempio di misure tecniche, le interfacce di programmazione delle applicazioni (API), già segnalate dal WP29 (*Linee guida*, cit., 15), a commento dell'art. 20 GDPR, come strumento per facilitare il trasferimento dei dati nell'ambito dei servizi offerti dalla società dell'informazione. Secondo la definizione dello stesso organismo (ivi, nota 27), si tratta di «interfacce di

Tali caratteri, implicando la superfluità di una ripetuta richiesta da parte dell'interessato in relazione a specifici set di dati, rappresentano un'evoluzione già auspicata dalla dottrina in sede di interpretazione dell'art. 20 GDPR[45]. I rilievi relativi ai benefici di una c.d. continuous portability in termini di rafforzamento della posizione del consumatore e di conseguente stimolo per la concorrenza e lo sviluppo tecnologico si ritrovano citati anche nel considerando 59 DMA: in particolare, questa modalità di esercizio asseconda la tendenza degli utenti finali al c.d. multihoming, situazione che perdura per un tempo anche considerevole, in cui, anziché mutare il fornitore di servizi *online*, gli stessi preferiscono mantenere attivi entrambi i servizi.

È peraltro significativo che il Regolamento abbia tenuto conto di uno dei principali rischi di un requisito qualitativo così elevato della portabilità, ossia quello di un costo eccessivamente alto per le piccole e medie imprese: secondo un approccio basato sulla proporzionalità, l'obbligo è infatti posto solamente a carico dei colossi digitali, appunto i gatekeepers[46].

Titolari del diritto alla portabilità previsto dal DMA sono gli «utenti finali», ossia coloro che utilizzano il servizio di piattaforma per scopi diversi (commerciali o non) da quelli di fornire beni o servizi (art. 1, n. 20, DMA). Invero, anche agli utenti commerciali, ossia a coloro che fanno ricorso alla piattaforma («nell'ambito delle proprie attività commerciali o professionali (…) ai fini della fornitura di beni o servizi agli utenti finali o nello svolgimento di tale attività»: art. 1, n. 21, DMA) è riconosciuto un diritto di «accesso efficace, di elevata qualità, continuo e in tempo reale a dati aggregati e non aggregati, compresi i dati personali» e il gatekeeper deve garantire l'uso di tali dati (art. 6, par. 10, DMA)[47]. Questo diritto si riferisce anche ai dati degli utenti finali (quindi di soggetti diversi da quello che esercita la prerogativa): «quanto ai dati personali», il gatekeeper ne fornisce l'accesso e ne garantisce l'uso «solo se i dati sono direttamente connessi con l'uso effettuato dagli utenti finali in relazione ai prodotti o servizi offerti dal pertinente utente commerciale mediante il pertinente servizio di piattaforma di base e nel caso in cui gli utenti

applicazioni o servizi web che i titolari rendono disponibili per consentire ad altri sistemi o applicazioni di connettersi e operare con i propri sistemi»; v. pure D. COPETTI CRAVO, *op. cit.*, 56 s.; sulle possibili costellazioni tecniche che possono consentire ad una effettiva portabilità, v. J. KRANZ *et al.*, *op. cit.*, 606 s.

[45] J. KRÄMER, *op. cit.*, 296: «In summary, we therefore argue in favour of a new proportionate rule that gives consumers the right to transfer their personal data (as under Article 20 GDPR) continuously and in real time from their existing digital service provider to another provider».

[46] Nell'ampliare l'ambito di applicazione oggettivo del diritto, il legislatore europeo supera, almeno in buona parte, un ulteriore rischio, lucidamente messo in rilievo dalla dottrina (v. J. KRÄMER, *op. cit.*, 296 s.), ossia amplificare le incertezze giuridiche che riguardano questo aspetto nella versione 'base' della portabilità: è infatti evidente che la versione 'rafforzata' dal DMA si muove decisamente nella direzione di privilegiare le istanze del mercato. Rimane però aperto il tema del pericolo di incentivare prassi di migrazione dei dati, magari dietro promessa di incentivi economici, verso ambienti meno sicuri, rischio che si è proposto di mitigare facendo ricorso alle cautele adottate dalla legislazione europea nel settore bancario, dove pure è presente una portabilità *real-time* e continua (che, in questo senso, integra il GDPR): v. ancora J. KRÄMER, *op.* cit., 297. Il riferimento è alla direttiva UE 2015/2366 relativa ai servizi di pagamento nel mercato interno (c.d. PSD2, in particolare agli artt. 66, par. 4, e 67, par. 3): v. J. KRÄMER, P. SENELLART, A. DE STREEL, *op. cit.*, 31 s.

[47] Come precisa lo stesso art. 6, par. 10, DMA, si tratta dei «dati che sono forniti o generati nel contesto dell'uso dei pertinenti servizi di piattaforma di base o dei servizi forniti contestualmente o in ausilio ai pertinenti servizi di piattaforma di base». V. pure il considerando 60 DMA. Un ulteriore obbligo di condivisione riguarda taluni dati generati dagli utenti finali sui motori di ricerca online del gatekeeper ("dati relativi a posizionamento, ricerca, click e visualizzazione"): questi deve garantirne ai prestatori di servizi di motori di ricerca che ne facciano richiesta, l'accesso "a condizioni eque, ragionevoli e non discriminatorie" (Art. 6, par. 11, DMA, che prevede, per i dati personali, la loro anonimizzazione).

finali accettano tale condivisione esprimendo il [loro] consenso» (art. 6, par. 10, DMA).

5. L'ulteriore evoluzione della portabilità nell'architettura dei più recenti interventi normativi dell'UE: la compiuta rottura degli argini soggettivi del diritto dell'interessato nella Legge europea sui dati (Data Act).

L'apertura, a soggetti diversi dall'interessato, dell'accesso e della condivisone dei dati dischiude un'ulteriore traiettoria evolutiva del diritto alla portabilità, che ne proietta l'ambito di applicazione soggettivo in una dimensione più ampia rispetto alla sfera dell'interessato. Allo stato, la più significativa espressione di questa dimensione è oggi contenuta nel Reg. UE 2023/2854, riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo (regolamento sui dati o Data Act, d'ora in avanti DA)[48].

Lo scopo dello strumento, rispetto alla cui compatibilità con il GDPR il legislatore europeo è molto attento, non è tutelare i diritti dell'interessato, ma incentivare la circolazione dei dati, personali e non, generati dai prodotti connessi e dai servizi ad essi correlati[49].

Dalla prospettiva che qui interessa, la figura centrale è quella dell'utente del prodotto connesso o del servizio correlato [50] : a questo soggetto, il Regolamento garantisce il diritto di accesso e di condivisione con terzi, per scopi commerciali e non, di una serie molto ampia di dati [51] detenuti da un «titolare dei dati» (data holder) [52] , purché nella "pronta disponibilità" di

[48] Cfr. D. POLETTI, *op. cit.*, 373 ss., che osserva come la normativa abbia lo scopo di incentivare la circolazione dei dati dal titolare dei dati al destinatario (entrambi soggetti imprenditoriali), mentre il ruolo dell'interessato è per così dire relegato ad «agente legittimante», al quale rimane però il potere di scegliere dove veicolare i dati che lo riguardano.

[49] Come specificato nel considerando 32, l'obiettivo del Data Act «non è solo promuovere lo sviluppo di prodotti connessi o di servizi correlati nuovi e innovativi e stimolare l'innovazione nei servizi post-vendita, ma anche stimolare lo sviluppo di servizi completamente nuovi che utilizzano i dati in questione, anche sulla base di dati provenienti da una varietà di prodotti connessi o servizi correlati».

[50] La definizione di prodotto connesso richiama l'idea di "Internet of Things" (IoT): «un bene che ottiene, genera o raccoglie dati relativi al suo utilizzo o al suo ambiente e che è in grado di comunicare dati del prodotto tramite un servizio di comunicazione elettronica, una connessione fisica o l'accesso su dispositivo, e la cui funzione primaria non è l'archiviazione, il trattamento o la trasmissione dei dati per conto di una parte diversa dall'utente» (art. 2, n. 5, DA). Il servizio correlato è il servizio digitale, presente sin dall'origine o successivamente installato, grazie al quale il prodotto svolge tutte o anche solo una delle sue funzioni (cfr. art. 2, n. 6, DA). Sono compresi gli assistenti virtuali, anche se forniti da soggetti diversi (considerando 23), che interagiscono con un prodotto connesso o un servizio correlato (art. 1, par. 4, DA). La definizione di utente del prodotto o del servizio è molto ampia (art. 2, n. 12, DMA: «una persona fisica o giuridica che possiede un prodotto connesso o a cui sono stati trasferiti contrattualmente diritti temporanei di utilizzo di tale prodotto connesso o che riceve un servizio correlato»), con la conseguenza che più soggetti possono rivestire contemporaneamente questa qualifica (considerando 18).

[51] Per un'attenta analisi del contenuto di questi diritti, v. G. VERSACI, *I nuovi diritti ai sensi del Data Act: accesso ai dati, utilizzo e condivisione dei dati con terzi*, in AA. VV., *Data Act. Accesso equo ai dati e loro utilizzo: profili sistematici e applicativi nell'orizzonte del diritto privato*, a cura di V. BACHELET, GIA. MARINO, A. RACANO, Milano, 2025, 125 ss.; v. anche A. MICHINELLI, *Diritti e obblighi degli utenti e dei titolari dei dati*, in AA. VV., *Data Act. Regolamento europeo sui dati*, a cura di L. BOLOGNINI, E. PELINO, M. SCIALDONE, Milano, 2025, 55 ss.

[52] Il data holder è definito come «una persona fisica o giuridica che ha il diritto o l'obbligo, conformemente al presente regolamento, al diritto applicabile dell'Unione o alla legislazione nazionale adottata conformemente al diritto dell'Unione, di utilizzare e mettere a disposizione dati, compresi, se concordato contrattualmente, dati del prodotto o di un servizio correlato che ha reperito o generato nel corso della fornitura di un servizio correlato» (art. 2, n. 13, DA). Si tratta, in sostanza, di un proprietario 'di fatto' dei dati (v. A. METZGER, H. SCHWEITZER, *op. cit.*, 54), ossia di un soggetto che ha un controllo materiale sugli stessi. V., a

quest'ultimo[53]. Sono compresi i dati osservati, non solo nella forma "grezza", ma anche in quella definita dal Regolamento "pretrattata", oltre ai cc.dd. metadati[54]; rimangono ancora esclusi dal campo di applicazione della disciplina i dati inferenziali[55].

Gli standard qualitativi imposti per l'accesso, la «messa a disposizione» dei dati (art. 4 DA) e la condivisione con terzi[56] degli stessi su richiesta dell'utente (art. 5 DA) sono molto elevati, nel senso di garantire l'effettività e l'interoperabilità: «senza indebito ritardo, con la stessa qualità di cui dispone il titolare dei dati, in modo facile, sicuro, a titolo gratuito per l'utente[57], in un formato completo, strutturato, di uso comune e leggibile da dispositivo automatico». Se «pertinente e tecnicamente possibile», il flusso di dati è «continuo e in tempo reale».

Superando una evidente limitazione della versione di base della portabilità, l'attenzione a questo risultato si traduce altresì in norme destinate ai fabbricanti dei prodotti connessi e ai fornitori dei servizi correlati (affinché prodotti e servizi siano realizzati di modo che, di default, i dati concernenti il loro utilizzo siano agevolmente accessibili in formati fruibili), e, in aggiunta, a coloro che vendano o concedano in godimento tali prodotti (che sono gravati da precisi obblighi informativi da soddisfare prima della conclusione del contratto)[58].

---

proposito degli scenari aperti dal Data Act sui diritti sui dati non personali generati dall'IoT, M. ECKARDT, W. KERBER, *Property rights theory, bundles of rights on IoT data, and the EU Data Act*, in *European Journal of Law and Economics*, 2024, vol. *Data Economy*. Consultabile al sito: https://link.springer.com/article/10.1007/s10657-023-09791-8.

[53] L'art. 2, n. 17, DA definisce 'prontamente disponibili': i «dati del prodotto e dati di un servizio correlato che un titolare dei dati ottiene o può ottenere legittimamente dal prodotto connesso o dal servizio correlato senza che ciò implichi uno sforzo sproporzionato che vada al di là di una semplice operazione».

[54] Il 'pretrattamento' consiste nel procedimento attraverso il quale i dati grezzi (raw data) raccolti dai prodotti connessi o dai servizi ad essi correlati vengono resi comprensibili ed utilizzabili per successive attività di trattamento (cfr. considerando 15 DA); i «metadati» sono invece definiti dall'art. 2, n. 2, DA come «una descrizione strutturata del contenuto o dell'uso dei dati che agevola la ricerca o l'utilizzo di tali dati».

[55] Dalla lettura del considerando 15 DA, emerge la moltitudine di dati oggetto dei diritti degli utenti dei prodotti connessi e dei servizi correlati, intesi in senso ampio come «digitalizzazione delle azioni o degli eventi degli utenti». Alla luce degli obiettivi del Regolamento, non rientrano invece i dati relativi ai software e ai contenuti non correlati, ossia «i dati generati da tali prodotti connessi dotati di sensori quando l'utente registra, trasmette, visualizza o riproduce contenuti, nonché i contenuti stessi, spesso soggetti a diritti di proprietà intellettuale, anche per l'uso da parte di un servizio online» (considerando 16 DA, che altresì precisa che il Data Act «non dovrebbe inoltre applicarsi ai dati ottenuti, generati o consultati dal prodotto connesso, o ad esso trasmessi, a fini di archiviazione o altre operazioni di trattamento per conto di altre parti diverse dall'utente, come nel caso di server o infrastrutture cloud gestiti dai rispettivi proprietari interamente per conto di terzi, anche per uso da parte di un servizio online»).

[56] Sui quali gravano gli obblighi previsti dall'art. 6 DA, tra i quali spicca il principio di minimizzazione, esteso anche ai dati non personali (ma, solo in questo caso, derogabile).

[57] Il compenso può essere chiesto non già all'utente, ma al destinatario dei dati, alla luce di un accordo che, ai sensi degli artt. 8 ss. DA, quest'ultimo deve stipulare con il titolare dei dati. È significativa la precisazione dell'art. 5, par. 8, DA, secondo la quale «[l]a mancanza di accordo, da parte del titolare dei dati e del terzo, sulle modalità per la trasmissione dei dati non ostacola, impedisce o interferisce con l'esercizio dei diritti dell'interessato a norma del regolamento (UE) 2016/679 e, in particolare, con il diritto alla portabilità dei dati di cui all'articolo 20 di tale regolamento».

[58] Art. 3 e considerando 20-24. L'art. 7 e il considerando 41 DA prevedono eccezioni per le microimprese e le piccole imprese (e dettano talune regole di favore anche per le medie imprese), alla luce di una valutazione di opportunità di mercato. Sempre valutazioni di questo tipo (ma di segno contrario) sono alla base dell'esclusione dei *gatekeeper* dalla possibilità di «chiedere o ottenere l'accesso ai dati degli utenti generati dall'uso di un prodotto connesso o di un servizio correlato o da un assistente virtuale ai sensi del presente regolamento. Inoltre, i terzi cui i dati sono messi a disposizione su richiesta dell'utente non possono

Dalla prospettiva dei dati personali[59], le definizioni soggettive del Data Act devono collegarsi con quelle, imprescindibili, del GDPR. Se l'utente del prodotto è anche l'interessato (data subject) è evidente che gli artt. 4 e 5 DA si sovrappongono al diritto alla portabilità di cui all'art. 20 GDPR, amplificandolo e superandone molte delle limitazioni sopra esaminate, in linea con l'evoluzione normativa che si è tratteggiata[60]. L'inclusione dei dati 'osservati', in particolare, supera in modo definitivo il dilemma interpretativo relativo alla nozione di dati "forniti", almeno con riguardo a quelli collegati all'Internet of Things. Se invece le informazioni personali di cui l'utente del prodotto domanda l'accesso e la condivisione si riferiscono ad altre persone fisiche, il diritto riconosciuto dal Data Act getta luce su una diversa manifestazione della portabilità, che, per non urtare contro i principi del GDPR, deve essere considerata un trattamento: ne discende che l'utente del prodotto può assumere la qualifica di titolare del trattamento (salvo che, naturalmente, ricorra una delle eccezioni che esclude l'applicazione della disciplina sui dati personali: art. 2 GDPR), come pure, prima di lui e poi assieme a lui, il titolare dei dati (al quale è infatti domandato di compiere una certa attività con riguardo a quei dati). L'equilibrio raggiunto tra le due normative è dunque a favore del GDPR: rispetto a nessuna delle attività previste dal *Data Act* (messa a disposizione o condivisione dei dati) e per entrambi i soggetti, tale disciplina fornisce una base giuridica che legittima il trattamento, la quale continuerà pertanto ad essere necessaria ai sensi dell'art. 6 GDPR[61].

Pur con tutte queste cautele, rimane sicuramente impressa all'interprete questa ulteriore configurazione della portabilità, la quale sottende qui non solo un diritto dell'interessato, ma integra altresì una prerogativa del titolare del trattamento[62], seppure alla condizione dell'esistenza di una base giuridica a sostegno di tale operazione[63].

---

mettere i dati a disposizione di un gatekeeper»: così il considerando 40 DA, che si traduce nelle stringenti previsioni degli artt. 5, par. 3, e 6, par. 2, lett. d), DA.
Si noti, infine, che al tema dell'interoperabilità è dedicato un capo specifico del Regolamento (VIII).

[59] Lo stesso vale «anche qualora i dati personali e non personali all'interno di un insieme di dati siano indissolubilmente legati»: considerando 34 DA.

[60] Questo diritto di portabilità rafforzato non sostituisce, ma si affianca a quello generale: v. *supra* nota 57 e considerando 35.

[61] Come ribadito più volte nel testo normativo, il legislatore non ha inteso conferire ai data holder un nuovo diritto di utilizzare i dati: v. considerando 5, 7 e 25 DA. Anche gli utenti del prodotto connesso o del servizio correlato devono avere una base giuridica, allorché non siano i data subject e nella misura in cui si applichi il GDPR (non dunque nel caso di un uso domestico condiviso di un prodotto connesso), in quanto titolari del trattamento: così gli artt. 4, par. 12, e 5, par. 7, e il considerando 34 DA, il quale ultimo prende altresì in considerazione l'ipotesi in cui titolare dei dati e utente del prodotto siano entrambi, nella prospettiva del Regolamento sulla protezione dei dati personali, contitolari del trattamento e precisa che, una volta che l'utente abbia a disposizione i dati per averli ricevuti dal titolare dei dati, può divenire a sua volta, a norma del Data Act, un titolare dei dati. Il legislatore europeo ha dunque seguito un Trennungsprinzip rispetto alla disciplina delle informazioni personali, la quale continua a regolare in via esclusiva le basi giuridiche che legittimano qualsiasi attività di trattamento: M. SCHMIDT-KESSEL, *Einordnung des Data Act in das Mehrebenensystem des Unionsprivatrechts*, in *MMR. Zeitschrift für IT-Recht und Recht der Digitalisierung*, 2024, I, 127; v. pure A. METZGER, H. SCHWEITZER, *op. cit.*, 76 ss.

[62] Così perlomeno rievocando la costruzione di un "diritto" al trattamento, da intendersi come insieme di prerogative del titolare: v. F. BRAVO, *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Milano-Padova, 2018, *passim*.

[63] In termini generali, l'art. 5, par. 13, DA specifica che «Il diritto di cui al paragrafo 1 non deve ledere i diritti degli interessati a norma del diritto dell'Unione e nazionale applicabile in materia di protezione dei dati personali».

6. La duplice veste della portabilità nel Regolamento sullo spazio europeo dei dati sanitari (European Health Data Space Act).

Un'ultima evoluzione del diritto (e del concetto di) portabilità si rinviene Regolamento sullo spazio europeo dei dati sanitari[64]. Come preannunciato nelle linee programmatiche della Commissione emanate all'avvio del decennio in corso[65], ad una normativa orizzontale in materia di dati (il cui perno, con riguardo ai dati personali, continua a trovarsi nel GDPR), sono destinate ad affiancarsi alcune discipline settoriali, che mirano a rafforzare il quadro giuridico e ad incentivare la circolazione delle informazioni rilevanti nell'ambito di settori strategici. Il testo normativo interviene con riguardo sia al c.d. uso primario dei dati sanitari elettronici[66], ossia per finalità concernenti la cura delle persone – intesa in termini piuttosto ampi (art. 2, lett. d, Reg. UE 2025/327) – sia al c.d. uso secondario degli stessi dati, vale a dire per scopi diversi da quelli iniziali (ad esempio attinenti alla finalità di cura tipica dell'uso primario), alla luce dei quali sono stati raccolti o generati (art. 2, par. 2, lett. e, Reg. UE 2025/327). Le finalità legittime dell'uso secondario sono elencate nel capo IV del Regolamento (ad esempio, la ricerca scientifica: art. 53, par. 1, lett. e Reg. UE 2025/327).

Nel contesto dell'uso primario, la nuova normativa mira a «specificare» e «integrare» [67] i diritti dell'interessato sui propri dati sanitari elettronici personali, con prevalente riguardo al diritto all'accesso e al diritto alla

---

[64] Regolamento UE 2025/327 sullo spazio europeo dei dati sanitari (noto con l'acronimo inglese EHDS, European Health Data Space). Per un inquadramento delle nuove regole, v. S. CORSO, *Lo spazio europeo dei dati sanitari. Prime riflessioni sul regolamento UE 2025/327*, in *Nuove leggi civ. comm.*, 2025, 563 ss.; A. MORACE PINELLI, *Lo spazio europeo dei dati sanitari*, in *Nuova giur. civ. comm.*, 2025, II, 1016 ss. Con specifico riguardo ai diritti persone fisiche nell'ambito dell'uso primario, v. S. FAILACE, *I diritti dell'interessato nell'uso primario dei dati sanitari elettronici secondo il nuovo Regolamento EHDS*, in *Contr. impresa*, 2025, 379 ss. Per prime osservazioni sulla proposta (COM (2022) 197 final, 3 maggio 2022), cfr. I. RAPISARDA, *Sul costituendo spazio europeo dei dati sanitari*, in *Resp. medica*, 2023, IV, 413 – 425.

[65] COM (2020) 66 *final*, *Una strategia europea per i dati*, cit., 24 ss.

[66] I dati sanitari elettronici possono essere personali o non personali e sono trattati in formato elettronico (art. 2, par. 2, lett. c. Reg. UE 2025/327); i dati sanitari elettronici personali comprendono i «dati relativi alla salute e i dati genetici» trattati in tale formato (art. 2, par. 2, lett. a); i dati sanitari elettronici non personali sono individuati per differenza rispetto a quelli personali della stessa categoria (art. 2, par. 2, lett. b). La difficoltà di discernere quali informazioni della persona vi rientrino concretamente, segnalata dal soppresso riferimento nella definizione ai fattori determinanti lo stato di salute (sul quale v. W. LI, P. QUINN, *The European Health Data Space: An expanded right to data portability*, in *Computer Law & Security Review*, 2024, Vol. 52, 8), è solo in parte riassorbita dall'attuale richiamo al GDPR. In ogni caso, la mole dei dati è estremamente ampia, se si considera che nella categoria possono essere annoverate anche le informazioni raccolte da applicazioni scaricate su dispositivi mobili o indossabili. Altra problematica, segnalata già dal Parere congiunto del Comitato europeo per la protezione dei dati personali e del Garante europeo per la protezione dei dati personali sulla proposta, (EDPB-EDPS, *Opinion 3/2022*, adottato il 12 luglio 2022, 14), è quella, pratica, di distinguere i dati personali da quelli non personali (ed è anche noto che l'anonimizzazione non escluda il rischio di reidentificazione, attraverso procedimenti logici e di data mining: v. pure considerando 92 e 103 Reg. UE 2025/327). Su raccomandazione di queste stesse Istituzioni, la definizione di dati non personali precisava, nel testo emendato dal Parlamento europeo, che «laddove i dati personali e non personali una serie di dati siano indissolubilmente legati, l'intera serie di dati e trattata come dati sanitari elettronici personali» (art, 2, par. 2, lett. b, della proposta). Tale precisazione è però scomparsa nel testo del Regolamento.

[67] Art. 1, par. 2, lett. a), Reg. UE 2025/327. Nella formulazione originaria della proposta della Commissione, si accentuava l'idea che tali diritti fossero "rafforzati".

portabilità[68], specialmente con riferimento alle informazioni che rientrano nelle categorie prioritarie definite dal Regolamento[69]. Sciogliendo un nodo interpretativo che la proposta rischiava di lasciare insoluto, il Regolamento precisa che i diritti di nuova generazione non si sostituiscono a quelli previsti dal GDPR, ma ad essi si affiancano, lasciando all'interessato la scelta del quadro giuridico di riferimento sul quale poggiare la propria richiesta (a patto che, naturalmente, ne ricorrano i rispettivi presupposti)[70].

Con riguardo al diritto alla portabilità, la formulazione del testo normativo ha conosciuto alcune significative evoluzioni. Nella proposta della Commissione, l'art. 3, par. 8, riconosceva alle persone fisiche il diritto di richiedere ai «titolari dei dati» (data holder)[71], purché si trattasse di soggetti «del settore sanitario o della sicurezza sociale o dei servizi di rimborso»[72], la trasmissione (diretta) dei propri dati sanitari elettronici ad altri soggetti dello stesso settore. Nella versione attuale, che risulta dalla formulazione dell'art. 7 Reg. UE 2025/327, destinatari della richiesta degli individui – oltre che dei dati trasmessi su iniziativa degli stessi – sono, più specificamente, i prestatori di assistenza sanitaria. In aggiunta, è consentita la trasmissione («unidirezionale»)

[68] Mentre la proposta della Commissione faceva riferimento al solo diritto di accesso (pur già imbastendo un confronto con l'Art. 20 GDPR nei considerando), il Reg. UE 2025/327 definisce espressamente come "diritto delle persone fisiche alla portabilità dei dati", l'insieme delle facoltà degli individui ora descritte nell'art. 7 (cfr. l' originario art. 3, par. 8, della proposta). Invero, una tale qualificazione, tanto più che il diritto è parso sin da subito modellato sulla base della forma più avanzata della portabilità nota al GDPR (quella "diretta", di cui all'Art. 20, par. 2), appariva già fuori di dubbio: v. W. LI, P. QUINN, *op. cit.*, 6. Vi è peraltro da osservare che, in questa nuova disciplina, la differenza tra il diritto di accesso (Art. 3) e diritto alla portabilità nella versione base dell'Art. 20, par. 1, GDPR tende a farsi evanescente. La persona fisica che esercita questo diritto, infatti, riceve i dati in formato elettronico, «immediatamente» («dopo la registrazione dei dati sanitari elettronici personali in un sistema di cartelle cliniche elettroniche, nel rispetto della praticabilità tecnologica»), «gratuitamente e in un formato facilmente leggibile, consolidato e accessibile». A cavallo tra tali diritti, si aggiunge ora (dopo il passaggio al Parlamento europeo) «il diritto di scaricare gratuitamente una copia elettronica almeno dei dati sanitari elettronici personali che rientrano nelle categorie prioritarie (…), nel formato europeo di scambio delle cartelle cliniche elettroniche» (art. 3, par. 2, Reg. UE 2025/327).

[69] Art. 14 Reg. UE 2025/327. Si tratta di dati essenziali a ricostruire lo stato di salute della persona fisica, in larga parte già digitalizzati nell'UE (ad esempio i profili sanitari sintetici dei pazienti, i risultati di laboratorio, i referti di immagini e le lettere di dimissioni). Il diritto di accesso è garantito «almeno» in relazione a questi dati (art. 3, par. 1, Reg. UE 2025/327); secondo il considerando 14, il diritto alla portabilità dovrebbe, tra l'altro «consentire alle persone fisiche di rendere accessibili almeno le categorie prioritarie dei loro dati sanitari elettronici personali ai professionisti sanitari di loro scelta, di scambiarli con questi e di scaricarli».

[70] Cfr. il considerando 8 Reg. UE 2025/327. Per un confronto con le potenzialità del diritto alla portabilità di cui all'art. 20 GDPR, che infatti già può avere ad oggetto dati sanitari (nei limiti della sua disciplina), v. D. TUZZOLINO, *La portabilità dei dati sanitari*, in AA. VV., *La protezione dei dati sanitari. Privacy e innovazione tecnologica tra salute pubblica e diritto alla riservatezza*, a cura di A. THIENE e S. CORSO, Napoli, 2023, 59-90.

[71] Il Regolamento definisce ora la figura del "titolare dei dati sanitari", ai sensi dell'art. 2, par. 2, lett. t), Reg. UE 2025/327: «una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo del settore dell'assistenza sanitaria o delle cure assistenziali, compresi, ove necessario, i servizi di rimborso, nonché una persona fisica o giuridica che sviluppi prodotti o servizi destinati al settore sanitario, dell'assistenza sanitaria o delle cure assistenziali, sviluppi o fabbrichi applicazioni per il benessere, svolga attività di ricerca in relazione al settore dell'assistenza sanitaria o delle cure assistenziali o funga da registro della mortalità, nonché un'istituzione, un organo o un organismo dell'Unione che abbia», alternativamente, «i) il diritto o l'obbligo, conformemente al diritto dell'Unione o nazionale applicabile e in qualità di titolare o contitolare del trattamento, di trattare dati sanitari elettronici personali per la prestazione di assistenza sanitaria o cure assistenziali o a fini di sanità pubblica, rimborso, ricerca, innovazione, definizione delle politiche, statistiche ufficiali o sicurezza dei pazienti o a fini di regolamentazione; o ii) la capacità di rendere disponibili dati sanitari elettronici non personali, mediante il controllo della progettazione tecnica di un prodotto e dei servizi correlati, anche in termini di registrazione, fornitura, limitazione dell'accesso o scambio».

[72] Non erano quindi comprese le applicazioni per il benessere, pur essendo queste in grado di registrare dati sanitari, utili tanto ad un uso primario (v. *infra*), quanto ad un uso secondario.

di una parte dei dati ad un soggetto, «chiaramente identificato» del settore della sicurezza sociale o dei servizi di rimborso. Queste modifiche soggettive valgono come conferma di un'ulteriore limitazione, sul piano oggettivo, che invero già traspariva dal testo originario della proposta: in questa forma[73], il diritto alla portabilità può essere esercitato nel solo contesto dell'uso primario dei dati sanitari elettronici personali[74].

Nonostante queste limitazioni sul piano oggettivo e soggettivo, per un verso, riemergono i progressi altrove già segnati dalla portabilità (in particolare: l'irrilevanza della base giuridica, l'immediatezza della trasmissione, il coinvolgimento dei fabbricanti dei servizi informatici nei conseguenti obblighi[75])[76], e sono raggiunti, per altro verso, ulteriori traguardi.

Anzitutto, questa versione del diritto alla portabilità, che ripete il modello "diretto" dell'art. 20, par. 2, GDPR, non è limitato, come in quella sede, ai casi in cui risulta «tecnicamente fattibile». La fattibilità tecnica, oltre che l'immediatezza della trasmissione, è, infatti, data per presupposta dal nuovo Regolamento[77]. Superando un ulteriore limite di effettività della portabilità generale del GDPR, l'interoperabilità dei dati è garantita dall'impiego del formato europeo di scambio delle cartelle elettroniche elaborato dalla Commissione, pure nel caso in cui i prestatori di attività sanitarie sono situati in diversi Stati membri[78].

---

[73] Rimane dunque ferma la possibilità di esercitare il diritto generale alla portabilità dei dati, ai sensi dell'art. 20 GDPR.

[74] Tale limitazione poteva già ricavarsi, nella formulazione dell'art. 3, par. 8, della proposta, oltre che dalla collocazione della disposizione, anche dalla specificazione che il "titolare dei dati" dovesse essere affiliato al «settore sanitario o della sicurezza sociale». Cfr., su questo punto, W. LI, P. QUINN, *op. cit.*, 8 s. Secondo l'opinione che tali Autori hanno prospettato con riguardo alla formulazione originaria della proposta, tuttavia, dall'assenza di un riferimento specifico alla finalità nell'articolato normativo, sembrava più convincente ritenere che, pur dovendo i dati provenire dal contesto dell'uso primario, tale uso non fosse poi vincolante per il destinatario, a condizione che tale soggetto potesse dirsi comunque appartenente alla categoria dei prestatori di servizi sanitari (ivi, 9 s.).

[75] V. artt. 7, parr. 1 e 3, e, inoltre gli 30 ss. Reg. UE 2025/327, in relazione alle cartelle cliniche e alle applicazioni per il benessere che dichiarano l'interoperabilità con un sistema di cartelle cliniche elettroniche. V. anche S. FAILACE, *I diritti dell'interessato*, cit., 397.

[76] Cfr. Considerando 14 Reg. UE 2025/327.

L'art. 7 Reg. UE 2025/327 fa ora espresso riferimento ai «dati sanitari elettronici personali». Poteva dirsi dubbio, nel contesto della proposta, se il diritto contemplato potesse riguardare oltre ai dati personali, anche quelli non personali. Sul punto, si registravano indicazioni letterali contrastanti: da un lato, infatti, il riferimento ai dati *tout court* e al *data holder* (anziché al titolare del trattamento) suggeriva una risposta positiva al quesito; d'altro canto, l'intitolazione della Sezione I in cui era inserito l'art. 3 induceva a restringere il campo di applicazione ai soli dati personali (v., in questo senso, W. LI, P. QUINN, *op. cit.*, 7 s.).

Invero, se si confronta questa evoluzione del diritto alla portabilità con quella che ha caratterizzato altri strumenti recenti del diritto dell'Unione (ad esempio, il Data Act: v. *supra*, par. precedente), si nota come questo diritto tenda ad estendersi anche ai dati non personali se tale situazione soggettiva è strumentale ad una logica di mercato, aprendosi piuttosto il problema di selezionare un criterio di rilevanza che giustifichi la portabilità di informazioni non legate ad un individuo (nel citato Data Act, tale criterio consiste nel fatto che il dato non personale rientra pur sempre nell'ambito di una definizione che scopre un qualche collegamento con l'utente del bene o del servizio correlato, trattandosi di una «digitalizzazione delle azioni e degli eventi» ad essi relativi: v., *supra* nota 55). Tale logica non è però condivisa dal provvedimento normativo ora in esame.

[77] I. RAPISARDA, *Sul costituendo spazio europeo dei dati sanitari*, cit., 417.

[78] V. art. 7, par. 2, Reg. UE 2025/327; l'art. 15 dello stesso Regolamento manda alla Commissione la definizione del formato europeo di scambio delle cartelle cliniche elettroniche. I dati ricevuti in questo formato, oltre che dovere essere accettati, devono potere essere pure fruiti: v. artt. 7, parr. 2 e 4, e 15, par. 4, Reg. UE 2025/327. V. infine anche il considerando 15.

Con riferimento alla «copia elettronica delle loro categorie prioritarie di dati sanitari elettronici» scaricata, ai sensi dell'art. 3, par. 2, Reg. UE 2025/327, nel formato europeo di scambio delle cartelle cliniche

Meritano, infine, di essere segnalate l'inclusione dei dati inferenziali [79], nonché la completa gratuità (non solo per l'interessato ma) anche per il destinatario dei dati, qualità, questa, già prevista dalla proposta[80], confermata dal Regolamento[81].

Sempre nel contesto dell'uso primario, riaffiora altresì una diversa idea della portabilità, che non ha i contorni della situazione soggettiva, ma che si ricollega immediatamente all'obiettivo della libera circolazione dei dati sanitari attraverso canali sicuri[82], direttamente funzionale al diritto alla salute nella sua dimensione digitale [83], attraverso l'alimentazione delle cartelle sanitarie elettroniche [84]. Qui confluiscono i dati dei pazienti, ai quali i professionisti sanitari possono accedere[85] per prestare l'attività di cura e per aggiornarli[86],

elettroniche, l'art. 7, par. 4, Reg. UE 2025/327 precisa che «le persone fisiche sono in grado di trasmettere tali dati ai prestatori di assistenza sanitaria di loro scelta» in tale formato.

[79] Vi rientrano diagnosi, test e esami medici: considerando 6. L'inclusione di questi dati consente una visione olistica del paziente (W. LI, P. QUINN, *op. cit.*, 7), ciò che è alla base della medicina personalizzata e di precisione.

[80] Nella versione originaria l'art. 3, par. 8, comma 3, della proposta prevedeva una "deroga" all'art. 9 DA (allora anch'esso in proposta).

[81] Art. 18 Reg. UE 2025/327.

[82] Per l'uso secondario dei dati sanitari, la proposta mira a creare una base giuridica per il trattamento, ai sensi degli artt. 6 e 9 GDPR (cfr., in particolare, considerando 52 Reg. UE 2025/327). Si specifica, tuttavia, il diritto delle persone fisiche di esercitare un (revocabile) opt out rispetto all'uso dei propri dati per l'uso secondario (art. 71 Reg. UE 2025/327): v., in argomento, S. CORSO, *Lo spazio europeo dei dati sanitari*, cit., 588 ss.

[83] Come ricorda il considerando 26 Reg. UE 2025/327, obiettivo dell'Unione è che tutti i cittadini abbiano accesso alle proprie cartelle cliniche elettroniche entro il 2030: Programma strategico per il decennio digitale 2030 (Decisione UE 2022/2481del Parlamento europeo e del Consiglio dell'Unione del 14 dicembre 2022).

[84] La «cartella clinica elettronica», secondo una nomenclatura che non corrisponde a quella nazionale in uso (v. C. SARTORIS, *Sanità digitale e tutela dei dati personali*, in AA. VV., *Protezione dei dati personali e nuove tecnologie. Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze giuridiche e sulle loro conseguenze giuridiche*, a cura di A. ADINOLFI e A. SIMONCINI, Napoli, 2022, 356 ss.) è definita dall'art. 2, par. 2, lett. j), Reg. UE 2025/327 come «una raccolta di dati sanitari elettronici relativi a una persona fisica e rilevati nell'ambito del sistema sanitario, il cui trattamento avviene ai fini della prestazione di servizi di assistenza sanitaria». Nell'ordinamento italiano, l'art. 12 d.lg. n. 179/2012, modificato numerose volte, ha introdotto il fascicolo sanitario elettronico (FSE), definito al co. 1°, come «l'insieme dei dati e documenti digitali di tipo sanitario e socio-sanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito, riferiti anche alle prestazioni erogate al di fuori del Servizio sanitario nazionale»: v., per una chiara sintesi, S. CORSO, *Sanità digitale riservatezza. Interpretazioni sul fascicolo sanitario elettronico*, in AA. VV., *La protezione dei dati sanitari*, cit., 91 – 128. La disciplina, oltre che nel menzionato articolo, è attualmente contenuta nel d.m. 7 settembre 2023, emanato a seguito delle *Linee guida per l'attuazione del Fasciolo sanitario elettronico* (d.m. 20 maggio 2022) nell'ambito degli obiettivi del PNRR (v. S. CORSO, *Il fascicolo sanitario elettronico 2.0. Spunti per una lettura critica*, in *Leggi civili comm*, 2024, II, 334 – 462; I. RAPISARDA, *Appunti sul fascicolo sanitario elettronico 2.0*, in *Resp. medica*, 2024, I, 57 – 68). In linea di principio, al fascicolo i sanitari possono accedere solo con il consenso esplicito dell'assistito (salvo casi di emergenza: artt. 8 e 20); non sono visibili i «dati soggetti a maggiore tutela dell'anonimato» (elencati nell'art. 6 d.m. cit., ad es., la sieropositività all'HIV), salva diversa determinazione dell'interessato. L'alimentazione (art. 12) delle informazioni non richiede il consenso dell'assistito, il quale può però esercitare un diritto all'oscuramento di alcuni dati, peraltro sempre revocabile (art. 9). Lo stesso interessato può aggiungere, in una sezione particolare del fascicolo (c.d. «taccuino personale») alcuni dati ulteriori, «anche generati dai dispositivi medici e/o wearable» (art. 5).

[85] Ai sensi dell'art. 11 Reg. UE 2025/327. Tali dati possono comprendere quelli raccolti dalle applicazioni per il benessere che offrono l'interoperabilità con la infrastruttura tecnica della cartella clinica: art. 48 Reg. UE 2025/327, il quale precisa che, in ogni caso, la condivisione la trasmissione di tali dati deve basarsi sul consenso della persona fisica.

[86] Alla luce dei principi di minimizzazione e di limitazione della finalità, l'accesso è limitato per entità ed estensione alla funzione di cura prestata dal professionista. Su invito del Parere congiunto dell'EDPB e dell'EDPS (ivi,18 s.), era stato precisato da un emendamento del Parlamento europeo all'art. 4, par. 3, dell'originaria proposta che il trattamento è lecito in forza della base giuridica di cui all'art. 9, par. 2, lett. h), GDPR (e nei limiti della medesima, senza la necessità del consenso). Nonostante tale precisazione non sia

salve limitazioni poste dai pazienti medesimi[87], i quali non sono invece tenuti ad un'azione positiva per rendere possibile la fruizione delle informazioni che li riguardano[88].

7. Osservazioni conclusive. La declinazione al plurale della portabilità e la sua rilevanza al di fuori della disciplina dei dati.

Se si guarda dalla prospettiva dell'interessato (data subject), il diritto alla portabilità sui propri dati personali, nei pochi anni di vita a far data dalla sua codificazione nell'art. 20 GDPR, ha conosciuto una evoluzione significativa, grazie ai numerosi interventi legislativi che, affinandone le potenzialità, ne hanno via via esteso l'ambito di applicazione (per un verso, quanto all'oggetto, includendo chiaramente, oltre ai dati forniti, quelli osservati e, persino, in certi casi, quelli inferenziali; per altro verso, superando, quanto a presupposti, il riferimento alle basi giuridiche del consenso o dell'esecuzione del contratto). In linea con la dimensione di compromesso del diritto (tra interesse della persona fisica e interessi contrapposti del titolare del trattamento, da un lato, e tra quello che rappresenta l'ottimo ideale sul piano degli obiettivi e la realtà della tecnica e la condizione economica delle imprese, dall'altro), il rafforzamento della portabilità non è stato generalizzato, ma ha riguardato, per così dire a macchia di leopardo, diverse realtà, alla luce ora della tipologia dei soggetti coinvolti (ad esempio i gatekeeper, per la posizione che essi hanno sul mercato), ora del tipo di dati oggetto della disciplina (ad esempio, i dati raccolti dall'IoT), ora del particolare settore a cui questi si riferiscono (i cc.dd. spazi europei dei dati, ad iniziare da quello dei dati sanitari). L'espansione della portabilità ha assunto diverse forme: in alcuni casi, il legislatore europeo ha fissato, nella veste di una sorta di obblighi di risultato, determinati standard qualitativi che superano quelli della 'versione base' dell'art. 20 GDPR (art. 6, par. 9, DMA); ancora, in molti casi, sono stati previsti diritti che si affiancano alla portabilità originaria, finendo per 'integrarla' nel perimetro in cui le due situazioni soggettive coincidono, ma disvelando altresì un contenuto che va ben oltre. Mentre l'estensione ai dati non personali è sempre più frequente, tali diritti concernono, in alcuni casi (art. 6, par. 10, DMA e art. 5 DA), financo dati personali di terzi.

---

più ripresa, almeno in termini chiari, dal Regolamento, si può confermare tale conclusione anche nel nuovo assetto, movendo specialmente dalla valorizzazione della volontà negativa del paziente: v. *infra*.

[87] Artt. 8 e 10 Reg. UE 2025/327, che prevedono rispettivamente il diritto di limitare l'accesso dei professionisti sanitari e dei prestatori di assistenza sanitaria ai dati sanitari elettronici personali e un diritto, che può essere introdotto dagli Stati membri e che deve essere reversibile, di esclusione dall'accesso ai dati sanitari elettronici personali nel contesto dell'uso primario.

L'art. 10, par. 2, Reg. UE 2025/327 precisa che «gli Stati membri possono prevedere che un prestatore di assistenza sanitaria o un professionista sanitario possa accedere ai dati sanitari elettronici personali nei casi in cui il trattamento sia necessario per tutelare gli interessi vitali dell'interessato o di un'altra persona fisica conformemente all'articolo 9, paragrafo 2, lettera c), del regolamento (UE) 2016/679, anche se il paziente ha esercitato il diritto di esclusione riguardo all'uso primario».

[88] V. A. Morace Pinelli, *Lo spazio europeo dei dati sanitari*, cit., 1025.

Le persone fisiche possono inserire nella propria cartella clinica elettronica dati relativi alla loro salute: questi devono essere contraddistinti per la loro provenienza e in nessun caso possono alterare i dati inseriti dai professionisti sanitari (art. 5 Reg. UE 2025/327), ferma la possibilità di esercitare il diritto di rettifica (art. 6 Reg. UE 2025/327).

Ne discende una declinazione al plurale della portabilità, che si afferma già sul piano della tutela dell'individuo e del controllo che questo deve potere esercitare sui propri dati, ma che lo trascende, disvelando una prospettiva nuova con la quale il legislatore europeo guarda ai dati.

Nella direzione del rafforzamento del controllo dell'individuo sui propri dati, va segnalato che, nella *Dichiarazione europea sui diritti e i principi digitali per il decennio digitale*, proclamata solennemente dalla Commissione, dal Parlamento e dal Consiglio, le Istituzioni dell'Unione si sono impegnate, tra le altre cose, «a garantire l'effettiva possibilità per i singoli individui di trasferire facilmente i propri dati personali e non personali tra diversi servizi digitali, in linea con i diritti di portabilità» (Capitolo V, "Vita privata e controllo individuale sui dati")[89].

Più in generale, emerge chiaramente, dal rapido incedere legislativo, la tendenza all'emancipazione della portabilità dalla logica e dai confini della tutela dei data subject, per divenire, altresì, veicolo di trasmissione anche di dati non personali (nei limiti in cui chi ne ha interesse sia legittimato a domandarla), fino a dare forma ad una pretesa esercitabile anche da un titolare del trattamento, purché ricorra una base giuridica ai sensi del GDPR (art. 6 oltre che, in caso di informazioni sensibili, un'eccezione al divieto di trattamento di cui all'art. 9 del Regolamento) che legittimi una simile operazione sui dati personali altrui. Il tutto senza trascurare che, in taluni settori, il trasferimento dei dati si giustifica in via automatica, ciò che richiede, anche in questo caso (nella misura in cui si abbia a che fare con dati personali), una base giuridica.

In questa veste plurale, la portabilità dei dati si è così progressivamente consolidata come uno degli assi portanti dell'economia europea dei dati[90]. Nel continuo e complesso bilanciamento tra protezione della persona ed esigenze di circolazione, prendono piede meccanismi di condivisione dei dati sempre più articolati[91], che enfatizzano la natura strumentale delle informazioni rispetto ad obiettivi che si iscrivono sia all'interno della sfera della personalità (come nel caso del diritto alla salute), sia nella logica di mercato (potenziare il consumatore, favorire lo sviluppo di nuovi servizi, incentivare la concorrenza).

Alla complessità delle dimensioni della portabilità e al collegamento funzionale dei dati con finalità ulteriori, si collega inevitabilmente la necessità, da parte degli interpreti e degli operatori, di ampliare lo sguardo, uscendo dal diritto dei dati in senso stretto, per esaminare anche gli ambiti rispetto ai quali questo è contiguo.

Due esempi riguardano la tutela del diritto dei consumatori e del mercato, dalla cui prospettiva può divenire rilevante il mancato raggiungimento di determinati standard qualitativi della portabilità dei dati, e ciò persino dove la normativa ad essa dedicata non è ancora giunta ad imporre obblighi specifici in termini di risultati da garantire all'interessato (ad esempio, con riguardo alla interoperabilità).

---

[89] Sul valore programmatico della Carta, sulle orme della Carta dei diritti fondamentali dell'Unione europea, proclamata a Nizza nel dicembre del 2000, v. G. ALPA, *La dichiarazione europea dei diritti digitali*, in *Contratto e impresa Europa*, 2023, II, 182 ss.

[90] Accesso ai dati, interoperabilità e portabilità transfrontaliera dei dati sono tra gli obiettivi dell'attività legislativa europea in materia di dati, come si legge nella Risoluzione del Parlamento europeo del 25 marzo 2021 su una strategia europea per i dati (2021/C494/04).

[91] G. MARINO, *op. cit.*, 53 ss.

Con riguardo ai consumatori, la dottrina tedesca ha già messo in evidenza che l'utilizzo da parte di fornitori di contenuti o servizi digitali di formati per i dati personali trattati che compromettono l'interoperabilità e, dunque, l'effettività del diritto alla portabilità *ex* art. 20 GDPR, può rilevare nei termini di un difetto di un requisito di conformità – in relazione a ciò che può normalmente attendersi il consumatore – dell'oggetto dell'acquisto [92]. Sul versante della tutela della concorrenza, infine, è emersa, anche prima del DMA, la prospettiva che rinviene un possibile abuso di posizione dominante nelle condotte delle piattaforme digitali che ostacolano la portabilità effettiva dei dati dei propri utenti, impedendo loro di estrarli e di trasmetterli alle imprese concorrenti, e così finendo per ledere principalmente la contendibilità del mercato[93].

---

[92] M. SCHMIDT-KESSEL, *La responsabilità contrattuale del gestore di una piattaforma per la protezione dei dati personali del cliente nella prospettiva dei requisiti di qualità dell'adempimento*, in *Pactum*, 2023, 153 – 162: 159; M. DÜMELAND, *Sachmangelhaftigkeit von Software bei nicht DSGVO-konformer Entwicklung*, in *DSRI-Tagungsband*, 2018, Edewecht, 649. Che la violazione delle regole sul trattamento dei dati personali possa tradursi in un difetto di conformità (arg. *ex* considerando 48 dir.) è del resto chiaro anche alla dottrina italiana: v. già C. CAMARDI, *Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali. Operazioni di consumo e circolazione di dati personali*, in *Giust. civ.*, 2019, III, 514; C. IRTI, *Consenso negoziato e circolazione dei dati personali*, Torino, 2021, 140.

[93] L'AGCM, su segnalazione di una società operativa nel mercato emergente dell'intermediazione dei dati (e la cui attività si fonda, in particolare, sull'esercizio del diritto alla portabilità da parte degli utenti di grandi piattaforme digitali, al fine di raccogliere i dati da questi condivisi e investirli riversando sugli stessi utenti buona parte dei profitti), ha avviato il 5 luglio 2022 un'istruttoria contro Google-Alphabet (provvedimento disponibile al sito https://www.agcm.it/dotcmsCustom/getDominoAttach?urlStr=192.168.14.10:8080/41256297003874BD/0/B7FC348D8D737417C1258883004DD3E7/$File/p30215.pdf; sul caso, v. S. TROIANO, *Potential and Limitations of the Right to Data Portability Eight Years after the Adoption of the GDPR*, in AA. VV., *Recht der Digitalisierung II*, a cura di P. ANZENBERGER e K. SCHWAIGHOFER, Tübingen, 2025, 176 s.), rilevando che il servizio da questo creato per consentire ai propri utenti l'esercizio del diritto alla portabilità (*Google Takeout*) non fosse sufficiente a garantire l'effettività di questo diritto, a causa della farraginosità del servizio e della necessità di un continuo intervento da parte degli interessati. Nella sostanza, sono stati rilevati «ostacoli all'individuazione di meccanismi di interoperabilità idonei a rendere i dati presenti nella (…) piattaforma disponibili a piattaforme alternative», così determinando «un indebito sfruttamento (…) dei consumatori finali». Tale condotta limiterebbe i «benefici che i consumatori potrebbero trarre dalla valorizzazione dei loro dati personali», oltre che «la possibilità di operatori alternativi a Google di sviluppare forme innovative di utilizzo» degli stessi, così consentendo a Google di «preservare la propria posizione nello sfruttamento commerciale della mole dei dati personali resi a essa disponibili attraverso la posizione detenuta su una varietà di mercati digitali». Il presupposto del ragionamento dell'Autorità è che la portabilità configuri «uno strumento normativo teso a garantire il pieno esplicarsi di dinamiche competitive nell'ambito dei mercati digitali». Con successivo provvedimento del 18 luglio 2023 (://www.agcm.it/dotcmsCustom/getDominoAttach?urlStr=192.168.14.10:8080/41256297003874BD/0/42A8996C723B26AAC12589FD003925C3/$File/p30736.pdf), l'AGCM ha reso vincolanti gli impegni assunti da Google, i quali, nella sostanza, vertono, sullo sviluppo dell'automatizzazione di *Takeout* e sul miglioramento dei meccanismi di interoperabilità che assicurino alle altre piattaforme l'accessibilità ai dati raccolti da Google. È previsto, infine, il rilascio di una soluzione di portabilità diretta da servizio a servizio, tramite un API (*Application Programming Interface*). Da ultimo il progetto è stato ribadito da Oliver Bethell, *Legal Director* presso Google, nel post «*Un aggiornamento su come ci stiamo preparando al Digital Markets Act*», pubblicato il 17 gennaio 2024 sul Blog di Google Italy (https://blog.google/intl/it-it/notizie-aziendali/un-aggiornamento-su-come-ci-stiamo-preparando-al-digital-markets-act), soprattutto in vista dell'obiettivo di adeguarsi all'obbligo di portabilità effettiva a cui la stessa Google (Alphabet) è soggetta in base al DMA in quanto *gatekeeper* (*supra*, par. 3). Oltre a *Takeout*, è stata altresì richiamata la *Data Transfer Initiative*, organizzazione di esperti creata su impulso di Apple, Meta, and Google per la creazione di soluzioni interoperabili finalizzate all'attuazione della portabilità diretta (https://dtinit.org/). Un successivo post dello stesso autore sul medesimo blog («*Come ottemperiamo al Digital Markets Act*», pubblicato il 5 marzo 2024, https://blog.google/intl/it-it/come-ottemperiamo-al-digital-market-acts) ha annunciato il lancio della "Data Portability API per gli sviluppatori". Sul possibile collegamento tra la portabilità e l'abuso di posizione dominante v. pure da H. SCHWEITZER, A. METZGER, *Data Access under the Draft Data Act, Competition Law and the DMA: Opening the Data Treasures for Competition and Innovation?*, in *GRUR International*, 2023, IV, 340 ss.