



Collana di Diritto Digitale

Dipartimento di Ingegneria dell'Impresa

Università degli Studi di Roma "Tor Vergata"

Direttore: Arnaldo Morace Pinelli

6

SANITÀ DIGITALE

Regolamento "EHDS" (UE 2025/327)

sullo spazio europeo dei dati sanitari

I

Uso dei dati e assetti organizzativi

a cura di

Arnaldo Morace Pinelli

Collana di Diritto Digitale

Dipartimento di Ingegneria dell'Impresa dell'Università degli Studi di Roma "Tor Vergata"

Diretta da:

Prof. Arnaldo Morace Pinelli

Comitato scientifico: Prof. Agostino La Bella, Prof. Nathan Levialdi Ghiron, Prof. Vincenzo Tagliaferri, Prof. Roberto Basili, Prof. Massimiliano Caramia, Prof. Andrea Clementi

Responsabile della redazione: Prof. Valentina Bellomia

Il presente Volume si inserisce nell'ambito delle attività della Cattedra Jean Monnet di "European Digital Law of the Person, of the Contract and of the Technological Marketplace", istituita presso il Dipartimento di Ingegneria dell'Impresa dell'Università di Roma "Tor Vergata".

Il Volume trae spunto dal Convegno "Sanità digitale. Regolamento sullo spazio europeo dei dati sanitari e fonti interne", organizzato dalla Università di Roma "Tor Vergata" e svoltosi a Roma il 21 e 22 marzo 2025.

© Copyright 2025 by Pacini Editore Srl

ISSN 3034-9397

ISBN 978-88-3379-928-5

Realizzazione editoriale



Via A. Gherardesca
56121 Pisa

Responsabile di redazione

Valeria Savallo

Fotolito e Stampa

IGP Industrie Grafiche Pacini

Le fotocopie per uso personale del lettore possono essere effettuate nei limiti del 15% di ciascun volume /fascicolo di periodico dietro pagamento alla SIAE del compenso previsto dall'art. 68, commi 4 e 5, della legge 22 aprile 1941 n. 633.

Intermediazione di dati sanitari e diritto alla portabilità

SOMMARIO: 1. Inquadramento e obiettivi dell'analisi. – 2. Intermediazione di dati personali e diritto alla portabilità nel GDPR e criticità emergenti dalla prassi operativa. – 3. La risposta europea in tema di intermediazione dei dati e la sua regolamentazione nel *Data Governance Act*. – 4. Connessioni e ricorrenze tra disciplina in tema di spazio europeo di dati sanitari nel nuovo Regolamento EHDS e disciplina del fenomeno di *data intermediation* negli impianti normativi precedenti (GDPR e DGA). – 4.1. Il diritto alla portabilità nel Reg. EHDS e nel GDPR. – 4.2. La delega tra ammissibilità e limiti. – 5. *European Health Data Space* e *data intermediation*.

1. Inquadramento e obiettivi dell'analisi

Il tema relativo al rapporto tra intermediazione di dati sanitari e diritto alla portabilità si colloca nel punto di intersezione di ambiti normativi distinti, ma intimamente connessi, tra i quali vanno annoverati il *Data Governance Act*¹, che disciplina, *inter alia*, l'intermediazione dei dati in forma non cooperativa e in forma cooperativa, il GDPR (*General Data Protection Regulation*), che all'art. 20 ha introdotto il diritto alla portabilità dei dati personali quale nuovo diritto per l'interessato, ed il nuovo regolamento EHDS (*European Health Data Space*), che è intervenuto nuovamente sul diritto alla portabilità con integrazioni specificamente dedicate agli spazi di condivisione di dati sanitari, preservando comunque l'impianto del GDPR, che è rimasto inalterato. Si può dire che, sul punto, l'EHDS introduce, in tale ambito, un segmento ulteriore di normazione, che va tuttavia coordinato con le altre fonti sul piano sistematico. La rilevanza del diritto alla portabilità dei dati è ben presente al legislatore europeo, che lo menziona e lo regola anche in altre

¹ Reg. UE 2022/868 del 30 maggio 2022 relativo alla governance europea dei dati e che modifica il regolamento UE 2018/1724 (Regolamento sulla *governance* dei dati).

fonti normative, tra cui il DMA (*Digital Markets Act*)² per i *gatekeepers* ed il *Data Act*³.

La portabilità dei dati è di particolare interesse in relazione all'intermediazione dei dati⁴, fenomeno nel quale un soggetto si interpone tra *data users*, da un lato, e *data subjects* o *data holders*, dall'altro lato, favorendo la circolazione dei dati e, al contempo, svolgendo un ruolo di tutela dei superiori interessi dell'interessato, consentendo a quest'ultimo di esercitare un maggior controllo sui propri dati personali, anche nella prospettiva della *data governance* e della *data valorisation*⁵.

La rilevanza del ruolo degli intermediari di dati è stata sottolineata anche dalla Commissione europea nella Comunicazione dedicata ad una strategia europea per i dati⁶, a cui ha fatto seguito anche la relativa Risoluzione del Parlamento europeo⁷.

La Commissione aveva rimarcato, con riguardo al potere delle persone di avere un maggiore controllo dei propri dati, che «È opportuno sostenere ulteriormente le persone nell'esercizio dei loro diritti per quanto riguarda l'utilizzo dei dati che generano, dando loro la possibilità di controllare i propri dati attraverso strumenti e mezzi per poter decidere di volta in volta in dettaglio ciò che può essere fatto con essi ("spazi di dati personali")».

Il diritto alla portabilità è già da tempo disciplinato nell'art. 20 del GDPR. La Commissione, nella Comunicazione di due anni successiva all'applicazione di tale regolamento, ha sostenuto che, proprio al predetto fine di rinviare ulteriormente la *governance* dell'interessato sui propri dati personali, «si potrebbe rafforzare, per le persone, il drit-

² Reg. UE 2022/1925 del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le dir. (UE) 2019/1937 e UE 2020/1828 (Regolamento sui mercati digitali).

³ Reg. UE 2023/2854 del 13 dicembre 2023 riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il regolamento UE 2017/2394 e la dir. UE 2020/1828 (Regolamento sui dati).

⁴ In materia si rimanda a BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in *Contratto e impresa Europa*, 2021, 1, 199-256; BRAVO, *Il commercio elettronico dei dati personali*, in PASQUINO, RIZZO, TESCARO (a cura di), *Questioni attuali in tema di commercio elettronico*, Napoli, 2020, 83-130.

⁵ In tal senso si veda, con riguardo al settore pubblico, BRAVO, VALERO TORRIJOS, *Data in the Public Sector and Data Valorisation*, in *European Review of Digital Administration & Law (ERDAL)*, 2022, Vol. 3, Issue 2, 5-8.

⁶ Commissione della Commissione europea al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni del 19 febbraio 2020 dal titolo «Una strategia europea per i dati» (COM(2020)0066).

⁷ Risoluzione del Parlamento europeo del 25 marzo 2021 su «Una strategia europea per i dati» (2020/2217(INI)), pubblicata in GUUE dell'8 dicembre 2021, C-494/37.

to alla portabilità di cui all'articolo 20 del RGPD, offrendo loro un maggiore controllo su chi può accedere ai dati generati automaticamente e utilizzarli, ad esempio mediante requisiti più rigorosi per le interfacce di accesso ai dati in tempo reale e rendendo i formati leggibili meccanicamente obbligatori per i dati relativi a determinati prodotti e servizi, ad esempio i dati provenienti da elettrodomestici o dispositivi indossabili intelligenti. Inoltre potrebbero essere prese in considerazione norme per i fornitori di applicazioni che utilizzano dati personali o per i *nuovi intermediari di dati*, come i *fornitori di spazi di dati personali*, che garantiscano il loro ruolo di *intermediari neutrali*. Si tratta di temi che possono essere ulteriormente esaminati nel contesto della legge sui dati menzionata in precedenza. Il programma Europa digitale sosterrà inoltre lo sviluppo e il lancio di “*spazi di dati personali*”⁸.

È chiara la connessione tra portabilità dei dati e *data intermediaries*, con un ventaglio di figure che possono ambire a svolgere tale ruolo. Nella visione strategica della Commissione europea, del 2020, i «fornitori di spazi di dati personali», dunque, si vengono già a configurare come «nuovi intermediari di dati», che si vanno ad aggiungere ad altri intermediari indipendenti, operanti o meno in forma cooperativa, che contribuiscono a valorizzare il riuso dei dati ben al di là delle finalità di primo utilizzo, fornendo nuovi strumenti di controllo per gli interessati e ponendosi al contempo come volano per lo sviluppo socio-economico e la ricerca, nella prospettiva del *secondary use*⁹.

⁸ V. p. 23, Comunicazione cit.

⁹ A p. 11 della Comunicazione cit., la Commissione ha avuto modo di precisare anche che «le persone apprezzano l'elevato livello di protezione garantito dal RGPD e dalla normativa sull'*ePrivacy*, pur risentendo dell'assenza di norme e strumenti tecnici che rendano l'esercizio dei loro diritti più semplice e non eccessivamente oneroso. Le potenzialità dell'articolo 20 del RGPD in termini di abilitazione di nuovi flussi di dati e promozione della concorrenza sono riconosciute in relazioni destinate alla Commissione e ai governi degli Stati membri, come pure al di fuori dell'UE. La concezione di tale articolo, tuttavia, privilegiando il cambiamento di fornitori del servizio a scapito del riutilizzo dei dati negli ecosistemi digitali, impone limiti pratici al diritto in questione. Dato che quando utilizzano dispositivi IoT e servizi digitali i consumatori generano quantità sempre crescenti di dati, essi stessi possono essere confrontati a rischi di discriminazione, pratiche sleali e effetti di dipendenza (“*lock-in*”). Alla base delle disposizioni sull'accesso ai dati e il loro riutilizzo contenute nella direttiva sui servizi di pagamento vi sono considerazioni in materia di autonomia dei consumatori e innovazione. In risposta a questa situazione sono stati formulati (dal movimento *MyData* e da altri soggetti) inviti a fornire alle persone gli strumenti e i mezzi per decidere di volta in volta in dettaglio come sono utilizzati i loro dati. Ciò fa sì che si profilino notevoli vantaggi per i cittadini, in particolare per quanto riguarda la salute e il benessere, il miglioramento delle finanze personali, la riduzione dell'impronta ambientale, un accesso semplice e rapido a servizi pubblici e privati e un controllo e una trasparenza

Anche il Parlamento, nella propria risoluzione del 2021, ha evidenziato «il ruolo fondamentale degli intermediari dei dati in quanto facilitatori strutturali dell'organizzazione dei flussi di dati»¹⁰ ed ha dichiarato di voler «accoglie[re] favorevolmente i piani della Commissione per la classificazione e la certificazione degli intermediari in vista della creazione di ecosistemi di dati interoperabili e non discriminatori (...)»¹¹.

La figura degli intermediari di dati e la connessione tanto con il diritto alla *data portability* quanto con la disciplina degli spazi di dati personali è stata oggetto di interventi normativi volti a dare concretamente attuazione alle linee strategiche della Commissione e se ne trova traccia anche nel nuovo Regolamento europeo sugli spazi di condivisione di dati sanitari (*European Health Data Space*, EHDS), che tuttavia sul punto presenta una disciplina non scevra da ambiguità e non esaustiva, con tratti fortemente distintivi in ragione della forte specificità del suo ambito di normazione. Basti pensare che il *considerando* n. 59 dell'EHDS fa testuale riferimento a «intermediari di dati sanitari [che] svolgono compiti diversi da quelli dei servizi di intermediazione dei dati nell'ambito del regolamento (UE) 2022/868»¹².

I differenti piani normativi che intervengono sul tema oggetto di quest'analisi – dedicata all'intermediazione dei dati e alla loro portabilità nel settore sanitario – richiedono una disamina critica di carattere sistematico, volta a ripercorrere trasversalmente i tratti connotanti della disciplina di settore nei principali ambiti di regolamentazione, per poi affrontare aspetti critici e prospettive di soluzioni con riguardo alla più recente disciplina europea degli spazi di condivisione di dati sanitari.

2. Intermediazione di dati personali e diritto alla portabilità nel GDPR e criticità emergenti dalla prassi operativa

La connessione tra intermediazione di dati e diritto alla portabilità ha avuto avvio con l'originale previsione, nell'art. 20 del GDPR, del diritto alla portabilità dei dati, quale inedito diritto dell'interessato

maggiori in relazione ai propri dati personali. Tra tali strumenti e mezzi figurano strumenti per la gestione del consenso, *app* per la gestione delle informazioni personali, comprese soluzioni completamente decentralizzate basate sulla *blockchain*, come pure cooperative o *trust* per i dati personali, che agiscono da intermediari neutrali di nuova concezione nell'economia dei dati personali. Si tratta di strumenti ancora in una fase embrionale, che mostrano tuttavia potenzialità significative e necessitano di un contesto favorevole».

¹⁰ V. par. 25, Risoluzione cit.

¹¹ V. par. 25, Risoluzione cit.

¹² *Considerando* n. 59, Regolamento EHDS.

nell'ambito di quelli previsti dalla disciplina sulla protezione dei dati personali.

Rispetto al precedente impianto normativo di cui alla dir. 95/46/CE, l'innovazione è stata profonda. Il diritto alla portabilità mira, in primo luogo, ad attribuire un maggior potere di controllo in capo all'interessato, consentendogli di ottenere dati in formato strutturato, di uso comune, leggibili da dispositivo automatico e, dunque, dati immediatamente (ri)usabili. Mira altresì ad eliminare (o quantomeno ad arginare) l'effetto *lock-in*, ovvero la dipendenza tecnologica dell'interessato dal titolare del trattamento. Mira inoltre a favorire la circolazione dei dati nel mercato europeo e il loro riuso. Mira, infine, a favorire le dinamiche concorrenziali tra diversi fornitori di servizi, dato che l'interessato può chiedere al titolare del trattamento sia che i dati in formato strutturato siano trasferiti all'interessato medesimo, che potrà poi trasferirli ad altri titolari, sia che i dati siano trasmessi direttamente da un titolare ad un altro titolare, il quale, dunque, potrà addirittura subentrare al primo nella fornitura di un servizio basato su tali dati.

Al di là delle originarie aspettative del legislatore europeo, il diritto alla portabilità di cui all'art. 20 GDPR, prima ancora dell'emanazione del *Data Governance Act*, ha avuto un ulteriore effetto dirompente: ha contribuito alla nascita e all'affermazione di nuovi *player* sul mercato dei dati: gli intermediari di dati, ovvero i fornitori dei servizi di *data intermediation*, il cui rilevante ruolo strategico, manifestatosi nella prassi, ha successivamente indotto la Commissione europea a prenderli in considerazione nella citata Comunicazione sulla *Strategia europea per i dati* e, quindi, nella disciplina normativa sulla *governance* europea dei dati e nell'ulteriore regolamentazione di settore in tema di dati, anche in ambito sanitario.

L'avvento degli intermediari di dati sotto l'egida del GDPR è stato possibile mediante l'uso congiunto di due strumenti giuridici: il diritto alla portabilità di cui all'art. 20 e la delega dell'interessato all'intermediario, che consentisse a quest'ultimo di agire per conto del primo, al fine di richiedere ed ottenere i dati personali da utilizzare per ulteriori finalità.

Seppur con talune differenze da intermediario a intermediario, lo schema operativo generalmente applicato prevede i seguenti *step*: (i) l'intermediario, in fase di contrattualizzazione del rapporto con il proprio cliente (che riveste il ruolo di interessato al trattamento di dati posto in essere da un soggetto terzo, titolare del trattamento e fornitore di servizi), si fa conferire da questi la delega per l'esercizio del diritto

alla portabilità nei confronti del titolare del trattamento; (ii) ottenuta la delega, l'intermediario richiede al titolare del trattamento, per conto dell'interessato, il trasferimento diretto dei dati presso di sé, mettendoli a disposizione dello stesso interessato per successivi utilizzi; (iii) l'intermediario reitera le richieste verso altri titolari del trattamento, fornitori di servizi, collazionando ulteriori dati presso di sé per conto dell'interessato, mettendoglieli a disposizione; (iv) d'accordo con il cliente-interessato, l'intermediario attiva strategie di valorizzazione, ovvero di riuso, dei dati personali con soggetti terzi (*data users*), a beneficio anche dei medesimi interessati, in una logica "*win-win*", ottenendo remuneratività e altri vantaggi, con trattenimento di una quota concordata con i propri clienti (ad es. 10%) quale commissione per l'attività di intermediazione.

Generalmente l'intermediario, acquisiti i dati da un certo numero di clienti-interessati, rende accessibile ai *data users* – pubbliche amministrazioni, università, imprese, enti non lucrativi – l'insieme dei dati in forma aggregata ed anonimizzata, per analisi statistiche, scientifiche o di mercato.

A ben guardare, attraverso l'uso congiunto della portabilità dei dati e della delega, gli aspetti innovativi che sono emersi nella prassi sono almeno tre:

- (a) per un verso si è avuta l'affermazione di nuovi *player* europei, in un mercato dominato dalle multinazionali straniere, soprattutto americane, nel quale l'intermediario, dotato di mezzi e *know-how* adeguati, riesce ad acquisire con una certa facilità e senza eccessivi sforzi, da una pluralità di titolari del trattamento e fornitori di servizi, i dati personali che questi ultimi hanno raccolto nel tempo con ingenti risorse e che ora, in tal modo, cumulati, ritornano (anche) nella disponibilità degli stessi interessati;
- (b) per altro verso si è avuta anche l'emersione del ruolo attivo, potenzialmente tutorio, dell'intermediario di dati, che, agendo per conto dell'interessato e meglio attrezzato di quest'ultimo, può assisterlo nell'esercizio dei suoi diritti e nella cura dei suoi interessi;
- (c) v'è poi da considerare anche la (parziale) effettiva riappropriazione di poteri e facoltà, da parte degli interessati, sui propri dati personali, grazie all'azione svolta dall'intermediario. Gli interessati, grazie a tale nuovo *player* ed all'utilizzo della *data portability*, ottengono la disponibilità dei propri dati collazionandoli da sorgenti e fornitori diversi, con la possibilità di negoziare in proprio favore, tramite la capacità dell'intermediario, l'utilizzo secondario dei dati perso-

nali che intendono veicolare a soggetti terzi, nelle forme adeguate a garantire la loro tutela. Generalmente i *providers*, nel fornire i diversi servizi (navigazione *online*, *social network*, motori di ricerca, mappe satellitari e geolocalizzazione, etc.) raccolgono una grande mole di dati che riutilizzano a proprio vantaggio in un mercato secondario di dati, da cui l'interessato viene estromesso, lasciandogli, quale esclusivo beneficio, il solo servizio con cui viene acquisita la disponibilità materiale dei dati¹³. L'intervento dell'intermediario, viceversa, consente all'interessato, suo tramite, non solo di riottenere la disponibilità materiale di quei dati, "rastrellandoli" da una molteplicità di *providers* titolari del trattamento e concentrandoli in un unico contesto, ma anche di riappropriarsi delle possibilità di *governance* del loro utilizzo secondario, possibile proprio grazie alla capacità tecnica dell'intermediario. In tal modo si può rendere effettiva quell'autodeterminazione informativa da cui l'interessato finiva per essere "espropriato" e di cui ora, grazie al ruolo dell'intermediario, riesce a "riappropriarsene".

Accanto alle evidenti potenzialità dell'intermediazione dei dati v'è anche qualche preoccupazione, dovuta sia al quadro regolamentare ancora incerto ai tempi dell'emanazione e della prima applicazione del GDPR su tale specifica materia, sia ai potenziali nuovi rischi che possono emergere dal fenomeno in esame, non adeguatamente ponderati in sede di emanazione del Regolamento sulla *data protection*.

Il Garante per la protezione dei dati personali, in Italia, ha iniziato a prendere cognizione del fenomeno al momento di prima emersione delle segnalazioni sull'operato di un intermediario di dati con sede a Milano, inoltrate nei primi mesi del 2019 da operatori della grande distribuzione commerciale. Costoro, nella loro qualità di titolari del trattamento, si erano visti rivolgere numerose richieste di portabilità dei dati in favore dell'intermediario medesimo, per delega dei propri clienti, secondo lo schema sopra richiamato e, dubitando della liceità dell'operazione, tra l'altro non gradita, l'avevano prontamente segnalata all'Autorità di settore.

Il Garante per la protezione dei dati personali, sotto la presidenza di Antonello Soro, avviata l'istruttoria, decideva di interessare della questione l'EDPB, ritenendo che il tema fosse di interesse europeo e non esclusivamente nazionale.

¹³ ZENO ZENCOVICH, *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, in *Media Laws*, 2018, 1 ss.; RESTA, ZENO ZENCOVICH, *Volontà e consenso nella fruizione dei servizi in rete*, in *Riv. trim. dir. e proc. civ.*, 2018, 411 ss.

Nella nota di trasmissione al Comitato europeo veniva evidenziato che «si tratta di una questione molto rilevante che, pur venuta in evidenza in Italia, impone una riflessione generale che non può essere rimessa alle singole autorità di protezione dati. Il caso riguarda l'applicazione del diritto alla portabilità dei dati: un'impresa italiana si è infatti proposta come intermediaria nel rapporto fra titolari ed interessati chiedendo, su delega di questi ultimi, di ottenere le informazioni personali custodite presso importanti soggetti imprenditoriali, in particolare nel settore della grande distribuzione al fine di riunirle all'interno di una propria banca dati da sottoporre ad *enrichment*. Il tema è dunque legato alla "commercibilità" dei dati, con l'ulteriore complicazione dell'esercizio per delega del diritto ed il conseguente non remoto rischio di possibili duplicazioni delle banche dati oggetto di portabilità»¹⁴.

La discussione innanzi all'EDPB non sarebbe stata affrontata da Antonello Soro, per via della scadenza del mandato. Nel Comunicato stampa relativo a tale questione, il Garante chiariva che «(...) attenderà dunque il parere dell'EDPB per concludere l'istruttoria»¹⁵ e che «Nel frattempo, i soggetti privati che riceveranno le richieste di portabilità dei dati da parte (...) [dell'intermediario] dovranno operare nel rispetto del principio di *accountability* stabilito dal Regolamento Ue e valutare se ottemperare alle richieste o motivare un eventuale rifiuto»¹⁶.

3. La risposta europea in tema di intermediazione dei dati e la sua regolamentazione nel *Data Governance Act*

Nell'attesa, il Garante rinunciava espressamente dunque a prendere una propria posizione sui temi sopra evidenziati, così come a fornire indicazioni agli operatori, lasciandoli "soli" di fronte ai nuovi problemi applicativi sollevati dalla prassi, nell'attesa di un intervento di respiro europeo.

¹⁴ Lettera del Presidente del Garante per la protezione dei dati personali al Presidente dell'*European Data Protection Board* (EDPB), avente ad oggetto «*Richiesta di parere in tema di commercializzazione dei dati personali e diritto alla portabilità*» (Garante per la protezione dei dati personali, doc web n. 9126725 del 1° agosto 2019, reperibile online all'indirizzo <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9126725>, consultato da ultimo in data 30 giugno 2025). Si veda anche, di ugual tenore, il Comunicato Stampa del 1° agosto 2019, «*Dati in cambio di soldi: il Garante privacy porta la questione in Europa. Sotto la lente dell'Autorità la app "Weople"*», consultabile all'indirizzo <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9126709>.

¹⁵ Garante per la protezione dei dati personali, *Comunicato stampa del 1° agosto 2019*, cit.

¹⁶ *Ibidem*.

Le iniziali preoccupazioni del Garante sul fronte domestico non sono sfociate, nell'immediatezza, in un'azione repressiva o sanzionatoria del fenomeno, né in altri interventi connotati dall'applicazione del meccanismo di cooperazione tra le diverse autorità di controllo nazionali, né, ancora, hanno dato adito ad interventi, anche solo di *soft law*, da parte dell'EDPB o dell'EDPS.

Una significativa risposta istituzionale sembra sia pervenuta in via legislativa, con l'emanazione del *Data Governance Act*¹⁷, ove, in linea con una progettualità delineata mediante la Comunicazione della Commissione sulla strategia europea per i dati, s'è provveduto a disciplinare il fenomeno della *data intermediation* agendo su tre piani distinti, che configurano tre diversi modelli di intermediazione:

- (a) quella affidata ad *enti pubblici*, che possono consentire il *riuso dei dati*, di cui hanno la disponibilità per fini istituzionali, mediante il consenso degli interessati ed avvalendosi di "organismi competenti", chiamati ad effettuare le operazioni tecniche necessarie per rendere disponibili i dati ai *data users*, per finalità commerciali e non commerciali, nel contesto di *ambienti controllati* e con possibilità di applicazione di tariffe *ad hoc* per garantire la sostenibilità del servizio;
- (b) quella affidata ai "*fornitori dei servizi di intermediazione dei dati*", ossia a soggetti che operano per scopi commerciali, raccogliendo dati provenienti da interessati e *data holders*, per renderli disponibili a terzi (*data users*), rispettivamente con il consenso degli interessati medesimi o con l'autorizzazione dei *data holders*, nel rispetto delle condizioni di liceità indicate dal GDPR¹⁸. Si tratta di attività di intermediazione che può essere svolta in forma tradizionale, mettendo in relazione soggetti estranei all'intermediario,

¹⁷ Per un commento al *Data Governance Act* si veda MORACE PINEALLI (a cura di), *Dalla «Data Protection» alla «Data Governance»: il regolamento (UE) 2022/868. Commentario al «Data Governance Act»*, Pisa, 2024.

¹⁸ Sull'intermediazione di dati, in particolare sulle connessioni che a tal riguardo si hanno tra il GDPR e il *Data Governance Act*, si veda BRAVO, *Il commercio elettronico dei dati personali*, cit., 83-130; BRAVO, *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in *Contratto e impresa Europa*, 2021, 1, 199-256; POLETTI, *Gli intermediari dei dati*, in *European Journal of Privacy Law & Technologies*, 2022, 1, 46 ss.; G. RESTA, *Pubblico, privato e collettivo nel sistema europeo di governo dei dati*, in *Riv. trim. dir. pubbl.*, 2022, 4, 971-995, e, *ivi*, spt. par. 5, ripubblicato anche all'interno del volume seguente: G. RESTA, ZENO ZENCOVICH (a cura di), *Governance off through data*, Roma, 2023, 605-630 e, *ivi*, spt. par. 5, 622 ss.; MORACE PINELLI, *Dalla «Data Protection» alla «Data Governance»: il Regolamento UE 2022/868*, in *Nuova giur. civ. comm.*, 2024, 2, 486 ss.

oppure in forma cooperativa, mediante vere e proprie cooperative di dati¹⁹, ove l'intermediario è soggetto che aggrega dati conferiti dai propri "membri" – generalmente "soci" della cooperativa di dati – che mantengono il controllo e la gestione dell'ente²⁰. L'intermediario è tenuto a notificare all'autorità competente (l'AgID, per l'Italia) l'intenzione di svolgere la propria attività di fornitore di servizi di intermediazione dei dati, rispettare determinate condizioni di mercato, previste dall'art. 12 del DGA, rimanendo soggetta all'azione di controllo della predetta *Authority*. Il modello di intermediazione ivi delineato impone al fornitore di agire in posizione neutrale, senza utilizzare per sé i dati personali nei cui confronti si pone come intermediario, ma assicurando comunque il perseguimento del superiore interesse degli interessati. Sicché questi ultimi, soprattutto in caso di cooperative di dati, si trovano di fronte ad un soggetto che li supporta nella selezione dei dati da condividere (e di quelli da escludere dalla condivisione), nell'esercizio dei propri diritti e nella negoziazione dei vantaggi a proprio favore, portando ad un rafforzamento significativo della loro posizione di interessati, sul piano economico, relativo alla posizione (di forza) sul mercato, e sul piano giuridico²¹;

¹⁹ In tema di cooperative di dati, disciplinate nel *Data Governance Act*, si veda F. BRAVO, *Le cooperative di dati*, in *Contratto e impresa*, 2023, 3, 757 ss.; L. PETRONE, *Il mercato digitale europeo e le cooperative di dati*, in *Contratto e impresa*, 2023, 3, 800 ss.; nonché i contributi raccolti all'esito del progetto di terza missione dell'Università di Bologna in materia di Cooperative di dati, nel volume BRAVO (a cura di), *EU Data Cooperatives. L'ingresso delle cooperative di dati nell'ordinamento europeo*, Torino, 2024.

²⁰ All'art. 2, par. 1, n. 15, del DGA si trova la definizione di «servizi di cooperative di dati», intesi quali «servizi di intermediazione dei dati offerti da una struttura organizzativa costituita da interessati, imprese individuali o da PMI, che sono membri di tale struttura, avente come obiettivi principali quelli di *aiutare i propri membri nell'esercizio dei loro diritti* in relazione a determinati dati, anche per quanto riguarda il *compiere scelte informate* prima di acconsentire al trattamento dei dati, di procedere a uno *scambio di opinioni* sulle finalità e sulle *condizioni del trattamento dei dati che rappresenterebbero al meglio gli interessi dei propri membri in relazione ai loro dati*, o di *negoziare i termini e le condizioni per il trattamento dei dati per conto dei membri* prima di concedere l'autorizzazione al trattamento dei dati non personali o prima che essi diano il loro consenso al trattamento dei dati personali».

²¹ Cfr. BRAVO, *Le cooperative di dati*, in *Contratto e impresa*, 2023, 3, 757 ss.; POLETTI, *Il quadro normativo del "Data Governance Act": l'esercizio dei diritti dell'interessato nell'attività di intermediazione dei dati*, in *Nuove leggi civ. comm.*, 2024, 3, 533 ss.; A. RICCI, SPANGARO, *La tutela dell'interessato nell'economia dei dati: il ruolo delle cooperative di dati*, in BRAVO (a cura di), *EU Data Cooperatives. L'ingresso delle cooperative di dati nell'ordinamento europeo*, Torino, 2024, 82 ss., nonché CARDINALI, *Tutela degli interessati e esercizio dei diritti: l'efficace intermediazione delle cooperative di dati*, in BRAVO (a cura di), *EU Data Cooperatives*, cit., 908 ss.

- (c) quella altruistica, affidata alle organizzazioni per l'altruismo dei dati, che si indirizza al soddisfacimento di obiettivi di interesse generale, inclusa l'assistenza sanitaria²². È una declinazione in senso solidaristico²³ dell'attività di intermediazione commerciale sui dati, la quale ultima, tuttavia, può emergere anche in tale settore qualora le organizzazioni per l'altruismo di dati perseguano, unitamente ad un intento altruistico-solaristico – che dunque non è esclusivo – anche un concomitante scopo lucrativo (puntando a stabilire anche relazioni commerciali tra *data users* e un numero indeterminato di interessati e *data holders*)²⁴.

L'intermediazione dei dati, a prescindere dal modello di riferimento, è strumento delineato per incentivare il riuso dei dati, esaltando quella libera circolazione delle informazioni, personali e non personali, che finora è risultata sottodimensionata, in quanto imbrigliata sia da vincoli normativi volti ad assicurare un rigido sistema di protezione dai rischi derivanti dal trattamento, sia da dinamiche di mercato chiuse, segnate da fenomeni di concentrazione in mano di pochi, desiderosi di sfruttare per sé il potenziale economico e dunque non incentivati a

²² L'*altruismo dei dati* viene definito, all'art. 2, par. 1, n. 16, del DGA, come «la condivisione volontaria di dati sulla base del consenso accordato dagli interessati al trattamento dei dati personali che li riguardano, o sulle autorizzazioni di altri titolari dei dati volte a consentire l'uso dei loro dati non personali, senza la richiesta o la ricezione di un compenso che vada oltre la compensazione dei costi sostenuti per mettere a disposizione i propri dati, per obiettivi di interesse generale, stabiliti nel diritto nazionale, ove applicabile, quali l'*assistenza sanitaria*, la lotta ai cambiamenti climatici, il miglioramento della mobilità, l'agevolazione dell'elaborazione, della produzione e della divulgazione di statistiche ufficiali, il miglioramento della fornitura dei servizi pubblici, l'elaborazione delle politiche pubbliche o la ricerca scientifica nell'interesse generale».

²³ Quanto al principio di solidarietà si vedano le insuperabili pagine di RODOTÀ, *Solidarietà. Un'utopia necessaria*, Roma-Bari, 2014 e di ALPA, *Solidarietà. Un principio normativo*, Bologna, 2022. Con riguardo alla declinazione di tale principio rispetto ai dati personali si rimanda a BRAVO, *Il principio di solidarietà*, in BRAVO (a cura di), *Dati personali. Protezione, libera circolazione e governance. – Vol. 1. Principi*, Pisa, 2023, 541-601; BRAVO, *Il principio di solidarietà tra data protection e data governance*, in *Dir. inf.*, 2023, 3, 481-518; BRAVO, *Il principio di solidarietà in materia di protezione dei dati personali nelle decisioni del Garante e della Corte di Cassazione*, in *Contratto e impresa*, 2023, 2, 405-441.

²⁴ Si veda, al riguardo, il tenore dell'art. 15 del DGA, rubricato «*Deroghe*», di chiusura del Capo III dedicato alla fornitura dei servizi commerciali di intermediazione dei dati, nel quale si trova statuito che «Il presente capo non si applica alle organizzazioni per l'altruismo dei dati riconosciute o ad altre entità senza scopo di lucro nella misura in cui le loro attività consistono nel cercare di raccogliere, per obiettivi di interesse generale, dati messi a disposizione da persone fisiche o giuridiche sulla base dell'altruismo dei dati, a meno che tali organizzazioni e entità non puntino a stabilire relazioni commerciali tra un numero indeterminato di interessati e titolari dei dati, da un lato, e utenti dei dati, dall'altro».

consentirne la circolazione o la condivisione in favore del concomitante interesse altrui o di quello generale.

A ben guardare il fenomeno del riuso dei dati detenuti da enti pubblici e da questi intermediati, in proprio o tramite altri “organismi competenti” che operano in ambienti sicuri di trattamento, è intimamente connesso a quello degli spazi di condivisione dei dati, enunciato con enfasi nella Comunicazione della Commissione europea su «*Una strategia europea per i dati*» e poi regolamentato, con riguardo ai dati sanitari, dal Regolamento EHDS (*European Health Data Space*)²⁵. Ne costituisce, in qualche modo, anche l’antecedente giuridico. Si tenga presente quanto ribadito nel *considerando* n. 24 del DGA, ove si trova affermato che «Al fine di creare fiducia nei meccanismi di riutilizzo, può essere necessario prevedere condizioni più rigorose per determinati tipi di dati non personali che possono essere ritenuti altamente sensibili in futuri specifici atti legislativi dell’Unione per quanto riguarda il trasferimento a paesi terzi, se tale trasferimento può compromettere obiettivi di politica pubblica dell’Unione, in linea con gli impegni internazionali. Nel settore della sanità, ad esempio, determinati set di dati detenuti da soggetti operanti nel sistema sanitario pubblico, quali gli ospedali pubblici, potrebbero essere considerati dati sanitari altamente sensibili. Altri settori pertinenti comprendono i trasporti, l’energia, l’ambiente e la finanza. Per garantire pratiche armonizzate in tutta l’Unione, tali tipologie di dati pubblici non personali altamente sensibili dovrebbero essere definite dal diritto dell’Unione, ad esempio nel contesto dello spazio europeo dei dati sanitari o di altra normativa settoriale. È opportuno stabilire mediante atti delegati tali condizioni cui è subordinato il trasferimento di tali dati a paesi terzi. Le condizioni dovrebbero essere proporzionate, non discriminatorie e necessarie per tutelare i legittimi obiettivi di politica pubblica dell’Unione individuati, quali la protezione della salute pubblica, la sicurezza, l’ambiente, la morale pubblica e la protezione dei consumatori, della vita privata e dei dati personali. Le condizioni dovrebbero corrispondere ai rischi identificati in relazione alla sensibilità di tali dati, anche in termini di rischi di reidentificazione dei singoli individui. Tali condizioni potrebbero includere termini applicabili per il trasferimento o modalità tecniche, quali l’obbligo di utilizzare un ambiente di trattamento sicuro, limiti relativi al riutilizzo dei

²⁵ Reg. UE 2025/327 del Parlamento europeo e del Consiglio, dell’11 febbraio 2025, sullo spazio europeo dei dati sanitari e che modifica la direttiva 2011/24/UE e il regolamento (UE) 2024/2847 (Reg. EHDS).

dati nei paesi terzi o categorie di persone aventi facoltà di trasferire tali dati a paesi terzi o che possono accedere ai dati nel paese terzo. In casi eccezionali tali condizioni potrebbero inoltre comprendere restrizioni al trasferimento dei dati a paesi terzi per tutelare l'interesse pubblico».

4. Connessioni e ricorrenze tra disciplina in tema di spazio europeo di dati sanitari nel nuovo Regolamento EHDS e disciplina del fenomeno di *data intermediation* negli impianti normativi precedenti (GDPR e DGA)

Proseguendo l'attuazione del programma di politica normativa delineato dalla Commissione europea con la più volte citata Comunicazione per «*Una strategia europea dei dati*», in cui s'è dato grande peso alla creazione di spazi di condivisione di dati, settoriali e non²⁶, il legislatore eurounitario ha deciso di intervenire *in primis* nel settore sanitario, dettando un'articolata disciplina degli spazi di condivisione di dati sanitari (*European Health Data Space*, EHDS) con il Reg. UE n. 2025/327²⁷.

²⁶ Nella predetta Comunicazione della Commissione europea, *Una strategia europea dei dati*, Bruxelles, 19 febbraio 2020, COM(2020) 66 final, si precisa infatti che «L'UE dovrebbe creare un contesto politico attraente, cosicché entro il 2030 la quota dell'UE dell'economia dei dati (dati conservati, elaborati e utilizzati proficuamente in Europa) corrisponda almeno al suo peso economico, non per imposizione ma per scelta. L'obiettivo è creare uno spazio unico europeo di dati – un autentico mercato unico di dati, aperto ai dati provenienti da tutto il mondo – nel quale sia i dati personali sia quelli non personali, compresi i dati commerciali sensibili, siano sicuri e le imprese abbiano facilmente accesso a una quantità pressoché infinita di dati industriali di elevata qualità, che stimolino la crescita e creino valore, riducendo nel contempo al minimo la nostra impronta di carbonio e ambientale. Dovrebbe trattarsi di uno spazio nel quale il diritto dell'UE possa essere applicato con efficacia e nel quale tutti i prodotti e i servizi basati sui dati siano conformi alle pertinenti normative del mercato unico dell'UE. Quest'ultima dovrebbe a tal fine combinare una legislazione e una *governance* idonee allo scopo per garantire la disponibilità dei dati, investendo in norme, strumenti e infrastrutture, come pure in competenze per la gestione dei dati. Un simile contesto favorevole, che offre incentivi e maggiori possibilità di scelta, comporterà un aumento dei dati conservati ed elaborati nell'UE (...). Per quanto i dati siano essenziali per tutti i settori dell'economia e della società, ogni settore vanta le proprie specificità e non tutti i settori stanno avanzando alla stessa velocità. È pertanto necessario accompagnare le *azioni intersettoriali volte a creare uno spazio europeo di dati con lo sviluppo di spazi di dati settoriali in ambiti strategici quali l'industria manifatturiera, l'agricoltura, la sanità e la mobilità*».

²⁷ Per un inquadramento si veda, in materia, oltre che agli scritti contenuti nel presente volume, FAILLACE, *I diritti dell'interessato nell'uso primario dei dati sanitari elettronici secondo il nuovo Regolamento EHDS*, in *Contratto e impresa*, 2025, 2, 379 ss.; CORSO, *Lo spazio europeo dei dati sanitari. Prime riflessioni sul Regolamento UE 2025/327*, in *Nuove leggi civ. comm.*, 2025, 3, 563 ss.; RAPOSO, *Can Personal Data Be Recycled? The Reuse and Repurposing of Data Under the EHDS*, in SSRN, <https://ssrn.com/ab>

In tale provvedimento vi sono numerosi elementi ricorrenti, emergenti dagli impianti normativi precedenti, di particolare significatività per la disciplina del fenomeno dell'intermediazione dei dati. Il riferimento è, ovviamente, sia al *General Data Protection Regulation* (GDPR), che, come s'è avuto modo di rimarcare, con il diritto alla portabilità dei dati ha consentito l'operatività e la diffusione del modello di *data intermediation* sviluppatosi in Italia e posto all'attenzione delle istituzioni europee, sia al *Data Governance Act*, che ha esplicitato diversi modelli di intermediazione – nel settore pubblico e nel settore privato, in ambito commerciale e in quello altruistico – fornendo la prima disciplina di settore volta ad incentivare il fenomeno circolatorio dei dati personali per il loro *secondary use*.

Ebbene, nel Reg. EHDS si rinvergono, con riguardo agli spazi di dati sanitari, diversi elementi, presenti anche nell'esperienza giuridica pregressa, sopra richiamata, quali:

- (i) il diritto alla portabilità dei dati, previsto nell'art. 20 GDPR, che trova ora una specifica e concorrente disciplina nell'art. 7 del Reg. EHDS, con norme che necessitano di essere coordinate sul piano sistematico ed operativo, anche in relazione al fenomeno dell'intermediazione;
- (ii) il meccanismo della delega, previsto espressamente nell'art. 4 del Reg. EHDS e nel *considerando* n. 21 del medesimo testo normativo, istituto giuridico utilizzato, congiuntamente al diritto alla portabilità, per realizzare il *business and operative model* in tema di *data intermediation*, nella prima esperienza italiana di intermediazione dei dati posta all'attenzione del Garante per la protezione dei dati personali;
- (iii) la previsione di un ruolo attivo, di sostegno degli interessati, svolto nell'ambito dei *servizi di assistenza*, che dovrebbero essere istituiti dagli Stati membri, con «personale adeguatamente formato per assistere la persona fisica nell'esercizio dei propri diritti» (*considerando* n. 21, Reg. EHDS). Viene in tal modo realizzato l'effetto di *empowerment* dei diritti dell'interessato, grazie alla loro funzione “protettiva” e “ausiliatrice”, che richiama quella introdotta per gli

abstract=4397699; QUINN-ELLYNE, YAO, *Limits to Health Data Access Body Discretion and a Need to Comply with the Gdpr – Enough to Protect Against Improper Sharing of Health Data Through the EHDS?*, in SSRN, <https://ssrn.com/abstract=4662816>; DEIMEL, HENTGES, THIEL, *The European Health Data Space and the Future of Cross-Border Healthcare*, in SCHEUER, STUDZINSKI (ed. by), *Digital Maturity in Hospitals. Strategies, Frameworks, and Global Case Studies to Shape Future Healthcare*.

- intermediari di dati nel *Data Governance Act*, soprattutto con riguardo all'azione ed al ruolo delle *data cooperatives*²⁸;
- (iv) la disciplina del *riuso dei dati* detenuti da soggetti pubblici e resa possibile dall'attività svolta dagli *organismi competenti*, responsabili dell'accesso (art. 55 Reg. EHDS) in *ambiente protetto* e con applicazioni di *tariffe* (art. 62 Reg. EHDS), con un sistema incentrato sul precedente impianto delineato nel Capo II del *Data Governance Act*, in materia di «Riutilizzo di determinate categorie di dati protetti detenuti da enti pubblici».

4.1. Il diritto alla portabilità nel Reg. EHDS e nel GDPR

Quanto al diritto alla portabilità dei dati previsto nella nuova disciplina sugli spazi di condivisione dei dati, il *considerando* n. 23 del Reg. EHDS chiarisce il rapporto sussistente con il diritto alla portabilità di cui all'art. 20 del GDPR, precisando che «Il presente regolamento stabilisce *diritti complementari* per le persone fisiche in merito all'uso primario, *che vanno al di là dei diritti di accesso e portabilità sanciti dal regolamento (UE) 2016/679 e li integrano (...)*». Il diritto di cui all'art. 20 del GDPR, dunque, rimane fermo, anche nella materia *de qua*, salva l'introduzione di una disciplina ulteriore, integrativa e complementare, del diritto alla portabilità per gli spazi di condivisione di dati sanitari, prevista all'art. 7 del Reg. EHDS, su cui le autorità di protezione dei dati personali esercitano i propri poteri²⁹.

²⁸ Si tenga presente che nel *considerando* n. 21 del Reg. EHDS viene «(...) *Oltre ai servizi di delega*, gli Stati membri dovrebbero istituire anche *servizi di assistenza* facilmente accessibili forniti da personale adeguatamente formato per assistere le persone fisiche nell'esercizio dei propri diritti. Al fine di tenere conto dei casi in cui la visualizzazione, da parte dei tutori, di alcuni dati sanitari elettronici personali dei loro tutelati possa essere contraria agli interessi o alla volontà dei tutelati, compresi i minori, gli Stati membri dovrebbero poter prevedere nel diritto nazionale limitazioni e garanzie, nonché meccanismi per la loro attuazione tecnica (...)».

²⁹ Nel *considerando* n. 23 cit., infatti, il nuovo regolamento si preoccupa di rimarcare che «Le autorità di controllo istituite ai sensi del regolamento (UE) 2016/679 sono competenti per monitorare e assicurare l'applicazione di tale regolamento, in particolare per il monitoraggio del trattamento dei dati sanitari elettronici personali e per rispondere a eventuali reclami presentati dalle persone fisiche interessate (...)», aggiungendo altresì, con riguardo ai nuovi diritti complementari di accesso e di portabilità, che «(...) tali ulteriori diritti dovrebbero essere garantiti anche dalle autorità di controllo istituite a norma del regolamento (UE) 2016/679», ragion per cui «(...) gli Stati membri dovrebbero provvedere affinché le autorità di controllo siano dotate delle risorse umane e finanziarie, dei locali e delle infrastrutture necessari per l'efficace adempimento di tali compiti aggiuntivi (...)».

Le ragioni che hanno indotto ad una disciplina integrativa del diritto alla portabilità sono evidenti. Quello previsto, seppur innovativamente, all'art. 20 del GDPR soffre di evidenti limitazioni.

La prima concerne la base giuridica del trattamento, venendosi a configurare tale diritto solamente qualora la condizione di liceità sia il consenso, *ex art. 6, par. 1, lett. a)*, o art. 9, par. 2, lett. *a)*, del GDPR, o il contratto, *ex art. 6, par. 1, lett. b)*, GDPR. Ciò porterebbe ad escludere l'applicazione del diritto alla portabilità ove la base giuridica fosse di diverso tipo, come ben potrebbe avvenire per i trattamenti di dati sanitari.

La seconda limitazione riguarda la fonte dei dati, giacché il diritto alla portabilità previsto nella disciplina generale sulla protezione dei dati prevede la sua esercitabilità solamente con riguardo ai dati personali che siano stati «forniti» dall'interessato al titolare del trattamento, includendo dunque sia quelli espressamente ed attivamente conferiti dall'interessato, sia quelli raccolti dal titolare mediante l'osservazione di dati “grezzi” (*raw data*)³⁰, ma escludendo i dati che siano stati oggetto di successiva elaborazione da parte del titolare del trattamento o che siano stati da questi generati³¹.

³⁰ ARTICLE 29 DATA PROTECTION WORKING PARTY (WP29), *Guidelines on the right to data portability*, Revised and adopted on 5 April 2017, WP 242 rev. 01, 9, ove si rimarca che «*There are many examples of personal data, which will be knowingly and actively “provided by” the data subject such as account data (e.g. mailing address, user name, age) submitted via online forms. Nevertheless, data “provided by” the data subject also result from the observation of his activity. As a consequence, the WP29 considers that to give its full value to this new right, “provided by” should also include the personal data that are observed from the activities of users such as raw data processed by a smart meter or other types of connected objects, activity logs, history of website usage or search activities (...)*».

³¹ WP29, *Guidelines on the right to data portability*, cit., p. 10, ove viene evidenziato che tra i dati forniti, oggetto di osservazione da parte del titolare del trattamento, non possono essere inclusi «*(...) data that are created by the data controller (using the data observed or directly provided as input) such as a user profile created by analysis of the raw smart metering data collected*». Sicché, «*A distinction can be made between different categories of data, depending on their origin, to determine if they are covered by the right to data portability. The following categories can be qualified as “provided by the data subject”:*

- *Data actively and knowingly provided by the data subject (for example, mailing address, user name, age, etc.)*

- *Observed data provided by the data subject by virtue of the use of the service or the device. They may for example include a person’s search history, traffic data and location data. It may also include other raw data such as the heartbeat tracked by a wearable device.*

In contrast, inferred data and derived data are created by the data controller on the basis of the data “provided by the data subject”. For example, the outcome of an assessment regarding the health of a user or the profile created in the context of risk management and financial regulations (e.g. to assign a credit score or comply with anti-money laundering rules) cannot in themselves be considered as “provided by” the data subject. Even though such data may be part of a profile kept by a data controller and are inferred

Una terza limitazione riscontrabile nel diritto alla portabilità dei dati di cui all'art. 20 GDPR è data dalla possibilità di ottenere il trasferimento dei dati da un titolare ad un altro solamente qualora l'operazione sia «tecnicamente fattibile»³². Ciò finisce per escludere l'esercizio del diritto alla portabilità dei dati nel caso in cui il titolare del trattamento riscontri (non una mera difficoltà ma una sostanziale) impossibilità tecnica nel realizzare la portabilità dei dati mediante la trasmissione diretta ad altro titolare del trattamento, in formato strutturato e leggibili da dispositivo.

V'è poi una quarta limitazione, che si estrae dalla lettura di sistema nel combinato disposto dell'art. 20 cit. con l'art. 12 del GDPR: di fronte alla richiesta di esercizio del diritto alla portabilità, come di qualsiasi altro diritto contemplato nella disciplina generale in materia di protezione dei dati personali, il titolare del trattamento non ha l'obbligo di immediata esecuzione. Come previsto nel par. 3 della disposizione normativa da ultimo cit., «Il titolare del trattamento fornisce all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta ai sensi degli articoli da 15 a 22 [e dunque anche ai sensi dell'art. 20 in tema di portabilità dei dati, *n.d.a.*] senza ingiustificato ritardo e, comunque, al più tardi *entro un mese* dal ricevimento della richiesta stessa. Tale termine può essere *prorogato di due mesi*, se necessario, tenuto conto della complessità e del numero delle richieste. Il titolare del trattamento informa l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta. Se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'interessato»³³. Anche il difetto di immediatezza del trasferimento,

or derived from the analysis of data provided by the data subject (through his actions for example), these data will typically not be considered as "provided by the data subject" and thus will not be within scope of this new right.

In general, given the policy objectives of the right to data portability, the term "provided by the data subject" must be interpreted broadly, and should exclude "inferred data" and "derived data", which include personal data that are created by a service provider (for example, algorithmic results). A data controller can exclude those inferred data but should include all other personal data provided by the data subject through technical means provided by the controller.

Thus, the term "provided by" includes personal data that relate to the data subject activity or result from the observation of an individual's behaviour, but does not include data resulting from subsequent analysis of that behaviour. By contrast, any personal data which have been» (Ibidem).

³² In questo senso v. l'art. 20, par. 2, GDPR.

³³ Art. 12, par. 3, GDPR. Inoltre, qualora si registri il caso di mancata ottemperanza «alla richiesta dell'interessato, il titolare del trattamento informa l'interes-

non certo ottimale in ambito sanitario soprattutto in relazione alle esigenze di cura dei pazienti, ha reso indispensabile l'emanazione di una disciplina *ad hoc*.

Si comprende bene, dunque, la ragione che ha portato all'avvento di un diritto alla portabilità, nell'art. 7 del Reg. EHDS, complementare ed integrativo rispetto all'analogo diritto alla portabilità previsto nell'art. 20 GDPR³⁴, che in un certo qual modo vede estendere la sua portata applicativa al nuovo contesto³⁵.

La correlazione è evidente, sia per la dichiarata competenza dell'autorità in materia di protezione dei dati personali anche su tali diritti di nuova (ri)formulazione, sia per il chiaro tenore del *considerando* n. 15 del Reg. EHDS, nel quale si ribadisce testualmente che «Il quadro stabilito dal presente regolamento dovrebbe basarsi sul diritto alla portabilità dei dati previsto dal regolamento (UE) 2016/679 garantendo che le persone fisiche, in qualità di interessati, possano trasmettere i loro dati sanitari elettronici personali, compresi i dati desunti, nel formato europeo di scambio delle cartelle cliniche elettroniche, a prescindere dalla base giuridica per il trattamento dei dati sanitari elettronici. I professionisti sanitari dovrebbero astenersi dall'ostacolare l'applicazione dei diritti delle persone fisiche, ad esempio rifiutandosi di tenere conto dei dati sanitari elettronici personali provenienti da un altro Stato membro e forniti tramite il formato europeo di scambio delle cartelle cliniche elettroniche, interoperabile e affidabile».

In tale contesto, la disciplina del «*Diritto delle persone fisiche alla portabilità dei dati*» è scolpita nell'art. 7 del nuovo regolamento,

sato senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale» (art. 12, par. 4, GDPR).

³⁴ La *ratio* è scolpita nel testo del *considerando* n. 14 del nuovo regolamento sugli spazi di condivisione dei dati sanitari, ove si legge che «Ai sensi del regolamento (UE) 2016/679 il diritto alla portabilità dei dati è limitato ai dati trattati sulla base del consenso o di un contratto e forniti dall'interessato a un titolare del trattamento. Inoltre, ai sensi dello stesso regolamento, le persone fisiche hanno il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro solo se tecnicamente fattibile. Tale regolamento non prevede tuttavia l'obbligo di rendere questa trasmissione diretta tecnicamente fattibile. Il diritto alla portabilità dei dati dovrebbe essere integrato nel quadro del presente regolamento, così da 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. Inoltre, alle persone fisiche dovrebbe essere garantito il diritto di chiedere a un prestatore di assistenza sanitaria la trasmissione di una parte dei loro dati sanitari elettronici a un destinatario chiaramente identificato nel settore della sicurezza sociale o dei servizi di rimborso. Tale trasmissione dovrebbe avvenire in una sola direzione».

³⁵ Cfr. *considerando* n. 15 del Reg. EHDS.

nel quale viene stabilito, nel par. 1, che «Le persone fisiche hanno il diritto di *concedere l'accesso* alla totalità o a parte dei loro dati sanitari elettronici personali *a un altro prestatore* di assistenza sanitaria di loro scelta *o di chiedere a un prestatore di assistenza sanitaria di trasmettere* la totalità o parte dei loro dati sanitari elettronici a un altro prestatore di assistenza sanitaria di loro scelta *immediatamente*, gratuitamente e senza ostacoli da parte del prestatore di assistenza sanitaria o dei fabbricanti dei sistemi utilizzati dal prestatore di assistenza sanitaria»³⁶.

Ulteriori differenze si rinvencono anche sul piano esecutivo.

Si noti che nell'art. 20 GDPR la *data portability* trova esecuzione nelle forme del trasferimento dei dati, in formato strutturato e leggibile da dispositivo elettronico (i) all'interessato medesimo (che, dunque, riceve i dati personali con facoltà di ritrasmetterli ad altro titolare senza che il primo possa ostacolare tale trasferimento), oppure (ii) direttamente verso altro titolare del trattamento, ove ciò risulti tecnicamente fattibile (e quindi l'interessato, in tale declinazione della *data portability*, ottiene la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, con accesso all'ambiente informatico di quest'ultimo).

Nell'art. 7 del nuovo regolamento la modalità esecutiva – e dunque i contenuti stessi del diritto – appaiono diversi, in quanto il sistema di trattamento rimane il medesimo, quello assicurato dallo spazio di condivisione dei dati, e il diritto a ricevere e trasmettere o a veder trasferiti da un soggetto ad un altro i propri dati personali assume, *in primis*, la diversa fisionomia del diritto a far ottenere (e dunque a *concedere*) un *accesso condiviso* a tutti o a parte dei propri dati e, *in secundis*, il diritto all'*immediata trasmissione* dei dati tra un prestatore di assistenza sanitaria ed un altro, ossia non tra un qualsiasi titolare del trattamento ed un qualsiasi altro titolare del trattamento, ma tra titolari qualificati in ragione della specifica natura dell'attività da questi svolta sul dato sanitario.

Ciò anche qualora, ai sensi del par. 3 del medesimo articolo, le persone fisiche esercitino il diritto loro riconosciuto alla portabilità dei dati quale «diritto di *chiedere* a un prestatore di assistenza sanitaria *di trasmettere* una parte dei loro dati sanitari elettronici personali a un *destinatario chiaramente identificato del settore della sicurezza sociale* o

³⁶ Al par. 2 di tale articolo si prevede poi che «Qualora i prestatori di assistenza sanitaria si trovino in Stati membri diversi, le persone fisiche hanno il diritto di chiedere la trasmissione dei loro dati sanitari elettronici personali nel formato europeo di scambio delle cartelle cliniche elettroniche di cui all'articolo 15 attraverso l'infrastruttura transfrontaliera di cui all'articolo 23. Il prestatore di assistenza sanitaria ricevente deve accettare tali dati ed è in grado di leggerli».

dei servizi di rimborso (...)», con l'ulteriore precisazione che «Tale trasmissione avviene *immediatamente*, gratuitamente e senza ostacoli da parte del prestatore di assistenza sanitaria o dei fabbricanti dei sistemi utilizzati dal prestatore di assistenza sanitaria *ed è solo unidirezionale*».

V'è poi la portabilità dei dati che si esercita, ai sensi dell'art. 7, par. 4, del Reg. cit., scaricando, da parte delle persone fisiche, «*una copia elettronica delle loro categorie prioritarie di dati sanitari elettronici personali* in conformità dell'articolo 3, paragrafo 2» per poi «*trasmettere tali dati ai prestatori di assistenza sanitaria di loro scelta* nel formato europeo di scambio delle cartelle cliniche elettroniche di cui all'articolo 15» e, in tal caso, «*Il prestatore di assistenza sanitaria ricevente deve accettare tali dati* e, se del caso, essere in grado di leggerli».

Si tratta tuttavia di una portabilità funzionale alla realizzazione del sistema di trattamento protetto, che avviene entro il “recinto” sicuro degli spazi di condivisione dei dati, amministrati centralmente e svolto solamente verso soggetti predeterminati: appunto, i “prestatori di assistenza sanitaria” o i “destinatari chiaramente identificati del settore della sicurezza sociale o dei servizi di rimborso”. Non è, questa, una portabilità pensata per i servizi di intermediazione di dati di cui al *Data Governance Act*. È, dunque, una portabilità “tipizzata”, preordinata al trasferimento dei dati verso figure soggettive predeterminate, incentrata sull'uso *primario* dei dati, come attesta anche la collocazione dell'art. 7 del Reg. EHDS nell'ambito della Sez. II («Diritti delle persone fisiche in relazione all'uso *primario* dei loro dati sanitari elettronici personali e relative disposizioni») del Capo II (intitolato proprio all'«*Uso primario*»)³⁷.

Poiché tuttavia i dati presenti nello spazio di condivisione dei dati vengono poi destinati, obbligatoriamente, anche all'uso secondario, in base alla disciplina delineata nel Capo IV («*Uso secondario*») del Reg. EHDS, agli artt. 50 ss.³⁸, risulta evidente che chi gestisce lo spazio di

³⁷ La definizione di «uso primario» è esplicitata all'art. 2, par. 2, lett. d), del Reg. EHDS, ai sensi del quale tale sintagma viene inteso come «il trattamento dei dati sanitari elettronici per la prestazione di assistenza sanitaria al fine di valutare, mantenere o ripristinare lo stato di salute della persona fisica cui si riferiscono tali dati, comprese la prescrizione, la dispensazione e la fornitura di medicinali e dispositivi medici, nonché per i pertinenti servizi sociali, amministrativi o di rimborso».

³⁸ Si consideri che all'art. 51 del Reg. EHDS vengono indicate le categorie minime che sono soggette all'obbligo di disponibilità per l'uso secondario, posto in essere a carico dei titolari dei trattamenti di dati sanitari che ne sono già in possesso per l'uso primario, con facoltà accordata agli Stati membri di inserire categorie di dati aggiuntive. Ai sensi dell'art. 51 dianzi citato, infatti, «I titolari dei dati sanitari mettono a disposizione per l'uso secondario, conformemente al presente capo, le categorie di dati sanitari elettronici seguenti: a) dati sanitari elettronici provenienti da cartelle cliniche elettroniche; b) dati su

condivisione dei dati finisce per assumere sostanzialmente il ruolo di “*intermediario*” istituzionalizzato, con un apparato normativo che ottimizza, per il settore sanitario, l’esperienza normativa già maturata nel settore dell’intermediazione dei dati e che ha il proprio modello in tutto il *Data Governance Act*. Si consideri, in particolare, il ruolo di intermediazione sostanzialmente svolto dagli enti pubblici, con riguardo ai dati da questi detenuti per fini istituzionali, che possono essere forniti agli utenti di dati mediante il ricorso ad “organismi competenti”, con applicazione di un sistema tariffario che permetta la sostenibilità del servizio.

Si tratta ovviamente di un’innovazione importante ed apprezzabile, destinata a potenziare in maniera significativa il regime di circolazione dei dati sanitari per uso secondario, per le finalità indicate nell’art. 53 del Reg EHDS, anche in ragione della ricerca di settore, nonché dello sviluppo e dell’innovazione di prodotti e servizi e per l’addestramento dei sistemi di intelligenza artificiale³⁹.

fattori con un’incidenza sulla salute, compresi i determinanti socioeconomici, ambientali e comportamentali della salute; *c*) dati aggregati sulle esigenze di assistenza sanitaria, sulle risorse assegnate all’assistenza sanitaria, sulla prestazione di assistenza sanitaria e sul suo accesso, sulla spesa per l’assistenza sanitaria e sul suo finanziamento; *d*) dati sugli agenti patogeni che incidono sulla salute umana; *e*) dati amministrativi relativi all’assistenza sanitaria, anche relativamente alle dispensazioni, alle domande di rimborso e ai rimborsi; *f*) dati genetici, epigenomici e genomici umani; *g*) altri dati molecolari umani, quali quelli provenienti dalla proteomica, dalla trascrittomica, dalla metabolomica, dalla lipidomica e altri dati omici; *h*) dati sanitari elettronici personali generati automaticamente mediante dispositivi medici; *i*) dati provenienti dalle applicazioni per il benessere; *j*) dati relativi allo status e alla specializzazione e all’istituzione dei professionisti sanitari coinvolti nella cura di una persona fisica; *k*) dati provenienti da registri dei dati sanitari basati sulla popolazione, come i registri di sanità pubblica; *l*) dati provenienti da registri medici e da registri della mortalità; *m*) dati provenienti da sperimentazioni cliniche, studi clinici, indagini cliniche e studi delle prestazioni soggetti al regolamento (UE) n. 536/2014, al regolamento (UE) 2024/1938 del Parlamento europeo e del Consiglio (35), al regolamento (UE) 2017/745 e al regolamento (UE) 2017/746; *n*) altri dati sanitari provenienti da dispositivi medici; *o*) dati provenienti da registri di medicinali e dispositivi medici; *p*) dati provenienti da coorti di ricerca, questionari e indagini in materia di salute, dopo la prima pubblicazione dei risultati; *q*) dati sanitari provenienti da biobanche e banche dati associate». Così co. 1, a cui segue poi, al co. 2, l’ulteriore possibile estensione di tali categorie minime da conferire obbligatoriamente per l’uso secondario dei dati, rimesse alle scelte degli ordinamenti nazionali: «Gli Stati membri possono stabilire nel loro diritto nazionale che categorie *aggiuntive* di dati sanitari elettronici siano messe a disposizione per l’uso secondario in conformità del presente regolamento».

³⁹ Nel cit. art. 53 del Reg. EHDS, rubricato «*Finalità per le quali è possibile trattare i dati sanitari elettronici per l’uso secondario*», si stabilisce, al par. 1, che «Gli organismi responsabili dell’accesso ai dati sanitari concedono l’accesso ai dati sanitari elettronici di cui all’articolo 51 per l’uso secondario a un utente dei dati sanitari solo se il trattamento dei dati da parte dell’utente è necessario per una delle finalità seguenti: *a*) pubblico

L'accesso ai dati di uso secondario è altresì riservato ad enti pubblici e a istituzioni, organi e organismi dell'UE solamente per alcune delle finalità ammesse, desumendosi quindi, *a contrario*, un'apertura anche ai soggetti privati per le finalità non riservate, tra le quali rientrano anche quella di ricerca scientifica in ambito sanitario e quelle finalità ad essa strumentale, di innovazione di prodotti e servizi e di addestramento dei sistemi di IA⁴⁰.

4.2. La delega tra ammissibilità e limiti

Altro istituto rilevante nel fenomeno di intermediazione di dati, riscontrabile anche nella disciplina del Reg. EHDS, è quello della «delega», originariamente usato dai fornitori dei servizi di *data intermediation* per recuperare i dati dei propri utenti dai diversi titolari del trattamento e, una volta acquisiti, attuare per loro conto le strategie di *secondary use*.

Nel nuovo regolamento europeo sui dati personali la delega viene espressamente contemplata nel *considerando* n. 21, nel quale si trova affermato che «*Le persone fisiche dovrebbero poter fornire un'autoriz-*

interesse nell'ambito della sanità pubblica o della medicina del lavoro, come nel caso delle attività per la protezione da gravi minacce per la salute a carattere transfrontaliero, della sorveglianza della sanità pubblica o delle attività per la garanzia di elevati livelli di qualità e sicurezza dell'assistenza sanitaria, inclusa la sicurezza dei pazienti, e di medicinali o dispositivi medici; *b*) definizione delle politiche e attività regolamentari a sostegno di enti pubblici o di istituzioni, organi e organismi dell'Unione, comprese le autorità di regolamentazione, del settore sanitario o dell'assistenza affinché svolgano i compiti definiti nei rispettivi mandati; *c*) statistiche quali definite all'articolo 3, punto 1), del regolamento (UE) n. 223/2009, come le statistiche ufficiali a livello nazionale, multinazionale e dell'Unione, relative al settore sanitario o dell'assistenza; *d*) attività d'istruzione o d'insegnamento nel settore sanitario o dell'assistenza al livello della formazione professionale o dell'istruzione superiore; *e*) ricerca scientifica nel settore sanitario o dell'assistenza che contribuisce alla sanità pubblica o alla valutazione delle tecnologie sanitarie o che garantisce elevati livelli di qualità e sicurezza dell'assistenza sanitaria, dei medicinali o dei dispositivi medici, con l'obiettivo di favorire gli utenti finali, quali i pazienti, i professionisti sanitari e gli amministratori sanitari, tra cui: *i*) attività di sviluppo e innovazione per prodotti o servizi; *ii*) attività di addestramento, prova e valutazione degli algoritmi, anche nell'ambito di dispositivi medici, dispositivi medico-diagnostici in vitro, sistemi di IA e applicazioni di sanità digitale; *f*) miglioramento della prestazione di assistenza, ottimizzazione delle cure ed erogazione di assistenza sanitaria sulla base dei dati sanitari elettronici di altre persone fisiche».

⁴⁰ Viene infatti previsto, al par. 2 dell'art. 53 cit. del Reg. EHDS, che «L'accesso ai dati sanitari elettronici per le finalità di cui al paragrafo 1, lettere *a*), *b*) e *c*), è riservato agli enti pubblici e alle istituzioni, agli organi e agli organismi dell'Unione che esercitano i compiti loro affidati dal diritto dell'Unione o dal diritto nazionale, anche quando il trattamento dei dati per lo svolgimento di tali compiti è effettuato da terzi per conto di tali enti pubblici o delle istituzioni, degli organi e degli organismi dell'Unione». La riserva di accesso non si estende dunque alle finalità di cui alle lett. *d*), *e*) ed *f*), per le quali v. nt. precedente.

zazione ad altre persone fisiche di loro scelta, come a parenti o ad altre persone fisiche loro vicine, che permetta a queste persone di loro scelta di accedere ai dati sanitari elettronici personali delle persone fisiche che forniscono l'autorizzazione o di controllarne l'accesso, oppure di utilizzare servizi di sanità digitale per loro conto. Tali autorizzazioni potrebbero anche risultare utili per altri usi alle persone fisiche che ricevono l'autorizzazione. Per consentire e attuare tali autorizzazioni è opportuno che gli Stati membri istituiscano servizi di delega che dovrebbero essere collegati a servizi di accesso ai dati sanitari elettronici personali, quali portali per i pazienti o applicazioni per dispositivi mobili rivolte ai pazienti. I servizi di delega dovrebbero anche permettere ai tutori di agire per conto dei loro tutelati, compresi i minori; in tali situazioni le autorizzazioni potrebbero essere automatiche (...)».

Si tratta di strumento autorizzatorio con il quale l'interessato, in forza degli atti di autonomia privata e di autodeterminazione informativa, per la cura dei propri interessi, conferisce ad un altro soggetto il potere di compiere atti o esercitare diritti per suo conto. In questo senso, la "delega" quale atto unilaterale autorizzatorio con cui si investe altri di poteri rappresentativi è accostabile alla "procura"⁴¹.

Il *considerando* cit., come s'è avuto modo di evidenziare, contempla che la "delega" – cioè, in questo contesto, l'attribuzione del potere rappresentativo per l'esercizio del diritto da parte di un altro soggetto per il soddisfacimento di interessi del delegante – sia effettuata in favore di un'altra *persona fisica*, ipotizzando espressamente che ciò avvenga nei confronti di "parenti" o "altre persone fisiche loro vicine". Si tratta ovviamente di menzione del tutto esemplificativa, ma è pacifico che l'assenza di parentela o di vicinanza non siano ostative al conferimento della delega, purché vi sia comunque la fiducia dell'interessato nei confronti del soggetto delegato. Si tratta, infatti, di atto *intuitus personae*, che, com'è noto, non richiede affettività o vicinanza amicale o sentimentale, ma l'esistenza di un rapporto basato sulla valutazione positiva delle altrui caratteristiche personali del soggetto a cui ci si affida,

⁴¹ La dottrina definisce la procura come «un atto unilaterale, con il quale un soggetto investe un altro soggetto del potere di rappresentarlo; ed è un atto unilaterale recettizio nei confronti del rappresentante, non recettizio nei confronti dei terzi: sotto questo aspetto non può dirsi rivolto ad un destinatario determinato, ma a tutti coloro con i quali il rappresentante si troverà a contrattare in nome del rappresentato». Così GALGANO, *Trattato di diritto civile*, Milano, 2014, 3^a ed. a cura di ZORZI GALGANO, vol. II, 485. Per la delega in ambito amministrativo si rimanda, invece, a MIELE, voce «Delega (dir. amm.)», in *Enc. dir.*, Milano, 1962, XI, 905 ss.

sia egli persona fisica o giuridica⁴². Si consideri che, nel caso specifico

⁴² L'*intuitus personae* non esige, secondo la ricostruzione della dottrina dominante, che la relazione giuridica per il compimento dell'atto sia instaurata nei confronti di una persona fisica, potendo l'*intuitus personae* essere riferito anche nei riguardi delle persone giuridiche. Si pensi, ad esempio, alla disciplina del contratto di appalto, ove, dal divieto di subappalto – in assenza di espressa autorizzazione dal committente – si argomenta del connotato *intuitus personae* del contratto concluso dall'appaltatore, anche se questi non svolge la prestazione in prevalenza con il proprio lavoro personale. In questo senso cfr. MUSOLINO, *Comm. sub art. 1656 c.c.*, in VALENTINO (a cura di), *Dei singoli contratti*, Vol. II, *Artt. 1655-1802 c.c.*, nel *Commentario al Codice Civile* diretto da E. Gabrielli, Torino, 2011, 30 s., il quale, sulla *ratio* del divieto di subappalto e l'*intuitus personae*, sostiene che «Secondo un orientamento, fine della statuizione *ex art. 1656 c.c.* sul divieto di subappalto sarebbe di evitare che l'imprenditore si trasformi in un accaparratore di lavori per scopi puramente speculativi. Tale posizione non appare, però, pienamente condivisibile, poiché comporterebbe l'indisponibilità della norma, in quanto sostanzialmente dettata per motivi di ordine pubblico. In realtà, il legislatore considera lecito il subappalto, qualora sia autorizzato dal committente, non perché affidi a quest'ultimo il compito di valutare quell'interesse pubblico, ma perché solo il suo interesse privato sta a fondamento del divieto, che quindi non ha più ragione di essere nel caso in cui l'interesse medesimo sia salvo. Si tratta dell'interesse del committente a che l'esecuzione dell'opera non venga effettuata da un'impresa senza che questa sia stata prima da lui autorizzata, poiché si è dato, anche in questa fattispecie, rilievo all'*intuitus personae*». Vero è che nell'appalto, diversamente dal contratto d'opera, non rileva che la prestazione sia eseguita personalmente dall'imprenditore, «tuttavia non si può ammettere, senza una specifica autorizzazione che l'appaltatore si liberi pure del compito di organizzazione, di direzione e di gestione, riversandolo sui subappaltatori» (*Ibidem*, 31). L'A. cit. aggiunge, *ivi* nella nt. 14, che «La considerazione secondo cui l'appalto è ascrivibile ai contratti stipulati *intuitu personae* è condivisa dalla dottrina dominante». Di diverso avviso è chi ha rilevato che «il c.d. *intuitus personae* negli appalti costituisce una sorta di retaggio di un'epoca nella quale l'esecuzione del contratto veniva affidata alle capacità – si potrebbe dire – personali dell'imprenditore/appaltatore. Ovviamente una siffatta configurazione è assai lontana dalla nostra realtà nella quale si è ormai in presenza di una dimensione aziendale che comporta inevitabilmente la "spersonalizzazione" del contratto di appalto. Anzi, l'*intuitus personae* – quantomeno nella contrattazione pubblica – sembra mutare di significato: infatti, mentre nell'accezione tradizionale esso implicava l'impossibilità di trasferire ad altro soggetto l'esecuzione del contratto, oggi pare emergere un'esigenza di immodificabilità del contraente riferita, tuttavia, non più alla figura di un determinato imprenditore, bensì a un determinato complesso aziendale». Così ALBERTI, *Le vicende soggettive dell'esecutore*, vol. V, *I settori speciali. L'esecuzione*, in *Trattato sui contratti pubblici*, diretto da M.A. Sandulli, De Nictoli, Garofoli, Milano, 2008, 3452. Si veda anche la lettura critica, quanto all'*intuitus personae* nei contratti di appalto, enunciata da IUDICA, *Il contratto di appalto*, in Lipari, P. Rescigno (diretto da), *Diritto civile*, III, Milano 2009, 300 ss.

Sulla pacifica riferibilità dei contratti *intuitus personae* anche alle persone giuridiche si veda anche GALGANO, *Trattato di diritto civile*, cit., 405, nota n. 70, il quale esemplificativamente fa riferimento a «quanto l'art. 1918, commi 3° e 4°, prevede per il caso di alienazione della cosa assicurata: l'acquirente subentra nel contratto di assicurazione, ma l'assicuratore può recedere dal contratto; ed è quanto prevede, per i contratti relativi all'azienda ceduta, l'art. 2558, comma 2°: l'*intuitus personae* opera qui come "giusta causa" di recesso del terzo contraente». Galgano traccia una linea di distinzione tra «contratti personali» e quelli «c.d. *intuitus personae*», che si hanno quando l'identità o le qualità personali

degli spazi di condivisione di dati sanitari, le ragioni che inducono a delegare un altro soggetto potrebbero essere diverse, incluso il difetto di competenze tecnologiche, come potrebbe capitare ad esempio con le persone anziane che non abbiano dimestichezza con la complessità della soluzione tecnologica proposta con l'EHDS⁴³.

Nel testo del nuovo Regolamento il tema è disciplinato all'art. 4, rubricato «*Servizi di accesso ai dati sanitari elettronici per le persone fisiche e i loro rappresentanti*», il quale, dopo aver menzionato, al par. 1, l'istituzione di «*uno o più servizi di accesso ai dati sanitari elettronici a livello nazionale, regionale o locale*» per consentire in tal modo «alle persone fisiche di accedere ai loro dati sanitari elettronici personali e di esercitare i loro diritti di cui all'articolo 3 e agli articoli da 5 a 10», viene ulteriormente precisato che «Tali servizi di accesso sono gratuiti per le persone fisiche e i loro *rappresentanti* di cui al paragrafo 2 del presente articolo».

Qui entra in gioco il meccanismo della “delega”, di cui se ne prevede l'istituzione in forma di “servizio”, quale «funzionalità dei servizi di accesso ai dati sanitari elettronici», in favore sia dei «rappresentati legali delle persone fisiche», sia delle persone fisiche scelte dagli interessati e da questi autorizzati, tramite il sistema di gestione delle autorizzazioni, «ad accedere ai loro dati sanitari elettronici personali, o anche a una parte di essi, per un periodo determinato o indeterminato e, in caso di necessità, solo per una finalità specifica»⁴⁴.

di uno dei contraenti sono determinanti del consenso dell'altro o degli altri contraenti, anche qualora il contraente medesimo, di cui rilevano l'identità o le qualità personali, sia una persona giuridica.

⁴³ IZZO, GUARDA, *Sanità elettronica, tutela dei dati personali e digital divide generazionale: ruolo e criticità giuridica della delega alla gestione dei servizi di sanità elettronica da parte dell'interessato*. – *E-health, Data Protection and Generational Digital Divide: Empowering the Interested Party with the Faculty of Nominating a Trusted Person Acting as a Proxy when Processing Personal Health Data within an Electronic PHR*, Università di Trento, Trento, 2010, 10 ss., documento reperibile online all'url <http://eprints.biblio.unitn.it/archive/00001921/> (consultato da ultimo in data 13 luglio 2025).

⁴⁴ Cfr. art. 4, par. 2, del Reg. EHDS, ove, testualmente, viene stabilito che «2. Gli Stati membri provvedono affinché siano istituiti uno o più *servizi di delega come funzionalità dei servizi di accesso* ai dati sanitari elettronici che consentano:

a) alle persone fisiche di autorizzare altre persone fisiche di loro scelta ad accedere per loro conto ai loro dati sanitari elettronici personali, o a una parte di essi, per un periodo determinato o indeterminato e, in caso di necessità, solo per una finalità specifica, e di gestire tali autorizzazioni; e

b) ai rappresentanti legali delle persone fisiche di accedere ai dati sanitari elettronici personali delle persone fisiche di cui curano gli interessi, conformemente al diritto nazionale.

Si noti che il termine *delega* è usato impropriamente con riguardo ai «rappresentanti legali delle persone fisiche», in quanto allude, generalmente, all'attribuzione volontaria del potere rappresentativo, mentre la rappresentanza legale ha la sua fonte nella legge e non nell'atto di autonomia privata.

V'è però da rilevare che il meccanismo di delega è comunque strutturato nell'ambito di un "servizio" fornito negli spazi di condivisione di dati sanitari, il che allude non solo all'atto autorizzatorio del delegare, ma anche all'allestimento tecnico del sistema informatico, tale da consentire, sia nella rappresentanza volontaria, sia in quella legale, di sostituire un soggetto (l'interessato) con un altro (il rappresentante designato in forza dell'atto di autonomia provata o quello individuato *ex lege*, come i genitori del minore o il tutore dell'incapace), abilitando quest'ultimo, dal punto di vista informatico, ad intervenire con le proprie credenziali e a svolgere l'attività per conto dell'interessato medesimo⁴⁵, all'interno di un sistema interoperabile a livello europeo che va adeguato alla disciplina del Reg. eIDAS⁴⁶.

Del resto, ove non vi fosse il meccanismo tecnico del "servizio di delega", potrebbe verificarsi che l'interessato finisca materialmente per far utilizzare le proprie credenziali ad altri, nell'intento di consen-

Gli Stati membri stabiliscono norme relative alle autorizzazioni di cui alla lettera a) del primo comma e alle azioni dei tutori e di altri rappresentanti legali».

⁴⁵ La previsione del servizio di delega previsto nel Reg. EHDS, quale servizio tecnico-informatico in grado di abilitare il rappresentante (istituito *ex lege* o in base all'autonomia privata) ad agire per conto dell'interessato si ricollega, in un certo senso, alla previsione contenuta nell'art. 8, par. 2, GDPR, ove prevede che «Il titolare del trattamento si adopera in ogni modo ragionevole per verificare in tali casi che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale sul minore, in considerazione delle tecnologie disponibili». Ciò che nel GDPR è rimesso all'*accountability* del titolare del trattamento, nel Reg. EHDS è istituzionalizzato con scelte predeterminate *ex lege*, rimesse agli Stati membri ai sensi dell'art. 4, par. 2, cit. («Gli Stati membri provvedono affinché siano istituiti uno o più servizi di delega come funzionalità dei servizi di accesso ai dati sanitari elettronici...»).

⁴⁶ In tal senso è significativa la parte finale del *considerando* n. 21 del Reg. EHDS, ove viene rimarcato che «I servizi di accesso ai dati sanitari elettronici personali, quali portali per i pazienti o applicazioni per dispositivi mobili rivolte ai pazienti, dovrebbero utilizzare tali autorizzazioni e consentire così alle persone fisiche autorizzate di accedere ai dati sanitari elettronici personali che rientrano nell'ambito dell'autorizzazione. Al fine di garantire una soluzione orizzontale con una maggiore facilità d'uso, le soluzioni digitali per i servizi di delega dovrebbero essere in linea con il regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio e alle specifiche tecniche del portafoglio europeo di identità digitale. Ciò contribuirebbe a ridurre gli oneri amministrativi e finanziari per gli Stati membri, riducendo il rischio di sviluppare sistemi paralleli non interoperabili a livello dell'Unione».

tire comunque al proprio rappresentante l'accesso di fatto al sistema di trattamento dei dati⁴⁷.

Ciò che tuttavia risulta più difficilmente comprensibile, sul piano teorico-giuridico e sistematico, è la scelta di rendere delegabile l'accesso solamente nei confronti delle sole persone fisiche e non anche delle persone giuridiche.

Con riferimento a queste ultima, si tratta di opzione normativa che il legislatore italiano aveva già percorso con l'art. 9, co. 2, del d.lgs. 196/2003, prima dell'abrogazione ad opera del d.lgs. 101/2018, ove, sulle modalità di esercizio dei diritti dell'interessato, si prevedeva testualmente che «(...) l'interessato può conferire, per iscritto, delega o procura a persone fisiche, *enti, associazioni* od organismi (...)»⁴⁸ e «(...) può, altresì, farsi assistere da una persona di fiducia»⁴⁹. Con la revisione del Codice in materia di protezione dei dati personali dovute ad esigenze di coordinamento con il GDPR, l'art. 9 cit. è stato abrogato, senza però che fosse vietata la delega all'esercizio dei diritti dell'interessato: ciò sulla base dei principi generali di diritto privato, che consente ad ogni persona dotata di capacità di agire di autorizzare altri al compimento di atti giuridici per proprio conto, quando ciò sia in linea con il proprio interesse e purché non si tratti di atti personalissimi. Che l'esercizio dei diritti dell'interessato, inclusa la prestazione del consenso, non rientri tra gli atti personalissimi risulta evidente dal tenore dell'art. 8 GDPR, che istituisce quali rappresentanti *ex lege*, per il consenso dei minori (ed ovviamente anche per l'esercizio dei diritti riconosciuti all'interessato), coloro che esercitano la responsabilità genitoriale sul minore medesi-

⁴⁷ Il tema è stato trattato, con riguardo al FSE, e con riferimento all'impianto normativo precedente al GDPR, da IZZO, GUARDA, *Sanità elettronica, tutela dei dati personali e digital divide generazionale: ruolo e criticità giuridica della delega alla gestione dei servizi di sanità elettronica da parte dell'interessato*, cit., 25 s. Gli autori precisano efficacemente che «Come sempre accade nel caso di scelte regolative che attengono a scenari ove la volontà giuridicamente rilevante di un soggetto e i suoi effetti concreti sono mediati dal *bit*, una soluzione estrema che accarezzi l'idea di dire semplicemente no alla possibilità che l'interessato deleghi ad un altro soggetto la gestione del proprio interesse ai dati inerenti la propria salute innescherebbe il rischio assai concreto che le credenziali di accesso dell'interessato al sistema di sanità elettronica finiscano per essere comunque irrualmente rese».

⁴⁸ Art. 9, par. 2, d.lgs. 196/2003, prima della riforma avvenuta con il d.lgs. 101/2018, che ne ha comportato l'abrogazione formale.

⁴⁹ *Ibidem*. Anche nella normativa precedente il principio era pacificamente affermato nel nostro ordinamento all'art. 13, co. 4, della l. n. 675/1996, poi confluito con modifiche nel Codice in materia di protezione dei dati personali (d.lgs. n. 196/2003), ove si prevedeva la possibilità di delega o procura in forma scritta non solo a persone fisiche ma anche ad «associazioni» («Nell'esercizio dei diritti di cui al comma 1 l'interessato può conferire, per iscritto, delega o procura a persone fisiche o ad associazioni»).

mo, al di fuori dei casi in cui gli sia consentito agire personalmente nei limiti oggettivi e d'età previsti dal GDPR e dal Codice in materia di protezione dei dati personali⁵⁰.

La scelta del Reg. EHDS è stata quella di limitare la delega alle sole persone fisiche: nulla vieta tuttavia di individuare come destinatario della delega il legale rappresentante di una persona giuridica o un soggetto che operi all'interno di un ente, individuato quale soggetto a cui ci si affida per la cura dell'interesse da salvaguardare. Del resto, qualora si fosse designato come destinatario dell'autorizzazione una persona giuridica, in linea con quanto era contemplato dal testo originario dell'art. 9 del d.lgs. 196/2003, si sarebbe dovuto pur sempre individuare al suo interno un soggetto, persona fisica, che agisse nell'ambito dell'ente e, in difetto di diversa precisazione, tale individuazione si sarebbe dovuta effettuare nei confronti del suo legale rappresentante *pro-tempore*.

Ulteriori considerazioni vanno però declinate con riguardo al particolare contesto in cui si colloca l'EHDS, quantomeno per l'uso primario dei dati sanitari personali, giacché in tale ambito ci si muove in quella

⁵⁰ Com'è noto, l'art. 8, par. 1, GDPR prevede che «Qualora si applichi l'articolo 6, paragrafo 1, lettera a), per quanto riguarda l'offerta diretta di servizi della società dell'informazione ai minori, il trattamento di dati personali del minore è lecito ove il minore abbia almeno 16 anni. Ove il minore abbia un'età inferiore ai 16 anni, tale trattamento è lecito soltanto se e nella misura in cui tale consenso è prestato o autorizzato dal titolare della responsabilità genitoriale.

Gli Stati membri possono stabilire per legge un'età inferiore a tali fini purché non inferiore ai 13 anni».

Lo Stato italiano, con l'art. 2 *quinquies* del novellato Codice in materia di protezione dei dati personali, ha determinato la soglia d'età a quattordici anni, precisando che «In attuazione dell'articolo 8, paragrafo 1, del Regolamento, il minore che ha compiuto i quattordici anni può esprimere il consenso al trattamento dei propri dati personali in relazione all'offerta diretta di servizi della società dell'informazione. Con riguardo a tali servizi, il trattamento dei dati personali del minore di età inferiore a quattordici anni, fondato sull'articolo 6, paragrafo 1, lettera a), del Regolamento, è lecito a condizione che sia prestato da chi esercita la responsabilità genitoriale». Dunque, chi esercita la responsabilità genitoriale esprime per conto del minore il consenso – ed esercita i diritti dell'interessato – nei seguenti casi: a) qualora non trovi applicazione l'art. 6, par. 1, lett. a), ma l'art. 9, par. 1, l'art. a), GDPR – e dunque quando il trattamento nei cui confronti si esprime il consenso abbia ad oggetto dati particolari – a prescindere dalle soglie d'età e dalla natura di servizio della società dell'informazione offerto al minore; b) ove il trattamento nei cui confronti si chiede di esprimere il consenso non abbia ad oggetto i servizi della società dell'informazione offerti ai minori; c) qualora il minore non abbia ancora raggiunto i quattordici anni e il trattamento abbia ad oggetto servizi della società dell'informazione offerti ai minori e il consenso sia fondato sull'art. 6, par. 1, lett. a), GDPR.

Va poi precisato che, in tutti i casi in cui il trattamento riguardi minori e non sia fondato sul consenso, ma su altra base giuridica, chi esercita la responsabilità genitoriale potrà comunque esercitare per conto del minore, quale rappresentante legale di quest'ultimo, tutti i diritti che sono riconosciuti all'interessato.

che può essere definita una «*relazione di cura*» tra medico e paziente, al cui cospetto il trattamento dei dati personali è da ritenersi funzionale alla cura dell'interessato e all'assistenza sanitaria da svolgersi nei suoi confronti. Sicché andrebbe tenuto conto, in prospettiva sistematica, che nel nostro ordinamento entra in rilievo l'impianto delineato nella legge 22 dicembre 2017 n. 219 recante «Norme in materia di consenso informato e disposizioni anticipate di trattamento», nella parte in cui, all'art. 1, co. 2, vengono individuati nei *familiari*, nella *parte dell'unione civile*, nel *convivente* o in un'altra *persona di fiducia del paziente* i soggetti coinvolgibili, a discrezione del paziente medesimo, nella relazione di cura che si instaura tra paziente e medico⁵¹, e, al successivo co. 3, viene previsto che il paziente possa indicare i familiari o altra persona di sua fiducia sia per ricevere, in sua vece, le informazioni sulle condizioni di salute del paziente (anche con riguardo alla diagnosi, alla prognosi, ai benefici e ai rischi degli accertamenti diagnostici e dei trattamenti sanitari, nonché alle possibili alternative e alle conseguenze dell'eventuale rifiuto del trattamento sanitario, dell'accertamento diagnostico o della rinuncia ai medesimi), sia per esprimere il consenso al trattamento sanitario, con annotazione nella cartella clinica e nel fascicolo sanitario elettronico⁵².

Il «servizio di delega» previsto nel Reg. EHDS, dunque, pare ritagliato su questo modello, che tuttavia finisce per estendersi anche con riguardo al trattamento dei dati personali di carattere sanitario e, quindi, ben al di là dei confini del solo trattamento sanitario⁵³.

⁵¹ Testualmente, l'art. 1, co. 2, della l. n. 219/2017, prevede che «È promossa e valorizzata la relazione di cura e di fiducia tra paziente e medico che si basa sul consenso informato nel quale si incontrano l'autonomia decisionale del paziente e la competenza, l'autonomia professionale e la responsabilità del medico».

Contribuiscono alla relazione di cura, in base alle rispettive competenze, gli esercenti una professione sanitaria che compongono l'equipe sanitaria. In tale relazione sono coinvolti, se il paziente lo desidera, anche i suoi familiari o la parte dell'unione civile o il convivente ovvero una persona di fiducia del paziente medesimo».

⁵² L'art. 1, co. 3, della l. n. 219/2017 stabilisce espressamente che «*Ogni persona ha il diritto di conoscere le proprie condizioni di salute e di essere informata in modo completo, aggiornato e a lei comprensibile riguardo alla diagnosi, alla prognosi, ai benefici e ai rischi degli accertamenti diagnostici e dei trattamenti sanitari indicati, nonché riguardo alle possibili alternative e alle conseguenze dell'eventuale rifiuto del trattamento sanitario e dell'accertamento diagnostico o della rinuncia ai medesimi. Può rifiutare in tutto o in parte di ricevere le informazioni ovvero indicare i familiari o una persona di sua fiducia incaricati di riceverle e di esprimere il consenso in sua vece se il paziente lo vuole. Il rifiuto o la rinuncia alle informazioni e l'eventuale indicazione di un incaricato sono registrati nella cartella clinica e nel fascicolo sanitario elettronico*».

⁵³ Si noti che la l. n. 219/2017 si colloca proprio nell'ottica del trattamento sanitario e non del trattamento dei dati carattere sanitario, anche se v'è un evidente collegamento

La questione della delega si incrocia con i modelli di intermediazione di dati in forma cooperativa recentemente disciplinati dal *Data Governance Act*⁵⁴, che trovano applicazione anche al settore sanitario⁵⁵.

Quando il testo di tale Regolamento europeo era ancora in forma di Proposta, il *considerando* n. 24, poi riformato sul punto, prevedeva l'esercitabilità dei diritti dell'interessato solamente in forma individuale e la non delegabilità dei diritti dell'interessato alla cooperativa di dati⁵⁶. Entrambi tali aspetti sono stati rivisti nel testo definitivo del Regolamento europeo, in cui sono stati espunti. Nella nuova formulazione del corrispondente *considerando*, contrassegnato ora con il n. 31, si trova affermato, invece, che «Le cooperative di dati mirano a raggiungere una serie di obiettivi, in particolare a rafforzare la posizione dei singoli individui, affinché compiano scelte informate prima di acconsentire all'utilizzo dei dati, influenzando i termini e le condizioni, stabiliti dalle

tra l'uno e l'altro, ad esempio sul piano del diritto a ricevere le informazioni nell'ambito della relazione di cura e a delegare altri a riceverle in propria vece. Che i due piani siano distinti lo si comprende bene sul versante del consenso: il consenso informato di cui all'art. 1 della predetta legge è il consenso informato al trattamento di carattere sanitario sul paziente, che comprende anche il diritto al rifiuto della cura, mentre il consenso informato in materia di protezione dei dati personali riguarda l'autorizzazione ad eseguire operazioni di trattamento dei dati personali per le finalità legittime, esplicite e determinate, stabilite dal titolare del trattamento e comunicate all'interessato nell'informativa ex art. 13 (e 14) del GDPR.

⁵⁴ Sulle cooperative di dati si veda BRAVO, *Le cooperative di dati*, cit., 757 ss.; PETRONE, *Il mercato digitale europeo e le cooperative di dati*, in *Contratto e impresa*, 2023, 3, 800 ss.; BRAVO (a cura di), *EU Data Cooperatives. L'ingresso delle cooperative di dati nell'ordinamento europeo*, cit.

⁵⁵ Si veda, a tale riguardo, BRAVO (a cura di), *EU Data Cooperatives. L'ingresso delle cooperative di dati nell'ordinamento europeo*, cit., e segnatamente, nel predetto volume, i seguenti contributi: PALLADINI, SCAGLIARINI, *Le cooperative di dati come forma di tutela collettiva degli interessati: un'opportunità per l'ambito sanitario?* (407 ss.); TAMPIERI, *Cooperative di dati per la tutela della salute* (434 ss.); FAILLACE, *Le cooperative di dati sanitari tra codice civile e Data Governance Act* (443 ss.); PROIETTI, *Cooperative di dati, Spazio europeo dei dati sanitari e Data Act nel dedalo normativo* (469 ss.); RUFO, *Data Governance Act e cooperative di dati: una "possibile" nuova frontiera per la ricerca in sanità* (487 ss.).

⁵⁶ Il testo del *considerando* n. 24 della Proposta di regolamento in materia di governance dei dati (*Data Governance Act*) prevedeva espressamente che «Le cooperative di dati mirano a rafforzare la posizione dei singoli individui, affinché compiano scelte informate prima di acconsentire all'utilizzo dei dati, influenzando i termini e le condizioni, stabiliti dalle organizzazioni di utenti dei dati, cui è subordinato l'utilizzo dei dati o risolvendo potenziali controversie tra membri di un gruppo sulle modalità di utilizzo dei dati quando tali dati riguardano più interessati all'interno di tale gruppo. In tale contesto è importante riconoscere che i diritti a norma del regolamento (UE) 2016/679 possono essere esercitati soltanto a titolo individuale e non possono essere conferiti o delegati a una cooperativa di dati. Le cooperative di dati potrebbero altresì rappresentare uno strumento utile per imprese individuali, microimprese e piccole e medie imprese che in termini di conoscenze in materia di condivisione dei dati sono spesso equiparabili ai singoli individui».

organizzazioni di utenti dei dati, cui è subordinato l'utilizzo dei dati, in modo da offrire scelte migliori ai singoli membri del gruppo, o trovando possibili soluzioni alle posizioni contrastanti dei singoli membri di un gruppo in merito alle modalità di utilizzo dei dati laddove tali dati riguardino più interessati all'interno di tale gruppo. In tale contesto è importante riconoscere che i diritti a norma del regolamento (UE) 2016/679 sono diritti personali dell'interessato e che quest'ultimo non può rinunciarvi (...).

L'irrinunciabilità dei diritti dell'interessato, pacificamente riconosciuta, è però cosa ben diversa dalla loro non delegabilità: anzi, il *revirement* del legislatore europeo sulla formulazione del considerando in esame e le funzioni di *empowerment* dei diritti dell'interessato affidate all'intermediario, lasciano supporre l'ammissibilità dell'attribuzione di poteri di rappresentanza volontaria alla cooperativa di dati e, in generale, all'intermediario di dati (anche ove non svolgesse la propria attività in forma cooperativa)⁵⁷.

Sull'ammissibilità della delega – ed in particolare nei confronti di persone giuridiche – si è espresso, nel tempo, anche il Garante per la protezione dei dati personali. In un caso concernente un'associazione sportiva, nell'ambito di una fattispecie relativa alla pubblicazione di elenchi, l'*Authority* aveva affermato che «non è ipotizzabile, né previsto

⁵⁷ Attenta dottrina ha affermato che «Sebbene gli esercizi di esegesi delle norme di matrice europea sulla base delle categorie del diritto interno debbano sempre essere condotti con grande prudenza, sembrerebbe ragionevole ritenere che mentre il divieto della rinuncia, quale tipico atto abdicativo, implichi l'impossibilità del conferimento in società (atto con efficacia reale), esso non preclude invece la stipula di un contratto di *mandato* (*con rappresentanza*), in quanto atto con mera efficacia obbligatoria. Sembrerebbe quindi aprirsi un più ampio spazio operativo quanto meno per la *tutela esterna dei diritti degli interessati da parte di una cooperativa di dati che operi come rappresentante dei suoi membri*». Così RESTA, *Pubblico, privato e collettivo nel sistema europeo di governo dei dati*, in *Riv. trim. dir. pubbl.*, 2022, 4, 971-995, e, *ivi*, par. 5.

Nella *Joint Opinion n. 3/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act)*, 2021, 35, l'EDPB e l'EDPS mostravano invero di condividere il principio di non delegabilità dei diritti dell'interessato (esplicitato nel citato *considerando* n. 24 della proposta di Regolamento sulla *governance* europea dei dati), mettendo in rilievo la contraddizione di tale principio con le norme che attribuivano alla cooperativa dei dati il potere di negoziare termini e condizioni di maggior vantaggio per gli interessati.

La scelta finale del legislatore europeo è stata però quella di comporre la contraddizione facendo salva la negoziabilità ad opera delle *data cooperatives* ed eliminando, al contempo, ogni riferimento al divieto di delega. Quest'ultima, dunque, è da ritenersi pienamente ammissibile in materia di protezione dei dati personali; ciò non solo per le considerazioni che attengono al ripensamento del legislatore europeo nel passaggio dalla proposta al testo definitivo del regolamento, ma anche per ragioni di carattere sistematico.

dalla legge (...) un diritto dell'associazione ad esercitare i diritti che rientrano nella personale disponibilità di ciascun interessato, a meno che essa possa dimostrare l'esistenza di una specifica *delega* da parte del singolo associato»⁵⁸.

Anche più recentemente, sotto l'egida del GDPR, è stata più volte confermata dal Garante l'ammissibilità della delega per l'esercizio dei diritti dell'interessato, ad esempio là dove ha precisato che «la disciplina in materia di protezione dei dati personali prevede – in ambito sanitario – che le informazioni sullo stato di salute devono essere comunicate all'interessato e possono essere comunicate a terzi solo sulla base di un idoneo presupposto giuridico o su indicazione dell'interessato stesso previa *delega* scritta di quest'ultimo (art. 9 Regolamento e art. 83 del Codice in combinato disposto con l'art. 22, comma 11, d.lgs. 10 agosto 2018, n. 101; cfr. anche provv. generale del 9 novembre 2005, consultabile in *www.gdpd.it*, doc. *web* n. 1191411, ritenuto compatibile con il suddetto Regolamento e con le disposizioni del decreto n. 101/2018; cfr. art. 22, comma 4, del citato d.lgs. n. 101/2018)»⁵⁹.

Ulteriore casistica è stata trattata con maggior incertezza da parte del Garante, proprio in tema di intermediazione di dati.

L'iniziale istruttoria, già richiamata, sul caso Hoda srl, intermediario di dati che fornisce il servizio Weople e l'omonima *app*, aveva portato

⁵⁸ Garante per la protezione dei dati personali, nota del 30 novembre 1999, doc. *web* n. 1164456. Cfr., *amplius*, BRAVO, *Associazioni sportive dilettantistiche (ASD) e protezione dei dati personali negli orientamenti del Garante*, in *Diritto dello Sport*, 2021, 2, 11-29, ivi p. 24 s.

⁵⁹ In questo senso v. Garante per la protezione dei dati personali, Provvedimento del 29 aprile 2021, n. 174, doc. *web* n. 9676143. La delega è stata ritenuta ammissibile anche per la prestazione del reclamo al Garante in luogo dell'interessato: si veda, in tal senso, il provvedimento del Garante n. 209 del 12 maggio 2022, doc. *web* n. 9790093, ove l'Autorità di settore si è pronunciata sul « (...) reclamo presentato al Garante, ai sensi dell'art. 77 del Regolamento, in data 10 maggio 2020 con il quale XX, su *delega* del fratello XX residente all'estero al momento della presentazione del reclamo, ha chiesto di ordinare a Google LLC la rimozione dai risultati di ricerca reperibili in associazione al nominativo del fratello di due URL che riportano una notizia risalente al 2017 relativa ad un procedimento penale che ha riguardato il reclamante per un fatto avvenuto nella città canadese di XX». Si noti che il GDPR, all'art. 80, par. 1, prevede espressamente che l'interessato abbia «il diritto di dare *mandato* a un organismo, un'organizzazione o un'associazione senza scopo di lucro, che siano debitamente costituiti secondo il diritto di uno Stato membro, i cui obiettivi statutari siano di pubblico interesse e che siano attivi nel settore della protezione dei dati personali, di proporre il reclamo per suo conto e di esercitare per suo conto i diritti di cui agli artt. 77, 78 e 79 nonché, se previsto dal diritto degli Stati membri, il diritto di ottenere il risarcimento di cui all'articolo 82». La norma *de qua* non è stata considerata di ostacolo, secondo l'interpretazione del Garante, per l'ammissibilità del reclamo ad opera del fratello dell'interessato su *delega* di quest'ultimo, al fine di esercitare il corrispondente diritto.

inizialmente l'Autorità a dubitare della legittimità della delega da utilizzare per l'esercizio del diritto alla portabilità dei dati dei propri clienti sul proprio sistema di trattamento, al fine di consentire il *secondary use* verso altri *data users*, con le dinamiche tipiche dei servizi di intermediazione⁶⁰. Sollevata la questione in ambito europeo, presso l'*European Data Protection Board*, l'istruttoria non aveva avuto un immediato seguito, se non sul piano legislativo tramite il recepimento dei servizi di intermediazione nell'ambito del *Data Governance Act*, in continuità con le nuove strategie europee sui dati delineati dalla Commissione europea⁶¹.

⁶⁰ Cfr. la Lettera del Presidente del Garante per la protezione dei dati personali al Presidente dell'*European Data Protection Board* (EDPB), del 1° agosto 2019, avente ad oggetto «*Richiesta di parere in tema di commercializzazione dei dati personali e diritto alla portabilità*» (Garante per la protezione dei dati personali, doc web n. 9126725 del 1° agosto 2019, reperibile online all'indirizzo <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9126725>, consultato da ultimo in data 30 giugno 2025). Significativo è il tenore di tale missiva, indirizzata al Presidente dell'EDPB e resa disponibile sul sito del Garante: «come deciso dal collegio del Garante, trasmetto copia della richiesta di parere all'EDPB che gli uffici dell'Autorità stanno inserendo sulla piattaforma IMI. Come vedrai, si tratta di una questione molto rilevante che, pur venuta in evidenza in Italia, impone una riflessione generale che non può essere rimessa alle singole autorità di protezione dati. Il caso riguarda l'applicazione del diritto alla portabilità dei dati: un'impresa italiana si è infatti proposta come intermediaria nel rapporto fra titolari ed interessati chiedendo, su delega di questi ultimi, di ottenere le informazioni personali custodite presso importanti soggetti imprenditoriali, in particolare nel settore della grande distribuzione al fine di riunirle all'interno di una propria banca dati da sottoporre ad *enrichment*. Il tema è dunque legato alla "commerciabilità" dei dati, con l'ulteriore complicazione dell'esercizio per delega del diritto ed il conseguente non remoto rischio di possibili duplicazioni delle banche dati oggetto di portabilità. Ti ringrazio per l'attenzione che vorrà dedicare a tale delicata questione (...), sinceramente dispiaciuto di non poter essere presente al momento della sua discussione a causa del termine del nostro mandato (...)».

⁶¹ La ricostruzione della vicenda si trova e le sfumature contenute nella richiesta di parere che il Garante ha avanzato all'EDPB sono state esplicitate nel Comunicato stampa del 1° agosto 2019, doc. web n. 9126709, nel quale si legge che «Con una lettera a firma del Presidente Antonello Soro, l'Autorità Garante per la *privacy* ha posto all'attenzione del Comitato europeo per la protezione dei dati personali (EDPB) la questione relativa a "Weople", l'*app* che promette ai propri iscritti una remunerazione in cambio della cessione dei loro dati personali. A partire dai primi mesi del 2019 sono state diverse le segnalazioni giunte all'Autorità da parte di imprese della grande distribuzione che lamentavano di aver ricevuto da parte di "Weople" numerosissime richieste di trasferire alla piattaforma dati personali e di consumo registrati nelle carte di fedeltà. L'impresa italiana, che gestisce la *app* e offre servizi di vario genere (offerte commerciali, analisti statistiche e di mercato), si propone infatti come intermediaria nel rapporto tra aziende e utenti chiedendo, su delega di questi ultimi, di ottenere le informazioni personali custodite presso grandi imprese allo scopo di riunirle all'interno della propria banca dati. L'attenzione del Garante si è concentrata, in particolare, sulla corretta applicazione, da parte della società, del cosiddetto diritto alla "portabilità dei dati" introdotto dal nuovo Regolamento europeo, con l'ulteriore complicazione determinata dall'esercitare tale diritto mediante una delega e con il conseguente

L'esperienza significativa sul caso Weople, tuttavia, ha alimentato un confronto anche su altri tavoli, in quanto la fattispecie è stata oggetto di disamina anche nell'*Indagine conoscitiva sui Big Data*, condotta congiuntamente dal Garante per la protezione dei dati personali, dall'Autorità Garante per la Concorrenza e il Mercato (AGCM) e dall'Autorità per le Garanzie nelle Comunicazioni (AGCOM), nell'ambito della quale il *business model* adottato per la fornitura del servizio di *data intermediation*, basato sull'esercizio del diritto alla portabilità dei dati accompagnato dal conferimento della delega all'intermediario, era stato positivamente valutato, in quanto «Tali iniziative potrebbero fungere da strumento di *consumer empowerment* potenzialmente in grado di superare in parte le descritte limitazioni derivanti dall'attuale disciplina del diritto alla portabilità dei dati, in termini di contribuzione alla costruzione di una consapevolezza da parte degli utenti circa il valore economico dei loro dati personali, grazie all'ottenimento di una remunerazione per l'utilizzo di tali dati da parte di soggetti terzi»⁶².

rischio di possibili duplicazioni delle banche dati oggetto di portabilità. L'altro aspetto segnalato dal Garante nella lettera riguarda il delicato tema della “*commerciabilità*” dei dati, causata dall'attribuzione di un vero e proprio *controvalore al dato personale*. Su entrambe le questioni, il Garante ha dunque chiesto al Comitato, che riunisce tutte le Autorità Garanti dell'Unione, di pronunciarsi. L'attività di “Weople”, scrive il Garante, “può produrre effetti in più di uno Stato dell'Unione” in ragione delle richieste di portabilità che potranno essere avanzate e delle questioni relative alla “valorizzazione economica dei dati personali ed alla natura ‘pro-concorrenziale’ del diritto alla portabilità”. Per questi motivi, pur essendo emerso in Italia, il caso della *app* impone, ad avviso del Garante, una riflessione generale che è più opportuno condividere con le altre Autorità di protezione dati. Il Garante attenderà dunque il parere dell'EDPB per concludere l'istruttoria avviata sulla *app* (...).».

⁶² GPDP-AGCM-AGCOM, *Indagine conoscitiva sui Big Data*, Rapporto finale, 10 febbraio 2020, disponibile *online*, doc. web n. 9264297, 99. Ivi le Autorità, nella rassegna in tema di *data portability*, hanno evidenziato che «(...) esempi di strumenti di portabilità dei dati attraverso un mezzo automatizzato (generalmente *app*) vengono, *inter alia*, dall'Italia, dove sono stati sviluppati sistemi che consentono agli utenti di richiedere a diversi titolari di trattamento l'estrazione dei propri dati personali e di archivarli in un'area dedicata (ad esempio, Weople). Con l'inserimento dei dati personali nell'area dedicata l'utente riceve una remunerazione, che deriva dai pagamenti che i titolari di trattamento effettuano per avere degli spazi pubblicitari all'interno di dette aree e per la mera lettura delle offerte commerciali da parte degli utenti destinatari (c.d. mercato dell'attenzione). I dati presenti nelle aree dedicate possono essere, peraltro, ulteriormente elaborati tramite un'attività di profilazione. Successivamente i risultati di tali attività verrebbero venduti alle imprese interessate alla loro acquisizione, anche in questo caso per lo svolgimento campagne pubblicitarie e/o offerte commerciali personalizzate, generando per gli utenti ulteriori fonti di remunerazione dell'utilizzo dei dati personali degli utenti medesimi». Ovviamente la destinazione di tali dati per l'uso secondario può ben riguardare il settore della ricerca scientifica, come ad esempio avviene nell'ambito del Progetto UE Next Generation PNRR PE09 “GRINS – *Growing Resilient, Inclusive and Sustainable*” (<https://www.grins.it/progetto>).

Nel frattempo proprio sul servizio Weople fornito da Hoda s'è pronunciata anche l'AGCM, che ha accolto le rimostranze da questa avanzate nei confronti di Google, là dove, in chiave anticoncorrenziale, appariva restia ad adeguare i propri sistemi informatici per favorire le richieste di portabilità avanzate dall'intermediario, su delega dei propri clienti⁶³.

Da ultimo, alla fine del 2024, il Garante per la protezione dei dati personali è tornato ad occuparsi ancora del caso Weople, in altro procedimento maturato a seguito di istruttoria avviata nel 2021, in base a segnalazioni e reclami provenienti prevalentemente da aziende della grande distribuzione, culminato con provvedimento n. 704 del 14 novembre 2024 doc. *web* n. 10108848⁶⁴.

Le questioni affrontate in tale provvedimento sono molteplici, tra cui: (i) l'individuazione della corretta base giuridica del trattamento posto in essere dall'intermediario, anche con riguardo al trattamento concernenti minori; (ii) l'inclusione, nella valutazione di impatto di cui all'art. 35 GDPR, delle ripercussioni che la commercializzazione dei dati ha sulla libera prestazione del consenso al trattamento dei dati e

⁶³ Cfr. provvedimento dell'AGCM del 5 luglio 2022, di avvio dell'istruttoria, reso nei confronti di Google LLC, su segnalazione di Hoda S.r.l., società italiana attiva nell'intermediazione di dati personali attraverso l'app denominata "Weople", seguito dal provvedimento dell'AGCM del 18 luglio 2023, di chiusura dell'istruttoria, con interventi di Mediaset Spa, Computer & Communications Industry Association, Associazione Italiana Internet Provider (AIIP) ed Altroconsumo. Il procedimento era nato a seguito delle lamentele di Hoda in ordine alla condotta asseritamente anticoncorrenziale di Google, che avrebbe frapposto ostacoli tecnici alla portabilità dei dati richiesti da Hoda per conto dei propri clienti, al fine del loro riuso anche in ambito commerciale. A pag. 4 (par. 9) del provvedimento del 2003 l'AGCM afferma che «La condotta contestata a Google, nel pregiudicare l'esercizio, da parte dell'utente finale, del diritto alla portabilità dei propri dati stabilito dall'articolo 20, comma 2, del GDPR, si risolve in un indebito sfruttamento, da parte della stessa Google, dei consumatori finali nella misura in cui determina una limitazione dei benefici che i consumatori potrebbero trarre dalla valorizzazione dei loro dati personali. Tale condotta presenta un ulteriore carattere restrittivo della concorrenza nella misura in cui limita la possibilità di operatori alternativi a Google di sviluppare forme innovative di utilizzo dei dati personali. In particolare, Hoda ha rappresentato gli effetti negativi della condotta di Google sulla sua iniziativa volta a sviluppare, attraverso la piattaforma Weople, una innovativa attività commerciale, consistente nel valorizzare i dati personali con l'autorizzazione del suo titolare in prospettive merceologiche ancora inesplorate, con particolare riferimento al contesto geografico nazionale». Nel corso del procedimento Google presentava, ai sensi della disciplina *antitrust*, una serie di impegni per far venir meno i profili anticoncorrenziali emersi in sede istruttoria, che l'*Authority* considerava idonei e rendeva conseguentemente obbligatori nei confronti di Alphabet Inc., Google LLC, Google Ireland Limited e Google Italy Srl.

⁶⁴ Non è chiaro, in realtà, se si tratti dell'epilogo della vicenda per la quale c'era stato l'interessamento dell'EDPB, in seguito dell'originaria istruttoria, o se si tratti di procedimento riavviato *ex novo*, sulla base di altre segnalazioni pervenute all'Autorità, in nuova composizione. Nel provvedimento tale aspetto non viene chiarito esplicitamente.

le misure da adottare per preservare tale libertà; (iii) il meccanismo di delega per l'esercizio dei diritti dell'interessato, incluso il diritto alla portabilità dei dati e i limiti alla sua estensione. Rimandando ad altra sede una più dettagliata analisi dell'intero provvedimento, ai fini del discorso che si sta conducendo in questa sede mi preme rimarcare i significativi passaggi argomentativi sul rapporto tra delega ed esercizio del diritto dell'interessato alla portabilità dei dati.

Il Garante, con il provvedimento ad esame, si pronuncia sia nel senso dell'*ammissibilità della delega* per l'esercizio dei diritti dell'interessato, sia nel senso che la medesima possa essere rivolta ad una *persona giuridica*, ma rimarca anche che, nel peculiare contesto del trattamento dei dati personali, l'ammissibilità di principio, sul piano giuridico, si accompagna con l'individuazione di requisiti rigorosi, volti ad accertare che la manifestazione di volontà dell'interessato sia specifica ed inequivoca e tale da circoscrivere l'operatività del rappresentante sia sul piano oggettivo che su quello temporale, non potendosi ritenere accettabile, nella materia *de qua*, una delega generale e *sine die*⁶⁵.

Per il Garante, nel provvedimento citato, la delega all'intermediario è dunque ammissibile, anche se è persona giuridica, ma deve riferirsi «ad un *singolo atto* – o ad una *serie predeterminata di atti* – di esercizio dei diritti nei confronti del titolare originario» e non può essere «utilizzata *illimitatamente e fino a “revoca”* (...) in ragione delle esigenze legate allo sfruttamento commerciale dei dati personali dell'interessato»⁶⁶.

La delega in altre parole, come argomentato dall'Autorità, eredita le caratteristiche dell'atto delegato e ciò conduce all'individuazione di limiti, desumibili dal sistema anche se non esplicitati sul piano normativo, che segnano i confini stessi della sua ammissibilità. Sul punto, infatti, il Garante rimarca che «Nel caso in argomento, (...) la medesima esigenza che la delega per l'esercizio del diritto alla portabilità assuma le caratteristiche dell'atto delegato (sia quindi *contenuta in un documento che si riferisca ad una o più specifiche attività* il cui oggetto è *compiutamente definito* e possa prevedere la *reiterazione di tali atti-*

⁶⁵ Nel provvedimento n. 704 del 14 novembre 2024, doc. web n. 10108848, il Garante per la protezione dei dati personali chiarisce che «Con riferimento alla *delega avente ad oggetto l'esercizio dei diritti dell'interessato* e, in particolare, il *diritto alla portabilità* è stato osservato nell'atto di avvio del procedimento amministrativo che la stessa, dovendo avere quantomeno i *requisiti* degli atti che si intendono compiere in rappresentanza dell'interessato, dovrebbe essere indicatrice di una *volontà specifica e inequivoca dell'interessato* stesso, *circoscrivendo l'operatività del delegato sia dal punto di vista oggettivo che temporale*».

⁶⁶ *Ibidem*.

vità solo se espressamente menzionata) rappresenta, in virtù del rango dei diritti oggetto di tutela, un requisito minimo sia per garantire agli interessati un reale ed effettivo controllo sul trattamento dei propri dati personali, sia per consentire al titolare originario di comprovare l'inequivoca volontà dei soggetti che intendono esercitare i propri diritti».

Altro problema riguarda l'estensione della delega e, in particolare, se la medesima possa concernere anche la *revoca del consenso*. Il Garante la esclude in considerazione della collocazione sistematica dell'art. 7 GDPR, in cui la revoca del consenso al trattamento dei dati personali trova la sua disciplina. L'articolo in questione si trova nel Capo relativo alle condizioni di liceità del trattamento e non in quello dedicato all'esercizio dei diritti dell'interessato, disciplinati invece agli artt. 12-23 GDPR. Meno condivisibile risulta invece l'assunto, contenuto del provvedimento in parola, secondo cui il consenso al trattamento sarebbe da ritenersi «atto personalissimo»: come s'è già avuto modo di rilevare⁶⁷, lo stesso GDPR, all'art. 8, prevede che, qualora il consenso non possa essere prestato direttamente dal minore per via dei limiti ivi delineati, deve essere manifestato da chi esercita la responsabilità genitoriale e ne ha dunque la rappresentanza *ex lege*⁶⁸.

È utile ripercorrere *verbatim* il passaggio argomentativo rinvenibile nel provvedimento citato, nel quale, con riguardo al tema ora in parola, si trova annotato che, «Quanto alla delegabilità della revoca del consenso, invece, si prende atto delle argomentazioni difensive tendenti a ricondurre tale azione nell'alveo dei diritti di cui agli artt. 15-22 del Regolamento e a consentirne la delegabilità. Tuttavia, deve confermarsi quanto osservato nell'atto di avvio del procedimento amministrativo, e cioè che la collocazione della previsione della facoltà di revoca del consenso nell'ambito dell'art. 7 del Regolamento ha una ragione sistematica ben chiara, e cioè quella di equiparare i connotati e gli effetti della dichiarazione di volontà negativa in ordine allo svolgimento dei trattamenti a quelli della dichiarazione di volontà positiva, sia con riferimento alle forme di espressione che agli effetti. Da questo punto

⁶⁷ Cfr. *supra*, nonché BRAVO, *Le condizioni di liceità del trattamento di dati personali*, in FINOCCHIARO (a cura di), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, 2019, 110-193, ed. *ivi*, spec. 167; BRAVO, *Il consenso e le altre condizioni di liceità del trattamento di dati personali*, in FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, 2017, 101-178, e. *ivi*, spec. 168.

⁶⁸ Ciò esclude, evidentemente, la natura di «atto personalissimo» del consenso, essendo altrimenti precluso al genitore o al tutore il compimento dell'atto per conto del minore, come ad esempio avviene in caso di riconoscimento del figlio naturale.

di vista l'istituto del consenso rappresenta ormai *atto personalissimo*, nonché lo strumento di garanzia del diritto fondamentale in grado di realizzare l'autodeterminazione informativa (l'art. 8 della Carta dei diritti fondamentali dell'Unione europea lo parifica alla riserva di legge) e non può, per tale ragione, essere ridotto ad atto dispositivo *stricto sensu* delegabile in grado di vanificare il contenuto stesso del diritto chiamato a garantire. Ricondurre la volontà di revoca del consenso nell'ambito dell'esercizio dei diritti dell'interessato, oltre a non trovare riscontro nelle disposizioni normative, sottrarrebbe all'interessato quella facoltà di espressione diretta e anche semplificata della propria volontà (in linea con il consenso precedentemente acquisito) di interrompere con effetto immediato il trattamento, determinando un ingiustificato disallineamento fra consenso e revoca, a tutto danno proprio dell'interessato»⁶⁹.

Si tratta di osservazioni che, seppur vagliabili criticamente, non possono essere trascurate neanche con riguardo ai servizi di delega che dovranno essere approntati per gli spazi di condivisione di dati, previsti dal Reg. EHDS, la cui definizione è rimessa al legislatore nazionale.

5. *European Health Data Space e data intermediation*

L'intermediazione di dati in ambito sanitario è fenomeno che trova la sua manifestazione a prescindere dalla regolamentazione di spazi di dati sanitari di cui al Reg. UE 2025/327⁷⁰.

A tal riguardo può considerarsi, innanzitutto, il *data altruism*, che sin dalla definizione contenuta nel *Data Governance Act*, è preordinato ad alimentare, *inter alia*, il flusso di dati dell'assistenza sanitaria, da inquadrare non solo nell'ambito dell'uso primario dei dati gestiti con l'EHDS, ma anche con riferimento ai trattamenti che possono essere svolti in relazione alle ulteriori finalità rilevanti per l'uso secondario, quali la ricerca scientifica e l'elaborazione di politiche pubbliche in ambito sanitario⁷¹.

⁶⁹ Garante per la protezione dei dati personali, Provvedimento n. 704 del 14 novembre 2024, doc. web n. 10108848, cit.

⁷⁰ Il riferimento è ai tre ambiti di intermediazione sostanziale delineati dal *Data Governance Act*: quello relativo al riuso dei dati detenuti da soggetti pubblici; quello relativo alla fornitura di servizi di intermediazione di dati in forma cooperativa e non cooperativa; quello relativo al *data altruism*. Che in tutti e tre gli ambiti si tratti di fenomeni di *data intermediation*, a prescindere dalle etichette usate dal legislatore europeo, è argomento che è stato affrontato in BRAVO, *Data Governance Act and Re-Use of Data in the Public Sector*, in *European Review of Digital Administration & Law (ERDAL)*, 2022, Vol. 3, Issue 2, 13-33, a cui *amplius* si rinvia.

⁷¹ L'«altruismo dei dati», infatti, viene definito, all'art. 2, par. 1, n. 16), del *Data Governance Act*, come «la condivisione volontaria di dati sulla base del consenso accordato

V'è poi da considerare l'intermediazione dei dati, svolta in forma cooperativa, in ambito sanitario⁷², ove ad esempio sia posta in essere da pazienti che, con l'aggregazione dei propri dati, possono trarre utilità valorizzabile su differenti piani, incluso quello della ricerca in ambito farmaceutico⁷³ o nelle relazioni di cura⁷⁴. Il fenomeno tende a creare dei "micro" spazi di condivisione di dati sanitari, con aggregatori di dati che possono essere utilizzati a beneficio dei propri membri con scopo mutualistico e destinati alla loro valorizzazione, con dinamiche gestorie e di controllo sui dati che, nell'intermediazione cooperativa, sono improntate a democraticità e al diretto coinvolgimento degli interessati⁷⁵.

Si pensi ancora all'intermediazione di dati sanitari provenienti da intermediari che gestiscono dispositivi biomedicali o strumenti *wearable* ed altri dati che possono avere rilevanza sia sul piano dell'assistenza

dagli interessati al trattamento dei dati personali che li riguardano, o sulle autorizzazioni di altri titolari dei dati volte a consentire l'uso dei loro dati non personali, senza la richiesta o la ricezione di un compenso che vada oltre la compensazione dei costi sostenuti per mettere a disposizione i propri dati, *per obiettivi di interesse generale*, stabiliti nel diritto nazionale, ove applicabile, *quali l'assistenza sanitaria*, la lotta ai cambiamenti climatici, il miglioramento della mobilità, l'agevolazione dell'elaborazione, della produzione e della divulgazione di statistiche ufficiali, il miglioramento della fornitura dei servizi pubblici, l'elaborazione delle politiche pubbliche o la ricerca scientifica nell'interesse generale».

⁷² Per l'esplorazione di una casistica si veda RUFO, *Data Governance Act e cooperative di dati: una "possibile" nuova frontiera per la ricerca in sanità*, in F. BRAVO (a cura di), *EU Data Cooperatives. L'ingresso delle cooperative di dati nell'ordinamento europeo*, cit., 487 ss. e, ivi, spec. 495 ss., con riferimento ai casi Savvy Cooperative, MIDATA, Salus Coop, LunaDNA.

⁷³ Si veda, a tal riguardo, DE VICO, *I servizi di cooperazione di dati nella ricerca clinica farmaceutica: analisi e prospettive*, in BRAVO (a cura di), *EU Data Cooperatives. L'ingresso delle cooperative di dati nell'ordinamento europeo*, cit., 500 ss.

⁷⁴ Anche al di fuori del modello di *data cooperatives* la valorizzazione di aggregazione di dati da parte di comunità di pazienti può seguire percorsi significativi. Si rimanda, ad esempio, alle riflessioni di una decina di anni orsono, esternate in tema di *communities* socio-sanitarie su piattaforme di *social network*: BRAVO, *EHealth e social networks per la realizzazione di communities socio-sanitarie in tema di malattie rare. Riflessioni giuridiche tra diritti fondamentali e responsabilità civile*, in FARALLI, BRIGHI, MARTONI (a cura di), *Strumenti, diritti, regole e nuove relazioni di cura. Il paziente europeo protagonista nell'eHealth*, Torino, 2015, 109-131.

⁷⁵ BRAVO, *Le cooperative di dati*, cit., 779 ss. e 781 ss. Si veda anche PALLADINI, SCAGLIARINI, *Le cooperative di dati come forma di tutela collettiva degli interessati: un'opportunità per l'ambito sanitario?*, cit., 416, là dove viene affermato che, con le «cooperative di dati, il legislatore europeo sembra aver colto l'esigenza di affiancare al singolo interessato enti collettivi capaci non solo di assisterlo, come potrebbe fare anche un soggetto terzo, ma anche di permettergli di farsi parte attiva dell'organizzazione e del funzionamento dell'ente, contribuendo ad una forma di rappresentanza e tutela mutualistica di un interesse comune ad altri soggetti cui i dati intermediati si riferiscono».

sanitaria, sia su quello della ricerca (o comunque del *secondary use*), anche in relazione all'acquisizione dei c.d. *real world data*⁷⁶.

Si tratta di dati che potrebbero alimentare l'EHDS mediante gli istituti previsti dal nuovo Regolamento e, tra questi, anche mediante il «*Diritto delle persone fisiche di inserire informazioni nella propria cartella clinica elettronica*» di cui all'art. 5, esercitabile pure tramite rappresentanti⁷⁷.

Quanto invece all'intermediazione di enti pubblici che siano detentori di dati appartenenti a particolari categorie e che intendano destinarli al riuso ai sensi del Capo II del *Data Governance Act*, ove operanti in ambito sanitario, va rilevato che essi finiscono per essere istituzionalizzati nel sistema di trattamento delineato con lo spazio europeo di dati sanitari e sono obbligati a rendere disponibili i predetti dati anche per l'uso secondario, ai sensi dell'art. 51 del Regolamento.

V'è infine da rilevare come il nuovo regolamento sull'*European Health Data Space* abbia concretamente affrontato il fenomeno dell'intermediazione dei dati.

Leggendo con attenzione il testo dei *considerando* e quello dell'articolo normativo del Reg. EHDS, ci si può rendere conto che il legislatore europeo vi abbia voluto fare esplicito riferimento e ciò merita di essere considerato per le implicazioni di sistema, soprattutto con riguardo ai «dati sanitari elettronici personali», da intendersi come «i dati relativi alla salute e i dati genetici che sono trattati in formato elettronico»⁷⁸.

A seguito della considerazione che gli «Stati membri dovrebbero designare autorità di sanità digitale competenti per la pianificazione e l'attuazione di norme per l'accesso ai dati sanitari elettronici e per la loro trasmissione, nonché per l'applicazione dei diritti delle persone fisiche e dei professionisti sanitari, sotto forma di autorità separate o come parte di autorità già esistenti (...)»⁷⁹, il nuovo Regolamento indica quali com-

⁷⁶ LIU, PANAGIOTAKOS, *Real-world data: a brief review of the methods, applications, challenges and opportunities*, in *BMC Med Res Methodol* 22, 287 (2022), <https://doi.org/10.1186/s12874-022-01768-6>.

⁷⁷ L'art. 5 cit. del Reg. EHDS stabilisce che «Le persone fisiche o i loro rappresentanti di cui all'articolo 4, paragrafo 2, hanno il diritto di *inserire informazioni* nella propria cartella clinica elettronica attraverso servizi o applicazioni di accesso ai dati sanitari elettronici collegati a tali servizi come indicato al medesimo articolo. *Le informazioni inserite dalla persona fisica o dal suo rappresentante sono chiaramente distinguibili come tali*. Le persone fisiche o i loro rappresentanti di cui all'articolo 4, paragrafo 2, non hanno la possibilità di modificare direttamente i dati sanitari elettronici e le relative informazioni inseriti dai professionisti sanitari».

⁷⁸ Art. 2, par. 2, lett. a), del Reg. EHDS.

⁷⁹ *Considerando* n. 30 del Reg. EHDS, il quale prosegue precisando che «(...) Nella maggior parte degli Stati membri esistono già autorità di sanità digitale che si occupa-

petenze e quali attività spettano loro, rimarcando anche che sono tenute all'adozione di «*soluzioni di intermediazione e portali per i pazienti*»⁸⁰.

Non viene però chiarito a quali soluzioni, nello specifico, si faccia riferimento, con ciò lasciando le predette autorità maggiormente libere di indirizzarsi verso le soluzioni che maggiormente soddisfino le esigenze, attingendo eventualmente a modelli già sperimentati o definiti nell'esperienza giuridica europea.

Nel Reg. EHDS l'intermediazione di dati sanitari viene considerata anche con riguardo allo snellimento degli oneri amministrativi e per giungere a soluzioni di maggior efficacia ed efficienza, qualora vi siano soggetti pubblici o privati che ricevano finanziamenti pubblici, da fondi nazionali o europei, «per raccogliere e trattare dati sanitari elettronici per la ricerca, le statistiche sia ufficiali che non ufficiali, o altre finalità simili, anche in ambiti in cui la raccolta di tali dati è frammentata o difficile, quali quelli relativi alle malattie rare o al cancro»⁸¹. In tal caso, «al fine di massimizzare l'impatto dell'investimento pubblico e sostenere la ricerca, l'innovazione, la sicurezza dei pazienti o la definizione delle politiche, a beneficio della società»⁸², siffatti dati «dovrebbero essere messi a disposizione degli organismi responsabili dell'ac-

no di cartelle cliniche elettroniche, interoperabilità, sicurezza o normazione. Nello svolgimento dei loro compiti, le autorità di sanità digitale dovrebbero cooperare in particolare con le autorità di controllo istituite a norma del regolamento (UE) 2016/679 e con gli organismi di vigilanza istituiti a norma del regolamento (UE) n. 910/2014. Le autorità di sanità digitale possono inoltre cooperare con il comitato europeo per l'intelligenza artificiale istituito dal regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, il gruppo di coordinamento per i dispositivi medici istituito dal regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, il comitato europeo per l'innovazione in materia di dati istituito a norma del regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio e le autorità competenti ai sensi del regolamento (UE) 2023/2854 del Parlamento europeo e del Consiglio (...).

⁸⁰ Segnatamente, l'indicazione è contenuta nel *considerando* n. 32, in cui si trova affermato che «Le autorità di sanità digitale dovrebbero avere competenze tecniche sufficienti, riunendo possibilmente esperti di differenti organizzazioni. Le attività di tali autorità dovrebbero essere ben pianificate e monitorate al fine di garantirne l'efficienza. Le autorità di sanità digitale dovrebbero adottare le misure necessarie per proteggere i diritti delle persone fisiche mettendo a punto soluzioni tecniche nazionali, regionali e locali quali cartelle cliniche elettroniche nazionali, *soluzioni di intermediazione* e portali per i pazienti. È opportuno che, nell'adottare tali misure di protezione necessarie, le autorità sanitarie digitali applichino norme e specifiche comuni in tali soluzioni, promuovano l'applicazione delle norme e delle specifiche negli appalti e utilizzino altri mezzi innovativi come il rimborso di soluzioni conformi alle prescrizioni in materia di interoperabilità e sicurezza dello spazio europeo dei dati sanitari (...).

⁸¹ *Considerando* n. 59 del Reg. EHDS.

⁸² *Ibidem*.

cesso ai dati sanitari (...)»⁸³, in ragione del fatto che vengono «raccolti e trattati dai titolari dei dati sanitari con il sostegno di finanziamenti pubblici nazionali o dell'Unione»⁸⁴. In tale contesto, nella consapevolezza che ciò possa tradursi in un aggravio di oneri amministrativi o in un affaticamento dell'ordinaria attività, che finirebbe per perdere anche solo in parte la sua efficacia o la sua efficienza, il legislatore eurounitario ha ritenuto di accordare agli Stati membri la facoltà di prevedere, nell'ordinamento nazionale, che, «per talune categorie di titolari di dati sanitari»⁸⁵, le *funzioni* siano svolte da *intermediari di dati sanitari*⁸⁶, precisando che «Tali *intermediari di dati sanitari* dovrebbero essere persone giuridiche in grado di trattare, rendere disponibili, registrare, fornire o scambiare dati sanitari elettronici per l'uso secondario forniti da titolari dei dati, o limitarne l'accesso», svolgendo tuttavia «*compiti diversi* da quelli dei *servizi di intermediazione dei dati nell'ambito del regolamento (UE) 2022/868*»⁸⁷.

Non appare chiarissimo quale sia il senso della contrapposizione con i servizi di intermediazione di dati di cui al *Data Governance Act*. Si noti, comunque, che la proclamata diversità non riguarda la natura o la qualità soggettiva del fornitore di servizi di intermediazione di dati

⁸³ *Ibidem.*

⁸⁴ *Ibidem.*

⁸⁵ Quanto alle categorie di titolari di dati sanitari, il *considerando* n. 59 cit. fa riferimento sia a soggetti pubblici che a soggetti privati. Viene precisato, a tal riguardo, che «(...) In alcuni Stati membri i soggetti privati, compresi i prestatori di assistenza sanitaria privati e le associazioni professionali, svolgono un ruolo di fondamentale importanza nel settore sanitario. I dati sanitari detenuti da tali prestatori dovrebbero essere resi disponibili anche per l'uso secondario. I titolari dei dati sanitari nel contesto dell'uso secondario dovrebbero pertanto essere soggetti che sono prestatori di assistenza sanitaria o cure assistenziali o svolgono attività di ricerca in relazione ai settori dell'assistenza sanitaria o delle cure assistenziali, o sviluppano prodotti o servizi destinati ai settori dell'assistenza sanitaria o delle cure assistenziali. Tali enti possono essere pubblici, senza scopo di lucro o privati. In linea con tale definizione, le case di cura, i centri di assistenza diurna, i soggetti che forniscono servizi alle persone con disabilità, i soggetti che svolgono le attività commerciali e tecnologiche connesse all'assistenza, come i centri ortopedici e le imprese che forniscono servizi di assistenza, dovrebbero essere considerati titolari di dati sanitari. Anche le persone giuridiche che sviluppano applicazioni per il benessere dovrebbero essere considerate titolari di dati sanitari. Anche le istituzioni, gli organi e gli organismi dell'Unione che trattano tali categorie di dati relativi alla salute e all'assistenza sanitaria nonché i registri di mortalità dovrebbero essere considerati titolari di dati sanitari. Al fine di evitare un onere sproporzionato a loro carico, di norma le persone fisiche e le microimprese dovrebbero essere esentate dagli obblighi dei titolari di dati sanitari. Gli Stati membri dovrebbero tuttavia poter estendere gli obblighi dei titolari di dati sanitari alle persone fisiche e alle microimprese nel loro diritto nazionale (...)».

⁸⁶ *Considerando* n. 59 del Reg. EHDS.

⁸⁷ *Ibidem.*

di cui al predetto regolamento, ma solamente i «*compiti*», sicché l'intermediario di dati a cui fare eventualmente ricorso potrebbe ben essere anche quello istituito ai sensi di tale disciplina, già dotato di competenze tecniche e *know-how* per operare correttamente nel settore della *data intermediation*, con una rimodulazione di compiti, da definire nell'ordinamento nazionale a cura degli Stati membri, che dovranno essere ritagliati per le esigenze degli spazi di condivisione dei dati sanitari precisati nel *considerando* in parola⁸⁸.

Vi sono comunque margini per il ricorso all'intermediazione di dati sanitari nell'*European eHealth Data Space*, che passano per il vaglio del legislatore nazionale.

Il ricorso agli intermediari non è però senza limiti: gli Stati membri, infatti, non possono farvi ricorso per designarli quali «titolari dei dati sanitari affidabili»⁸⁹, ossia quali soggetti, designati dagli Stati membri, che possono avvalersi di una «*procedura di rilascio dell'autorizzazione dei dati* [che] può essere eseguita in modo semplificato, al fine di *alleviare l'onere amministrativo a carico degli organismi responsabili dell'accesso ai dati sanitari* nella gestione delle richieste di dati da essi trattati»⁹⁰.

Al di fuori dei *considerando* citati, in cui l'intermediazione dei dati compare più volte, il Reg. EHDS mostra cautela nel considerare tale istituto giuridico.

V'è un parco riferimento all'art. 2, par. 2, lett. k), con riguardo alla definizione di «*sistema di cartelle cliniche elettroniche*», intesa come «qualsiasi sistema in cui il *software* oppure la combinazione tra l'*hardware* e il *software* del sistema consente ai dati sanitari elettronici personali rientranti nelle categorie prioritarie di dati sanitari elettronici personali stabilite a norma del presente regolamento di essere conservati, *intermediati*, esportati, importati, convertiti, modificati o visualizzati e destinato dal fabbricante a essere utilizzato dai prestatori di assistenza sanitaria nel fornire cure assistenziali ai pazienti o dai pazienti nell'accedere ai loro dati sanitari elettronici». L'enunciata *intermediabilità* dei

⁸⁸ Come già evidenziato si tratta di esigenze orientate all'alleggerimento degli oneri amministrativi e al mantenimento dell'efficienza e dell'efficacia del sistema.

⁸⁹ Il divieto è enunciato nella parte finale del *considerando* n. 76 del Reg. EHDS.

⁹⁰ *Considerando* n. 76 del Reg. cit., ove si aggiunge che «I titolari dei dati sanitari affidabili dovrebbero essere autorizzati a valutare le domande di accesso ai dati sanitari presentate nell'ambito di questa procedura semplificata, sulla base delle loro competenze nell'affrontare il tipo di dati sanitari che stanno trattando, e di rilasciare una raccomandazione in merito a un'autorizzazione ai dati. L'organismo responsabile dell'accesso ai dati sanitari dovrebbe rimanere responsabile del rilascio dell'autorizzazione finale ai dati e non dovrebbe essere vincolato dalla raccomandazione fornita dal titolare dei dati sanitari affidabile».

dati sanitari elettronici personali rafforza dunque l'idea che il sistema delineato nel Reg. EHDS sia improntato alla *data intermediation*, ma di per sé nulla aggiunge in merito alla possibilità di ricorrere a fornitori di servizi di intermediazione diversi dai titolari di dati sanitari: l'intermediabilità dei dati a cui si fa riferimento, infatti, potrebbe essere quella raggiunta mediante il sistema congegnato con la realizzazione dell'*European eHealth Data Space*, che ne permette la circolazione tra soggetti diversi tanto per l'uso primario che per l'uso secondario, e non con il ricorso ad ulteriori servizi di intermediazione di dati.

Diverso è invece l'ulteriore esplicito riferimento all'intermediazione contenuto nell'art. 50 del Reg. EHDS, di apertura del Capo IV, dedicato all'«*Uso secondario*», e, in esso, della Sezione 1, intitolata alle «*Condizioni generali relative all'uso secondario*».

Tale articolo, rubricato «*Applicabilità ai titolari dei dati sanitari*», enuncia quali categorie di titolari dei dati sanitari siano da considerarsi esonerate dagli obblighi spettanti ai titolari dei dati sanitari con riguardo alla disciplina in tema di uso secondario (e vengono menzionate le persone fisiche, compresi i singoli ricercatori, e le persone giuridiche considerate microimprese), salvo consentire agli Stati membri la facoltà di stabilire, con norme dell'ordinamento nazionale, che gli obblighi in questione siano applicabili anche alle categorie soggettive che il Regolamento europeo ha inteso esonerare⁹¹ oppure che per determinate categorie di titolari dei dati sanitari gli obblighi vengano «assolti da entità di intermediazione di dati sanitari»⁹², con la precisazione che «In tal caso, i dati sono comunque considerati come messi a disposizione da vari titolari dei dati sanitari»⁹³, ai fini del loro uso secondario.

Stante la rilevanza che l'intermediazione di dati ha nelle strategie europee di *data governance*, sinceramente, ci si aspettava di più dal legislatore europeo sul versante dello spazio europeo di dati sanitari.

Il sistema delineato nel nuovo regolamento, istitutivo dell'*European Health Data Space* – mediante la previsione di norme e infrastrutture comuni e di un quadro di *governance* che faciliti l'accesso ai dati sanitari elettronici per l'uso primario e secondario dei dati sanitari elettronici – costituisce indubbiamente un'ottima innovazione, che enfatizza la prospettiva della circolazione dei dati personali e la loro «funzione sociale», declamata nel GDPR al *considerando* n. 4⁹⁴, e crea

⁹¹ Art. 50, par. 2, del Reg. EHDS.

⁹² Art. 50, par. 3, del Reg. EHDS.

⁹³ Art. 50, par. 3, del Reg. EHDS.

⁹⁴ In tale considerando viene precisato che «Il trattamento dei dati personali do-

indubbiamente i presupposti per un salto di qualità nell'assistenza sanitaria, nella ricerca e nell'innovazione, anche con riguardo allo sviluppo di tecnologie di intelligenza artificiale, che necessitano di dati di addestramento significativi e qualitativamente controllati.

Si ha però l'impressione che tale sistema, centralizzato, venga realizzato in una logica esclusiva ed in gran parte escludente i nuovi *player* del mercato: quegli "intermediari di dati" che il *Data Governance Act*, in attuazione della strategia europea dei dati, aveva voluto affermare, come soluzione europea alle dinamiche di mercato, dominate dalle multinazionali straniere, soprattutto americane (le c.d. *Big Tech*).

Il lodevole intento di realizzare un sistema efficace, centralizzato, di condivisione di dati in ambito sanitario, per come è congegnato, rischia di essere doppiamente escludente se lo si considera nella prospettiva del mercato e delle dinamiche di autodeterminazione informativa dei pazienti.

Per un verso finisce per "tagliare fuori" i nuovi intermediari, che rimangono ai margini del sistema di condivisione dei dati sanitari; per altro verso il Reg. EHDS, nel concentrare l'attenzione sull'uso primario dei dati e nel favorire l'uso secondario per esigenze connesse al pubblico interesse (e a quello commerciale che ruota intorno alla gestione centralizzata del *secondary use*)⁹⁵, finisce per "espropriare" sostanzialmente i pazienti della possibilità di controllo e di valorizzazione dei dati, per le dinamiche di uso secondario, escludendoli dalla possibilità di negoziazione sull'uso dei propri dati che, tramite l'intermediario, consentirebbe loro di ottenere vantaggi dagli utenti di dati⁹⁶.

vrebbe essere *al servizio dell'uomo*. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua *funzione sociale* e va temperato con altri diritti fondamentali, in ossequio al principio di proporzionalità (...). Sul punto si veda RICCI, *Sulla "funzione sociale" del diritto alla protezione dei dati personali*, in *Contratto e impresa*, 2017, 2, 586 ss., nonché BRAVO, *Il principio di solidarietà tra data protection e data governance*, in *Dir. inf.*, 2023, 3, 481-518 e, *ivi*, spec. 483 ss.

⁹⁵ Si pensi allo sviluppo di soluzioni di IA, solo per fare un esempio.

⁹⁶ Va ricordato ancora una volta che con il servizio di cooperativa di dati, ex art. 2, par. 1, n. 15, del *Data Governance Act*, viene a realizzarsi un servizio di intermediazione dei dati offerti da una struttura organizzativa costituita a soggetti che partecipano a tale struttura quali membri e che tale struttura, quale intermediario di dati con finalità mutualistiche, ha come obiettivi principali non solo quelli di aiutare i propri membri nell'esercizio dei loro diritti in relazione a determinati dati, anche per quanto riguarda il compiere scelte informate prima di acconsentire al trattamento dei dati, e di procedere a uno scambio di opinioni sulle finalità e sulle condizioni del trattamento dei dati che rappresenterebbero al meglio gli interessi dei propri membri in relazione ai loro dati, ma anche quello di negoziare i termini e le condizioni per il trattamento dei dati per conto dei membri prima di concedere l'autorizzazione al trattamento dei dati non personali o prima che essi diano il loro consenso al trattamento dei dati personali, ottenendo vantaggi in termini di valorizzazione dei dati,

Si ha cioè l'impressione che con il nuovo regolamento EHDS l'autorità pubblica si sostituisca d'imperio agli intermediari privati nella realizzazione di un sistema funzionale di condivisione di dati a livello europeo e faccia venir meno, nei confronti degli interessati, quell'utilità che gli stessi avrebbero potuto conseguire facendo uso dell'autonomia privata, ottenendo per sé quei vantaggi che l'intermediazione dei dati gli avrebbe potuto far conseguire.

Così come strutturato dal nuovo Regolamento, l'*European Health Data Space*, con riguardo al *secondary use* dei dati dei pazienti, sembra comportare una sorta di depotenziamento degli intermediari dei dati e degli stessi interessati, che, pur beneficiando di sistemi di portabilità evoluti che portano ad un arricchimento, su scala europea, delle possibilità di uso primario dei dati personali, svuotano nei confronti dei privati le possibilità connesse alla *governance* dei dati sul fronte dell'uso secondario, sterilizzando di fatto la possibilità di una loro diretta valorizzazione.

Poiché, come s'è potuto ricostruire in queste pagine, il fenomeno dell'intermediazione, seppur compresso, non pare affatto scomparire nell'impianto del Regolamento, avendo margini di applicazione che sono per lo più rimessi alle scelte del legislatore nazionale e delle autorità competenti chiamate a darne attuazione, si dovrebbero percorrere soluzioni che portino a valorizzare i fenomeni di intermediazione delineati nel *Data Governance Act* ed emergenti sulla base degli strumenti che il GDPR già consente.

Tra le soluzioni percorribili, oltre a quelle che mirino a valorizzare i richiami all'intermediazione dei dati di cui v'è traccia nel Reg. EHDS, sopra passati in rassegna, v'è anche quella che transita per l'applicazione dell'art. 1, par. 8, ai sensi del quale «Il presente regolamento lascia impregiudicato l'accesso ai dati sanitari elettronici per l'uso secondario *concordato nel quadro di accordi* contrattuali o amministrativi tra soggetti pubblici o privati».

È forse questa la via che consente, a chi gestisce lo spazio europeo di dati sanitari, di valorizzare il ruolo degli intermediari, ricorrendo ad accordi *ad hoc* per la disciplina dei rapporti, che permettano di preservare, seppur con le garanzie che la particolare natura dei dati impone a tutela dei diritti degli interessati, le possibilità di valorizzazione a loro vantaggio, non necessariamente economica, connesse alla gestione del *secondary use* dei dati intermediati.

nella concessione dell'uso secondario, che altrimenti il singolo interessato, per difetto di potere contrattuale, non riuscirebbe ad ottenere.