RIVISTA ITALIANA DI INFORMATICA E DIRITTO
Periodico internazionale di diritto, giustizia e tecnologie

ISSN 2704-7318 • n. 2/2025 • DOI 10.32091/RIID0243 • articolo sottoposto a peer review • pubblicato in anteprima il 4 dic. 2025

Fabio Bravo

L'intermediazione dei dati e la sua evoluzione dal settore privato a quello pubblico

Il presente contributo si propone di analizzare gli aspetti giuridici dell'intermediazione dei dati, quale fenomeno che, sorto ed affermatosi nel settore privato, ha avuto un'espansione considerevole anche nel settore pubblico, grazie anche all'evoluzione normativa dell'ordinamento europeo, non slegata dalle dinamiche di regolazione del mercato. Il contributo, prendendo criticamente in esame le relazioni sussistenti tra intermediazione di dati, diritto alla portabilità e delega, anche alla luce dei provvedimenti resi dalle Authority di settore, conduce la disamina sull'intermediazione di dati nel recente quadro normativo delineato dal legislatore europeo in materia di Spazi europei di condivisione di dati sanitari, indagando i margini di applicazione degli istituti in esame di fronte a tale specifico settore.

Intermediazione di dati – Dati personali e governance dei dati – Diritto alla portabilità dei dati – Delega

Data intermediation and its evolution from the private to the public sector

This contribution examines the legal aspects of data intermediation, a phenomenon that originated in the private sector and has since extended into the public sector, in part owing to developments in European Union legislation and market-regulation dynamics. The author critically analyses the interaction between data intermediation, the right to *data portability* and delegation, with particular reference to decisions issued by sectoral authorities. It considers data intermediation in the context of the recent regulatory framework enacted by the European legislator for European Health Data Spaces, and assesses the applicability of the relevant legal constructs within that domain.

Data intermediation – Personal data and data governance – Data portability – Delegation

L'Autore è professore ordinario di Diritto privato, Alma Mater Studiorum Università di Bologna

Questo contributo fa parte della sezione monografica *I dati in ambito pubblico tra esercizio della funzione amministrativa e regolazione del mercato*, a cura di Marco Bombardelli, Simone Franca, Anna Simonati

1. Obiettivi e direzione del discorso

Il fenomeno dell'intermediazione dei dati, sviluppatosi soprattutto in ambito privato, sta acquisendo nuove prospettive con l'evoluzione dell'ordinamento europeo, delle tecnologie e dei modelli di *business* che si vanno consolidando nel mercato. Si tratta però di fenomeno a cui il settore pubblico non è estraneo ed ha ora assunto margini di espansione notevoli, la cui regolamentazione finisce per impattare inevitabilmente sul mercato, traducendosi, direttamente o indirettamente, anche in uno strumento di regolazione di mercato[1].

Il presente contributo si colloca proprio in tale direzione, avendo come obiettivo quello di indagare l'intersezione tra il fenomeno di "data intermediation", di origine privatistica, i "dati in ambito pubblico" e le criticità che si riverberano sulla "regolazione del mercato", di fronte agli sviluppi normativi unionali.

Il discorso trova il suo culmine proprio nella nuova disciplina sugli spazi di condivisione dei dati sanitari, in cui l'intermediazione guadagna nuovi campi di intervento, ma subisce anche nuove ed incisive spinte regolatorie suscettibili di impattare pesantemente sul mercato. Sicché proprio il recente Regolamento EHDS costituisce, in tale prospettiva, il banco di prova per testare la relazione tra i tre predetti elementi dell'indagine – *data intermediation, data in public sector e market regulation* – e per individuare, in chiave evolutiva, sia le criticità emergenti, sia i possibili percorsi per il loro superamento.

1. In materia si veda, per un inquadramento, Bombardelli 2023.

2. L'intermediazione dei dati. Genesi e sviluppo

2.1. Il caso americano: Lumeria

Le radici dell'intermediazione dei dati possono essere rinvenute verso la fine degli anni Novanta del secolo scorso[2], allorché venne posta attenzione, nella letteratura di settore, all'emergente ruolo delle *data company* che – quali nuovi *infomediaries* – svolgevano compiti di intermediazione in favore degli interessati, ponendosi quali nuove figure sul mercato in grado di agire per loro conto, negoziando in loro favore le migliori condizioni per l'utilizzo e la remuneratività dei dati medesimi e offrendo loro, al contempo, adeguati strumenti di controllo su tali dati, prima di riversarli sul mercato[3].

Si stavano affacciando nuovi imprenditori, capaci di intercettare nuovi modelli di *business* nell'emergente e inesplorato terreno dei *data markets*. Tra questi, uno dei pionieri è sicuramente Lumeria, società californiana operante già dalla fine del Novecento nel settore commerciale dell'*identity management* e della "*consumer privacy*": nell'ambito dei propri servizi aveva iniziato a fornire alle persone fisiche (*data subjects*) specifici strumenti per proteggere, condividere con altri (in termini di utilizzo commerciale) e dunque valorizzare i loro dati personali, ponendosi come soggetto capace di agire in nome e per conto dei medesimi, per la cura dei loro interessi[4]. Si poneva dunque quale loro rappresentante e mandatario, proteggendo ed estraendo valore dai loro dati personali, che venivano memorizzati in appositi database gestiti da tale società[5].

Le modalità operative di tale modello di *business*, estremamente significativa ai fini del nostro discorso, si colgono molto bene nelle parole del fondatore e amministratore delegato della predetta società, nella parte in cui ha precisato che "Our model was that the individual should be able to control what information is shared with what entities – people, Web sites, commerce partners, whatever. What we needed was a system that could present information about you without revealing who you are, not even to us at Lumeria. So what I did was, I went out and hired a bunch of hackers and security nuts, and said, 'Let's re-engineer. Let's create a system that is comprehensive enough so that even when all of your information – browsing habits, medical data, bank accounts, school transcripts – becomes digitized and moves into the Internet age, you can have a unified way to control and reveal and protect it.' Basically, we created a new piece of Internet infrastructure for the secure communication and authentication of transmissions across the Internet. It took us a few years and millions of dollars to develop it, but now it's here, and it's pretty cool. The consumer has complete control for the first time. And the legislative future plays into our hands. Soon we'll be a compliance mechanism for new privacy regulations. It's a great sell. It's a no-brainer. *Businesses* won't have to understand all of the great things we do for our customers. It's just, the feds are going to bust you if you don't use it!"[6].

Altrettanto significative sono le ulteriori parole spese per descrivere i meccanismi di funzionamento sia dell'intermediazione dei dati, sia le modalità

2. Cfr. Bravo 2020 e Bravo 2021.
3. In questo senso si veda Hagel–Rayport 1997-a, i quali, con una lucida analisi di mercato, anticipando i tempi, ebbero modo di evidenziare che "Companies have good reason to collect information about customers. It enables them to target their most valuable prospects more effectively, tailor their offerings to individual needs, improve customer satisfaction and retention, and identify opportunities for new products or services. But even as more and more managers begin to build strategies based on capturing information about their customers, a major change is under way that may undermine their efforts. We believe that consumers are going to take ownership of information about themselves and demand value in exchange for it. As a result, negotiating with consumers for information will become costly and complex. That process has already begun to unfold, but it could take several years to play out across broad segments of customers and products". Nello stesso senso v. anche Hagel–Rayport 1997-b, p. 54 ss.
4. Cfr. Lester 2001.
5. *Ibidem*.
6. *Ibidem*.

per ottenere redditività tanto per la società di intermediazione, quanto per gli interessati loro clienti: "A customer will store personal data in what is called a SuperProfile. The more specific the information stored (about such things as age, sex, family status, sexual orientation, income level, assets, consumer preferences, and current shopping interests), the more valuable that profile will become to advertisers, who will pay handsomely to participate in Lumeria's network. They will do this because Lumeria will give them the chance to do highly targeted, permission-based marketing – to offer special deals on, say, new cars or house-painting services or plane tickets – exclusively to people of a predetermined demographic profile, and often only to people who have already expressed an interest in the very things being advertised. Most of the money from advertisers will go directly to Lumeria's users; Lumeria will take a small cut"[7].

2.2. L'importazione del modello americano in Italia: il caso Hoda (Weople). L'impatto dell'intermediazione dei dati e della *data portability* sulle dinamiche concorrenziali nei *data markets*

Tale modello, in Italia, è stato importato da Hoda, società milanese attiva nell'intermediazione di dati, che ha ben interpretato nel contesto europeo le dinamiche di mercato americane, calandole efficacemente entro i margini di operatività della disciplina sulla protezione dei dati personali, grazie anche all'innovazione avutasi con l'introduzione del diritto alla portabilità dei dati, assicurata dall'art. 20 del Reg. 679/2016 (GDPR)[8].

Com'è noto, ai sensi di tale articolo, ove la base giuridica del trattamento sia il consenso o il contratto[9], e il trattamento sia effettuato con mezzi automatizzati, l'interessato ha diritto di ricevere i propri dati in formato strutturato, di uso comune e leggibile da dispositivo automatico, così come di trasmetterli ad altro titolare del trattamento, diverso rispetto a quello che li ha inizialmente raccolti e trattati, senza che quest'ultimo possa addurre impedimenti. Ancora, l'art. 20 cit. assicura all'interessato anche il diritto di ottenere la trasmissione diretta dei dati personali dal primo titolare dei dati ad altro titolare, sempreché ciò sia tecnicamente fattibile.

L'idea di fondo del legislatore europeo, nell'introdurre il diritto alla *data portability*, è stata, in primo luogo, quella di 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. Altro obiettivo è stato altresì quello di eliminare – o comunque arginare – l'effetto di dipendenza tecnologica dell'interessato dal titolare del trattamento (c.d. effetto *lock-in*), generalmente riscontrabile nella prassi. Inoltre, l'introduzione di tale innovativo diritto era ricollegato con l'idea di poter favorire la circolazione dei dati nel mercato europeo e il loro riuso, incoraggiando anche le dinamiche concorrenziali tra diversi fornitori di servizi, dato che l'interessato può chiedere a un fornitore (titolare del trattamento) che i dati personali da questi trattati siano trasferiti ad un fornitore concorrente (nella veste di altro titolare del trattamento), il quale potrà dunque subentrare agevolmente al primo nella fornitura di un servizio, analogamente a quanto sperimentato in altri settori commerciali[10].

Tale diritto ha avuto tuttavia un'applicazione ulteriore, di maggior impatto sul mercato, proprio nella sua intersezione con il fenomeno dell'intermediazione dei dati. Al di là delle originarie aspettative del legislatore europeo, infatti, il diritto alla portabilità di cui all'art. 20 GDPR, pima ancora dell'emanazione del *Data Governance Act*, ha contribuito alla nascita e all'affermazione di nuovi *player* operanti sui *data markets*: gli "intermediari di dati", ovvero i fornitori dei servizi di *data intermediation*.

Il loro rilevante ruolo strategico, manifestatosi nella prassi, ha successivamente indotto la Commissione europea a prendere in considerazione tali

7. *Ibidem*.
8. Per un commento all'art. 20 GDPR si veda Troiano 2019.
9. Ci si riferisce, segnatamente, alle condizioni di liceità di cui all'art. 6, par. 1, lett. a), e 9, par. 2, lett. a), nonché all'art. 6, par. 1, lett. b), GDPR.
10. Si pensi, a titolo meramente esemplificativo, alla portabilità del mutuo e alla portabilità dei numeri di cellulare tra operatori telefonici diversi.

operatori nella Comunicazione del 2020 dedicata alla *Strategia europea per i dati*[11], portando l'Ue a varare, successivamente, la disciplina normativa sulla governance europea dei dati[12] e l'ulteriore regolamentazione di settore, inclusa quella sugli spazi di condivisione dei dati sanitari[13], nelle quali l'intermediazione dei dati è tassello fondamentale dell'impianto regolatorio[14].

Prima ancora della disciplina giuridica europea in tema di fornitura dei servizi di intermediazione dei dati – avutasi con il *Data Governance Act* – l'operatività dei *data intermediaries* trovava una disciplina nell'ambito del Regolamento europeo sui dati personali, volto non solo a fornire un sistema di protezione agli interessati, ma anche a garantire la libera circolazione di tali dati nel mercato europeo. Sicché, facendo leva sulla liceità delle finalità del trattamento dei dati personali nell'attività di intermediazione[15] e sull'art. 20 in tema di *data portability*, sono state avanzate richieste, da parte di Hoda e per conto dei propri clienti, ad una serie di operatori commerciali della grande distribuzione e ai *big player* del settore tecnologico – Google *in primis* – ottenendo, dai propri interlocutori, forti resistenze sul mercato, proprio a causa dell'incidenza del diritto alla portabilità sul mercato dei dati e sulle dinamiche concorrenziali. Le resistenze sono sfociate *sia* in procedimenti innanzi al *Garante per la protezione dei dati personali*, che gli operatori della grande distribuzione hanno intentato nei confronti dell'intermediario, al fine di paralizzare la sua richiesta volta ad ottenere l'intero patrimonio informativo sui dati relativo ai singoli clienti, esercitata dall'intermediario medesimo per conto degli interessati in esercizio del diritto alla portabilità dei dati, *sia* in un procedimento innanzi all'*Autorità Garante per la Concorrenza e il Mercato* (AGCM), questa volta per iniziativa dell'intermediario, che lamentava una condotta anticoncorrenziale di Google volta ad ostacolare il flusso di dati richiesto da Hoda per conto dei propri clienti[16].

Sul fronte concorrenziale la minaccia percepita sul mercato dagli operatori era chiara: un nuovo *player*, l'intermediario, senza alcuno sforzo in termini di raccolta del dato, facendo valere la portabilità in nome e per conto dei propri clienti, avrebbe accumulato in un batter d'occhio e senza investimenti iniziali sui propri server quell'insieme molteplice di dati che, con grande dispendio di energie e risorse, gli operatori avevano faticato ad avere per le proprie esigenze di mercato: si pensi agli investimenti in termini di tecnologie di raccolta dei dati, al tempo prolungato per ottenerli in quantità e qualità significativa per impieghi commerciali ed industriali, e così via. L'intermediario invece, attraverso l'art. 20 GDPR, a semplice richiesta, otterrebbe per conto degli interessati, la disponibilità di tutte quelle informazioni che i diversi operatori hanno raccolto nel tempo, nell'ambito delle loro attività.

Non solo.

L'intermediario è in grado di raccogliere, sui propri server, in corrispondenza di ciascun interessato e sempre per suo conto, una quantità di gran lunga maggiore di dati rispetto al titolare del trattamento originario, in quanto accentrerebbe su di sé, per ciascun cliente-interessato, i dati personali provenienti da una pluralità di operatori. Si pensi ad esempio alla possibilità che l'intermediario ha, tramite l'esercizio del diritto alla portabilità

11. Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato Economico e Sociale europeo e al Comitato delle Regioni, *Una strategia europea per i dati*, del 19 febbraio 2020, COM(2020) 66.
12. Cfr. Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio del 30 maggio 2022 relativo alla governance europea dei dati e che modifica il regolamento (UE) 2018/1724 (Regolamento sulla governance dei dati – *Data Governance Act*). Per un commento a tale regolamento cfr. Morace Pinelli 2024.
13. Regolamento (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 (Regolamento EHDS). Per una disamina delle questioni giuridiche relative a tale regolamento si veda lo studio monografico di Faillace 2025, nonché l'opera collettanea di Morace Pinelli 2025.
14. Sul rapporto tra intermediazione di dati e diritto alla portabilità nel settore sanitario, con particolare riferimento agli spazi di condivisione dei dati sanitari disciplinati nel Regolamento EHDS si veda Bravo 2025.
15. In tema di diritto a trattare dati personali nello svolgimento dell'attività economica v., *amplius*, Bravo 2018.
16. Si veda, per i procedimenti innanzi ad entrambe le *Authority*, quanto illustrato *infra*, nel prosieguo del discorso.

su delega dell'interessato, di concentrare, per ogni *data subject*, dati provenienti da titolari diversi, come ad esempio i dati gestiti dai singoli *Internet Service Providers* (Google, Meta, Apple, Amazon, Booking, ecc.) con cui l'utente si relaziona, i dati accumulati nelle "carte fedeltà" dei diversi distributori sul mercato (ad esempio le carte fedeltà dei grandi magazzini, dei supermercati, delle catene di distribuzione di libri, ecc.), oltre, eventualmente, a dati di altro tipo come quelli bancari, sanitari e quant'altro il singolo interessato voglia far confluire nell'intermediario. Il senso dell'operazione è, per l'interessato, quello di riappropriarsi del controllo sui propri dati e della loro gestione, tramite l'ausilio di un soggetto che professionalmente agirà per valorizzarli anche in prospettiva di mercato, traendo benefici per l'interessato e trattenendo una quota ridotta per il servizio di intermediazione fornito.

Il *data subject*, generalmente, vede i propri dati raccolti in grande quantità da operatori di mercato senza tuttavia poterne avere il controllo e senza poter ottenere benefici diretti o indiretti dal loro utilizzo, salvo eventualmente trascurabili "concessioni", come sconti di modesta entità, piccole donazioni di prodotti o fornitura senza controprestazioni in denaro, più che ripagate in realtà dall'accumulo di dati da utilizzare sui mercati secondari[17]. Con l'attività svolta dall'intermediario, in qualche modo, l'interessato interagisce con l'intermediario, che ha competenze tecnico-giuridiche per acquisire i dati da altri titolari del trattamento, restituire governance e controllo all'interessato sui propri dati e concordare con quest'ultimo le modalità di utilizzo e i benefici negoziabili.

In altre parole, l'intermediario finisce per costituire dei "super-profili" degli interessati, per loro conto, da gestire in maniera profittevole o comunque vantaggiosa nei rapporti con altri soggetti terzi, secondo modalità di riuso da programmare, riversando sugli interessati i vantaggi (economici e non) ottenuti dal *secondary use* di tali dati, trattenendo al contempo, in logica *win-win*, una parte che costituisce il margine di profitto per l'intermediazione professionale svolta. Al contempo, l'intermediario agisce ne superiore interesse dell'interessato, che deve essere sempre fatto salvo[18].

Si comprendono bene le resistenze degli operatori di mercato nei confronti degli intermediari, così come le strategie dell'Ue nel valorizzarli, sul piano degli intenti normativi di regolazione del mercato. La fornitura dei servizi di intermediazione, infatti, consente a imprese anche di piccole dimensioni, come start-up nel settore high-tech, di competere rapidamente anche con i più consolidati giganti attivi da tempo sul medesimo settore: le imprese europee, in tal modo, finiscono per avere l'occasione di recuperare fette di mercato nei *digital markets*, ipercontrollati dalle multinazionali soprattutto americane in regime di oligopolio, se non di pressoché sostanziale monopolio – o quasi – nei sottoinsiemi in cui i mercati digitali trovano esplicazione[19].

2.3. Segue: La portabilità dei dati e la questione della delega

L'avvento degli intermediari di dati, sul piano giuridico, è stato possibile sotto l'egida del GDPR 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, interessato al trattamento di dati posto in essere da un soggetto terzo, titolare del trattamento e fornitore di servizi, si fa conferire la delega per l'esercizio del diritto alla portabilità nei confronti di quest'ultimo; (ii) ottenuta la delega, l'intermediario richiede al titolare del trattamento, per conto dell'interessato, il trasferimento

17. Quanto ai *two-sided markets* con riferimento ai mercati di dati si veda Zeno Zencovich 2019.
18. Cfr. art. 12, par. 1, lett. m), del DGA, ai sensi del quale " il fornitore di servizi di intermediazione dei dati che offre servizi agli interessati agisce nell'interesse superiore di questi ultimi nel facilitare l'esercizio dei loro diritti, in particolare informandoli e, se opportuno, fornendo loro consulenza in maniera concisa, trasparente, intelligibile e facilmente accessibile sugli utilizzi previsti dei dati da parte degli utenti dei dati e sui termini e le condizioni standard cui sono subordinati tali utilizzi, prima che gli interessati diano il loro consenso".
19. Si pensi ad Amazon per il commercio elettronico diretto, a Google per i motori ricerca, ecc.

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 remunerativitá e altri vantaggi, con trattenimento di una quota concordata con i propri clienti (ad esempio, 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* – incluso pubbliche amministrazioni, università, imprese, enti non lucrativi – l'insieme di tali dati (o una parte di essi) 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, già richiamati sopra e qui di seguito ricapitolati, sono almeno tre:

(i) 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;

(ii) 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 diritti e nella cura dei suoi interessi;

(iii) 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 personali 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, ecc.), 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 dati[20]. 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 provider 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 "riappropriarsi".

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 proprio sull'operato di Hoda, alle prese con il suo servizio di punta denominato "Weople", segnalazioni inoltrate nei primi mesi del 2019 da operatori della grande distribuzione commerciale: questi ultimi, nella loro qualità di titolari del trattamento, si erano visti rivolgere numerose richieste di portabilità dei dati dal predetto intermediario, per delega dei propri clienti, secondo lo schema di operatività sopra richiamato e, dubitando della liceità dell'operazione, tra l'altro non

20. Zeno Zencovich 2018; Resta-Zeno Zencovich 2018.

gradita, l'avevano prontamente segnalata all'Autorità di settore[21].

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. 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 '*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"[22].

La discussione innanzi all'EDPB non sarebbe stata affrontata dal Collegio presieduto da Antonello Soro, per via della scadenza del mandato. Nel Comunicato stampa relativo a tale questione, il Garante chiariva comunque che "(…) attenderà dunque il parere dell'EDPB per concludere l'istruttoria"[23] 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"[24].

Nell'attesa, il Garante – anche per via della prossima scadenza del mandato – rinunciava dunque a prendere espressamente una propria posizione,

21. La ricostruzione della vicenda 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 *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* (…)".
22. 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. Si veda anche, di ugual tenore, il Comunicato Stampa del 1° agosto 2019, cit.
23. GPDP, Comunicato stampa del 1° agosto 2019, cit.
24. *Ibidem*.

così come a fornire indicazioni agli operatori, lasciandoli di fatto "soli" di fronte ai nuovi problemi applicativi sollevati dalla prassi, nell'attesa di un intervento di respiro europeo.

L'esperienza significativa sul caso Weople, tuttavia, ha alimentato un confronto anche su altri tavoli, in quanto è stata oggetto di disamina anche nell'ambito dell'*Indagine conoscitiva sui Big Data*, condotta congiuntamene 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). In tale indagine, il confronto tra le tre autorità aveva portato a valutare positivamente 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. Ciò in quanto "Tali iniziative [di *data intermediation*] 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"[25].

Poco dopo, proprio sul servizio Weople fornito da Hoda, s'è pronunciata anche l'AGCM, che, nel 2022, 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 clienti[26].

25. GPDP-AGCM-AGCOM, *Indagine conoscitiva sui Big Data*, Rapporto finale, 10 febbraio 2020, disponibile online, doc. web n. 9264297, p. 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 archiviarli 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*".

26. 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 anticorrenziale 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 2023 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

Da ultimo, alla fine del 2024, il Garante è ritornato ad occuparsi ancora una volta del caso Weople, in altro procedimento, con 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. 10108848[27].

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 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 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, s'è pronunciato 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 ha rimarcato 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*[28].

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"[29].

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 ha affermato 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 attività 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

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.

27. 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.

28. 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*".

29. *Ibidem*.

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, nella parte dedicata alle condizioni di liceità del trattamento e non all'esercizio dei diritti dell'interessato, disciplinati 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 rilevare[30], lo stesso GDPR, all'art. 8, prevede che, qualora il consenso non possa essere prestato direttamente dal minore per via dei limiti ivi delineati, viene manifestato da coloro che esercitano la responsabilità genitoriale e che ne hanno dunque la rappresentanza *ex lege*[31].

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 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"[32].

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 Regolamento EHDS, la cui definizione è rimessa al legislatore nazionale.

2.4. L'attenzione dell'Ue per il fenomeno dell'intermediazione dei dati come fattore di sviluppo e la regolamentazione del mercato. L'intermediazione dei dati nel *Data Governance Act*

S'è visto come le iniziali preoccupazioni del Garante sul fronte domestico relative alla prima istruttoria del 2019 sul caso Hoda non siano 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, nonostante le sollecitazioni della *Data Protection Authority* nostrana.

Una prima significativa risposta istituzionale a tale sollecitazioni sembra sia pervenuta sia con la Comunicazione della Commissione sulla *Strategia europea dei dati*, già citata, significativamente resa nel 2020, sia, in via legislativa, con

30. Cfr. Bravo 2017; Bravo 2019.

31. 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.

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

l'emanazione del *Data Governance Act*[33], ove, in linea con una progettualità delineata mediante la predetta Comunicazione, s'è provveduto a disciplinare il fenomeno della *data intermediation* agendo su tre piani distinti, che configurano tre diversi modelli di intermediazione:

(i) v'è il modello di intermediazione di dati affidato 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 GDPR[34]. Si tratta di attività di intermediazione che può essere svolta in forma tradizionale, mettendo in relazione soggetti estranei all'intermediario, oppure in forma *cooperativa*, mediante vere e proprie cooperative di dati[35], 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'ente[36]. 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 soggetto 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 supporta gli interessati 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 posizione dell'interessato, su quello economico relativo alla posizione (di forza) sul mercato e sul piano giuridico[37];

(ii) v'è altresì il modello di *data intermediation* altruistico, affidato alle organizzazioni per l'altruismo dei dati, che si indirizza al soddisfacimento di obiettivi di interesse generale, inclusa l'assistenza sanitaria[38]. È una declinazione in

33. Per un commento al *Data Governance Act* si veda Morace Pinelli 2024.

34. 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 2020; Bravo 2021; Poletti 2022; Resta 2022; Resta-Zeno Zencovich 2023; Morace Pinelli 2024.

35. In tema di cooperative di dati, disciplinate nel *Data Governance Act*, si veda Bravo 2023; Petrone 2023; nonché i contributi raccolti all'esito del progetto di terza missione dell'Università di Bologna in materia di Cooperative di dati, nel volume curato da Bravo 2024.

36. 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".

37. Cfr. Bravo 2023; Poletti 2024; Ricci-Spangaro 2024; nonché Cardinali 2024.

38. 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,

senso solidaristico[39] dell'attività di intermediazione commerciale sui dati, la quale ultima riemerge anche in tale settore qualora le organizzazioni per l'altruismo di dati perseguano, unitamente ad un intento altruistico-solidaristico – che dunque non è esclusivo – anche un concomitante scopo lucrativo, puntando a stabilire (anche) relazioni commerciali tra un numero indeterminato di interessati e *data holders*, da un lato, e *data users*, dall'altro lato[40];

(iii) v'è, poi, il modello di *data intermediation* affidato 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. Il legislatore europeo non usa esplicitamente il termine "intermediazione" per il ruolo degli enti pubblici, volti a garantire il riuso dei dati personali da questi detenuti in ragione dei loro compiti istituzionali. Che di *data intermediation* si tratti, tuttavia, può essere chiaramente desunto anche nella definizione stessa di "riutilizzo", la quale, ai sensi dell'art. 2, par. 1, n. 2, del DGA, si riferisce all'"utilizzo di dati in possesso di enti pubblici da parte di persone fisiche o giuridiche a fini commerciali o non commerciali diversi dallo scopo iniziale nell'ambito dei compiti di servizio pubblico per i quali i dati sono stati prodotti, fatta eccezione per lo scambio di dati tra enti pubblici esclusivamente in adempimento dei loro compiti di servizio pubblico".

3. L'intermediazione dei dati nel settore pubblico e il *reuse of data held by public bodies*

Dunque, l'intenzione del legislatore, con la regolamentazione del riuso dei dati personali raccolti in ambito pubblico, è quella di consentirne il riuso, anche per fini commerciali, in favore di persone fisiche o giuridiche, al di fuori delle finalità istituzionali per le quali il trattamento è inizialmente avvenuto, restituendo alla collettività la possibilità di trarre conoscenza e occasioni commerciali da tali dati, con le garanzie per il rispetto della disciplina posta a protezione delle persone fisiche con riguardo ai trattamenti dei dati personali che li riguardano.

La prospettiva seguita dal legislatore europeo, per tale modello di intermediazione, è quella indicata nel considerando n. 6 del DGA, ove espressamente si enuncia che "l'idea che i dati generati o raccolti da enti pubblici o altre entità a carico dei bilanci pubblici debbano apportare benefici alla società è da tempo parte integrante delle politiche dell'Unione. La direttiva (UE) 2019/1024 e la normativa settoriale dell'Unione garantiscono che gli enti pubblici rendano facilmente disponibile per l'utilizzo e il riutilizzo una quota maggiore dei dati che producono. Spesso talune categorie di dati conservati in basi di dati pubbliche, quali dati commerciali riservati, dati soggetti a segreto statistico e dati protetti da diritti di proprietà intellettuale di terzi, compresi segreti commerciali e dati personali, spesso non sono messe a disposizione, nemmeno per attività di ricerca o di innovazione nel pubblico interesse, nonostante tale disponibilità sia possibile in conformità del diritto dell'Unione applicabile, in particolare del regolamento

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".

39. Quanto al principio di solidarietà si vedano le insuperabili pagine di Rodotà 2014 e di Alpa 2022. Con riguardo alla declinazione di tale principio con riguardo ai dati personali si rimanda a Bravo 2023-b; Bravo 2023-c; Bravo 2023-d.

40. 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".

(UE) 2016/679 e delle direttive 2002/58/CE e (UE) 2016/680. A causa della sensibilità di tali dati, prima che essi siano messi a disposizione si devono soddisfare alcuni requisiti procedurali tecnici e giuridici al fine, se non altro, di garantire il rispetto dei diritti di terzi sui dati in questione o di limitare l'effetto negativo sui diritti fondamentali, sul principio di non discriminazione e sulla protezione dei dati. L'adempimento di tali requisiti risulta abitualmente molto dispendioso in termini di tempo e richiede un livello molto elevato di conoscenze. Ciò ha determinato un utilizzo insufficiente di tali dati. Per quanto alcuni Stati membri stiano istituendo strutture, procedure o adottando norme per agevolare tale tipo di riutilizzo, ciò non accade in tutta l'Unione. Al fine di agevolare l'utilizzo dei dati per la ricerca e l'innovazione europee da parte di soggetti pubblici e privati, sono necessarie condizioni chiare per l'accesso a tali dati e il loro utilizzo in tutta l'Unione".

Il *Data Governance Act*, per i dati appartenenti a categorie protette, incluso i dati personali, detenuti da enti pubblici, consente dunque a questi ultimi di concedere l'accesso a terzi ai fini del riuso di tali dati, anche per fini commerciali, purché ciò avvenga alle condizioni previste dall'art. 5 del predetto Regolamento, assicurando un livello di protezione conforme alla natura protetta dei dati da sottoporre a riuso. In particolare, gli enti pubblici, a fronte di una richiesta di riutilizzo dei dati, sono tenuti a concedere l'accesso per il riutilizzo dei dati soltanto qualora abbiano garantito che, a seguito della richiesta medesima, i dati siano stati anonimizzati, nel caso di dati personali, e modificati, aggregati o trattati mediante qualsiasi altro metodo di controllo della divulgazione, nel caso di informazioni commerciali riservate, compresi i segreti commerciali o i contenuti protetti da diritti di proprietà intellettuale[41]. Inoltre, gli enti interessati dal riuso devono assicurarsi che l'accesso ai dati e il loro riutilizzo avvenga da remoto, all'interno di un ambiente di trattamento sicuro, fornito o controllato dall'ente pubblico, oppure all'interno dei locali fisici in cui si trova l'ambiente di trattamento sicuro, nel rispetto di rigorose norme di sicurezza, qualora l'accesso remoto non possa essere consentito senza compromettere i diritti e gli interessi di terzi[42].

La disciplina contempla anche l'ipotesi di *secondary use* dei dati in assenza di anonimizzazione e di una specifica base giuridica per la trasmissione dei dati personali a soggetti terzi (*data users*). In tal caso l'art. 5, par. 5, del DGA prevede che "l'ente pubblico si adoper[i] al meglio, conformemente al diritto dell'Unione e nazionale, per fornire assistenza ai potenziali riutilizzatori nel *richiedere il consenso degli interessati o l'autorizzazione dei titolari dei dati* i cui diritti e interessi possono essere interessati da tale riutilizzo, ove ciò sia fattibile senza un onere sproporzionato per l'ente pubblico (…)", con la precisazione che "qualora fornisca tale assistenza, l'ente pubblico può essere assistito dagli organismi competenti (…)".

Immaginando una difficoltà tecnica strutturale degli enti pubblici a svolgere le attività connesse al riuso dei dati appartenenti a categorie protette che sono nella loro disponibilità per i compiti istituzionali che già svolgono, la disciplina ha previsto, opportunamente, la facoltà di essere coadiuvati da organismi dotati delle necessarie competenze ad attuare le strategie di riuso degli enti, con costi che possono essere assorbiti e recuperati tramite un sistema di tariffazione volto a garantire la sostenibilità delle operazioni[43].

I predetti enti, infatti, in base all'art. 7 del DGA, possono farsi eventualmente assistere da "organismi competenti", dotati di risorse giuridiche, finanziarie, tecniche, umane e di know-how, aventi il compito di fornire assistenza tecnica agli anti pubblici impegnati nel riuso, finanche mettendo a loro disposizione un *ambiente di trattamento sicuro* per la fornitura dell'accesso, nonché sulle modalità per garantire tecnicamente, anche con tecniche di pseudonimizzazione, anonimizzazione,

41. In tal senso v. art. 5, par. 3, lett. *a)*, del DGA.

42. V. art. 5, par. 3, lett. *b)* e *c)*, del DGA.

43. Diversamente dalla disciplina sull'open data, con il *Data Governance Act* possono essere richieste delle tariffe da parte degli enti pubblici che mettano a disposizione i dati per il *secondary use* e ciò anche per coprire i costi necessari per porre in essere le attività di anonimizzazione o di raccolta del consenso degli interessati previste dalla disciplina in parola. L'art. 6, par. 1, del DGA, infatti, espressamente stabilisce che "Gli enti pubblici che consentono il riutilizzo delle categorie di dati di cui all'articolo 3, paragrafo 1, possono imporre tariffe per consentire

generalizzazione, soppressione, randomizzazione o altri metodi all'avanguardia, il rispetto dei requisiti e dei limiti previsti dalla disciplina sulla protezione dei dati personali, nonché per richiedere, se del caso, il consenso al riuso dei dati da parte degli interessati o dell'autorizzazione da parte dei titolari dei dati, e quant'altro si rendesse necessario per l'applicazione della disciplina in esame[44].

Il modello incentrato sul riuso dei dati detenuti dagli enti pubblici a beneficio anche della società civile e delle imprese può essere dunque interpretato, al di là delle etichette usate dal legislatore europeo nel *Data Governance Act*, come un modello di *data intermediation* in ambito pubblico.

L'intermediazione dei dati, a prescindere dal modello di riferimento, è pensata come uno 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 consentirne la circolazione o alla condivisione in favore del concomitante interesse altrui o di quello collettivo.

4. Intermediazione dei dati nel nuovo scenario normativo avutosi con il Regolamento EHDS in tema di spazi di condivisione di dati sanitari

4.1. L'intermediazione in ambito pubblico dal *Data Governance Act* al Regolamento sull'*European Health Data Space*

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, di più recente introduzione, avutosi con la predisposizione degli spazi di condivisione dei dati, enunciato con enfasi nella Comunicazione della Commissione europea su *Una strategia europea per i dati* e poi regolamentato,

il riutilizzo di tali dati". Al contrario, la Direttiva 2019/1024/UE del Parlamento europeo e del Consiglio del 20 giugno 2019 relativa all'apertura dei dati e al riutilizzo dell'informazione nel settore pubblico prevede, all'art. 6 ("Principi di tariffazione"), par. 1, che "Il riutilizzo di documenti è gratuito", anche se poi il principio di gratuità è stemperato subito dopo dalla previsione di un'eccezione: "Tuttavia, può essere autorizzato il recupero dei costi marginali sostenuti per la riproduzione, messa a disposizione e divulgazione dei documenti, nonché per l'anonimizzazione di dati personali o per le misure adottate per proteggere le informazioni commerciali a carattere riservato (…)". Fanno altresì eccezione, ai sensi del par. 2, gli "enti pubblici che devono generare proventi per coprire una parte sostanziale dei costi inerenti allo svolgimento dei propri compiti di servizio pubblico", le "biblioteche, comprese le biblioteche universitarie, musei e archivi" e le "imprese pubbliche", ai quali non si applica il principio di gratuità per il riutilizzo.

44. Segnatamente, l'assistenza fornita dagli *organismi competenti* agli *enti pubblici* per il *riuso dei dati* appartenenti a categorie protette (incluso i dati personali) da questi detenuti, comprende, "ove necessario: a) fornire assistenza tecnica mettendo a disposizione un *ambiente di trattamento sicuro* per la fornitura dell'accesso ai fini del riutilizzo dei dati; b) fornire orientamenti e assistenza tecnica su come strutturare e conservare al meglio i dati per renderli facilmente accessibili; c) fornire assistenza tecnica per la *pseudonimizzazione* e garantire il trattamento dei dati in modo da tutelare efficacemente la vita privata, la riservatezza, l'integrità e l'accessibilità delle informazioni contenute nei dati per i quali è consentito il riutilizzo, comprese le tecniche di *anonimizzazione, generalizzazione, soppressione e randomizzazione* dei dati personali o altri metodi all'avanguardia di tutela della vita privata, e la *cancellazione* di informazioni commerciali riservate, tra cui segreti commerciali o contenuti protetti da diritti di proprietà intellettuale; d) se del caso, fornire assistenza agli enti pubblici affinché aiutino i riutilizzatori a *richiedere agli interessati il consenso al riutilizzo o ai titolari dei dati l'autorizzazione al riutilizzo*, in linea con le loro decisioni specifiche, anche in merito alla giurisdizione in cui si intende effettuare il trattamento dei dati, e fornire assistenza agli enti pubblici nell'istituire meccanismi tecnici che permettano di trasmettere le richieste di consenso o di autorizzazione formulate dai riutilizzatori, ove ciò sia fattibile nella pratica; e) fornire assistenza agli enti pubblici in merito alla valutazione dell'adeguatezza degli impegni contrattuali assunti da un riutilizzatore (…)" (v. art. 7, par. 4, DGA).

con riguardo ai dati sanitari, dal Regolamento EHDS (*European Health Data Space*).

Ne costituisce, in qualche modo, anche l'antecedente giuridico.

Si pensi al tenore del considerando n. 24 del *Data Governance Act*, nel quale si menziona il riutilizzo dei dati nel settore della sanità pubblica, con riguardo ai dati detenuti da soggetti operanti nel settore sanitario (come ad esempio di ospedali pubblici) e la creazione di ambienti di condivisione nell'Ue quali lo spazio europeo di dati sanitari, con obbligo di utilizzo di un ambiente di trattamento sicuro quale modalità tecnica per assicurare il rispetto della protezione delle persone fisiche, dei loro dati personali e della loro vita privata[45].

Sono temi che, anticipati nel Regolamento sulla governance europea dei dati, trovano una loro dettagliata attuazione nell'ambito del successivo Regolamento sullo spazio di condivisione dei dati sanitari. Infatti il Reg. EHDS, nella parte relativa al *secondary use* dei dati sanitari ospitati nello spazio di condivisione dei dati provenienti dalle strutture sanitarie, essenzialmente pubbliche, ripropone il medesimo modello di fondo, basato sull'intermediazione di dati personali svolta da enti pubblici, con l'assistenza di organismi competenti, in ambienti sicuri di trattamento, tracciato, in via embrionale e con caratteri generali, nel *Data Governance Act*.

Ritornano, tra i due modelli di intermediazione in ambito pubblico, con necessari riadattamenti ed evoluzioni, anche i principali istituti giuridici che hanno caratterizzato il fenomeno dell'intermediazione dei dati, tra cui, primariamente, il *diritto alla portabilità* dei dati e l'esercizio della *delega*.

4.2. 4.2. Il diritto alla portabilità dei dati nel Regolamento EHDS e il rapporto con il diritto alla *data portability* delineato 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 con il diritto alla portabilità di cui all'art. 20 del GDPR, rimarcandone la complementarità. Ivi si afferma, infatti, che il nuovo regolamento in tema di *European Health Data Space* "(…) 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 ed inalterato anche nella materia *de qua*, nella quale si aggiunge 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

45. Nel considerando n. 24 del DGA, in particolare, viene 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 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".

Reg. EHDS, su cui le autorità di protezione dei dati personali continuano ad esercitare i propri poteri[46].

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 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 svolti in ambito pubblico, tenendo conto, tra l'altro, che la natura particolare dei dati sanitari rende insufficiente ed inadeguato il ricorso alle condizioni di liceità contemplate all'art. 6 del GDPR.

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*) [47], ma escludendo i dati che siano stati oggetto di successiva elaborazione da parte del titolare del trattamento o che siano stati da questi generati[48].

Una terza limitazione riscontrabile nel diritto alla portabilità dei dati di cui all'art. 20 GDPR si

46. 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 (…)".

47. 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, p. 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 (…)".

48. 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 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

riscontra nella possibilità di ottenere il trasferimento dei dati da un titolare ad un altro solamente qualora l'operazione sia "tecnicamente fattibile"[49]. 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. Ciò potrebbe avvenire, ad esempio, nei casi in cui non v'è a monte l'interoperabilità tra i dati o tra un sistema di trattamento e l'altro.

V'è poi una quarta limitazione, che si estrare dalla lettura di sistema nel combinato disposto con l'art. 12 del GDPR: di fronte alla richiesta di esercizio del diritto alla portabilità, come di qualsiasi altro diritto previsto 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"[50]. Anche il difetto di immediatezza del trasferimento, 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* per gli spazi di condivisione di dati sanitari.

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 GDPR[51], che in un certo qual modo vede estendere la sua portata applicativa al nuovo contesto[52].

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

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".

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

50. Art. 12, par. 3, GDPR. Inoltre, qualora si registri il caso di mancata ottemperanza "alla richiesta dell'interessato, il titolare del trattamento informa l'interessato 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).

51. 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".

52. Cfr. considerando n. 15 del Reg. EHDS.

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, 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"[53].

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 (nella declinazione della *data portability* del diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro). Nell'art. 7 del nuovo regolamento, invece, le 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 entro i tempi (dilatati) congrui all'esecuzione della prestazione richiesta e non preventivata, 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 altri titolare del trattamento, ma tra titolari qualificati in ragione della specifica natura dell'attività da questi svolta[54].

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

53. Al par. 2 di tale articolo di 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".

54. 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 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*".

rimborso". Non è, questa, una portabilità pensata per i fornitori dei servizi di intermediazione di dati di cui al *Data Governance Act*. È, dunque, una portabilità "tipizzata", preordinata al trasferimento dei dati a 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")[55].

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.[56], risulta evidente che chi gestisce lo spazio di 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 con il *Data Governance Act*. Il riferimento è, in particolare, al 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 ad un significativo potenziamento, per le finalità indicate nell'art. 53 del Reg EHDS, anche in ragione della ricerca di settore, nonché dello sviluppo e dell'innovazione

55. 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".

56. 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 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 il comma 1, a cui segue poi, al comma 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".

di prodotti e servizi e per l'addestramento dei sistemi di intelligenza artificiale[57].

L'accesso ai dati di uso secondario è riservato a enti pubblici e a istituzioni, organi e organismi dell'Ue solamente per alcune delle finalità ammesse, desumendosi quindi un'apertura anche ai soggetti privati per le finalità, anche di ricerca scientifica in ambito sanitario e per le finalità ad essa strumentale, di innovazione di prodotti e servizi e per l'addestramento dei sistemi di IA[58].

4.3. L'istituto della delega nel Regolamento EHDS e servizi di *data intermediation*

Altro istituto rilevante nel fenomeno di intermediazione di dati, riscontrabile anche nella disciplina del Reg. EHDS, è quello della "delega", 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'*autorizzazione 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

57. 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 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".

58. Viene infatti previsto, all'art. 53, par. 2, 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.

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"[59]. Il considerando citato, come s'è avuto modo di evidenziare, prevede 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, sia egli persona fisica o giuridica[60]. Si consideri che, nel caso specifico degli spazi di

59. 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 dei 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 2014. Per la delega in ambito amministrativo si rimanda, invece, a Miele 1962.

60. 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 2011, 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 detto, 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*, p. 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 dominate". 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* personale – 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, oggigiorno 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 2008. Si veda anche la lettura critica, quanto all'*intuitus personae* nei contratti di appalto, enunciata da Iudica 2009. Sulla pacifica riferibilità dei contratti *intuitus personae* anche alle persone giuridiche si veda anche Galgano 2014, p. 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:

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'EHDS[61].

Nel testo normativo il tema è disciplinato all'art. 4 del Regolamento, rubricato "Servizi di accesso ai dati sanitari elettronici per le persone fisiche e i loro rappresentanti", nel 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 si prevede l'istituzione in forma di "servizio", quale "funzionalità di servizio 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"[62].

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 sul sistema, svolgendo l'attività per conto dell'interessato medesimo[63], con un sistema interoperabile a

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 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.

61. Izzo-Guarda 2010.

62. 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. 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".

63. 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…").

livello europeo che va adeguato alla disciplina del Regolamento eIDAS[64].

Del resto, ove non vi fosse il meccanismo tecnico del "servizio di delega", potrebbe verificarsi che di fatto l'interessato finisca materialmente per far utilizzare le proprie credenziali ad altri, nell'intento di far consentire comunque l'accesso al sistema di trattamento dei dati da parte di chi è chiamato ad agire per conto dell'interessato, quale rappresentante su base volontaria o per disposizione di legge[65].

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 persone fisiche e non anche delle persone giuridiche.

Si tratta di opzione normativa che il legislatore italiano aveva già percorso con l'art. 9, co. 2, del d.lgs. 196/2023, prima dell'abrogazione ad opera del d.lgs. 101/2018, ove, con riguardo alle 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 (…)"[66] e "(…) può, altresì, farsi assistere da una persona di fiducia"[67]. Con la revisione del Codice in materia di protezione dei dati personali dovuta 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, 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, quando ciò è in linea con il proprio interesse e purché non si tratti di atti personalissimi. Che l'esercizio dei diritti dell'interessato non sia atto personalissimo risulta evidente dall'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, al di fuori dei casi in cui ai minori sia consentito agire personalmente nei limiti oggettivi e d'età previsti dal GDPR e dal Codice in materia di protezione dei dati personali[68].

64. 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".

65. Il tema è stato trattato, con riguardo al FSE, e con riferimento all'impianto normativo precedente al GDPR, da Izzo-Guarda 2010, p. 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 irritualmente rese".

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

67. *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. 196/2023), 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*").

68. 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

La scelta del Regolamento 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, che si individua quale soggetto a cui ci si affida per la cura dell'interesse da salvaguardare. Del resto, qualora si individuasse come destinatario dell'autorizzazione una persona giuridica, in linea con quanto era contemplato dal testo originario dell'art. 9 del d.lgs. 196/2003, occorreva pur sempre individuare un soggetto, persona fisica, che agisse nell'ambito dell'ente e, in difetto di diversa precisazione, si sarebbe dovuto individuare nel legale rappresentante *pro-tempore*.

Ulteriori considerazioni vanno declinate con riguardo al particolare contesto in cui si colloca l'EHDS, quantomeno con riguardo all'uso primario dei dati sanitari personali, giacché ci si muove nell'ambito di quella che può essere definita una "*relazione di cura*" tra medico e paziente, in cui il trattamento dei dati personali è funzionale alla cura dell'interessato e all'assistenza sanitaria nei suoi confronti. Sicché va 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 medico[69], 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 elettronico[70].

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 tutti i diritti che sono riconosciuti all'interessato, quali rappresentati legali.

69. 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".

70. 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

Il "servizio di delega" previsto nel Regolamento EHDS, dunque, è ritagliato su questo modello, che si estende anche con riguardo al tema del trattamento dei dati personali di carattere sanitario, ben al di là dei confini del solo trattamento sanitario[71].

La questione della delega si incrocia con i modelli di intermediazione di dati in forma cooperativa recentemente disciplinati dal *Data Governance Act*[72], che trovano applicazione anche al settore sanitario[73].

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 alla cooperativa di dati[74]. 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 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 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'irrinunziabilità dei diritti dell'interessato, pacificamente riconosciuta, è 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

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".

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

72. Si veda, a tale riguardo, Bravo 2023-a.

73. Bravo 2024, Palladini-Scagliarini 2024; Tampieri 2024; Faillace 2024; Proietti 2024; Rufo 2024.

74. 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".

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)[75].

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 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"[76].

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, 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)"[77].

75. 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 rinunzia, 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 2022. 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, p. 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.

76. Garante per la protezione dei dati personali, nota del 30 novembre 1999, doc. web n. 1164456.

77. 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

Ulteriore casistica in tema di delega è stata trattata con maggior incertezza da parte del Garante, proprio in tema di intermediazione di dati, con riguardo al caso Hoda e alla fornitura del servizio Weople, di cui s'è già dato conto sopra[78].

5. Intermediazione di dati in ambito sanitario, *European Health Data Space* e regolazione di mercato

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 Regolamento (UE) 2025/327[79].

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 nell'ambito dell'uso primario dei dati gestiti con l'EHDS, ma anche le ulteriori finalità rilevanti per l'uso secondario, quale la ricerca scientifica e l'elaborazione di politiche pubbliche in ambito sanitario[80].

V'è poi da considerare l'*intermediazione dei dati, svolta in forma cooperativa*, in ambito sanitario[81], 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 farmaceutico[82] o nelle relazioni di cura[83]. 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 interessati[84].

Si pensi ancora all'intermediazione di dati sanitari provenienti da intermediari che gestiscono dispositivi biomedicali o strumenti *wearable* ed

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.

78. Si veda anche, *amplius*, Bravo 2025.

79. 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 2022, a cui *amplius* si rinvia.

80. L'"altruismo dei dati", infatti, viene definitivo, all'art. 2, par. 1, n. 16), del *Data Governance Act*, 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".

81. Per l'esplorazione di una casistica si veda Rufo 2024, con riferimento ai casi Savvy Cooperative, MIDATA, Salus.Coop, LunaDNA.

82. Si veda, a tal riguardo, De Vico 2024.

83. 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 2015.

84. Bravo 2023-a. Si veda anche Palladini-Scagliarini 2024, 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".

altri dati che possono avere rilevanza sia sul piano dell'assistenza sanitaria, sia su quello della ricerca (o comunque del *secondary use*), anche in relazione all'acquisizione dei c.d. *real world data*[85].

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 anche tramite rappresentanti[86].

L'intermediazione di soggetti 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, finiscono invece per essere istituzionalizzati nel sistema di trattamento delineato con lo spazio europeo di dati sanitari. Si noti però che in tale ambito, ai sensi dell'art. 51 del Reg. EHDS, tali soggetti sono obbligati a rendere disponibili i predetti dati anche per l'uso secondario, diversamente da quanto invece previsto nel DGA, che lascia agli enti pubblici una facoltà (non già un obbligo) di riuso dei dati, rientranti in particolari categorie, da questi detenuti[87].

Leggendo con attenzione il testo dei considerando e quello dell'articolato normativo del predetto Regolamento, ci si può rendere conto che, per gli spazi di condivisione di dati sanitari, il legislatore europeo ha voluto fare riferimento esplicito all'intermediazione dei dati, e ciò merita di essere considerato soprattutto per le implicazioni di sistema, in special modo 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"[88].

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 (…)"[89], il nuovo Regolamento indica quali competenze e quali attività spettano loro, rimarcando anche che sono tenute all'adozione di "*soluzioni di intermediazione* e portali per i pazienti"[90].

85. Liu-Panagiotakos 2022.

86. 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".

87. Chiaro è, a tal riguardo, l'art. 5, par. 1, del DGA, ove si prevede che "Gli enti pubblici che, a norma del diritto nazionale, hanno facoltà di concedere o negare l'accesso per il riutilizzo di una o più delle categorie di dati di cui all'articolo 3, paragrafo 1, rendono pubbliche le condizioni per consentire tale riutilizzo nonché la procedura di richiesta del riutilizzo attraverso lo sportello unico di cui all'articolo 8. Qualora concedano o neghino l'accesso per il riutilizzo, possono essere assistiti dagli organismi competenti di cui all'articolo 7, paragrafo 1".

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

89. 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 occupano 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 (…)".

90. 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

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 Regolamento 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 fonti nazionali o europee, "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"[91]. 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"[92], siffatti dati "dovrebbero essere messi a disposizione degli organismi responsabili dell'accesso ai dati sanitari (…)"[93], in ragione del fatto che vengono "raccolti e trattati dai titolari dei dati sanitari con il sostegno di finanziamenti pubblici nazionali o dell'Unione"[94]. 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[95], le *funzioni* siano

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 (…)".

91. Considerando n. 59 del Reg. EHDS.
92. *Ibidem*.
93. *Ibidem*.
94. *Ibidem*.
95. 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 (…)".

svolte da *intermediari di dati sanitari*"[96], 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*"[97].

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 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 parola[98].

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 all'intermediazione non è però senza limiti: gli Stati membri, infatti, non possono farvi ricorso per designarli quali "titolari dei dati sanitari affidabili"[99], 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"[100].

Al di fuori dei considerando, in cui l'intermediazione dei dati compare più volte, il Regolamento 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", inteso 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 dati sanitari elettronici personali rafforza dunque l'idea che il sistema delineato nel Regolamento 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

96. Considerando n. 59 del Reg. EHDS.

97. *Ibidem*.

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

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

100. Considerando n. 76 del Reg. EHDS, 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".

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 esonerare[101] oppure che per determinate categorie di titolari dei dati sanitari gli obblighi vengano "assolti da entità di intermediazione di dati sanitari"[102], con la precisazione che "an tal caso, i dati sono comunque considerati come messi a disposizione da vari titolari dei dati sanitari"[103], 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, in particolare sul fronte delle dinamiche concorrenziali e degli effetti di regolazione del mercato.

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 facili 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. 4[104], e crea 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 l'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*)[105], 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 dati[106].

101. Art. 50, par. 2, del Reg. EHDS.

102. Art. 50, par. 3, del Reg. EHDS.

103. *Ibidem*.

104. In tale considerando viene precisato che "Il trattamento dei dati personali dovrebbe 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 contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità (…)" (corsivi aggiunti). Sul punto si veda Ricci 2017, nonché Bravo 2023-c.

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

106. 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

Si ha cioè l'impressione che con l'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[107].

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. In altre parole, sembra si sia voluto intervenire anche con norme volte a regolamentare, in senso restrittivo, il *data market* in ambito sanitario e il ruolo di intermediazione svolto in tale ambito da operatori privati.

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 passa 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 consentano di preservare, seppur con le garanzie che la particolare natura dei dati imporne a tutela dei diritti degli interessati, le possibilità di controllo e valorizzazione a loro vantaggio, connesse alla gestione del *secondary use* dei dati intermediati.

Riferimenti bibliografici

P. Alberti (2008), *Le vicende soggettive dell'esecutore*, vol. V, *I settori speciali. L'esecuzione*, in "Trattato sui contratti pubblici", diretto da M.A. Sandulli, R. De Nictoli, R. Garofoli, Giuffrè, 2008

G. Alpa (2022), *Solidarietà. Un principio normativo*, il Mulino, 2022

M. Bombardelli (2023), *Le relazioni tra istituzioni pubbliche e mercati*, in Id. (a cura di), "L'intervento amministrativo sui mercati", Giappichellli, 2023

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

107. In questo senso, la regolazione del mercato in tale ambito specifico, seppur mossa dalla necessità di raggiungere finalità di interesse generale, finisce per creare ingerenze delle istituzioni pubbliche tali da alterare la logica di funzionamento delle dinamiche di mercato, la cui spontaneità si sarebbe invece dovuta preservare. In materia si veda ancora una volta, per l'impostazione di carattere generale, Bombardelli 2023.

F. Bravo (2025), *Intermediazione di dati sanitari e diritto alla portabilità*, in A. Morace Pinelli (a cura di), "Sanità digitale. Regolamento EHDS (UE 2025/327) sullo spazio europeo dei dati sanitari. Vol. 1, Uso dei dati e assetti organizzativi", Pacini, 2025

F. Bravo (a cura di) (2024), *EU Data Cooperatives. L'ingresso delle cooperative di dati nell'ordinamento europeo*, Giappichelli, 2024

F. Bravo (2023-a), *Le cooperative di dati*, in "Contratto e impresa", 2023, n. 3

F. Bravo (2023-b), *Il principio di solidarietà*, in Id. (a cura di), "Dati personali. Protezione, libera circolazione e governance. Vol. 1. Principi", Pacini, 2023

F. Bravo (2023-c), *Il principio di solidarietà tra data protection e data governance*, in "Il diritto dell'informazione e dell'informatica", 2023, n. 3

F. Bravo (2023-d), *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, n. 2

F. Bravo (2022), *Data Governance Act and Re-Use of Data in the Public Sector*, in "European Review of Digital Administration & Law", vol. 3, 2022, n. 2

F. Bravo (2021), *Intermediazione di dati personali e servizi di data sharing dal GDPR al Data Governance Act*, in "Contratto e impresa Europa", 2021, n. 1

F. Bravo (2020), *Il commercio elettronico dei dati personali*, in T. Pasquino, A. Rizzo, M. Tescaro (a cura di), "Questioni attuali in tema di commercio elettronico", ESI, 2020

F. Bravo (2019), *Le condizioni di liceità del trattamento di dati personali*, in G. Finocchiaro (a cura di), "La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101", Zanichelli, 2019

F. Bravo (2018), *Il "diritto" a trattare dati personali nello svolgimento dell'attività economica*, Wolters Kluwer-Cedam, 2018

F. Bravo (2017), *Il consenso e le altre condizioni di liceità del trattamento di dati personali*, in G. Finocchiaro (a cura di), "Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali", Zanichelli, 2017

F. Bravo (2015), *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 C. Faralli, R. Brighi, M. Martoni (a cura di), "Strumenti, diritti, regole e nuove relazioni di cura. Il paziente europeo protagonista nell'eHealth", Giappichelli, 2015

F. Bravo, J. Valero Torrijos (2022), *Data in the Public Sector and Data Valorisation*, in "European Review of Digital Administration & Law", vol. 3, 2022, n. 2

I. Cardinali (2024), *Tutela degli interessati e esercizio dei diritti: l'efficace intermediazione delle cooperative di dati*, in F. Bravo (a cura di), "EU Data Cooperatives. L'ingresso delle cooperative di dati nell'ordinamento europeo", Giappichelli, 2024

A. De Vico (2024), *I servizi di cooperazione di dati nella ricerca clinica farmaceutica: analisi e prospettive*, in F. Bravo (a cura di), "EU Data Cooperatives. L'ingresso delle cooperative di dati nell'ordinamento europeo", Giappichelli, 2024

S. Faillace (2025), *Prospettive civilistiche in ordine agli spazi di condivisione dei dati sanitari alla luce del Regolamento EHDS*, Wolters Kluwer, 2025

S. Faillace (2024), *Le cooperative di dati sanitari tra codice civile e Data Governance Act*, in F. Bravo (a cura di), "EU Data Cooperatives. L'ingresso delle cooperative di dati nell'ordinamento europeo", Giappichelli, 2024

F. Galgano (2014), *Trattato di diritto civile*, Wolters Kluwer-Cedam, 2014 (3a ed. agg. a cura di N. Zorzi Galgano, vol. II)

J. Hagel, J.F. Rayport (1997-a), *The Coming Battle for Customer Information*, in "Harvard *Business* Review", 1997, January-February

J. Hagel, J.F. Rayport (1997-b), *The new infomediaries*, in "The McKinsey Quarterly", 1997, Autumn

G. Iudica (2009), *Il contratto di appalto*, in N. Lipari, P. Rescigno (diretto da), "Diritto civile", vol. III, Giuffrè, 2009

U. Izzo, P. Guarda (2010), *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*, Università di Trento, 2010

T. Lester (2001), *The Reinvention of Privacy*, in "The Atlantic", 2001, March

F. Liu, D. Panagiotakos (2022), *D. Real-world data: a brief review of the methods, applications, challenges and opportunities*, in "BMC Med Res Methodol", vol. 22, 2022, n. 287

G. Miele (1962), voce *Delega (dir. amm.)*, in "Enciclopedia del diritto", vol. XI, Giuffrè, 1962

A. Morace Pinelli (a cura di) (2025), *Sanità digitale. Regolamento EHDS (UE 2025/327) sullo spazio europeo dei dati sanitari*. Vol. 1, *Uso dei dati e assetti organizzativi*, Pacini, 2025

A. Morace Pinelli (a cura di) (2024), *Dalla "Data Protection" alla "Data Governance": il regolamento (UE) 2022/868. Commentario al "Data Governance Act"*, Pacini, 2024

G. Musolino (2011), *Comm. sub art. 1656 c.c.,* in D. Valentino (a cura di), "Dei singoli contratti, Vol. II, Artt. 1655-1802 c.c.", nel Commentario al Codice Civile diretto da E. Gabrielli, Utet, 2011

V. Palladini, S. Scagliarini (2024), *Le cooperative di dati come forma di tutela collettiva degli interessati: un'opportunità per l'ambito sanitario?*, in F. Bravo (a cura di), "EU Data Cooperatives. L'ingresso delle cooperative di dati nell'ordinamento europeo", Giappichelli, 2024

L. Petrone (2023), *Il mercato digitale europeo e le cooperative di dati*, in "Contratto e impresa", 2023, n. 3

D. Poletti (2024), *Il quadro normativo del "Data Governance Act": l'esercizio dei diritti dell'interessato nell'attività di intermediazione dei dati*, in "Nuove leggi civili commentate", 2024, n. 3

D. Poletti (2022), *Gli intermediari dei dati*, in "European Journal of Privacy Law & Technologies", 2022, n. 1

G. Proietti (2024), *Cooperative di dati, Spazio europeo dei dati sanitari e Data Act nel dedalo normativo*, in F. Bravo (a cura di), "EU Data Cooperatives. L'ingresso delle cooperative di dati nell'ordinamento europeo", Giappichelli, 2024

G. Resta (2022), *Pubblico, privato e collettivo nel sistema europeo di governo dei dati*, in "Rivista trimestrale di diritto pubblico", 2022, n. 4

G. Resta, V. Zeno Zencovich (a cura di) (2023), *Governance of/through data*, Roma Tre Press, 2023

G. Resta, V. Zeno Zencovich (2018), *Volontà e consenso nella fruizione dei servizi in rete*, in "Rivista trimestrale di diritto e procedura civile", 2018, n. 2

A. Ricci, A. Spangaro (2024), *La tutela dell'interessato nell'economia dei dati: il ruolo delle cooperative di dati*, in F. Bravo (a cura di), "EU Data Cooperatives. L'ingresso delle cooperative di dati nell'ordinamento europeo", Giappichelli, 2024

A. Ricci (2017), *Sulla "funzione sociale" del diritto alla protezione dei dati personali*, in "Contratto e impresa", 2017, n. 2

S. Rodotà (2014), *Solidarietà. Un'utopia necessaria*, Laterza, 2014

L. Rufo (2024), *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", Giappichelli, 2024

M. Tampieri (2024), *Cooperative di dati per la tutela della salute*, in F. Bravo (a cura di), "EU Data Cooperatives. L'ingresso delle cooperative di dati nell'ordinamento europeo", Giappichelli, 2024

S. Troiano (2019), *Il diritto alla portabilità dei dati*, in N. Zorzi Galgano (a cura di), "Persona e mercato dei dati. Riflessioni sul GDPR", Wolters Kluwer-Cedam, 20219

V. Zeno Zencovich (2019), *Do "Data Markets" Exist?*, in "MediaLaws", 2019, n. 2

V. Zeno Zencovich (2018), *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, in "Media Laws", 2018, n. 2