

SULLA NECESSITÀ DI UNA VISIONE RICOSTRUTTIVA DELL'APPROCCIO ALLA CONDIVISIONE DEI DATI SANITARI ED IL RUOLO DELL'INTEROPERABILITÀ (GIURIDICA)*

| 61

Di Paolo Guarda

SOMMARIO: 1. *L'approccio europeo alla gestione (giuridica) dei dati tra obiettivi generali e regole.* – 2. *La condivisione dei dati sanitari ed il Regolamento EHDS.* - 3. *Alla ricerca di una definizione al concetto di interoperabilità giuridica.* – 4. *Considerazioni conclusive, ovvero verso una visione ricostruttiva dell'approccio alla gestione dei dati (sanitari).*

ABSTRACT. *L'articolo esamina la complessità del panorama normativo europeo relativo alla condivisione e al riutilizzo dei dati, con un focus specifico sul settore medico e sul nuovo Regolamento sullo Spazio Europeo dei Dati Sanitari (EHDS). In un contesto segnato dalla spinta verso la Scienza Aperta e dalla necessità di bilanciare il diritto alla riservatezza del singolo con il beneficio collettivo della ricerca, si individua nell'interoperabilità giuridica il fattore determinante per il successo delle iniziative dell'UE. L'interoperabilità viene interpretata non solo come requisito tecnico, ma come uno strumento sistemico e un "ponte terminologico" tra il sapere giuridico e quello informatico, capace di armonizzare regole e prassi tra diversi ordinamenti per facilitare il libero fluire delle informazioni. L'analisi affronta le criticità derivanti dalla "bulimia normativa" europea — che include atti come il GDPR, il Data Governance Act, il Data Act e l'AI Act — evidenziando il rischio di una frammentazione che ostacoli l'uso secondario dei dati. In conclusione, l'interoperabilità giuridica emerge come il presupposto strutturale per trasformare l'armonizzazione formale in una reale capacità di circolazione dei dati, superando le barriere nazionali e promuovendo l'innovazione scientifica attraverso un approccio interdisciplinare e comparatistico.*

The article examines the complexity of the European regulatory framework regarding data sharing and reuse, with a specific focus on the healthcare sector and the new European Health Data Space (EHDS) Regulation. Within a context marked by the push toward Open Science and the necessity of balancing the individual's right to privacy with the collective benefit of research, legal interoperability is identified as the determining factor for the success of EU initiatives. Interoperability is interpreted not merely as a technical requirement, but as a systemic tool and a "terminological bridge" between legal and technical-informational knowledge, capable of harmonizing rules and practices across different legal systems to facilitate the free flow of information. The analysis addresses the critical issues arising from European "regulatory bulimia" - which includes acts such as the GDPR, the Data Governance Act, the Data Act, and the AI Act - highlighting the risk of fragmentation that may hinder the secondary use of data. In conclusion, legal interoperability emerges as the structural prerequisite for transforming formal harmonization into a real capacity for data circulation, overcoming national barriers and promoting scientific innovation through an interdisciplinary and comparative approach.

Sulla necessità di una visione ricostruttiva dell'approccio alla condivisione dei dati sanitari ed il ruolo dell'interoperabilità (giuridica) (Paolo Guarda)



1. L'approccio europeo alla gestione (giuridica) dei dati tra obiettivi generali e regole.

I dati ricoprono un ruolo fondamentale in ambito medico, in particolare in quello della ricerca scientifica. La collaborazione tra gruppi e la condivisione di dati ed informazioni diventano cruciali e necessarie per lo sviluppo della conoscenza e, più in generale, per il progresso della scienza. Occorre, pertanto, individuare criteri idonei a determinare il giusto equilibrio tra esigenze e interessi pubblici ed individuali, in questo contesto riferiti al paziente o al partecipante alla sperimentazione¹.

La pandemia ha fatto da catalizzatore nell'adozione di alcuni principi della Scienza Aperta (Open Science), le cui policy, sia a livello internazionale che nazionale, spingono sempre più verso una maggiore apertura dei dati della ricerca (Open Research Data)². È innegabile che la situazione emergenziale abbia dimostrato la necessità di un cambiamento di approccio rispetto alle pratiche tipiche della condivisione dei dati (o, più spesso, alla loro mancanza o limitazione)³. Purtroppo, si è passati rapidamente dall'euforia al disappunto, poiché con il ritorno alla normalità a livello sociale, anche le politiche editoriali e di valorizzazione dei contributi scientifici sembrano essersi riallineate a modalità pregresse.

A livello normativo, il legislatore europeo ha chiaramente manifestato l'intenzione di compiere alcuni passi importanti verso l'apertura di dati e in-

* La pubblicazione è stata preparata nel contesto del Progetto "Security and Rights in the CyberSpace- SERICS" - tematica 7 "Cybersecurity, new technologies and protection of rights" e in particolare: "Digital sovereignty" (DISE), finanziato nel contest del programma "Human, social, and legal aspects", per lo Spoke 1, no. 2, CUP: B53C22003950001, della Missione 4 "Education and Research", componente 2, (PE 0000014) del PNRR.

¹ Per maggiori approfondimenti sull'importanza dei dati in ambito scientifico e sulla necessità di trovare il corretto bilanciamento tra interessi contrapposti si v., *ex plurimis*, E. CREMONA, *Quando i dati diventano beni comuni: modelli di data sharing e prospettiva di riuso*, in *Rivista italiana di informatica e diritto*, 2023, n. 2, 111-130; S. LEONELLI, *La ricerca scientifica nell'era dei big data*, Sesto San Giovanni, Meltemi, 2018; P. GUARDA, *Il regime giuridico dei dati della ricerca scientifica*, Napoli, 2021.

² Si v. UNESCO, *Recommendation on Open Science*, 2021, in Rete: <https://unesdoc.unesco.org/ark:/48223/pf0000379949>. Si v. anche G. Bincoletto, *Health Data Sharing for Scientific Research: Closing Data "As Necessary" and Opening it "As Possible"*, in M. CATANZARITI, F. INCARDONA, G. RESTA, A. SÖNNERBORG (a cura di), *Data Privacy, Data Property, And Data Sharing: An Interdisciplinary Perspective For Post-Pandemic Transnational Scientific Research*, Boca Raton, Florida: CRC Press; Taylor & Francis, 2025, 225-254.

³ Cfr. R. CASO, *La scienza non sarà più la stessa. Più condivisione, cooperazione e solidarietà dopo il Covid-19?*, in *BioLaw Journal – Rivista di BioDiritto*, 2020, Special issue n. 1, in

Rete: <http://rivista.biodiritto.org/ojs/index.php?journal=biolaw&page=article&op=view&path%5B%5D=620>, 617-622; K. WALSH, A. WALLACE, M. PAVIS, N. OLSZOWY, J. GRIFFIN, N. HAWKINS, *Intellectual Property Rights and Access in Crisis*, in *IIC*, 2021, vol. 52, 379-416, dove si ribadiva come la pandemia avrebbe potuto offrire un'opportunità cruciale per una rivalutazione sistematica dei diritti di proprietà intellettuale e per riconsiderare l'interesse del pubblico all'accesso alle informazioni. Più in generale sulle politiche europee in tema di scienza aperta si v. L. PASERI, *Scienza aperta. Politiche europee per un nuovo paradigma della ricerca*, Sesto San Giovanni, 2024; R. CASO, *La rivoluzione incompiuta. La scienza aperta tra diritto d'autore e proprietà intellettuale*, Milano, 2020.

formazioni. Diversi atti e disposizioni normative sono stati, così, emanati o proposti in linea con la c.d. “Strategia europea sui dati”, ossia il programma adottato dall’Unione europea volto a creare un mercato unico in cui i dati possano fluire liberamente e in tutti i settori a vantaggio di imprese, ricercatori e pubbliche amministrazioni⁴. In particolare, con esso si mira a creare un mercato unico digitale per i dati, promuovendone la libera circolazione all’interno dell’Unione e tra i diversi settori in modo trasparente ed equo. Il rafforzamento del controllo dei cittadini sui propri dati e sul loro utilizzo costituisce l’imperativo che spinge a definire un quadro normativo chiaro, equo e affidabile per l’accesso e l’utilizzo di questi⁵. Nel tentativo di individuare questo equilibrio, la Strategia europea sui dati si articola su quattro pilastri: i) adottare misure legislative in materia di governance, accesso e riutilizzo dei dati; ii) investire in dati, tecnologie digitali e competenze; iii) creare spazi di dati europei comuni in aree strategiche; e iv) dare potere alle imprese e ai cittadini europei⁶.

In tale ambito si inserisce, seppure precedente alla suddetta Strategia, il famoso Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (Regolamento generale sulla protezione dei dati; di seguito: “GDPR”), il quale conferma il *favor* del legislatore europeo per il trattamento di dati a fini di ricerca, già previsto nella precedente Direttiva 95/46/CE⁷.

In ordine di tempo, è necessario fare menzione della Direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio del 20 giugno 2019 relativa all’apertura dei dati e al riutilizzo dell’informazione del settore pubblico (Open Data Directive - ODD), volta a fornire un quadro giuridico comune per un mercato europeo dei dati detenuti dalle pubbliche amministrazioni. Questa ha sostituito la Direttiva sull’informazione del settore pubblico, nota come “Direttiva PSI” (Direttiva 2003/98/CE) che risale al 2003⁸. La nuova disciplina è costruita attorno a due pilastri fondamentali del mercato interno: la trasparenza e la concorrenza leale.

Ricordiamo, poi, il 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, conosciuto come “Data Governance Act” o DGA)⁹. Esso si

⁴ 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*, Bruxelles, 19.2.2020, COM(2020) 66 final.

⁵ Cfr. D. POLETTI, *Gli intermediari dei dati*, in *EJPLT*, 2022, 1, 48.

⁶ Cfr. C. SGANGA, *Ventisei anni di direttiva database alla prova della nuova strategia europea per i dati: evoluzioni giurisprudenziali e percorsi di riforma*, in *Il Diritto dell’informazione e dell’informatica*, 2022, 3, 696.

⁷ Cfr. P. GUARDA, *op. cit.*, 134-172; R. DUCATO, *Data protection, scientific research and the role of information*, in *Computer Law and Security Review*, 2020, vol. 37, in Rete: <https://doi.org/10.1016/j.clsr.2020.105412>.

⁸ Successivamente modificata dalla Direttiva 2013/37/UE. Cfr. F. FAINI, *Data society. Governo dei dati e tutela dei diritti nell’era digitale*, Milano, 2019, 141-144.

⁹ Per maggiori approfondimenti sull’articolato di questo regolamento si v. L. SPECHT-RIEMENSCHNEIDER, M. HENNEMANN (a cura di), *Data Governance Act. Article-by-Article Commentary*, Baden-Baden, Nomos, 2025.



propone di mettere a disposizione i dati del settore pubblico per il riutilizzo qualora questi siano oggetto di diritti di terzi: non prevede specifici obblighi, ma regole da applicarsi qualora si decida di consentire l'utilizzo di dati (anche dietro compenso). In breve, questo regolamento disciplina tre aspetti importanti: 1) il riutilizzo dei dati detenuti da enti pubblici (Capo II); 2) la creazione di servizi di intermediazione per lo scambio di dati (Capo III); e 3) la possibilità di allocare i dati per scopi altruistici (Capo IV). Il riutilizzo dei dati detenuti dagli enti pubblici riguarda specifiche categorie di informazioni protette, come quelle soggette a riservatezza commerciale (inclusi i segreti industriali) o statistica. Tale normativa trova applicazione anche nei confronti dei dati protetti da diritti di proprietà intellettuale di terzi, nonché di quelli soggetti alla disciplina sulla tutela dei dati personali (art. 3 DGA). I servizi di intermediazione favoriranno la possibilità di rendere disponibili i dati a condizioni di mercato tra titolari e utenti. Le autorità nazionali competenti per i servizi di intermediazione sono definite dal diritto degli Stati membri. Sotto altro profilo si prevede al Capo IV una nuova forma di consenso all'utilizzo dei dati per scopi altruistici ("data altruism") al fine di incentivare la condivisione volontaria senza compenso per obiettivi di interesse generale, secondo una logica della non rivalità e del tutto volontaristica: ciò dovrebbe anche favorire la creazione di "spazi comuni europei di dati" (Cons. 27)¹⁰. Affinché si possa parlare di altruismo dei dati ai sensi della normativa, il trattamento dovrà essere finalizzato a scopi di interesse pubblico generale, secondo quanto stabilito dalle leggi nazionali. Tale previsione è volta a trasformare un concetto radicato nell'etica in un pilastro strutturato dell'economia digitale europea, definendone chiaramente la funzione¹¹. Il concetto di consenso volontario per la condivisione dei dati per finalità generali dovrà, tuttavia, essere allineato alla nozione di consenso nel diritto in materia di protezione dei dati¹².

Il Regolamento (UE) 2023/2854 emanato il 13 dicembre 2023 (noto come Data Act), invece, mira a dare impulso non solo alla progettazione di soluzioni innovative e prodotti intelligenti, ma anche a favorire lo sviluppo di servizi complementari basati su dati già acquisiti da una vasta gamma di dispositivi interconnessi. Tra questi rientrano l'Internet of Things (IoT)¹³, i veicoli smart, i macchinari industriali automatizzati e i moderni elettrodomestici. Tale normativa è finalizzata a garantire: una maggiore competitività agli operatori economici, grazie all'incremento della disponibilità di informazioni sul mercato; ai fornitori di assistenza e manutenzione, la possibilità di proporre soluzioni altamente personalizzate in regime di libera concor-

¹⁰ Cfr. F. CREMONA, *op. cit.*, 118-119.

¹¹ Cfr. L. PASERI, *The ethical and legal challenges of data altruism for the scientific research sector*, in M. ARIAS-OLIVA, M. ET AL. (a cura di), *The leading role of smart ethics in the digital world*, Logroño, Universidad de La Rioja, 2024, 189-200.

¹² Un'approfondita riflessione in tema di consenso come strumento per la gestione dei flussi di dati si trova in S. THOBANI, *Il consenso nella regolazione della circolazione dei dati*, in *Persona e Mercato*, 2025, vol. 2, 469-486.

¹³ Per un completo ed esaustivo approfondimento volto affrontare i tanti diversi contesti giuridici nei quali i dispositivi IoT hanno un impatto si v. G. NOTO LA DIEGA, *Internet of Things and the Law. Legal strategies for consumer-centric smart technologies*, New York, Routledge, 2023.

renza con i produttori; infine, ai consumatori, un controllo effettivo sugli asset digitali generati dai propri dispositivi¹⁴. Il Regolamento impone, poi, che la progettazione e l'erogazione di prodotti e servizi interconnessi garantiscano all'utente per impostazione predefinita la fruizione dei dati, che dovranno essere accessibili in un formato completo, strutturato, di uso comune e leggibile da un dispositivo automatico e, ove possibile, in modo diretto (art. 3, par. 1). All'art. 5 si prevede, ancora, la facoltà per l'utilizzatore di trasmettere e condividere i propri dati con soggetti terzi. Infine, l'art. 14 introduce l'obbligo di fornirne l'accesso a enti pubblici, alla Commissione, alla Banca Centrale Europea o ad altri organismi dell'Unione qualora sussista una necessità eccezionale legata allo svolgimento di un compito di interesse pubblico¹⁵.

Entrambi questi interventi normativi riconoscono la precedenza al GDPR.

Altro tassello importante della strategia europea è il Regolamento (Ue) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale (regolamento sull'intelligenza artificiale, più spesso citato come AI ACT)¹⁶. Si prevedono una serie di norme basate sul rischio per gli sviluppatori e i produttori di intelligenza artificiale stabilendo quattro livelli cui conseguono specifici obblighi: rischio inaccettabile, rischio elevato (i sistemi connessi a contesti di sanità digitale di regola configureranno questa categoria), rischio limitato e rischio minimo o nullo¹⁷.

Inoltre, incoraggiare la condivisione in settori chiave può essere ottenuto istituendo specifici "spazi" di dati interoperabili a livello europeo. Pertanto, in linea con tale obiettivo, si pone il Regolamento sullo Spazio Europeo dei Dati Sanitari dell'11 febbraio 2025 (meglio conosciuto come "European Health Data Space" – EHDS)¹⁸. Questo consiste in un ecosistema specifico per la salute costituito da regole, standard e pratiche comuni, infrastrutture e un quadro di governance. Il suo scopo è quello di garantire agli individui un maggiore accesso digitale e controllo sui loro dati sanitari personali elettro-

¹⁴ Per approfondimenti si v. M. HENNEMANN, G.K. EBNER, B. KARSTEN, G. LIENEMANN, M. WIENROEDER, *Data Act. An Introduction*, Baden-Baden, Nomos, 2024.

¹⁵ Cfr. F. CREMONA, *op. cit.*, 121-123.

¹⁶ Regolamento (Ue) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale). Per approfondimenti sul suo contenuto si v., *ex plurimis*, C. NECATI PEHLIVAN, N. FORGO, P. VALCKE (a cura di), *The EU Artificial Intelligence (AI) Act*, Alphen aan den Rijn, Kluwer Law International, 2025.

¹⁷ Completano il quadro il Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio del 19 ottobre 2022 relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali) ed il Regolamento (Ue) 2022/1925 del Parlamento europeo e del Consiglio del 14 settembre 2022 relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali).

¹⁸ Regolamento (UE) 2025/327 o 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).



nici sia a livello nazionale che a livello di UE, supportandone la libera circolazione. Ancora, il Regolamento mira a promuovere un autentico mercato unico per i sistemi di cartella clinica elettronica e le applicazioni cosiddette app di e-health. L'EHDS propone, pertanto, un assetto coerente, affidabile ed efficiente per il riuso dei dati sanitari per la ricerca, l'innovazione, l'elaborazione delle politiche e le attività di regolamentazione per questo uso secondario.

Questo pacchetto di interventi normativi è sicuramente ispirato a nobili principi ed è volto a definire il contesto giuridico all'interno del quale sia possibile creare un vero e proprio mercato unico relativo alla circolazione ed al riuso dei dati. Esso presenta, però, criticità di non poco momento. In primo luogo, l'articolato stesso delle diverse disposizioni citate risulta particolarmente complesso e di non diretta comprensione, rendendo particolarmente complessa l'applicazione concreta di quanto in esso previsto. Non risulta del tutto chiara, inoltre, l'interazione e l'integrazione tra questi strumenti, determinando situazioni di sovrapposizione o di apparente contrasto normativo tutte da risolvere. Infine, il coordinamento con la disciplina prevista dal GDPR, cui tutti i testi normativi citati fanno riferimento, risulta tutt'altro che scontata¹⁹.

La trasformazione digitale richiama direttamente il concetto di "sovranità digitale dell'UE" per la tutela dei valori e dei principi fondamentali nello spazio virtuale, inserendosi nel dibattito dottrinale volto a definirne i confini e la relativa declinazione normativa²⁰. Si tratta di un concetto generale che individua la prerogativa degli Stati di imporre regole sulle attività in Rete, in special modo quando riguardano direttamente i propri cittadini²¹. Rimane complessa la possibilità di regolare fenomeni che si caratterizzano per una dimensione globale e transnazionale²². Nel contesto UE, l'"Europe's ability to act independently in the digital world" ha fornito nel 2020 una prima definizione²³. Da questo documento in poi l'approccio dell'Unione è stato sempre chiaramente politico più che giuridico e volto a promuovere una

¹⁹ Se si pensa, peraltro, al fatto che molte sperimentazioni e ricerche mediche e biomediche sono multicentriche e coinvolgono istituti in diverse parti del mondo (es. nel caso di sponsor negli Stati Uniti e ospedali in nell'UE o di centri in tutto il mondo su malattie rare), lo scenario diventa ancora più complesso e le esigenze di interoperabilità devono essere valutate con un approccio comparatistico.

²⁰ Cfr. F. CASOLARI, C. BUTTABONI, L. FLORIDI, *The EU Data Act in context: a legal assessment*, in *International Journal of Law and Information Technology*, 2023, 31, 399-412; G. FINOCCHIARO, *La sovranità digitale*, in *Diritto pubblico*, 2022, 3, 809-827; G. RESTA, F. SIMONETTI, *La c.d. sovranità digitale e il progetto Gaia-X*, in *Contratto e impresa Europa*, 2022, 3, 479-489; V. ZENO ZENCOVICH, *Data Protection[ism]*, in *Media Laws*, 2022, 2, 1-9; L. FLORIDI, *The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU*, in *Phil. & Tech.*, 2020, 369-378.

²¹ Cfr. S. MANGIAMELI, *La sovranità digitale*, in *Diritti fondamentali.it*, 2023, 3, 279-297; V. BERTOLA, *La sovranità digitale e il futuro di internet*, in *Riv. It. Inf. Dir.*, 2022, 1, 39-47.

²² Cfr. H. ROBERTS, *Digital sovereignty and artificial intelligence: a normative approach*, in *Ethics Inf Technol*, 2024, 26, (in Rete: <https://doi-org.ezp.biblio.unitn.it/10.1007/s10676-024-09810-5>).

²³ Si v. T. MADIEGA, *Digital sovereignty for Europe*, European Parliamentary Research Service, 2020, in Rete: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI\(2020\)651992_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf).

propria autonomia strategica in ambito digitale²⁴. In ciò provando a dare risposta alle minacce che le aziende ad alta tecnologia, di regola con sede in paesi extra-UE e che controllano il mercato degli strumenti e delle applicazioni digitali, hanno posto (le cosiddette “Big-Tech”).

In tale scenario caratterizzato da flussi di dati e dalla necessità di eliminare eventuali barriere alla loro condivisione, assume un ruolo rilevante il concetto di “interoperabilità”. Essa non riguarda solo gli aspetti tecnici, come gli standard per la creazione di architetture digitali e la strutturazione di database. Essa concerne anche, e soprattutto, questioni di carattere giuridico che, se non correttamente analizzate, considerate e governate possono portare al fallimento di progetti ambiziosi, quali l’EHDS, e alla limitazione di iniziative che coinvolgono più ordinamenti giuridici.

Il contributo è organizzato come segue. Dopo questo paragrafo introduttivo ci si concentrerà sulle peculiarità tipiche del contesto sanitario ed in particolare del nuovo Regolamento EHDS (par. 2). Il terzo paragrafo sarà, invece, dedicato all’approfondimento del concetto di interoperabilità, declinato nei vari contesti applicativi. L’ultimo paragrafo, infine, presenterà alcune riflessioni conclusive per una visione ricostruttiva dell’approccio alla gestione dei dati (sanitari).

2. La condivisione dei dati sanitari ed il Regolamento EHDS

La ricerca in ambito sanitario rappresenta una sottocategoria della ricerca scientifica²⁵. In questo peculiare contesto si enfatizza il rapporto tra gli interessi individuali e quelli collettivi: il trattamento dei dati relativi allo stato di salute del paziente diviene, infatti, utile al singolo al fine di curare la patologia che lo affligge, ma, al contempo, anche essenziale per contribuire al progresso scientifico. Tale scenario è sicuramente connotato da un elevato tasso di complessità ed è, pertanto, necessario addivenire ad un corretto bilanciamento dei diritti coinvolti²⁶. L’evidente vantaggio in termini di cura dei singoli deve essere, infatti, bilanciato con la più generale esigenza di tutelare la salute pubblica. È, quindi, essenziale individuare alcuni criteri volti a determinare il corretto punto di contatto tra tali necessità.

In quest’ottica, il trattamento dei dati sanitari evolve in un vero e proprio diritto-dovere del singolo, chiamato a condividere le proprie informazioni cliniche con operatori e ricercatori²⁷. Tale disponibilità non si traduce sol-

²⁴ Si v. G. FINOCCHIARO, *op. cit.*; G. RESTA, F. SIMONETTI, *op. cit.*

²⁵ Cfr. W.W. LOWERNCE, *Privacy, Confidentiality, and Health Research*, Cambridge, Cambridge University Press, 2013.

²⁶ Cfr. F. DI CIOMMO, *Il trattamento dei dati sanitari tra interessi individuali e collettivi*, in *Danno e resp.*, 2002, 2, 121. Sul bilanciamento dei diritti a livello costituzionale si v., *ex plurimis*, A. VON BOGDANDY, J. BAST, *Principles of European Constitutional law*, Oxford, Oxford University Press, 2020; R. ALEXI, *A theory of constitutional rights*, Oxford, Oxford University Press, 2010.

²⁷ Cfr. M. MOSTERT, A.L. BRENDENOORD, B. VAN DER SLOOT, J.J.M. VAN DELDEN, *From Privacy to Data Protection in the EU: Implications for Big Data Health Research*, in *European Journal of Health Law*, 2017, vol. 25, n. 1, 44, che fa riferimento ad un «ethical and scientific imperative» dell’individuo di condividere i dati personali a fini di ricerca scien-



tanto in un beneficio individuale — derivante da un'assistenza basata su un quadro anamnestico completo — ma genera una ricaduta positiva per l'intera collettività, favorendo la sicurezza sanitaria pubblica e il progresso scientifico²⁸. A questa “disponibilità” richiesta al paziente fa da contraltare un obbligo, in capo ai soggetti che professionalmente svolgono l'attività sanitaria e di ricerca scientifica, di trattare i dati con l'impegno di adottare misure e garanzie idonee a tutelarne la riservatezza.

Il legislatore europeo in tema di finalità di ricerca stabilisce alcuni principi di base e codifica l'art. 89 come punto di riferimento per una disciplina che viene lasciata agli Stati membri per quanto riguarda le regole di dettaglio²⁹. Il GDPR ha, quindi, standardizzato la legislazione a livello europeo, ma allo stesso tempo ha consentito agli Stati membri di specificare condizioni e requisiti nel contesto del trattamento dei dati per scopi di ricerca scientifica e statistica. Ciò potrebbe creare un ostacolo in quanto le attività (e quindi il trattamento dei dati personali ad esse collegati) sono spesso condotte da gruppi di partner appartenenti a diverse nazioni³⁰.

I dati relativi allo stato di salute sono quei: “*dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute*” (art. 4, pt. 15, GDPR.)³¹. Essi sono inclusi nell'elenco delle ca-

tifica; I.G. COHEN, *Is There a Duty to Share Healthcare Data?*, in I.G. COHEN, H.F. LYNCH, U. GASSER, E. VAYENA (a cura di), *Big Data, Health Law, and Bioethics*, Cambridge, Cambridge University Press, 2018, 209-222.

²⁸ Cfr. F. DI CIOMMO, *op. cit.*; F. PERLINGERI, *La personalità umana nell'ordinamento giuridico*, Il rist., Napoli-Camerino, 1982, 313.

²⁹ Un interessante approfondimento ricco di spunti di carattere comparatistico in tema di ricerca medica, GDPR ed implementazioni nazionali si legge in D. AMRAM, *Building up the “Accountable Ulysses” model. The impact of GDPR and national implementations, ethics, and health-data research: Comparative remarks*, in *Computer Law & Security Review*, 2020, vol. 37, in Rete: <https://www.sciencedirect.com/science/article/pii/S0267364920300182>. Cfr. anche G. SCHNEIDER, *Disentangling Health Data Networks: a Critical Analysis of art. 9.2 and art. 89 GDPR*, in *International Data Privacy Law*, 2019, vol. 9, n. 4, 253; G. COMANDÉ, *Ricerca in sanità e data protection... un puzzle risolvibile*, in *Riv. it. medicina legale*, 2019, 189. Circa l'applicazione del GDPR al contesto della ricerca in ambito sanitario si v. EDPB, *EDPB Document on response to the request from the European Commission for clarification on the consistent application of the GDPR, focusing on health research*, 2021, in Rete: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_replyec_questionnairesearch_final.pdf.

³⁰ Sul punto c'è da sperare che l'uniformazione delle regole, essenziale per attivare proficui processi di ricerca nell'ambito dell'Unione europea, sia garantita da strumenti di soft law quali i ‘codici di condotta’ che vengono direttamente richiamati all'art. 40 GDPR. In ambito biomedico si segnala, allora, l'iniziativa della rete europea ‘Biobanking and BioMolecular Resources Research Infrastructure-European Research Infrastructure Consortium (BBMRI-ERIC)’, che sta lavorando alla redazione di una bozza di ‘Code of Conduct for Health Research’: <https://www.bbmri-eric.eu/news-events/code-of-conduct-for-health-research/>.

³¹ Per maggiori approfondimenti in tema di dati relativi allo stato di salute si v. T. MULDER, *The Protection of Data Concerning Health in Europe*, in *Eur. Data Prot. L. Rev.*, 2019, vol. 5, 209-220; P. GUARDA, *I dati sanitari*, in *I dati personali nel diritto europeo*, (a cura di) V. CUFFARO, R. D'ORAZIO, V. RICCIUTO, Torino, 2019, 591-626; M. GRANIERI, *Il trattamento di categorie particolari di dati personali nel reg. UE 2016/679*, in *Nuove leggi civ. comm.*, 2017, n. 1, 165-190.

tegorie particolari di dati personali di cui all'art. 9 GDPR e quindi oggetto del generale divieto di trattamento sancito al primo paragrafo. Esistono alcune eccezioni a tale divieto³². Queste possono essere suddivise in tre gruppi: 1) il consenso dell'interessato ai sensi dell'art. 9, par. 2, lett. a) GDPR e, strettamente correlati ad esso, la necessità di tutelare un interesse vitale dell'interessato (lett. c)), nonché la manifesta pubblicità dei dati personali (lett. e)); 2) il trattamento necessario per motivi di rilevante interesse pubblico ai sensi dell'art. 9, par. 2, lett. g), per le finalità di medicina preventiva o del lavoro, diagnosi medica, prestazione di cure o cure sanitarie o sociali o gestione dell'assistenza sanitaria o sociale e dei sistemi e servizi di cui all'art. 9, par. 2, lett. h) e per motivi di interesse pubblico in materia di sanità pubblica ex art. 9, par. 2, lett. i); 3) il trattamento necessario per finalità di archiviazione nel pubblico interesse, di ricerca scientifica o storica o per finalità statistiche ai sensi dell'art. 9, par. 2, lett. j)³³. Tale disciplina è da intendersi come complementare rispetto ai requisiti generali per un trattamento lecito dei dati di cui all'art. 6 GDPR: l'esistenza di una base legale di carattere generale diviene allora il presupposto per il trattamento di categorie particolari di dati³⁴.

Come anticipato il Regolamento EHDS mira a creare un ecosistema sanitario specifico costituito da norme, standard e pratiche comuni, infrastrutture e un quadro di governance³⁵. Il suo obiettivo è quello di responsabilizzare gli individui fornendo un maggiore accesso digitale e un maggiore controllo sui propri dati sanitari elettronici a livello nazionale e dell'UE, nonché sup-

³² Per maggiori approfondimenti si v. G. SCHNEIDER, *Health Data Pools under European Policy and Data Protection Law: Research as a New Efficiency Defence*, in *JIPITEC*, 2020, vol. 11, 49, 61 ss., dove si propone una divisione in tre sottocategorie di possibili basi giuridiche per il trattamento dei dati relativi alla salute.

³³ La "research exemption" prevista dall'art. 9, par. 2, lett. j) solleva alcune incertezze interpretative. Si v. G. SCHNEIDER, *Health Data Pools*, cit., 61-63.

³⁴ Alla luce del possibile rischio che anche attività orientate a fini commerciali possano giovare del regime di favore previsto per la ricerca scientifica nel GDPR, è stato rimarcata la necessità di limitare l'ampia interpretazione fornita alla nozione di ricerca scientifica in modo da poterla circoscrivere alle sole attività orientate all'interesse pubblico. Alcuni hanno, infatti, espresso dei dubbi che la ricerca in ambito privato e per fini commerciali possa abusare della disciplina di favore sancita dall'art. 89 GDPR: si v. P. QUINN, *Research under the GDPR – a level playing field for public and private sector research?*, *Life Sciences, Society and Policy*, 2021, 17:4, in Rete: <https://link.springer.com/article/10.1186/s40504-021-00111-z> (dove si sostiene che benché la nozione di ricerca possa ricomprendere sia soggetti pubblici che privati, la disciplina di favore prevista dal GDPR non offre le stesse condizioni a tutti gli attori coinvolti, in special modo quando il trattamento riguarda dati sensibili); M. SHABANI, P. BORRY, *Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation*, in *European Journal of Human Genetics*, 2018, vol. 26, 149, 153.

³⁵ Prima della pubblicazione, il Comitato europeo per la protezione dei dati e il Garante europeo della protezione dei dati hanno sollevato una serie di critiche ("Parere congiunto 03/2022 sulla proposta di regolamento sullo Spazio Europeo dei Dati Sanitari"). Per un'analisi puntuale dei rilievi mossi si v. G. BINCOLETTI, *The EDPB-EDPS Joint Opinion on the Commission Proposal for a Regulation on the European Health Data Space: Key Issues to be Considered in the Legislative Process*, in *European Data Protection Law Review*, 2022, 8, n. 3, 398-404. Cfr. anche O. GRABER-SOUDRY, T. MINNSEN, D. NILSSON, M. CORRALES, J. WESTED, B. ILLIEN, *Legal interoperability and the FAIR data principles*, EOSC Study, December 2020, in Rete: <https://zenodo.org/record/4471312>.

portandone la libera circolazione. Il Regolamento è volto a promuovere un autentico mercato unico per i sistemi di cartelle cliniche elettroniche e le applicazioni per il benessere. L'EHDS ha l'obiettivo di creare un quadro coerente, affidabile ed efficiente per l'utilizzo dei dati sanitari a fini di ricerca, innovazione, definizione delle politiche e attività di regolamentazione per uso secondario³⁶.

L'EHDS dovrà essere interconnesso con i diversi sistemi nazionali di fascicolo sanitario elettronico (FSE) che sono adottati in tutti gli Stati membri. A livello europeo il quadro normativo è costituito dall'articolo 8 della Carta dei diritti fondamentali dell'UE, dal GDPR e dalla Direttiva 2011/24/UE sui diritti dei pazienti nell'assistenza sanitaria transfrontaliera³⁷. A complicare lo scenario ogni Stato membro può prevedere norme specifiche³⁸ e differenze sussistono sia a livello di regole operazionali in materia di protezione dei dati personali che nelle soluzioni architetturali implementate³⁹. Prendendo il FSE italiano come caso paradigmatico⁴⁰, merita di essere ricordato che, già nel 2009, il Garante per la Protezione dei Dati Personali aveva pubblicato alcune linee guida sui sistemi di FSE, fornendo un elenco di garanzie da attuare per tutelare il diritto alla protezione dei dati dei pazienti italiani⁴¹. L'art. 12 del D.L. 18 ottobre 2012, n. 179 (convertito con modificazioni dalla L. 17 dicembre 2012, n. 221) ha, poi, creato il quadro normativo per l'utilizzo del FSE. Questo può essere alimentato da tutti i soggetti del SSN a livello regionale coinvolti nell'assistenza al paziente, incluso in alcuni casi dallo stesso paziente. Il FSE è istituito dalle Regioni e dalle Province Auto-

³⁶ Per un interessante approfondimento nel quale vengono individuati e discussi i settori giuridici nei quali la creazione di un EHDS può incontrare difficoltà o che possono influenzarne lo sviluppo si v. A. KISELEVA, P. DE HERT, *Creating a European Health Data Space. Obstacles in Four Key Legal Areas*, in *European Pharmaceutical Law Review*, 2021, vol. 5, issue 1, 21-36.

³⁷ Il Regolamento 910/2014 sull'identificazione elettronica può anche trovare applicazione con riferimento alla sicurezza delle firme elettroniche, all'identificazione elettronica e all'autenticazione degli individui nel sistema; la Direttiva 2016/1148 sulla sicurezza delle reti e dei sistemi informativi e i suoi recepimenti nazionali stabiliscono altre norme. Il trattamento attuato tramite FSE deve, peraltro, essere conforme a quanto stabilito dall'articolo 8 della CEDU, dalla Convenzione del Consiglio d'Europa, dalla Raccomandazione del Consiglio d'Europa n. R(97) 5 e dalla Raccomandazione del Consiglio d'Europa CM/Rec (2019).

³⁸ Cfr. J. DUMORTIER, G. VERHENNEMAN, *Legal regulations on electronic health records: a prerequisite or an unavoidable by-product? – The legal aspects of electronic health records in Europe and the US analysed*, in *ICRI Research Paper*, 2011, n. 5 (in Rete: <https://ssrn.com/abstract=1975758>).

³⁹ Per una completa disamina sui sistemi di fascicolo sanitario elettronico e per una dettagliata descrizione di alcuni modelli nazionali si v. G. BINCOLETTI, *Data Protection by Design in the E-Health Care Sector. Theoretical and Applied Perspectives*, Baden-Baden, Nomos, 2021, 229-283.

⁴⁰ Ma appunto sistemi simili sono adottati in altre esperienze nazionali. In Francia, ad esempio, il *dossier médical partagé* (DMP) conserva la storia clinica dei pazienti francesi e consente la raccolta di tutti gli altri dati sanitari personali in ambiti specifici, in conformità con il *Code de la Santé publique*. Il dossier è compilato da tutti i professionisti autorizzati al trattamento del paziente. Cfr. G. BINCOLETTI, *op.cit.*, 243-246.

⁴¹ Garante per la protezione dei dati, *Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario - 16 luglio 2009*, Doc. web. 1672821. G.U. n. 178 del 3 agosto 2009.

nome per finalità di assistenza, ricerca scientifica in campo medico, biomedico ed epidemiologico e per la programmazione sanitaria pubblica, la verifica della qualità dell'assistenza e la valutazione dell'assistenza sanitaria a livello di governance. Il sistema è stato recentemente sottoposto a *restyling* ed è ora denominato versione 2.0 a seguito della riforma operata dal Decreto del Ministero della Salute 7 settembre 2023 (in attuazione dell'art. 12, co. 7, del D.L. 179/2012). Il nuovo FSE 2.0 ha visto potenziare l'infrastruttura tecnologica e definire standard nazionali omogenei. Sebbene il FSE sia ora popolato automaticamente (senza alcuna richiesta di consenso esplicito per nuovi dati), l'interessato mantiene un elevato livello di controllo sulla possibilità di oscurare i propri dati e quindi di non renderli visibili a terzi (vedi i c.d. "dati a maggior tutela"). Inoltre, la segmentazione dell'accesso ai dati da parte degli operatori sanitari per scopi di cura o prevenzione è subordinata al consenso del paziente. Nella stessa direzione del FSE 2.0 si muove l'Ecosistema dei Dati Sanitari che, alimentato direttamente dal FSE, è uno strumento di coordinamento informativo volto a sviluppare un sistema centralizzato per la raccolta e l'analisi dei dati sanitari. Ciò consente l'erogazione di servizi per la cura, la prevenzione e la profilassi internazionale, nonché per la governance e la ricerca scientifica⁴².

Il Regolamento EHDS è entrato in vigore il 26 marzo 2025. Il periodo transitorio prima della sua piena applicazione è esteso. Fino a marzo 2027 saranno predisposti atti di attuazione chiave che definiranno importanti specifiche tecniche. Le parti interessate avranno poi altri due anni, fino a marzo 2029, per implementare tali specifiche e garantire che i loro sistemi siano pronti. Lo scambio delle categorie di dati prioritarie per l'uso primario (schede informative dei pazienti, prescrizioni/dispensazioni elettroniche) e le regole per la maggior parte delle categorie di dati per l'uso secondario entreranno in vigore a marzo 2029. Il secondo gruppo di categorie prioritarie per l'uso primario (immagini mediche, risultati di laboratorio, referti di dimissioni ospedaliere) e le regole per le restanti categorie di dati per l'uso secondario saranno soggette a scambio a partire da marzo 2031⁴³. A marzo 2035, paesi terzi e organizzazioni internazionali potranno aderire (a condizioni rigorose) all'eventuale condivisione per l'uso secondario.

L'EHDS non è in realtà uno spazio centralizzato per l'archiviazione dei dati, ma piuttosto una connessione punto a punto tra i titolari e gli utenti dei dati sanitari all'interno di un ambiente sicuro e incentrato sulla privacy per la messa in comune, l'accesso, la condivisione, l'elaborazione e l'utilizzo dei dati attraverso infrastrutture armonizzate.

Le categorie di dati che devono essere rese disponibili per l'uso secondario sono numerose. L'articolo 51, par. 1, del Regolamento EHDS elenca quelle minime. La procedura per ottenere l'accesso ai dati coinvolge i cosiddetti "Organismi per l'Accesso ai Dati Sanitari" (Health Data Access Body - HDAB). I richiedenti presentano le loro domande di accesso ai dati (art.

⁴² Cfr. C. FILIPPI, *L'impatto della digitalizzazione del SSN sulla protezione dei dati personali*, in G. CERRINA FERONI (a cura di), *Le nuove frontiere della medicina*, Bologna, 2024, 149.

⁴³ Ai sensi dell'art. 105 Regolamento EHDS, questi sono elencati nell'art. 51, par. 1, lett. b), f), g), m) e p).

67 Regolamento EHDS) agli HDAB, che poi autorizzano e rilasciano un permesso per l'accesso ai dati (art. 68). Come regola di base, l'accesso sarà concesso solo ai dati anonimizzati, a meno che il richiedente non dimostri in modo sufficiente che lo scopo non può essere raggiunto elaborando solo dati anonimizzati (par. 3)⁴⁴.

Aspetto di sicuro interesse è quanto previsto dall'art. 53, dedicato alle finalità per le quali è possibile trattare dati sanitari elettronici per uso secondario. Si prevede, infatti, 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: (...) 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”*⁴⁵. Gli interessati avranno il diritto di rifiutare tale trattamento attraverso un meccanismo di opt-out che sarà stabilito dagli Stati membri (art. 71 Reg. EHDS). Si tratta di un punto a lungo discusso nell'ambito del trilog e delle negoziazioni tra le istituzioni comunitarie e che non era previsto nella primissima versione della proposta di Regolamento della Commissione. Ai fini dell'esercizio di tale diritto, che è in ogni caso reversibile, gli Stati membri dovranno prevedere un meccanismo accessibile e facilmente comprensibile. Una volta esercitato il diritto di opt-out, il set di dati collegato alla persona non sarà più reso disponibile o altrimenti trattato, pur non essendo pregiudicato il trattamento dei dati sanitari elettronici personali relativi a tale persona fisica per un uso secondario ai sensi delle autorizzazioni o delle richieste di dati concesse prima che la persona fisica avesse optato per la cancellazione. Resta salva la facoltà degli Stati membri di introdurre, tramite normativa interna, meccanismi volti a consentire l'accesso ai dati anche in presenza di un opt-out dell'interessato. Tale deroga è subordinata al ricorrere di specifiche condizioni, segnatamente qualora la richiesta provenga da soggetti pubblici (enti del settore pubblico, istituzioni o agenzie dell'Unione) investiti di funzioni di sanità pubblica, o da entità che agiscano per conto di autorità pubbliche, laddove il tratta-

⁴⁴ Al fine di incentivare un uso secondario dei dati realmente efficace, occorre operare un delicato bilanciamento tra l'utilità sociale derivante dall'innovazione sanitaria e l'esigenza, sia pubblica che privata, di salvaguardare i dati. In tale alveo, la tutela dei segreti commerciali può assumere un ruolo cardine, ponendosi come presupposto indispensabile per garantire la competitività degli innovatori nel rispetto della cornice normativa vigente. Cfr. G. RESTA, *Pubblico, privato, collettivo nel sistema europeo di governo dei dati*, in *Rivista trimestrale di diritto pubblico*, 2022, n. 4, 971-995.

⁴⁵ Sul rapporto tra EHDS, disciplina in materia di protezione dei dati personali e impatto dei sistemi di intelligenza artificiale si v. I. SANCHEZ FRIAS, *Secondary uses of health data under the European Health Data Space. Connections with the GDPR and the impact of AI*, in *Revista General de Derecho Europeo*, 2025, n. 65, 212-223.

mento risulti strettamente necessario al perseguimento di finalità di interesse generale. La legislazione degli Stati membri può, inoltre, introdurre garanzie aggiuntive e più stringenti (inclusa la necessità del consenso, quindi una forma di opt-in) in merito ad alcune categorie di dati, quali ad esempio i dati genetici, epigenomici e genomici umani, altri dati molecolari umani, i dati sanitari dalle biobanche e dai database associati, o i dati dalle applicazioni wellness.

La previsione andrà, poi, coordinata con quanto previsto in materia di base legittima del trattamento dalla l. 23 settembre 2025, n. 132 “Disposizioni e deleghe al Governo in materia di intelligenza Artificiale”. Si tratta del primo quadro normativo organico italiano dedicato all’IA, che recepisce le indicazioni dell’AI ACT ed introduce regole chiare per lo sviluppo, l’adozione e l’uso delle nuove tecnologie. All’art. 8 di tale legge si prevede che il trattamento di dati personali eseguito dai soggetti ivi indicati per la ricerca e la sperimentazione in ambito medico siano dichiarati di rilevante interesse pubblico nel rispetto di quanto previsto dall’art. 9, par. 2, lett. g) GDPR (co. 1). Ai medesimi fini è autorizzato l’uso secondario di dati privi degli elementi identificativi diretti da parte dei soggetti di cui al comma 1, salvi i casi nei quali la conoscenza dell’identità degli interessati sia inevitabile o necessaria al fine della tutela della loro salute⁴⁶.

Ancora con riferimento alla corretta individuazione della base giuridica del trattamento per l’uso secondario, l’adattamento e l’interpretazione del GDPR da parte degli Stati membri consegna un quadro a tratti disomogeneo ed ha creato considerevoli incertezze da un punto di vista giuridico. Tutto questo determina evidenti ostacoli nell’uso secondario dei dati sanitari elettronici⁴⁷. Si aggiunga che, a causa di standard diversi e di un’interoperabilità limitata, i produttori ed i fornitori di servizi sanitari digitali che operano in uno Stato membro si trovano ad affrontare barriere e costi aggiuntivi quando circolano all’interno dell’Unione. Problematiche simili si rinvencono, allora, laddove troviamo Paesi nei quali è pacificamente ammesso il legittimo interesse (in combinato disposto, per i dati sanitari, con l’eccezione al divieto di trattamento per finalità di ricerca scientifica o altre eccezioni di cui all’articolo 9, par. 2 del GDPR), e altri che appaiono più conservativi e “consenso-centrici”, come l’Italia. Il Regolamento EHDS affronta esplicitamente il tema all’interno del Considerando 52, ove afferma che, senza ostacolare o sostituire i meccanismi contrattuali o di altro tipo esistenti, esso stesso è volto a stabilire un meccanismo comune di accesso ai dati sanitari elettronici per uso secondario in tutta l’Unione europea, in base al quale i titolari dei dati devono rendere disponibili i dati in loro possesso sulla base di un’autorizzazione. Più precisamente, per il trattamento dei dati sanitari

⁴⁶ A garanzia di ciò il comma 5 dell’art. 8 prevede che: “*I trattamenti di dati di cui ai commi 1 e 2 devono essere comunicati al Garante per la protezione dei dati personali con l’indicazione di tutte le informazioni previste dagli articoli 24, 25, 32 e 35 del regolamento (UE) 2016/679, nonché con l’indicazione espressa, ove presenti, dei soggetti individuati ai sensi dell’articolo 28 del medesimo regolamento (UE) 2016/679, e possono essere avviati decorsi trenta giorni dalla predetta comunicazione se non sono stati oggetto di provvedimento di blocco disposto dal Garante per la protezione dei dati personali*”.

⁴⁷ Si v. EUROPEAN COMMISSION, *Assessment of the EU Member States’ rules on health data in the light of the GDPR*, 2021, 57-80. Cfr. I. SANCHEZ FRIAS, *op. cit.*, 212-223, sec. III-1.

elettronici detenuti dai titolari di dati sanitari, è l'EHDS a creare l'obbligo legale ai sensi dell'art. 6, par. 1, lett. c) GDPR, in conformità con l'art. 9, par. 2, lett. i) e j), per la messa a disposizione di tali dati da parte del relativo titolare agli organismi di accesso ai dati sanitari, andandosi così a distinguere dalla base giuridica per lo scopo primario (quale, a titolo esemplificativo, la fornitura di assistenza sanitaria), che non viene intaccata. Inoltre, l'EHDS istituisce compiti di interesse pubblico ai sensi dell'art. 6, par. 1, lett. e) GDPR in capo agli organismi di accesso ai dati sanitari e soddisfa i requisiti dell'art. 9, par. 2, lett. g), h), i) e j) GDPR. Per quanto concerne, invece, l'utente dei dati sanitari, viene chiarito che, se lo stesso si basa su una base giuridica offerta dall'art. 6, par. 1, lett. e) o f) GDPR, allora l'EHDS dovrebbe fornire le garanzie richieste dall'art. 9, par. 2 dello stesso GDPR.

Sempre in merito al rischio di frammentazione normativa, si ricordi quanto previsto dall'art. 9, par. 4, del GDPR con riferimento al trattamento di categorie particolari di dati: *“gli Stati membri possano mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute”*. Questa disposizione ha aperto la strada a differenti adattamenti nazionali come era prevedibile avvenisse⁴⁸. In Francia, ad esempio, le linee guida legislative impongono vincoli al riconoscimento e all'utilizzo di dati sanitari anonimizzati per attività di ricerca prospettica, mentre la Finlandia ha emanato una recente legislazione volta a facilitare il trattamento secondario dei dati sanitari. I Paesi Bassi, invece, hanno adottato interpretazioni rigorose del GDPR, con conseguenti limitazioni all'utilizzo dei dati sanitari nell'ambito dell'intelligenza artificiale. Infine, l'ordinamento tedesco consente l'utilizzo dei dati per finalità di ricerca scientifica, sebbene con una esplicita esclusione del coinvolgimento dell'industria privata.

In chiusura, un fattore che in tale contesto gioca un ruolo rilevante è quello relativo al concetto di anonimizzazione dei dati. Il legislatore europeo sembra aver dato per scontato un problema che, invece, ha un effetto diretto nei processi di condivisione. Il confine tra anonimizzazione e pseudonimizzazione sembra farsi sempre più labile. Il settore sanitario presenta alcuni casi che dimostrano come una completa anonimizzazione dei dati non sia altro che una chimera. Un chiaro esempio sono le malattie rare, dove il numero limitato di casi riduce la possibilità di aggregare completamente i dati pubblicati per preservare la privacy delle persone fisiche. Studi recenti appaiono dimostrare che l'anonimizzazione completa semplicemente non sia possibile, soprattutto con l'avvento delle tecniche di intelligenza artificiale⁴⁹. Altri approfondimenti evidenziano come gli utilizzatori dei dati solitamente rilevano una mancanza di linee guida a livello nazionale e internazio-

⁴⁸ TEHDAS, *Report on secondary use of health data through European case studies*, 28 febbraio 2022, in Rete: <https://tehdas.eu/app/uploads/2022/08/tehdas-report-on-secondary-use-of-health-data-through-european-case-studies-.pdf>; OPEN DATA INSTITUTE, *Secondary use of health data in Europe*, 2021, 8-21, in Rete: <https://secondary-use-health-data.theodi.org/assets/pdf/Secondary-use-of-Health-Data-In-Europe-ODI-Roche-Report-2021-5-1.pdf>.

⁴⁹ Cfr. D. NUNAN, M. DI DOMENICO, *Exploring Reidentification Risk: Is Anonymisation a Promise we can Keep?*, in *International Journal of Market Research*, 2016, vol. 58, issue 1, 19-34.

nale sul concetto di pseudonimizzazione, il che porta ad approcci diversi, sia all'interno che tra i paesi europei⁵⁰. Gli operatori del settore dei dati rimarcano, peraltro, la mancanza di consenso sul grado di separazione necessario tra la chiave di reidentificazione e l'utilizzatore dei dati affinché questi possano essere considerati pseudonimizzati, e una mancanza di coerenza sulla scelta tra pseudonimizzazione o anonimizzazione⁵¹. Inoltre, a dimostrazione di come il concetto di anonimizzazione si sia evoluto rispetto a quello incluso nel GDPR, in un caso relativo ad una procedura di indennizzo degli azionisti e creditori in seguito alla risoluzione di un ente creditizio, la Corte di Giustizia dell'Unione Europea ha recentemente stabilito che i dati pseudonimizzati trasmessi a un destinatario non saranno considerati dati personali se quest'ultimo non dispone dei mezzi per reidentificare l'interessato⁵².

Gli evidenti rischi di reidentificazione dei dati, sia anonimizzati che pseudoanonimizzati, ha portato il legislatore europeo ad inserire nel Regolamento EHDS un esplicito obbligo in capo agli utenti di dati sanitari all'art. 61, par. 3: “[questi] non reidentificano e non cercano di reidentificare le persone fisiche a cui si riferiscono i dati sanitari elettronici ottenuti dagli utenti dei dati sanitari sulla base di un'autorizzazione ai dati, di una richiesta di dati sanitari o di un'approvazione dell'accesso da parte di un partecipante autorizzato a DatiSanitari@UE (HealthData@EU)”. Ovvero, il divieto non è limitato ai soli dati pseudonimizzati, ma appare riconosciuto (indirettamente) anche il rischio di reidentificazione dei dati sottoposti a tecniche di anonimizzazione.

3. Alla ricerca di una definizione al concetto di interoperabilità giuridica

La connessione dei sistemi tra gli Stati membri implica il raggiungimento della cosiddetta “interoperabilità”⁵³. Questo termine non ha una connotazione giuridica diretta, essendo piuttosto un'espressione del mondo tecnico. Esso, infatti, si declina su più livelli: quello tecnico evidentemente, avendo a riferimento standards, struttura delle banche dati, scelte infrastrutturali; quello semantico, con riferimento all'utilizzo di “linguaggi” atti a far comprendere ai diversi sistemi interconnessi i dati nello stesso modo e senza ambiguità; quello organizzativo, al fine di garantire che processi aziendali

⁵⁰ TEHDAS, *op.cit.*, 13-24.

⁵¹ TEHDAS, *op. loc. ult. cit.*

⁵² Sent. Corte di Giustizia dell'Unione europea (Prima sezione), 4 settembre 2025, *Garante europeo della protezione dei dati contro Comitato di risoluzione unico*, C-413/23 P (in Rete:

<https://curia.europa.eu/juris/document/document.jsf?text=&docid=303863&pageIndex=0&doclang=IT&mode=req&dir=&occ=first&part=1&cid=16795348>).

⁵³ Si v. P. GUARDA., *op.cit.*, 39-43; O. GRABER-SOUDRY, T. MINNSEN, D. NILSSON, M. CORRALES, J. WESTED, B. ILLIEN, *Legal Interoperability and the FAIR Data Principles (1.0)*, An X-officio study commissioned by the EOSC FAIR Working Group, 2021, 18-23 (in Rete: <https://doi.org/10.5281/zenodo.4471312>).



separati possano agire in modo indipendente⁵⁴. Un ambiente aperto e interoperabile può stimolare l'innovazione.

Il termine “interoperabilità giuridica”, sviluppato solo di recente, si riferisce al processo di cooperazione tra norme giuridiche tra giurisdizioni diverse: questa accezione può facilitare la comunicazione globale, ridurre i costi delle attività commerciali transfrontaliere e stimolare l'innovazione, creando così condizioni di parità per la prossima generazione di tecnologie e scambi culturali⁵⁵.

L'Organizzazione Internazionale per la Standardizzazione (ISO) definisce l'interoperabilità come la “*ability of two or more systems or components to exchange information and to use the information that has been exchanged*”⁵⁶; lo European Interoperability Framework Report la descrive come “*the ability of organisations to interact towards mutually beneficial goals, involving the sharing of information and knowledge between these organisations, through the business processes they support, by means of the exchange of data between their ICT systems*”⁵⁷.

Le definizioni proposte dal legislatore europeo sono, invece, specifiche per i diversi contesti. Una versione si ritrova nel Considerando 12 della Direttiva sui programmi per elaboratore⁵⁸, che stabilisce che l'interoperabilità è “*la capacità di scambiare informazioni e di utilizzare reciprocamente le informazioni scambiate*”. La Direttiva INSPIRE⁵⁹ afferma che essa rappresenta “*possibilità per i set di dati [spaziali] di essere combinati e per i servizi di interagire, senza interventi manuali ripetitivi, in modo tale che il risultato sia coerente e il valore aggiunto il valore dei set di dati e dei servizi è accresciuto*”. Da ultimo, anche il Regolamento EHDS propone una definizione del concetto di “interoperabilità” all'art. 2, par. 1, lett. f) che rimane evidentemente sul piano tecnico: “*la capacità delle organizzazioni, nonché delle applicazioni software o dei dispositivi dello stesso fabbricante o di fabbricanti diversi, di interagire tra loro attraverso i processi che supporta-*

⁵⁴ Per un'approfondita analisi che propone alcune prime prospettive ricostruttive in tema di interoperabilità nel contesto dei sistemi di FSE si v. G. BINCOLETTI, *Data protection issues in cross-border interoperability of Electronic Health Record systems within the European Union*, in *Data & Policy*, 2020, v. 2, e3.1-e3.11.

⁵⁵ Per maggiori approfondimenti in tema di interoperabilità giuridica si v. R.H WEBER, *Legal Interoperability as a Tool for Comatting Framnetation*, Global Commission on Internet Governance, Paper Series: No. 4, December 2014, in Rete: https://www.cigionline.org/static/documents/gcig_paper_no4.pdf.

⁵⁶ *International Organization for Standardization*, ISO/TS 27790:2009, in Rete: <https://www.iso.org/standard/44316.html>.

⁵⁷ European Commission, *New European interoperability framework - Promoting seamless services and data flows for European public administrations*, 2017, in Rete: <https://op.europa.eu/en/publication-detail/-/publication/bca40dde-deee-11e7-9749-01aa75ed71a1/language-en>.

⁵⁸ Direttiva 2009/24/CE del Parlamento europeo e del Consiglio, del 23 aprile 2009, relativa alla tutela giuridica dei programmi per elaboratore [GU L 111/16 del 2009] (originariamente Direttiva 91/250/CEE del Consiglio, del 14 maggio 1991, relativa alla tutela giuridica dei programmi per elaboratore [GU L 122/42 del 1991]) (“Direttiva sui programmi per elaboratore”).

⁵⁹ Direttiva 2007/2/CE del Parlamento europeo e del Consiglio, del 14 marzo 2007, che istituisce un'Infrastruttura per l'informazione territoriale nella Comunità europea [2007] GU L 108 (“Direttiva INSPIRE”).

no, il che comporta lo scambio di informazioni e conoscenze tra tali organizzazioni, applicazioni software o dispositivi, senza che sia modificato il contenuto dei dati”.

Sempre soffermandoci sul contesto normativo oggetto di analisi in questo contributo, alcuni autori rilevano come si possano fare dei parallelismi e sviluppare interessanti considerazioni prendendo a riferimento il diritto alla portabilità dei dati così come previsto nel GDPR e nel nuovo Regolamento EHDS⁶⁰. Il nucleo del diritto alla portabilità previsto dall’art. 20 GDPR risiede nel requisito che i dati siano forniti e trasmessi “in un formato strutturato, di uso comune e leggibile da dispositivo automatico” (par. 1)⁶¹. Le linee guida del Gruppo di Lavoro art. 29 ritengono che “strutturato”, “di uso comune” e “leggibile da dispositivo automatico” siano un insieme di “requisiti minimi” tra cui l’interoperabilità è il risultato auspicato⁶². Tuttavia, dalla lettura dell’articolo 20 si evince che, oltre ai tre requisiti obbligatori, il raggiungimento dell’interoperabilità non rappresenta un obbligo di legge. Inoltre, l’articolo al secondo paragrafo fa riferimento al termine “tecnicamente fattibile” quando si determina se un titolare del trattamento debba trasferire i dati richiesti direttamente a un altro (senza passare attraverso l’interessato). Per spiegare cosa implichi la “fattibilità tecnica”, il Gruppo articolo 29 suggerisce che, sebbene la valutazione debba essere effettuata caso per caso, la trasmissione diretta dovrebbe avvenire “quando la comunicazione tra due sistemi è possibile, in modo sicuro, e quando il sistema ricevente è tecnicamente in grado di ricevere i dati in entrata”⁶³. Il GDPR non impone nemmeno ai titolari del trattamento (o ai destinatari) l’obbligo di raggiungere tale fattibilità tecnica.

Per quanto concerne, invece, il Regolamento EHDS, l’art. 7, par. 2, prevede un vero e proprio diritto in capo alle persone fisiche: “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”. In una certa misura, con la specificazione del formato europeo di scambio delle cartelle cliniche elettroniche e i requisiti di interoperabilità obbligatori per i sistemi di FSE, il Regolamento EHDS appresta un possibile rimedio alla mancanza di certezza del GDPR in materia di interoperabilità. Se l’interoperabilità dei sistemi di FSE e delle app per il benessere, guidata dai requisiti legali, può essere migliorata a livello tecnico, ciò faciliterà certamente l’applicazione delle norme sulla

⁶⁰ Cfr. W. LI, P. QUINN, *The European Health Data Space: An expanded right to data portability*, in *Computer Law & Security Review*, 2024, vol. 52, 105913, in part. par. 6 (in Rete: <https://doi.org/10.1016/j.clsr.2023.105913>)

⁶¹ Questo rappresenta un fondamento importante che distingue il diritto alla portabilità dei dati dal diritto di accesso. Cfr. P. DE HERT ET AL., *The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services*, in *Computer Law & Security Review*, 2018, vol. 34, 193.

⁶² Gruppo di lavoro Art. 29, *Linee-guida sul “diritto alla portabilità dei dati”*, adottate il 13 dicembre 2016, versione emendata e adottata il 5 aprile 2017, WP 242 rev.01.

⁶³ *Ibidem*, 16.

portabilità dei dati sia nel GDPR che nell'EHDS, e quindi la responsabilizzazione degli individui in termini di controllo più flessibile e funzionale dei propri dati sanitari elettronici.

L'interoperabilità, in ambito giuridico, può essere perseguita applicando due tipi di modelli: top-down, il quale richiede necessariamente l'istituzione di un'agenzia globale o comunque un organismo internazionale che abbia una competenza sovra-statale; o un processo bottom-up, basato su un modello graduale che comprenda il coinvolgimento delle principali entità e soggetti coinvolti ed interessati rispetto allo scenario applicativo di riferimento.

Per quanto riguarda gli strumenti e le modalità che possono esser utilizzate possiamo distinguere tra armonizzazione, standardizzazione e riconoscimento reciproco⁶⁴. L'armonizzazione normativa, pilastro fondamentale dell'interoperabilità giuridica, si configura come lo strumento volto a istituzionalizzare la cooperazione tra ordinamenti, inquadrando attori e politiche entro un perimetro definito di diritti e obblighi. Tale processo spesso muove da una fase preliminare di standardizzazione intesa come adozione di principi e linee guida condivise in un settore; rappresenta, pertanto, un avanzamento decisivo verso la convergenza giuridica. Distinto da ciò è il mutuo riconoscimento, il quale presuppone una valutazione di equivalenza tra le misure normative dei diversi ordinamenti: esso implica un parziale sacrificio dell'autonomia nazionale, fondandosi sul consenso a ritenere le discipline straniere come intercambiabili e, pertanto, applicabili all'interno del proprio ordinamento.

L'interoperabilità giuridica, allora, risulta volta ad evitare o, almeno, a ridurre barriere affinché soggetti che operano all'interno di ordinamenti giuridici diversi possano essere in grado di lavorare assieme. Da questa prospettiva è sovrapponibile al concetto di ricostruzione in chiave sistematica del quadro giuridico di riferimento: quella sistematicità che si è progressivamente perduta nell'affastellarsi, a tratti nebuloso, degli interventi normativi ma per ritrovare la quale la comparazione potrebbe fornire strumenti efficaci.

In sintesi, l'interoperabilità giuridica definisce l'assetto di norme, policy e accordi necessari per garantire il flusso costante e il riuso dei dati tra soggetti e giurisdizioni differenti⁶⁵. Tale sinergia tra dataset eterogenei è possibile solo se vengono soddisfatti tre criteri fondamentali⁶⁶: la chiara determinabilità automatizzata delle condizioni d'uso, la facoltà di creare opere derivate e la possibilità di accedere ai dati senza autorizzazioni ad hoc per ogni singolo fornitore. Laddove sussistano vincoli normativi (es. privacy, proprietà intellettuale o sicurezza nazionale), l'accessibilità deve comunque essere garantita tramite l'adozione dei principi FAIR (Findable, Accessible, Interope-

⁶⁴ Per maggiori approfondimenti si v. R.H. WEBER, *Legal interoperability*, cit., 7-9.

⁶⁵ Essa riguarda, quindi, situazioni in cui misure normative o politiche limitano la divulgazione dei dati o in cui i set di dati possono essere resi disponibili solo in determinate giurisdizioni o a determinate condizioni. Tra gli esempi figurano restrizioni legali basate sulla proprietà intellettuale, sulla sicurezza nazionale, sulle normative sulla protezione dei dati personali, ecc.

⁶⁶ C. DOLDIRINA, A.R. EISENSTADT, H. ONSRUD, P.F. UHLIR, *Legal Approaches for Open Access to Research Data*, 2018, in Rete: <https://doi.org/10.31228/osf.io/n7gfa>.

nable, Reusable)⁶⁷, assicurando che i metadati permettano l'individuazione e la comprensione dei termini d'uso. In quest'ottica, l'interoperabilità si configura come uno strumento analitico per decodificare le logiche strutturali dei diversi formanti dell'ordinamento e le regole tecniche del digitale, evidenziando i principi che ne governano le reciproche relazioni⁶⁸.

L'implementazione di sistemi interoperabili deve essere conforme alle disposizioni previste nei vari interventi normativi che caratterizzano la Strategia europea sui dati ed in particolare sulla protezione dei dati personali. Un approccio che sin dalla progettazione tenga conto di questo interesse garantisce il rispetto dei requisiti previsti a livello normativo oltre che uno sviluppo di architetture tecnologiche caratterizzate da standard aperti.

4. Considerazioni conclusive, ovvero verso una visione ricostruttiva dell'approccio alla gestione dei dati (sanitari)

La sovrabbondanza, per certi aspetti bulimia, normativa del legislatore europeo incide negativamente sull'uso secondario dei dati sanitari elettronici e finisce per rappresentarne l'ostacolo principale⁶⁹. Tale apparato normativo comprende, come già descritto, GDPR, ODD, AI Act, DGA e DA. Si aggiunga che incidono direttamente, nello specifico, anche altre previsioni quali: la c.d. Direttiva e-Privacy⁷⁰, il Regolamento sulle Sperimentazioni Cliniche⁷¹, il Regolamento sui Dispositivi Medici⁷² e la Direttiva sui diritti dei pazienti nell'assistenza sanitaria transfrontaliera⁷³. Un tale sovraccarico di legislazione crea una sorta di effetto “nebbia” che aumenta i costi transattivi e soprattutto rischia, nella confusione relativa alla regola finalmente utilizzabile per i diversi scenari applicativi, di disincentivare fenomeni di con-

⁶⁷ I “FAIR Data Principle”, redatti per la prima volta nel 2014 e pubblicati nel 2016, consistono in una serie di principi guida volti ad aumentare la riusabilità dei dati e degli oggetti digitali (compresi i dati relativi agli algoritmi, strumenti, flussi di lavoro, protocolli, servizi e altri tipi di oggetti digitali e di ricerca). L'acronimo sta per: “Findable”, “Accessible”, “Interoperable”, “Reusable”. Il conio dell'acronimo è legato ad un seminario tenuto presso il Centro Lorentz a Leiden, Paesi Bassi nell'ambito di una comunità di studiosi, bibliotecari, archivisti, editori e finanziatori della ricerca su invito del eScience Center e del Dutch Techcentre for Life Sciences (DTL). La prima pubblicazione si deve a: M. WILKINSON, M. DUMONTIER, I. AALBERSBERG ET AL., *The FAIR Guiding Principles for scientific data management and stewardship*, in *Sci Data* 3, 160018, 2016, in Rete: <https://doi.org/10.1038/sdata.2016.18>.

⁶⁸ Per maggiori approfondimenti sulla teoria dei formanti del Prof. Sacco si v. Cfr. R. SACCO, P. ROSSI, *Introduzione al diritto comparato*, in *Trattato di diritto comparato* (diretto da R. SACCO), Torino, 2024, 55-70.

⁶⁹ Cfr. I SANCHEZ FRIAS, *op. cit.*, par. II-2.

⁷⁰ Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (Direttiva relativa alla vita privata e alle comunicazioni elettroniche).

⁷¹ Regolamento (UE) n. 536/2014 del Parlamento europeo e del Consiglio, del 16 aprile 2014, sulla sperimentazione clinica di medicinali per uso umano.

⁷² Regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio del 5 aprile 2017 sui dispositivi medici.

⁷³ Direttiva 2011/24/UE sull'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera.



divisione dei dati a fronte di rischi (legali ma non solo) di difficile ponderazione. A completamento di questa complessa stratificazione normativa, merita una menzione la proposta relativa al pacchetto “Digital Omnibus” presentata dalle istituzioni UE a fine 2025. Tale iniziativa si pone l’obiettivo di agire come norma di coordinamento orizzontale per risolvere le antinomie tra i diversi atti della Strategia sui dati, intervenendo proprio su quei nodi critici di interoperabilità giuridica e coerenza sistematica che rappresentano, allo stato attuale, il principale ostacolo al libero fluire dei dati sanitari⁷⁴. Nonostante le ambizioni di semplificazione, la proposta non è esente da riserve, in quanto è stato da più parti evidenziato il rischio che un coordinamento eccessivamente orientato all’efficienza economica possa produrre un abbassamento dei livelli di tutela dei diritti fondamentali, generando possibili incertezze nel sistema delle fonti rispetto al primato del GDPR e alimentando una disomogeneità applicativa in sede giurisprudenziale⁷⁵.

Alcune prime traiettorie per provare a parzialmente diradare questa nebbia possono essere tracciate.

Anzitutto, è necessario promuovere standard comuni a livello europeo, i quali sono fondamentali perché favoriscono la creazione di un mercato unico e la libera circolazione di beni e servizi, garantiscono la sicurezza dei cittadini (prodotti alimentari, dispositivi medici, prodotti pericolosi), stimolano la competitività e l’innovazione tecnologica, supportando la transizione digitale attraverso la creazione di quadri comuni e “spazi” per la gestione dei dati. Inoltre, è importante che chiare linee guida e policy sull’interoperabilità siano redatte al fine di favorire l’accesso ed il riuso di dati. La Commissione europea può giocare un ruolo fondamentale nella creazione di standard e policy incoraggiando la loro redazione nell’ambito di istituti e centri specializzati e, soprattutto, promuovendone l’elaborazione attraverso il finanziamento di progetti di ricerca. Occorre, poi, individuare in modo esplicito quali tipi di utilizzi di dati siano vietati al fine di non violare i diritti degli individui: in tal senso si veda l’art. 54 del Reg. EHDS sull’uso vietato dei dati. Questione fondamentale, come già affrontato sopra, è anche quella relativa alla base giuridica per il trattamento di dati personali che de-

⁷⁴ Il pacchetto non è un unico atto, ma si divide in una proposta “orizzontale” sulla semplificazione dei dati e una specifica per l’Intelligenza Artificiale. Ad onor del vero è intervenuto nelle more di pubblicazione di questo saggio. Si vedano: Commissione Europea, Proposta di Regolamento del Parlamento europeo e del Consiglio che modifica i regolamenti (UE) 2016/679, (UE) 2018/1725, (UE) 2023/2854 e le direttive 2002/58/CE e (UE) 2022/2555 per quanto riguarda la semplificazione e il coordinamento delle norme digitali (Omnibus digitale), COM(2025) 835 definitivo, Bruxelles, 19.11.2025 (in Rete: <https://digital-strategy.ec.europa.eu/it/library/digital-omnibus-regulation-proposal>); Commissione Europea, Proposta di Regolamento del Parlamento europeo e del Consiglio che modifica il regolamento (UE) 2024/1689 per quanto riguarda la semplificazione dell’attuazione di regole armonizzate sull’intelligenza artificiale (Omnibus digitale sull’IA), COM(2025) 836 definitivo, Bruxelles, 19.11.2025 (in Rete: <https://digital-strategy.ec.europa.eu/it/library/digital-omnibus-ai-regulation-proposal>).

⁷⁵ Con riferimento alle questioni privacy si veda anche: EDPB-EDPS, *Joint Opinion 2/2026 on the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus)*, adottata il 10 febbraio 2026 (in Rete: https://www.edps.europa.eu/data-protection/our-work/publications/edps-edpb-joint-opinions/2026-02-10-edpb-edps-joint-opinion-digital-omnibus_en).

ve essere uniforme tra i vari Stati membri: le regole nazionali dovranno, quindi, essere adattate come è avvenuto in passato quando è divenuto applicativo il GDPR e ciò richiederà sicuramente del tempo. Infine, soluzioni giuridiche volte a favorire il riuso vanno sicuramente proposte e “sperimentate”: l’altruismo dei dati di cui al DGA ed il meccanismo di opt-out sull’uso secondario di dati nell’ambito dell’EHDS rappresentano interessanti proposte che devono trovare opportuna adozione a livello di regole applicative, evitando, però, il rischio di frammentazione che la delega agli Stati membri permette. Ciò anche al fine di scongiurare la possibilità che si producano fenomeni di c.d. “forum shopping” avendo, all’interno del contesto unionale, ordinamenti nell’ambito dei quali risulti più agevole condividere dati che in altri.

L’obiettivo normativo dell’interoperabilità giuridica consiste non solo nel contrastare la frammentazione tra ordinamenti causata dalla pluralità di sistemi giuridici nazionali, ma nel renderne effettiva l’integrazione. Tuttavia, le norme nazionali sono una conseguenza del principio di sovranità e, pertanto, sono legittime nella misura appunto dell’ambito della sovranità statale⁷⁶. Alla luce della crescente frammentazione del contesto giuridico nel cyberspazio, è necessario impegnarsi per raggiungere livelli più elevati di interoperabilità giuridica e politica al fine di facilitare la comunicazione globale, ridurre i costi delle attività commerciali transfrontaliere e promuovere l’innovazione e la crescita economica. Le norme giuridiche interoperabili possono anche creare condizioni di parità per la prossima generazione di tecnologie e scambi culturali⁷⁷.

L’analisi svolta in questo contributo, tesa a ricostruire una sistematicità all’intervento del legislatore europeo in materia di condivisione di dati (specie nel peculiare contesto sanitario), offre l’occasione di sviluppare alcune considerazioni finali di carattere comparatistico⁷⁸. Il comparatista, appunto, è alla ricerca di modelli, delle regole che ne governano la circolazione, di differenze e similitudini. Scenari applicativi come quello qui oggetto di studio si prestano a continui riferimenti ad ordinamenti giuridici diversi, in special modo con riguardo ad ambiti che presentano elementi di novità e per i quali non sono ancora state raggiunte soluzioni consolidate. Appare evidente la necessità di coordinamento tra le diverse soluzioni prospettate rispetto a fenomeni che trascendono i confini nazionali. Anzi, è possibile affermare che la polarizzazione espressa da una narrativa che esalta ed enfatizza l’intervento regolatorio unionale (livello declamatorio) determina a livello di regole operative una costellazione di tanti diversi regimi giuridici che insistono sullo stesso bene (i dati) e che vorrebbero realizzare gli stessi obiettivi (la condivisione). Infine, merita attenzione l’analisi del come e del perché questi fenomeni (giuridici) si sviluppino ed evolvono. Il diritto non è

⁷⁶ Cfr. R.H. WEBER, *Realizing a New Global Cyberspace Framework – Normative Foundations and Guiding Principles*, Zurigo, Schulthess and Springer, 2014.

⁷⁷ Cfr. R.H. WEBER, *op. ult. cit.*, 7-12; U. GASSER, J. PALFREY, *Fostering Innovation and Trade in the Global Information Society: The Different Facets and Roles of Interoperability*, in M. BURRI, T. COTTIER (a cura di), *Trade Governance in the Digital Age*, Cambridge, Cambridge University Press, 2012, 123-153.

⁷⁸ Ispira questi passaggi finali quanto si legge in G. SMORTO, *Il ruolo della comparazione giuridica nella contesa per la sovranità digitale*, in *DPCE Online*, 2023, 57(1), 339-369.

statico, bensì profondamente dinamico, muta costantemente. Analizzare il perché di questo mutamento rientra tra gli interessi del giurista comparatista che studia, quindi, le tecniche dell'innovazione giuridica⁷⁹.

Infine, la nozione di interoperabilità giuridica può rappresentare un efficace strumento per facilitare il dialogo e creare “ponti terminologici” tra saperi (anzitutto quello giuridico e tecnico informatico) che si trovano ad operare a stretto contatto al fine di sviluppare ecosistemi volti a favorire il libero fluire di dati⁸⁰. Emerge, infatti, una stretta connessione con il tema dei c.d. “boundary objects” degli studi sui metodi interdisciplinari se si enfatizza la funzione di concetto che funge da punto di incontro e di mediazione tra diverse discipline⁸¹. L'ambiguità intrinseca di cui è connotato il termine (essendo una “categoria” di fatto proveniente dal mondo tecnico che viene “forzata” a divenire principio volto ad una ricostruzione in chiave sistematica del contesto giuridico di riferimento) diventa fondamentale, poiché permette a prospettive diverse di interagire e di “attraversare” i confini disciplinari, abilitando la condivisione di significati senza necessariamente imporre una visione unica.

Per l'Unione europea si presentano all'orizzonte sfide legate a tradizioni e linguaggi (anche giuridici) diversi, così come ad infrastrutture che si sono sviluppate negli anni lungo traiettorie distinte, spesso con disparità significative tra paesi più o meno tecnologicamente avanzati. Nello sviluppo di piattaforme di condivisione dei dati come l'EHDS è essenziale dare priorità al concetto di interoperabilità, consentendo una comunicazione sicura e aperta, linguaggi comuni e norme giuridiche armonizzate. Per far questo, solo un approccio veramente interdisciplinare, volto a valutare la norma giuridica all'interno di un ecosistema determinato da aspetti di carattere tecnico-informatico, può consegnare al giurista un'affidante chiave di lettura al fine di governare fenomeni dinamici ed in costante mutamento.

Alla luce delle considerazioni svolte, è possibile formulare una riflessione conclusiva di carattere sistematico. In questa prospettiva, l'interoperabilità giuridica riveste una duplice funzione: da un lato, opera come principio di coordinamento tra strumenti normativi eterogenei; dall'altro, agisce come dispositivo di traduzione tra linguaggi giuridici e tecnico-informatici. In sua assenza, l'armonizzazione normativa rischia di rimanere confinata a un piano meramente formale, senza tradursi in una reale capacità di circolazione e riutilizzo dei dati. Essa non costituisce, dunque, soltanto uno strumento funzionale al mercato unico dei dati, ma ne rappresenta un presupposto strutturale.

⁷⁹ Cfr. R. SACCO, P. ROSSI, *op. cit.*, 123-139.

⁸⁰ In tema di creatività del giurista e di strategie dell'innovazione si v. G. PASCUIZZI, *La creatività del giurista. Tecniche e strategie dell'innovazione giuridica*, II ed., Bologna, 2018.

⁸¹ Cfr. J.T. KLEIN, *Beyond Interdisciplinarity*, Oxford, Oxford University Press, 2021, 15-25.

