



TEORIA E STORIA DEL DIRITTO PRIVATO

RIVISTA INTERNAZIONALE ONLINE

PEER REVIEWED JOURNAL

ISSN: 2036-2528

CIRO MARIA RUOCCO

***EHDS, Health data beyond borders
e uso secondario dei dati sanitari:
spunti di microcomparazione giuridica***

Numero XIX – Anno 2026

www.teoriaestoriadeldirittoprivato.com

Proprietario e Direttore responsabile

Laura Solidoro

Comitato Scientifico

A. Amendola (Univ. Salerno), E. Autorino (Univ. Salerno), P. Buongiorno (Univ. Macerata), C. Corbo (Univ. Napoli Federico II), J.P. Coriat (Univ. Paris II), J.J. de Los Mozos (Univ. Valladolid), F. Fasolino (Univ. Salerno), L. Garofalo (Univ. Padova), P. Giunti (Univ. Firenze), R. Laurendi (Univ. Genova), L. Loschiavo (Univ. Teramo), A. Petrucci (Univ. Pisa), P. Pichonnaz (Univ. Fribourg), J.M. Rainer (Univ. Salzburg), S. Randazzo (Univ. LUM Bari), L. Solidoro (Univ. Salerno), J.F. Stagl (Univ. Autònoma de Barcelona), E. Stolfi (Univ. Siena), V. Zambrano (Univ. Salerno)

Comitato Editoriale

A. Bottiglieri (Univ. Salerno), M.V. Bramante (Univ. Telematica Pegaso), A. Guasco (Univ. Telematica Giustino Fortunato), L. Gutiérrez Massón (Univ. Complutense de Madrid), L. Monaco (Univ. Campania L. Vanvitelli), P. Pasquino (Univ. Cassino), M. Scognamiglio (Univ. Salerno), A. Trisciungoglio (Univ. Torino)

Redazione

Coordinatore: C. De Cristofaro (Univ. Salerno) – **Membri:** M. Amabile (Univ. Salerno), G. Balestra (Univ. Salerno), M. Beghini (Univ. Roma Tre), A.M.S. Caldoro (Univ. Roma Tor Vergata), P. Capone (Univ. Napoli Federico II), D. Ceccarelli Morolli (P.I.O. – Univ. G. Marconi), S. Cherti (Univ. Cassino), N. Donadio (Univ. Milano), C. Iovacchini (Univ. Roma 'La Sapienza'), M. Melone (Univ. Roma 'La Sapienza'), A. Natale (Univ. Salerno)

Segreteria di Redazione

C. Cascone, M.S. Papillo

Sede della Redazione della rivista

Prof. Laura Solidoro
Via R. Morghen, 181
80129 Napoli, Italia
Tel. +39 333 4846311

Con il patrocinio di



Ordine degli Avvocati di Salerno



Dipartimento di Scienze Giuridiche
(Scuola di Giurisprudenza)
Università degli Studi di Salerno

Teoria e Storia del Diritto Privato

ISSN: 2036-2528

Aut. Tr. Napoli n. 78 del 03.10.2007

Provider: Aruba S.p.A., Via San Clemente n. 53, Ponte San Pietro (BG), P.I. 01573850616 – C.F. 04552920482

EHDS, *Health data beyond borders* e uso secondario dei dati sanitari: spunti di microcomparazione giuridica

SOMMARIO: 1. Oltre la circolazione informativa: lo Spazio Europeo dei Dati Sanitari tra ambizioni infrastrutturali e nodi di legittimazione – 2. La comparazione come stress test dell’EHDS: Stati Uniti, Giappone e il caso ChatGPT Health – 3. La legittimazione giuridica dell’EHDS tra protezione dei dati e armonizzazione del mercato interno – 4. *Secondary Use of Electronic Health Data*: disciplina procedurale e allocazione del rischio – 5. L’HealthData@EU e la creazione di infrastrutture digitali transfrontaliere – 6. Dal consenso alla procedura: il riuso dei dati sanitari tra interesse pubblico, accountability e nuove tecniche di de-identificazione nel diritto italiano. Interrogativi aperti.

1. Oltre la circolazione informativa: lo Spazio Europeo dei Dati Sanitari tra ambizioni infrastrutturali e nodi di legittimazione

La creazione dello Spazio Europeo dei Dati Sanitari (d’ora in avanti EHDS)¹ si colloca nell’alveo delle iniziative volte a superare

¹ Sul punto, v. Reg. (UE) 2025/327 del Parlamento europeo e del Consiglio, dell’11 febbraio 2025, che istituisce lo Spazio europeo dei dati sanitari (c.d. EHDS) e modifica il Reg. (UE) 2016/679, il Reg. (UE) 2018/1725 e la Dir. 2011/24/UE. Il Regolamento si iscrive nel più ampio disegno di costruzione di un ecosistema digitale europeo fondato su valori di solidarietà informativa e

le persistenti barriere che ostacolano la piena circolazione e l'impiego efficiente delle informazioni cliniche tra gli Stati membri dell'Unione europea².

Pur in presenza di elevati standard assistenziali e di una consolidata cultura della protezione dei dati personali, il settore sanitario europeo soffre di una marcata frammentazione normativa e tecnologica, con ricadute immediate su accessibilità, interoperabilità e fruibilità dei dati³. Ciascuno Stato membro ha

responsabilità condivisa, volto a garantire, nel rispetto della dignità della persona e della tutela dei dati sensibili, una circolazione fiduciaria delle informazioni sanitarie tra gli Stati membri. Si realizza così una nuova architettura del diritto alla salute, nella quale l'accesso, l'interoperabilità e il riuso secondario dei dati sanitari diventano strumenti di promozione dell'autonomia informativa e, al contempo, di progresso scientifico collettivo. Cfr., sulla transizione digitale della sanità, C. PERLINGIERI, *Transizione digitale nella sanità ed ecosistema dei dati sanitari: profili ricostruttivi del fenomeno circolatorio e implicazioni sui dati genetici*, in *Tecnologie e diritto*, 2024, 2, 485 ss.; nonché, sul processo di istituzione dell'EHDS, S. THOBANI, *Verso il regolamento UE sullo spazio europeo dei dati sanitari (European Health Data Space)*, in *Persona e Mercato*, 2024, 4, 1393 ss.; M.S. ESPOSITO, *Tutela dei dati personali e ricerca scientifica in ambito sanitario: il GDPR e il Regolamento sullo Spazio Europeo dei Dati Sanitari (EHDS)*, in *Jus Civile*, 2024, 6, 932 ss.

² Per un primo spunto efficace sull'istituzione dell'EHDS e sulle finalità a cui ambisce, v. R. CASO, P. GUARDA, *Ricerca e Spazio Europeo dei Dati Sanitari tra regole proprietarie e apertura*, in *Accademia*, 2025, 9, 837 ss.

³ In tale contesto assume rilievo centrale il tema della data quality, intesa non come mera esattezza formale dell'informazione, ma come idoneità complessiva del dato a essere utilizzato in modo affidabile e legittimo per finalità cliniche, di ricerca o di *policy*. In ambito sanitario, la qualità del dato dipende da fattori quali accuratezza, completezza, aggiornamento, standardizzazione semantica e tracciabilità del processo di raccolta e trattamento. La frammentazione normativa e tecnologica incide direttamente su tali dimensioni, compromettendo non solo l'interoperabilità, ma anche la fruibilità effettiva del dato e la sostenibilità del suo riuso, specie in contesti transfrontalieri e data-driven. La data quality si configura, pertanto, come presupposto funzionale e giuridico del secondary use, nonché come elemento rilevante ai fini dell'accountability e della responsabilità nel trattamento dei dati sanitari. Sul

storicamente sviluppato proprie infrastrutture di raccolta e gestione delle informazioni cliniche – spesso costruite su architetture non comunicanti – rendendo complessa la condivisione dei dati tra autorità sanitarie, operatori e cittadini⁴.

Tale disomogeneità non rallenta soltanto la digitalizzazione⁵, ma impedisce la costruzione di un ecosistema davvero patient-centred, nel quale il dato divenga leva di continuità assistenziale e di effettivo empowerment informativo.

In questa prospettiva, l'EHDS si presenta come tentativo di trasformare il dato sanitario da 'documento' della relazione di cura a risorsa infrastrutturale, governata da standard e procedure comuni⁶.

concetto giuridico di data quality, seppur analizzato in prospettiva differente, si v., V. ZENO-ZENCOVICH, *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, in *Media Laws - Rivista di diritto dei media*, 2018, 2, 32 ss.

⁴ La Commissione Europea ha evidenziato come i sistemi nazionali di gestione dei dati sanitari si siano sviluppati in modo frammentato, sulla base di architetture tecniche e standard non omogenei, con effetti negativi sulla portabilità dei dati e sulla continuità delle cure. Cfr. COMMISSIONE EUROPEA, *Impact Assessment accompanying the Proposal for a Regulation on the European Health Data Space*, SWD, 2022, 131 final; OECD, *Health Data Governance for the Digital Age*, Paris, 2015.

⁵ In relazione al concetto di 'digitalizzazione sanitaria', *ex multis*, C. SARTORIS, *Sanità digitale e tutela dei dati personali*, in *Protezione dei dati personali e nuove tecnologie. Ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze giuridiche*, a cura di A. Adinolfi e A. Simoncini, Napoli, 2022, 347 ss.; R. MICCÙ, M. FERRARA, C. INGENITO, *La digitalizzazione dei servizi sanitari, il diritto alla salute e la tutela dei dati personali*, a cura di R. Miccù, M. Ferrara e C. Ingenito, numero monografico di *Federalismi*, 2021, 5, in www.federalismi.it, 12 febbraio 2021.

⁶ Sugli obiettivi e sulla natura dello Spazio Europeo dei Dati Sanitari, non possono non menzionarsi le riflessioni di S. CORSO, *Lo spazio europeo dei dati sanitari. Prime riflessioni sul regolamento UE 2025/327*, in *Nuove Leggi civ. comm.*, 2025, 3, 563 ss.; L. SOTTILE, *Lo Spazio europeo dei dati sanitari come 'strumento' di rimozione delle disuguaglianze. Prime riflessioni sul Regolamento (UE) 2025/327*, in *Corti Supreme e Salute*, 2025, 3, 1068 ss.

Tra le finalità che hanno indotto la Commissione europea a proporre l'istituzione dell'EHDS, si annovera l'esigenza di garantire ai cittadini un accesso pieno e sicuro ai propri dati sanitari, in un'ottica transfrontaliera e uniforme⁷. La persistente disparità dei quadri nazionali rende spesso complesso il trasferimento delle informazioni⁸, generando inefficienze note: duplicazione di esami, rallentamenti nei percorsi terapeutici, discontinuità nella presa in carico e, in ultima analisi, una potenziale compromissione della qualità delle cure. L'EHDS mira a realizzare un'infrastruttura capace di assicurare un accesso standardizzato e protetto alle informazioni cliniche, conferendo ai cittadini il potere di disporre e condividere i propri dati con i professionisti della salute a prescindere dal territorio in cui si trovino⁹. Il nodo critico, tuttavia, non è soltanto l'accesso 'in sé', ma la proceduralizzazione dell'accesso: chi abilita, a quali condizioni, con quali controlli e con quali rimedi in caso di disfunzioni.

⁷ Sulla centralità dell'*European Health Data Space* quale strumento volto non solo a migliorare l'efficienza delle cure sanitarie, ma anche a valorizzare i dati a fini di ricerca e di policy, v. T. SOKOL, *European Health Data Space, Use of Data and Data Subjects' Control over Their Own Health Data: Can an Opt-Out Restore the Balance?*, in *European Journal of Health Law*, 2024, 31, 365 ss. L'analisi sottolinea come il punto nevralgico dell'EHDS sia proprio nel bilanciamento tra la disponibilità di dati funzionali al perseguimento di obiettivi pubblici e la garanzia, per i pazienti, di un effettivo controllo sui propri dati sanitari. In quest'ottica, un ruolo cruciale è attribuito all'istituto dell'opt-out armonizzato per gli usi secondari, visto quale condizione imprescindibile per realizzare un equilibrio equo e sostenibile.

⁸ Con riferimento alla circolazione dei dati sanitari, in ottica utilitaristica e di mercato, si v. V. RICCIUTO, *Una circolazione dei dati sanitari anche nella prospettiva del mercato?*, in *Accademia*, 2025, 9, 823 ss.

⁹ Precipuamente, con riferimento agli assetti organizzativi derivati dall'istituzione dello Spazio Europeo dei Dati Sanitari, una corposa e variegata analisi è da ricondurre al pensiero di A. MORACE PINELLI, *Riflessioni introduttive sul Regolamento c.d. EHDS*, in *Sanità digitale. Regolamento 'EHDS' (UE 2025/327) sullo spazio europeo dei dati sanitari. Uso dei dati e assetti organizzativi*, a cura di A. Morace Pinelli, Pisa, 2025, 1, XVII ss.

Di pari rilevanza è l'impatto dell'iniziativa sul versante della ricerca scientifica e dell'innovazione tecnologica. Le odierne limitazioni tecniche e giuridiche ostacolano l'accesso dei ricercatori a dati sanitari di qualità, riducendo il potenziale euristico degli studi clinici e della sperimentazione medica.

L'emergenza pandemica ha reso manifesto quanto il possesso tempestivo di dati aggregati e attendibili sia determinante per monitorare la diffusione delle malattie e predisporre risposte sanitarie efficaci¹⁰. L'EHDS intende colmare tali carenze predisponendo un quadro normativo e tecnologico omogeneo che consenta l'utilizzo di dati anonimizzati o pseudonimizzati a supporto della ricerca biomedica, della prevenzione e dell'innovazione terapeutica. Qui emerge una prima frizione sistemica: l'apertura del dato per finalità collettive richiede garanzie

¹⁰ L'esperienza emergenziale determinata dalla pandemia da SARS-CoV-2 ha rappresentato un punto di svolta paradigmatico nell'impiego dei dati personali, evidenziando in modo inequivoco come la loro elaborazione – anche in ambito sanitario – possa generare un patrimonio informativo di straordinaria rilevanza per la tutela della salute pubblica. Proprio in tale contesto si è rivelato il potenziale applicativo degli algoritmi predittivi e dei sistemi di analisi automatizzata, capaci di trasformare la disponibilità massiva di dati in strumenti decisionali e di intervento tempestivo. Da quel momento in avanti, il ricorso ai dati sanitari ha conosciuto una significativa espansione, divenendo elemento centrale nelle strategie di governance digitale della sanità, nonché leva strutturale per politiche di prevenzione, programmazione e gestione dell'emergenza. Si v., C. PERLINGIERI, *Coronavirus e tracciamento tecnologico: alcune riflessioni sull'applicazione e sui relativi sistemi di interoperabilità dei dispositivi*, in *Actual jur. iberoam.*, 2020, 12-bis, 836 ss.; M. D'AMBROSIO, *Tracciamento tecnologico del contagio*, in *Actual jur. iberoam.*, 2020, 12-bis, 868 ss.; G. RESTA, *La protezione dei dati personali nel diritto dell'emergenza Covid-19*, in *Giust. civ. online*, 5 maggio 2020; V. CUFFARO, R. D'ORAZIO, *La protezione dei dati personali ai tempi dell'epidemia*, in *Corr. giur.*, 2020, 6, 729 ss. N. MINISCALCO, *La sorveglianza attiva per contrastare la diffusione dell'epidemia da Covid-19: strumento di controllo e di garanzia per i cittadini?*, in *Osservatorio costituzionale AIC*, 2020, 3, *passim*.

che non si esauriscano nella liceità del trattamento, ma che incidano su tracciabilità, controlli e responsabilità lungo l'intera filiera¹¹.

Dal punto di vista degli operatori sanitari, l'attuale frammentazione informativa costituisce un limite significativo alla continuità assistenziale. Spesso, infatti, i professionisti non dispongono di accesso immediato a dati clinici aggiornati¹², soprattutto in caso di pazienti in mobilità tra differenti strutture o Paesi. L'EHDS mira a rimuovere tali ostacoli, garantendo accesso tempestivo e sicuro alle informazioni necessarie, migliorando la qualità delle decisioni cliniche, riducendo la ripetizione di accertamenti diagnostici e favorendo un approccio personalizzato e tempestivo. Anche in questo ambito, la promessa

¹¹ In dottrina è stato efficacemente osservato come l'analisi e il riutilizzo dei dati su larga scala non si esauriscano in una mera operazione di accumulo informativo, ma presuppongano un articolato assetto organizzativo e decisionale che incide direttamente sulle modalità di trattamento e sulle forme di tutela della persona. In tal senso, A.C. NAZZARO, *L'utilizzo dei Big data e i problemi di tutela della persona*, in *Rass. dir. civ.*, 2018, 1242, evidenzia come i sistemi di Big Data analytics celino una complessa infrastruttura di gestione dei dati, dalla quale discendono criticità ulteriori rispetto alla tradizionale protezione fondata sul consenso. Su un piano analogo, G. COMANDÉ, *Ricerca in sanità e data protection: un puzzle [...] risolvibile*, in *Riv. it. med. leg.*, 2019, 1, 189 ss., sottolinea la distanza strutturale tra i modelli di ricerca basati sui *Big Data* e quelli convenzionali, osservando come ciò metta in discussione l'impostazione tradizionale che, in ambito medico, individuava nell'alternativa tra consenso specifico e anonimizzazione l'unico schema di legittimazione del trattamento.

¹² Sul punto, nuovamente, cfr. con Reg. (UE) 2025/327 del Parlamento europeo e del Consiglio che istituisce lo Spazio europeo dei dati sanitari (EHDS), e specialmente con l'art. 10. L'articolo disciplina le modalità di accesso dei professionisti della salute ai dati sanitari elettronici, specificando che tale accesso è consentito solo nella misura necessaria alla prestazione delle cure e subordinato al rispetto delle preferenze dell'interessato (art. 8 EHDS) e delle normative nazionali in materia di segreto professionale e riservatezza. In tal senso, la temporanea 'inibizione' all'accesso ai dati da parte di taluni operatori trova giustificazione nel bilanciamento tra il diritto alla protezione dei dati personali e l'interesse pubblico alla continuità assistenziale.

dell'interoperabilità si misura con un problema di fiducia: la disponibilità del dato diventa utile solo se accompagnata da qualità, standard semantici condivisi e accountability¹³.

Di non minore importanza è il profilo relativo alla sicurezza informatica. Il settore sanitario è tra i più esposti ad attacchi informatici, con conseguenze potenzialmente gravi sulla riservatezza dei dati e sulla continuità operativa delle strutture. L'incremento degli scambi, soprattutto in chiave transfrontaliera, amplia fisiologicamente la superficie di rischio e impone un innalzamento dei presidi. In tale quadro, il Regolamento sull'EHDS prevede misure di sicurezza rafforzate, imponendo agli Stati membri¹⁴ l'implementazione di protocolli avanzati – quali crittografia, pseudonimizzazione e autenticazione forte – idonei a garantire integrità, riservatezza e disponibilità delle informazioni cliniche. In prospettiva, la sicurezza non è più mero requisito tecnico, ma elemento strutturale di legittimazione del sistema: senza un presidio cyber credibile, la circolazione dei dati rischia di diventare fattore di vulnerabilità anziché di efficienza.

¹³ Con precipuo riferimento alla protezione del dato sanitario, si v. M.A. SANDULLI, *Introduzione*, in *La protezione dei dati sanitari. Privacy e innovazione tecnologica tra salute pubblica e riservatezza*, a cura di A. Thiene e S. Corso, Napoli, 2023, 1 ss.

¹⁴ Sul piano dell'architettura istituzionale, un precedente rilevante è rappresentato dalla Recommendation on a European Electronic Health Record exchange format, adottata dalla Commissione europea il 6 febbraio 2019, che anticipa alcune delle direttrici poi recepite nel regolamento EHDS. La Raccomandazione si colloca nell'ambito dell'iniziativa eHealth Digital Service Infrastructure (eHDSI), promossa nell'ambito del programma Connecting Europe Facility, quale strumento di supporto tecnico e finanziario volto a favorire l'interoperabilità transfrontaliera dei sistemi sanitari digitali. L'obiettivo dichiarato è quello di definire un formato comune europeo per lo scambio dei dati sanitari elettronici, quale prerequisito tecnico per l'attuazione di standard di sicurezza e protezione dei dati allineati ai più elevati livelli di tutela richiesti dalla normativa europea in materia di salute e privacy.

Sotto il profilo economico, la mancata interoperabilità tra i sistemi sanitari nazionali determina inefficienze e aggravii di costi, ostacolando lo sviluppo di un mercato unico europeo delle soluzioni digitali in sanità. L'armonizzazione promossa dall'EHDS mira ad abbattere tali barriere, stimolando la crescita di un ecosistema innovativo capace di attrarre investimenti e sostenere la diffusione di tecnologie emergenti – tra cui intelligenza artificiale e big data analytics – con benefici sia per operatori consolidati sia per start-up. In questa dimensione, tuttavia, l'iniziativa europea sollecita anche una domanda di policy giuridica: quale equilibrio tra incentivo all'innovazione e tutela di diritti fondamentali, specie quando il dato sanitario viene trattato come fattore produttivo e input per prodotti e servizi digitali?

Dal punto di vista politico-istituzionale, l'EHDS si iscrive nel più ampio disegno della Strategia europea per i dati, finalizzato a consolidare l'autonomia strategica dell'Unione in settori chiave, tra cui la salute. L'istituzione di uno spazio comune per i dati sanitari presuppone cooperazione rafforzata tra Stati membri, istituzioni europee e operatori privati, con l'obiettivo di definire standard comuni e garantire una tutela effettiva dei diritti fondamentali dei cittadini.

Ne discende un assetto istituzionale multilivello che, per funzionare, deve essere non solo formalmente armonizzato, ma anche operativamente coerente: regole comuni, capacità amministrative comparabili, infrastrutture compatibili, e un sistema di controlli e rimedi capace di mantenere la fiducia degli interessati.

In definitiva, l'EHDS nasce dall'urgenza di superare le inefficienze strutturali dei sistemi nazionali, valorizzando le potenzialità della digitalizzazione per migliorare l'accesso alle cure, promuovere la ricerca scientifica, potenziare la sicurezza delle informazioni e favorire la creazione di un mercato integrato delle

soluzioni sanitarie digitali¹⁵. Il Regolamento che istituisce lo Spazio Europeo dei Dati Sanitari si configura, dunque, come tassello decisivo nella costruzione di un sistema sanitario europeo più efficiente, equo e resiliente. Proprio per questo, l'analisi non può arrestarsi alla ricostruzione delle finalità, ma deve interrogare i nodi critici di governance: procedure, controlli, responsabilità e strumenti di legittimazione dell'accesso e del riuso.

2. La comparazione come stress test dell'EHDS: Stati Uniti, Giappone e il caso ChatGPT Health

Una prospettiva comparata consente di cogliere ancor meglio la portata sistemica dell'iniziativa europea. Negli Stati Uniti, l'Health Information Technology for Economic and Clinical Health Act (c.d. HITECH Act) del 2009 ha rappresentato il principale strumento federale per promuovere la digitalizzazione dell'assistenza sanitaria, incentivando l'adozione diffusa degli Electronic Health Records¹⁶, e favorendo la circolazione elettronica delle informazioni cliniche tra gli attori del sistema.

¹⁵ Tematiche alternativamente trattate, *ex multis*, da N. POSTERARO, *La digitalizzazione della sanità in Italia: uno sguardo al fascicolo sanitario elettronico (anche alla luce del Piano nazionale di ripresa e resilienza)*, in *Federalismi it. Osservatorio di diritto sanitario*, 2021, 24, 189 ss.

¹⁶ Prima dell'intervento del legislatore federale, l'adozione dei sistemi di Electronic Health Records negli Stati Uniti era estremamente limitata: solo una minima parte delle strutture ospedaliere – circa un decimo – disponeva di un'infrastruttura digitale capace di sostituire la documentazione cartacea. Tale arretratezza non derivava da una mancanza di interesse da parte degli operatori sanitari, quanto piuttosto dai costi elevati necessari per l'implementazione delle piattaforme informatiche e dalle incertezze legate alla sicurezza dei flussi informativi. Con il varo dell'Health Information Technology for Economic and Clinical Health Act nel 2009, il quadro mutò in maniera radicale. La riforma predispose un sistema di incentivi economici volto a sostenere ospedali e clinici nella transizione verso l'EHR e a promuovere modelli di gestione digitale

L'intervento normativo rispondeva a una duplice finalità: da un lato, migliorare la qualità, la sicurezza e l'efficienza delle cure mediante una più ampia disponibilità e condivisibilità dei dati sanitari; dall'altro, sostenere lo sviluppo di un'infrastruttura informativa idonea a rendere il settore sanitario più trasparente, competitivo e orientato all'innovazione tecnologica. Tuttavia, l'assenza di un'infrastruttura federale unificata ha prodotto un ecosistema fortemente frammentato, caratterizzato da una limitata interoperabilità e da un crescente coinvolgimento di intermediari privati nella gestione delle informazioni cliniche. Inoltre, il modello statunitense attribuisce ampio spazio all'utilizzo dei dati sanitari anche per finalità economiche e commerciali, nei limiti delle discipline settoriali – *in primis* l'HIPAA – configurando un approccio sensibilmente diverso dalla centralità, tipicamente europea, del controllo dell'interessato e dall'ancoraggio del trattamento a finalità solidaristiche e di interesse pubblico¹⁷. Il

dell'assistenza fondati su interoperabilità, continuità delle cure e condivisione efficiente delle informazioni tra i soggetti qualificati ai sensi dell'HIPAA. L'adozione degli EHR divenne così una condizione essenziale per migliorare la qualità dei servizi, ridurre errori clinici e favorire un coordinamento più efficace tra gli attori della filiera sanitaria. Il HITECH Act ebbe anche un impatto significativo sul piano regolatorio: pur non modificando gli obblighi di conformità all'HIPAA, già vigenti, ne rafforzò l'attuazione, imponendo alle covered entities e ai business associates nuovi adempimenti in materia di sicurezza informatica e introducendo per la prima volta un obbligo federale di notifica delle violazioni dei dati sanitari. Tale previsione consentì all'Office for Civil Rights di intensificare l'attività di enforcement, aumentando la trasparenza del sistema e la responsabilizzazione degli operatori nella protezione delle informazioni cliniche digitali.

¹⁷ Il tema della possibile remunerazione connessa alla condivisione e allo sfruttamento dei dati personali – e, in particolare, dei dati sanitari – costituisce oggetto di un ampio e articolato dibattito dottrinale, che travalica il solo contesto statunitense. In tale prospettiva, anche nell'ordinamento europeo si discute criticamente della riconducibilità del dato a schemi negoziali e patrimoniali, nonché dei limiti strutturali di modelli fondati sulla mercificazione

confronto evidenzia come l'interoperabilità, se affidata prevalentemente a dinamiche di mercato, rischi di tradursi in fenomeni di data brokerage e in asimmetrie di potere informativo tra operatori e cittadini¹⁸.

In questa traiettoria si collocano anche sviluppi più recenti riconducibili all'impiego di sistemi di intelligenza artificiale generativa rivolti direttamente agli utenti finali. Soluzioni come ChatGPT Health, che consentono all'utente di interagire con informazioni di salute anche mediante l'integrazione di dati provenienti da cartelle cliniche o da applicazioni di benessere¹⁹,

dell'informazione personale. Sul punto, si v. V. D'ANTONIO, *Autodeterminazione informativa e dinamiche remuneratorie: i limiti dello schema negoziale*, in I «poteri privati» delle piattaforme e le nuove frontiere della privacy, a cura di P. Stanzone, Torino, 2022, 151 ss.

¹⁸ In relazione alle asimmetrie del potere informazionale, con precipuo riguardo al ruolo centrale della sorveglianza algoritmica in altri assetti giuridici e, segnatamente, quello cinese, si v. X. LIN, *A Dangerous Game: China's Big Data Advantage and How the U.S. Should Respond*, in *University of Illinois Journal of Law, Technology & Policy*, 2020, 253 ss.

¹⁹ Sullo sviluppo e sulla crescente diffusione delle applicazioni digitali per il benessere e delle app mediche, nonché sulle criticità che esse pongono in termini di protezione dei dati sanitari e qualificazione giuridica delle informazioni trattate, si v. I. RAPISARDA, *La privacy sanitaria alla prova del mobile ecosystem. Il caso delle app mediche*, in *Nuove leggi civ. comm.*, 2023, 1, 184 ss. Con specifico riferimento alla condivisione dei dati generati da dispositivi medici portatili o connessi, si v. F. GENNARI, F. CASAROSA, *La condivisione dei dati nei dispositivi medici connessi (IoMT): tra il Data Act e lo Spazio europeo dei dati sanitari*, in *BioLaw Journal - Rivista di BioDiritto*, 2025, 1, 667 ss., le quali evidenziano come i sistemi sanitari nazionali ricorrano in misura crescente alle tecnologie dell'Internet of Medical Things, attraverso dispositivi dotati di sensori e connessi in rete, capaci di raccogliere dati sanitari estremamente accurati anche al di fuori dei contesti clinici tradizionali. Sulle c.d. mHealth app per dispositivi smartphone, in particolare per la televisita e il telemonitoraggio, v. inoltre G. BINCOLETTI, *mHealth app per la televisita e il telemonitoraggio. Le nuove frontiere della telemedicina tra disciplina sui dispositivi medici e protezione dei dati personali*, in *BioLaw Journal - Rivista di BioDiritto*, 2021, 4, 383 ss.

mostrano come il trattamento dei dati sanitari possa avvenire al di fuori di infrastrutture pubbliche formalizzate e di procedure di accesso tipizzate dal diritto. Tali strumenti trovano un impiego crescente non solo per finalità informative generali, ma anche quale supporto preliminare all'orientamento sanitario e alla comprensione di condizioni cliniche, contribuendo a ridurre le barriere geografiche e temporali nell'accesso alle informazioni sanitarie. In tale prospettiva, essi possono attenuare le disuguaglianze nell'accesso alle informazioni di salute, offrendo un canale informativo immediato anche a soggetti residenti in aree geografiche remote o caratterizzate da una limitata presenza di infrastrutture sanitarie, come avviene in contesti territoriali estesi e scarsamente urbanizzati.

Al contempo, tuttavia, il loro funzionamento si fonda su architetture tecniche e modelli di governance dei dati non riconducibili alle categorie tradizionali del diritto sanitario europeo. Pur accompagnati da dichiarazioni di tutela della privacy e da limitazioni nell'utilizzo dei dati per finalità di addestramento, tali sistemi si collocano in un'area di significativa incertezza regolatoria nel contesto europeo, non essendo riconducibili né ai tradizionali fornitori di servizi sanitari né a spazi di dati disciplinati come l'EHDS. La loro operatività risulta pertanto esposta a valutazioni autoritative caso per caso da parte delle Autorità di protezione dei dati personali, come dimostrato dai recenti interventi e dalle iniziative istruttorie adottati in alcuni Stati membri²⁰.

²⁰ Particolarmente significativo è il noto provvedimento adottato dal Garante per la Protezione dei Dati Personali in data 30 marzo 2023 (doc. web n. 9870832), con cui l'Autorità, ai sensi dell'art. 58, par. 2, lett. f), del Reg. (UE) 2016/679, ha disposto la limitazione provvisoria del trattamento dei dati personali degli interessati stabiliti nel territorio italiano effettuato da OpenAI. A seguito delle misure prospettate dal fornitore, l'Autorità ha comunicato la sospensione della limitazione provvisoria in data 28 aprile 2023 (doc. web n. 9874751). In Spagna, l'Agencia Española de Protección de Datos (c.d. AEPD)

In questa prospettiva, ChatGPT Health assume rilievo non tanto come modello alternativo di sanità digitale, quanto come contro-esempio regolatorio, idoneo a evidenziare i limiti di un accesso ai dati sanitari fondato su architetture private, condizioni contrattuali e policy aziendali, prive di una procedura pubblica di legittimazione, di ambienti sicuri certificati e di una chiara allocazione delle responsabilità lungo la filiera del trattamento²¹.

Un quadro distinto, ma ugualmente istruttivo, proviene dal Giappone, dove l'invecchiamento della popolazione ha accelerato la transizione verso forme avanzate di sanità digitale, facendo leva su tecnologie di intelligenza artificiale e big data per il monitoraggio delle patologie croniche²² e l'assistenza domiciliare²³. La disciplina

ha avviato d'ufficio, il 13 aprile 2023, actuaciones previas de investigación nei confronti di OpenAI, evidenziando l'esigenza di un coordinamento europeo in ragione del possibile impatto su larga scala dei trattamenti. In Francia, la Commission nationale de l'informatique et des libertés (c.d. CNIL) ha reso noto, nel proprio piano d'azione sull'intelligenza artificiale, di aver ricevuto plurime denunce relative a OpenAI/ChatGPT e di aver aperto una procédure de contrôle. In Germania, la valutazione del servizio è stata oggetto di iniziative coordinate tra autorità di controllo, come attestato, da un lato, da comunicazioni ufficiali di autorità regionali (es. LDI Nordrhein-Westfalen) circa la prosecuzione della verifica e l'invio di ulteriori quesiti a *OpenAI* e, dall'altro, da atti della Datenschutzkonferenz (DSK) relativi allo stato della 'Prüfung von ChatGPT'. Sul piano sovranazionale, il Comitato Europeo per la Protezione dei Dati (EDPB) ha deliberato il 13 aprile 2023 l'istituzione di una task force dedicata a ChatGPT per favorire cooperazione e scambio informativo su possibili azioni di enforcement, e ha successivamente pubblicato un report sul lavoro svolto dalla task force.

²¹ Così, sul trattamento degli health data, S. CORSO, *Il trattamento dei dati personali in ambito sanitario*, in *Rivista italiana di informatica e diritto* (RIID), 2025, 2, 2 ss.

²² Con esplicito riferimento ai *big data*, v. A. CINQUE, *Privacy, big-data e 'contact tracing': il delicato equilibrio fra diritto alla riservatezza ed esigenze di tutela della salute*, in *Nuova giur. civ. comm.*, 2021, 957 ss.

²³ In tale contesto, un ruolo centrale è assunto dalla telemedicina, intesa, com'è noto, come insieme di pratiche sanitarie a distanza che consentono il monitoraggio continuativo delle condizioni di salute del paziente e l'erogazione

introdotta con l'Act on the Protection of Personal Information (APPI) e con i '2020 Amendments'²⁴ riflette un modello in parte analogo al GDPR, basato su una protezione rafforzata dei dati sensibili, tra cui quelli sanitari. Tuttavia, persiste una significativa frammentazione infrastrutturale e una marcata cautela verso la centralizzazione dei flussi informativi, anche in ragione di diffuse preoccupazioni legate alla sicurezza e alla vulnerabilità cibernetica.

di prestazioni assistenziali in ambito domiciliare, mediante l'impiego di strumenti digitali e sistemi di raccolta e analisi dei dati sanitari. Sul punto, v. G. BINCOLETTI, *L'uso secondario di dati sanitari per fini di ricerca nella telemedicina. La tutela dei dati personali tra regole e prassi*, in *Ricerca in sanità e protezione dei dati personali: scenari applicativi e prospettive future. Atti del Convegno di Trento, 29 settembre 2023*, a cura di E. Chizzola, P. Guarda, V. Maroni e L. Rufo, 2024, 83, 105 ss., ove si evidenzia come i modelli di assistenza sanitaria a distanza pongano questioni specifiche in tema di trattamento e riuso dei dati sanitari.

²⁴ In Giappone, i '2020 Amendments' alla Act on the Protection of Personal Information hanno segnato un significativo aggiornamento del quadro giapponese in materia di protezione dei dati personali. Le modifiche hanno, da un lato, rafforzato in modo sensibile le prerogative degli interessati – già oggetto di un primo intervento riformatore nel 2017 – e, dall'altro, esteso l'ambito di applicazione extraterritoriale della normativa, superando le precedenti limitazioni e avvicinando l'ordinamento nipponico ai modelli europei di tutela. Gli emendamenti hanno inoltre introdotto obblighi più stringenti in materia di trasferimenti internazionali, imponendo ai titolari una maggiore trasparenza sulle condizioni di trattamento all'estero e una più accurata informazione agli interessati. Una delle innovazioni di maggior rilievo riguarda la disciplina delle nuove categorie di dati personali elaborate tramite tecniche di pseudonimizzazione, cui si affianca – per la prima volta nel diritto giapponese – una definizione normativa di 'data breach', comprensiva degli obblighi di notifica e gestione della violazione. L'attuazione e il controllo del nuovo impianto regolatorio sono stati affidati alla Personal Information Protection Commission (c.d. PPC), cui competono l'emanazione di linee guida interpretative e l'esercizio dei poteri ispettivi e sanzionatori, secondo un modello che presenta significative affinità con le autorità di protezione dati europee e con le recenti normative di adeguamento adottate, tra gli altri, anche dall'Italia.

Entrambi gli ordinamenti mostrano come, in assenza di standard condivisi e di un sistema interoperabile sostenuto da procedure pubbliche di accesso e controllo, l'efficiente riuso dei dati sanitari e la piena integrazione delle tecnologie digitali nei percorsi di cura restino strutturalmente limitati.

In questo scenario eterogeneo, l'EHDS emerge come uno dei tentativi più avanzati di dotare la sanità digitale di una cornice unitaria, capace di rispondere in modo sistemico alle esigenze di interoperabilità, sicurezza e tutela dei diritti fondamentali.

Entrambi gli ordinamenti mostrano come, in assenza di standard condivisi e di un sistema interoperabile sostenuto da procedure pubbliche di accesso e controllo, l'efficiente riuso dei dati sanitari e la piena integrazione delle tecnologie digitali nei percorsi di cura restino strutturalmente limitati.

Le differenze tra i modelli esaminati emergono con particolare evidenza anche sul terreno della responsabilità derivante dal trattamento dei dati sanitari. Nei sistemi fondati su una protezione settoriale e frammentata del dato personale, come quello statunitense, la distribuzione delle responsabilità tende a seguire logiche prevalentemente contrattuali, regolatorie e di mercato, con un ruolo centrale attribuito ai soggetti privati che gestiscono le infrastrutture informative e ai meccanismi di compliance previsti dalla disciplina di settore. In tale contesto, la responsabilità per l'uso improprio dei dati sanitari si concentra soprattutto sulla violazione degli obblighi di sicurezza, confidenzialità e notifica delle violazioni, mentre resta meno marcata la dimensione pubblicistica della tutela dell'interessato quale titolare di un diritto fondamentale al controllo delle proprie informazioni personali.

Diversamente, il modello europeo – costruito attorno al GDPR e ora rafforzato dall'EHDS – configura la protezione dei dati sanitari come elemento strutturale di legittimazione del trattamento, incidendo direttamente sull'allocazione del rischio e sull'intensità delle responsabilità gravanti sui soggetti coinvolti

nella filiera informativa. La centralità dei principi di accountability, minimizzazione, tracciabilità, sicurezza e limitazione delle finalità comporta che la responsabilità non si esaurisca nella mera gestione tecnica del dato, ma investa l'intero assetto organizzativo del trattamento, imponendo ai data holder, agli organismi di accesso e agli eventuali intermediari obblighi continui di verifica, documentazione e controllo.

Anche l'esperienza giapponese mostra come un modello improntato a maggiore cautela rispetto alla centralizzazione dei flussi informativi produca effetti specifici sul piano della responsabilità.

La persistente frammentazione infrastrutturale e la forte attenzione ai rischi di cybersecurity determinano infatti una tendenza a circoscrivere la condivisione dei dati sanitari entro circuiti maggiormente controllati, con conseguente enfasi sugli obblighi di sicurezza tecnica, prevenzione delle vulnerabilità sistemiche e affidabilità delle infrastrutture.

Proprio sotto questo profilo, l'EHDS si distingue per il tentativo di costruire un sistema nel quale interoperabilità e responsabilità evolvano parallelamente: quanto più aumenta la circolazione transfrontaliera del dato sanitario, tanto più si rafforzano gli obblighi di governance, supervisione e accountability posti a carico dei soggetti che ne rendono possibile l'accesso e il riuso. La comparazione evidenzia così come il diverso modello di protezione dei dati personali non incida soltanto sulle modalità di accesso, circolazione e utilizzo delle informazioni sanitarie, ma anche sulla stessa configurazione delle responsabilità giuridiche derivanti dal trattamento.

In questo scenario eterogeneo, l'EHDS emerge come uno dei tentativi più avanzati di dotare la sanità digitale di una cornice unitaria, capace di rispondere in modo sistemico alle esigenze di interoperabilità, sicurezza, tutela dei diritti fondamentali e coerente allocazione delle responsabilità lungo la filiera del dato sanitario. È

proprio alla luce di questa vocazione armonizzatrice che va ora esaminato il fondamento giuridico del nuovo impianto europeo.

3. La legittimazione giuridica dell'EHDS tra protezione dei dati e armonizzazione del mercato interno

Se la comparazione evidenzia che l'interoperabilità può produrre esiti opposti – dalla mera frammentazione di mercato alla centralizzazione prudente per ragioni di sicurezza – l'EHDS si distingue per l'ambizione di 'proceduralizzare' l'accesso e il riuso entro un modello europeo di garanzie. Ne discende che il punto non è soltanto descrittivo, ma di legittimazione: occorre individuare il fondamento giuridico che consente all'Unione di combinare protezione dei dati e armonizzazione del mercato interno in un settore ad altissima sensibilità.

Dal punto di vista giuridico, l'EHDS trova il proprio fondamento negli articoli 16 e 114 TFUE.

L'art. 16, nel riconoscere a ogni persona il diritto fondamentale alla protezione dei dati personali e nell'attribuire all'Unione la competenza a definire le norme che regolano il trattamento, costituisce la base primaria del sistema europeo di tutela dei dati. È da questo quadro 'costituzionale' che discende il GDPR, il quale specifica requisiti di liceità, correttezza, sicurezza e accountability cui ogni trattamento – compresi quelli relativi ai dati sanitari – deve conformarsi. In un settore ad alta sensibilità, l'art. 16 TFUE opera come criterio di orientamento: l'innovazione regolatoria deve essere compatibile con il nucleo del diritto fondamentale, non soltanto mediante principi astratti, ma attraverso garanzie effettive²⁵.

²⁵ Più precipuamente, come affermato da S. FAILLACE, *Prospettive civilistiche in ordine agli spazi di condivisione dei dati sanitari alla luce del Regolamento EHDS*, Milano,

L'EHDS si innesta in continuità con tale architettura, integrando il GDPR attraverso strumenti normativi e tecnologici finalizzati a rendere possibile, da un lato, la protezione rigorosa delle informazioni cliniche e, dall'altro, il loro impiego per ricerca scientifica, innovazione terapeutica, programmazione sanitaria e valutazione delle tecnologie mediche. La disciplina del nuovo spazio europeo, pur senza derogare ai principi del GDPR, è modellata per affrontare esigenze specifiche del settore health, nel quale il dato sanitario – appartenendo a categorie particolari – richiede misure più stringenti e un bilanciamento particolarmente attento tra riservatezza, utilità pubblica e progresso scientifico. In questa prospettiva, la questione del consenso tende a trasformarsi: non scompare, ma viene 'riarticolata' entro un insieme di garanzie tecniche e procedurali che mirano a rendere sostenibile il riuso su scala europea.

Il Regolamento valorizza altresì il diritto del cittadino ad accedere e a disporre liberamente dei propri dati sanitari, assicurandone portabilità e fruibilità oltre i confini nazionali. Attraverso formati interoperabili e infrastrutture digitali sicure, l'EHDS mira a garantire continuità delle cure e personalizzazione dei percorsi terapeutici, riducendo asimmetrie informative tra operatori, favorendo la mobilità dei pazienti e rendendo più efficiente l'ecosistema sanitario europeo. Il 'diritto all'accesso' assume così una dimensione non solo individuale, ma sistemica: è lo strumento con cui l'Unione tenta di tradurre in operatività la centralità del paziente.

L'art. 114 TFUE riveste, a sua volta, un ruolo cardine nella costruzione dello Spazio Europeo dei Dati Sanitari, consentendo l'adozione di misure volte a eliminare gli ostacoli derivanti dalla

2025, 5, il Regolamento configura «un'architettura condivisa per stabilire regole comuni, procedure, standard tecnologici e infrastrutture».

frammentazione legislativa tra Stati membri²⁶. La creazione di standard tecnici comuni e di regole armonizzate per gestione,

²⁶ L'art. 114 TFUE rappresenta, come noto, la base giuridica di riferimento per l'adozione di misure di armonizzazione funzionali all'istituzione e al corretto funzionamento del mercato interno. La giurisprudenza della Corte di Giustizia dell'Unione europea ha progressivamente valorizzato una lettura ampia di tale disposizione, chiarendo che essa non si limita a legittimare interventi diretti alla rimozione di ostacoli già esistenti alla libera circolazione, ma consente altresì l'adozione di misure volte a prevenire l'emergere di future divergenze normative idonee a compromettere l'unità del mercato interno. In questa direzione si colloca, in particolare, la sentenza *Tobacco Advertising I* (C-376/98), nella quale la Corte ha precisato che il legislatore dell'Unione può fondare i propri interventi sull'art. 114 TFUE qualora le differenze tra le normative nazionali siano tali da incidere negativamente sulle libertà fondamentali o da determinare distorsioni della concorrenza. Al contempo, la Corte ha individuato limiti sostanziali all'esercizio di tale competenza, escludendo che l'armonizzazione possa essere perseguita in modo avulso dall'obiettivo di migliorare le condizioni di funzionamento del mercato interno, o utilizzata esclusivamente per innalzare il livello di tutela di interessi diversi – quali la salute pubblica – in assenza di un nesso diretto con la circolazione transfrontaliera. Tali principi sono stati ulteriormente sviluppati nella successiva pronuncia *Tobacco Advertising II* (C-380/03), con la quale la Corte ha riconosciuto la legittimità di interventi armonizzatori anche a carattere preventivo, finalizzati a scongiurare il rischio di futuri ostacoli derivanti da evoluzioni normative divergenti negli ordinamenti nazionali. Ne emerge una concezione dell'art. 114 TFUE come strumento di armonizzazione dinamica, capace di operare tanto in funzione correttiva quanto anticipatoria. Non è un caso che tale disposizione sia stata frequentemente utilizzata quale base giuridica per l'adozione di atti normativi in settori caratterizzati da un'elevata sensibilità, come la protezione dei dati personali o la sicurezza alimentare, come dimostra, tra l'altro, il Reg. (CE) n. 178/2002. In questa prospettiva, l'adozione del Regolamento sullo Spazio europeo dei dati sanitari (EHDS) trova un solido fondamento nell'art. 114 TFUE, in quanto mira a superare le frammentazioni dei regimi nazionali in materia di gestione dei dati sanitari, favorendo la libera circolazione delle informazioni cliniche e, al contempo, assicurando un livello elevato di tutela dei diritti fondamentali. La compatibilità del ricorso all'art. 114 TFUE con la protezione di interessi generali, quali la salute pubblica, è stata peraltro ribadita dalla Corte anche in ambiti contigui, come quello dei dispositivi medici (v., *ex multis*, *Philips*, C-547/14),

conservazione e condivisione dei dati sanitari rafforza la libera circolazione delle informazioni e promuove l'innovazione digitale nel settore.

Attraverso tale armonizzazione, si ambisce a facilitare l'accesso ai dati sanitari in tutta l'Unione, incrementando l'efficienza delle cure e favorendo lo sviluppo di nuove tecnologie applicate alla medicina²⁷.

In tal modo, l'EHDS si configura quale strumento strategico per il consolidamento del mercato unico digitale europeo e per l'affermazione di un modello di sanità basato sulla centralità del paziente, sull'efficienza informativa e sulla tutela rigorosa dei dati

purché l'intervento armonizzatore persegua in via principale l'obiettivo di garantire il buon funzionamento del mercato interno. Alla luce di tale orientamento costante, il ricorso all'art. 114 TFUE quale base giuridica dell'EHDS appare coerente con l'interpretazione funzionale ed evolutiva adottata dalla Corte, delineando un modello di armonizzazione idoneo a coniugare l'efficienza del mercato interno con l'esigenza di tutela dei diritti fondamentali dei cittadini dell'Unione.

²⁷ La letteratura sul rapporto tra nuove tecnologie e medicina è ormai estremamente ampia e articolata, rendendo impossibile darne conto in modo esaustivo nei limiti del presente contributo. Senza alcuna pretesa di esaustività, e al solo fine di richiamare alcuni dei principali filoni di riflessione rilevanti per l'analisi qui condotta, si rinvia pertanto ai seguenti contributi, che affrontano, da diverse prospettive, le implicazioni giuridiche dell'impiego delle tecnologie digitali, dei big data e dei sistemi di intelligenza artificiale in ambito sanitario. Segnatamente, F. VIMERCATI, *L'intelligenza artificiale in sanità*, in *Rapporti civilistici e intelligenze artificiali: attività e responsabilità*, a cura di P. Perlingieri, S. Giova e I. Prisco, Napoli, 2020, 211 ss.; E. FAZIO, *Robotica Medica, Human Enhancement e tutela dei fragili*, in *Jus civile*, 2023, 2, 513 ss.; N. FARIE, S. HINDER, R. WILLIAMS, R. RAMAESH, M.O. BERNABEU, E. VAN BEEK, K. CRESSWELL, *Early experiences of integrating an artificial intelligence-based diagnostic decision support system into radiology settings: a qualitative study*, in *Journal of the American Medical Informatics Association*, 2024, 31, 24 ss.; N. CONDITI, O. POLLICINO, F.A. SACCHI, *Is AI the perfect doctor? Artificial intelligence's global impact on the legal and policy boundaries in healthcare*, Milano, 2025, *passim*.

personali, contribuendo a edificare un'Unione europea della salute più solida, inclusiva e resiliente.

4. *Secondary Use of Electronic Health Data: disciplina procedurale e allocazione del rischio*

L'art. 50 del Reg. (UE) 2025/327 introduce una disciplina articolata sulle condizioni di esonero dagli obblighi legati al riutilizzo dei dati sanitari per finalità ulteriori rispetto a quelle originarie²⁸.

Il legislatore europeo, consapevole dell'eterogeneità dei soggetti coinvolti nella gestione e nel trattamento delle informazioni sanitarie, individua in modo differenziato i destinatari degli obblighi, escludendo dall'ambito applicativo alcune categorie strutturalmente meno attrezzate sul piano organizzativo e tecnologico. Tra queste rientrano le persone fisiche – ivi inclusi i ricercatori individuali – e le microimprese, esentate da taluni

²⁸ L'art. 50 del Reg. (UE) 2025/327 delinea i limiti soggettivi all'applicazione degli obblighi previsti per l'uso secondario dei dati sanitari, articolando un sistema finalizzato a bilanciare l'efficienza informativa europea con il principio di proporzionalità. Sono esentati – in ragione della loro capacità operativa contenuta – le persone fisiche che trattano dati per scopi personali o accademici e le microimprese, secondo la definizione europea (Raccomandazione 2003/361/CE). Tuttavia, l'articolo prevede che ciascun Paese possa estendere gli obblighi a queste categorie attraverso disposizioni interne. Viene altresì previsto che l'adempimento degli obblighi possa essere delegato a intermediari autorizzati, pur mantenendo la responsabilità primaria in capo al titolare originario del dato. Infine, per garantire trasparenza e omogeneità, il Regolamento impone agli Stati membri di notificare alla Commissione Europea – entro quarantotto mesi dall'entrata in vigore – le eventuali deroghe adottate a livello nazionale, consolidando un regime di *disclosure* multilivello e sorveglianza istituzionale.

adempimenti connessi alla condivisione e all'uso secondario²⁹. La scelta segnala un approccio pragmatico: costruire un sistema europeo 'esigibile' senza imporre, indiscriminatamente, oneri sproporzionati.

Tuttavia, la disposizione non si arresta a un approccio uniformante: attribuisce agli Stati membri un potere di adattamento, consentendo di sottoporre anche soggetti formalmente esclusi ai medesimi obblighi imposti ai titolari di dati sanitari, qualora ciò sia previsto dal diritto interno. Ne discende un modello di regolazione 'aperto', in cui la discrezionalità nazionale coesiste con l'impianto europeo. In controluce si intravede un potenziale rischio: che questa elasticità, se esercitata in modo non coordinato, alimenti una frammentazione latente e incida sull'obiettivo di armonizzazione del mercato dei dati sanitari.

Il Regolamento consente altresì agli Stati membri di delegare l'adempimento di determinati obblighi a entità terze, quali organismi di intermediazione o strutture centralizzate, cui sono affidati compiti di supporto operativo nella gestione e nella messa a disposizione dei dati, senza che ciò comporti una discontinuità nella filiera delle responsabilità gravanti sui titolari originari del trattamento. Tale architettura, ispirata a criteri di efficienza, specializzazione e standardizzazione tecnica, solleva tuttavia rilevanti questioni sul piano della distribuzione delle responsabilità, imponendo di chiarire quali obblighi residuino in capo al data holder, quali doveri gravino sui soggetti intermediari e secondo quali modalità debba essere assicurata la piena tracciabilità delle operazioni di trattamento, in particolare in caso di incidenti

²⁹ Sul tema delle differenti strategie di condivisione dei dati sanitari e del bilanciamento tra esigenze di accesso e tutela della riservatezza, v. B. MALIN, K. GOODMAN, *Between Access and Privacy: Challenges in Sharing Health Data*, in *Yearbook of Medical Informatics*, 2018, 27, 55 ss.

informatici, accessi non autorizzati o violazioni dei diritti degli interessati.

Il punto è che l'EHDS non mira esclusivamente alla definizione di un'architettura di interoperabilità. Esso istituisce, piuttosto, un regime di allocazione del rischio connesso al trattamento dei dati sanitari, nel quale la facilitazione dell'accesso e del riuso dei dati per finalità secondarie si accompagna a una redistribuzione degli obblighi di vigilanza, sicurezza e accountability tra i diversi soggetti coinvolti nella filiera del trattamento, incidendo conseguentemente anche sulla configurazione delle rispettive responsabilità.

A presidio della trasparenza e della coerenza del sistema, l'art. 50 impone agli Stati membri l'onere di notificare alla Commissione europea l'adozione di norme nazionali che amplino l'ambito applicativo degli obblighi o istituiscano meccanismi di intermediazione. L'obbligo di comunicazione – da adempiersi entro quarantotto mesi dall'entrata in vigore del Regolamento – mira a garantire una visione unitaria dell'attuazione nei diversi ordinamenti e a consentire un monitoraggio coerente delle prassi interne. In prospettiva, questa clausola riflette un modello di governance multilivello che tenta di prevenire divergenze applicative prima che producano effetti sistemici.

A presidio della coerenza dell'assetto europeo, l'obbligo di notifica imposto agli Stati membri delle misure nazionali che incidono sul riuso dei dati sanitari non svolge una mera funzione informativa, ma opera quale strumento di controllo preventivo della frammentazione regolatoria³⁰. Attraverso tale meccanismo,

³⁰ Sul punto, appare particolarmente utile distinguere, come evidenziato da F. Cascini, tra le differenti tipologie di dati sanitari che confluiscono nel sistema dell'uso secondario. L'A. evidenzia infatti che la categoria degli 'electronic health data' non è unitaria, ma comprende: (i) i Real-World Data (c.d. RWD), ossia informazioni eterogenee provenienti da fonti non sperimentali, raccolte al di fuori dei clinical trial; (ii) gli Electronic Health Records (c.d. EHR), che costituiscono dati strutturati generati all'interno dei sistemi sanitari e utilizzati

l'EHDS introduce una forma di vigilanza sistemica sull'evoluzione dei regimi nazionali, impedendo che l'esercizio delle competenze interne comprometta l'unitarietà dello spazio europeo dei dati sanitari. La notifica non è, dunque, un adempimento neutro, ma una tecnica di integrazione giuridica funzionale a preservare l'uniformità delle condizioni di accesso e riuso del dato sanitario su scala europea.

In questo quadro, la definizione delle categorie di dati accessibili al riuso assume un significato che trascende la mera classificazione tipologica.

L'inclusione di dati clinici, genomici, amministrativi e derivati da dispositivi digitali riflette la volontà del legislatore europeo di costruire un'infrastruttura informativa idonea a sostenere forme avanzate di ricerca, innovazione e governance sanitaria³¹. Ciò che

per finalità primarie di diagnosi e cura; (iii) i Patient-Generated Health Data (c.d. PGHD), prodotti direttamente dal paziente tramite dispositivi indossabili, app di monitoraggio o strumenti di auto-misurazione. Tale distinzione – lungi dall'essere meramente classificatoria – è decisiva per valutare i differenti livelli di qualità, accuratezza, rischio di bias e intensità dei profili di protezione richiesti per il riuso. Cfr., F. CASCINI, *Secondary Use of Electronic Health Data. Public Health Perspectives, Use Cases and Challenges*, Springer, 2025, spec. 15 ss.

³¹ L'art. 51 del Reg. (UE) 2025/327 individua in maniera puntuale le categorie di dati sanitari elettronici che i titolari sono tenuti a rendere accessibili ai fini dell'uso secondario, nell'ottica di favorire l'interoperabilità dei sistemi informativi e di sostenere la ricerca scientifica, nel rispetto dei diritti fondamentali della persona interessata. Il perimetro oggettivo delineato dalla disposizione è particolarmente ampio e comprende, tra l'altro, i dati contenuti nelle cartelle cliniche elettroniche; le informazioni relative ai determinanti della salute, inclusi quelli socio-economici, ambientali e comportamentali; i dati aggregati concernenti bisogni e risorse sanitarie, accesso alle cure, spesa e finanziamento; i dati relativi agli agenti patogeni, anche di natura epidemiologica e virologica; i dati amministrativi dell'assistenza sanitaria, quali prescrizioni, dispensazioni e rimborsi; i dati genetici, epigenomici e genomici; i dati molecolari umani, inclusi quelli di proteomica, trascrittomica, metabolomica e lipidomica; i dati generati da dispositivi medici, anche nell'ambito del monitoraggio remoto; i

rileva, sul piano giuridico, è che l'estensione dell'ambito oggettivo del riuso amplia correlativamente la superficie del rischio, rendendo centrale la qualificazione giuridica del dato e delle sue trasformazioni. Operazioni quali pseudonimizzazione, arricchimento o inferenza non sono tecnicamente neutrali, ma incidono sul regime di accesso, sulla distribuzione delle responsabilità e sull'intensità delle misure di protezione richieste, rendendo la governance del dato un processo continuo, che si estende ben oltre la fase originaria della raccolta.

Ancora più significativa è la delimitazione delle finalità ammissibili, che segna il passaggio da una logica fondata sulla disponibilità del dato a una logica fondata sulla legittimità dell'uso. L'EHDS non si limita a rendere accessibili i dati, ma condiziona tale accesso alla sussistenza di finalità qualificate, riconducibili a interessi pubblici determinati e verificabili³².

dati provenienti da applicazioni digitali per il benessere; i dati identificativi e professionali degli operatori sanitari; i dati estratti da registri sanitari popolazionali, epidemiologici e di sanità pubblica, nonché da registri medici e anagrafi di mortalità; i dati derivanti da sperimentazioni cliniche e studi regolamentati ai sensi della normativa unionale vigente (Reg. (UE) 536/2014, 2024/1938, 2017/745, 2017/746); i dati relativi ai dispositivi medici, anche ai fini della vigilanza post-commercializzazione; i dati raccolti nell'ambito di coorti di ricerca, questionari e indagini sanitarie ufficiali; nonché quelli conservati in biobanche e in banche dati affini, impiegati in medicina traslazionale. La disposizione riconosce inoltre agli Stati membri la facoltà di ampliare l'elenco delle categorie di dati rese disponibili ovvero di introdurre misure rafforzate di tutela per quelle particolarmente sensibili, nel rispetto di criteri di adeguatezza scientifica e di proporzionalità regolativa. Per un'analisi approfondita del regime dell'uso primario e secondario dei dati sanitari elettronici, v. M. IASELLI, *Le nuove regole per l'uso primario e secondario dei dati sanitari*. Reg. UE 11 febbraio 2025, n. 327 (EHDS), Santarcangelo di Romagna (RN), 2025, 71 ss., spec. 73.

³² L'art. 53 del Reg. (UE) 2025/327 individua in modo tassativo le finalità per cui è consentito l'uso secondario dei dati sanitari elettronici, ancorandone la legittimazione alla tutela dell'interesse pubblico e prevenendo utilizzi meramente utilitaristici o privatistici. Tra tali finalità rientrano, in particolare, la prevenzione

In tal modo, la finalità non opera come semplice requisito formale, ma come criterio sostanziale di legittimazione del riuso, consentendo di distinguere tra valorizzazione informativa compatibile con l'interesse collettivo e sfruttamento incompatibile con la funzione solidaristica del sistema sanitario europeo³³. Il dato

e la sorveglianza epidemiologica, il miglioramento della qualità dell'assistenza sanitaria, la valutazione delle tecnologie sanitarie, l'elaborazione delle politiche pubbliche in ambito sanitario e lo sviluppo di soluzioni innovative, inclusi dispositivi medici e sistemi algoritmici impiegati in ambito clinico. La disposizione riconosce la valenza strategica del dato sanitario per la trasformazione dei sistemi sanitari europei, subordinandone tuttavia l'utilizzo al rispetto del principio di finalità, della proporzionalità del trattamento e del quadro di garanzie delineato dal Reg. (UE) 2016/679, in un equilibrio tra innovazione e tutela dei diritti fondamentali dell'interessato.

³³ Cfr. Commission staff working document impact assessment report accompanying the document proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, Strasbourg, 3 maggio 2022, SWD (2022) 131 final, 78, punto 6.4.3, Policy Option 2. Il documento sottolinea l'impatto positivo dell'ampia disponibilità di dati sanitari di alta qualità sull'efficienza regolatoria, sulla sostenibilità economica dei farmaci e sulla ricerca in ambiti clinici complessi, affermando che: «Abundance and diversity of data would support better decision making, including of regulatory authorities. It would increase transparency, negotiation capacity, bringing down the prices for some drugs, supporting the repurposing of medicinal products, to the benefit of patients. For example, rare diseases include small population sizes where clinical trials may not be feasible. A mix of randomised trials and access to high quality health data would be required to study populations with unmet medical needs and contextualisation of treatment benefits for single-arm studies», la cui traduzione testuale è: «L'abbondanza e la varietà dei dati favorirebbero decisioni più consapevoli, anche da parte delle autorità regolatorie. Ciò aumenterebbe la trasparenza, la capacità negoziale, contribuendo alla riduzione dei prezzi di alcuni farmaci e supportando il riutilizzo dei medicinali, a beneficio dei pazienti. Ad esempio, le malattie rare includono popolazioni di dimensioni ridotte per le quali i trial clinici potrebbero non essere fattibili. Sarebbe quindi necessaria una combinazione tra studi randomizzati e accesso a dati sanitari di alta qualità, al fine di studiare popolazioni con bisogni medici

sanitario cessa, così, di essere una risorsa liberamente riutilizzabile e diventa un bene giuridicamente vincolato alla realizzazione di scopi normativamente predeterminati.

Questa impostazione trova il proprio completamento nel divieto di utilizzi suscettibili di arrecare pregiudizio agli interessati, che introduce un limite sostanziale all'autorizzabilità del riuso anche in presenza di finalità astrattamente ammissibili. Il legislatore europeo riconosce, in tal modo, che la conformità procedurale non esaurisce il giudizio di legittimità del trattamento: l'uso del dato resta subordinato alla verifica dei suoi effetti concreti, in particolare sotto il profilo del rischio di discriminazione, esclusione o compressione dei diritti fondamentali³⁴.

insoddisfatti e di contestualizzare i benefici dei trattamenti nei casi di studi a braccio singolo».

³⁴ L'art. 54 del Reg. (UE) 2025/327 stabilisce un limite essenziale all'impiego secondario dei dati sanitari elettronici, vietandone in modo categorico l'utilizzo ogniqualvolta da esso possa derivare un pregiudizio concreto e rilevante per le persone fisiche, specie se tale pregiudizio incide in misura significativa sulla loro condizione giuridica, economica o sociale. La norma esclude, in particolare, che i dati possano essere trattati per l'adozione di decisioni discriminatorie, automatizzate o comunque pregiudizievoli che producano effetti giuridici sull'interessato, come ad esempio in materia di occupazione, credito, assicurazione o accesso a beni e servizi. È altresì vietato il trattamento per finalità di marketing, profilazione commerciale o promozione, al fine di impedire derive funzionalmente estranee alla logica di tutela sottesa all'impiego dei dati per scopi di ricerca o interesse pubblico. In tal senso, la disposizione si configura come un presidio garantistico volto a salvaguardare la dignità dell'individuo, impedendo che l'utilizzo secondario di informazioni clinico-assistenziali possa divenire strumento di esclusione, manipolazione o vulnerazione dell'autodeterminazione informativa. Seppur in prospettiva differente, sul trattamento dei dati per finalità di marketing e profilazione commerciale, nonché nel contesto delle dinamiche remuneratorie, si v. A. DE FRANCESCHI, *Il «pagamento» mediante dati personali*, in *I dati personali nel diritto europeo*, a cura di V. Cuffaro, R. D'Orazio e V. Ricciuto, Torino, 2019, 1389 ss.; V. RICCIUTO, *Il contratto ed i nuovi fenomeni patrimoniali: il caso della*

Considerate nel loro insieme, queste disposizioni rivelano che l'EHDS non si limita a disciplinare l'accesso ai dati sanitari, ma costruisce un vero e proprio regime di governabilità del loro riuso, nel quale l'apertura informativa è subordinata a un sistema articolato di condizioni, controlli e limiti sostanziali. Il risultato è la trasformazione del dato sanitario in risorsa circolante entro uno spazio giuridicamente strutturato, in cui interoperabilità e protezione non operano come principi antagonisti, ma come componenti complementari di un medesimo modello regolatorio.

Rectius, le disposizioni sul secondary use delineano una governance multilivello in cui la valorizzazione informativa si accompagna a garanzie sostanziali per la persona, in un equilibrio dinamico tra innovazione e tutela dei diritti fondamentali, sotto la regia di un diritto europeo attento alle implicazioni bioetiche e giuridiche dell'informazione digitale. In questa cornice, un punto di osservazione privilegiato è la 'procedura' come strumento di legittimazione: autorizzazione, controlli, tracciabilità e ambienti sicuri diventano componenti essenziali del bilanciamento.

Questo impianto regolatorio complesso non è esente da criticità: l'eterogeneità dei livelli di maturità digitale tra Stati membri potrebbe acuire un data divide sistemico, generando disomogeneità nella capacità di adesione effettiva all'infrastruttura e, di riflesso, nell'equità dell'accesso al patrimonio informativo sanitario europeo³⁵. Se l'EHDS punta a una circolazione 'ordinata' del dato,

circolazione dei dati personali, in *Riv. dir. civ.*, 2020, 3, 642 ss. Si rinvia anche a P. PERLINGIERI, *L'informazione come bene giuridico*, in *Rass. dir. civ.*, 1990, 2, 326 ss.

³⁵ Sulle disegualianze strutturali tra Stati membri nella capacità di accesso, gestione e riuso transfrontaliero dei dati sanitari, v. R. BECKER, D. CHOKOSHVILI, E.S. DOVE, *Legal bases for effective secondary use of health and genetic data in the EU: time for new legislative solutions to better harmonize data for cross-border sharing?*, in *International Data Privacy Law*, 2024, 14, 223 ss. Gli Autori evidenziano come le differenze nei livelli di maturità infrastrutturale e tecnologica possano tradursi in asimmetrie nell'effettiva valorizzazione dei dati sanitari, con il rischio

la sua efficacia dipenderà anche dalla capacità di colmare gap infrastrutturali e amministrativi, pena l'emersione di asimmetrie tra Stati 'data-rich' e Stati 'data-poor'.

L'effettiva operatività dell'infrastruttura rimane altresì subordinata alla capacità degli Stati membri di convergere su standard interoperabili e meccanismi di governo armonizzati³⁶. In assenza di tale convergenza, il rischio di una frammentazione regolatoria latente potrebbe compromettere la vocazione unitaria e integrativa del sistema, rendendo l'armonizzazione solo nominale e non sostanziale. Da qui l'importanza di strumenti di coordinamento e di prassi applicative comuni (anche tramite soft law), capaci di evitare interpretazioni divergenti di concetti come 'finalità ammissibile', 'misure di de-identificazione' o 'sicurezza adeguata'.

In tale prospettiva, si pone con urgenza la necessità di una rinnovata architettura di legittimazione, capace di valorizzare la partecipazione informata e dinamica del paziente, superando

di accentuare una frattura informativa tra sistemi sanitari nazionali e di incidere negativamente sulla coesione normativa e sull'equità dell'accesso alla risorsa informativa.

³⁶ In tale contesto si inseriscono anche le più recenti iniziative di razionalizzazione del diritto digitale europeo. Con il c.d. Digital Omnibus Package (proposte di regolamento nn. 836 e 837/2025), la Commissione europea ha avviato un intervento volto a ridurre sovrapposizioni e oneri applicativi derivanti dalla stratificazione di discipline quali AI Act, GDPR e normativa sulla sicurezza dei dati, senza rimettere in discussione l'impianto garantista complessivo. L'iniziativa ha già formato oggetto di attenzione critica da parte dell'EDPB-EDPS, che nell'Opinion 1/2026 del 20 gennaio ha sottolineato l'esigenza di preservare un elevato livello di tutela dei diritti fondamentali, in particolare in relazione al trattamento dei dati personali, evidenziando come le semplificazioni procedurali debbano accompagnarsi a presidi effettivi di responsabilità, trasparenza e controllo. In tale prospettiva, il riuso dei dati sanitari e l'impiego di sistemi di IA si confermano come ambiti nei quali la sostenibilità regolatoria non può tradursi in un arretramento delle garanzie, ma richiede un bilanciamento strutturato e multilivello.

modelli autorizzativi statici e rafforzando il legame tra trasparenza, fiducia e accettabilità sociale del trattamento transfrontaliero³⁷. L'attenzione al controllo dell'interessato – anche mediante forme di informazione effettiva e non meramente formale – si rivela decisiva per la sostenibilità dell'intero disegno.

5. *L' HealthData@EU e la creazione di infrastrutture digitali transfrontaliere*

In questo orizzonte regolatorio, l'art. 75 del Reg. (UE) 2025/327 introduce l'infrastruttura transfrontaliera 'DatiSanitari@UE' (HealthData@EU), concepita quale architrave tecnico-organizzativo per rendere effettiva la condivisione e l'accesso ai dati sanitari elettronici a fini di riutilizzo tra Stati membri³⁸.

³⁷ In chiave comparata, v. W.B. LEE, S.J. CHOI, *Secondary Use Provisions in the European Health Data Space Proposal and Policy Recommendations for Korea*, in *Healthcare Informatics Research*, 2023, 29, 199 ss., i quali osservano come la proposta di Regolamento sullo Spazio europeo dei dati sanitari sia suscettibile di fungere da modello di riferimento anche al di fuori dell'Unione europea, in quanto introduce una disciplina organica del riutilizzo dei dati sanitari elettronici a fini di ricerca, innovazione e sviluppo di applicazioni di intelligenza artificiale in ambito sanitario. Gli Autori rilevano che, nel contesto sudcoreano, l'eventuale recepimento di un impianto analogo incontrerebbe rilevanti criticità, in particolare con riferimento all'obbligo di condivisione dei dati in capo ai soggetti privati; nondimeno, essi suggeriscono l'opportunità di ampliare l'accessibilità, per finalità secondarie, almeno ai dati generati nell'ambito di ricerche finanziate con risorse pubbliche. La comparazione evidenzia così l'ambizione dell'EHDS di coniugare tutela della riservatezza e promozione della ricerca, attraverso un bilanciamento strutturato tra diritti individuali e interesse collettivo all'innovazione.

³⁸ Sul punto, v. art. 75 del Reg. (UE) 2025/327, che istituisce l'infrastruttura transfrontaliera DatiSanitari@UE (HealthData@EU), definendone l'assetto organizzativo, le funzioni e i meccanismi di coordinamento multilivello. Tale infrastruttura si configura quale snodo tecnico-organizzativo volto a rendere

L'HealthData@EU non si esaurisce in una funzione di interconnessione tecnica tra sistemi nazionali, ma costituisce il dispositivo attraverso cui il legislatore europeo rende operativa la procedura di legittimazione dell'uso secondario dei dati sanitari³⁹.

L'accesso al dato non avviene più come atto isolato tra titolare e utilizzatore, ma si inserisce in una sequenza procedurale mediata da nodi istituzionali e tecnici che ne rendono verificabili presupposti, condizioni e limiti. L'infrastruttura diventa, in tal senso, lo spazio giuridico in cui il riuso del dato viene trasformato da possibilità tecnica a operazione normativamente qualificata.

La previsione di punti di contatto nazionali incaricati di gestire le richieste di accesso riflette questa logica di proceduralizzazione.

effettivo l'accesso e la disclosure dei dati sanitari elettronici per finalità di uso secondario a livello europeo, in un quadro normativo orientato alla circolazione controllata delle informazioni a beneficio della ricerca, della sanità pubblica e dell'innovazione terapeutica. Il Regolamento prevede, in particolare, la designazione di un punto di contatto nazionale in ciascuno Stato membro e l'istituzione, in capo alla Commissione europea, di un Health Data Access Service centrale, destinato a facilitare l'interazione tra i sistemi nazionali. Entrambe le strutture confluiscono nella piattaforma comune HealthData@EU, gestita dalla Commissione in qualità di responsabile del trattamento, con l'obiettivo di garantire interoperabilità, tracciabilità e sicurezza dei flussi informativi. Rilevante è inoltre l'introduzione del principio della 'richiesta unica', che consente la presentazione di un'unica istanza valida per più ordinamenti, riducendo la frammentazione procedurale. Sul quadro di interoperabilità e sugli standard applicabili, v. R. HUSSEIN, A. GYRARD, S. ABEDIAN, P. GRIBBON, S.A. MARTÍNEZ, *Interoperability Framework of the European Health Data Space for the Secondary Use of Data*, in *Journal of Medical Internet Research*, 2025, 27, consultabile all'indirizzo: <https://www.jmir.org/2025/1/e69813/>.

³⁹ La letteratura in materia non è tutta concorde in relazione alle tecniche di riutilizzo, difatti, in senso critico rispetto alla disciplina del riutilizzo dei dati sanitari, si segnala il contributo di A. CABRIO, *La seconda vita dei dati. Luci ed ombre della normativa privacy in materia di secondary data use*, in *I dati. Il futuro della sanità. Strumenti per una reale innovazione*, a cura di F. Frattino ed E. Massimino, Milano, 2022, 25.

Tali organismi non svolgono una funzione meramente amministrativa, ma operano come garanti della conformità del riuso al quadro normativo europeo, assicurando che ogni accesso sia tracciabile, motivato e riconducibile a finalità legittime. In questo passaggio si realizza una trasformazione significativa: la legittimità del trattamento non deriva esclusivamente dalla base giuridica astratta, ma dalla conformità a un processo autorizzatorio strutturato, che consente di ricostruire *ex post* la sequenza decisionale e le responsabilità dei soggetti coinvolti.

Il ruolo di coordinamento attribuito alla Commissione europea si inserisce nella medesima architettura. L'istituzione di un servizio di accesso ai dati sanitari dell'Unione e la gestione della piattaforma centralizzata non rispondono soltanto a esigenze di interoperabilità, ma introducono un livello ulteriore di garanzia, volto a ridurre il rischio di divergenze applicative e a rendere omogenee le condizioni di accesso al dato su scala europea. La piattaforma non rappresenta, pertanto, un semplice strumento tecnologico, ma una componente essenziale del sistema di accountability, in quanto consente di assicurare tracciabilità delle operazioni, verificabilità delle autorizzazioni e integrità dei flussi informativi⁴⁰.

⁴⁰ La piattaforma DatiSanitari@UE (c.d. HealthData@EU) non si configura come una banca dati centralizzata dei dati sanitari europei, bensì come un'infrastruttura digitale comune destinata a connettere e coordinare i punti di accesso nazionali e i soggetti legittimati al riuso dei dati. Essa svolge una funzione di intermediazione tecnico-organizzativa, finalizzata a rendere omogenee le procedure di presentazione, gestione e monitoraggio delle richieste di accesso per finalità secondarie, assicurando interoperabilità, sicurezza e tracciabilità dei flussi informativi. I dati restano, in linea di principio, nella disponibilità dei titolari o degli organismi nazionali competenti, mentre la piattaforma fornisce un quadro armonizzato per lo scambio delle informazioni e per il controllo degli accessi, sotto il coordinamento della Commissione europea. In questa prospettiva, HealthData@EU assume il ruolo di infrastruttura abilitante del riutilizzo transfrontaliero dei dati sanitari,

Particolarmente significativo è, in questa prospettiva, il ruolo degli ambienti sicuri di elaborazione dei dati. La loro previsione non può essere letta come mera misura tecnica di sicurezza, ma deve essere intesa quale elemento integrante del regime giuridico del trattamento. L'adozione di un ambiente sicuro contribuisce, infatti, a definire lo standard di diligenza esigibile dai soggetti coinvolti nella gestione e nel riuso dei dati sanitari, operando come parametro oggettivo per la valutazione della correttezza delle condotte e per la delimitazione delle rispettive responsabilità. In caso di accessi non autorizzati, perdita di dati o utilizzi impropri, la conformità – o non conformità – alle condizioni operative dell'ambiente sicuro potrà assumere rilievo decisivo nella ricostruzione del nesso causale e nella valutazione della colpa, trasformando l'infrastruttura tecnologica in un vero e proprio presidio giuridico di imputazione della responsabilità.

Ne emerge un modello in cui la dimensione tecnica e quella giuridica risultano inscindibilmente integrate: l'infrastruttura non si limita ad abilitare la circolazione del dato, ma contribuisce a definirne le condizioni di liceità e i criteri di imputazione delle responsabilità. In questa prospettiva, la governance tecnologica si configura come componente strutturale della governance giuridica del riuso, confermando come, nell'EHDS, la legittimazione del trattamento non dipenda soltanto da presupposti normativi astratti, ma dalla conformità a un ecosistema procedurale e infrastrutturale progettato per rendere il riuso dei dati al tempo stesso possibile, controllabile e giuridicamente imputabile.

consentendo di evitare una concentrazione materiale delle informazioni e preservando un modello di distribuzione e controllo multilivello. Sul punto, v. L.S. SVINGEL, C.E. JENSEN, G.F. KJELDSSEN, M.H. PEDERSEN, D. KALRA, C.F. CHRISTIANSEN, K.H. VAD, *Shaping the future EHDS: recommendations for implementation of Health Data Access Bodies in the HealthData@EU infrastructure for secondary use of electronic health data*, in *European Journal of Public Health*, 2025, 35, iii32-iii38.

Tra le innovazioni più significative figura il principio della ‘richiesta unica’, secondo cui i soggetti interessati possono presentare un’unica istanza valida per più Stati membri, valutata congiuntamente dai rispettivi organismi responsabili. Ne deriva una semplificazione procedurale rilevante: si abbatte la frammentazione burocratica e si agevola un utilizzo omogeneo dei dati su scala sovranazionale⁴¹. Tuttavia, la semplificazione procedurale accresce l’esigenza di regole chiare sulla competenza, sulla tracciabilità e sulla gestione delle divergenze decisionali tra autorità coinvolte.

La disposizione in parola segna così un avanzamento decisivo verso la costruzione di un ecosistema digitale europeo in ambito sanitario, teso a rafforzare il potenziale informativo in un’ottica di coesione, efficienza e progresso scientifico. L’attuazione concreta richiederà ingenti investimenti tecnologici e organizzativi, oltre a un elevato livello di coordinamento tra ordinamenti disomogenei per maturità digitale e capacità operativa. È qui che la governance multilivello mostra la propria fragilità: l’infrastruttura è comune, ma le capacità di alimentarla e governarla non lo sono necessariamente.

Permangono inoltre interrogativi sul piano della protezione dei dati personali e della sicurezza informatica, in particolare rispetto al rischio di accessi non autorizzati o incidenti di sicurezza.

In questo contesto, la cybersicurezza emerge non soltanto come requisito tecnico, ma come nodo critico della sostenibilità giuridica

⁴¹ Il principio della ‘richiesta unica’ trova il proprio fondamento nell’art. 67 del Reg. (UE) 2025/327, che consente agli utenti dei dati di presentare un’unica istanza di accesso ai dati sanitari elettronici per uso secondario anche quando essi siano detenuti in più Stati membri. La procedura, ulteriormente disciplinata dagli artt. 68 e 69 EHDS, si basa su un coordinamento tra gli organismi nazionali competenti, realizzato attraverso l’infrastruttura HealthData@EU. L’istituto è volto a ridurre la frammentazione amministrativa e a favorire un utilizzo transfrontaliero più efficiente e omogeneo dei dati sanitari per finalità di ricerca, innovazione e definizione delle politiche pubbliche.

dell'intero sistema. L'estensione transfrontaliera dei flussi informativi e la concentrazione dei dati sanitari in infrastrutture interoperabili accrescono fisiologicamente la superficie di esposizione a rischi di accessi non autorizzati, perdite di integrità o utilizzi impropri. Ciò pone un interrogativo che il quadro normativo lascia solo parzialmente risolto: se l'adozione di misure avanzate di sicurezza debba essere intesa come un obbligo di risultato o, piuttosto, come un obbligo di diligenza, e secondo quali criteri debba essere valutata l'adeguatezza delle misure adottate in contesti caratterizzati da elevata complessità tecnica e organizzativa.

In altri termini, quanto più il sistema favorisce la circolazione del dato, tanto più la sicurezza diventa condizione strutturale della sua legittimità, ma anche parametro potenzialmente rilevante per la delimitazione delle responsabilità. Il rischio è che, in assenza di standard tecnici e interpretativi sufficientemente determinati, la valutazione dell'adeguatezza delle misure di cybersicurezza resti affidata a un giudizio *ex post*, esposto a margini di incertezza e a possibili divergenze applicative tra ordinamenti e autorità competenti⁴². In chiave di responsabilità, l'interrogativo è se (e

⁴² In tema di sicurezza dei dati sanitari nell'era dell'IA, v. B.N. ROMANO, *In the Era of AI. Exploring New Frontiers in Cybercrime and Safeguarding Personal and Health Data*, in *Corti Supreme e Salute*, 2024, 1, 2 ss., la quale mette in evidenza come la crescente digitalizzazione dei sistemi sanitari, pur favorendo interoperabilità ed efficienza dei processi clinico-assistenziali, accresca in modo significativo l'esposizione degli asset informativi a nuove forme di vulnerabilità. L'A. segnala, in particolare, i rischi connessi ad accessi non autorizzati, violazioni dei dati e utilizzi distorti delle informazioni sanitarie, evidenziando al contempo la persistente disomogeneità dei quadri normativi e la fragilità delle architetture nazionali di sicurezza informatica. In tale contesto, viene sottolineata la necessità di un presidio di cybersecurity strutturato su più livelli, adeguatamente sostenuto sul piano tecnico e istituzionale, quale condizione essenziale per l'effettiva tutela dei dati sanitari nello spazio digitale.

come) tali misure divengano criteri di imputazione in caso di danno o violazione.

Ulteriori criticità potrebbero emergere sul piano dell'equilibrio tra accessibilità e tutela dei diritti degli interessati, soprattutto con riferimento al diritto alla trasparenza e al controllo sull'impiego dei propri dati sanitari⁴³. La sostenibilità del secondary use dipenderà dalla capacità di rendere comprensibili e verificabili i percorsi del dato: chi lo usa, per quali fini, con quali limiti e per quanto tempo.

In stretta connessione con quanto sopra, l'art. 76 disciplina l'accesso a registri e banche dati transfrontaliere contenenti dati sanitari elettronici, delineando un assetto di competenze volto a garantire certezza giuridica e snellezza procedurale⁴⁴. Se il registro

⁴³ Come argutamente osservato da F. DI CIOMMO, *Il trattamento dei dati sanitari tra interessi individuali e collettivi*, in *Danno e resp.*, 2002, 2, 121 ss., il trattamento delle informazioni relative alla salute si colloca al crocevia fra esigenze contrapposte. Da un lato, tali dati rappresentano un presupposto indispensabile per la diagnosi, la cura e il progresso della ricerca scientifica; dall'altro, la loro particolare sensibilità espone l'individuo a rischi rilevanti, idonei a comprimere la sfera privata e il diritto alla riservatezza. L'A. mette così in luce il necessario equilibrio tra utilità sociale della circolazione del dato sanitario e tutela della persona cui esso si riferisce.

⁴⁴ Nel disegno dell'EHDS, l'art. 76 del Reg. (UE) 2025/327 svolge una funzione di raccordo tra la dimensione nazionale delle banche dati sanitarie e la circolazione transfrontaliera delle informazioni. La norma, ispirata a esigenze di certezza giuridica e di semplificazione procedurale, individua i criteri di attribuzione della competenza nei procedimenti di accesso ai registri contenenti dati sanitari elettronici: la competenza spetta all'organismo dello Stato membro in cui è stabilito il titolare del registro, ovvero, in caso di contitolarità, a quello di uno degli Stati coinvolti; qualora i registri siano organizzati in una rete coordinata, essa è attribuita allo Stato in cui ha sede il soggetto coordinatore. L'impianto mira a razionalizzare l'esercizio dei poteri amministrativi e a garantire coerenza nelle decisioni di accesso. Permane tuttavia una criticità, legata alla mancanza di un meccanismo espresso di composizione dei conflitti tra autorità nazionali, che potrebbe rendere necessario il ricorso a strumenti di soft law o a futuri interventi correttivi a livello unionale. Cfr., ancora una volta, M. IASELLI, *Le nuove regole*, cit., 106.

è detenuto da un titolare stabilito in uno Stato membro, la competenza spetta all'organismo di quello Stato; in caso di contitolarità tra più Stati membri, si fa riferimento allo Stato in cui è stabilito uno dei contitolari; ove più registri siano unificati in una rete, la competenza è attribuita all'organismo dello Stato in cui ha sede il coordinatore della rete. *Rectius*, la norma tenta di 'mappare' la competenza in un ecosistema distribuito, ma resta esposta a tensioni interpretative nei casi limite.

Tale assetto mira a evitare sovrapposizioni o conflitti di competenza, ma la sua efficacia dipenderà dalla reale capacità degli Stati di cooperare nella designazione di coordinatori efficienti e dotati delle risorse necessarie. Infine, la disposizione non prevede esplicitamente meccanismi per la risoluzione delle controversie interpretative tra autorità nazionali, lacuna che potrebbe essere colmata da interventi futuri o mediante prassi di soft law a livello unionale⁴⁵. In termini sistematici, è un punto che si presta bene a un approfondimento sul 'diritto procedurale' dell'accesso ai dati: strumenti di composizione, standard comuni e responsabilità in caso di conflitto.

In definitiva, il progetto dell'European Health Data Space mostra come la prospettiva europea sia sempre più orientata a favorire il riuso dei dati sanitari in chiave di ricerca e innovazione,

⁴⁵ La disposizione in esame si concentra sulla definizione dei criteri di riparto della competenza amministrativa, senza tuttavia introdurre strumenti di coordinamento rafforzato né meccanismi specifici per la composizione di eventuali divergenze interpretative o applicative tra le autorità nazionali coinvolte. Tale carenza assume particolare rilievo in un contesto caratterizzato dalla coesistenza di una pluralità di ordinamenti, da assetti organizzativi eterogenei e dal rischio di conflitti nella qualificazione giuridica delle richieste di accesso ai dati. In questa prospettiva, potrebbe rendersi necessario il ricorso a strumenti di soft law a livello unionale – quali linee guida o raccomandazioni della Commissione o dell'organo europeo competente – ovvero un successivo intervento normativo volto a garantire un'applicazione più uniforme ed efficace del regime di accesso transfrontaliero ai dati sanitari.

pur nel rispetto delle garanzie fondamentali. La tensione tra valorizzazione del dato e tutela della persona non resta confinata alla dimensione sovranazionale, ma trova già riflessi significativi nell'esperienza italiana, che sembra anticipare taluni tratti del paradigma europeo.

6. Dal consenso alla procedura: il riuso dei dati sanitari tra interesse pubblico, accountability e nuove tecniche di de-identificazione nel diritto italiano. Interrogativi aperti

Dunque, in questa prospettiva, l'European Health Data Space non si limita a configurare un'infrastruttura transfrontaliera, ma sollecita gli Stati membri ad adeguare i propri ordinamenti, così da rendere effettiva la circolazione dei dati sanitari a fini di ricerca e innovazione⁴⁶.

Difatti, l'ordinamento italiano ha compiuto un passo significativo con l'adozione della Legge 23 settembre 2025, n. 132 («Disposizioni e deleghe al Governo in materia di intelligenza artificiale»), pubblicata in G.U. n. 223 del 25 settembre 2025 ed entrata in vigore il 10 ottobre 2025⁴⁷. Il dato rilevante, è che il legislatore nazionale interviene su un terreno da tempo controverso: la possibilità di riuso dei dati sanitari tra ricerca, responsabilità sanitaria e tutela della persona.

⁴⁶ Per primo spunto sul tema della circolazione dei dati per uso secondario, soprattutto in relazione al progresso e allo sviluppo che la ricerca scientifica potrebbe trarre, v. L. TRAPANI, *La circolazione dei dati sanitari per uso secondario e la riduzione dei divari*, in *Italian Papers On Federalism*, 2025, 3, 165 ss.

⁴⁷ Il disegno di legge n. 1146, intitolato «Disposizioni e deleghe al Governo in materia di intelligenza artificiale», è stato presentato, com'è noto, al Senato il 20 maggio 2024 e successivamente approvato in via definitiva con la conversione in legge nell'ambito della seduta del 17 settembre 2025 (A.S. 1146-B). Trattasi della l. 23 settembre 2025, n. 132, pubblicata in G.U. n. 223 del 25 settembre 2025 ed entrata in vigore il 10 ottobre 2025.

L'art. 8 della nuova legge si colloca nel solco delle evoluzioni europee rappresentate dall'EHDS, costituendo al contempo un tentativo di colmare le incertezze applicative che, a livello nazionale, avevano a lungo ostacolato la piena valorizzazione del patrimonio informativo sanitario.

In controluce, la norma segnala una transizione: dal paradigma 'consenso-centrico' a un paradigma 'interesse pubblico + garanzie', nel quale la legittimità del trattamento dipende dalla qualità delle misure e dei controlli⁴⁸.

La disposizione, in primo luogo, qualifica il riuso dei dati sanitari per finalità di ricerca come attività di rilevante interesse pubblico, offrendo così una base normativa idonea a integrare il presupposto di cui all'art. 9, par. 2, lett. g), GDPR. La scelta assume un significato che trascende la tecnica legislativa: essa stabilizza il fondamento giuridico del trattamento, sottraendolo all'incertezza interpretativa che aveva caratterizzato il precedente assetto, nel quale il bilanciamento tra consenso dell'interessato e interesse pubblico alla ricerca risultava oscillante e talora frammentario. La legittimazione del riuso viene così ancorata a una valutazione normativa *ex ante* dell'interesse collettivo, in linea con la razionalità sottesa al secondary use europeo, dove la protezione dei dati non

⁴⁸ La logica di una vigilanza dinamica e non meramente consensuale trova un precedente significativo nell'esperienza tedesca. Il § 27 del Bundesdatenschutzgesetz (c.d. BDSG) consente infatti di derogare agli obblighi informativi e al consenso dell'interessato qualora il loro adempimento risulti sproporzionato o idoneo a compromettere il conseguimento delle finalità di ricerca scientifica, purché il trattamento dei dati sanitari sia necessario, proporzionato e sorretto da un interesse pubblico prevalente. Tale impostazione anticipa la razionalità sottesa allo Spazio Europeo dei Dati Sanitari, segnando un passaggio dal paradigma consensocentrico a un modello di gestione fondato sulla responsabilizzazione degli attori istituzionali e sul bilanciamento strutturale degli interessi in gioco. Cfr. V. ZAMBRANO, *EHDS e soggetti vulnerabili: tra esigenze di condivisione dei dati sanitari e tutela della persona*, in *Accademia*, 2025, 9, 1097 ss., spec. 1104.

è compressa, ma riorganizzata entro un quadro di garanzie strutturali.

In questa cornice si inserisce anche la possibilità di procedere al riuso senza una nuova manifestazione di consenso, a condizione che siano adottate misure idonee a ridurre l'impatto sui diritti dell'interessato, in particolare attraverso tecniche di de-identificazione⁴⁹. Il consenso perde, dunque, la funzione di snodo esclusivo della liceità, mentre assumono centralità le misure organizzative e tecniche volte a contenere il rischio di re-identificazione e di utilizzi eccedenti. La tutela si sposta dal piano della volontà individuale a quello della governabilità del trattamento: non è l'assenza di rischio a fondare la legittimità del riuso, ma la sua gestione secondo standard verificabili e controllabili, in un'ottica di responsabilizzazione degli attori coinvolti.

La disposizione richiama, anche implicitamente, la giurisprudenza della Corte di Giustizia (si pensi alla recente sentenza *EDPS v. SRB*, C-413/23 P⁵⁰), che ha ribadito come la de-

⁴⁹ In una fase antecedente all'approvazione definitiva del DDL 1146/2025, l'Autorità Garante per la protezione dei dati personali è intervenuta sullo schema normativo con il Parere del 2 agosto 2024 («Parere su uno schema di disegno di legge recante disposizioni e deleghe in materia di intelligenza artificiale»). In tale sede, pur esprimendo un orientamento favorevole alla valorizzazione del riuso dei dati sanitari per finalità di ricerca, l'Autorità ha evidenziato l'esigenza di circoscrivere con maggiore precisione l'ambito dell'esenzione dal consenso prevista dal comma 2, nonché di rafforzare le garanzie connesse all'informativa agli interessati, anche mediante forme di informazione generale. Il testo del parere è disponibile sul sito istituzionale dell'AUTORITÀ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI: <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10043532>.

⁵⁰ In giurisprudenza, la Corte di Giustizia dell'Unione Europea ha costantemente adottato un'interpretazione estensiva della nozione di 'dato personale', ricomprendendovi qualsiasi informazione idonea a rendere identificabile, anche

identificazione non elimini del tutto il rischio di re-identificazione, ma rappresenti una misura idonea a ridurre l'impatto sul diritto alla protezione dei dati, mantenendo un livello di garanzia. Il punto è cruciale: se il rischio residuo è fisiologico, allora la legittimazione del riuso non può fondarsi su un 'mito' di anonimato perfetto, ma su standard, audit e responsabilità in caso di fallimento delle misure.

La disciplina non si limita a ridefinire la base di legittimazione del riuso per finalità di ricerca, ma ne estende l'ambito alle attività di programmazione, gestione e valutazione dell'assistenza sanitaria, includendo anche i rapporti con soggetti accreditati o convenzionati con il Servizio sanitario nazionale. In tal modo, il dato sanitario viene esplicitamente configurato come infrastruttura conoscitiva del governo del sistema, non solo come risorsa scientifica. L'estensione delle finalità legittimanti accresce, tuttavia, la rilevanza delle tecniche di trattamento impiegate, poiché quanto più ampio è il perimetro del riuso, tanto più decisivo diventa il controllo sul rischio di identificazione e di utilizzi impropri. In questo contesto, l'espresso riconoscimento di strumenti quali anonimizzazione, pseudonimizzazione e sintetizzazione segna un passaggio rilevante: la legittimità del riuso non viene ancorata

indirettamente, una persona fisica. In tal senso, v. Corte di Giustizia UE, *Novak*, C-434/16, 20 dicembre 2017, nella quale la Corte ha riconosciuto natura di dato personale anche alle risposte fornite da un candidato in sede di esame; nonché Corte di Giustizia UE, *GC e a.*, C-136/17, 24 settembre 2019, che ha confermato l'ampiezza dell'ambito di applicazione della tutela, includendovi categorie di informazioni di particolare sensibilità. Con riferimento specifico ai dati sanitari e al loro trattamento per finalità di ricerca, assume rilievo anche la recente Corte di Giustizia UE, *EDPS c. SRB*, C-413/23 P, 11 aprile 2024, nella quale la Corte ha chiarito che le tecniche di de-identificazione non escludono in modo assoluto il rischio di re-identificazione, ma possono costituire strumenti adeguati per realizzare un bilanciamento proporzionato tra le esigenze della ricerca scientifica e la salvaguardia dei diritti fondamentali degli interessati.

all'assenza assoluta di rischio, ma alla sua riduzione mediante tecniche conformi a un approccio risk-based⁵¹.

La scelta di valorizzare anche la sintetizzazione – elevando i dati sintetici (c.d. synthetic data) a tecnica giuridicamente utilizzabile – mostra una progressiva maturazione dell'ordinamento verso modelli di produzione dell'informazione alternativi al trattamento diretto del dato originario. Tuttavia, l'efficacia di tale opzione dipende dalla definizione di standard metodologici affidabili e verificabili, poiché in assenza di criteri condivisi il rischio è quello di una tutela solo formale, incapace di prevenire fenomeni di re-identificazione indiretta o distorsioni.

In questa architettura si inserisce il ruolo attribuito ad Agenas nella predisposizione di linee guida tecniche, previo coinvolgimento dell'Autorità di controllo. La regolazione del riuso si sposta così, almeno in parte, su un piano tecnico-amministrativo, nel quale la determinazione concreta degli standard assume una funzione decisiva per l'effettività delle garanzie. Se tale processo di definizione non sarà coerente e coordinato con il quadro europeo,

⁵¹ Con riferimento alle tecniche di anonimizzazione – e, in particolare, alla pseudonimizzazione – resta centrale il Parere 05/2014 sulle tecniche di anonimizzazione (WP216), adottato il 10 aprile 2014 dal Article 29 Data Protection Working Party. In tale documento la pseudonimizzazione è descritta come un processo di sostituzione degli attributi identificativi con elementi alternativi, idonei a ridurre il collegamento diretto con l'identità dell'interessato. La nozione è stata poi recepita e sistematizzata dall'art. 4, n. 5, GDPR, che qualifica la pseudonimizzazione come una modalità di trattamento volta a impedire l'attribuzione dei dati a una persona determinata senza l'uso di informazioni aggiuntive, le quali devono essere conservate separatamente e protette mediante adeguate misure tecniche e organizzative. In dottrina si è sottolineato come tale tecnica, pur non eliminando in radice il rischio di re-identificazione, rappresenti uno strumento centrale nell'approccio risk-based al trattamento dei dati personali: cfr. S. SICA, V. D'ANTONIO, G. GIANNONE CODIGLIONE, G. SCIANCALEPORE, *Privacy, tutela del consumatore e risk based approach*, in www.comparazionedirittocivile.com, spec. 9.

il rischio è una frammentazione applicativa che potrebbe incidere sulla certezza delle condizioni di liceità.

Sul piano procedurale, la previsione di un meccanismo fondato sul silenzio dell'autorità competente, a fronte di una comunicazione corredata dalle informazioni richieste dal GDPR e dal previo vaglio etico, segna un mutamento significativo del modello di controllo. Il sistema si allontana da una logica autorizzatoria pienamente *ex ante* e si orienta verso una vigilanza strutturata, nella quale la responsabilità dell'operatore assume un peso maggiore. Quanto più si riduce il filtro preventivo, tanto più centrale diventa la capacità di documentare l'adozione di misure adeguate e di garantire la tracciabilità delle operazioni compiute. In tale prospettiva, la semplificazione procedurale non attenua le esigenze di tutela, ma ne modifica la tecnica di attuazione, spostando l'asse dalla preventiva abilitazione formale alla verifica successiva della conformità.

Tale mutamento di tecnica regolatoria non resta confinato alla disposizione in esame, ma si riflette nel coordinamento con la disciplina generale del trattamento dei dati personali, confermando la volontà del legislatore di stabilizzare il nuovo paradigma entro l'architettura complessiva del Codice Privacy. Le previsioni dell'art. 8 trovano riscontro nel nuovo art. 110 del d.lgs. 196/2003, come modificato dal d.lgs. 123/2025, che ne recepisce la disciplina in chiave attuativa: i trattamenti per ricerca scientifica, sanitaria e di governo sono qualificati di rilevante interesse pubblico, possono avvenire anche senza consenso e seguono il modello del parere dei comitati etici, della comunicazione preventiva al Garante e del silenzio-assenso⁵².

⁵² Sul riuso dei dati sanitari per finalità di ricerca scientifica, v. G. CERRINA FERONI, *Ricerca scientifica e protezione dei dati personali alla luce dell'EHDS: un equilibrio necessario*, in *Sanità digitale*, cit., 245 ss.; nonché A.M.S. CALDORO, A. MENDOLA,

L'art. 110 assume così una funzione di consolidamento del nuovo paradigma, trasponendo nel sistema generale del Codice Privacy la medesima logica di interesse pubblico, di ridimensionamento della centralità del consenso e di vigilanza strutturata che connota l'art. 8, in coordinamento con il GDPR e in prospettiva con l'EHDS.

In parallelo, il «Decalogo sull'uso dell'intelligenza artificiale in sanità», adottato dal Garante nell'ottobre 2023, individua principi di trasparenza, supervisione umana e non discriminazione algoritmica come pilastri dell'impiego etico dell'IA⁵³. Tali principi assumono rilievo non soltanto sul piano valoriale, ma anche quale parametro di conformità nell'utilizzo dei dati sanitari per lo sviluppo di modelli predittivi, costituendo un raccordo tra protezione dei dati, qualità della ricerca e fiducia dei cittadini, e potendo essere valorizzati come criteri per la definizione della diligenza esigibile nell'impiego di sistemi automatizzati, specie quando l'uso dei dati sanitari alimenta modelli predittivi e sistemi di supporto alle decisioni.

La recente riforma dell'art. 110 e il rafforzamento del ruolo di Agenas – già delineato da interventi precedenti e consolidato dalla l. 132/2025 – si inseriscono in un disegno più ampio di governance digitale e promozione della ricerca. In tale cornice, la co-

AI Health e dati sanitari tra ricerca scientifica e uso secondario, in *Diritto di Internet*, 2026, 3, 409 ss.

⁵³ Il documento, adottato dall'Autorità Garante per la protezione dei dati personali nell'ottobre 2023, si colloca nell'ambito degli strumenti di *soft law* volti a orientare l'impiego dell'intelligenza artificiale in sanità, rafforzando l'attenzione ai profili di responsabilità, controllo umano e tutela dei diritti fondamentali nell'uso di sistemi algoritmici in ambito clinico. Per ulteriori approfondimenti, si rinvia al sito istituzionale dell'Autorità Garante al seguente *link*: <https://www.garanteprivacy.it/documents/10160/0/Decalogo+per+la+realizzazione+di+servizi+sanitari+nazionali+attraverso+sistemi+di+Intelligenza+Artificiale.pdf/>.

regolazione (regole deontologiche, linee guida, prassi applicative) è destinata a svolgere un ruolo decisivo: l'apertura al riuso richiede non solo basi giuridiche, ma anche standard tecnici e procedure uniformi, capaci di rendere effettivo il bilanciamento⁵⁴.

Particolare attenzione merita la disciplina dei summenzionati dati sintetici, già considerati dal Data Governance Act⁵⁵ (Considerando 7) e dall'AI Act (artt. 10 e 59) come strumenti utili anche in ottica di debiasing e sperimentazione regolatoria

⁵⁴ Difatti, testualmente, osserva P. STANZIONE, *Intelligenza artificiale, dati sanitari e FSE nel quadro sanitario dell'Unione Europea*, in *Sanità digitale*, cit., 5: «È recente (d.l. PNRR bis, del marzo scorso) la previsione strutturale del ricorso all'I.A. in sanità, con un ruolo centrale di Agenas, ulteriormente rafforzato dal ddl governativo sull'I.A. approvato da poco dal Senato. Ed è stata anche riformata, con lo stesso decreto, la disciplina del trattamento dei dati negli studi retrospettivi (art. 110 Codice privacy), agevolando gli adempimenti per promuovere la ricerca. Il Garante ha avviato di recente i lavori per la stesura delle regole deontologiche cui la riforma dell'art. 110 demanda la disciplina di dettaglio per la ricerca medica, biomedica ed epidemiologica, secondo il paradigma di co-regolazione che rappresenta uno dei maggiori punti di forza della disciplina di protezione dei dati».

⁵⁵ Per un'analisi della struttura e delle finalità del Data Governance Act, nonché del suo impatto sui modelli di gestione e circolazione dei dati anche in ambito sanitario, v. F. MASCHIO, *Innovazione digitale dei sistemi sanitari, eHealth e questioni di data governance, nell'agenda digitale sanitaria nazionale ed europea*, in *Comparazione e diritto civile*, 2021, 2, *passim*. L'Autrice colloca il DGA all'interno della più ampia strategia europea per il mercato unico digitale, sottolineandone la funzione di quadro di riferimento per forme di condivisione dei dati fondate su fiducia, interoperabilità e riutilizzo responsabile. Con specifico riguardo alla sanità digitale, il Regolamento contribuisce a ridefinire le modalità di accesso e riuso dei dati, rafforza la disciplina degli intermediari dei dati e anticipa alcuni presupposti funzionali alla realizzazione dello Spazio Europeo dei Dati Sanitari, incidendo tanto sull'assetto delle infrastrutture informative quanto sulle garanzie poste a tutela dei diritti fondamentali nelle attività di eHealth, telemedicina e ricerca clinica.

(sandbox)⁵⁶. L'ordinamento interno, con la l. 132/2025 e le linee guida Agenas, si allinea a tale prospettiva, riconoscendo ai synthetic data un ruolo potenzialmente decisivo nel conciliare esigenze di privacy e di ricerca.

Resta aperta, tuttavia, la questione degli standard: senza metriche condivise di utilità, robustezza e rischio di re-identificazione indiretta, la sintetizzazione potrebbe diventare una 'soluzione apparente', incapace di offrire parametri oggettivi di controllo e di imputazione delle responsabilità in caso di utilizzo improprio o di fallimento delle misure adottate.

In questo quadro, l'art. 7 della l. 132/2025 disciplina espressamente l'impiego dell'intelligenza artificiale in sanità, subordinandone l'uso al controllo umano e vietando forme di selezione o condizionamento nell'accesso alle cure basate su criteri algoritmici⁵⁷. Il sistema di IA assume funzione ausiliaria rispetto alla decisione medica, che resta riservata al professionista sanitario secondo principi di affidabilità, verificabilità e aggiornamento dei

⁵⁶ Nel lessico del diritto europeo, la 'sperimentazione regolatoria' (c.d. sandbox) designa strumenti normativi che consentono l'applicazione controllata e temporalmente delimitata di regimi giuridici differenziati, finalizzati a valutare la compatibilità di soluzioni tecnologiche innovative con i principi dell'ordinamento, in particolare con la tutela dei diritti fondamentali. In tale prospettiva, il ricorso ai dati sintetici assume rilievo quale tecnica giuridicamente funzionale a ridurre l'impatto del trattamento su persone identificabili nella fase sperimentale, consentendo la verifica di sistemi algoritmici e modelli di intelligenza artificiale senza l'impiego diretto di dati personali reali. Il noto riferimento contenuto nel Data Governance Act (Considerando 7) e nell'AI Act (artt. 10 e 59) si inserisce, dunque, in una logica di regolazione prudenziale, nella quale la sperimentazione tecnologica è ammessa solo se accompagnata da presidi idonei a garantire proporzionalità, sicurezza e rispetto delle garanzie fondamentali.

⁵⁷ Sull'approccio umano-centrico, risulta altamente calzante la riflessione di A. ALPINI, *Sull'approccio umano-centrico all'intelligenza artificiale. Riflessioni a margine del progetto europeo di orientamenti etici per una IA affidabile*, in www.comparazionedirittocivile.it, aprile 2019, 1 ss.

sistemi. Tale disciplina si integra con il tema del secondary use: i dati riutilizzati per sviluppare modelli devono rispettare vincoli di non discriminazione e supervisionabilità, pena la perdita di legittimazione dell'intero circuito informativo.

Nel complesso, l'art. 8 della l. 132/2025 – letto in connessione con il nuovo art. 110 Codice Privacy e con il quadro delineato da EHDS, AI Act e Data Governance Act⁵⁸ – realizza un duplice obiettivo: da un lato, semplificare le condizioni per il riutilizzo dei dati sanitari, aprendo la strada a una più ampia disponibilità di informazioni per ricerca e governance⁵⁹; dall'altro, consolidare un

⁵⁸ Sul Data Governance Act e sui riflessi che questo ha avuto in tema di *data protection* vale la pena richiamare, A. MORACE PINELLI, *Dalla Data Protection alla Data Governance: il Regolamento (UE) 2022/868 - Commentario al Data Governance Act*, a cura di A. Morace Pinelli, Pisa, 2024.

⁵⁹ Un bilanciamento analogo tra promozione della ricerca e tutela dei diritti fondamentali può essere rinvenuto anche nell'ambito del diritto d'autore. In tale prospettiva si colloca la decisione del Landgericht Hamburg, *Robert Kneschke c. LAION e.V.*, n. 310 O 227/23, 27 settembre 2024, nella quale è stata affermata la legittimità dell'utilizzo di opere protette ai fini di text and data mining per l'addestramento di sistemi di intelligenza artificiale, in quanto coperto dall'art. 60d dell'Urheberrechtsgesetz tedesco e dall'art. 3 della dir. 2019/790. Il giudice ha qualificato la costruzione di dataset come fase preliminare e funzionalmente necessaria dell'attività di ricerca scientifica, valorizzando un impianto normativo che, pur operando in un settore distinto, risponde a una logica di temperamento tra innovazione tecnologica e salvaguardia delle posizioni individuali. In una prospettiva europea, la medesima tensione tra tutela delle posizioni individuali e interesse collettivo alla ricerca emerge anche in alcuni dei primi contenziosi relativi all'impiego di opere protette nell'addestramento di sistemi di intelligenza artificiale mediante archivi open source, come nel noto caso Stable Diffusion. In tali vicende, i giudici hanno valorizzato un approccio dinamico al bilanciamento tra diritti patrimoniali e morali degli autori, da un lato, ed esigenze della ricerca e dell'innovazione dall'altro, ammettendo l'uso di opere coperte da diritto d'autore nel rispetto delle condizioni previste dalla disciplina sul text and data mining. La vicenda può essere letta come un leading case in senso funzionale, che – pur collocandosi nel diritto d'autore – offre un termine di raffronto utile per comprendere come anche in ambito sanitario il riutilizzo dei

sistema di garanzie fondato su trasparenza, supervisione umana e responsabilità istituzionale. La norma si propone così come cerniera tra livello nazionale e sovranazionale e come occasione per sperimentare bilanciamenti innovativi tra tutela della persona e interesse pubblico.

Pur trattandosi, per larga parte, di disposizioni immediatamente applicabili, l'effettiva operatività di alcuni profili della disciplina – in particolare quelli relativi agli standard tecnici e alle procedure di riuso – resta condizionata all'adozione di atti attuativi e di indirizzo nei termini stabiliti. Solo tali atti potranno chiarire il coordinamento concreto con il Regolamento EHDS e con il quadro del GDPR, soprattutto con riferimento alla definizione di misure tecniche 'adeguate' e alle modalità di controllo e tracciabilità lungo la filiera.

Resta aperto l'interrogativo sulla reale efficacia delle nuove disposizioni: il passaggio da un modello autorizzatorio a uno fondato sul silenzio-assenso, la centralità attribuita ad Agenas, la valorizzazione dei dati sintetici e il ruolo dei comitati etici delineano un quadro promettente, ma che richiederà applicazione coerente e dialogo costante con l'ordinamento europeo⁶⁰. In assenza di coordinamento, il rischio è che l'innovazione si traduca in un mosaico frammentario, con conseguenze problematiche per certezza del diritto e competitività della ricerca nazionale, nonché in un'indeterminatezza dei parametri di liceità e degli obblighi di

dati a fini scientifici richieda soluzioni di equilibrio tra valorizzazione dell'informazione e tutela delle posizioni soggettive.

⁶⁰ Allo stato, non risulta ancora delineato un meccanismo organico e formalizzato di coordinamento tra l'attuazione interna della l. 132/2025 e l'operatività dell'European Health Data Space. Il richiamo al 'dialogo' con l'ordinamento europeo va pertanto inteso in senso prospettico e sistemico, quale esigenza di interpretazione conforme e di integrazione multilivello tra disciplina nazionale e Regolamenti europei direttamente applicabili.

diligenza lungo la filiera del riuso, compromettendo la stessa chiarezza dei criteri di imputazione della responsabilità.

ABSTRACT

L'analisi prende le mosse dall'analisi dello Spazio Europeo dei Dati Sanitari come snodo centrale della trasformazione del diritto europeo della sanità digitale, concentrandosi in particolare sul regime dell'uso secondario dei dati sanitari per finalità di ricerca scientifica. Muovendo da una prospettiva comparata, il contributo mostra come l'EHDS non si limiti a favorire la circolazione transfrontaliera delle informazioni cliniche, ma introduca un mutamento più profondo nelle condizioni di legittimità del trattamento, segnando il progressivo superamento di un modello fondato esclusivamente sul consenso dell'interessato.

L'attenzione è rivolta ai meccanismi procedurali, infrastrutturali e organizzativi che sorreggono il riuso dei dati – quali interoperabilità, ambienti sicuri, accountability e qualità del dato – e al loro ruolo nel bilanciamento tra tutela dei diritti fondamentali, interesse pubblico e innovazione scientifica. In tale prospettiva, l'uso secondario dei dati sanitari emerge come banco di prova di un nuovo paradigma di legittimazione, nel quale la protezione della persona è affidata non solo a presupposti soggettivi, ma a garanzie sistemiche e multilivello.

The analysis begins with the European Health Data Space as a central driver of the transformation of European digital health law, with a particular focus on the legal regime governing the secondary use of health data for scientific research purposes. Adopting a comparative perspective, the analysis shows that the European Health Data Space does not merely facilitate the cross-border circulation of clinical information, but rather introduces a deeper

shift in the conditions underpinning the legitimacy of data processing, highlighting the gradual move beyond a model based exclusively on the data subject's consent.

The discussion focuses on the procedural, infrastructural and organizational mechanisms supporting data reuse – such as interoperability, safe processing environments, accountability frameworks and data quality – and on their role in balancing the protection of fundamental rights, public interest objectives and scientific innovation. From this perspective, the secondary use of health data emerges as a testing ground for a new paradigm of legitimacy, in which the protection of individuals not only relies on subjective grounds, but on systemic and multi-level safeguards.

PAROLE CHIAVE

Spazio Europeo dei Dati Sanitari – sanità digitale – Intelligenza Artificiale in sanità – protezione dei dati – uso secondario dei dati sanitari

European Health Data Space – digital health – data protection – artificial intelligence in healthcare – secondary use of health data

CIRO MARIA RUOCCO
ciruocco@unisa.it

(online dal 25/06/2026)