

# Comparative Law Review

Vol. 17 · No. 2  
2026



REGULAR ISSUE

ISSN 2038 – 8993

## COMPARATIVE LAW REVIEW

The Comparative Law Review is a biannual journal published by the  
I. A. C. L. under the auspices and the hosting of the University of Perugia Department of Law.

Office address and contact details:  
Email: [complawreview@gmail.com](mailto:complawreview@gmail.com)

## EDITORS

Giuseppe Franco Ferrari  
Tommaso Edoardo Frosini  
Pier Giuseppe Monateri  
Giovanni Marini  
Salvatore Sica  
Alessandro Somma  
Massimiliano Granieri

## EDITORIAL STAFF

Fausto Caggia  
Giacomo Capuzzo  
Cristina Costantini  
Virgilio D'Antonio  
Sonja Haberl  
Edmondo Mostacci  
Alessandra Pera  
Giacomo Rojas Elgueta  
Tommaso Amico di Meane  
Lorenzo Serafinelli

## REFEREES

Salvatore Andò  
Elvira Autorino  
Ermanno Calzolaio  
Diego Corapi  
Giuseppe De Vergottini  
Tommaso Edoardo Frosini  
Fulco Lanchester  
Maria Rosaria Marella  
Antonello Miranda  
Elisabetta Palici di Suni  
Giovanni Pascuzzi  
Maria Donata Panforti  
Roberto Pardolesi  
Giulio Ponzanelli  
Andrea Zoppini  
Mauro Grondona  
Biagio Andò  
Marina Timoteo

## SCIENTIFIC ADVISORY BOARD

Christian von Bar (Osnabrück)  
Thomas Duve (Frankfurt am Main)  
Erik Jayme (Heidelberg)  
Duncan Kennedy (Harvard)  
Christoph Paulus (Berlin)  
Carlos Petit (Huelva)  
Thomas Wilhelmsson (Helsinki)

COMPARATIVE  
LAW  
REVIEW  
VOL. 17/2 - 2026

5

VINCENZO ZENO-ZENCOVICH

For a Theory of Duties: A Roadmap

12

ALESSANDRO SOMMA

Tra moderno e postmoderno: ha ancora senso discutere di una funzione sovversiva della comparazione giuridica?

39

ENRICO BAFFI

Mistake as a Defect of Consent: Strengths and Weaknesses of the Italian Rules Compared with the U.S. Approach

67

MOHAMMED ABDELAAL

Beyond Borders: The Reception Of Foreign Law In The Jurisprudence Of Egypt's Supreme Constitutional Court

*Spazio europeo dei dati sanitari*

121

MARIO NATALE - ONOFRIO TROIANO

L'ambito di applicazione oggettivo e soggettivo del Regolamento (UE) 2025/327 sullo Spazio Europeo dei Dati Sanitari.

149

LUCIA BOZZI

Uso primario dei dati e fascicolo sanitario elettronico: non è solo una questione di privacy...

175

ADRIANA ADDANTE

Vicende circolatorie ed esercizio dei diritti nell'uso primario dei dati sanitari

205

VALENTINA VINCENZA CUOCCI

Spazio Europeo dei Dati Sanitari: uso secondario dei dati sanitari elettronici e interesse generale alla ricerca

230

MARIELLA CUCCOVILLO

Uso secondario dei dati sanitari e tutela dell'interessato: tra rimedi e sanzioni

246

MIRIAM I. NIGRO DI GREGORIO – ALESSIA P. MANGIACOTTI

Il sistema sanzionatorio dell'*European Health Data Space*: tra armonizzazione e frammentazione normativa.

270

ROBERTA PICCOLO

Biobanche sotto esame: dall'incertezza giuridica alla prospettiva regolatoria.



## SPAZIO EUROPEO DEI DATI SANTARI



SPAZIO EUROPEO DEI DATI SANITARI:  
USO SECONDARIO DEI DATI SANITARI ELETTRONICI E INTERESSE GENERALE  
ALLA RICERCA

*Valentina Vincenza Cuocci\**

SOMMARIO:

I. DATI RELATIVI ALLA SALUTE E RICERCA SCIENTIFICA. UNA MAPPA RICOSTRUTTIVA ALLA LUCE DEL REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI E DEL CODICE PRIVACY. II. SPAZIO EUROPEO DEI DATI SANITARI E USO SECONDARIO: L'APPROCCIO PUBBLICISTICO E L'INTERESSE GENERALE ALLA RICERCA IN AMBITO SANITARIO. II.1 DIGRESSIONI ATTORNO ALLE BASI GIURIDICHE PER L'USO SECONDARIO DEI DATI SANITARI ELETTRONICI E IL SUPERAMENTO DEL CONSENSO. II.2. LO STATUTO SPECIALE DEI DATI SANITARI ELETTRONICI (PER USO SECONDARIO). II.3. USO SECONDARIO DEI DATI SANITARI ELETTRONICI TRA FINALITÀ (CONSENTITE) E DIVIETI. III. DIRITTO DI ESCLUSIONE E USO SECONDARIO DEI DATI SANITARI PERSONALI ELETTRONICI. LA RIEMERSONE DELLE PROBLEMATICHE LEGATE AL CONSENSO? IV. USO SECONDARIO E SPERIMENTAZIONE SCIENTIFICA PER LA REALIZZAZIONE DI SISTEMI DI INTELLIGENZA ARTIFICIALE IN AMBITO SANITARIO NELLA LEGGE ITALIANA SULL'INTELLIGENZA ARTIFICIALE E NEL REGOLAMENTO SULLO SPAZIO EUROPEO DEI DATI SANITARI. TRA COMPLESSITÀ E FRAMMENTAZIONE DELLE FONTI.

*Il contributo analizza l'uso secondario dei dati sanitari personali elettronici alla luce del nuovo quadro delineato dal Regolamento sullo Spazio europeo dei dati sanitari (EHDS), soffermandosi sul progressivo superamento del consenso quale base giuridica del trattamento. Il contributo affronta, altresì, il tema dell'utilizzo dei dati sanitari per finalità di ricerca e sviluppo di sistemi di intelligenza artificiale, evidenziando alcune criticità derivanti dalla frammentazione delle fonti normative tra diritto nazionale e diritto dell'Unione europea. Ne emerge un quadro complesso nel quale l'esigenza di promuovere l'innovazione tecnologica e la ricerca si confronta con la necessità di assicurare un elevato livello di protezione dei diritti fondamentali.*

**Keywords:** Spazio Europeo dei Dati Sanitari - Dati Sanitari Elettronici  
- Uso secondario - Ricerca scientifica - Intelligenza Artificiale

I. DATI RELATIVI ALLA SALUTE E RICERCA SCIENTIFICA. UNA MAPPA RICOSTRUTTIVA ALLA LUCE DEL REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI E DEL CODICE PRIVACY

Il rapporto tra ricerca scientifica e protezione dei dati relativi alla salute sottende un difficile bilanciamento tra valori fondamentali parimenti meritevoli di tutela: da un lato, la ricerca medica che si nutre di dati personali (dati relativi alla salute, dati genomici, dati genetici, dati generati da dispositivi indossabili, dati contenute nelle cartelle cliniche e fascicoli sanitari elettronici), anche grazie all'utilizzo di tecniche di intelligenza artificiale, cerca di migliorare la vita delle persone attraverso nuove scoperte e nuove cure; dall'altro, l'esigenza di protezione (e della riservatezza) dei dati, quale diritto fondamentale di ogni persona<sup>1</sup>.

---

\*Il presente scritto si inserisce nell'ambito del progetto di ricerca di Ateneo PRA 2023 – Università di Foggia "Health Data: protection and free movement in the digital age".

<sup>1</sup> G.Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer: Dordrecht, 2014; M. Tzanou, *Data protection as a fundamental right next to privacy? 'Reconstructing' a not so new right*, *International Data Privacy Law*, 2013; 3: 88-99.

La normativa europea e la normativa nazionale in materia di protezione dei dati personali – Regolamento Generale sulla Protezione dei Dati Personali (d'ora in poi GDPR) e *Codice Privacy* – consentono, a determinate condizioni, l'uso dei dati personali e delle categorie particolari di dati per finalità di ricerca scientifica/interesse pubblico. Trama normativa, a dire il vero, particolarmente complessa, che presenta non pochi aspetti problematici legati all'uso di alcune basi giuridiche per finalità di ricerca scientifica.

In primo luogo, si evidenzia che la base giuridica del consenso nell'ambito della ricerca medico scientifica ha, da sempre, suscitato qualche perplessità<sup>2</sup>: il consenso raccolto in contesti di vulnerabilità (come nel caso dei pazienti) non potrebbe configurarsi come un consenso libero (ai sensi delle linee guida sul consenso adottate dallo EDPB)<sup>3</sup> poiché potrebbe innescarsi uno squilibrio tra l'interessato (paziente) e il titolare del trattamento. Parimenti suscita qualche perplessità il requisito della specificità e granularità del consenso al trattamento dei dati personali per fini di ricerca scientifica tanto che si è ipotizzata una interpretazione flessibile di tali requisiti ai sensi del considerando n. 33 GDPR<sup>4</sup>. Sulla base di quanto stabilito nel considerando 33 GDPR e nelle linee guida sul consenso sarebbe possibile descrivere la finalità del trattamento in modo generale, ma tale flessibilità potrebbe venir meno quando si tratta di categorie particolari di dati di cui all'art. 9 GDPR<sup>5</sup> e, quindi, - come nel caso che qui interessa - di dati relativi alla salute. Ove si verta in quest'ultima ipotesi, le linee guida sul consenso precisano che l'applicazione dell'approccio flessibile di cui al considerando 33 GDPR sarà soggetta a un'interpretazione più rigorosa

---

Sull'uso secondario dei dati per finalità di ricerca scientifica: F. Cascini, M.A. Arcuri, *Uso secondario dei dati personali relativi alla salute: panoramica della normativa europea e nazionale*, in *Dir. Inf.*, 2024, 837.AA.VV., *Ricerca in sanità e protezione dei dati personali. Scenari applicativi e prospettiva future*, (a cura di) P. Guarda, E. Chizzola, V. Maroni, L. Rufo, Napoli, 2024, 1-169. C. Perlingieri, *eHealth and Data*, in *Privacy and Data Protection in Software services*, (a cura di) R. Senigaglia, C. Irti e A. Bernes, Springer ed., 2021, 130; I. Rapisarda, *Ricerca scientifica e circolazione dei dati personali*, in *Eur. dir. priv.*, 2021, 326. R. Sharma, N. Kshetri, *Digital healthcare: Historical development, applications, and future research directions*, in *International Journal of Information Management* 53 (2020) 102-105; L. Stephanie, S. Sharma, *Digital health eco-systems: An epochal review of practice-oriented research*, in *International Journal of Information Management* 53 (2020) 102032. G. Capilli, *Digital Twin in sanità: innovazioni, opportunità e sfide giuridiche*, in *Rivista Italiana di Medicina Legale (e del Diritto in campo sanitario)*, 2024, 527.

<sup>2</sup> D. J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 *Harvard Law Rev.* 1880 (2013).

C. Lazaro, D. le Metayer, *Consent to Personal Data Processing: A Comparative Perspective on Data Subject's Autonomy*, 48 *Revue Juridique Themis* 765 (2014). Gli Autori parlano di «*fragilisation de la force normative du consentement*». Vedi anche: C. Lazaro, D. le Metayer, *The Control over Personal Data: True Remedy or Fairy Tale?*, 2015, 1-25, <https://arxiv.org/ftp/arxiv/papers/1504/1504.03877.pdf>.

In chiave critica sul consenso come base giuridica del trattamento: L. Gatt, I.A. Caggiano, R. Montanari, *Privacy and Consent. A Legal and UX & HMI Approach for Data Protection*, Napoli, 2021, 1; L. Gatt, I.A. Caggiano, R. Montanari, *Consenso al trattamento dei dati personali e analisi giuridico-comportamentale, Spunti di riflessione sull'effettività della tutela dei dati personali*, in (a cura di) P. Passaglia, D. Poletti, *Nodi virtuali, Legami informali: Internet alla ricerca di regole*, Pisa, 2016, 57. L. Bozzi, *La protezione dei dati personali del minore in ambito scolastico. Educare alla privacy. Non solo consentire al trattamento*, in (a cura di) S. Delle Monache, G. Gabrielli, *I maestri del diritto civile. Alberto Trabucchi*, Napoli, 2021, 207. Alcuni autori hanno messo in rilievo che il consenso conferisce solo una «illusione» sul controllo delle proprie informazioni. L. Brandimarte, A. Acquisti, G. Loewenstein, *Misplaced Confidences*, 4(3) *Social Psychological and Personality Science* 340 (2013). A. Marwick, D. Boyd, *Networked Privacy: How Teenagers Negotiate Context in Social Media*, 16(7) *New Media & Society* 1051 (2014). Si veda il contributo di S. Orlando, *Libertà e liceità del consenso nel trattamento dei dati personali*, in *Persona e Mercato*, 2024, 39.

<sup>3</sup> [https://www.edpb.europa.eu/sites/default/files/files/file1/edpb\\_guidelines\\_202005\\_consent\\_it.pdf](https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_it.pdf)

<sup>4</sup> Considerando 33 GDPR.

<sup>5</sup> Sul punto si vedano le osservazioni di G. Comandè, *Ricerca in sanità e data protection...un puzzle risolvibile*, in *Riv. It. Medicina legale*, 2019, 195.

e ad un elevato livello di controllo e, quando non è possibile specificare la finalità della ricerca, il titolare dovrebbe individuare altri modi per garantire il rispetto dell'essenza dei requisiti del consenso, ad esempio permettendo agli interessati di acconsentire a una finalità di ricerca in termini prima più generali e, poi, a fasi specifiche e progressive (mano a mano che la ricerca avanza, sarà necessario ottenere un nuovo consenso per ognuna delle fasi successive del progetto e, in ogni caso, prima dell'inizio della fase corrispondente).

Il consenso, inoltre, dovrebbe essere in linea con le norme deontologiche applicabili alla ricerca scientifica nel rispetto delle garanzie previste dall'art. 89, par. 1 GDPR (si possono individuare come possibili garanzie la minimizzazione dei dati, l'anonimizzazione e sicurezza).

In ogni caso il 'broad consent' come anche il consenso a fasi progressive sono strumenti 'pericolosi' e, certamente, non risolvono il problema del trattamento dei dati per finalità di ricerca scientifica per due ragioni essenziali: la prima, la vaghezza della nozione di consenso ampio potrebbe innescare comportamenti opportunistici da parte del titolare del trattamento (ricordiamo che la l'indicazione della finalità e il principio di limitazione sono il primo baluardo della protezione dei dati); la seconda, il consenso a fasi progressive non risulta di semplice ed agevole applicazione sul piano pratico della ricerca (pensiamo ad una ricerca che vede coinvolto un numero elevato di persone che dovranno essere di volta in volta ricontattate per esprimere il consenso per la fase successiva della ricerca)<sup>6</sup>.

Non solo. Il consenso è sempre revocabile (art. 7, par 3, GDPR)<sup>7</sup>: il dato non sarebbe più utilizzabile qualora l'interessato decidesse, appunto, di revocare il consenso con un impatto negativo sugli esiti della ricerca stessa<sup>8</sup>. Inoltre, se la base giuridica utilizzata per la finalità principale è il consenso, allora il titolare dovrebbe, ai sensi dell'art. 13, par. 3, informare l'interessato delle finalità ulteriori (rispetto a quelle per le quali i dati sono stati raccolti) e l'interessato, ricevuta l'informativa relativa al trattamento ulteriore dei dati, potrebbe esercitare il suo diritto di opposizione, con impatto negativo sugli esiti della ricerca<sup>9</sup>.

Le menzionate criticità portano a valorizzare le altre basi giuridiche individuate nel GDPR che, in qualche misura, si sganciano dal meccanismo privatistico del consenso, quale espressione di autodeterminazione, e guardano ad un meccanismo pubblicistico/regolatorio che considera il dato personale in chiave solidaristica (i dati sono necessari per l'avanzamento della ricerca e per l'interesse generale)<sup>10</sup>.

<sup>6</sup> D. Sborlini, *Il broad consent come mezzo per la valorizzazione dei dati personali nell'ambito della ricerca scientifica e il suo rilievo negli spazi di condivisione dei dati*, in *Contratto e Impresa*, 2024, 223.

<sup>7</sup> Linee Guida sul Consenso n. 5/2020 punto 162

<sup>8</sup> Si veda sul punto il parere EDPB 3/2019 relativo alle domande e risposte sull'interazione tra il regolamento sulla sperimentazione clinica e il regolamento generale sulla protezione dei dati (articolo 70, paragrafo 1, lettera b)). Il parere è reperibile al seguente link [https://www.edpb.europa.eu/sites/default/files/files/file1/cdpb\\_opinionctrq\\_a\\_final\\_it.pdf](https://www.edpb.europa.eu/sites/default/files/files/file1/cdpb_opinionctrq_a_final_it.pdf)

<sup>9</sup> Si veda: Arcuri, Cascini, *Uso secondario*, cit., 847.

<sup>10</sup> Si evidenzia che il Data Governance Act valorizza, in qualche misura, il riutilizzo dei dati per finalità di ricerca scientifica senza introdurre una specifica base per l'uso secondario dei dati. Il DGA promuove l'altruismo dei dati. Il testo del Data Governance Act: <https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32022R0868>.

Lungo questo sentiero analizziamo la complessa trama del Regolamento Generale sulla Protezione dei Dati che consente il trattamento dei dati per finalità diverse da quelle per cui i dati sono stati raccolti. Il punto da cui partire è l'art. 5 GDPR che, letto alla luce del Considerando 50, considera lecito un trattamento ulteriore dei dati personali ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica a fini statistica in conformità all'art. 89 GDPR. La finalità di ricerca scientifica non è considerata incompatibile con le finalità iniziali<sup>11</sup>. Il trattamento ulteriore di dati personali, per finalità diverse da quelle per le quali i dati personali sono stati inizialmente raccolti, risulta lecito ove non in contrasto con le finalità per le quali i dati personali sono stati inizialmente raccolti senza una necessaria ulteriore base giuridica<sup>12</sup>.

A tale principio generale si affianca il combinato disposto contenuto nell'art. 6, paragrafo 4, e nell'art. 9, paragrafo 2, del GDPR, secondo cui è lecito il trattamento delle categorie particolari di dati personali - tra cui figurano quelli relativi alla salute ed i dati genetici -, in assenza del consenso, quando sussistono motivi di interesse pubblico rilevante sulla base del diritto dell'Unione Europea o degli Stati che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali del *data subject* (art. 9, GDPR lett. g); quando sussistono motivi di interesse pubblico e fini di ricerca scientifica o statistica di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato (art. 9 GDPR, lett. j)<sup>13</sup>. Non è ben chiaro come debba intendersi il riferimento all' "essenza della normativa sulla protezione dei dati personali" (art. 9, paragrafo 2, lettera g e j): la dottrina ha interpretato "l'essenza della normativa dei dati personali" alla luce dell'art. 8 della Carta dei Diritti Fondamentali dell'Unione Europea e, ritenendo, quindi, che la normativa non dovrebbe limitarsi a riconoscere l'interesse pubblico al trattamento dei dati ma dovrebbe rispettare i requisiti di liceità, correttezza e limitazione delle finalità<sup>14</sup>. Tale opzione ermeneutica dovrebbe essere arricchita e ricomprendere il principio di accountability e cioè della responsabilizzazione del titolare. L'art. 9 GDPR lett. i invece consente il trattamento delle categorie particolari di dati, tra cui appunto i dati relativi alla salute, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato per motivi di interesse pubblico

---

Tra i numerosi commenti sul DGA: A. Morace Pinelli, *Dalla Data Protection alla Data Governance: il Regolamento UE 2022/86*, in *Nuove leggi civ. comm.*, 2024, 486. AA.VV., *Dalla «Data Protection» alla «Data Governance»: il regolamento (UE) 2022/868. Commentario al «Data Governance Act»*, (a cura di) A. Morace Pinelli 2024, 1-520.

<sup>11</sup> Vedi: Cascini, Arcuri, *Uso secondario dei dati personali*, cit., 844.

<sup>12</sup> Sul regime giuridico dei dati per ricerca scientifica: P. Guarda, *Il regime giuridico dei dati della ricerca scientifica*, Trento, 2021, 1 e ss.

Il Considerando 50 GDPR considera lecito e compatibile l'ulteriore trattamento a fini di archiviazione nel pubblico interesse, o di ricerca scientifica o storica o a fini statistici.

<sup>13</sup> Si veda il pensiero critico di M. Granieri, *Il trattamento di categorie particolari di dati personali nel Reg. UE 2016/679*, in *Nuove leggi civ. comm.*, 2017, 165-190. Risalente ma sempre interessante il riferimento a: V. Zambrano, *Dati sanitari e tutela della sfera privata*, in *Dir. informatica*, 1999, 1, p. 1 e ss.

<sup>14</sup> In tal senso Comandè, *Ricerca in sanità e data protection*, cit., 195.

nel settore della sanità pubblica<sup>15</sup>. In quest'ultima ipotesi non vi è, come nelle lettere g e j, il riferimento al rispetto dell'essenza della normativa sulla protezione dei dati personali, quanto a dire che potrebbe anche non essere rispettata l'essenza della normativa sulla privacy? I dubbi permangono.

Sulla complessa architettura europea si innesta la normativa nazionale - il d.lgs del 10 agosto 2018, e successive modifiche ed integrazioni che ha adeguato il codice privacy alle disposizioni contenute nel Regolamento 2016/679<sup>16</sup> -. Nello specifico si richiama l'art. 2 sexies Codice Privacy<sup>17</sup> - 'Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante - che ha introdotto una specifica base giuridica per il trattamento delle categorie particolari di dati di cui all'art. 9, paragrafo 1, per motivi di interesse pubblico di cui all'art. 9, paragrafo 2, lettera g, GDPR, anche per l'uso relativo programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, ivi incluse l'instaurazione, la gestione, la pianificazione e il controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati con il servizio sanitario nazionale; z) vigilanza sulle sperimentazioni, farmacovigilanza, autorizzazione all'immissione in commercio e all'importazione di medicinali e di altri prodotti di rilevanza sanitaria come anche per trattamenti effettuati a fini di archiviazione nel pubblico interesse o di ricerca storica, concernenti la conservazione, l'ordinamento e la comunicazione dei documenti detenuti negli archivi di Stato negli archivi storici degli enti pubblici, o in archivi privati dichiarati di interesse storico particolarmente importante, per fini di ricerca scientifica, nonché per fini statistici da parte di soggetti che fanno parte del sistema statistico nazionale (così art. 2 sexies lettera v, lettera z e lettera cc). Tale articolo, dunque, consente l'utilizzo delle categorie particolari di dati per fini ricerca scientifica, epidemiologia e statistica.

Con specifico riferimento al trattamento dei dati relativi alla salute per finalità di ricerca scientifica è certamente utile analizzare l'art. 110 Codice Privacy : non è necessario il consenso dell'interessato per il trattamento dei dati relativi alla salute per finalità di ricerca scientifica in campo medico, biomedico o epidemiologico quando la ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea in conformità all'articolo 9, paragrafo 2, lettera j), e cioè quando il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato ed è stata effettuata una valutazione di impatto ai sensi dell'art. 35 GDPR. Il consenso, inoltre, non è necessario quando sulla base di particolari ragioni è impossibile informare gli interessati o implica uno sforzo sproporzionato, oppure rischia

<sup>15</sup> Così l'art. 6, comma 4, GDPR.

<sup>16</sup> G.U., Serie Generale, 4 settembre 2018, n. 205. Ulteriori modifiche sono state introdotte dal decreto-legge 2 marzo 2024, n. 19, convertito, con modificazioni dalla legge 29 aprile 2024, n. 56.

Con riferimento all'adeguamento della disciplina nazionale al GDPR: S. Messina, *L'adeguamento della normativa nazionale al Regolamento, in I dati personali nel diritto europeo*, (a cura di) V. Cuffaro, R. D'Orazio, V. Ricciuto, Torino, 2019, 119.

<sup>17</sup> Si veda la modifica introdotta dal decreto-legge 2 marzo 2024, n. 19, convertito, con modificazioni dalla legge 29 aprile 2024, n. 56.

di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca.

Nella precedente versione dell'art. 110 Codice Privacy, nelle ipotesi in cui non veniva raccolto il consenso, il programma di ricerca doveva essere sottoposto ad autorizzazione preventiva del Garante per la Protezione dei Dati Personali. L'autorizzazione preventiva di carattere pubblicistico regolatorio veniva vista come 'sostitutiva' del consenso e volta a rendere lecito il trattamento dei dati nel rispetto delle garanzie previste dalla normativa nazionale ed europea.

Di recente è entrata in vigore una modifica dell'art. 110 Codice Privacy: l'autorizzazione preventiva del Garante Privacy è stata sostituita dall'individuazione da parte del Garante Privacy di garanzie da osservare<sup>18</sup>. Il provvedimento del Garante Privacy ha individuato garanzie specifiche per i dati delle persone decedute, delle persone c.d. non contattabili per motivi etici (l'informazione potrebbe provocare danni psichici o anche materiali) ed organizzativi (non è possibile contattare tutti gli interessati per via della numerosità del campione o dati di contatto non aggiornati).

Il titolare del trattamento deve effettuare una valutazione di impatto ai sensi dell'art. 35 GDPR, quando i dati riguardano persone decedute e non contattabili, da comunicare al Garante; deve adottare misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, e acquisire il parere favorevole del competente comitato etico a livello territoriale sul progetto di ricerca come previsto dall'art. 110 del Codice; deve motivare nel progetto di ricerca le ragioni etiche o organizzative per le quali informare gli interessati e, quindi, acquisire il consenso, risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di compromettere il conseguimento delle finalità della ricerca, se del caso documentando i ragionevoli tentativi di contatto<sup>19</sup>.

Quest'ultima modifica dell'art. 110 Codice Privacy non prevede più l'autorizzazione preventiva del Garante, ma il rispetto delle misure di garanzie individuate nel provvedimento sopra menzionato, e sembra aver semplificato la procedura di uso dei dati per finalità di ricerca scientifica<sup>20</sup>.

Tale modifica riesce ad agevolare gli studi retrospettivi e in casi in cui risulta impossibile contattare gli interessati.

Un'ultima riflessione, infine, sull'art. 110 bis Codice Privacy – che regola la diversa ipotesi di trattamento ulteriore dei dati da parte di terzi, per fini di ricerca scientifica quando non è possibile informare direttamente gli interessati o quando l'informazione potrebbe compromettere gli esiti della ricerca – che prevede la richiesta di autorizzazione al Garante

---

<sup>18</sup> L'art. 110 Codice Privacy è stato modificato dall'art. 44, comma 1-bis, d.l. 2 marzo 2024, n. 19, convertito, con modificazioni, dalla L. 29 aprile 2024, n. 56.

<sup>19</sup> Il provvedimento può essere consultato sul sito ufficiale del Garante per la Protezione dei Dati Personali: <https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10016146>

<sup>20</sup> Vedi: Arcuri, Cascini, *Uso secondario*, cit., 870. Vedi anche: V. Fusco, *Il trattamento di dati personali per l'addestramento di sistemi di intelligenza artificiale in ambito medico: criticità del consenso e basi giuridiche alternative*, in *Riv. It. Med. Legale*, 2025, 85.

M. Liotta, *Il favor per la ricerca scientifica e la sua effettiva applicazione nella normativa europea, nazionale e da parte dell'Autorità Garante*, in *Dir. Inf.*, 2024, 363.

Privacy. La richiesta, nel rispetto dei requisiti previsti dall'art. 89 GDPR, deve indicare le misure di protezione adottate - pseudonimizzazione e anonimizzazione -.

Il Garante Privacy concede l'autorizzazione, che prevede ulteriori misure di protezione per gli interessati anche in relazione alle categorie particolari di dati, nel termine di 45 giorni; la mancata risposta costituisce una ipotesi di silenzio rigetto. L'art. 110 bis Codice Privacy, nell'introdurre una vera e propria presunzione, precisa senza troppi dubbi che non costituisce ulteriore trattamento di dati quello effettuato da Istituti di Ricovero e Cura a Carattere Scientifico) per finalità di ricerca, se collegato all'attività clinica e nel rispetto delle garanzie previste dall'art. 89 del GDPR<sup>21</sup>.

Il quadro normativo sopra descritto suscita alcuni sentimenti contrastanti. Da un lato, va visto con favore il 'declino' del consenso come base giuridica del trattamento dei dati per finalità di ricerca scientifica - in contesti di vulnerabilità come il caso, appunto, di dati personali sanitari raccolti in ospedali case di cura etc. - in favore di un approccio pubblicistico regolatorio che coinvolge i comitati etici e il Garante Privacy (art. 110 Codice Privacy). Dall'altro, suscita qualche perplessità la recente modifica dell'art. 110 Codice Privacy che ha eliminato l'autorizzazione preventiva del Garante Privacy lasciando al titolare del trattamento, pur previa approvazione del comitato etico, l'adozione delle misure di garanzie e di protezione dei dati che devono essere conformi a quelle individuate dal Garante nel provvedimento (sopra menzionato). In buona sostanza il Garante Privacy non opera più un controllo in concreto sulle garanzie adottate da chi intende utilizzare i dati per ricerca scientifica ai sensi dell'art. 110 Codice Privacy ma individua misure di protezione che dovrebbero, auspicabilmente, seguire tutti coloro che intendono utilizzare i dati per ricerca scientifica. La complessa trama normativa sopra descritta pone l'ulteriore aspetto problematico riguardante l'utilizzo dei dati sanitari nei sistemi di intelligenza artificiale e nell'addestramento degli algoritmi, finalità non espressamente menzionate negli articoli indicati. Vero che il titolare del trattamento è tenuto pur sempre ad effettuare una valutazione d'impatto, ai sensi dell'art. 35 GDPR, che diviene obbligatoria nei casi in cui i dati siano trattati mediante nuove tecnologie (come appunto IA) ma, certamente, non risolve il problema della finalità per addestramento di algoritmi e sistemi di intelligenza artificiale.

## II. SPAZIO EUROPEO DEI DATI SANITARI E USO SECONDARIO: L'APPROCCIO PUBBLICISTICO E L'INTERESSE GENERALE ALLA RICERCA IN AMBITO SANITARIO.

I dati sanitari rappresentano una linfa vitale per il miglioramento dei servizi sanitari digitali, per la ricerca medica e scientifica anche alla luce dell'evoluzione delle tecniche di intelligenza artificiale<sup>22</sup>. Non a caso, l'Organizzazione Mondiale della Sanità ha

<sup>21</sup> S. Melchionna, F. Cecamore, *Le nuove frontiere della sanità e della ricerca scientifica*, in *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 679/2016 (GDPR) e al novellato d.lgs 101/2018 (Codice Privacy)*, Milano, 2019, 579. A. Thiene, *Protezione dei dati sensibili e uso di App per il benessere delle donne. Una questione di consapevolezza*, in *BioLaw Journal- Rivista di BioDiritto*, 2023, fasc. 3, 65 ss.

<sup>22</sup> Esistono una pluralità di documenti che mettono in evidenza l'importanza dell'uso dei sistemi di intelligenza artificiale nel settore sanitario. Sul punto può certamente richiamarsi il libro Bianco dell'Unione

sottolineato che i dati - più correttamente la conoscenza derivante dall'uso dei dati - dovrebbero essere considerati come beni pubblici a livello globale e che dovrebbe essere incentivata la condivisione e il riutilizzo dei dati sanitari in modo efficace, etico ed equo in una logica volta al miglioramento della salute pubblica<sup>23</sup>.

Il rapporto tra ricerca scientifica e dati personali descritto nel paragrafo che precede è destinato a mutare alla luce dell'approvazione del Regolamento sullo Spazio Europeo dei Dati Sanitari (*European Health Data Space*, d'ora in poi EHDS)<sup>24</sup>. Il Regolamento EHDS

Europea che già dal 2020 metteva in rilievo l'importanza dei sistemi di intelligenza artificiale in ambito sanitario

([https://commission.europa.eu/document/download/d2ec4039-c5be-423a-81ef-b9e44e79825b\\_it?filename=commission-white-paper-artificial-intelligence-feb2020\\_it.pdf](https://commission.europa.eu/document/download/d2ec4039-c5be-423a-81ef-b9e44e79825b_it?filename=commission-white-paper-artificial-intelligence-feb2020_it.pdf)). Più di recente anche il documento dell'OCSE del 17 gennaio 2024 mette in rilievo benefici e rischi dell'IA nel settore sanitario:

AI in Health: Huge potential, Huge Risks: [https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/01/ai-in-health-huge-potential-huge-risks\\_ff823a24/2f709270-en.pdf](https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/01/ai-in-health-huge-potential-huge-risks_ff823a24/2f709270-en.pdf). Nel documento si legge altresì che il 97 % dei dati viene non viene utilizzato per decisioni cliniche ed invece potrebbe essere utilizzato per addestrare gli algoritmi in chiave di medicina personalizzata e di prevenzione.

M. Mostert, A.L., Brendord, M.C.I.H. Biesart, J.J.M. Van Delden, *Big Data in medical research and EU data protection law: challenges to the consent or anonymise approach*, in *Eur J. Hum Genet*, 2016; 24: 956-960.

<sup>23</sup> Si veda il documento dell'Organizzazione Mondiale della Sanità "Global Strategy on Digital Health 2020–2025". Il documento è reperibile al seguente link: <https://iris.who.int/bitstream/handle/10665/344249/9789240020924-eng.pdf?sequence=1>

F. Cascini, *Secondary Use of Electronic Health Data*, Springer, 2025, 51.

<sup>24</sup> Regolamento (UE) 2025/327 del Parlamento europeo e del Consiglio, dell'11 febbraio 2025, sullo spazio europeo dei dati sanitari e che modifica la direttiva 2011/24/UE e il regolamento (UE) 2024/2847, GUUE, 5 marzo 2025, 327/L. E. Calzolaio, *Il Regolamento sullo Spazio Europeo dei Dati Sanitari nella prospettiva della cittadinanza europea*, in *Dir. Informatica inf.*, 2025, 315; A. Morace Pinelli, *Lo spazio europeo dei dati sanitari*, in *Nuova giur. civ. comm.*, 2025, 106. M. Iaselli, *Le nuove regole per l'uso primario e secondario dei dati sanitari*, Maggioli Editore, 2025, 1-167; S. Navas Navarro, *Datos sanitario Electrónicos. El espacio europeo de datos sanitarios*, Madrid, 2023. S. Corso, *Lo spazio europeo dei dati sanitari. Prime riflessioni sul Regolamento UE 2025/327*, *Nuove leggi civ. comm.*, 2025, 56; Aa.Vv., *Sanità digitale Regolamento "EHDS" (UE 2025/327) sullo spazio europeo dei dati sanitari*, (a cura di) A. Morace Pinelli, Pisa, 2025, 1 e ss.

Regolamento 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) GUUE, 4 maggio 2016, L-119, 1. La letteratura formatasi intorno al Regolamento è sterminata, sia a livello nazionale che europeo. Si segnalano alcuni scritti: A.A.VV., *I dati personali nel diritto europeo*, (a cura di) V. Cuffaro, R. D'Orazio, V. Ricciuto, Torino, 2019, 1- 1427; G. Finocchiaro, *Riflessioni sul poliedrico regolamento europeo sulla privacy*, *Quaderni costituzionali*, 2018, 895; A.A.VV., *Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali*, opera diretta da G. Finocchiaro, Bologna, 2017, 1-764. V. Ricciuto, *L'equivoco della privacy. Persona v.s. Dato Personale*, Napoli, 2022, 1 e 22.

Alcuni riferimenti alla letteratura straniera: A.A.VV., *Data Protection Around the World*, (Eds) E. Kiesow Cortez, The Hague, 2021, 1-279; M. Krzysztosek, *GDPR: General Data Protection Regulation (EU) 2016/679*, Wolter Kluwer, 2019, 1 -319.

Con riferimento al sistema delle fonti prima dell'entrata in vigore del GDPR si segnalano alcuni contributi: A.A.VV., *La protezione dei dati personali - Commentario al d.leg. 30 giugno 2003 n. 196 («codice della privacy»)*, (a cura di) C.M. Bianca e F.D. Busnelli, Padova, 2007, volume I e volume II. A.A.VV., *Diritto alla riservatezza e circolazione dei dati personali*, (a cura di) R. Pardolesi, Milano, 2003, vol.I e vol. II.

Sul Regolamento (UE) 2024/1689 del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale) la bibliografia è alluvionale a livello nazionale ed europeo: R. Pardolesi, *Intelligenza artificiale (de)generativa? Svolazzi a cavallo tra orvietà e disincanto*, in *Foro it.*, 2025, V, 5; S. Orlando, *Sugli inviti rivolti dalla commissione europea all'Italia di modificare il d.d.l. sulla IA relativamente all'utilizzo dei sistemi di IA in ambito sanitario, nelle professioni intellettuali e nell'amministrazione della giustizia*, *id.*, 49; G. Vettori, *La*

nasce dalla necessità di adottare una governance settoriale, specifica e pubblicistica relativa all'uso secondario dei dati sanitari per finalità di ricerca ed innovazione<sup>25</sup>.

Il Regolamento EHDS ambisce, dunque, alla creazione di un ecosistema protetto per l'uso e per lo scambio di dati sanitari elettronici nell'Unione Europea per uso secondario attraverso l'armonizzazione delle regole relative all'accesso e al controllo dei dati sanitari da parte delle persone fisiche ai propri dati sanitari elettronici per consentire, appunto, il riutilizzo di determinati dati per finalità rilevanti di interesse pubblico e di ricerca scientifica<sup>26</sup>.

## II.1 Digressioni attorno alle basi giuridiche per l'uso secondario dei dati sanitari elettronici e il superamento del consenso.

Uno degli aspetti più innovativi del Regolamento EHDS è il c.d. uso secondario dei dati sanitari elettronici e cioè il riutilizzo, affidabile e sicuro, per finalità di ricerca, innovazione, elaborazione delle politiche ed attività regolatorie<sup>27</sup>. Il Regolamento EHDS segna il superamento del consenso quale base giuridica del trattamento per finalità di ricerca scientifica e valorizza un approccio pubblicistico/regolatorio che guarda all'interesse generale per ricerca in ambito sanitario<sup>28</sup> ma pur sempre salvaguardando la riservatezza dei dati.

Il buon funzionamento dello Spazio Europeo dei Dati Sanitari dovrebbe derivare dall'utilizzo di basi giuridiche del trattamento (per uso secondario dei dati sanitari) che si innestano nel quadro generale del Regolamento Generale sulla Protezione dei Dati Personali. Tale spazio dovrebbe costituire un giusto bilanciamento tra gli interessi dei singoli interessati e l'interesse comune della società all'innovazione scientifica.

Proviamo a formulare alcune osservazioni sul tema delle basi giuridiche.

In primo luogo, si evidenzia che il Regolamento EHDS, all' art.51, al fine di agevolare la circolazione e la raccolta di dati sanitari, introduce l'obbligo giuridico per i titolari di dati sanitari elettronici di mettere a disposizione degli Organismi responsabili per l'accesso le categorie di dati sanitari elettronici per uso secondario<sup>29</sup>. Tale obbligo giuridico si configura come base giuridica di cui all'art. 6, paragrafo 1 lett. c ed eccezione al divieto di cui

---

*"crisi del diritto" e il regolamento IA. Un esempio di positivismo inclusivo, id., 12; E. Palmerini, La governance dei sistemi ad alto rischio nell'Artificial Intelligence Act: uno sguardo panoramico, id., 35; S. Pagliantini, La base giuridica dell'AI Act ex art. 114 Tjue: l'intelligenza artificiale tra mercato e persona, id., 19.*

<sup>25</sup> G. Bincoletto, *L'uso secondario di dati sanitari per fini di ricerca scientifica nella telemedicina*, in *Ricerca in sanità e protezione dei dati personali*, in (a cura di) P. Guarda, E. Chizzolla, V. Maroni, L. Rufo, Napoli, 2024, 119. Sulla complessità del sistema delle fonti e delle basi giuridiche per il trattamento dei dati per finalità di ricerca scientifica: Comandè, *Ricerca in sanità e data protection*, cit., 88; AA.VV., *I dati della sperimentazione clinica tra chiusura e apertura della conoscenza scientifica. Filosofia, politica, etica, diritto e prassi*, (a cura di), R. Caso, G. Bincoletto, P. Guarda, Milano, 2026.

<sup>26</sup> Sull'ambito di applicazione del Regolamento EHDS vedi: M. Natale-O. Troiano, *L'ambito di applicazione oggettivo e soggettivo del Regolamento (UE) 2025/327 sullo Spazio Europeo dei Dati Sanitari*, in questa Rivista.

<sup>27</sup> AA.VV., *La protezione dei dati sanitari. Privacy e innovazione tecnologica tra salute e riservatezza* (a cura di A) Thiene, S. Corso, Napoli, 2023, 1 e ss. 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, 485.

<sup>28</sup> S. Thobani, *Il consenso nella regolazione della circolazione dei dati*, in *Persona e mercato*, 2025, 469.

<sup>29</sup> Vedi: R. Ambrosino, *Governance profiles of secondary use of health data in the EHDS*, in *Comparative Law Review*, 2026, 126; M. Cuccovillo, *Uso secondario dei dati sanitari e tutela dell'interessato: tra rimedi e sanzioni*, in questa Rivista.

all'articolo 9, paragrafo 1, GDPR per il trattamento (quindi la messa a disposizione e la fornitura) dei dati sanitari elettronici personali da parte del titolare dei dati. Siffatto obbligo giuridico, tuttavia, non sussiste, ai sensi dell'art. 50, comma 1, EHDS, per le persone fisiche, compresi i ricercatori, e le persone giuridiche che hanno la forma di microimprese ai sensi dell'articolo 2, paragrafo 3, dell'allegato della raccomandazione 2003/361/CE. Si realizza così un doppio binario normativo tra titolari sui quali incombe l'obbligo di mettere a disposizione i dati sanitari e titolari esenti da tale obbligo. Tale frammentazione normativa presenta non pochi riflessi sul piano della certezza del diritto e risulta ulteriormente acuita dal margine di discrezionalità lasciato agli Stati membri che, ai sensi dell'art. 50 comma 2, potrebbero ricomprendere nell'ambito di applicazione del EHDS anche i titolari esclusi dall'art. 50, comma 1. Dunque, l'obbligo dei titolari di mettere a disposizione i dati sanitari potrebbe variare da Stato a Stato con riflessi negativi in termini in termini di armonizzazione che l'EHDS mira a perseguire<sup>30</sup>.

Una volta definita la base giuridica che 'obbliga' i titolari a mettere i dati sanitari a disposizione degli Organismi di accesso, verifichiamo le basi giuridiche che, invece, legittimano il trattamento dei dati per uso secondario.

Su questo aspetto il regolamento EHDS, considerando n. 52, stabilisce che senza ostacolare o sostituire accordi contrattuali o meccanismi di altro tipo in vigore mira a istituire un meccanismo comune di accesso ai dati sanitari elettronici per l'uso secondario in tutta l'Unione. In buona sostanza il Regolamento EHDS segna, come anticipato, il superamento del consenso quale condizione di liceità del trattamento ed individua le basi giuridiche per l'uso secondario dei dati sanitari elettronici personali a norma dell'articolo 9, paragrafo 2, lettere g), h), i) j), GDPR che consente il trattamento di categorie particolari di dati con finalità legittime, governance affidabile per fornire l'accesso ai dati sanitari, attraverso il coinvolgimento di organismi responsabili dell'accesso ai dati sanitari e il trattamento in un ambiente sicuro.

Ai fini del trattamento dei dati sanitari elettronici per l'uso secondario è richiesta una delle basi giuridiche di cui all'articolo 6, paragrafo 1, lettere a), c), e) o f), GDPR in combinato disposto con l'articolo 9, paragrafo 2, GDPR.

Il sistema delineato, dunque, utilizzando la base giuridica dell'art. 6, lett. c, GDPR introduce, per un verso, l'obbligo giuridico per i titolari di dati sanitari elettronici di trasferire siffatti dati agli Organismi per l'accesso; per altro, chi vuole accedere ai dati sanitari elettronici per uso secondario deve in ogni caso dimostrare l'esistenza di una valida base giuridica di cui all'articolo 6, paragrafo 1, lettere a), c), e) o f), GDPR in combinato disposto con l'articolo 9, paragrafo 2, del medesimo regolamento. Di conseguenza, il Regolamento fornisce la base giuridica per l'uso secondario dei dati sanitari elettronici personali, comprese le garanzie richieste a norma dell'articolo 9, paragrafo 2, lettere da g) a j), GDPR.

Le disposizioni sopra menzionate del Regolamento EHDS destano qualche dubbio interpretativo.

---

<sup>30</sup> Si veda il Considerando n. 110 EHDS.

Il Regolamento EHDS esclude il consenso quale base giuridica del trattamento, tanto vero che al considerando n. 52 si legge che gli Stati membri non dovrebbero più poter mantenere o introdurre, a norma dell'articolo 9, paragrafo 4, GDPR, ulteriori condizioni, comprese limitazioni e disposizioni specifiche che richiedono il consenso delle persone fisiche, per quanto riguarda il trattamento per l'uso secondario dei dati sanitari elettronici personali. Viene lasciato, però, un margine di discrezionalità agli Stati membri che, ai sensi dell'art. 51 paragrafo 4, possono introdurre misure più rigorose per talune categorie di dati, considerati particolarmente sensibili, indicati nell'art. 51, paragrafo 1, lettera f), g), i) e q) e, quindi, dati genetici, epigenomici, e genomici umani, altri dati molecolari umani, quali quelli provenienti dalla proteomica, dalla trascrittomica, dalla metabolomica, dalla lipidomica e altri dati omici, dati provenienti dalle applicazioni di benessere, e biobanche. Non è ben chiaro, tuttavia, cosa debba intendersi per misure più rigorose e garanzie supplementari a livello nazionale e cioè se si possa, in particolare, ricomprendere la base giuridica del consenso quale misure più rigorosa.

In ultimo, il Regolamento sembrerebbe far salvi eventuali accordi contrattuali o meccanismi di altro tipo in vigore in tema accesso ai dati sanitari elettronici per uso secondario (considerando n. 52 EHDS). Questa soluzione lascia non pochi spazi di discrezionalità all'autonomia privata che, tramite contratti, potrebbe sottrarsi al sistema pubblicistico regolatorio delineato nel Regolamento EHDS volto a bilanciare l'uso secondario del dato e la riservatezza. Inoltre, non risulta limpido il significato del 'meccanismo di altro tipo'. Il riferimento potrebbe riguardare i meccanismi già previsti nei sistemi nazionali come, ad esempio, quelli previsti dall'art. 110 e 110 bis del Codice Privacy, o a quello previsto dall'art. 8, legge 132/25 (legge italiana sull'intelligenza artificiale).

Nelle prossime pagine analizzeremo alcuni profili relativi all'uso secondario dei dati sanitari elettronici ed alcuni problemi di coordinamento tra la normativa europea in tema di protezione dei dati personali (GDPR) e la legge italiana sull'intelligenza artificiale.

## II.2. *Lo statuto speciale dei dati sanitari elettronici (per uso secondario).*

L'uso secondario è consentito per una particolare categoria di dati: i dati sanitari elettronici. La definizione di dato sanitario elettronico personale è contenuta nell'art. 2, par. 2, lett. a, EHDS - «i dati relativi alla salute e i dati genetici che sono trattati in formato elettronico» - <sup>31</sup> - e non risulta perfettamente sovrapponibile alla definizione di dati relativi alla salute o categorie particolari di dati contenute nel Regolamento Generale sulla Protezione dei Dati Personali<sup>32</sup>.

<sup>31</sup> Si veda l'elenco delle definizioni: art. 2, EHDS.

Sulla definizione di dato sanitario elettronico vedi: L. Bozzi, *Uso primario dei dati e fascicolo sanitario elettronico: non è solo una questione di privacy...*, in questa Rivista. A. Addante, *Vicende circolatorie ed esercizio dei diritti nell'uso primario dei dati sanitari*, in questa Rivista.

<sup>32</sup> Sulla definizione di dato personale è interessante il parere del WP art. 29. <<https://www.garanteprivacy.it/documents/10160/10704/ARTICOLO+29+-+WP+136.pdf>>.

Vedi: R. Ducato, *La crisi di definizione di dato personale nell'era del web 3.0*, in *Le definizioni nel diritto*, 2016, Trento, 149. Sulle categorie particolari di dati tra i numerosi contributi possono qui segnalarsi: Quinn-Malgieri, *The Difficulty of Defining Sensitive Data – The Concept of Sensitive Data in the EU Data Protection Framework*, in *German*

L'EHDS regola, dunque, in modo settoriale l'utilizzo secondario dei soli dati sanitari elettronici personali come dati relativi alla salute e i dati genetici che sono trattati in formato elettronico. Dal tenore letterale e, in particolare, l'utilizzo della congiunzione 'e' che unirebbe due elementi senza esprimere alternative - dato sanitario elettronico personale è il dato relativo alla salute e il dato genetico trattato in forma elettronica - deriva che il solo dato alla salute o il solo dato genetico trattato elettronicamente non dovrebbe considerarsi dato sanitario elettronico personale e, pertanto, sottratto all'applicazione del regolamento EHDS.

I dubbi derivanti da una interpretazione aderente al dato letterale potrebbero essere superati se si guarda l'elenco delle categorie minime di dati personali per uso secondario (art. 51 EHDS) e categorie prioritarie di dati sanitari elettronici personali per uso primario (art.14 EHDS) che individuano documenti che potrebbero contenere solo il dato alla salute e non anche il dato genetico.

La definizione di dato sanitario elettronico per uso secondario va letta anche alla luce dell'art. 51 EHDS che elenca le categorie minime di dati sanitari elettronici<sup>33</sup>. L'elenco non è esaustivo e può essere altresì integrato a livello nazionale.

Proprio con riferimento alle categorie minime di dati sanitari elettronici da ricomprendere per l'uso secondario sono sorti non pochi dubbi in sede di lavori preparatori. Nel parere

---

*Law Journal*, 2021, 22, 1583; Ciancimino, *Protezione e controllo dei dati in ambito sanitario e intelligenza artificiale. I dati relativi alla salute tra novità normative e innovazione tecnologiche*, Napoli, 2020, 24 ss.; C.Irti, *Dato personale, dato anonimo e crisi del modello normativo dell'identità*, in *Jus civile*, 2020, 379

<sup>33</sup> Art. 51 paragrafo 1, Categorie minime di dati sanitari elettronici per l'uso secondario, EHDS

1. I titolari dei dati sanitari mettono a disposizione per l'uso secondario, conformemente al presente capo, le categorie di dati sanitari elettronici seguenti:

- a) dati sanitari elettronici provenienti da cartelle cliniche elettroniche;
- b) dati su fattori con un'incidenza sulla salute, compresi i determinanti socioeconomici, ambientali e comportamentali della salute;
- c) dati aggregati sulle esigenze di assistenza sanitaria, sulle risorse assegnate all'assistenza sanitaria, sulla prestazione di assistenza sanitaria e sul suo accesso, sulla spesa per l'assistenza sanitaria e sul suo finanziamento;
- d) dati sugli agenti patogeni che incidono sulla salute umana;
- e) dati amministrativi relativi all'assistenza sanitaria, anche relativamente alle dispensazioni, alle domande di rimborso e ai rimborsi;
- f) dati genetici, epigenomici e genomici umani;
- g) altri dati molecolari umani, quali quelli provenienti dalla proteomica, dalla trascrittomica, dalla metabolomica, dalla lipidomica e altri dati omici;
- h) dati sanitari elettronici personali generati automaticamente mediante dispositivi medici;
- i) dati provenienti dalle applicazioni per il benessere;
- j) dati relativi allo status e alla specializzazione e all'istituzione dei professionisti sanitari coinvolti nella cura di una persona fisica;
- k) dati provenienti da registri dei dati sanitari basati sulla popolazione, come i registri di sanità pubblica;
- l) dati provenienti da registri medici e da registri della mortalità;
- m) dati provenienti da sperimentazioni cliniche, studi clinici, indagini cliniche e studi delle prestazioni soggetti al regolamento (UE) n. 536/2014, al regolamento (UE) 2024/1938 del Parlamento europeo e del Consiglio, al regolamento (UE) 2017/745 e al regolamento (UE) 2017/746;
- n) altri dati sanitari provenienti da dispositivi medici;
- o) dati provenienti da registri di medicinali e dispositivi medici;
- p) dati provenienti da coorti di ricerca, questionari e indagini in materia di salute, dopo la prima pubblicazione dei risultati;
- q) dati sanitari provenienti da biobanche e banche dati associate.

---

congiunto reso dallo *European Data Protection Board* (EDPB) e dallo *European Data protection Supervisor* (EDPS), con riferimento all'uso secondario, si raccomandava di eliminare dall'ambito di applicazione della Proposta di regolamento EHDS i dati derivanti dalle applicazioni per il benessere e altre applicazioni digitali, così come i dati relativi al benessere e ai comportamenti pertinenti per la salute in considerazione del fatto che i dati sanitari generati dalle applicazioni per il benessere (pensiamo alle applicazioni che monitorano i passi, le applicazioni relative al calcolo delle calorie) non sono soggetti agli stessi requisiti in materia di qualità di dati, oltre a non presentare le stesse caratteristiche di affidabilità, di quelli generati da dispositivi medici (pensiamo ad un dispositivo medico come l'holter pressorio). Inoltre, le applicazioni per il benessere generano un'enorme quantità di dati e possono essere altamente invasive in quanto tali dati fanno riferimento a ogni azione che le persone compiono quotidianamente (pensiamo all'applicazione contapassi, all'applicazione contacalorie).

Nella versione finale del Regolamento EHDS si legge, al considerando 56, che le categorie di dati sanitari elettronici che possono essere trattati per l'uso secondario dovrebbero anche includere dati generati automaticamente provenienti da dispositivi medici e dati generati dalla persona, quali dati provenienti da applicazioni per il benessere e l'art. 51, paragrafo 1, lett. i, comprende, tra le categorie minime di dati sanitari elettronici per l'uso secondario, anche i dati provenienti dalle applicazioni per il benessere.

Nella versione finale del Regolamento, dunque, non sembrano essere state prese in considerazione le osservazioni critiche contenute nel parere reso dal Comitato Europeo per la Protezione dei Dati (EDPB) e dal Garante Europeo per la Protezione dei Dati (GEPD) relativamente alle applicazioni per il benessere ma viene lasciato un margine di discrezionalità agli Stati che possono introdurre misure più restrittive e rigorose ed adottare garanzie supplementari per tutela i dati provenienti da applicazioni per il benessere ai sensi dell'art. 51, paragrafo 4.

Siffatto margine di discrezionalità lasciato agli Stati genera, tuttavia, non pochi profili problematici legati alla frammentazione della tutela degli interessati quando sono immesse in commercio tali applicazioni per il benessere in Stati dove non sono previste garanzie aggiuntive per la tutela dei dati generati dalle applicazioni stesse per uso secondario.

Qualche dubbio interpretativo emerge dalla lettura dell'art. 51, paragrafo 1, lettera i, EHDS, e, in particolare è possibile chiedersi se siffatta disposizione si riferisce alle applicazioni per il benessere *tout court* o solo alle applicazioni per il benessere per le quali è stata rilasciata una etichetta ai sensi dell'art. 47 EHDS. Non risulta ben delineato il coordinamento tra le applicazioni per il benessere *tout court* e le applicazioni etichettate ai sensi dell'art. 47 EHDS, dichiarate interoperabili con il sistema di cartelle cliniche elettroniche, ove la condivisione o la trasmissione di tali dati è possibile solo se conforme all'articolo 5 EHDS, previo consenso della persona fisica interessata, e l'interoperabilità è limitata esclusivamente ai fini della condivisione e della trasmissione e la persona fisica interessata può scegliere quali categorie dei dati sanitari dell'applicazione per il benessere inserire nel sistema di cartelle cliniche elettroniche.

Se il legislatore avesse voluto ricomprendere solo i dati generati da applicazioni di benessere etichettate interoperabili con cartelle cliniche non avrebbe avuto necessità di indicare espressamente all'art. 51, lettera i, tra le categorie minime di dati per uso secondario anche i dati generati dalle applicazioni del benessere perché, appunto, già ricomprese nella lettera a) (non a caso l'art. 51, paragrafo 1, lettera a, ricomprende tra le categorie di dati sanitari per uso secondario quelli contenute nelle cartelle cliniche che dovrebbero contenere anche i dati provenienti dalle applicazioni per il benessere etichettate e, per le quali, la persona fisica interessata abbia scelto quali dati condividere nel sistema di cartelle cliniche elettroniche). Deve, quindi, ritenersi, che il legislatore europeo abbia voluto espressamente includere tutte le applicazioni per il benessere e rendere utilizzabile l'enorme mole di dati generati da tali applicazioni per fini secondari. Tale soluzione potrebbe generare qualche perplessità in termini di riservatezza e protezione dei dati, ma il sistema pubblicistico - previsto dal Regolamento EHDS relativo al controllo degli accessi per uso secondario solo per le finalità indicate nell'art. 53 EHDS - dovrebbe garantire la riservatezza delle informazioni e il rispetto della normativa relativa alla protezione dei dati.

Si può osservare che va guardata con favore l'impronta pubblicistica impressa dal Regolamento EHDS per l'uso secondario dei dati in ambito sanitario ma, i numerosi margini di discrezionalità lasciati agli Stati previsti dall'art. 51 EHDS, sia con riferimento all'individuazione di ulteriori categorie di dati sanitari (art. 51, comma 2, EHDS), che all'introduzione di garanzie supplementari per alcune categorie di dati particolarmente sensibili (art. 51, paragrafo 1, lettere f, g, i e q) potrebbero incidere negativamente sul piano della certezza del diritto ed avere ripercussioni negative sul piano applicativo (si pensi ad una ricerca condotta da ricercatori residenti in Stati che si sono avvalsi del margine di discrezionalità e che hanno, quindi, introdotto ulteriori categorie di dati sanitari elettronici e garanzie supplementari per dati considerati particolarmente sensibili e Stati che, invece, non si sono avvalsi del margine di discrezionalità e non 'riconoscono' ulteriori dati oltre a quelli indicati nell'art. 51, paragrafo 1, e non hanno introdotto garanzie supplementari per alcune categorie di dati particolarmente sensibili).

A complicare il quadro si evidenzia, inoltre, che la definizione di dato sanitario elettronico - inteso come dato relativo alla salute e dato genetico - potrebbe risentire dell'ambivalenza della definizione di dato relativo alla salute elaborata dalla Corte di Giustizia UE. In una recente decisione la Corte di Giustizia ha adottato una interpretazione di "dato relativo alla salute" particolarmente ampia<sup>34</sup>, che ricomprende non solo dati relativi alla salute - cartella clinica, referti medici etc - ma anche i dati personali - quali nome, indirizzo di consegna - che attraverso un'operazione intellettuale siano in grado di rivelare le condizioni di salute dell'interessato. Tale interpretazione ampia di dato relativo alla salute, emersa nell'ambito di una controversia avente ad oggetto l'acquisto online di farmaci senza obbligo di prescrizione medica su una piattaforma digitale, potrebbe generare non pochi

---

<sup>34</sup> Corte Giust. 4 ottobre 2024, causa C-21/23, in *Nuova giur. civ. comm.*, 2025, 588 con nota di A. Bernes, *La nozione di dati relativi alla salute al vaglio della Corte di Giustizia quali conseguenze per il commercio elettronico e la concorrenza*.

problemi poiché la Corte non indica criteri precisi per determinare con un certo grado di certezza - e non una semplice supposizione - che le informazioni possano essere rivelatrici dello stato di salute. Tale interpretazione così ampia porta a conseguenze rilevanti sul piano applicativo poiché potrebbero considerarsi dati relativi alla salute anche dati personali trattati mediante analisi aggregata e utilizzo di strumenti di data analytics<sup>35</sup>. Tuttavia, ci si deve domandare se, sul piano applicativo, possano rientrare nel perimetro della definizione di dati relativi alla salute – e quindi compresi nella definizione di dato sanitario personale elettronico - anche quelle informazioni che svelano solo in modo equivoco e non diretto aspetti dello stato di salute di una persona ma creino una mera supposizione relativa allo stato di salute.

In realtà sarebbe auspicabile un certo grado di certezza e, non una mera supposizione, relativa allo stato di salute, altrimenti, si corre il rischio di confondere le tipologie di dati come anche i meccanismi che presidono il trattamento (e la circolazione), la tutela e, quindi, il regime normativo applicabile.

Al fine di superare la problematica legata alla interpretazione estensiva formulata dalla Corte di Giustizia si potrebbe tener conto non solo del contesto in cui i dati sono stati raccolti ma, soprattutto, delle specifiche finalità perseguita da chi raccoglie e tratta i dati: se chi raccoglie dati non effettua trattamenti in grado di incidere sulla salute dell'interessato allora dati personali non dovrebbero essere considerati dati relativi alla salute<sup>36</sup>. Dunque, con riferimento alla definizione di dato sanitario elettronico, trattandosi di dati raccolti in ambiente sanitario con finalità di cura ed utilizzati in forma anonima o pseudonima non dovrebbero porsi particolari problemi<sup>37</sup>.

Il trattamento del dato sanitario deve avvenire elettronicamente: quanto a dire, dunque, che i dati relativi alla salute e i dati genetici trattati in modo non elettronico, e quindi in modo cartaceo, non dovrebbero rientrare nell'ambito di applicazione dell'EHDS<sup>38</sup> ma dovrebbero seguire il regime generale previsto nel GDPR e nel Codice Privacy descritto nelle pagine che precedono<sup>39</sup>.

<sup>35</sup> Bernes, *La nozione di dati relativi alla salute*, cit., 597. Vedi anche F. Piraino, *Il contrasto sulla nozione di dato sensibile, sui presupposti e sulle modalità del trattamento*, in *Nuova giur. civ. comm.*, 2017, I, 1232 ss.

<sup>36</sup> Sul punto: Bernes, *La nozione di dato relativo alla salute*, cit., 599.

<sup>37</sup> Sul problema del dato pseudonimo/anonimo nel diritto europeo si può vedere la recente decisione della Corte di Giustizia: Corte Giust. 4 settembre 2025, causa c-413/23P (consultabile al seguente link <https://curia.europa.eu/jcms/upload/docs/application/pdf/2025-09/cp250107en.pdf>). La Corte di Giustizia, con riferimento al problema dei dati pseudonimi, ha precisato che i dati pseudonimi inviati ad un terzo non sempre mantengono, automaticamente, tale natura solo in ragione del fatto che “esistono” informazioni che teoricamente consentirebbero l'identificazione dell'interessato ma si deve, di volta in volta, effettuare una analisi del rischio di de-identificabilità (che riduce il rischio di associare il dato alla persona) in concreto non rilevando l'esistenza di informazioni supplementari che consentono l'identificazione dell'interessato.

<sup>38</sup> Si veda il contributo di Corso, *Lo spazio europeo dei dati sanitari*, cit., 565.

<sup>39</sup> La definizione di dato sanitario elettronico comprende i dati personali sia i dati non personali. Questo elemento risulta essere particolarmente utile poiché nell'ambito della ricerca scientifica possono avere un ruolo determinante anche i dati non personali intesi non solo come dati anonimizzati ma anche come dati non riferiti ad un *data subject* ma che possono incidere sullo sviluppo di una malattia (pensiamo a fattori climatici o ambientali che incidono sullo sviluppo di una determinata malattia: tempo di esposizione ai raggi solari in una ricerca sul melanoma, o alla latitudine; o fattori alimentari in ricerca sul diabete o di tipo endocrinologico).

### II.3 *Uso secondario dei dati sanitari elettronici tra finalità (consentite) e divieti.*

La definizione 'uso secondario' dei dati sanitari, assente nel quadro normativo generale del GDPR analizzato nelle pagine che precedono come anche nel Codice Privacy, è presente per la prima volta nel Regolamento EHDS.

L'art. 2, lett e, Regolamento EHDS stabilisce che per uso secondario si intende il trattamento dei dati sanitari elettronici per le finalità indicate al capo IV del regolamento EHDS, che sono diverse dalle finalità iniziali per le quali tali dati sono stati raccolti o prodotti.

Tale definizione sembra composta da due parti legate da uno stretto nesso di interdipendenza e complementarità. Da un lato, la definizione di uso secondario è costruita in negativo rispetto alla definizione di uso primario (è uso secondario il trattamento dei dati per finalità diverse per le quali i dati sono stati originariamente raccolti e trattati); dall'altro, non è considerato uso secondario qualsiasi uso diverso dall'uso primario ma, solo quello che persegue finalità specifiche elencate nel capo IV EHDS e che possono essere sintetizzate come interesse generale per la ricerca in ambito sanitario. L'elenco attuale delle finalità individuate dall'art. 53 EHDS – pubblico interesse, definizione delle politiche nel settore sanitario e dell'assistenza, statistiche, attività di istruzione, ricerca scientifica e miglioramento della prestazione di assistenza - sembra tenere conto delle critiche sollevate dal Comitato Europeo per la Protezione dei Dati (EDPB) e dal Garante Europeo per la Protezione dei Dati durante i lavori preparatori. Infatti, nel parere congiunto reso dal Comitato Europeo per la Protezione dei Dati (EDPB) e dal Garante Europeo per la Protezione dei Dati si evidenziava che la mancata delimitazione delle finalità per cui i dati sanitari elettronici potevano essere ulteriormente trattati rappresentava un serio rischio per i diritti e le libertà degli interessati e, in particolare, si ritenevano troppo ampie - e vaghe - le finalità relative all'uso secondario contenute nell'art. 34, paragrafo 1, lettere f) e g), della proposta di Regolamento sullo Spazio Europeo dei Dati Sanitari che comprendevano qualsiasi forma di "attività di sviluppo e innovazione per prodotti o servizi che contribuiscono alla sanità pubblica o alla sicurezza sociale" o "attività di addestramento, prova e valutazione degli algoritmi, anche nell'ambito di dispositivi medici, sistemi di IA e applicazioni di sanità digitale, che contribuiscono alla sanità pubblica o alla sicurezza sociale" e si suggeriva di circoscrivere, con rigore, siffatte finalità. Il parere sopra menzionato evidenziava, nello specifico, la necessità di un riferimento sufficientemente preciso alla salute pubblica e/o alla sicurezza sociale. La restrizione delle finalità, a parere di EDPB e GEPD, era essenziale per conseguire un equilibrio tra degli obiettivi perseguiti dal Regolamento EHDS e la protezione dei dati personali degli interessati coinvolti in tale trattamento.

La versione finale del Regolamento EHDS circoscrive le finalità, seguendo le indicazioni del parere congiunto del Comitato Europeo per la Protezione dei Dati e del Garante Europeo per la Protezione dei Dati, e considera uso secondario per finalità di ricerca scientifica nel settore sanitario o dell'assistenza che contribuisce alla sanità pubblica o alla valutazione delle tecnologie sanitarie o che garantisce elevati livelli di qualità e sicurezza

dell'assistenza sanitaria, dei medicinali o dei dispositivi medici, con l'obiettivo di favorire gli utenti finali, quali i pazienti, i professionisti sanitari e gli amministratori sanitari (tra cui devono essere menzionate l'attività di sviluppo ed innovazione per prodotti e servizi ed attività di addestramento e valutazione degli algoritmi anche nell'ambito di dispositivi medici, dispositivi medico diagnostici in vitro, sistemi di IA ed applicazioni di sanità digitale). Tra le finalità per uso secondario è ricompreso anche l'utilizzo dei dati per addestramento di algoritmi nell'ambito di dispositivi medico diagnostici e sistemi di IA, finalità non espressamente indicata nel GDPR e nella normativa nazionale di attuazione del GDPR. Il riferimento all'utilizzo di dati personali, comprese le categorie particolari di dati di cui all'art. 9 GDPR, nell'ambito dei sistemi di intelligenza artificiale viene invece espressamente menzionata nell'art. 8 della legge italiana sull'intelligenza artificiale (ma su questo profilo si ritornerà nel paragrafo 4).

Tra le finalità per uso secondario dei dati sanitari elettronici è utile menzionare l'attività d'istruzione o d'insegnamento nel settore sanitario o dell'assistenza al livello della formazione professionale o dell'istruzione superiore: quindi, i dati sanitari potranno essere utilizzati non solo per finalità scientifica ma anche per attività didattico formativo in ambito sanitario.

La definizione di uso secondario deve essere completata anche alla luce di quanto previsto dall'art. 54 EHDS che vieta espressamente l'uso secondario dei dati sanitari elettronici per determinate finalità. Quindi non è consentito l'uso secondario dei dati personali elettronici per finalità pubblicitarie e di marketing; per sviluppare prodotti in grado di danneggiare le persone, la sanità pubblica, prodotti che siano in grado di creare dipendenza o modificati in modo da creare dipendenza, in grado di violare l'ordine pubblico o la moralità o causare un rischio per la salute umana; svolgere attività in contrasto con le disposizioni etiche a norma del diritto nazionale; adottare decisioni pregiudizievoli; adottare decisioni, in relazione a una persona fisica o a un gruppo di persone fisiche, per quanto riguarda offerte di lavoro, offrire condizioni meno favorevoli nella fornitura di beni o servizi, compresa l'esclusione di tali persone o gruppi dal beneficio di un contratto di assicurazione o di credito, la modifica dei loro contributi e premi assicurativi o le condizioni dei prestiti, o adottare altre decisioni, in relazione a una persona fisica o a un gruppo di persone fisiche, che risultino in una discriminazione nei loro confronti sulla base dei dati sanitari ottenuti. La logica dell'art. 54 EHDS è volta ad evitare un uso discriminatorio dei dati che possa incidere negativamente sui diritti e sulle libertà delle persone<sup>40</sup>. I divieti di cui all'art. 54 EHDS certamente contribuiscono a delineare con maggior rigore la definizione di uso secondario ma non sono privi di dubbi interpretativi.

In particolare, non privo di ambiguità risulta l'art. 54 EHDS, lettera e) che vieta l'uso secondario in contrasto con le disposizioni etiche a norma del diritto nazionale. Questa disposizione risulta problematica sotto due diversi e complementari profili. Sotto il primo profilo non è ben chiaro cosa si intenda per norme etiche ai sensi del diritto nazionale e a quale specifico settore ci si riferisca: se le disposizioni etiche sono riferite solo al settore sanitario (es. codici deontologici di settore) o più latamente al settore dell'Intelligenza

---

<sup>40</sup> Iaselli, *Le nuove regole per l'uso primario e secondario*, cit., 75.

Artificiale o a qualsiasi disposizione etica generale presente a livello nazionale. Sotto il secondo profilo, la lettera e) potrebbe innescare una vera e propria frammentazione applicativa del Regolamento EHDS perché alcuni usi secondari potrebbero essere ritenuti etici in alcuni Stati ma non in altri Stati. La lettera e) così come strutturata potrebbe prestare il fianco ad interpretazioni estensive volte a consentire il trattamento di dati per uso secondario. La lettera e) consente alcuni, forse troppo ampi, margini di flessibilità. Sarebbe stato auspicabile circoscrivere con rigore il riferimento alle disposizioni etiche. Una soluzione ermeneutica, forse, potrebbe essere quella di richiamare i principi europei dell'etica per la salute digitale adottati dalla rete eHealth il 26 gennaio 2022 e il principio di riservatezza tra i professionisti sanitari e i pazienti. Tali principi forniscono orientamenti rivolti a professionisti, ricercatori, innovatori, responsabili politici e autorità di regolamentazione ma sono individuati a livello europeo - e non a livello nazionale come invece previsto dalla lettera e) -.

Nel delineare ulteriormente le finalità per uso secondario, il Regolamento EHDS stabilisce che la definizione di uso secondario non comprende, appunto, i dati sanitari a fini di contrasto. La prevenzione, l'indagine, l'accertamento o il perseguimento di reati o l'esecuzione di sanzioni penali da parte delle autorità competenti, quindi, non dovrebbero rientrare tra le finalità di uso secondario contemplate indicate nel regolamento EHDS.

Si evidenzia, infine, che l'art. 53 EHDS precisa che gli organismi responsabili dell'accesso ai dati sanitari per uso secondario concedono l'uso dei dati solo se il trattamento è necessario per il perseguimento di una delle finalità secondarie previste dall'art. 53, paragrafo 2<sup>41</sup> e ciò in linea di continuità con l'art. 9, paragrafo 2, GDPR. Si deve notare che nella proposta di Regolamento EHDS figurava il termine 'conforme' e solo nella versione definitiva ha trovato spazio il termine 'necessario', utilizzato per rendere coerente il Regolamento EHDS con il Regolamento Generale sulla Protezione dei Dati che fa della necessità un principio fondamentale per la protezione dei dati<sup>42</sup>.

### III. DIRITTO DI ESCLUSIONE E USO SECONDARIO. LA RIEMERSIONE DELLE PROBLEMATICHE LEGATE AL CONSENSO?

Il criterio soggettivo-personalistico del 'consenso' riemerge nell'ambito del c.d. diritto di esclusione di cui all'art. 71 del Regolamento EHDS. Il Regolamento EHDS, al fine di trovare un equilibrio tra l'interesse pubblico all'uso secondario dei dati e l'autodeterminazione delle persone fisiche rispetto ai loro dati sanitari elettronici personali considerati particolarmente sensibili, introduce il c.d. diritto di esclusione in relazione alla messa a disposizione di tali dati per l'uso secondario. Il meccanismo di esclusione previsto dall'art. 71 EHDS è una chiara espressione del

<sup>41</sup> Vedi: Corso, *Lo spazio europeo dei dati sanitari*, cit., 585.

<sup>42</sup> Si veda il Considerando n. 50 GDPR "(...)Se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o per l'esercizio di pubblici poteri di cui è investito il titolare del trattamento, il diritto dell'Unione o degli Stati membri può stabilire e precisare le finalità e i compiti per i quali l'ulteriore trattamento è considerato lecito e compatibile...". Si veda anche art. 9, paragrafo 2, GDPR.

principio di autodeterminazione che si concretizza nella manifestazione di volontà del soggetto di escludere l'uso secondario dei propri dati sanitari elettronici. Tale diritto deve essere oggetto di uno specifico obbligo informativo che comprende vantaggi e svantaggi relativi all'esercizio di tale diritto e la persona fisica nel momento in cui decide esercitare tale diritto non deve essere obbligata ad indicare le ragioni e può, in qualsiasi momento, riconsiderare la propria scelta in relazione al diritto di esclusione.

Sul piano teorico il diritto di esclusione si struttura come una manifestazione di volontà con la quale l'interessato dichiara di escludere l'uso secondario dei propri dati personali elettronici<sup>43</sup> e porta con sé alcune delle problematiche emerse già in relazione al consenso. Nel diritto di esclusione, però, la manifestazione di volontà non opera come base giuridica che rende lecito il trattamento, e quindi a monte del trattamento, ma si configura come uno strumento di tutela a valle per escludere il trattamento ulteriore per uso secondario<sup>44</sup>. L'art. 71 EHDS non definisce quali debbano essere le caratteristiche della volontà con cui si manifesta il dissenso/opt out all'uso secondario dei propri dati sanitari elettronici e se, al pari del consenso quale base giuridica del trattamento, debba essere libero specifico ed informato. Se non sussistono dubbi relativi al requisito dell'informazione – l'art. 71 EHDS espressamente richiede che vi sia l'informativa relativa al diritto di esclusione e, quindi, la manifestazione di volontà con cui si esprime il dissenso deve essere informata – qualche perplessità permane in relazione agli altri due requisiti - libero e specifico -. Con riferimento alla libertà si pone il problema dello squilibrio tra titolare del trattamento e il *data subject* inteso in termini generali come qualsiasi azione di pressione o influenza inappropriata sull'interessato e, difficilmente, potrebbe considerarsi libera una volontà raccolta, ad esempio, in ospedale o più in generale in contesti di vulnerabilità. L'esercizio del diritto di *opt out* – e, quindi, della manifestazione di volontà con cui si esprime il dissenso all'uso secondario dei dati – presenta non poche criticità nei confronti di soggetti vulnerabili, pensiamo ai pazienti, agli anziani ma anche agli analfabeti che non sono in grado di leggere e comprendere l'informativa relativa al diritto di *opt out*<sup>45</sup>. In ultima analisi questa soluzione certamente agevola la circolazione dei dati per uso secondario per fini di ricerca in ambito sanitario e si pone in linea con le finalità del Regolamento EHDS ma suscita qualche dubbio sulla tutela effettiva degli interessati e qualche dubbio di coerenza con il principio di autodeterminazione.

<sup>43</sup> Cascini, Arcuri, *Uso secondario dei dati sanitari*, cit., 878.

<sup>44</sup> Vedi Corso, *Spazio europeo*, cit., 589.

<sup>45</sup> Nel tentativo di circoscrivere il quadro della vulnerabilità, il chiarimento interpretativo n. 467, 11 ottobre 2018 reso dal Garante per la Protezione dei dati personali relativo all'elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, fa riferimento ai trattamenti non occasionali di dati relativi a soggetti vulnerabili e sono individuati i minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo. Sia consentito il rinvio a V.V. Cuocci, *La protezione dei dati personali dei soggetti vulnerabili. Uno studio di diritto comparato*, Bari, 2022, 1-242. Il problema della vulnerabilità in materia di *privacy* è stato affrontato da R. Calo, *Privacy, Vulnerability and Affordance*, 66 *DePaul L. Rev.* 594 (2017). Si veda anche lo studio particolarmente interessante di G. Malgieri, J. Niklas, *Vulnerable Data Subject*, in *Computer Law and Security Review*, 2020, 2 e ss.

Con riferimento all'ultimo requisito - specifico - ci si chiede se il diritto di esclusione/opt out al trattamento dei dati sanitari possa riferirsi in generale all'uso secondario o anche a specifiche finalità contemplate nell'art. 53 EHDS.

Il diritto di opt out/esclusione sembra un diritto destinato a rimanere un contenitore vuoto non solo per le difficoltà concretamente operative ma anche per alcuni margini di discrezionalità lasciati agli Stati membri.

L'art. 71 EHDS prevede, appunto, un margine di discrezionalità per gli Stati membri che possono, sulla base del diritto nazionale, restringere l'operatività del diritto di esclusione: il principio di autodeterminazione e la volontà dell'interessato cedono il passo al preminente interesse pubblico alla ricerca in ambito sanitario.

Tale limitazione del diritto di esclusione prevede un elemento soggettivo ed uno oggettivo.

Sul piano soggettivo la domanda di accesso ai dati sanitari elettronici per uso secondario deve essere formulata da un ente pubblico o una istituzione o un organo che agisce nel settore della sanità pubblica. Sul piano oggettivo, l'eccezione al diritto di esclusione è circoscritta al perseguimento di specifiche finalità di ricerca scientifica per rilevante interesse pubblico e per pubblico interesse nell'ambito della sanità pubblica, per finalità statistiche e definizione delle politiche e attività regolamentari a sostegno di enti pubblici o di istituzioni, organi e organismi dell'Unione, comprese le autorità di regolamentazione, del settore sanitario. Inoltre, il richiedente deve dimostrare che i dati non possono essere ottenuti con mezzi alternativi in modo tempestivo ed efficace in condizioni equivalenti e, inoltre, deve sempre assicurare il rispetto dell'essenza dei diritti e delle libertà fondamentali e costituire una misura necessaria e proporzionata in una società democratica per servire ragioni di interesse pubblico nel perseguimento di obiettivi scientifici e sociali legittimi.

Il margine di discrezionalità lasciato agli Stati membri, per quanto circoscritto sia sul piano soggettivo che su quello oggettivo attraverso una precisa specificazione delle finalità, lascia qualche dubbio in termini di frammentazione della tutela degli interessati che potrebbe variare da Stato a Stato.

Il quadro appena descritto potrebbe risultare ulteriormente complicato dalla concorrenza dei meccanismi di tutela già previsti dal GDPR, come il diritto di cancellazione che, però, incontra il limite dell'interesse pubblico nel settore della sanità pubblica ai sensi dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3 e, quindi, non dovrebbe operare nell'ambito dei dati sanitari elettronici per uso secondario. Il diritto di esclusione di cui all'art. 71 EHDS, invece, non comporta la cancellazione ma implica semplicemente il divieto di utilizzare dei dati per uso secondario. Tra l'altro, i dati potrebbero essere oggetto di trattamento ulteriore nei limiti previsti dal Regolamento EHDS con misure specifiche e adeguate per proteggere i diritti fondamentali e i dati personali delle persone fisiche.

Sul punto occorre ricordare che la giurisprudenza nazionale ha precisato che il sistema di tutela dei dati personali deve porre l'utente al centro, così obbligando il titolare del trattamento ad una tutela effettiva da un punto sostanziale, non solo formale: non è

sufficiente, cioè, che la progettazione del sistema sia conforme alla norma se, poi, il soggetto interessato non è tutelato<sup>46</sup>.

Un'ultima osservazione riguarda i dati sanitari relativi a persone decedute che potrebbero essere utilizzati per fini di ricerca scientifica (pensiamo alla morte come effetto collaterale di un farmaco in fase sperimentale o agli studi clinici retrospettivi). Il Regolamento EHDS non fa riferimento al problema dei dati sanitari delle persone decedute e, per questa categoria di dati, dovrebbe applicarsi la regola generale contenuta nel GDPR a tenore del quale, appunto il Regolamento non si applica alle persone decedute (considerando 27 del GDPR). Il GDPR lascia un margine di discrezionalità agli Stati membri circa l'introduzione di norme a tutela dei soggetti deceduti: nell'ordinamento italiano il Codice privacy stabilisce che i diritti previsti dall'art. 15 all'art. 22 GDPR riferiti a persone decedute possono essere esercitati da chi ha un interesse proprio, chi agisce a tutela dell'interessato (es. mandatario), chi lo fa per ragioni familiari meritevoli di protezione, a meno che l'interessato non lo abbia espressamente vietato con una dichiarazione scritta presentata al titolare del trattamento. In ogni caso il divieto non può produrre effetti pregiudizievoli per l'esercizio da parte dei terzi dei diritti patrimoniali che derivano dalla morte dell'interessato nonché del diritto di difendere in giudizio i propri interessi. (art. 2 terdecies Codice Privacy). Ci si chiede, dunque, se nell'ambito dell'uso secondario di dati di persone decedute, gli eredi o chi vi ha un interesse possano, ad esempio, esercitare un diritto di opt out.

#### IV. USO SECONDARIO E SPERIMENTAZIONE SCIENTIFICA PER LA REALIZZAZIONE DI SISTEMI DI INTELLIGENZA ARTIFICIALE IN AMBITO SANITARIO NELLA LEGGE ITALIANA SULL'INTELLIGENZA ARTIFICIALE E NEL REGOLAMENTO SULLO SPAZIO EUROPEO DEI DATI SANITARI. TRA COMPLESSITÀ E FRAMMENTAZIONE DELLE FONTI.

Il sistema delle fonti analizzato nelle pagine che precedono sembra ulteriormente complicato dalla legge italiana sull'intelligenza artificiale di recente approvazione, che espressamente regola l'utilizzo dei dati, anche personali, per finalità di ricerca e sperimentazione scientifica nella realizzazione di sistema di intelligenza artificiale in ambito sanitario<sup>47</sup>.

Il quadro delle fonti che emerge risulta particolarmente complesso e non privo di incoerenze che potrebbero alimentare dubbi interpretativi, difficoltà applicative ma anche la corsa verso la scelta del modello normativo più flessibile e meno costoso – o quello che determina minori adempimenti – per il titolare del trattamento come anche per chi intende usare i dati per finalità secondarie.

<sup>46</sup> Cass.11 ottobre 2023, n. 28385.

<sup>47</sup> La legge sull'intelligenza artificiale 23 settembre 2025, n. 132, GU, 25 settembre 2025.

Per un primo commento sulla legge italiana sull'IA: G.M. Riccio, G. Resta, *Il ddl AI è legge: primi spunti di riflessione*, <https://www.altalex.com/documents/2025/09/18/ddl-legge-primi-spunti-riflessione>.

Sul disegno di legge: V. Fusco, *Il Garante della Privacy e l'IA in ambito sanitario: il parere sul d.d.l. n. 1146/2024*, sul sito del Centro Studi "Diritto e Sanità" dell'Università degli Studi di Pavia (consultabile su <https://dirittoesanita.unipv.it/aggiornamenti/trattamento-dati-personali-intelligenza-artificiale-sanita-pareregarante-privacy.kl>).

Proviamo a fare qualche riflessione anche in riferimento al coordinamento tra le disposizioni contenute nel Regolamento EHDS e legge italiana sull'Intelligenza Artificiale. L'art. 8 della legge italiana sull'intelligenza artificiale (legge 132/25)<sup>48</sup> introduce una nuova base giuridica per il trattamento dei dati per fini di ricerca scientifica, ai sensi dell'art. 9, paragrafo 2, lettera g, GDPR. Nello specifico la norma qualifica espressamente come interesse pubblico rilevante i dati trattati per ricerca e sperimentazione scientifica da soggetti pubblici e privati senza scopo di lucro, dagli Istituti di ricovero e cura a carattere scientifico (IRCCS), di cui al decreto legislativo 16 ottobre 2003, n. 288, nonché da soggetti privati operanti nel settore sanitario nell'ambito di progetti di ricerca a cui partecipano soggetti pubblici e privati senza scopo di lucro o IRCCS, per la ricerca e la sperimentazione scientifica nella realizzazione di sistemi di intelligenza artificiale per finalità di prevenzione, diagnosi e cura di malattie, sviluppo di farmaci, terapie e tecnologie riabilitative, realizzazione di apparati medicali, incluse protesi e interfacce fra il corpo e strumenti di sostegno alle condizioni del paziente, salute pubblica, incolumità della persona, salute e sicurezza sanitaria nonché studio della fisiologia, della biomeccanica e della biologia umana anche in ambito non sanitario, in quanto necessari ai fini della realizzazione e dell'utilizzazione di banche dati e modelli di base. Tale indicazione si pone essenzialmente in linea con il Regolamento EHDS.

Il secondo comma dell'art. 8, legge 132/25, autorizza espressamente, senza necessità di ulteriore consenso, e fermo l'obbligo di informativa che può essere anche generale e pubblicata dal titolare sul sito web, l'uso secondario di dati personali privi degli elementi identificativi diretti, anche appartenenti alle categorie particolari di dati indicate all'articolo 9 GDPR, da parte dei soggetti di cui all'art. 8, comma 1, salvi i casi nei quali la conoscenza dell'identità degli interessati sia inevitabile o necessaria al fine della tutela della loro salute. Tale formulazione desta qualche dubbio circa la coerenza con il GDPR, a tenore del quale non sarebbe sufficiente una mera informativa generale sul sito web in caso di riutilizzo dei dati per finalità diversa per la quale i dati sono stati raccolti, trovando applicazione l'art. 13 paragrafo 3 e art. 14 paragrafo 4 che impongono una informativa specifica<sup>49</sup>.

Inoltre, sarebbe stato auspicabile con riferimento all'uso secondario dei dati il richiamo alle complesse garanzie previste dall'art. 89 GDPR. Non vi è, invece, neppure il richiamo al principio di minimizzazione dei dati in coerenza con il GDPR e con i principi generali in materia di protezione dei dati.

Suscita perplessità anche l'ultima parte dell'art. 8, paragrafo 2, che consente l'utilizzo dei dati relativi alla salute e delle categorie particolari di dati privi degli elementi identificativi diretti da parte dei soggetti di cui al comma 1, salvi i casi nei quali la conoscenza dell'identità degli interessati sia inevitabile o necessaria al fine della tutela della loro salute. La disposizione normativa risulta, infatti, troppo vaga dato che non specifica i parametri alla luce dei quali stabilire quando la conoscenza dell'identità degli interessati risulti 'inevitabile'. Non risulta chiaro neppure il sintagma "necessario ai fini della tutela della loro

<sup>48</sup> Legge italiana sull'intelligenza artificiale 23 settembre 2025, n. 132, cit.

<sup>49</sup> Si veda il parere del Garante Privacy sul disegno di legge sull'Intelligenza Artificiale che raccomanda l'abrogazione del comma 2 dell'art. 8 de ddl nella misura in cui prevede una informativa generale(<https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/10043532>).

salute”. Ricordiamo che si tratta di uso secondario dei dati e, quindi, di dati che dovrebbero essere usati per fini di ricerca scientifica il cui uso non potrebbe incidere direttamente sulla salute dell’interessato. Tale disposizione risulta particolarmente pericolosa anche perché l’interessato non avrebbe uno strumento per escludere l’uso secondario: non è previsto il diritto di esclusione/opt out come nel Regolamento EHDS. E qui si innesta un ulteriore dubbio interpretativo che riguarda la definizione stessa di ‘uso secondario’ che non è specificata con rigore nella legge italiana sull’intelligenza artificiale e che sembra richiamare il linguaggio del legislatore europeo nel Regolamento EHDS. Peccato, però, che il Regolamento EHDS ha un ambito di applicazione ben circoscritto ai dati sanitari elettronici - intesi come dati relativi alla salute e dati genetici trattati elettronicamente – e non ai dati personali *tout court*; e l’uso secondario è circoscritto alle finalità individuate dall’art. 53 EHDS e con espresso divieto di uso secondario dei dati per determinate finalità che potrebbero ledere i diritti e le libertà degli interessati (marketing).

Un’ultima riflessione riguarda l’art. 8, comma 5, legge 132/25, a tenore del quale i trattamenti di dati di cui ai commi 1 e 2, sopra analizzati, devono essere comunicati al Garante per la protezione dei dati personali con l’indicazione di tutte le informazioni previste dagli articoli 24, 25, 32 e 35 del regolamento (UE) 2016/679, nonché con l’indicazione espressa, ove presenti, dei soggetti individuati ai sensi dell’articolo 28 del medesimo regolamento (UE) 2016/679, e possono essere avviati decorsi trenta giorni dalla predetta comunicazione se non sono stati oggetto di provvedimento di blocco disposto dal Garante per la protezione dei dati personali. Nella formulazione attuale del comma 5 scompare il riferimento alla preventiva approvazione dei comitati etici. Questa indicazione va verso una ulteriore semplificazione dell’uso dei dati per finalità di ricerca scientifica e per finalità secondaria. Inoltre, l’art. 8, comma 5, richiama solo le ipotesi di cui al comma 1 e 2, e non anche quella di cui al comma 3, con la conseguenza che per le finalità di cui al comma 2 sexies, lettera v, Codice Privacy, non dovrà esserci la comunicazione al Garante. Alla luce delle osservazioni sopra formulate si impone l’individuazione del rapporto esistente tra l’uso secondario dei dati ai sensi dell’art. 8 legge 132/25 e l’uso secondario ai sensi del Regolamento EHDS. Potrebbero ipotizzarsi due sistemi paralleli e concorrenti: l’uno disciplinato dall’art.8, legge 132/25, che consente l’uso secondario di dati relativi alla salute - senza specificare che debba trattarsi di dati trattati elettronicamente - per fini di ricerca scientifica nella realizzazione dei sistemi di intelligenza artificiale; l’altro, disciplinato dal Regolamento EHDS, che fa riferimento ai dati sanitari elettronici usati per le finalità secondarie previste dal capo IV EHDS (e tra le finalità vi è quella prevista dall’art. 53, lett. 2, ii - ricerca scientifica nel settore sanitario ...tra cui attività di addestramento, prova e valutazione degli algoritmi, anche nell’ambito di dispositivi medici, dispositivi medico-diagnostici in vitro, sistemi di IA e applicazioni di sanità digitale-).

Ma, anche a voler ipotizzare la realizzazione di sistemi paralleli, risulta difficile, però, tracciare un netto confine e individuare, di conseguenza, la normativa applicabile: cioè, quando si raccolgono dati relativi alla salute e i dati genetici che servono per realizzare sistemi di intelligenza artificiale in ambito sanitario, gioco forza si tratterà di dati in formato elettronico e, dunque, dovrebbe trovare applicazione sempre il Regolamento EHDS e non

l'art. 8 della legge 132/25. Forse una soluzione potrebbe essere quella di richiamare il considerando n. 52 EHDS, a tenore del quale il regolamento EHDS non ostacola o sostituisce accordi contrattuali o meccanismi di altro tipo con la conseguenza che chi vuole accedere ai dati sanitari per uso secondario potrà 'scegliere' se accedere, o non, al sistema previsto, appunto, dal menzionato regolamento EHDS o 'scegliere' altro meccanismo come quello previsto dall'art. 8, legge 132/25.

Il Regolamento EHDS sembra particolarmente protettivo perché individua con rigore le modalità di accesso e di controllo ai dati sanitari elettronici attraverso un sistema pubblicistico regolatorio costituito dai c.d. organismi responsabili dell'accesso; sistema assente nel quadro dell'art. 8 legge 132/25. Ricordiamo, tra l'altro, che gli Organismi di accesso effettuano un controllo anche sulla 'necessità' della richiesta di accesso ai dati per fini di ricerca scientifica.

L'analisi condotta evidenzia la creazione di microsistemi normativi relativi all'uso dei dati per fini di ricerca scientifica che potrebbe portare alla corsa verso il modello che prevede minori costi o adempimenti per chi intende 'usare' i dati per finalità secondarie.

