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

Comparative Law Review is registered at the Courthouse of Monza (Italy) - Nr. 1988 - May, 10th 2010.
Editor on the Register: Alessandro Somma

COMPARATIVE
LAW
REVIEW
VOL. 17/2 - 2026

Spazio europeo dei dati sanitari

SPAZIO EUROPEO DEI DATI SANITARI

L'AMBITO DI APPLICAZIONE DEL REGOLAMENTO (UE) 2025/327 SULLO SPAZIO EUROPEO DEI DATI SANITARI*

*Mario Natale – Onofrio Troiano***

SOMMARIO:

This article examines the objective and subjective scope of Regulation (EU) 2025/327 on the European Health Data Space through a systematic reading of the EHDS in relation to the GDPR and the EU legal framework on data governance. It argues that the Regulation's field of application cannot be determined solely by reference to the nature of electronic health data, whether personal or non-personal, but requires a functional qualification of the processing operation, centred on the distinction between primary and secondary use. This functional criterion also allows the article to address borderline cases, including telemedicine, informal communication channels, sports, wearable devices and post-mortem health data, and to reconstruct the role of the main actors under the EHDS: the natural person, the healthcare professional, the healthcare provider, the health data holder and the health data user.

Keywords: Electronic health data - Primary and secondary use - Functional qualification of processing - Health data holder - Health data user.

I. BREVE PREMESSA METODOLOGICA

La trattazione degli ambiti rispettivamente oggettivo e soggettivo del recente Regolamento (UE) 2025/327 (EHDS)[1] si presenta complessa per la varietà di variabili che determinano l'individuazione dell'oggetto e dei soggetti e per la circostanza che, non poche volte, la disciplina va coordinata con precedenti atti normativi, anzitutto il regolamento generale (UE) 2016/679 (GDPR). Perciò si è preferito affrontare la nostra problematica con un approccio che potremmo definire casistico, ma non nel senso tradizionale di privilegiare le applicazioni giurisprudenziali, ancora a venire, ma nel senso di chiarire il significato e la

* 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*".

** Nell'ambito del presente articolo, condiviso da entrambi gli Autori, il dott. Mario Natale ha redatto i §§ 2, 4, 7, 8, 9 e 10, mentre il prof. Onofrio Troiano i §§ 1, 3, 5 e 6.

[1] 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. Nell'ultimo anno la novella disciplina è stata oggetto di alcuni studi monografici e collettanei: v. A. FIORENTINI, *Lo spazio europeo dei dati sanitari. Nuovi equilibri costituzionali tra mercato unico digitale e Unione europea della salute*, Torino, 2026; A. MORACE PINELLI (a cura di), *Sanità digitale. Regolamento "EHDS" (UE 2025/327) sullo spazio europeo dei dati sanitari*, I, *Uso dei dati e assetti organizzativi*, Pisa, 2025; ID. (a cura di), *Sanità digitale. Regolamento "EHDS" (UE 2025/327) sullo spazio europeo dei dati sanitari*, II, Commentario, Pisa, 2026; S. CORSO, *Autodeterminazione e dati sanitari,* Torino, 2025; F. TRUBIANI (a cura di), *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari. Un dialogo multidisciplinare,* Torino, 2025; C. DE MENECH - M. FOGLIA (a cura di), *Autodeterminazione, cura e ricerca nell'era digitale. Interessi antagonisti e modelli di bilanciamento*, Torino, 2026.

rilevanza di alcuni concetti chiave intorno a cui ruota l'intera disciplina, ad iniziare da quello di "dati sanitari elettronici". Prima di analizzare tali aspetti, è necessario chiarire l'ambito geografico al cui interno opererà la novella disciplina europea.

II. SPAZIO EUROPEO DEI DATI SANITARI: CONFINI E APPLICAZIONI

Lo Spazio Europeo dei Dati Sanitari (*European Health Data Space*, EHDS) è un ambizioso intervento normativo dell'Unione europea nel settore della sanità digitale, pensato per offrire un quadro comune per la condivisione e la gestione dei dati sanitari elettronici. Maturato nel solco della Strategia europea dei dati e del rilancio dell'Unione della salute dopo la pandemia da COVID-19, l'EHDS segna un cambio di passo[2], che supera la precedente cooperazione volontaria (dir. 2011/24/UE) e introduce uno standard vincolante e interoperabile per lo scambio transfrontaliero delle cartelle cliniche elettroniche (*Electronic Health Record*, EHR)[3].

La portata dell'EHDS non si arresta ai confini degli Stati membri. Il suo orizzonte coincide con lo spazio giuridico dell'Unione e si proietta nello Spazio economico europeo (SEE)[4], ove l'infrastruttura di rete opera in via nativa[5]. L'architettura resta aperta a collegamenti con Paesi terzi e organizzazioni internazionali (quali l'OMS) mediante i nodi *MyHealth@EU* (uso primario) e *HealthData@EU* (uso secondario), ove necessario tramite intese dedicate, nel rispetto cumulativo del Capo V GDPR e delle condizioni speciali

[2] La pandemia ha messo a nudo i *deficit* d'interoperabilità e di accesso tempestivo a dati sanitari transfrontalieri; l'EHDS nasce per assicurare circolazione effettiva dei dati elettronici a sostegno di continuità delle cure, resilienza/sostenibilità dei sistemi e ricerca-innovazione: cfr. Comm. UE, Comunicazione 19 febbraio 2020, «Una strategia europea per i dati», COM(2020) 66 final, con osservazioni di F. RUGGERI, in *Persona e mercato*, 2022, 150; Comm. UE, Comunicazione 11 novembre 2020, «Costruire un'Unione europea della salute: rafforzare la resilienza dell'UE di fronte alle minacce sanitarie transfrontaliere», COM(2020) 724 final; Reg. (UE) 2022/2371, sulle gravi minacce transfrontaliere per la salute; Reg. (UE) 2021/522 (programma EU4Health); Reg. (UE) 2021/953 (Certificato COVID digitale UE); nonché Reg. (UE) 2025/327 (EHDS), Considerando 1 e 2.

[3] Dal modello volontario della rete *eHealth* di cui all'art. 14 dir. 2011/24/UE si passa, con il Reg. (UE) 2025/327, a una cornice cogente e uniforme: tipizzazione delle categorie prioritarie per l'uso primario (art. 14, §1), definizione di struttura, metadati e requisiti minimi (All. I), ancoraggio all'EEHRxF, nonché istituzione dei servizi *MyHealth@EU* (artt. 23-24). L'art. 103 abroga l'art. 14 dir. 2011/24/UE con effetto dal 26 marzo 2031.

[4] L'EHDS è un regolamento dell'Unione e, in quanto tale, si applica direttamente e in modo uniforme negli Stati membri, senza necessità di recepimento (art. 288, § 2, TFUE). La sua estensione allo Spazio economico europeo (SEE) non è automatica: essa interviene solo quando l'atto è incorporato nell'Accordo SEE tramite decisione del Comitato misto SEE, con eventuali adattamenti (art. 7 e 102 Accordo SEE). A seguito di tale incorporazione, l'EHDS diventa vincolante anche per Islanda, Liechtenstein e Norvegia secondo le modalità previste dall'Accordo e dalle corrispondenti misure interne di attuazione negli Stati EFTA, nel rispetto del principio di omogeneità dell'ordinamento del mercato interno esteso.

[5] Nel perimetro unionale «allargato», il Reg. (UE) 2025/327 disegna un'architettura bifronte: *MyHealth@EU*, per l'uso primario, quale piattaforma centrale con punti di contatto nazionali deputati allo scambio transfrontaliero di dati sanitari elettronici tra Stati membri (artt. 23-24 EHDS); e *HealthData@EU*, per l'uso secondario, come rete degli organismi responsabili dell'accesso ai dati degli Stati membri, funzionale a ricerca, innovazione e sanità pubblica (art. 66 ss., in specie 66 e 75 EHDS).

dell'EHDS su collegamenti, ammissibilità e controllo[6]. Ne risulta un vero «mercato unico» dei dati sanitari, che non cancella gli ordinamenti nazionali ma li coordina[7].

Senza infrastrutture, però, il disegno resta sulla carta. Spetta agli Stati membri agganciare i fascicoli sanitari elettronici alla rete *MyHealth@EU*, rafforzare le dorsali digitali e attivare i nuovi snodi di *governance* – le autorità di sanità digitale per l'uso primario e gli organismi di accesso ai dati per l'uso secondario – così da tradurre in pratica diritti e doveri previsti dal regolamento[8].

Sul versante dell'uso primario, il collegamento di punti di contatto nazionali di Paesi terzi o di sistemi istituiti da organizzazioni internazionali è consentito solo previa adozione di atti di esecuzione della Commissione, nel segno di una reciprocità sostanziale: l'accesso ai dati da parte di soggetti dell'Unione nel Paese terzo deve avvenire alle stesse condizioni e con le stesse garanzie vigenti all'interno dell'UE[9]; la Commissione tiene un elenco pubblico dei collegamenti autorizzati e può disporre la disconnessione ove vengano meno i presupposti[10].

Specularmente, per l'uso secondario, Paesi terzi e organizzazioni internazionali possono partecipare a *HealthData@EU* solo se rispettano il Capo IV e garantiscono agli utenti UE condizioni di accesso equivalenti. Le richieste di soggetti extra-UE sono ammissibili se: (i) il Paese è autorizzato con atto di esecuzione; oppure (ii) la Commissione, con distinto atto di esecuzione, attesta che l'accesso per gli utenti UE non è più restrittivo di quanto previsto dal Regolamento[11].

Particolare attenzione è riservata ai dati elettronici non personali che presentano un rischio concreto di re-identificazione: sono qualificati "altamente sensibili" e protetti da misure definite con atto delegato[12]. Restano imprescindibili l'uso di ambienti di trattamento sicuri

---

6 Per i collegamenti *extra*-UE, le norme-cardine sono: per l'uso primario, art. 24 EHDS (*MyHealth@EU*: atti di esecuzione della Commissione, elenco pubblico dei nodi autorizzati, disconnessione: in specie § 3; Considerando 94 e 105); per l'uso secondario, art. 75, § 5 EHDS (partecipazione di Paesi terzi a *HealthData@EU*) e art. 90 (ammissibilità delle richieste extra-UE, atti di esecuzione, monitoraggio/abrogazione), nel quadro istituito dagli art. 66 ss. In ogni caso, resta applicabile cumulativamente il Capo V GDPR (Reg. (UE) 2016/679, artt. 45-49).

7 C. JANDA, *Digitalisation of health data and their interoperability in the European Union*, in *Ceridap*, 2022, 55, nota 18.

8 Cfr. Reg. (UE) 2025/327, Capi II («Uso primario») e IV («Uso secondario»); quanto al primo obiettivo (*empowerment* dei pazienti), artt. 3-10 e All. I; quanto al secondo (riuso a fini di interesse generale), art. 53 e artt. 66-75; nonché Considerando 1, 2 e 27.

9 Un banco di prova concreto è il Regno Unito. In tema di trasferimenti di dati personali, le decisioni di adeguatezza GDPR dell'UE sono state oggetto di proroga tecnica sino al 27 dicembre 2025, al fine di consentire la valutazione dell'impatto della *Data (Use and Access) Act* 2025 (DUAA) sul livello di protezione britannico; il 21 luglio 2025 la Commissione ha posto in consultazione la bozza di decisione di rinnovo, segnalando, in linea di principio, un quadro «essenzialmente equivalente». In attesa della decisione definitiva, resta aperta – ai fini EHDS – la verifica che l'accesso ai dati da parte di professionisti dell'UE nel Regno Unito avvenga effettivamente «alle stesse condizioni e con le stesse garanzie» (v. Reg. (UE) 2025/327, art. 24, Considerando 94 e 105). In caso di regressione (ad es., irrigidimento sui diritti degli interessati o mutamento del regime di riutilizzo), la Commissione dovrebbe revocare l'atto di esecuzione e disconnettere il nodo UK da *MyHealth@EU*, con effetti immediati su *ePrescription* e *patient summary* e, dunque, sulla continuità assistenziale transfrontaliera.

10 Reg. (UE) 2025/327, Considerando 94 e 105; art. 24.

11 È previsto un monitoraggio periodico, con possibilità di revoca se le condizioni vengono meno: cfr. Reg. (UE) 2025/327, art. 75, § 5, e art. 91, §§ 1-3; oltre al Capo V Reg. (UE) 2016/679 (GDPR).

12 Per questi dati valgono tutele rafforzate *ex* art. 88 Reg. (UE) 2025/327 (v. anche Considerando 82) in combinato disposto con l'art. 5, § 13 del Reg. (UE) 2022/868 (*Data Governace Act*).

e la minimizzazione dei dati. In sintesi: la circolazione è possibile solo se l'ecosistema esterno è allineato a regole, garanzie e rimedi europei, con atti di esecuzione che regolano ammissione e revoca nel tempo[13].

Sul piano sistematico, lo Spazio europeo dei dati sanitari va letto come applicazione settoriale del principio di libera circolazione dei dati nel quadro del «Mercato unico digitale»[14]. La sua genesi si colloca infatti nella scia del Reg. (UE) 2018/1807, che ha sancito la libera circolazione dei dati non personali nell'Unione, e degli atti orizzontali di *data law*: il Reg. (UE) 2022/868 (*Data Governance Act*) e il più recente Reg. (UE) 2023/2854 (*Data Act*). Sul piano delle fonti, il Regolamento si affianca alla normativa UE già vigente in materia di sanità digitale e mobilità dei pazienti[15]; non intende sostituirla, bensì coordinarla, delineando un quadro orizzontale per la circolazione – primaria e secondaria - dei dati sanitari[16].

---

[13] Cfr. K. Ó CATHAOIR, *The EHDS and Electronic Health Records. GDPR+ or Transforming Patients' Rights?*, in S. Slokenberga – K. Ó Cathaoir – M. Shabani (a cura di), *The European Health Data Space. Examining a New Era in Data Protection*, Routledge, 2025, 22 ss., spec. §§ 2.1-2.2, ove si registra il passaggio dall'opzionalità all'obbligatorietà del Formato europeo di scambio e dell'interoperabilità delle EHR, con atti di esecuzione della Commissione che determinano le soglie minime di qualità/interoperabilità e fungono da condizione per la connettività e per la portabilità transfrontaliera effettiva cui i prestatori devono allinearsi; nonché J. REICHEL, *Administrative tools for balancing societal and individual interests. Data protection safeguards and administrative procedural guarantees in secondary use in the European Health Data Space*, ivi, cap. 10, sulla proceduralizzazione dell'ammissibilità nell'uso secondario e sul ruolo degli atti esecutivi come *«switch»* che consentono di aprire il circuito a nuove domande di riuso, di aggiornare condizioni e garanzie, o, se necessario, di revocare autorizzazioni e collegamenti. In tal modo, la Commissione diventa garante dell'equilibrio tra interessi collettivi (ricerca, innovazione, sanità pubblica) e diritti individuali, con la possibilità di modulare nel tempo l'accesso e la circolazione.

[14] La nozione di «Mercato unico digitale» discende dalla strategia delineata dalla Commissione europea nella Comunicazione COM(2015) 192 *final, «Una strategia per il mercato unico digitale in Europa»*, quale articolazione della politica di mercato interno (art. 26 TFUE), fondata sulla base giuridica dell'art. 114 TFUE per le misure di armonizzazione e integrata dal diritto fondamentale alla protezione dei dati personali (art. 16 TFUE; artt. 7-8 Carta UE). Tra gli atti di attuazione più rilevanti: Reg. (UE) 2018/1807 (libera circolazione dei dati non personali), Reg. (UE) 2022/868 (*Data Governance Act*), Reg. (UE) 2023/2854 (*Data Act*), dir. (UE) 2019/770 (contratti digitali), dir. (UE) 2019/790 (*copyright* digitale).

[15] L'art. 1, §§ 3-8, Reg. (UE) 2025/327 reca la clausola di salvaguardia: restano «impregiudicati» gli atti UE settoriali vigenti – tra cui GDPR, ePrivacy, DGA, *Data Act*, Reg. 2018/1725, *Clinical Trials*, *Trade Secrets*, MDR/IVDR e *AI Act* – che continuano a presidiare i profili specifici dell'uso dei dati sanitari elettronici. In filigrana all'EHDS sta la dir. 2011/24/UE, che ha aperto la via all'interoperabilità degli EHR e allo scambio transfrontaliero via nodi nazionali. Il fondamento di diritto primario combina art. 16 TFUE (protezione dati) e 114 TFUE (mercato interno), legittimando una disciplina unitaria che saldi diritti fondamentali e funzionamento del mercato: cfr. M. IASELLI, *Le nuove regole per l'uso primario e secondario di dati sanitari*, Maggioli Editore, Santarcangelo di Romagna, 2025, 11 ss.

[16] C. PERLINGIERI, *Transizione digitale nella sanità ed ecosistema dei dati sanitari: profili ricostruttivi del fenomeno circolatorio e implicazioni sui dati genetici*, in *Tecn. e dir.,* 2024, 485 ss., che sottolinea l'esigenza di un raccordo chiaro tra le discipline orizzontali (Reg. (UE) 2018/1807; Reg. (UE) 2022/868 e Reg. (UE) 2023/2854) e la normativa settoriale di sanità digitale, per evitare zone d'ombra di *accountability* nelle fasi di interoperabilità, autorizzazione e circolazione; con particolare cautela per i dati genetici (rischio di re-identificazione) e un monito contro derive mercantilistiche, a tutela della centralità della persona e dei necessari controlli e rimedi.

III. AMBITO DI APPLICAZIONE OGGETTIVO: I DATI SANITARI ELETTRONICI

Lo spazio europeo dei dati sanitari, istituito con il Regolamento UE 2025/327 dell'11 febbraio 2025, persegue il fine di «facilitare l'accesso ai dati sanitari elettronici» per il loro uso primario e secondario[17].

Tra le disposizioni che definiscono la materia regolata un ruolo primario è rivestito dai "dati sanitari elettronici", nozione che, ai sensi dell'art. 2, lett. c), comprende sia i dati "personali", sia quelli "non personali", questi ultimi definiti in via residuale perché comprendono (art. 2, lett. b) tutti i dati sanitari elettronici «diversi dai dati sanitari elettronici personali», inclusi i dati anonimizzati e quelli «che non si sono mai riferiti ad un interessato»[18].

La nozione di "dati sanitari elettronici personali" rimanda anzitutto a quella più ampia di "dato personale", per la cui definizione – specifica il regolamento all'art. 1, lett. a) – bisogna

[17] Reg. (UE) 2025/327, art. 1, §1 Per una prima ricognizione della normativa v. S. FAILLACE, *I diritti dell'interessato nell'uso primario dei dati sanitari elettronici secondo il nuovo regolamento EHDS*, in *Contr. e impr.*, 2025, 379 e ss.; S. CORSO, *Lo spazio europeo di dati sanitari. Prime riflessioni sul regolamento UE 2025/327*, in *Nuove leggi civ. comm.,* 2025, 563; S. THOBANI, *Verso il regolamento UE sullo spazio europeo di dati sanitari (European Health Data Space)*, in *Persona e mercato* 2024, 1393 e ss., nonché, con riferimento alla precedente Proposta, C. PERLINGIERI, *Transizione digitale nella sanità ed ecosistema dei dati sanitari: profili ricostruttivi del fenomeno circolatorio e implicazioni sui dati genetici*, cit., 485, 490 e ss.; M.R. NUCCIO, *Digitalizzazione e circolazione di dati sanitari*, in *Tecn. e dir.,* 2024, 357, il quale specifica a p. 361, che "l'ipotesi dell'uso primario dei dati soggiace, pur sempre, all'applicazione degli articoli 6 e 9 del GDPR" in quanto la disciplina dell'EHDS "non sostituisce ma completa quanto in via generale disposto dalla normativa in materia di protezione dei dati personali" e poi, a proposito dell'uso secondario, osserva, a pagg. 372-373, che "in campo medico vigerebbe una presunzione di compatibilità tra "finalità iniziale" sovente integrata dalla diagnosi e cura, e "finalità secondaria di ricerca". Sicché, qualora il trattamento principale sia stato autorizzato dall'interessato, l'avvio di quello secondario non necessiterebbe del consenso". In proposito v. F.G. VITERBO, *Principi di trattamento e di* governance *dei dati personali in ambito sanitario*, in *Rass. dir. civ.*, 2023, 1443. L'Autore rileva come nei più recenti sviluppi normativi – alimentati dal dato di fatto che i dati personali sanitari "possono acquistare sia un elevato valore commerciale nel mercato (...) sia un valore estremamente rilevante sul piano sociale in funzione della loro centralità per la ricerca scientifica (...) ma anche per la gestione della *policy* relativa alla sanità pubblica" – "la base giuridica del trattamento si rinviene in misura sempre più preponderante al di fuori del consenso dell'interessato" (pp. 1450-1451). Certamente le esigenze di condivisione e di riutilizzo dei dati sanitari non sempre possono conciliarsi con la logica del consenso come base di trattamento e sempre più emergono esigenze di elevare a base del trattamento ragioni di interesse generale alla diffusione di tali dati. Nell'ambito della nuova strategia europea dei dati, questi vengono considerati "come risorsa per la creazione di nuovi prodotti e servizi, nonché come strumento di sviluppo delle imprese e, quindi, di crescita economica" (ID., cit., 1461). In sostanza, una prospettiva in cui il valore dei dati, sia sul piano del progresso delle cure sanitarie, sia della ricerca scientifica, si accresce grazie al loro uso ripetuto e circolazione (G. LOFARO, *Dati sanitari e* E-Health *europea tra trattamento dei dati personali e decisione amministrativa algoritmica*, in *Media Laws* 2023, 179, spec. 206 e ss.). Nondimeno – sempre a parere di F.G. VITERBO, *Principi di trattamento e di* governance *dei dati personali in ambito sanitario*, cit., 1465, - è opportuno "escludere l'equiparazione tra l'uso secondario (...) per scopi di interesse generale quali la ricerca scientifica o la sperimentazione *no profit*, (...) e (...) il riutilizzo dei dati per attività strumentali al perseguimento di scopi industriali o commerciali – ancorché pur sempre inerenti all'ambito scientifico/sanitario – da parte di soggetti privati … [nel qual caso] … sarebbe necessario acquisire un nuovo consenso dagli interessati" ai sensi dell'art. 110 codice *privacy*. Sulle problematiche del superamento della prospettiva del (necessario) consenso dell'interessato, v. pure in questo volume il contributo di V.V. CUOCCI, *Uso secondario dei dati sanitari e interesse generale alla ricerca: riflessioni sul Regolamento sullo Spazio Europeo sui Dati Sanitari e sul Regolamento Generale sulla Protezione dei Dati Personali*, § 1 e di L. BOZZI, *Uso primario dei dati e fascicolo sanitario elettronico: non è solo una questione di privacy...*, § 5.

[18] In tema v. pure le riflessioni di L. BOZZI, *Uso primario dei dati e fascicolo sanitario elettronico: non è solo una questione di privacy...*, cit., § 1, che evidenzia differenze sostanziali tra la definizione dell'art. 2 e quanto si ricava dalla lettura del Considerando 6, sempre a proposito del dato sanitario elettronico.

fare riferimento all'art. 4 della disciplina del regolamento 2016/679, normativa generale sul trattamento dei dati all'interno della UE[19].

Il numero 1) di quest'ultimo articolo definisce quale dato personale «qualsiasi informazione riguardante una persona fisica identificata o identificabile», e pertanto integra la nozione di "dati sanitari elettronici personali", che riguarda specificatamente, ai sensi dell'art. 2.2, lett. a), del regolamento 2025/327, i «dati relativi alla salute ed i dati genetici...». Di conseguenza, i dati sanitari elettronici personali sono da intendersi quali dati relativi alla salute, ovvero dati genetici, che riguardano una persona fisica identificata o identificabile[20].

Come esposto, la più recente disciplina amplia lo spettro applicativo rispetto alla disciplina generale contenuta nel regolamento del 2016 perché quest'ultimo fa riferimento ai soli dati personali mentre il regolamento 2025/327 disciplina tutti i dati sanitari, anche quelli non personali, nel senso che non sono riferibili, o non sono più riferibili, ad una persona determinata o determinabile[21].

La differenza si spiega proprio con il differente ambito oggettivo. Il regolamento 2025/327, sebbene circoscritto ai dati sanitari, ha ambiti applicativi molto differenti, contrassegnati dall'uso primario e dall'uso secondario. La disciplina dell'uso primario nella sua applicazione concreta è riferita ai dati di un singolo paziente e tratta dati (sanitari) personali[22]. L'uso secondario richiede invece l'accesso alle «informazioni sanitarie raccolte nelle strutture pubbliche e private» per, ad esempio, "scopi scientifici e tecnologici" al fine «di sviluppare cure più efficaci, migliorare la prevenzione e favorire un'assistenza sanitaria più personalizzata e tempestiva». Ha quindi necessità di un ampio patrimonio informativo

---

[19] Per l'analisi della disciplina dei dati sensibili nel Regolamento 2016/679 v. M. GRANIERI, *Il trattamento di categorie particolari di dati personali nel Reg. UE 2016/679*, in *Nuove leggi civ. comm.,* 2017, 165, spec. 188 e ss., con serrata critica della disciplina dell'art. 9 (e del generale impianto del regolamento) definita come "un ammasso di regole disposte orizzontalmente … non strutturate secondo la logica del generale, speciale, eccezionale", difficile da ricondurre ad un insieme dotato di coerenza.

[20] V.V. CUOCCI, *Uso secondario dei dati sanitari e interesse generale alla ricerca: riflessioni sul Regolamento sullo Spazio Europeo sui Dati Sanitari e sul Regolamento Generale sulla Protezione dei Dati Personali*, cit., §§ 2.2, rileva come l'articolo citato testualmente faccia riferimento ai "dati relativi alla salute e i dati genetici …" non ponendoli in alternativa e lasciando spazio ad una possibile interpretazione, a cui tenore il nuovo regolamento trovi applicazione solo quando siano trattati entrambi congiuntamente, dubbio tuttavia fugato, a parere dell'Autrice, dall'interpretazione sistematica con altre norme.

[21] Con una recentissima decisione, pur concentrandosi su aspetti diversi non rilevanti in questa sede, la CGUE 04 settembre 2025 (causa C-413/23P) si è anche pronunciata sull'interpretazione di "dati personali", analogamente definiti, sia nel Regolamento 2018/1725, sia nel Regolamento 2016/679 come pure nella direttiva che lo ha preceduto. Si trattava di stabilire se, in tale definizione, rientrino – come sostenuto dal Garante europeo dei dati personali – i dati personali pseudonimizzati in quanto non sottratti all'applicazione del diritto europeo quando «trasmessi ad una entità esterna al titolare del trattamento, che non dispone di informazioni aggiuntive che consentano di identificare l'interessato» (punto 64) senza perciò che possano assimilarsi a dati anonimi. In sostanza si trattava di decidere se la disponibilità di informazioni aggiuntive, che consentano di identificare una persona i cui dati sono stati pseudonimizzati, renda tali ultimi dati personali, sebbene dette informazioni aggiuntive siano nel solo possesso del titolare del trattamento e non degli ulteriori soggetti a cui sono stati comunicati. La Corte invita a distinguere le ipotesi in cui i dati pseudonimizzati trasmessi a terzi dal titolare del trattamento possano consentire a detti terzi di individuare i soggetti interessati, rendendoli identificabili (ad esempio tramite un controllo incrociato con dati di cui si dispone), dai casi in cui tale possibilità è preclusa con la conseguenza che, per il terzo, non sarà più possibile procedere ad identificazione, partendo dal dato pseudonimizzato.

[22] L'intento è favorire la prestazione di servizi sanitari alle persone fisiche ovunque si trovino nello spazio europeo garantendo "la portabilità e il pieno diritto di accesso ai loro dati sanitari personali": E. SORRENTINO-A.F. SPAGNUOLO, *Gestione e conservazione di dati sanitari. Il* vulnus *normativo che impatta su sicurezza e* data protection, in *Federalismi*, n. 29/2024, 137, 143.

e grandi volumi di dati sanitari da elaborare con analisi quantitative condotte con il supporto dell'intelligenza artificiale, ad esempio per migliorare i protocolli sanitari[23]. Ma i dati sanitari per tale uso sono pseudonimizzati o anonimizzati, e quindi assumono forma non personale[24].

L'ambito applicativo dei dati sanitari elettronici personali differisce da quello dei dati non personali perché la disciplina del regolamento 2025/327 riguarda solo i dati sanitari elettronici personali "trattati in formato elettronico" e pertanto non si applica ad un trattamento di tipo più tradizionale[25]. Va da sé tuttavia che la conversione di un originario dato elettronico in dato analogico (documentale) non consente di eludere l'applicazione della normativa. Occorre fare riferimento alla circostanza che il dato sia originariamente elettronico, ma andranno sicuramente ricompresi i dati originariamente analogici (una 'antica' cartella clinica) se successivamente processati in via elettronica. Gli unici dati che sfuggono alla disciplina sono quelli originariamente analogici e che tali permangono.

La limitazione del trattamento in formato elettronico non è ripetuta nella successiva lettera b), con riferimento ai dati sanitari elettronici non personali, a cui pertanto la disciplina si applicherà in ogni caso.

La nozione di "dati sanitari elettronici personali" riguarda, come già esposto, sia i "dati relativi alla salute", sia i "dati genetici", per la cui definizione – specifica il regolamento all'art. 1, lett. a) – bisogna ancora una volta fare riferimento all'art. 4 della disciplina generale del regolamento 2016/679.

I numeri 15 e 13 di tale articolo definiscono, rispettivamente, i dati relativi alla salute quali «dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute» ed i dati genetici quali «dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione».

Quanto ai "dati relativi alla salute", essi rivelano informazioni relative allo stato di salute di una persona fisica: rientrano perciò non solo i dati relativi ad eventuali patologie o all'assenza di patologie, ma anche tutti quei dati dai quali, indirettamente, possano ricavarsi informazioni sullo stato di salute di una persona fisica, quali, ad esempio, l'informazione

[23] M. IASELLI, *Le nuove regole per l'uso primario e secondario di dati sanitari*, cit., 22-23. Tali peculiarità inducono la dottrina e lo stesso legislatore europeo a cercare basi giuridiche diverse dal consenso per legittimare il trattamento, evidenziandosi come la tradizionale prospettiva consensocentrica, adoperata dallo stesso regolamento generale del 2016 e basata sulla necessità di chiedere l'esplicito consenso a ciascun interessato, salva sempre la possibilità di revocarlo in momenti successivi, non consenta più un efficiente regolamentazione degli interessi in gioco, specie quando si tratti di uso dei dati per finalità di addestramento dei sistemi di intelligenza artificiale: in tema, da ultimo, v. 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. medicina legale*, 2025, 85. Per alcuni esempi concreti di uso di dati sanitari elettronici in sistemi di intelligenza artificiale v. F. CASCINI, *Secondary Use of Electronic Health Data*, Springer, 2025, 87 e ss.

[24] Ma sulla possibilità di re-identificare dati anonimizzati v. A. MANTELERO, *La* privacy *all'epoca dei* big data, in V. Cuffaro, R. D'Orazio, V. Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino 2019, 1190.

[25] S. CORSO, *Lo spazio europeo di dati sanitari. Prime riflessioni sul regolamento UE 2025/327*, cit., 571-573.

sull'acquisto di un'apparecchiatura di ausilio alla mobilità, fatta presso un rivenditore o l'acquisto di medicinali in farmacia o una ricetta medica[26].

In ogni caso, i "dati relativi alla salute" sono nozione diversa dai dati sanitari elettronici perché questi ultimi, a differenza dei primi, possono anche essere non personali[27].

La descritta definizione normativa dei "dati relativi alla salute" non contiene alcuna restrizione ai dati "elettronici", in quanto tratta dal regolamento generale del 2016, che non fa alcun riferimento a tale restrizione. E tuttavia il più recente regolamento 2025/327 fa riferimento ai "dati relativi alla salute" comprendendoli nella più ampia nozione di "dati sanitari elettronici personali". Per tale ragione sembra opportuno considerare, in sede interpretativa, tale contesto e perciò propendere a ritenere che il rinvio alla nozione di "dati relativi alla salute" come definita dal regolamento del 2016 vada inteso, nell'ambito del regolamento 2025/327 come riguardante i soli dati elettronici.

Per la stessa ragione, anche il riferimento ai dati genetici credo vada inteso come ristretto ai soli dati in forma elettronica.

Sotto un differente profilo, va osservato che le definizioni di "dati relativi alla salute" e di "dati genetici" fanno riferimento alla persona fisica e potrebbero indurre a ritenere che la sua esistenza sia requisito di applicazione della normativa[28].

Il regolamento 2025/327 nulla dice in proposito; l'art. 2, numero 9), che menziona i casi in cui il regolamento "non si applica", non fa cenno a tale ipotesi.

Peraltro, potrebbe revocarsi in dubbio che, una volta cessata la vita di una persona fisica, possa continuarsi a parlare di "dati sanitari elettronici personali" piuttosto che di "dati sanitari elettronici non personali" la cui definizione, come anticipato, comprende non solo i dati non riferibili ad un interessato, ma pure (art. 2, lett. b) tutti i dati sanitari elettronici «diversi dai dati sanitari elettronici personali».

A voler ritenere che il regolamento si applichi solo ai dati relativi a persone ancora in vita, si dovrebbe concludere per la libera circolazione dei dati sanitari elettronici personali successivamente al decesso dell'interessato: uso libero.

Questa conclusione va però temperata con riferimento ai "dati genetici", che non sono esclusivi di una singola persona fisica ed appartengono, nel senso di essere comuni, alla comunità che li condivide. Per tale ragione, il decesso di una persona fisica non implica la cessazione di ogni interesse alla loro diffusione. E tanto, sia che si tratti – argomentando dalla nozione sopra riportata – delle "caratteristiche genetiche ereditarie", sia di quelle

---

[26] V. da ultima Corte di Giustizia UE, grande sezione, 04.10.2024 (causa C-21/23), in *Nuova giur. civ. comm.,* 2025, 588 con nota parzialmente critica 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?* Nella specie, una farmacia aveva intrapreso la vendita, attraverso Amazon Marketplace, di prodotti non soggetti a prescrizione medica, previa raccolta di dati personali dell'ordinante, che doveva inserire dati necessari per il compimento dell'operazione di acquisto (nome, indirizzo, tipologia del medicinale, ecc.). La Corte non ha dubbi nel ritenere che tali dati, in quanto idonei a rivelare le condizioni di salute, siano da qualificarsi "dati relativi alla salute" ai sensi del regolamento 2016/679 e pertanto assoggettati alla stringente disciplina divisata dallo stesso (art. 9: divieto di trattamento, salvo eccezioni). Nella nota l'a. evidenzia alcuni rischi che, a suo parere, potrebbero scaturire da una nozione "eccessivamente ampia di dato sensibile".

[27] S. CORSO, *Lo spazio europeo di dati sanitari. Prime riflessioni sul regolamento UE 2025/327*, cit., 571. Da ultima v., in questo volume, A. ADDANTE, *Vicende circolatorie ed esercizio dei diritti nell'uso primario dei dati sanitari*, § 3.

[28] Con particolare riferimento alla definizione di "dati relativi alla salute", v. A. IULIANI, *Gli incerti confini della nozione di "dati relativi alla salute"*, in C. DE MENECH, M. FOGLIA (a cura di), *Autodeterminazione, cura e ricerca nell'era digitale. Interessi antagonisti e modelli di bilanciamento*, cit., 237.

"acquisite di una persona fisica" perlomeno nella misura in cui il raggio di azione di queste ultime non si esaurisce nell'ambito di una singola persona fisica, ma è condiviso con la comunità di appartenenza.

La conclusione, con la predetta precisazione, dell'applicabilità della normativa solo alle persone fisiche in vita assume rilievo con esclusivo riferimento all'uso secondario (l'uso primario termina con il decesso dell'interessato) e, volendo postulare che, nei limiti predetti, non trovi più applicazione la disciplina del regolamento (applicabile ai soli dati sanitari elettronici personali di una persona fisica vivente) si dovrà comunque prospettare, laddove vi siano ulteriori interessi in gioco rispetto a quello del richiedente, l'opportunità di una loro valutazione comparativa.

Da questo punto di vista il regolamento non fornisce alcuna disciplina perché detta regole di composizione di interessi con riferimento alla permanenza in vita della persona fisica.

Saremmo quindi a fronte di un vuoto normativo, da risolversi in via interpretativa.

Nella legislazione italiana, la disciplina del Codice della *privacy* – cogliendo la possibilità offerta dal regolamento generale 2016/679 e concessa agli Stati membri di introdurre norme a tutela delle persone decedute[29] – contiene una norma sui diritti riguardanti le persone decedute (art. 2-*terdecies*), ma non è dato rinvenire alcuna disposizione analoga, né nel regolamento generale 2016/679, né, come già detto, nel regolamento 2025/327. Non può quindi una norma nazionale sortire alcun ausilio interpretativo di una disciplina eurounitaria, ma ciò non esclude che la predetta normativa nazionale possa rivestire interesse al solo scopo di un'utile ricognizione di modelli differenti[30].

La norma in questione fa riferimento ai diritti «di cui agli articoli da 15 a 22 del regolamento» relativi a dati personali di persone decedute: si tratta, nello specifico, del diritto di accesso, di rettifica, alla cancellazione (oblio), di limitare il trattamento, obblighi di notifica delle rettifiche, cancellazioni e limitazioni del trattamento, diritto alla portabilità dei dati, diritto di opposizione, diritto di non essere sottoposto ad una decisione basata esclusivamente su trattamenti automatizzati, compresa la profilazione.

L'esercizio di tali diritti *post mortem* da parte di terzi è ristretto: occorre che si abbia «un interesse proprio» (come potrebbe accadere per i dati genetici), oppure che si agisca a tutela dell'interessato «in qualità di suo mandatario o per ragioni familiari meritevoli di protezione» ed anche in tale ambito, l'esercizio *post-mortem* di tali diritti è escluso in presenza di un espresso divieto del *de cuius* comunicato al titolare del trattamento, sebbene «limitatamente all'offerta diretta di servizi della società dell'informazione» (divieto che però non può pregiudicare, né l'esercizio di diritti patrimoniali che derivano a terzi dalla morte dell'interessato, né il diritto di difendere in giudizio i propri interessi).

Va inoltre considerato che la disciplina nazionale testé richiamata riguarda i dati personali in generale e può trovare difficoltà applicative quando applicata allo specifico ambito dell'uso secondario di dati sanitari. Difficile, anche se non impossibile, appare rinvenire "un interesse proprio" di un terzo a contrastare l'uso secondario di tali dati (salvo quanto

[29] V., *infra*, il contributo di V.V. CUOCCI, *Uso secondario dei dati sanitari e interesse generale alla ricerca: riflessioni sul Regolamento sullo Spazio Europeo sui Dati Sanitari e sul Regolamento Generale sulla Protezione dei Dati Personali*, cit., § 3.

[30] Con riferimento alla disciplina italiana richiamata in testo v. C. PERLINGIERI, *Transizione digitale nella sanità ed ecosistema dei dati sanitari: profili ricostruttivi del fenomeno circolatorio e implicazioni sui dati genetici*, cit., 501 e ss.

già esposto per i dati genetici), ovvero la presenza di ragioni di tutela dell'interessato, come pure quella delle ragioni familiari.
Se si condivide tale impostazione dovrà convenirsi che, in linea di massima, l'uso di dati sanitari elettronici personali successivamente al decesso dell'interessato sarà di regola consentito, nel senso di libero e senza restrizioni di sorta, salvo quanto appena detto per i dati genetici, in presenza di controinteressati della comunità di appartenenza.
Concludere nel senso che l'uso di dati sanitari elettronici personali è libero successivamente al decesso dell'interessato, comporta precludere qualsiasi possibilità di valorizzazione patrimoniale di tali dati da parte di successivi titolari (eredi o legatari).
Questa conclusione potrebbe tuttavia essere parzialmente inficiata ove si ritenga applicabile, anche *post mortem*, quella norma del regolamento 2025/327 (art. 71), che attribuisce ad ogni persona fisica il diritto di poter escludere dal trattamento i propri dati sanitari per uso secondario[31].
A voler ammettere che l'esercizio di tale opzione in vita possa anche riguardare utilizzazioni che avvengano successivamente al decesso, ne scaturirebbe l'impossibilità, nei limiti normativi, di avvalersi dei dati sanitari ad uso secondario. Salvo che, come disposto dal regolamento, uno Stato membro abbia previsto condizioni, al ricorso delle quali, potrebbe comunque essere concesso l'accesso a tali dati purché le regole derogatorie rispettino «l'essenza dei diritti e delle libertà fondamentali» e costituiscano «una misura necessaria e proporzionata in una società democratica per servire ragioni di interesse pubblico nel perseguimento di obbiettivi scientifici e sociali legittimi» (art. 71.5).
A voler condividere tale impostazione, si porrebbe il quesito se l'interessato, ancora in vita, con disposizione di ultima volontà, possa trasferire agli eredi la possibilità di revocare la propria scelta di esclusione dall'uso secondario, attribuendo loro poteri di gestione conformemente al regolamento (ovvero alla disciplina nazionale, nella misura in cui uno Stato membro abbia fatto uso del potere derogatorio concesso dall'art. 71).
In sostanza: fermo l'uso libero come regola generale, e rilevato che l'interessato ancora in vita ha la possibilità di scegliere, ai sensi dell'art. 71, di interdire l'uso secondario dei propri dati sanitari elettronici personali, nei limiti ammessi, e di farlo anche con riferimento al tempo successivo al proprio decesso, si potrebbe ipotizzare che – una volta operata tale scelta – l'interessato possa indicare uno o più soggetti i quali, successivamente al proprio decesso, abbiano il potere di revocare tale scelta.
Nelle pieghe di queste problematiche fa capolino la possibilità di gestione economica del dato sanitario elettronico personale da parte di successori. Le vicende a cui può farsi riferimento sono molteplici, ad iniziare dal prelievo del cervello di Einstein, oppure postulando, sempre ad esempio, un interesse scientifico/economico per studiare, con riferimento a dati sanitari elettronici personali, prestazioni sportive al limite dell'umano, quali la potenza di tiro di un campione del calcio o del tennis. Non è dubbia la rilevanza patrimoniale e scientifica di tali dati e chi voglia imbarcarsi nello studio di tali questioni,

[31] Su tale aspetto v., in questo volume, le considerazioni di V.V. CUOCCI, *Uso secondario dei dati sanitari e interesse generale alla ricerca: riflessioni sul Regolamento sullo Spazio Europeo sui Dati Sanitari e sul Regolamento Generale sulla Protezione dei Dati Personali*, cit., § 3; E. CALZOLAIO, *Il regolamento sullo spazio dei dati sanitari nella prospettiva della cittadinanza europea,* in *Dir. inf*., 2025, 315, 326.

dovrebbe anzitutto chiedere il consenso ai successori e tenersi pronto alla richiesta di contropartite economiche.

Infine, per l'ambito di applicazione oggettivo della nostra disciplina occorre considerare l'art. 53, che delimita le finalità in presenza delle quali è possibile concedere l'accesso ai dati sanitari elettronici per uso secondario da parte degli organismi responsabili dell'accesso e il successivo art. 54, che regola le ipotesi in cui vi è divieto di utilizzare i dati sanitari elettronici.

IV. USO PRIMARIO E SECONDARIO DEI DATI SANITARI: DEFINIZIONI, APPLICAZIONI E ZONE D'OMBRA

Nell'EHDS la dicotomia "uso primario/secondario" è la grammatica con cui l'ordinamento riorienta i trattamenti dei dati sanitari elettronici, non un mero criterio classificatorio. Il Considerando (1) ne fissa la *ratio*: rafforzare l'accesso e il controllo degli interessati e, a condizioni definite, abilitare l'uso del dato oltre l'assistenza sanitaria a ulteriori finalità di interesse generale. Le considerazioni che seguono investono l'ambito oggettivo per tracciare il perimetro applicativo di entrambi gli usi, muovendo dalla definizione normativa, individuando un criterio di demarcazione e offrendo esempi operativi e casi-limite per provare ad apprezzare, sul banco di prova dell'applicazione concreta, le zone d'ombra e la portata effettiva del Reg. (UE) 2025/327.

Nel lessico dell'EHDS, l'«uso primario» è la cerniera che riporta il dato al suo *telos* naturale: la cura della persona.

L'art. 2, §2, lett. d), del Reg. (UE) 2025/327 definisce l'«uso primario» come «il trattamento dei dati sanitari elettronici per la prestazione di assistenza sanitaria al fine di valutare, mantenere o ripristinare lo stato di salute della persona fisica cui si riferiscono tali dati, comprese la prescrizione, la dispensazione e la fornitura di medicinali e dispositivi medici, nonché per i pertinenti servizi sociali, amministrativi o di rimborso». Ne discende un perimetro ampio e non tassativo, ancorato allo scopo di cura e alla connessione con il percorso clinico, nel quale rientrano fascicoli ed EHR, ricette digitali e le «categorie prioritarie» dell'art. 14 (profilo sanitario, prescrizioni e dispensazioni, referti, *imaging*, lettere di dimissione) per le quali il legislatore prevede standard comuni abilitanti[32].

Invero, nel quadro unionale, il trattamento dei dati sanitari per finalità di diagnosi, assistenza e terapia era già legittimato dal GDPR mediante la combinazione degli artt. 6 e 9 (in particolare l'art. 9, § 2, lett. h), applicabile anche alla sanità pubblica e alla medicina preventiva) e, sul piano interno, dalle discipline nazionali di settore. Il cambio di baricentro sta qui: il GDPR non definiva in positivo l'«uso primario», sicché la liceità restava ancorata alla base dell'art. 6, integrata dall'art. 9 per le categorie particolari; l'EHDS, invece, adotta una definizione funzionale, indifferente al titolo giuridico prescelto e alla natura (pubblica o privata) del titolare, assumendo quale criterio ordinante l'idoneità del dato a servire il

[32] Reg. (UE) 2025/327, art. 2, lett. d); art. 14 («Categorie prioritarie») e Allegato I (caratteristiche delle categorie prioritarie).

percorso di cura[33]. Il Capo II dà corpo ai diritti e ne rafforza il perimetro di tutela[34], come si dirà oltre[35].

D'altra parte, nel disegno sistematico dell'EHDS, la vera discontinuità rispetto al passato è la categoria dell'«uso secondario» dei dati sanitari elettronici. Prima del Reg. (UE) 2025/327, il riuso per finalità diverse dalla cura era già praticabile, ma dentro un quadro disomogeneo, costruito su GDPR e diritto interno[36]. La regola era il consenso specifico[37]; in alternativa operava l'anonimizzazione; e, ove necessario, si ricorreva a basi di interesse pubblico o di ricerca, spesso filtrate da leggi nazionali, autorizzazioni delle *Authorities* e pareri dei comitati etici[38]. L'EHDS razionalizza e unifica la disciplina: per «uso secondario» intende «il trattamento dei dati sanitari elettronici per le finalità indicate al capo IV del presente regolamento, diverse dalle finalità iniziali per le quali tali dati sono stati raccolti o prodotti». In sostanza, è uso secondario qualsiasi trattamento di dati sanitari elettronici destinato a finalità diverse dall'assistenza sanitaria individuale (uso primario), dunque a scopi ulteriori rispetto alla cura dell'interessato, entro i limiti di interesse generale tassativamente indicati dall'art. 53 del Reg. (UE) 2025/327[39].

Rinviando alla trattazione completa svolta altrove, per i nostri fini – l'ambito oggettivo dell'uso secondario – va chiarito che esso è ammesso solo, se necessario, nei limiti della finalità perseguita, lungo sei binari complementari:

(a) interesse pubblico in sanità pubblica o medicina del lavoro (epidemiologia, minacce transfrontaliere, qualità e sicurezza delle cure, farmacovigilanza e vigilanza sui dispositivi);

(b) politiche e regolazione a sostegno di enti pubblici o istituzioni/organismi dell'Unione (*evidence-based policy*, programmazione sanitaria, valutazioni regolatorie anche di agenzie come EMA);

(c) statistiche sanitarie o dell'assistenza, con richiamo al Reg. (CE) n. 223/2009;

(d) istruzione e insegnamento nel settore sanitario/assistenziale, a livello di formazione professionale o istruzione superiore (*case study* e simulazioni nel rispetto della privacy);

(e) ricerca scientifica in sanità/assistenza che contribuisca alla sanità pubblica o garantisca qualità e sicurezza di cure, medicinali e dispositivi, inclusi sviluppo, addestramento, test e validazione di algoritmi (anche di IA) e soluzioni di sanità digitale[40];

(f) miglioramento della prestazione ed ottimizzazione delle cure sulla base dei dati sanitari elettronici di altre persone fisiche (analisi di coorte, *clinical audit*, miglioramento continuo).

---

33 S. Corso, *Lo spazio europeo dei dati sanitari. Prime riflessioni sul Regolamento UE 2025/327*, cit., 563 ss., spec. §6, sottolinea la costruzione funzionale della nozione e la sua alterità rispetto alla tassonomia GDPR.

34 Cfr. K. Ó CATHAOIR, *The EHDS and Electronic Health Records. GDPR+ or Transforming Patients' Rights?*, cit., 24-25 ss.

35 *Infra,* A. ADDANTE, *Vicende circolatorie ed esercizio dei diritti nell'uso primario dei dati sanitari*, *passim*.

36 F. VITERBO, *Principî di trattamento e di* governance *dei dati personali in àmbito sanitario*, cit.,1443 ss.

37 Reg. (UE) 2016/679, art. 6(1)(a) e 9(2)(a).

38 Reg. (UE) 2016/679, art. 6(1)(e), 9(2)(g), (i), (j) e 89.

39 Reg. (UE) 2025/327, art. 2, lett. e), in necessario combinato disposto con il Capo IV, artt. 50-80, spec. art. 53 («Finalità per le quali è possibile trattare i dati sanitari elettronici per l'uso secondario»).

40 Cfr., sul tema, G. LOFARO, *Dati sanitari e* E-Health *europea tra trattamento dei dati personali e decisione amministrativa algoritmica*, cit., spec. 206 e ss.

Circolazione sì, dunque, ma ancorata a scopi tipizzati e a un controllo di necessità[41], previa autorizzazione e limitatamente ai *dataset* elencati all'art. 51 EHDS[42].

Ciò posto, può dirsi che la «prestazione di assistenza sanitaria»[43] operi quale perno della definizione e criterio di demarcazione tra uso primario e altri usi dei dati. In effetti, se il trattamento è diretto alla cura del singolo, si è nell'uso primario; se guarda alla collettività e ricade in una delle sei finalità tipizzate, si entra nell'uso secondario.

Alcune fattispecie mostrano bene la linea di demarcazione funzionale tra primario e secondario; nei casi di confine, contano le finalità effettive.

Da qui una griglia di esempi oggettivi e, *a latere*, opzioni interpretative e spunti *de iure condendo* per chiudere i varchi normativi.

Non v'è dubbio che rientri nell'«uso primario» il trattamento dei dati necessario all'assistenza del paziente – diagnosi, terapia, *follow-up*, telemedicina[44] –, cui si sommano gli adempimenti amministrativi strettamente funzionali alla cura (prescrizioni, rimborsi, referti)[45]. È invece quantomeno opinabile ricondurre al medesimo alveo: (i) l'erogazione di servizi di "*wellness*" e le raccolte informative di mera organizzazione (si pensi alla richiesta di un certificato da parte di una palestra); (ii) la raccolta di allergie da parte di un *wedding planner* o di un ristorante, ovvero la medesima indicazione affidata a un messaggio *WhatsApp* inviato ad amici o a un *tour operator* in vista di un viaggio organizzato; (iii) l'elaborazione di parametri da un'*app* di *fitness* destinata a programmi di allenamento.

In simili evenienze l'attore non eroga cure e la finalità non è la salute individuale: opera, dunque, il solo GDPR, di regola sulla base del consenso esplicito *ex* art. 9, § 2, lett. a).

È, per contro, «uso primario» il trattamento compiuto dal medico che visita e rilascia il certificato richiesto; l'attività del farmacista che interviene su un callo o consiglia un dispositivo medico; l'esecuzione di un ECG con registrazione nel fascicolo sanitario elettronico; il caricamento, da parte dell'ospedale, della lettera di dimissione e dei referti di *imaging* nel sistema EHR.

Viceversa, appartiene all'«uso secondario» ogni trattamento che non è strumentale alla cura in atto del singolo, bensì persegue una delle finalità tipizzate dal Capo IV del Reg. (UE) 2025/327. Ne sono esempi: (i) un ospedale che analizza cartelle cliniche per individuare *pattern* e migliorare protocolli e percorsi assistenziali (miglioramento qualità); (ii) l'impiego,

---

41 Ai sensi dell'art. 53 EHDS, l'accesso per sanità pubblica e *policy*/regolazione (lett. a-b) e per la statistica ufficiale (lett. c) è riservato a enti pubblici (anche UE); i privati, in tali casi, possono operare quali responsabili per conto dell'autorità. Le restanti finalità – ricerca, formazione, miglioramento della qualità – sono aperte anche a richiedenti privati qualificati, nel rispetto delle condizioni del Reg. (UE) 2025/327.

42 L'accesso ai dati per uso secondario avviene tramite gli *Health Data Access Bodies* (HDAB) che valutano le richieste e rilasciano permessi; i dati sono forniti di norma in forma anonima o pseudonimizzata e l'utente deve pubblicare i risultati entro 18 mesi: cfr., sul tema, *infra*, R. AMBROSINO, *Profili di* governance *dell'uso secondario dei dati sanitari nell'*European Health Data Space, in questa *Rivista*, 2026, p. 126 ss.

43 *Infra*, § VIII.

44 Le linee guida nazionali sulla telemedicina (D.M. 21.9.2022) confermano l'inquadramento funzionale della prestazione a distanza e l'indipendenza del successivo riuso a fini collettivi. Cfr. Ministero della Salute, *Linee guida per la telemedicina*, 2022 (Intesa Conferenza Stato–Regioni 17 dicembre 2020, agg. 2022).

45 Appartengono all'uso primario, oltre alla prestazione, la liquidazione del rimborso tramite flussi amministrativi strettamente funzionali, l'accesso del medico curante al FSE per adeguare la terapia o programmare il *follow-up* e lo scambio transfrontaliero di ricette e referti via *MyHealth@EU* quando rivolto all'assistenza del singolo paziente. Parimenti, l'uso personale dell'interessato – scaricare e gestire i propri referti – integra l'esercizio dei diritti di accesso e controllo e resta nell'alveo dell'uso primario.

da parte di un'università o di istituti di formazione, di dati pseudonimizzati per attività didattiche e di ricerca, nei limiti e con le garanzie previste; (iii) un'agenzia regolatoria che accede a serie di dati per valutare la sicurezza o l'efficacia di un dispositivo; (iv) un organismo pubblico che elabora statistiche su una malattia rara; (v) una società farmaceutica che addestra un algoritmo di intelligenza artificiale su *dataset* sanitari in ambiente sicuro, con finalità di ricerca.

Fuori campo EHDS e, perciò, interdetti come "*secondary use*", sono i riutilizzi per fini di *marketing* sanitario, la segmentazione assicurativa privata e le richieste dei datori di lavoro per selezione del personale o analisi predittive volte a discriminare individui (art. 54 EHDS). Parimenti, non vi rientrano: la formazione della prova nel giudizio civile (*malpractice,* risarcimento), che attiene alla funzione giurisdizionale ed è estranea al Capo IV; le acquisizioni per finalità di indagine penale o di polizia, riconducibili al *law enforcement* e non abilitate dal regolamento[46]; l'impiego didattico nelle scuole secondarie – non qualificabile come "*vocational*" né "*higher education*" ai sensi dell'art. 53, § 1, lett. d) –, estraneo all'ambito educativo ammesso. Quando la finalità non è tra quelle tipizzate, l'EHDS cede il passo: trova applicazione il solo GDPR, di regola sul fondamento del consenso esplicito *ex* art. 9, § 2, lett. a), ferme le regole *ePrivacy* e le discipline nazionali pertinenti[47].

Ecco, allora, che il discrimine – in entrambi i casi – è teleologico e contestuale: rilevano la funzione che il dato assolve nel percorso di cura e la natura sanitaria (o meno) dell'intervento, non il "tipo" di dato in quanto tale. Insomma, la linea di confine corre sul fine perseguito e sul contesto d'impiego, non sull'ontologia dell'informazione.

I casi di confine, più di ogni enunciazione astratta, rendono visibile il criterio.

Nel tele-monitoraggio del paziente dimesso, finché il medico si serve delle misurazioni per seguire il singolo, calibrare la terapia, modulare il *follow-up*, l'operazione rimane nell'orbita dell'uso primario: il dato è strumentale alla cura e ne condivide il destino. Se, viceversa, quella stessa traccia informativa viene riutilizzata dalla struttura per elaborare protocolli, misurare esiti o costruire modelli predittivi di eventi futuri, il baricentro si sposta sull'uso

[46] Per i trattamenti svolti dalle autorità competenti ai fini di prevenzione, indagine o repressione dei reati, il quadro applicabile non è il GDPR bensì la Dir. (UE) 2016/680 (LED), come conferma l'esclusione dell'art. 2, § 2, lett. d), GDPR. Diverso il piano dell'ospedale o del medico che comunica dati all'autorità: per quell'atto opera il GDPR, giacché il prestatore sanitario non è "autorità competente" ai sensi della LED. La base di liceità è, di regola, l'adempimento di un obbligo legale o l'esecuzione di un compito di interesse pubblico (art. 6, §1, lett. c) o e), GDPR) fondati su norma di diritto interno; per i dati relativi alla salute è inoltre necessaria la condizione dell'art. 9, § 2, lett. g) (rilevante interesse pubblico previsto dal diritto dell'Unione o nazionale, con garanzie adeguate). Restano fermi i principi di necessità, minimizzazione e tracciabilità dell'accesso. Una volta ricevuti, i dati sono trattati dall'autorità di pubblica sicurezza nel perimetro della LED e non del GDPR.

[47] Per «regole *ePrivacy*» si intende la disciplina UE sulla riservatezza delle comunicazioni elettroniche (dir. 2002/58/CE, come modificata), che opera quale *lex specialis* rispetto al GDPR per profili quali: segretezza delle comunicazioni, dati/metadati di traffico e di localizzazione, elenchi e identificazione del chiamante, comunicazioni indesiderate (*marketing/spam*), nonché accesso o archiviazione di informazioni nel terminale dell'utente (*cookies* e tecnologie affini), normalmente subordinati a consenso preventivo salvo eccezioni tipizzate (es. stretta necessità tecnica). Il rapporto con il GDPR è chiarito da art. 95 GDPR e Considerando 173. Per «discipline nazionali pertinenti» si intendono, da un lato, le norme interne di attuazione della direttiva *ePrivacy* (in Italia, ad es., artt. 121-132 del d.lgs. 196/2003, incl. art. 122 su *cookies* e art. 130 su *marketing*), nonché i provvedimenti dell'Autorità garante (linee guida su *cookie/telemarketing*, ecc.); dall'altro, le regole settoriali che impattano sul trattamento in ambito sanitario-digitale (es. ecosistema dei dati sanitari (D.M. 31 dicembre 2024), fascicolo sanitario elettronico, telemedicina, protocolli regionali), oltre agli obblighi deontologici e sanitari applicabili.

secondario; e con esso si attivano le garanzie – anche autorizzative – che il Capo IV pretende.

Analoga la dinamica degli algoritmi di stratificazione del rischio in ambito ospedaliero: quando l'*output* serve al governo complessivo dei pazienti (programmazione, qualità, sicurezza), si entra nel terreno del secondario; quando, invece, l'algoritmo orienta l'accesso o la modulazione di una terapia per un determinato paziente, si torna al primario e scattano, senza mediazioni, le cautele del Capo II dell'EHDS. Quanto al teleconsulto transfrontaliero, la prestazione resa nello spazio UE/SEE si allinea all'ecosistema EHDS e alla rete *MyHealth@EU*; se il flusso si dirige verso Paesi terzi privi di accordi, riemergono le regole sui trasferimenti del Capo V GDPR, con possibili frizioni rispetto alle garanzie del regolamento settoriale. La linea di confine, si vede, non è ontologica ma funzionale: è la finalità a dare forma al diritto applicabile.

Una zona d'ombra, divenuta prassi quotidiana, è la comunicazione "fuori canale" tramite *WhatsApp* e affini. La sostanza, di regola, non è controversa: referti fotografati, descrizioni di sintomi, richieste di rinnovo di ricette restano trattamenti orientati alla cura e dunque riconducibili all'uso primario per scopo. È il canale a non tenere il passo: estraneo alle infrastrutture EHDS (FSE/EHR, *MyHealth@EU*) e non conforme allo *European Electronic Health Record Exchange Format* (EHRxF), difetta di standardizzazione, tracciabilità, auditabilità. Nell'oggi operano le cautele del GDPR – base di liceità *ex* art. 9, misure di sicurezza *ex* art. 32, principi di minimizzazione e limitazione della conservazione – con l'ulteriore onere professionale di riversare nel FSE/EHR i contenuti clinicamente rilevanti, per riallinearli all'ecosistema EHDS.

Alcune fattispecie meritano un fuoco dedicato.

La raccolta scolastica delle allergie degli alunni, destinata al servizio mensa per adattare i pasti e prevenire reazioni, non integra di per sé un'erogazione di cure: la mensa non è prestatore sanitario (*infra*) e la finalità è organizzativo-preventiva. Il trattamento resta dunque nel perimetro del GDPR per categorie particolari (artt. 6 e 9).

Diverso sarebbe il caso di un servizio medico interno che interloquisca con pediatri/ASL: il nesso con il percorso di cura potrebbe attrarre l'uso primario, ma solo ove vi sia integrazione con FSE/EHR, allineamento a *MyHealth@EU*/EHRxF e, soprattutto, ove la struttura sia legalmente qualificabile come "prestatore" di assistenza sanitaria (profilo, ad oggi, non scontato). Sul piano ordinamentale, gioverebbe chiarire che le scuole operano, di regola, nel solo alveo GDPR e che ogni riuso per sanità pubblica transita dalle autorità sanitarie (ASL/Regioni) quali *data holder*: una simile precisazione evita indebite estensioni dell'EHDS al contesto educativo e mette in coerenza finalità, soggetti e infrastrutture.

Anche il mondo sportivo mostra la duplice faccia. Le federazioni sportive raccolgono dati sanitari per valutare l'idoneità degli atleti ed eseguono test antidoping. La visita di idoneità sportiva integra uso primario: il medico presta assistenza; alla federazione compete, al più, la mera annotazione dell'esito binario "idoneo/non idoneo". Diverso l'antidoping: non cura il singolo, ma presidia equità e salute collettiva. Qui l'inquadramento può migrare nell'uso secondario: l'agenzia antidoping agisce da *data user* autorizzato, la federazione che detiene i risultati da *data holder* (art. 2, lett. t), con passaggi subordinati ad autorizzazione HDAB, pseudonimizzazione/anonimizzazione e ambienti sicuri.

In alternativa, se prevale la *lex* sportiva (WADA e normativa d'attuazione), la materia resta fuori EHDS: si applicano GDPR e diritto nazionale. Forse, un chiarimento europeo sulla qualificazione dei ruoli (federazioni/agenzie: *data holder/data user*) e, se del caso, l'inserimento nell'art. 53 di una finalità *ad hoc* "sport ed etica sportiva" aiuterebbero a tutelare proporzionalità e netta separazione tra cura, regolazione e mercato.
Infine, *smartwatch* e sensori indossabili. Essi raccolgono parametri fisiologici (frequenza cardiaca, sonno, saturazione) che i produttori elaborano per generare raccomandazioni: siamo nell'area del benessere, con produttori talora qualificabili come potenziali *data holder*. L'EHDS rileva solo quando quei dati sono integrati nella cartella clinica elettronica o utilizzati su indicazione medica: allora l'uso è primario, perché funzionale al percorso di cura; altrimenti resta fuori dall'EHDS e trova disciplina nel GDPR. Però, la gran parte degli impieghi tipici – condivisione con assicurazioni o datori per sconti/premi, profilazioni - non rientra nelle finalità del Capo IV e pone seri profili di non discriminazione: l'utente deve poter negare l'accesso e, ove avvengano trattamenti ulteriori, esigere almeno pseudonimizzazione e robuste misure di sicurezza.
In controluce, il medesimo insegnamento: è la funzione a ordinare il diritto del dato. Lo stesso flusso informativo può mutare regime passando dalla cura al governo del sistema; e il compito dell'interprete è riconoscere il punto di volta, senza indulgere né alle scorciatoie della tecnica né alle astrazioni della norma.

V. CASI DI NON APPLICAZIONE

La definizione dell'ambito oggettivo di applicazione della nostra disciplina va precisata anche alla luce della norma che indica i casi in cui la stessa non trova applicazione: l'art. 1, n. 9.
Si precisano due fattispecie di trattamento – dati nelle quali il regolamento "non si applica": trattamenti «nel corso di un'attività che non rientra nell'ambito di applicazione del diritto dell'Unione» (lett. a); e trattamenti effettuati «dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse» (lett. b).
Entrambe le fattispecie ribadiscono quanto già disposto dal regolamento generale 2016/679, che espressamente esclude all'art. 2.2, lett. a), quei trattamenti «per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione» e poi esclude all'art. 2.2, lett. d), in termini letteralmente identici i trattamenti effettuati dalle autorità competenti in fattispecie aventi rilevanza penale.
Un'ulteriore disposizione, l'art. 50.1, esclude dall'applicazione della sola disciplina relativa agli obblighi dei titolari dei dati sanitari (per l'uso secondario) le «persone fisiche, compresi i singoli ricercatori» (art. 50.1, lett. a) e le «persone giuridiche considerate microimprese» (art. 50.1, lett. b), salvo che gli Stati membri stabiliscano diversamente.
Si noti che già il regolamento generale 2016/679 esclude dalla sua applicazione (art. 2.2, lett. c) i trattamenti effettuati dalla persona fisica «per l'esercizio di attività a carattere esclusivamente personale o domestico».

Esclusione che non è più richiamata nell'art. 1, § 9 (che regola le esclusioni nel regolamento 2025/327) e che sembrerebbe non applicabile al contesto dei dati sanitari elettronici, che fa riferimento alle persone fisiche (ed alle persone giuridiche "considerate microimprese": con rinvio alla raccomandazione 2003/361/CE, art. 2, § 3, dell'allegato) solo nel più limitato ambito dell'uso secondario e relativamente all'esenzione dagli obblighi che gravano sui titolari di dati sanitari.

VI. Ambito di applicazione soggettivo: la persona fisica

Come disposto dall'art. 1.2, lett. a), il regolamento 2025/327 «specifica e integra» i diritti di cui al regolamento generale 2016/679 «delle persone fisiche in relazione all'uso primario e all'uso secondario dei loro dati sanitari elettronici personali».

Il riferimento alle persone fisiche si comprende agevolmente considerando che i dati sanitari non possono che appartenere a persone fisiche ed è pertanto da escludersi qualsiasi riferibilità alle persone giuridiche. Peraltro, il regolamento non contiene alcuna definizione di persona fisica, né fa rinvio ad altre normative, per cui occorre riferirsi alla nozione di diritto comune, elaborata però nell'ambito delle esperienze nazionali, non avendo il diritto dell'Unione europea provveduto ad un'elaborazione comune, se non con riferimento ai noti progetti dottrinali elaborati a cavallo tra i due secoli.

In linea solo teorica, sarebbe ammissibile concepire un dato sanitario con riferimento agli animali, ma il regolamento non si è posto alcun problema di tutela in merito, sebbene si discuta sempre più frequentemente, sia in dottrina, sia in giurisprudenza, della possibilità che anche a questi soggetti possa attribuirsi una capacità giuridica limitata.

Così pure, anche le piante, come esseri senzienti.

Eppure, non può certo escludersi una rilevanza del dato sanitario inerente ad animali (si pensi alla passata epidemia della c.d. "mucca pazza") e così pure in ambito vegetale (si pensi all'attuale problematica della diffusione della Xylella, il batterio che causa la 'morte' degli ulivi, e che si sta diffondendo ad altre piante). Esiste, in questi casi, un interesse pubblico indubbio all'accesso e diffusione di dati 'sanitari' di animali e piante per la rilevanza che potrebbero avere, sia (anche) per la salute dell'essere umano, sia per la conservazione degli *habitat* naturali[48].

Ma, si diceva, la scelta del legislatore europeo è stata chiara: tener fuori tali problematiche, con indubbi risvolti giuridici, dalla disciplina dell'accesso ai dati sanitari di persone fisiche, per il diverso assetto dell'equilibrio tra diritti/doveri tra ambito 'umano' ed ambiti differenti.

Il riferimento alla persona fisica non è quindi estensibile, neppure parzialmente, ad altri 'soggetti'.

La circostanza che il legislatore faccia riferimento alla persona fisica attribuisce alla disciplina un indubbio connotato di universalità.

[48] Una recente riflessione su tali tematiche, con riferimento ai rapporti tra la salute degli esseri umani, degli animali e dell'ambiente ed alle implicazioni sul piano giuridico è svolta da K. F. Gärditz, *One Health*, Mohr Siebeck, München, 2025.

Nessun riferimento è fatto alla cittadinanza, neppure a quella europea, e pertanto questa normativa si applicherà anche a soggetti provenienti da ambiti extraeuropei, indifferentemente dalla circostanza che siano stati attribuiti titoli di permanenza, quale un permesso di soggiorno, o si tratti di immigrazione clandestina. Anche l'immigrato, che sia stato fermato dalle forze dell'ordine in un'operazione di contrasto all'immigrazione clandestina, e sottoposto ad accertamenti medico-sanitari, potrà vantare, in quanto persona fisica, gli stessi diritti spettanti agli altri, ai sensi del regolamento 2025/327.
Sulla problematica dell'uso di dati sanitari elettronici personali successivamente al decesso dell'interessato, si fa rinvio a quanto già osservato in precedenza, al § 3.

VII. IL PROFESSIONISTA SANITARIO

Nel sistema EHDS il «professionista sanitario» è l'attore centrale dell'uso primario. Egli può accedere e scambiare, esclusivamente per finalità di cura, i dati sanitari elettronici personali del paziente nella sola misura pertinente e necessaria, durante l'attività assistenziale, tramite i servizi di accesso per professionisti sanitari. Al contempo è produttore del dato clinico: genera le informazioni, le inserisce nei sistemi e ne presidia accuratezza, completezza e aggiornamento[49].
L'EHDS non introduce una definizione autonoma di «professionista sanitario»: l'art. 2, § 1, lett. b), rinvia all'art. 3, lett. f), dir. 2011/24/UE, per cui è professionista sanitario ogni persona fisica che esercita a titolo professionale un'attività sanitaria secondo il diritto dello Stato membro di cura. Vi rientrano, in particolare, medico, infermiere responsabile dell'assistenza generale, odontoiatra, ostetrica e farmacista, quali professioni settoriali riconosciute dalla dir. 2005/36/CE (art. 21 e all. V), nonché ogni altra figura la cui attività sanitaria sia, per legge, riservata a una professione regolamentata (art. 3, § 1, lett. a), dir. 2005/36/CE)[50].
Ne discende un perimetro ampio ma giuridicamente presidiato, che abbraccia tutte le figure legalmente riconosciute e autorizzate – incluse quelle regolamentate in sede

[49] Reg. (UE) 2025/327, artt. 11-12.
[50] Ad esempio, nell'ordinamento italiano, il fisioterapista è professione sanitaria a pieno titolo, con profilo definito dal D.M. 14 settembre 1994, n. 741, ricondotta all'area delle professioni sanitarie della riabilitazione (art. 6, co. 3, d.lgs. 30 dicembre 1992, n. 502; l. 26 febbraio 1999, n. 42; l. 10 agosto 2000, n. 251) e inserita negli albi istituiti presso l'Ordine TSRM-PSTRP (l. 11 gennaio 2018, n. 3). La figura del "nutrizionista" richiede distinzione per titolo abilitante: il medico chirurgo con specializzazione in Scienza dell'alimentazione appartiene alle professioni sanitarie mediche (d.lgs. 17 agosto 1999, n. 368; d.m. 1° agosto 2005 e succ. mod.); il dietista è professione sanitaria con profilo delineato dal D.M. 14 settembre 1994, n. 744 (art. 6, co. 3, d.lgs. 502/1992; l. 3/2018). Il biologo nutrizionista opera, invece, quale professione ordinistica dei biologi (l. 24 maggio 1967, n. 396; d.P.R. 5 giugno 2001, n. 328), svolgendo attività in ambito sanitario secondo la propria disciplina di settore.

nazionale (es. l'osteopata[51]) – che, nel concreto dell'agire clinico, accedono e utilizzano i dati del paziente ai fini dell'erogazione della cura[52].

Per converso, restano fuori dal perimetro dell'uso primario gli operatori non sanitari: istruttori di *fitness* o di *wellness*, estetiste, addetti di strutture ricreative; e, più in generale, *coach* sportivi o figure affini, salvo che svolgano un'attività sanitaria regolamentata (es. medico dello sport) secondo il diritto interno. Anche qui, un ristorante che riceve informazioni su allergie dei propri clienti non diviene «professionista sanitario» e non entra nel perimetro EHDS. Le figure non qualificate (es. «nutrizionisti» non abilitati come professione sanitaria in base alla legge nazionale; fisioterapisti non riconosciuti) restano assoggettate al solo GDPR e al diritto interno: non accedono alle cartelle cliniche tramite *MyHealth@EU* e, se trattano dati relativi alla salute, devono ancorarsi alle basi giuridiche del GDPR (consenso o altra base applicabile) e ai relativi limiti.

Le forme organizzative – studio singolo, associazione, struttura complessa - non attenuano, né potrebbero attenuare, il dovere di *accountability*. L'EHDS lo positivizza in modo puntuale: tracciabilità degli accessi, identificazione di chi scrive, imputazione di chi modifica e valida; sempre nel perimetro teleologico della cura, secondo i canoni di necessità e minimizzazione[53]. La tecnica è quella, tipicamente pubblicistica, della responsabilizzazione "per tracce": ciò che si vede, si fa e si altera deve poter essere ricondotto, senza smagliature, a un soggetto determinato lungo l'intera catena clinica.

Proprio perché l'esternalizzazione dei servizi e le filiere di fornitura moltiplicano i punti di contatto con il dato, crescono la circolazione e il rischio di riusi non conformi.

Da qui l'esigenza, non negoziabile, di una separazione funzionale netta: da un lato il trattamento strettamente strumentale all'assistenza individuale; dall'altro ogni ulteriore lavorazione, oggi incanalata nel binario tipizzato dell'"uso secondario". Non rileva, in questa prospettiva, la veste dell'ente o la distribuzione interna dei compiti: conta la finalità effettiva del trattamento, che solo quando serve il percorso di cura legittima l'accesso pieno al dato.

Resta fermo che "professionista sanitario" è persona fisica. Ciò non esclude che, nell'organizzazione del *provider*, altri soggetti cooperino al processo (si pensi alle segreterie per agende e fatturazione): il loro accesso è derivato, limitato allo stretto necessario, e non

[51] Che l'osteopata stia "dalla parte" delle professioni sanitarie è oggi dato di diritto positivo, non più di prassi o *marketing*: l'art. 7 della l. 11 gennaio 2018, n. 3, individua la professione; il D.P.R. 7 luglio 2021, n. 131 – che recepisce l'Accordo Stato-Regioni 5.11.2020 – scrive nero su bianco che «l'osteopata è il professionista sanitario» e ne tipizza competenze e ambiti; il D.I. MUR-Salute 1° dicembre 2023, n. 1563 ha poi definito l'ordinamento del relativo corso di laurea (L/SNT/4). Dunque, malgrado l'enorme "SAT" (il magma indistinto delle pratiche manuali para-sanitarie cresciute nell'area grigia), il recinto è tracciato.

[52] F. DI CIOMMO, *La privacy sanitaria*, in R. Pardolesi (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003, 259 ss.

[53] Nel quadro dell'EHDS, i professionisti svolgono un duplice ruolo, insieme beneficiari e responsabili dell'ecosistema dei dati: da un lato accedono, tramite servizi digitali interoperabili, alle informazioni cliniche (referti, anamnesi, terapie) anche conservate in altri Stati membri, purché autenticati, autorizzati e nell'ambito della cura; dall'altro, tale accesso più ampio e tempestivo alimenta la qualità e la continuità dell'assistenza, riducendo duplicazioni, errori e costi – come rimarca il Considerando 19. Ciascun professionista indicato dall'assistito accede solo ai dati necessari: in un'*équipe* multidisciplinare, ogni componente consulta esclusivamente le informazioni pertinenti all'episodio di cura assegnato; anche se il sistema consente una visione più ampia del fascicolo, l'accesso va ristretto allo stretto indispensabile per lo specifico intervento. Questa granularità discende dall'art. 11, § 3, Reg. (UE) 2025/327, ed è funzionale alla minimizzazione dei dati *ex* art. 5, §1, lett. c, GDPR.

muta la qualifica soggettiva. Non possono compiere atti clinici, né alimentare l'EHR con contenuti valutativi. Laddove l'ordinamento ammetta deleghe controllate (a personale infermieristico o tecnico), la responsabilità non si disperde: resta ancorata alla catena clinica e si riflette nei profili di audit richiesti – chi inserisce è identificato; chi valida è imputabile. Regola pratica per il professionista: vedere solo ciò che serve, lasciare traccia di ciò che si vede, non riusare *extra curam*[54].

Resta, infine, una linea di confine tipica della *digital health*, sulla quale gli ordinamenti faticano a trovare un assetto stabile. Si pensi alla figura dell'"*health coach*" che opera tramite un'*app* con marcatura CE quale dispositivo medico ai sensi del *Medical Device Regulation* (MDR, Reg. (UE) 2017/745): la certificazione qualifica il prodotto, non *ipso facto* l'operatore[55]. Se l'attività è regolamentata e si svolge sotto effettiva supervisione clinica, una riconduzione alla sfera delle professioni sanitarie potrà trovare appiglio nel diritto nazionale; diversamente, l'operatore resta nel perimetro del benessere e, quanto ai dati, soggiace al solo GDPR. Ma la pratica introduce ambiguità: quando la stessa *app* alimenta l'EHR con contenuti valutativi, orienta decisioni terapeutiche o si integra nei Percorsi Diagnostico-Terapeutico-Assistenziali (PDTA), la linea tra *wellness* e cura si assottiglia fino a diventare porosa.

Il rischio è duplice: da un lato, uno "scivolamento funzionale" verso atti di cura senza le garanzie proprie dell'uso primario; dall'altro, il ricorso a formule organizzative (*franchising*, piattaforme, *outsourcing*) che disperdono responsabilità e rendono opaco il tracciato di imputazione.

In questa chiave, la chiosa resta prudente: un'*app* può essere "medica" (MDR/CE) senza che l'operatore lo sia; e tuttavia, quando l'operatore tocca la sostanza della cura – modificando il piano terapeutico o alimentando l'EHR con valutazioni – la soglia dell'uso primario va considerata superata *ex lege*, con tutte le conseguenze in termini di qualificazione soggettiva, responsabilità e garanzie a presidio del dato e della persona (EHDS/GDPR).

VIII. IL PRESTATORE DI ASSISTENZA SANITARIA

La nozione di «prestatore di assistenza sanitaria» (o fornitore di assistenza sanitaria) designa qualsiasi soggetto che eroga servizi sanitari. Anche qui l'art. 2, §1, lett. b), del Reg. (UE) 2025/327 rinvia, per la definizione, alla dir. 2011/24/UE: è prestatore «qualunque

[54] Sul punto, cfr. già la ricostruzione classica dei profili soggettivi e organizzativi del trattamento in ambito sanitario (con attenzione a contitolarità, *outsourcing* e rischi di riuso), in F. DI CIOMMO, *La privacy sanitaria*, cit., 239 ss., §§ 3 e 5.3.

[55] Esempio pratico. *FibriCheck* è un'*app* per *smartphone* qualificata dal fabbricante come *software* dispositivo medico che misura il ritmo cardiaco tramite fotopletismografia e segnala possibili aritmie; il produttore dichiara la marcatura CE ai sensi del Reg. (UE) 2017/745 sui dispositivi medici (MDR), e l'*app* risulta disponibile negli *store* con tale qualifica. La Guida Blu della Commissione europea (*The Blue Guide on the implementation of EU product rules*) chiarisce tuttavia che la marcatura CE attesta la conformità del prodotto ai requisiti applicabili e non costituisce certificazione della persona che lo utilizza. Per il *software*, la qualificazione e la classificazione seguono lo scopo d'uso (*intended purpose*) dichiarato dal fabbricante (v. MDCG, *Medical Device Coordination Group*, 2019-11, agg. rev.1): in particolare, la regola 11 dell'Allegato VIII MDR governa il rischio del *software* destinato a fornire informazioni usate per decisioni diagnostiche o terapeutiche o a monitorare processi fisiologici. Nella letteratura clinica e nei materiali del produttore, *FibriCheck* è presentata come *app* medica CE per lo *screening*/monitoraggio della fibrillazione atriale.

persona fisica o giuridica o qualsiasi altro ente, pubblico o privato, che fornisca legalmente assistenza sanitaria sul territorio di uno Stato membro»[56]. La stessa direttiva definisce «assistenza sanitaria» come i servizi prestati da professionisti sanitari a pazienti per valutare, mantenere o ripristinare lo stato di salute, incluse prescrizione, dispensazione e fornitura di medicinali e dispositivi medici[57], e precisa che, in caso di telemedicina, l'assistenza si considera prestata nello Stato membro in cui è stabilito il prestatore[58].

Questa nozione, più organizzativa che personale, abbraccia l'intero spettro dei soggetti che erogano cure: ospedali, aziende sanitarie locali (ASL), agenzie di tutela della salute (ATS) ove previste dall'ordinamento regionale, cliniche e poliambulatori, studi associati, laboratori, farmacie (limitatamente all'attività sanitaria che svolgono), nonché piattaforme di telemedicina e altri erogatori legittimamente stabiliti (ivi compresi istituti di ricerca clinica) che erogano servizi sanitari alle persone. Può coincidere con il singolo studio di un professionista (soggetto che è, al tempo stesso, prestatore e professionista) oppure con un'istituzione che impiega più professionisti.

La distinzione conserva rilievo sistematico: la direttiva qualifica separatamente il «professionista sanitario» (art. 3, lett. f), mentre il prestatore è il contenitore giuridico-organizzativo dell'assistenza; e l'EHDS include nell'uso primario anche prescrizione, dispensazione e fornitura, il che rende evidente l'inclusione, nel perimetro dei prestatori, di strutture come farmacie e laboratori (art. 2, §2, lett. d, EHDS)[59].

Restano invece esclusi quei soggetti che si limitano a raccogliere o trattare dati "relativi alla salute" per scopi organizzativi, assicurativi o di verifica estranei all'erogazione di cure[60]. Per essi, la disciplina di riferimento resta il GDPR (ed eventuali leggi nazionali di settore), mentre l'applicabilità dell'EHDS non è invocabile: mancando l'attività sanitaria in senso proprio, non ricorrono gli obblighi di interoperabilità, tracciabilità e raccordo transfrontaliero predisposti dal nuovo regolamento.

Nel primario, i prestatori sono di regola titolari del trattamento nelle EHR poiché ne determinano finalità e mezzi[61], restano vincolati ai principi generali e all'*accountability*[62] e operano dentro l'architettura di diritti e doveri tracciata dall'EHDS.

Sul versante dei diritti digitali, il prestatore è l'interfaccia dell'*empowerment* del paziente – accesso, integrazione, rettifica, limitazioni selettive, trasparenza degli accessi (artt. 4, 5, 6, 8, 9 EHDS) – mentre, in chiave organizzativa, gli Stati membri assicurano il collegamento di tutti i prestatori ai punti di contatto nazionali e gli scambi bidirezionali via

[56] Dir. 2011/24/UE, art. 3, lett. g).
[57] Dir. 2011/24/UE, art. 3, lett. a).
[58] Dir. 2011/24/UE, art. 3, lett. d).
[59] È prestatore di assistenza sanitaria chi eroga servizi di diagnosi, cura e riabilitazione: ospedali pubblici e privati, ambulatori, centri diagnostici, laboratori, farmacie, case di cura, servizi di telemedicina, ma anche medici convenzionati e operatori di cure assistenziali (home care) riconosciuti.
[60] Non sono prestatori di assistenza sanitaria i soggetti che semplicemente raccolgono dati sanitari per finalità organizzative o di verifica: palestre e *club* sportivi che gestiscono certificati per l'iscrizione, agenzie di viaggio che acquisiscono informazioni per l'idoneità al viaggio, società di assicurazione che valutano il rischio, datori di lavoro che richiedono attestazioni di idoneità, o anche ristoranti che annotano allergie dei clienti.
[61] Reg. (UE) 2016/679, art. 4, n. 7. Reg. (UE) 2025/327, art. 2, § 1, lett. a).
[62] Reg. (UE) 2016/679, art. 5 e art. 24.

MyHealth@EU secondo specifiche e misure unionali di sicurezza, con conseguenti adeguamenti organizzativi e tecnologici lato prestatore[63].

Quanto all'uso secondario, i prestatori che detengono *dataset* sanitari (archivi clinici, banche immagini) assumono – solo ai fini del Capo IV EHDS – la qualifica funzionale di "titolari dei dati sanitari" (*data holder*), distinta dal titolare del trattamento in senso GDPR, e mettono i dati a disposizione su richiesta degli organismi di accesso, alle condizioni e con le garanzie previste[64]. Di regola, sono esentati gli individui e le microimprese, ferma la facoltà degli Stati membri di estendere gli obblighi[65].

L'esperienza pratica mostra, però, configurazioni ibride.

Alcune palestre offrono percorsi di riabilitazione fisioterapica con personale abilitato; in quel perimetro, se l'attività è resa come vera prestazione sanitaria – presa in carico, finalità terapeutica o riabilitativa, eventuale prescrizione, tenuta della documentazione – la struttura può qualificarsi «prestatore di assistenza sanitaria» ai sensi dell'art. 2, § 1, lett. b), Reg. (UE) 2025/327. Quando la piattaforma della palestra diventa il luogo tecnico della prestazione (professionista abilitato, protocolli clinici, produzione di dati sanitari elettronici destinati all'EHR), l'inquadramento nell'uso primario è plausibile, con ricadute sugli obblighi di interoperabilità e qualità. In mancanza di una presa in carico sanitaria e del nesso con il percorso di cura, l'attività resta di benessere e l'EHDS non si applica.

La qualifica, tuttavia, non si estende automaticamente all'intera organizzazione. Serve una scissione funzionale dei trattamenti e delle basi giuridiche: solo il segmento clinico-assistenziale attiva gli obblighi del Capo II EHDS; il resto permane nel GDPR. Insomma, dove gli indici mancano, l'ancoraggio resta il GDPR; quando ricorrono cumulativamente, la qualifica da prestatore è sostenibile per quel sottoinsieme di attività, a condizione di una *governance* dei dati che eviti slittamenti dall'uso primario a trattamenti estranei alla cura.

Un dubbio ricorrente riguarda, infine, la "struttura amministrativa" dei luoghi di cura.

Non è un varco laterale: appartiene organicamente al prestatore di assistenza sanitaria (art. 3 dir. 2011/24/UE) e, quando tratta dati sanitari elettronici personali funzionali alla presa in carico – prenotazioni, accettazione, refertazione, rendicontazione sanitaria[66] – opera in uso primario al pari dei reparti clinici[67]. In tale perimetro l'ente agisce quale titolare (art. 4, n. 7 GDPR); ove alcune funzioni siano esternalizzate a CUP, *billing*, *call-center*, archiviazione documentale, *cloud* o manutentori, i terzi non divengono prestatori autonomi, ma responsabili *ex* art. 28 GDPR o, eccezionalmente, contitolari nei limiti di un accordo *ex* art. 26 GDPR[68]. Quando però si passa alla messa a disposizione di dati per uso secondario,

---

63 Reg. (UE) 2025/327, art. 23, §5.

64 Reg. (UE) 2025/327, artt. 50 ss. e 60, incluse le regole su ambienti sicuri, divieto di reidentificazione e tariffe.

65 Reg. (UE) 2025/327, art. 50, §1-2.

66 Quanto alla tipizzazione, rientrano nei «dati sanitari elettronici personali» (art. 2, punto 2, EHDS; art. 4, n. 15 GDPR) anche agende, codici prestazione, tracciati di refertazione/fatturazione riconducibili al paziente e log di accesso, in quanto rivelano – anche per inferenza – lo stato di salute o la fruizione di cure; ne restano fuori soltanto gli atti amministrativo-contabili davvero "puri", privi di riferimenti individualizzanti e incapaci di veicolare informazioni sanitarie.

67 Reg. (UE) 2025/327 art. 2, § 2, lett. d, che include i «pertinenti servizi […] amministrativi o di rimborso»; v. anche Capo III, *MyHealth@EU*.

68 Si veda CUP regionale Piemonte: nell'Informativa *privacy* è scritto che «il Titolare del trattamento del servizio "CUP Regionale" è la Struttura sanitaria che dovrà erogare la prestazione e, per l'assistito in Piemonte, anche l'ASL di residenza/assistenza; il Responsabile è il RTI *Rekeep Digital* s.r.l. – Telecom Italia

l'ente che li detiene assume anche il ruolo EHDS di *data holder* (art. 2, lett. t, Reg. (UE) 2025/327), mentre il soggetto che richiede l'accesso è il *data user*; i fornitori esternalizzati, di regola, non sono data *holder* perché non hanno un autonomo diritto/obbligo di messa a disposizione.

Ne discendono esiti netti: i flussi orientati alla cura del singolo restano uso primario e devono essere tracciati e interoperabili nell'ecosistema *MyHealth@EU* (Capo III); gli impieghi diversi dalla cura ricadono nell'uso secondario, ammesso soltanto per le finalità tassative del Capo IV (art. 53), con istanza e autorizzazione presso l'HDAB, uso di ambienti sicuri e rigorosa minimizzazione; ogni altro trasferimento costituisce comunicazione illecita in violazione degli artt. 5 e 32 GDPR e del quadro EHDS[69].

IX. Il titolare dei dati sanitari

Tra i molti neologismi che l'EHDS porta con sé, «titolare dei dati sanitari» è quello che più rischia di far inciampare il giurista abituato al lessico GDPR. Non è il «titolare del trattamento» di cui all'art. 4, n. 7, GDPR[70]; non coincide necessariamente con lui; e tuttavia spesso con lui si sovrappone. L'EHDS chiede di cambiare fuoco: non più solo chi decide «finalità e mezzi» del trattamento, ma anche chi – per ruolo istituzionale o per controllo tecnico – detiene dati sanitari elettronici e può renderli disponibili in un circuito di riuso regolato[71].

S.p.A. – *Engineering* Ingegneria Informatica S.p.A.». L'atto colloca prenotazione/accettazione dentro l'organizzazione del prestatore (ente sanitario) e qualifica l'*outsourcer* come responsabile, non come prestatore autonomo. Analogo esito nel CUP di Gemelli Isola: l'Informativa indica Gemelli Isola S.B. S.p.A. come Titolare per le prenotazioni telefoniche di prestazioni sanitarie; il servizio di *call-center* è mero ausilio organizzativo. Ciò è perfettamente coerente con: (i) la definizione UE di "prestatore di assistenza sanitaria" come «qualsiasi persona fisica o giuridica (…) che prest(i) legalmente assistenza sanitaria» (art. 3, lett. g, dir. 2011/24/UE); (ii) la nozione EHDS di "uso primario" che ricomprende anche i servizi amministrativi o di rimborso connessi alla presa in carico (art. 2, § 2, lett. d, reg. (UE) 2025/327); (iii) gli obblighi di tracciabilità e logging (D.P.C.M. 29.9.2015, n. 178 – FSE – e art. 14 EHDS sulla registrazione in EHR). In breve: CUP/accettazione/billing sono funzioni interne del prestatore in uso primario; i terzi esternalizzati agiscono *ex* art. 28 GDPR.

[69] È operativo lo scambio di ricette elettroniche tra Finlandia ed Estonia nell'infrastruttura *MyHealth@EU*: un cittadino finlandese può farsi dispensare il farmaco in una farmacia estone; la farmacia – "prestatore di assistenza sanitaria" ai sensi dell'art. 3, lett. g), dir. 2011/24/UE – acquisisce la *ePrescription* e, dopo la consegna, invia il riscontro di dispensazione al punto di contatto nazionale del Paese che ha emesso la ricetta. Tale flusso integra uso primario disciplinato dal Capo II del Reg. (UE) 2025/327 sullo Spazio europeo dei dati sanitari, che prevede il collegamento dei prestatori, comprese le farmacie, a *MyHealth@EU* e l'obbligo di segnalazione della dispensazione allo Stato di origine della prescrizione. Se, invece, quella stessa dispensazione fosse richiesta per finalità diverse dalla cura (ricerca scientifica, vigilanza sanitaria, supporto alle politiche), la messa a disposizione ricadrebbe nell'uso secondario: l'accesso dovrebbe avvenire tramite HDAB competente, in ambiente di trattamento sicuro e nei soli casi tassativi indicati dall'art. 53 EHDS (Capo IV).

[70] Il «titolare del trattamento» ai sensi del GDPR è chi determina finalità e mezzi del trattamento; se questi sono fissati dal diritto UE o nazionale, la legge individua direttamente il titolare o i criteri per designarlo.

[71] Resta la questione semantica: sarebbe meglio bandire l'ossimoro «titolare dei dati (sanitari)» – che in italiano porta con sé l'eco proprietaria – e restare ai termini dell'EHDS (*data holder*/detentore) e del GDPR (titolare del trattamento). Il primo qualifica una disponibilità funzionale alla condivisione regolata; il secondo, una responsabilità decisionale sul trattamento. Mescolarli equivale a confondere piani, e responsabilità. Il legislatore, su questo, è stato chiaro; sta alla prassi non tornare all'indistinto.

Il diritto dei dati, qui, diventa diritto della circolazione dei dati, con un'idea di «detenzione qualificata» che funge da cerniera tra interessi pubblici e posizioni soggettive[72].

La definizione positiva – contenuta nell'art. 2, § 2, lett. t, del Reg. (UE) 2025/327 – è volutamente ampia: sono «titolari dei dati sanitari» soggetti pubblici o privati (persone fisiche o enti) operanti nel settore sanitario o della ricerca/innovazione, registri pubblici, ma anche fabbricanti di soluzioni digitali che, per scelta tecnica o giuridica, hanno il diritto/obbligo di trattare dati sanitari elettronici o di renderli disponibili (pure se non personali, perché già anonimizzati)[73]. È l'angolo soggettivo dell'EHDS: accanto al «titolare» sta l'«utente di dati sanitari» (lett. u, *infra*), cui l'accesso è concesso per usi secondari sulla base di un titolo amministrativo (*data permit*), nell'ambito di una *governance* che istituzionalizza organismi di accesso nazionali. La letteratura ha sottolineato questa torsione concettuale e la necessità di tenere distinto il piano EHDS dal piano GDPR[74].
Nell'uso secondario, il titolare dei dati sanitari è il perno del *data sharing*: chi intende riutilizzare dati presenta domanda all'HDAB[75]; l'HDAB verifica l'inquadramento nelle finalità dell'art. 53 EHDS e, se i requisiti ricorrono, rilascia il permesso di accesso (art. 68 EHDS)[76].
Il confronto con il titolare GDPR si gioca su due assi.
Da un lato, il criterio di imputazione: nel GDPR è titolare chi decide finalità e mezzi del trattamento, nell'EHDS invece è titolare chi detiene dati sanitari elettronici e, proprio per questo, è gravato da un dovere legale di condividerli secondo uno statuto oggettivo di obblighi. Non muta l'etichetta, muta la funzione. La definizione ampia impone una mappatura puntuale degli attori: immediati i casi di ministeri della salute o registri pubblici, meno scontati quelli di soggetti privati, come produttori extra-UE di dispositivi *wearable* che raccolgono dati di cittadini europei, verosimilmente inclusi se i prodotti sono destinati al mercato sanitario UE[77]. Opportuno, dunque, che gli Stati forniscano elenchi o criteri uniformi per chiarire chi sia effettivamente obbligato.
Sul piano applicativo non mancano "zone d'ombra".

---

[72] S. CORSO, *Lo spazio europeo dei dati sanitari. Prime riflessioni sul Regolamento UE 2025/327*, cit., 574.
[73] È "*data holder*" ai fini EHDS chi: (i) opera nella sanità o nell'assistenza ed è per legge legittimato/obbligato a trattare dati sanitari personali; ovvero (ii) detiene dati sanitari non personali in ragione di un controllo tecnico sulla progettazione/erogazione di prodotti o servizi (es. produttori di dispositivi medici, sviluppatori di *app* salute) ed è in grado di metterli a disposizione per l'uso secondario. Non basta il contatto episodico con dati sulla salute: un ristorante o una mensa che raccolgano allergie, un'assicurazione che acquisisca informazioni per l'*underwriting*, un'*app* di fitness a fini ludico-motivazionali e non qualificata come dispositivo medico non acquistano, di regola, la qualifica. La figura EHDS non si sovrappone al "titolare" GDPR: spesso il *data holder* è (co)-titolare ai sensi del GDPR, non viceversa. La categoria resta ampia: strutture sanitarie pubbliche e private, laboratori, imprese farmaceutiche con dati da *trial*, registri di patologia, gestori di *wearables* o app di *wellness* (ove generino "*electronic health data*" rilevanti), nonché istituzioni UE (p.es. EMA) titolari di banche dati.
[74] S. CORSO, *Lo spazio europeo dei dati sanitari. Prime riflessioni sul Regolamento UE 2025/327*, cit., 574.
[75] Reg. (UE) 2025/327, artt. 55, 67.
[76] Da qui la ripartizione: *data holder* mette a disposizione i *dataset* indicati nel permesso; *data user* li tratta solo entro i limiti autorizzati e nell'ambiente sicuro; HDAB resta il regista che autorizza, condiziona e controlla.
[77] *Apple Inc.* (USA) ha ottenuto la marcatura CE per l'«*ECG app*» e la funzione di notifica del ritmo irregolare di *Apple Watch*, rendendole disponibili in vari Paesi europei; analogamente, *Fitbit* (Google, USA) ha ricevuto marcatura CE per la propria *app* ECG per l'identificazione della fibrillazione atriale. In scenari di questo tipo, ove siano soddisfatte le condizioni di cui all'art. 2, § 2, lett. t, i fabbricanti possono qualificarsi come «titolari dei dati sanitari» EHDS in relazione ai flussi di dati che controllano o sono tenuti a rendere disponibili.

Rispetto al concetto di titolare del trattamento (*data controller*) del GDPR, il titolare dei dati sanitari è focalizzato sul settore sanitario e sulle capacità di condivisione di dati per scopi delineati dal regolamento. Essere «titolare dei dati sanitari» ai fini EHDS non presuppone necessariamente la qualifica di titolare del trattamento *ex* GDPR: la definizione (art. 2, § 2, lett. t) include anche chi detiene dati sanitari elettronici (anche non personali, perché anonimizzati) o ne governa tecnicamente la disponibilità ai fini del riuso regolato. Un'azienda che tratta dati sanitari solo internamente ma non può (o non deve) condividerli, potrebbe essere titolare del trattamento secondo il GDPR ma non essere considerata titolare dei dati sanitari ai fini EHDS se non rientra nei casi suddetti. Viceversa, l'EHDS allarga la prospettiva includendo anche dati non personali sanitari (es. *dataset* già anonimizzati) e figure non strettamente cliniche (es. sviluppatore di un'*app* di salute): costoro non sarebbero «titolari del trattamento» di dati personali (in quanto i dati o non sono personali o non li trattano come *controller*), ma vengono coinvolti come *data holder* se possono condividere dati sanitari[78].

In chiusura, il titolare dei dati sanitari segna il cambio di paradigma: dal controllo "proprietario" alla cooperazione obbligatoria e regolata, con la legge che bilancia senza azzerare l'interesse privato. È una figura-ponte che tiene insieme l'asse personalista del GDPR e la "quinta libertà" dei dati in sanità, traducendo l'interesse pubblico in doveri concreti di messa a disposizione. Resistenze e contenziosi sono fisiologici, specie quando il dato è anche *asset* economico, ma l'EHDS incanala il conflitto in una *routine* amministrata; il resto lo faranno giurisprudenza e *soft law*, traghettando la categoria alla prassi e consolidando quella fiducia, anche dei privati, che fa del 'bene comune' dei dati sanitari un investimento, non una perdita di controllo.

X. L'UTENTE DEI DATI SANITARI

Nel sistema EHDS l'«utente dei dati sanitari» non è il paziente né l'utente del servizio, ma la figura tecnico-istituzionale che, su titolo pubblicistico, converte l'informazione clinica in decisione, conoscenza e innovazione.

L'art. 2, §2, lett. u) del Reg. (UE) 2025/327 lo qualifica come la persona fisica o giuridica – incluse istituzioni e organi dell'Unione – cui sia legittimamente concesso l'accesso a dati sanitari elettronici ai fini dell'«uso secondario», per effetto di una *data permit*, dell'approvazione di una richiesta di dati o mediante un partecipante autorizzato alla rete *HealthData@EU*[79].

[78] Un altro esempio, in breve. L'Università/IRCCS è utente di dati sanitari; riceve via HDAB *dataset* pseudonimizzati/anonimizzati nei limiti del *permit* e delle finalità *ex* art. 53, con pubblicazione dei risultati entro 18 mesi; il *data holder* (p.es. registro tumori) alimenta l'ambiente sicuro; l'utente non esce dal recinto autorizzato, vietati *marketing*, *pricing* assicurativo e altri impieghi pregiudizievoli.

[79] È utente chi riceve un'autorizzazione ai dati o un permesso di accesso nell'ambito di *HealthData@EU* per una finalità ammessa (sanità pubblica, politica, statistica, formazione, ricerca, miglioramento qualità). Non è utente chi utilizza dati sanitari per fini privati o non rientranti tra le finalità del Capo IV. Il ristoratore che riceve l'elenco delle allergie degli invitati o un datore di lavoro che ottiene i certificati medici dei dipendenti non *diventano data user* EHDS: si applica solo il GDPR e, se previsto dal diritto interno, la disciplina della medicina del lavoro.

Dentro il perimetro dell'uso secondario rientra, così, l'università che ottiene dati pseudonimizzati per una ricerca sulla prevenzione del diabete; vi rientra l'agenzia di sanità pubblica che accede ai dati per monitorare l'efficacia di un vaccino; vi rientra l'organismo statistico nazionale che elabora indicatori sulla salute mentale; e vi rientra, ancora, l'impresa biomedica che addestra un algoritmo in un ambiente sicuro al fine di migliorare la diagnosi precoce del cancro. In tutti questi casi, l'elemento qualificante è la finalità di interesse generale tipizzata dal Capo IV del Reg. (UE) 2025/327 (ricerca, sanità pubblica, statistica ufficiale, sviluppo e validazione di algoritmi in cornici controllate), con l'ulteriore presidio procedimentale dell'autorizzazione rilasciata dall'HDAB competente e delle cautele tecniche (pseudonimizzazione, accesso in ambienti sicuri, tracciabilità).

Il profilo di confine è istruttivo. Un consorzio pubblico-privato che intenda sviluppare un algoritmo predittivo per la prevenzione di un tumore potrà accedere all'EHDS se incardina la richiesta nella finalità di ricerca e innovazione, presentando istanza all'HDAB e accettando le condizioni tecniche e organizzative del Capo IV: in tal caso è, a pieno titolo, "*data user*". Se, invece, l'obiettivo sostanziale è creare un prodotto commerciale destinato a segmentare il mercato e discriminare i clienti, la domanda è inammissibile *ab origine*: mancando la finalità di interesse generale tipizzata, il consorzio dovrà cercare altrove la base giuridica del trattamento (nel solo perimetro GDPR), restando fuori dal circuito EHDS e dalle sue corsie privilegiate.

In breve, ancora una volta, è la teleologia dell'uso, non la veste dell'operatore, a tracciare la linea di demarcazione.

La mappa dei ruoli è espressamente tracciata dall'EHDS e si coordina con il GDPR: il detentore dei dati sanitari (*data holder*) è titolare del trattamento per la messa a disposizione dei dati verso l'organismo di accesso (HDAB) (art. 74 EHDS); l'HDAB è titolare per i propri compiti istituzionali e, quando mette a disposizione i dati nell'ambiente di trattamento sicuro, agisce come responsabile del trattamento per conto dell'utente (art. 74 EHDS); l'utente dei dati è titolare del trattamento per le attività svolte entro i limiti dell'autorizzazione e all'interno dell'ambiente sicuro (art. 74 EHDS; art. 4, n. 7, GDPR)[80]. Insomma, l'utente dei dati sanitari è un *controller* «incapsulato» entro un *habitat* tecnico-procedurale che "amministrativizza" la circolazione del dato e rende possibile, in dialogo con DGA e – sul versante primario – con la dir. 2011/24/UE, una sanità *data-driven* che tenga insieme libertà della ricerca e tutela della persona, senza dimenticare le ragioni antiche della riservatezza[81] e le ambivalenze sistemiche di un'economia dell'informazione che domanda regole eque di accesso e di riparto dei benefici[82].

[80] È una responsabilità distribuita per fasi: nessuna «presa in carico» dei fini dell'utente da parte dell'HDAB, e divieto di riuso extra-*permit*.

[81] F. DI CIOMMO, *Privacy e diritto alla salute: una convivenza difficile*, in *Danno e resp.*, 2002, 121 ss.

[82] G. MARCUS-B. MARTENS-F. CARUGATI-H. BUCHER-P. GODLOVITCH, *The European Health Data Space*, Policy Department for Economic, Scientific and Quality of Life Policies, Parlamento europeo, Luxembourg, Dec. 2022.