EHDS e soggetti vulnerabili: tra esigenze di condivisione dei dati sanitari e tutela della persona

Virgina Zambrano
Prof. ord. dell'Università di Salerno

1. Introduzione

Osservava Hegel che quando un fenomeno aumenta quantitativamente non si assiste solo ad un suo aumento, ma anche ad un radicale mutamento qualitativo. Concetto centrale della filosofia dialettica, la teoria del "Umschlag von Quantität in Qualität" restituisce le coordinate teoriche per riflettere sul rapporto fra quantità e qualità enfatizzando come l'accumulo quantitativo non sia mai solo un fatto isolato, ma ridefinisca l'intero contesto in cui quel fenomeno si manifesta conducendo inevitabilmente anche ad una variazione qualitativa[1]. Come dire che ogni variazione non è mai solo numerica ma investe lo stesso modo di essere della cosa. E questo è particolarmente vero quando si parla di salute, dati sanitari, e sfide sollevate dall'AI. Il problema è qui rappresentato dalla difficoltà di conciliare tre universi che hanno una diversa dimensione valoriale: quello della ricerca, della tutela della persona, della tecnologia.

[1] Hegel, *Wissenschaft der Logik*, A. Koch and F. Schick (ed.), Akademie Verlag, 2002, 52 ss. Celebre è l'esempio dell'acqua che, pur essendo tale anche quando si riscalda, va poi incontro alla trasformazione in vapore allorché raggiunge i 100°.

La crescente produzione di dati e la loro digitalizzazione, siano essi usati per migliorare l'approccio terapeutico o per potenziare la ricerca scientifica, solleva questioni che attengono alla tutela della privacy, alla *commodification* del dato, al suo sfruttamento economico e, in ultima analisi, alla possibilità per il soggetto di controllarne la circolazione[2]. All'obiettivo della tutela della salute, favorito dalla ricerca e dalle scoperte scientifiche, si accompagna, infatti, l'esigenza di assicurare la riservatezza del dato, cosa che ha a che vedere, ovviamente, con la tutela della dignità di una persona la quale (piaccia o no) si presenta sempre più come una sorta di grande "contenitore" di informazioni biogenetiche e psicologiche, condotte, relazioni affettive etc. in grado di alimentare processi di estrazione e di uso[3].

---

[2] Non è agevole fornire indicazioni esaustive sull'ampio panorama bibliografico che si è andato formando nel tempo sul tema dei dati sanitari. Si offre solo qualche indicazione cui si rinvia altresì per il corredo bibliografico: Corso, L*o spazio europeo dei dati sanitari. prime riflessioni sul regolamento ue 2025/327*, in *Nuove leggi civ. comm*., 3, 2025, *passim*. Cascini e Arcuri, *Uso secondario dei dati personali relativi alla salute: panoramica della normativa europea e nazionale*, in *Dir. inf.,* 2024, 837 ss.; C. Perlingieri, *Transizione digitale nella sanità ed ecosistema dei dati sanitari: profili ricostruttivi del fenomeno circolatorio e implicazioni sui dati genetici*, in *Tecnologie e Diritto*, Collana diretta da P. Femia e C. Perlingieri, 2, 2024, 485 ss.; Ricciuto, *L'equivoco della privacy. Persona vs dato personale*, Napoli, 2022, *passim*; Muciaccia, *Osservazioni preliminari per uno studio sul riutilizzo dei big healthcare data*, in *Riv. dir. priv*., 2020, 345 ss.; Séroussi *et al*., *Transforming Data into Knowledge: How to Improve the Efficiency of Clinical Care?*, in *Yearbook of Medical Informatics*, 2017, 4 ss.

[3] Nell'ambito di tali operazioni di estrazione e riutilizzo massivo dell'informazione, un ruolo centrale è svolto da quelle tecniche comunemente ricondotte al *Text and Data Mining* (TDM), vale a dire all'insieme di procedure - in larga parte automatizzate - destinate a individuare relazioni, *pattern* ricorrenti e strutture informative all'interno di *dataset* di dimensioni tali da eccedere la capacità di analisi umana. L'operazione consiste nella trasformazione di contenuti eterogenei, spesso non strutturati, in rappresentazioni concettuali suscettibili di impiego scientifico o operativo, secondo un percorso che tipicamente include la selezione delle fonti, la loro normalizzazione in formati *machine-readable*, l'estrazione mirata degli elementi rilevanti e, da ultimo, la modellizzazione delle conoscenze emergenti. In un ecosistema dominato dalla produzione continua di dati, il TDM si è progressivamente affermato come tecnica abilitante in numerosi ambiti disciplinari; fra questi, la ricerca biomedica e l'analisi dei dati sanitari costituiscono oggi uno dei terreni di applicazione più intensi e delicati, in quanto l'estrazione algoritmica di correlazioni latenti incide su informazioni altamente sensibili e potenzialmente idonee a generare inferenze sulle condizioni di salute dei soggetti coinvolti. È noto, infatti, che proprio nel settore medico l'impiego di TDM alimenta attività quali la predizione prognostica, l'identificazione di biomarcatori, la farmacovigilanza computazionale e l'addestramento di sistemi diagnostici basati su *machine learning*, con ricadute dirette sulla qualità e sulla tracciabilità del dato clinico. Nonostante la centralità crescente di tali tecniche, il quadro regolatorio che ne governa l'utilizzo rimane eterogeneo: disposizioni riconducibili al diritto d'autore, alla protezione dei dati personali, alla tutela delle banche dati e alla concorrenza si sovrappongono senza un coordinamento sistematico, generando una zona di incertezza che facilita, in alcuni contesti, l'emersione di pratiche di estrazione operate ai margini di un perimetro giuridico chiaramente definito. La dottrina ha evidenziato come questa frammentazione renda difficile individuare un vero e proprio "diritto al TDM" e, parallelamente, complichi la definizione dei limiti di liceità delle operazioni di mining, soprattutto quando esse coinvolgono

Che siffatto processo ponga in discussione l'idoneità ad esercitare quei diritti che esprimono la componente dinamica dell'essere persona non appare dubbio nella misura in cui – a leggere selettivamente i meccanismi di regolazione di cui all'EHDS – l'abbandono della dimensione "consensocentrica"[4] va nella direzione di evidenziare la presa di distanza da forme di autonomia deliberativa, da un lato, e di responsabilità, dall'altro. La conseguenza che, sotto il profilo giuridico, si apprezza è lo spostamento, secondo logiche di efficienza e di mercato, dell'asse regolatorio dalla persona ai dati che essa produce ed è in grado di trasferire. Si tratta di un processo il quale, a voler riprendere la teoria di Hegel, pone in rilevante un significativo capovolgimento di fronte, che va sicuramente rimarcato[5].

In effetti, detto che la produzione di informazioni relative alla salute è un dato di fatto e che queste informazioni attengono ai profili più delicati della persona, ciò che emerge è l'esigenza del legislatore di approdare ad una costruzione digitale della sua identità per assicurare – all'interno di una dimensione *market oriented* – lo sfruttamento econo-

---

dati sanitari o inferenze ad alto impatto. Sul punto, v. Orlando, *Il diritto di Text and Data Mining (TDM) non esiste*, in *Riv. it. di informatica e diritto (RIID)*, 1, 2023, 67 ss.; nonché, con specifico riferimento alle tecniche di estrazione, Tassone, Barbone, *Web harvesting, scraping or data extraction. Tutela delle banche dati secondo la legge sul diritto d'autore e i principi di diritto antitrust*, in *Diritto di Internet*, 1, 2020, 113 ss.

[4] Sul ridimensionamento della centralità del consenso nel sistema europeo di protezione dei dati, la dottrina ha più volte osservato come il GDPR, pur elencando il consenso dell'interessato quale prima condizione di liceità del trattamento, non lo configuri come fondamento privilegiato, ma come una delle molteplici basi giuridiche utilizzabili dal titolare, C. Perlingieri, *Transizione digitale nella sanità ed ecosistema dei dati sanitari: profili ricostruttivi del fenomeno circolatorio e implicazioni sui dati genetici*, cit., 495; D'Antonio, *Autodeterminazione informativa e dinamiche remuneratorie: i limiti dello schema negoziale*, in *I "poteri privati" delle piattaforme e le nuove frontiere della privacy*, Torino, 2022, 151 ss.; Poletti, *Le condizioni di liceità del trattamento dei dati personali*, in *Giur. it.*, 12, 2019, 2785. Tale ridimensionamento del consenso, fisiologico nel quadro del GDPR, assume tuttavia una portata diversa nel contesto dell'EHDS, dove la complessità e la strutturazione dei trattamenti sanitari possono ridurre la soglia effettiva di autodeterminazione dell'interessato, rendendo necessaria una riflessione critica sul rapporto tra autonomia, responsabilità e protezione dei diritti della persona.

[5] Una parte della dottrina ha osservato che l'architettura regolatoria dello Spazio europeo dei dati sanitari, pur animata dall'intento di favorire interoperabilità, circolazione e riuso secondario delle informazioni cliniche, presenta elementi di criticità che incidono sul bilanciamento tra esigenze di integrazione del mercato e tutela effettiva dei diritti fondamentali. In particolare, è stato evidenziato come il ricorso alla base giuridica dell'art. 114 TFUE – volta essenzialmente al funzionamento del mercato interno – risulti solo parzialmente coerente rispetto alla natura dei beni giuridici coinvolti, che attengono alla salute e alla protezione dei dati personali, settori nei quali un ancoraggio più saldo alla dimensione della cittadinanza europea consentirebbe un quadro di garanzie più robusto. Inoltre, la scelta di lasciare significativi margini attuativi ai legislatori nazionali rischia di perpetuare le frammentazioni già emerse nell'attuazione del GDPR, compromettendo l'obiettivo di un'armonizzazione sostanziale dei diritti digitali dei pazienti. Si veda, in questo senso, Calzolaio, *Il Regolamento sullo spazio dei dati sanitari nella prospettiva della cittadinanza europea*, in *Dir. inf.*, 2025, 3, 315 ss.

mico delle informazioni[6]. Il punto è che "Increasing computer power means that both uses and misuses of data are becoming more important" e, in relazione ai dati sanitari, ciò slatentizza una soggiacente tensione fra interesse pubblico e strategie proprietarie degli "intermediari" nella gestione di dati che sono inevitabilmente e continuamente prodotti e raccolti.

Certo, lo sforzo regolatorio dell'EHDS trova sintesi, forzando l'interoperabilità e garantendo l'acceso ai dati, in una scelta di selezione degli interessi da proteggere, come pure dimostra l'attenzione ai soggetti vulnerabili. Quanto preme segnalare, tuttavia, è il fatto che si è dinanzi ad un'attività condotta con lo sguardo attento all'economia la quale – per definire il *frame* degli investimenti all'interno di una logica di integrazione dei mercati – tiene conto di un progresso tecnologico che, però, in sé non ha un fine perché fondamentalmente serve sé stesso[7]. Circolo "virtuoso" quello appena descritto che consente di osservare che quando si parla di tecnologia, più che il suo uso, è in discussione il suo funzionamento e la creazione di adeguate condizioni di spiegabilità, trasparenza e responsabilità[8].

Che si tratti di obiettivo non facile da raggiungere, attraversato da tensioni e interessi contrastanti, è conferma il ritiro della *Proposal for an Artificial Intelligence Liability Directive* (AILD proposal)[9] che lascia, per contro, trasparire il timore di una espansione

---

[6] Sul processo di progressiva valorizzazione economica dell'informazione personale – e sulla riconduzione dei dati a veri e propri *asset* negoziali suscettibili di sfruttamento all'interno dei mercati digitali – si veda, Catala, *Ébauche d'une théorie juridique de l'information*, in *Inf. e dir.*, 1, 1983, 15 ss.; P. Perlingieri, *L'informazione come bene giuridico*, in *Rass. dir. civ.*, 2, 1990, 326 ss. Per le ricostruzioni più recenti, che analizzano la piena patrimonializzazione dei dati personali e l'inquadramento del loro impiego come forma di controprestazione nei contratti digitali, cfr. De Franceschi, *Il "pagamento" mediante dati personali*, in Cuffaro, D'Orazio, Ricciuto (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, 1389 ss.; Ricciuto, *La patrimonializzazione dei dati personali. Contratto e mercato nella ricostruzione del fenomeno*, in Cuffaro, D'Orazio, Ricciuto (a cura di), *op. cit.*, 2019, 25 ss.; Camardi, *Prime osservazioni sulla Direttiva (UE) 2019/770 sui contratti per la fornitura di contenuti e servizi digitali*, in *Giust. civ.*, 3, 2019, 499 ss.; nonché Ricciuto, *Il contratto ed i nuovi fenomeni patrimoniali: il caso della circolazione dei dati personali*, in *Riv. dir. civ.*, 3, 2020, 642 ss.

[7] Floridi, *Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide*, Milano, 2022, 75 ss.

[8] Sul punto, Amram, *La transizione digitale delle vulnerabilità e il sistema delle responsabilità*, in *Riv. it. med. leg.*, 1, 2023, 3.

[9] Cfr., *https://commission.europa.eu/business-economy-euro/doing-business-eu/contract-rules/digital-contracts/liability-rules-artificial-intelligence_en.* L'esigenza di una normazione, considerato la diversità di soluzioni adottate, traeva spunto dalla esigenza di uniformare i diversi regimi di responsabilità, specie in punto di prova del nesso causale. Di siffatte difficoltà è testimonianza un *case law* che ha messo in luce il fatto che la vittima del danno è pregiudicata in punto di regime probatorio a causa della tradizionale asimmetria informativa. Tanto senza considerare lo schermo offerto dalla tutela della proprietà intellettuale. Su queste premesse si sono prodotti orientamenti contrastanti. Si pensi, per un verso a CGUE, C-634/21 Schufa Holding ; C-203/22 Dun & Bradstreet Austria e, per l'altro, alla decisione del BGH 28 gennaio 2014 – VI ZR 156/13, dove i giudici hanno riconosciuto la difesa del segreto commerciale alla formula dell'algoritmo di punteggio creditizio di un'azienda privata e, per converso, alla decisione Rechtbank Den Haag, 05 febbraio 2020, C-09-

oltre le aspettative della disciplina della responsabilità per l'intelligenza artificiale, ritenendo preferibile un processo di semplificazione normativa a stimolo, appunto, della competitività tecnologica (su cui forse ha pesato l'esigenza di evitare una *overregulation* nella prospettiva dell'impresa francese Mistral)[10].

Resta il fatto, nella prospettiva del giurista, che la nuova frontiera dei dati sanitari è alimentata da una particolare attenzione a connettere fra loro profili economici, giuridici e ovviamente di tutela della persona e della sua dignità. Di siffatta "erosione delle prerogative della persona" che, da un lato, ne trasforma il corpo e, dall'altro, impone una crescente attenzione alla dignità della persona[11], è conferma il dibattito sull'uso dei dati sanitari, specie in rapporto alla tutela delle persone vulnerabili[12].

2. L'EHDS tra vulnerabilità, consenso e dati sanitari

Un punto di partenza obbligato per ogni possibile discorso in tema è comunque rappresentato dalla individuazione della base giuridica su cui innestare la tutela. Le cose, infatti, cambiano a seconda che a legittimare il trattamento sia il consenso ovvero l'insieme dei dati sia "adoperato con finalità pubblicistiche, per la determinazione – grazie all'utilizzo combinato di sistemi di intelligenza artificiale – delle politiche sanitarie per la salute pubblica, specie di tipo preventivo"[13].

550982-HA ZA 18-388, reperibile all'indirizzo *https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBDHA:2020:1878* che ha stabilito che il pregiudizio etnico nella valutazione automatizzata del rischio per indagini mirate sulle frodi sociali viola l'articolo 8 della CEDU).

[10] E, in vero, sono evidenti le chiare implicazioni politiche e ed economiche del ritiro di una proposta su cui sembrano aver pesato pressioni esterne e interessi nazionali. Nel caso di specie, il riferimento è al rischio che una regolamentazione rigorosa avrebbe avuto effetti negativi su Mistral AI, percepita come la risposta europea a colossi americani quali OpenAI e Google. Ritiro non a caso intervenuto a ridosso del Summit di Parigi sull'AI e, dunque, percepito come una manovra strategica per non spaventare gli investimenti e la competitività.

[11] Rodotà, *Privacy, libertà, dignità. Discorso conclusivo della Conferenza internazionale sulla protezione dei dati*, settembre 2004 in *https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1049293* il quale già osservava che "il rapporto tra privacy e dignità si presenta come un fondamentale fattore di contrasto delle potenti logiche che premono per la trasformazione delle nostre organizzazioni sociali in società, della sorveglianza, della classificazione, della selezione discriminatoria. Un compito, tuttavia, che sembra divenire sempre più difficile".

[12] Per prime riflessioni in tema, Bellomia, *Sanità digitale e persone vulnerabili*, in Morace Pinelli (a cura di), *Sanità digitale. Regolamento "EHDS" (UE 2025/327) sullo spazio europeo dei dati sanitari. Uso dei dati e assetti organizzativi*, I, Pisa, 2025, 391 ss.; Corso, *Alla frontiera del diritto privato. Nuove tecnologie e persona anziana*, in *Nuova giur. civ. comm.*, 2024, II, 1253 ss.

[13] Irti, *L'uso delle "tecnologie mobili" applicate alla salute: riflessioni al confine tra la forza del progresso e la vulnerabilità del soggetto anziano*, in *Persona e mercato*, 1, 2023, 43.

Elevata interoperatività delle piattaforme di raccolta dati, utilizzabilità dei dati raccolti suscettibili di essere conferiti, acquisiti, trattati, uso secondario[14] di questi, danno conto per un verso dell'importanza di una medicina che si avvale di un *set* di dati sempre più ampio e affidabile in rapporto all'uso primario di dati e, per l'altro dei rischi sottesi a tale ecosistema[15]. Rischi rispetto ai quali il consenso e le tecniche di informazione/comunicazione erigono una barriera molto diafana già a tutela della persona capace, finendo sostanzialmente con il promettere più di quanto siano poi in grado di realizzare.

Che l'obiettivo primario del quadro regolatorio sia quello di assicurare un adeguato contemperamento fra l'autodeterminazione informativa degli interessati e gli interessi della ricerca scientifica è evidente. La tensione, specie in relazione ai dati sanitari, emerge già dal GDPR (cfr. art. 9) che, ad esempio in relazione ai dati genetici, affianca al divieto di trattamento una serie di condizioni che ne giustificano la "cedevolezza" in virtù di interessi ritenuti idonei e rilevanti (art. 9, § 2, lett. j, con l'ulteriore limitazione rappresentata dal rispetto delle garanzie di cui all'art. 89 quali la pseudonimizzazione, il principio di minimizzazione etc.)[16].

Dal canto suo l'art. 5 GDPR (§1, lett. b) ammette al trattamento senza consenso in presenza di rilevanti interessi pubblici e a condizione del rispetto della disciplina di cui

---

[14] Una ricostruzione sistematica del *secondary use* in prospettiva di sanità pubblica, con analisi delle ricadute operative e dei casi d'uso, è offerta da Cascini, *Secondary Use of Electronic Health Data. Public Health Perspectives, Use Cases and Challenges*, Berlin, 2025, 15 ss.; di contro, sul versante critico dell'uso secondario dei dati sanitari, si veda Cabrio, *La seconda vita dei dati. Luci e ombre della normativa privacy in materia di secondary data use*, in Frattino, Massimino (a cura di), *I dati. Il futuro della sanità. Strumenti per una reale innovazione*, Milano, 2022, 25 ss., ove vengono evidenziate le tensioni tra obiettivi di ricerca e garanzie di protezione dell'interessato.

[15] Cfr., l'Opinion 28/2024 *on certain data protection aspects related to the processing of personal data in the context of AI models espressa dal Body of European Regulators for Electronic Communications* (BEREC) che di fatto ruota proprio intorno al concetto di legittimo interesse a base del trattamento dei dati sanitari.

[16] Il riferimento all'art. 9 del GDPR e alle sue relative eccezioni appare quanto mai emblematico in questa sede. Lo stesso, notoriamente, stabilisce un divieto tendenzialmente generale di trattare le categorie particolari di dati personali, fondato sulla necessità di predisporre un livello di protezione più elevato per diritti e libertà che possono essere incisi con particolare intensità. Il divieto non opera, tuttavia, in modo assoluto: il Regolamento individua una serie di basi giuridiche tipizzate che consentono il trattamento in casi eccezionali e strettamente delimitati, quali il consenso esplicito dell'interessato, motivi di rilevante interesse pubblico, esigenze di tutela della salute pubblica o finalità diagnostiche, di cura e gestione dei servizi sanitari. La disposizione si inserisce in un assetto sistematico improntato ai principi di proporzionalità e limitazione delle finalità, imponendo che ogni operazione su dati "sensibili" sia giustificata da condizioni sostanziali e da garanzie procedurali idonee a evitare interferenze indebite nella sfera personale. In tale quadro, la disciplina del trattamento dei "dati relativi alla salute" continua a porre questioni ermeneutiche aperte, non solo relativamente all'estensione della nozione ma anche in rapporto al restante diritto dell'UE, Corso, L*o spazio europeo dei dati sanitari. prime riflessioni sul regolamento UE 2025/327*, cit., 577; Donnelly, McDonagh, *Health Research, Consent and the GDPR Exemption*, in *European Journal of Health Law*, February 2021, p. 4 ss.

all'art. 9 (2)h i e 3 GDPR. Profilo, questo, che trova specchio altresì nella previsione di cui all'art. 2-*septies* codice Privacy e in una ricca normazione che dispone questa eccezione, conferendo poteri e obblighi alle autorità pubbliche, laddove in gioco siano interessi ritenuti rilevanti[17].

Progressiva presa di distanza dal consenso che giunge, appunto, ad effetto con l'EHDS e si compie in funzione di una prospettiva volta ad incentivare il mercato dei dati sanitari elettronici, regolamentato e sottoposto a controlli fin dalla richiesta di accesso ai dati secondari, cui il meccanismo di *opt-out* tenta realisticamente di dare risposta[18].

Il cammino era tuttavia già stato tracciato. In Francia, ad esempio, è emblematico che la *Commission Nationale de l'Informatique et des Libertés* avesse per tempo provveduto a definire, con la Délibération n° 2018-154 del 3 maggio 2018, e successive modifiche (MR-003), le ricerche che, in ambito sanitario, non richiedono la raccolta del consenso esplicito della persona. Sì che la recente modifica dell'art. 110 Codice Privacy[19] la quale bypassa

---

[17] Il panorama normativo è assai ricco ed è impossibile fornire un quadro esaustivo. Gli ambiti coinvolti sono quelli della salute, giustizia e assistenza sociale. Sul fronte della salute, basti pensare alla creazione e gestione dei registri dei pazienti in lista d'attesa e dei dati sui donatori e sui trapianti (L. 1° aprile 1999, n. 91); all'obbligo per le strutture trasfusionali di registrare e tracciare i dati sanitari dei donatori e delle unità di sangue (D.Lgs. 9 novembre 2007, n. 20); alla cd Legge Lorenzin in tema di verifica degli adempimenti vaccinali (Legge 31 luglio 2017, n. 119) o, ancora, da ultimo la Legge 22 marzo 2019, n. 29 (Rete nazionale dei registri dei tumori e sistemi di sorveglianza) che fornisce la base giuridica per il trattamento senza consenso.

[18] A seguito del parere favorevole dell'Autorità garante per la protezione dei dati personali, è stato pubblicato, nella Gazzetta Ufficiale n. 53 del 5 marzo 2025, il decreto del Ministero della salute del 31 dicembre 2024, che, in attuazione dell'art. 12, comma 15-*quater*, del d.l. n. 179/2012, istituisce l'Ecosistema dei dati sanitari (EDS). Si tratta di un'infrastruttura tecnologica progettata per comprendere al proprio interno i dati trasmessi al Fascicolo sanitario elettronico (FSE) dalle strutture sanitarie e sociosanitarie e dagli enti del Servizio sanitario nazionale, nonché i dati resi disponibili tramite la Tessera sanitaria. Attraverso la raccolta e il trattamento di tali informazioni, l'EDS si propone di fornire, in modo omogeneo sul territorio nazionale, servizi di supporto.

[19] Com'è ampiamente noto, l'art. 110 del Codice privacy ha subito una rilevante revisione ad opera del d.l. *PNRR-bis*, con cui il legislatore ha inteso semplificare il trattamento dei dati sanitari nell'ambito della ricerca medica, biomedica ed epidemiologica, soprattutto nei casi in cui la raccolta del consenso dell'interessato risulti impossibile o particolarmente gravosa. La nuova formulazione, pur mantenendo il principio di necessità e le garanzie richieste dal GDPR per l'uso di dati appartenenti a categorie particolari, introduce un modello più flessibile fondato su procedure standardizzate e su un più marcato ricorso agli strumenti di co-regolazione. Elemento centrale della riforma è l'attribuzione alle regole deontologiche – la cui elaborazione è stata avviata dal Garante – della funzione di disciplinare nel dettaglio le condizioni di liceità, le misure di sicurezza e i limiti del trattamento, così da garantire un equilibrio tra promozione della ricerca e tutela dei diritti fondamentali degli interessati. Tale revisione si inserisce, inoltre, in un quadro normativo che riconosce all'intelligenza artificiale un ruolo crescente nei processi sanitari, rendendo necessario un rafforzamento strutturale delle garanzie a presidio della dignità e dell'autonomia del paziente. Una lettura complessiva di tali interventi evidenzia come la modifica dell'art. 110 risponda all'esigenza di rendere più efficiente la ricerca senza indebolire la protezione dei dati, valorizzando proprio il modello di co-regolazione quale cardine della disciplina. Si veda, Stanzione, *Intelligenza*

il consenso preventivo dell'interessato – se sono adottate misure appropriate per tutelare i suoi diritti, le libertà e i legittimi interessi dell'interessato – in presenza di quelle misure appropriate di cui al Provvedimento 9 maggio 2024, n. 298 (dove sono, appunto, presi in considerazione i dati sanitari provenienti da diversi database quali i registri dei tumori, schede di dimissione ospedaliera, specialistica ambulatoriale, farmaceutica, hospice, assistenza protesica, pronto soccorso, assistenza domiciliare e flussi di anatomia patologica, appartenenti a milioni di utenti e resi fruibili sulla base di un attento procedimento di anonimizzazione) appare la risposta italiana alla esigenza di allontanarsi dalla regola del consenso per la ricerca su dati *esistenti* (soggetti deceduti o irreperibili). Esigenza che il legislatore tedesco del 2018[20] del Bundesdatenschutzgesetz (BDSG) aveva già avvertito "als diese Rechte voraussichtlich die Verwirklichung der Forschungs" (§ 27, abs 2 BDSG) e dove la stessa informazione è superata se, per renderla, occorre compiere uno sforzo non proporzionato. In questo senso, centrato come è sui pilastri della "necessità e prevalenza dell'interesse pubblico", il BDSG ha sviluppato un approccio molto simile a quello che legittima l'uso secondario nell'EHDS[21].

È considerando queste premesse che la riflessione sulla vulnerabilità prende respiro. A ben vedere, infatti, se si ritiene che base giuridica del trattamento sia il consenso, è conseguenziale ritenere che, in caso di soggetti vulnerabili, la soluzione vada individuata nel ricorso agli strumenti di sostituzione dell'incapace. Mentre se la base giuridica è l'interesse pubblico, la persona incapace è tutelata attraverso quelle garanzie che trovano sponda nel § 27 BDSG (necessità, bilanciamento, misure di sicurezza) nell'art. 110 Codice privacy o nel quadro delineato in Francia dalla MR-003 e che variamente chiamano in causa il parere di un Comitato Etico incaricato di procedere ad una verifica dell'adeguatezza delle tutele per i soggetti vulnerabili.

---

artificiale, dati sanitari e FSE nel quadro sanitario dell'Unione Europea, in Morace Pinelli (a cura di), *Sanità digitale. Regolamento "EHDS" (UE 2025/327)*, cit., 5.

[20] Bundesdatenschutzgesetz vom 30. Juni 2017 (BGBl. I S. 2097), modificata da ultimo dall'art. 7 della legge 6 maggio 2024 (BGBl. 2024 I Nr. 149).

[21] In un'ottica ulteriore di comparazione, merita richiamo l'analisi di Lee, Choi, *Secondary Use Provisions in the European Health Data Space Proposal and Policy Recommendations for Korea*, in *Healthcare Informatics Research*, 29, 3, 2023, 199-208, ove gli Autori mostrano come la proposta europea sullo Spazio dei dati sanitari si configuri quale modello normativo potenzialmente esportabile anche oltre i confini dell'Unione. Dallo studio emerge che l'EHDS introduce un quadro organico per il riutilizzo dei dati sanitari elettronici a fini di ricerca, innovazione tecnologica e sviluppo di applicazioni di intelligenza artificiale, assumendo così una funzione paradigmatica. Gli Autori evidenziano, peraltro, che l'eventuale trapianto di un sistema analogo in Corea del Sud incontrerebbe rilevanti ostacoli - in particolare rispetto agli obblighi di condivisione dei dati gravanti sui soggetti privati - pur riconoscendo che almeno i dati prodotti nell'ambito di progetti finanziati con risorse pubbliche dovrebbero essere resi più agevolmente accessibili per usi secondari. L'affresco comparatistico conferma, dunque, l'ambizione dell'EHDS di coniugare tutela dei diritti fondamentali e promozione dell'innovazione scientifica, bilanciando l'interesse individuale alla protezione dei dati con l'interesse collettivo allo sviluppo della ricerca.

3. I complessi confini della vulnerabilità

Sullo sfondo della tutela dei soggetti vulnerabili alla luce della disciplina di cui all'EHDS giace la consapevolezza che la "gestione" giuridica della vulnerabilità non è semplice. Si accompagna, alla difficoltà di offrirne una adeguata definizione, il suo essere utilizzata strumentalmente a volte come scudo, altre come spada. In quest'ultimo senso, specie quando impiegata come premessa per promuovere servizi innovativi di telemedicina, assistenza a domicilio e così via[22].

Riguardato dal punto di vista dei diritti umani (e, dunque, nella sua veste di "scudo") l'interesse per la vulnerabilità ha alimentato un interessante confronto filosofico e giuridico. L'ampiezza del dibattito è in funzione diretta di una crescente attenzione ai temi della fragilità e della dipendenza, legati ad una accelerazione delle relazioni umane che determina una inevitabile esposizione al rischio, con tutto ciò che ne consegue in termini di danno. Aspetto, questo, puntualmente confermato dalla stessa radice latina del lemma e che, in fondo, mette in rilievo il fatto che le relazioni umane tendono a generare danno; l'autonomia della persona essendo semmai il prodotto di interventi volti a "recuperare" situazioni di diseguaglianza[23]. In questo senso, attesa la complessità delle relazioni sociali, tutte le persone sono potenzialmente soggetti vulnerabili o, almeno, hanno fatto esperienza di una condizione di vulnerabilità.

Non v'è dubbio, che esistono delle categorie quali minori, anziani, incapaci, malati, minoranze storicamente determinate, richiedenti asilo, donne, comunità LGBT+ ma anche consumatori (e non solo) per i quali l'esposizione al rischio è di più immediata percezione. Per questi, l'operare congiunto di fattori economici, sociali, ambientali e naturali rende più rilevante la condizione di fragilità e più significativo il danno. L'unificazione del soggetto di diritto non cancella cioè le differenze che esistono e impediscono la completa partecipazione alla vita sociale ed economica.

Del pari vero che quello di vulnerabilità mette in circuito una visione articolata del concetto che, di là dall'appartenenza a determinate categorie, ne slatentizza la dimensione relazionale; una dimensione che espone tutti noi a forme "*disquieting hazard*"[24]. Così

---

[22] Un buon esempio viene dal richiamo che compare nel Considerando 28 del Reg. (UE) 2025/327 del Parlamento europeo e del Consiglio ai servizi di telemedicina come strumento per ridurre le diseguaglianze. Spunto si rinvia altresì all'*International Code of practice for Telehealth Service*. art. B4, consultabile al sito *https://sctt.org.uk/wp-content/uploads/2017/04/Workstream-4-2017-V2-INTERNATIONAL-TELEHEALTH-CODE-OF-PRACTICE-ASTER.pdf*. Su alcune riflessioni critiche relativamente all'uso di questi dispositivi, Corso, *Alla frontiera del diritto privato. Nuove tecnologie e persona anziana*, in *Nuova giur. civ. comm.*, 2024, II, 1264 ss.

[23] Esposito, *Investigating Digital Vulnerability with Theories of Harms: A Methodological Proposal with Three Illustrations*, in *The New Shapes of Digital Vulnerability in European Private Law*, 2024, 53-88.

[24] Mackenzie, Rogers and Dodds (eds.), *Vulnerability: New Ethics and Feminist Philosophy*, Oxford, 2014, 7-9, ove si distingue una vulnerabilità 1) "intrinsic to the human condition;" 2) situational vulnerability, in "context specific;" e 3) pathogenic vulnerability, which stems from abuse, injustice

intesa, essa sembra funzionare da compasso per misurare l'ampiezza del rischio cui è esposta la persona in rapporto alla situazione concreta che si trova a vivere e al modo in cui può affrontarla. La proliferazione dei meccanismi di *prosumption* e *commodification* in salute, che ovviamente varia in relazione al gradiente sociale cui individui e gruppi possono essere ascritti, apre a differenziazioni e stratificazioni generate dal peso dei determinanti economici, sociali e culturali della salute, esacerbando l'intersezione tra capacità della persona e disponibilità della tecnologia[25]. Il che dà conto di una sorta di "vulnerabilità strutturale" che "radica nel carattere intrinsecamente asimmetrico della relazione soggetto umano-agente artificiale"[26], proiettandosi sulla difficoltà di declinare una efficace risposta sul piano giuridico, politico, organizzativo. La vulnerabilità, quale misura dell'esposizione al rischio, finisce così per collocarsi nel solco delle storiche riflessioni sulla trasformazione della responsabilità civile nell'età tecnologica, ove il rischio diviene parametro ordinante delle tutele[27]. Certo, come si avvertiva, infermi di mente, minori, anziani appaiono soggetti vulnerabili *ex se* e verso costoro sono indirizzati gli sforzi normativi.

In questi casi la vulnerabilità si presenta però come il risultato di una scelta di *policy* fra ciò che è meritevole di specifica protezione e ciò che invece può essere lasciato alla normale dinamica relazionale. Il che spiega perché l'intervento di riequilibrio del legislatore si indirizzi esclusivamente nei confronti di quei soggetti verso i quali egli ritiene di avere una dichiarata responsabilità[28]. All'orizzonte di quanto si è andato allineando

---

or oppression; Ferrarese, *Vulnerability: a concept with which to undo the world as it is?*, in *Critical Horizons*, 17, 2, 2016, 151, nonché per un analisi della vulnerabilità dal punto di vista medico, Costa, *Vulnerabilità e fragilità in sanità pubblica, nelle politiche e nei metodi di studio*, in *Epidemiol Prev,* 44, 5-6, 2020, 14 ss.; Corso, *Alla frontiera del diritto privato. Nuove tecnologie e persona anziana*, in *Nuova giur. civ. comm*., 2024, II, 1253 ss.

[25] Pellegrino, *The commodification of medical and health care: the moral consequences of a paradigm shift from a professional to a market ethic*, in *Journal of Medicine and Philosophy*, 24, 3, 1999, 243-266; Morondo Taramundi, *Un nuovo paradigma per l'eguaglianza? La vulnerabilità tra condizione umana e mancanza di protezione*, in Casalini,Giolo, Re, *Vulnerabilità, etica, politica e diritto*, cit., 188-89; Botrugno, *Innovazione tecnologica in salute e* commodification. *Verso un nuovo dovere di protezione dell'individuo*?, in *Jura Gentium*, 2020, 142 ss.; Christiansen, *Commodification of healthcare and its consequences*, in *World Review of Political Economy*, 8 (2017). Sulla nozione di *prosumer*, Comor, *Contextualizing and Critiquing the Fantastic Prosumer: Power, Alienation and Hegemony*, in *Critical Sociology*, 37, 3, 2010, 309-327 (spec. 310).

[26] Irti, *L'uso delle "tecnologie mobili" applicate alla salute: riflessioni al confine tra la forza del progresso e la vulnerabilità del soggetto anziano,* cit., 449; Corso, L*o spazio europeo dei dati sanitari. prime riflessioni sul regolamento UE 2025/327*, 562.

[27] Cfr., Trimarchi, *Rischio e responsabilità oggettiva*, Milano, 1961, spec. 43 ss.; Rodotà, *Il problema della responsabilità civile*, Milano, 1964, spec. 175 ss.; Comporti, *Esposizione al pericolo e responsabilità civile*, Napoli, 1965; Monateri, *Le fonti delle obbligazioni. La responsabilità civile*, in Sacco (dir.), *Trattato di diritto civile*, III, Torino, 1998, 1011 ss.; Alpa, *La responsabilità civile. Parte generale*, Torino, 2010, 293 ss.; Frosini, *Cibernetica diritto e società*, Milano, 1968, spec. 124 s.

[28] Esposito, *Investigating Digital Vulnerability with Theories of Harms: A Methodological Proposal*

giace l'inevitabile conclusione che la vulnerabilità possiede una duplice connotazione, articolandosi in funzione di una dimensione oggettiva e soggettiva al tempo stesso, cosa che rende complesso stabilirne l'*ubi consistam*[29].

Indeterminatezza di confini che non manca di contagiare la stessa grammatica giuridica.

Si spiega così perché i discorsi sulla vulnerabilità finiscano con il ruotare sostanzialmente intorno al profilo, per un verso, dell'*empowerment* delle persone (Recital 6 EHDS)[30]; e, per l'altro, si concentrino sull'analisi del danno e delle soluzioni che ne permettano l'eliminazione. Di siffatta complessità semantica che poggia sui contenuti intrinseci di un concetto dai confini incerti si ha conferma nell'*AI Act*. Pur riconoscendone la natura non monolitica, il riferimento alla vulnerabilità, che compare in articoli chiave (gli artt. 5, 7, 9 e 60 e in oltre una decina di considerando) si fa tema trasversale nell'ambito di una regolamentazione il cui impianto, nella prospettiva che qui interessa, appa-

---

with Three Illustrations, in *The New Shapes of Digital Vulnerability in European Private Law,* in De Franceschi, Crea (eds), 2024, 56. In prospettiva europea, il ricorso alla vulnerabilità quale leva argomentativa a sostegno della telemedicina si riflette nelle stesse politiche dell'Unione. Il programma «EU4Health» (2021-2027) – principale strumento finanziario europeo per il settore sanitario – lega infatti il potenziamento della telesalute alla necessità di garantire accesso alle cure per i gruppi più fragili e per le aree territorialmente svantaggiate. Il Regolamento (UE) 2021/522, all'Allegato I, art. 1, par. 6, lett. d) e i), individua tra gli obiettivi il rafforzamento dei servizi sanitari digitali transfrontalieri, lo sviluppo di infrastrutture idonee a supportare l'erogazione di cure a distanza e la promozione di modelli assistenziali domiciliari pienamente interoperabili. L'impostazione del programma, orientata alla modernizzazione digitale dei sistemi sanitari e coerente con la prospettiva "*One Health*", conferma come la telemedicina sia divenuta un tassello strutturale nelle politiche europee di tutela della salute e di riduzione delle disuguaglianze nell'accesso ai servizi.

[29] Se a livello epidemiologico e di analisi delle patologie, dati genetici etc., l'apprezzamento della vulnerabilità è sostanzialmente agevole da effettuare, più complesso è la rilevazione e la riconduzione ad effetto di una serie di informazioni collegate alla vulnerabilità sociale (grado di istruzione, supporto familiare, reddito, classe, genere, esposizione al rischio etc.).

[30] Pasquale, *Grand Bargains for Big Data: The Emerging Law of Health Information*, in *University of Maryland Francis King Carey School of Law Legal Studies Research Paper*, 2013, reperibile all'indirizzo *http://ssrn.com/abstract=2831712.* Orofino, *One Digital Health e circolazione dei dati: tra mercato unico e diritti costituzionali*, in *Corti Supreme e Salute*, 1, 2025, 259; Catelani, *La digitalizzazione dei dati sanitari: un percorso ad ostacoli*, ivi, 2, 2023, dove chiaro è il riferimento all'importanza della *Digital Health* che rappresenta un cambio di paradigma importante che vede nella tecnologia un fattore di trasformazione per affrontare le sfide globali. Non si concorda, tuttavia, con quanto osserva Orofino, per il quale l'evoluzione tecnologica avrebbe contribuito a spostare il dibattito sul fronte della individuazione di tecniche di tutela dei diritti umani. Certo è innegabile che una rinnovata attenzione sia stata posta alla questione della tutela della dignità umana e che il dibattito sulle discriminazioni abbia trovato nuovo vigore. Tuttavia ciò non pare allontanarsi da una dimensione teorica e meramente speculativa che non trova risposta nelle concrete soluzioni giuridiche adombrate (come è appunto il caso della disciplina di cui all'EHDS e della gestione dei dati sanitari dei soggetti vulnerabili); Carnevale, *Tecno-vulnerabili. Per un'etica della sostenibilità tecnologica*, Napoli-Salerno, 2017, 35-39; Zullo, *Lo spazio sociale della vulnerabilità tra pretese di giustizia e pretese di diritto. Alcune considerazioni critiche*, in *Politica del diritto*, 2016, 475 ss.

re strutturalmente fiacco[31]. L'intera architettura normativa si configura piuttosto come una generica raccomandazione ad arginare situazioni di "fragilità", più che prevedere prescrizioni operative o meccanismi concreti volti a gestirne attivamente le condizioni e mitigarne l'impatto. L'impostazione appare sostanzialmente di tipo "principiale" e indiretta, non dissimile dunque da quella che permea il GDPR. Certo un approccio più sistemico e operativo è quello che, anche in considerazione agli obiettivi che il regolamento si prefigge, si scorge a base dell'EHDS. Ma, anche qui, non passa inosservata l'incapacità del lessico giuridico di abbracciare un concetto che (come si vedrà chiaramente a proposito dell'esperienza americana) presenta una forte valenza politica.

La vulnerabilità, prendendo forma all'esito della selezione degli interessi da tutelare e offrendosi alla riflessione – con buona pace di ogni tentativo di delinearne i contorni – quale strumento interpretativo chiave onde dare attuazione ai principi di dignità ed eguaglianza[32].

4. Il paradosso della vulnerabilità nell'EHDS: il disallineamento tra visione e strumenti di gestione

Al netto di nobili intenti, vale la pena rilevare che l'impianto regolatorio dell'EHDS – anche a prescindere da riflessioni sulla dinamicità o meno del consenso – appare pensato avendo in mente una persona capace, in grado di apprezzare le possibilità e le garanzie offerte dal sistema. Su questa scia si muove, d'altro canto, lo stesso GDPR il quale, per suo conto, non pone grande attenzione a situazioni che possono incidere sulla capacità, se si esclude il riferimento al minore di cui all'art. 8 e ai Considerando 38, 58 e 75 GDPR, nonché il richiamo a quella valutazione di impatto che compare all'art. 35 il quale, collocandosi nella prospettiva del rischio arrecato ai diritti e alle libertà delle persone, finisce con il riconoscere (ma indirettamente) anche l'esistenza di situazioni di "debolezza" meritevoli di particolare attenzione.

Nell'EHDS l'approccio alla vulnerabilità appare decisamente più sistemico rispetto a quello di cui al GDPR se non altro perché il regolamento, preoccupandosi di profili di *governance* del dato, è costretto a fare i conti con problemi legati all'accesso e alla alfabetizzazione informatica. Il riferimento a situazioni di *impairment* collegate a forme

---

[31] Si pensi, ad esemplificare, ai considerando 29, 48, 58, 60, 67, 93, 110, 132, 141 e 165.

[32] Sul nesso tra vulnerabilità e trasformazioni digitali in ambito sanitario, Romano, *In the Era of AI. Exploring New Frontiers in Cybercrime and Safeguarding Personal and Health Data*, in *Corti Supreme e Salute*, 1, 2024, 2 ss., il quale osserva come l'espansione delle infrastrutture digitali della sanità, pur generando nuove possibilità di integrazione dei dati e di efficientamento dei percorsi clinico-assistenziali, amplifichi contestualmente le superfici di rischio, esponendo le informazioni personali e sanitarie a forme di attacco e di manipolazione prima difficilmente configurabili. Si tratta di dinamiche che incidono in modo differenziato sui soggetti strutturalmente più fragili, contribuendo a ridefinire in senso tecnologico il perimetro stesso della vulnerabilità.

di limitata capacità di accesso si inserisce così in un ordito normativo dal quale sembra emergere il reale interesse del legislatore europeo a farsi carico del problema. È in siffatta prospettiva che vale il richiamo ai gruppi di popolazione vulnerabile (anche migranti e anziani); un richiamo che, tuttavia, appoggiandosi sulla prensile narrativa dei diritti umani, appare più che altro come un invito rivolto al legislatore nazionale a rimuovere qualsiasi forma di diseguaglianza (Considerando 28 e 89; art. 4, comma 5).

Sul piano operativo, comunque, il *focus* è sulla disabilità e di tanto sono conferma i richiami di cui ai Considerando 7-20-21-37-84, del Reg. (UE) 2025/327. Certo l'art. 4, comma 5, discorre di facile accessibilità per le persone con disabilità, gruppi vulnerabili e persone con scarsa alfabetizzazione digitale, ma l'attenzione, in concreto, è nell'istituzione di servizi di delega che dovrebbero "anche permettere ai tutori di agire per conto dei loro tutelati, compresi i minori" (Considerando 21).

In quest'ottica i *Servizi Proxy* di cui all'art. 4.2 lett. a-b, Reg., attraverso un sistema di validazione della legittimità della rappresentanza che è preliminare all'accesso, rappresentano il canale tecnico per dare attuazione a questo diritto, a livello transfrontaliero. Senonché ciò posto, è agevole rendersi conto che questo sistema dei "servizi di delega" (appunto i *proxy services* di cui all'art. 4 Reg. EHDS) solleva più di un interrogativo, legato alla difficoltà di operare un ragionevole bilanciamento tra esigenze di rispetto dell'autodeterminazione della persona, tutela dei soggetti vulnerabili e certezza del diritto nell'accesso a dati estremamente sensibili.

Se, infatti, l'obiettivo era la creazione di un ecosistema digitale europeo integrato ci si avvede subito – di là dalle buone intenzioni – che esistono una serie di variabili le quali non pare siano state adeguatamente considerate dal legislatore europeo e che si lasciano apprezzare sul piano 1) della definizione di quella rappresentanza di cui discorre l'art. 4, par. 3 del EHDS; 2) ruolo dell'autonomia decisionale dei minori e, più in generale, dei soggetti vulnerabili; 3) dei problemi di accesso e sicurezza.

Così, in primo luogo, in tema di verifica della legittimazione ad agire del rappresentante. Profilo che ha a che vedere con l'architettura normativa e istituzionale prescelta da ciascun sistema per gestire l'incapacità e dove (avuto riguardo ai diversi ordinamenti) l'elevata frammentazione giuridica del quadro regolatorio non sembra sia stata presa in considerazione.

Un buon esempio viene guardando all'esperienza tedesca. In un contesto normativo di gestione della incapacità composto – come noto – dalla *Vorsorgevollmacht* e dalla *Betreuung* e dove i §§1814 e 1820 BGB, cui si aggiunge il § 167 BGB, offrono le coordinate per il funzionamento della tutela preventiva dell'incapace, la definizione dei poteri del rappresentante legale si riversa direttamente sull'applicazione del Reg. EHDS e del BDSG. La sfida è nel fatto che il *Vorsorgevollmacht* è un mandato privato non necessariamente registrato, il che pone un primo problema legato alla verifica dei contenuti della procura[33].

[33] Sul punto, cfr. Markus, *Elder Law and Elder Law Attorney as a Model for Germany?*, in *Journal of the German Bar Association*, 2011, 671, reperibile all'indirizzo *https://ssrn.com/abstract=2135710* ove si evidenzia la centralità – e, al contempo, la problematicità – del *Vorsorgevollmacht* quale man-

Per cui se un medico italiano (tramite il suo Punto di Contatto Nazionale) richiedesse l'accesso al Riepilogo Paziente di un cittadino tedesco incapace, il *Servizio Proxy* tedesco non solo dovrebbe provvedere alla verifica della rappresentanza, ma anche garantire che l'accesso sia concesso solo per le finalità e nei limiti stabiliti dalla procura alla luce della normativa tedesca. Limiti questi che potrebbero non essere pienamente trasparenti o interpretabili da un sistema informatico estero. Non essendo obbligatoria la registrazione della *Vorsorgevollmacht* nel *Zentrales Vorsorgeregister*, siffatta verifica finisce con l'essere difficile, costringendo il *Servizio Proxy* a fare affidamento su dichiarazioni o documenti cartacei, incompatibili con un'infrastruttura digitale automatizzata.

Sfida tecnica questa cui va incontro il *Servizio Proxy* non meno complessa, avuto riguardo al sistema italiano. Della flessibilità dell'AdS non vi è a discutersi e si riflette in un decreto del giudice tutelare che non segue una impostazione standard. La modulazione dei poteri dell'AdS si proietta sul "confezionamento" di un provvedimento in grado di rispecchiare esattamente i poteri conferiti dal decreto del giudice, limitando l'accesso solo all'ambito sanitario. Il *Servizio Proxy* (o il suo sottosistema di verifica) dovrebbe teoricamente interpretare il decreto del giudice tutelare per capire se l'amministratore ha il potere di autorizzare l'accesso transfrontaliero ai dati sanitari elettronici. Laddove è chiaro che la variabilità contenutistica dei decreti rende tutto ciò praticamente impossibile. V'è dell'altro.

Se è vero che il *proxy service* deve operare nel rispetto – ove possibile – della volontà dell'amministrato è anche vero che, ad esempio, nell'ambito della ricerca biomedica, la possibilità di rivolgersi all'amministratore di sostegno è risultata strada non sempre concretamente percorribile. Gli enti di ricerca italiani, difatti, vedevano e (talvolta) sperimentavano la procedura di consultazione preventiva (di cui alle varie autorizzazioni del garante e alla vecchia formulazione dell'art. 110) come un ostacolo che rallentava eccessivamente le attività di ricerca e che, nella migliore delle ipotesi, li rendeva poco "competitivi", o comunque "appetibili" come partner di ricerca, nel contesto europeo e internazionale.

Esigenza definitivamente "esplosa" nell'intervento di riforma che ha aperto all'uso non consentito dei dati allorché "*a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca*" (art. 110).

Un ulteriore esempio viene dal modo in cui gli ordinamenti affrontano la questione della "gestione della volontà contraria". In Germania, ad esempio, la recente riforma del *Betreuungsrecht* in vigore dal 2023 ha aperto ad un principio di sussidiarietà della misura che intende rivalutare al massimo l'autodeterminazione del paziente[34]. Il *Betreuer* inter-

---

dato privatistico non necessariamente registrato, con ovvie ricadute sulla verificabilità del suo contenuto e sulla certezza dei poteri rappresentativi.

[34] Cfr. § 1821, Abs (2) BGB "Der Betreuer hat die Angelegenheiten des Betreuten so zu besorgen, dass dieser im Rahmen seiner Möglichkeiten sein Leben nach seinen Wünschen gestalten kann. Hierzu hat der Betreuer die Wünsche des Betreuten festzustellen. Diesen hat der Betreuer vorbehaltlich

viene solo dove necessario e gli strumenti di volontà anticipata prevalgono, limitando l'ingerenza statale negli affari dell'adulto. Il § 630g, Abs 3 BGB (*Einsichtnahme in die Patientenakte*) consente agli eredi l'accesso ai dati sanitari per far valere interessi patrimoniali (malpractice, risarcimento danni) ma salvo un presunto, chiaramente contrario, interesse del defunto (volontà precedentemente espressa). Tutela di interessi patrimoniali cui da ultimo la Corte di Giustizia UE (causa C-307/22) ha dato risalto stabilendo che la copia della cartella debba essere fornita gratuitamente anche se il paziente (o il *Betreuer*) la richiede per far valere diritti risarcitori (legati a casi di *malpractice*) contro il medico. Decisione, questa, importante che ha abrogato una prassi consolidata che subordinava l'ostensione ad un rimborso delle spese amministrative e ha rafforzato l'accesso ai dati sanitari, essenziale affinché il *Betreuer* possa adempiere ai suoi doveri di cura e tutela della persona (come ad esempio accertare la correttezza dei trattamenti). Le aporie appena segnalate si scaricano a tacer d'altro sulla necessità, per un verso, di definire (per il *proxy*) un chiaro quadro di responsabilità in relazione all'uso etico di tali informazioni e, per l'altro, di assicurare una tracciabilità dell'accesso effettuato dal rappresentante onde assicurare alla persona fisica – una volta riacquistata la capacità – la possibilità di conoscere chi, quando e perché ha avuto accesso ai suoi dati[35].

Analoghe considerazioni critiche valgono in relazione al profilo dell'autonomia decisionale dei minori, che pure si apre a divergenze significative. In una cornice normativa ricca ed articolata che trova sponda nella CRC (Convenzione di New York, artt. 12; 13 nonché nel divieto di qualsiasi arbitraria illecita interferenza di cui all'art. 16) e completamento nella CM/Rec(2018)7[36], la rottura definitiva del collegamento fra età e capacità

---

des Absatzes 3 zu entsprechen und den Betreuten bei deren Umsetzung rechtlich zu unterstützen. Dies gilt auch für die Wünsche, die der Betreute vor der Bestellung des Betreuers geäußert hat, es sei denn, dass er an diesen Wünschen erkennbar nicht festhalten will". In dottrina, Werner und Hunger, *Betreuungsrecht - Status quo nach der Gesetzesänderung 2023*, in *MMW - Fortschritte der Medizin*, 2023, s. 50 ss.; Mazur, *Betreuungsrecht: Ein Ratgeber für Betroffene, Betreuerinnen und Betreuer*, Beck, 2022, *passim*.

[35] Peraltro vale la pena osservare come la moltiplicazione delle possibilità di accesso ai dati crei un ambiente favorevole ad eventuali attacchi informatici, profilo sul quale si rinvia all'analisi di Longo, *La disciplina della cybersicurezza nell'Unione europea e in Italia*, in *La regolazione europea della società digitale*, cit., 203 ss.; Ong, *Mandatory data breach notification: its role in protecting personal data,* 10, 1, in *JICL*, 2023, 87 ss.

[36] Amram, *Standards to face Children and Patient Digital Vulnerability*, in *The New Shapes of Digital Vulnerability in European Private Law*, cit., 441. In proposito, si rinvia alla Raccomandazione del Comitato dei Ministri agli Stati Membri sulle linee guida relative al rispetto, alla tutela e alla realizzazione dei diritti del bambino nell'ambiente digitale, art. 3.4 "Gli Stati dovrebbero garantire che il trattamento di categorie speciali di dati considerati sensibili, come dati genetici, biometrici che identificano un bambino in modo unico, dati a carattere personale relativi a condanne penali, e dati a carattere personale che rivelano origini razziali o etniche, opinioni politiche, credi religiosi o altri, salute mentale e fisica, o vita sessuale", possa essere consentito solo a condizione che siano previste dalla legge idonee garanzie.

33. Gli Stati dovrebbero garantire che siano messe a disposizione dei bambini informazioni di facile accesso, utili, adatte ai bambini e alla loro età su strumenti, parametri di riservatezza e vie

e, dunque, il riconoscimento del diritto del minore ad essere informato ed esprimere la propria volontà (ad esempio, Legge 219/2017 sul consenso informato) fa emergere – considerata la differenza di approccio seguita – il diverso modo in cui gli ordinamenti danno seguito alla verifica della capacità evolutiva del minore.

Basti pensare alla previsione di cui all'art. L. 1111-4 del *Code de la santé publique* che stabilisce un'importante eccezione, affermando che il medico deve *systématiquement recherché s'il est apte à exprimer sa volonté et à participer à la décision*. La legge non fissa un'età precisa, spettando al medico valutare la *capacité de jugement* del minore nel comprendere l'informazione fornita e le implicazioni della decisione medica[37]. In Germania, l'intervento dello *Jugendamt* – che è mera autorità amministrativa con funzioni di assistenza, consulenza e protezione e opera in via preventiva e di supporto – è invece decisamente più pervasivo. Quella gestione del conflitto che in Italia (L. 219/2017) va nella direzione di tenere "conto della volontà della persona minore, in relazione alla sua età e al suo grado di maturità" (art. 3, comma 1) e di "sentire l'interdetto ove possibile" e che, dunque, sostanzialmente assegna al giudice tutelare un ruolo determinante, focalizzandosi sul migliore interesse e sulla dignità della persona, in particolare in ambito sanitario – qui trova invece sponda in un potere di intervento diretto che supera il consenso dei genitori in situazioni di *Kindeswohlgefährdung*.

Ma v'è dell'altro. E questo altro attiene al diritto – pure riconosciuto al minore – di evitare indebite invasioni nella sua *privacy*. In questo senso, se è vero che il genitore o l'esercente le responsabilità genitoriale è investito del potere di rappresentanza è anche vero che in certi casi (e penso ai dati relativi a interruzione volontaria di gravidanza, alle dipendenze, o alla possibilità di test volti ad accertare la salute sessuale, ai disturbi mentali), l'accesso da parte dei genitori potrebbe compromettere la fiducia del minore nel sistema sanitario[38].

---

di ricorso. I bambini e/o i loro genitori o assistenti o rappresentanti legali dovrebbero essere informati da un controllore dei dati sul modo in cui vengono trattati i loro dati personali. Queste informazioni dovrebbero indicare, per esempio, come vengono raccolti, immagazzinati, usati e diffusi i dati, precisare i loro diritti di accedere ai propri dati, di rettificarli o cancellarli od opporsi al loro trattamento, e come esercitare questi diritti.

34. Gli Stati dovrebbero garantire che i bambini e/o i loro genitori, assistenti o rappresentanti legali abbiano il diritto di ritirare il loro consenso al trattamento dei propri dati a carattere personale, abbiano accesso ai propri dati personali e possano farli rettificare o cancellare, soprattutto quando il trattamento sia illegale o quando compromette la loro dignità, sicurezza o privacy".

[37] In Italia è noto che quello dei 12 anni di cui alla Legge 219/2017 non un limite rigido, ma un'età che viene spesso richiamata in dottrina e giurisprudenza italiana come "indicatore presuntivo" di maturità, per tutti. Si veda in proposito la posizione del Comitato di bioetica, "Informazione e consenso all'atto medico", in *http://bioetica.governo.it/media/170114/p10_1992_informazione-econsenso_abs_it.pdf.*

[38] Irti, *L'uso delle "tecnologie mobili" applicate alla salute: riflessioni al confine tra la forza del progresso e la vulnerabilità del soggetto anziano*, cit., 441.

Esigenza di bilanciare responsabilità genitoriale, da un lato, e diritto alla riservatezza del minore, dall'altro, puntualmente intercettato, invece, dalla Sect. 6975 del *California Family Code* il quale consente ai minori di qualsiasi età di acconsentire ai test e al trattamento per malattie mentali, abuso di sostanze stupefacenti, malattie a trasmissione sessuale (MST/STI) e a tutti i trattamenti (eccezion fatta per aborto e sterilizzazione) per la *prevention or treatment of pregnancy*. Dal canto suo, il principio che guida l'*Health and Safety Code* (HSC), e disciplina l'accesso ai dati sanitari, istituisce una sorta di simmetria fra consenso al trattamento e consenso all'accesso. La "Minor Consent Laws" o "Mature Minor Doctrine" è in tal senso chiara: chi ha il diritto di dare il consenso per un servizio, ha anche il diritto di controllare l'accesso ai registri relativi a quel servizio.

In questa direzione la Section 123115 (a)(1) del HSC è nel senso che "*The representative of a minor shall not be entitled to inspect or obtain copies of the minor's patient record* (...). *(1) With respect to which the minor has a right of inspection under Sect. 123110*". Di siffatta *"reasonable expectation of privacy"* non a caso è traccia in American Academy of Pediatrics v. Lungren (1997) e trova altresì conferma in una implementazione delle politiche sanitarie sui portali elettronici per i pazienti che va nella direzione di disattivare il *proxy access* (attraverso il portale MyChart, sviluppato dalla società statunitense Epic Systems)[39]. Tanto, senza considerare l'ulteriore facoltà concessa al fornitore di servizi sanitari di negare l'accesso ai registri (anche se il minore non ha dato il consenso per il trattamento in questione) ove ritenga che l'accesso del genitore possa avere un "effetto dannoso" sulla relazione professionale con il minore o sul "benessere fisico o psicologico" del minore stesso.

Il principio, in sintesi, è chiaro e condivisibile, atteso che se il minore può dare il consenso per un servizio (come quelli di salute riproduttiva o salute mentale), il genitore/tutore non può avere automaticamente diritto di accesso a quei registri senza l'autorizzazione del minore. Il che val quanto riconoscere al fornitore di servizi medici, anche al di fuori delle cure riservate, un potere discrezionale per proteggere il minore da un potenziale danno derivante dalla divulgazione delle informazioni che lo riguardano.

Alla luce di quanto si è venuto allineando, appare chiaro allora come la sfida non sia se consentire il *proxy service* (che è un obbligo dell'EHDS), ma come integrarlo nel sistema giuridico e tecnico in modo da massimizzare la cura (uso primario dei dati) garantendo al contempo il diritto alla *privacy* e all'autodeterminazione del paziente.

[39] American Academy of Pediatrics v. Lungren, 16 Cal.4th 307 in relazione ad una vicenda in cui si discuteva se il consenso dei genitori all'aborto violasse il "constitutional right to privacy" (Calif. Const., art. I, section 1.).

5. Il conflitto fra autodeterminazione e accesso ai dati sanitari: l'esperienza americana

Di un altro aspetto della vulnerabilità vorrei dare atto: quella che, abbandonata la dimensione oggettiva, appare piuttosto l'espressione di una intersezionalità delle situazioni di vita che forse rende tutti noi vulnerabili.

In USA, in un panorama normativo articolato – che cade in un contesto privo di quella disciplina più ampia offerta dal GDPR e ora dal EHDR e dove il *focus* è sulla trasferibilità e la sicurezza dei dati nel sistema sanitario piuttosto che sulla tutela dei diritti fondamentali della persona – a definire i criteri per il trattamento dei dati sanitari concorrono non solo, come noto, *l'Health Insurance Portability and Accountability Act* del 1996 (HIPAA o Kennedy–Kassebaum Act) [40] ma, sebbene più *consumer orientend*, la disciplina del *California Protection Act* (CCPA).

Il sistema di *opt-out*[41]si presenta quale soluzione in grado di offrire ai consumatori la possibilità di rinunciare alla vendita e alla condivisione delle loro informazioni personali e di limitare l'uso di informazioni sensibili. Qui il collegamento *privacy*-dati personali è particolarmente evidente, alimentato come è dal fatto che – a differenza di quanto accade in EU – le *covered entities* possono usare le PHI (*Personal Health Information*) nel caso di trattamento, pagamento e operazioni sanitarie (TPO) senza l'autorizzazione esplicita del paziente (essendo il consenso implicito nel rapporto di cura)[42]. Su questo fronte, le evoluzioni più significative non provengono tanto da sentenze di *risarcimento danni* tradizionali, quanto da provvedimenti normativi (spesso contestati in tribunale) che cercano di affrontare le nuove vulnerabilità sociali[43].

La questione della protezione dei dati sanitari delle persone vulnerabili, invece, ha finito con l'investire due aree chiave: a) i servizi di salute riproduttiva e b) la condivisione di dati con le forze dell'ordine o per l'immigrazione. Gli sviluppi che hanno fatto seguito al caso Dobbs v. Jackson *Women's Health Organization* (2022)[44], sentenza che come noto ha

---

[40] Cfr., *https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html*.

[41] Per uno spunto critico sulla configurazione del diritto di *opt-out*, Ziaja, *The text and data mining opt-out in Article 4(3) CDSMD: Adequate veto right for rightholders or a suffocating blanket for European artificial intelligence innovations?*, in *Journal of Intellectual Property Law & Practice*, 19, 5, 2024, 453 ss.; Ottilia, *L'opt out commons nella nuova disciplina del data mining*, in *Giur. it.*, 1, 2022, 1253-1262.

[42] Si tratta di organismi (*covered entity*) giuridicamente tenuti a rispettare le norme sulla *privacy* e sulla sicurezza (*Protected Health Information* - PHI - *ex* 45 *Code of Federal Regulation* (CFR) § 160.103).

[43] Le violazioni, ove contestate, si chiudono di regola con un *Settlement Agreements*, utilizzato dall'OCR (*Office for Civil Rights*) per risolvere le violazioni di cui all'HIPAA e si accompagnano all'obbligo di adottare un Piano di Azione Correttiva (CAP). Per un'analisi della vicenda e dei motivi della sanzione, cfr., *https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html*.

[44] Cfr., *https://www.healthaffairs.org/content/forefront/biden-administration-finalizes-rule-*

rimosso il principio di *Roe vs Wade* (1973) e inciso sul riconoscimento del diritto all'aborto determinando un cambiamento radicale nell'assistenza sanitaria, sono significativi. La caduta del divieto decennale di legislazione anti-aborto – e la espansione delle cd *trigger laws* negli Stati conservatori – consente di perseguire le donne in cerca di cure riproduttive, in base alla loro impronta digitale. Il facile accesso ai dati sanitari rende fin troppo semplice l'applicazione della norma.

In *Purl v. U.S. Department of Health and Human Services* (2025), i giudici del Texas hanno sfidato la *Final Rule* del 26 aprile 2024 con la quale l'*Office for Civil Rights* (OCR) del Dipartimento della Salute e dei Servizi Umani degli Stati Uniti (HHS) tentava di rafforzare la tutela della *privacy* delle persone che accedono e forniscono assistenza sanitaria riproduttiva, allo scopo di creare il giusto equilibrio tra la protezione delle informazioni sanitarie sensibili e la possibilità di utilizzare tali informazioni per scopi pubblici e privati. La norma, che modificava gli *standard* per la *privacy* delle informazioni sanitarie identificabili individualmente ai sensi dell'HIPAA e dell'*Health Information Technology for Economic and Clinical Health Act* (HITECH Act)[45], aggiunge l'assistenza sanitaria riproduttiva all'elenco dei servizi sanitari che beneficiano di una maggiore tutela federale della privacy[46]. La reazione non si è fatta attendere.

Il giudice federale, infatti, ha *vacated* la Regola sulla Privacy dell'HIPAA del 2024 per la salute riproduttiva a livello nazionale ritenendo che, in questo modo, si finirebbe per ostacolare il normale corso della giustizia all'interno dei singoli Stati[47].

---

support-reproductive-health-care-privacy?utm_medium=social&utm_source=linkedin&utm_campaign=forefront.

[45] Prima dell'intervento federale del 2009, l'impiego di sistemi di *Electronic Health Records* negli Stati Uniti era residuale: soltanto una quota modesta delle strutture ospedaliere – stimata attorno al dieci per cento – disponeva di un'infrastruttura digitale in grado di sostituire la documentazione clinica cartacea. Tale ritardo non era espressione di inerzia organizzativa, bensì riflesso dei costi elevati richiesti per l'adozione delle tecnologie informatiche e delle persistenti incertezze circa l'affidabilità e la protezione dei flussi informativi. Con l'approvazione dell'*Health Information Technology for Economic and Clinical Health Act*, nel 2009, il legislatore federale ha profondamente modificato questo scenario, prevedendo un articolato sistema di incentivi volto a favorire la transizione verso gli EHR e a promuovere modelli assistenziali fondati su interoperabilità, continuità delle cure e condivisione sicura delle informazioni tra i soggetti regolati dall'HIPAA. Il *HITECH Act* ha inciso anche sul piano della *compliance*: pur senza alterare l'impianto della normativa HIPAA, ne ha rafforzato l'efficacia applicativa, introducendo nuovi obblighi in materia di sicurezza e – per la prima volta a livello federale – un regime di notifica obbligatoria delle violazioni dei dati sanitari, che ha permesso all'*Office for Civil Rights* di intensificare l'attività di vigilanza e di responsabilizzare in modo più marcato gli operatori sanitari.

[46] HIPAA Privacy Rule to Support Reproductive Health Care Privacy at 89 Federal Register 32976 (April 26, 2024), in *https://www.healthaffairs.org/content/forefront/texas-challenges-federal-privacy-protections-reproductive-health-care.*

[47] In particolare i giudici hanno osservato che la *Final Rule* "*impermissibly redefines 'person' and 'public health' in contravention of federal law and in excess of statutory authority*", precisando ancora che l'"*HHS regulations cannot preempt a contrary state law with more stringent health-information*

Si assiste insomma ad un uso strumentale delle informazioni sanitarie adoperate per perseguire obiettivi sostanzialmente politici in danno di categorie di soggetti vulnerabili. Così in State of California v. U.S. Department of Health and Human Services (2025) limitatamente all'accesso e trasmissione al Dipartimento della Sicurezza Nazionale (DHS) che sovrintende all'applicazione delle leggi sull'immigrazione (ICE), di dati sanitari relativi alla popolazione immigrata al fine di impedire ai non cittadini di ricevere i benefici *Medicaid*. La controversia non è stata ancora decisa ma il *claim* indica la necessità di approdare ad un equilibrio fra "*the government's legitimate need to obtain and manage personal information and the privacy rights we each hold*"[48]. Laddove, neppure tanto sullo sfondo, giace il timore che siffatta circolazione di informazioni sulla salute possa dissuadere il pubblico dal cercare assistenza medica e oscurare il diritto a comprendere e analizzare come vengono utilizzati i propri dati personali.

Che è poi quanto hanno riconosciuto, sia pur indirettamente, i giudici in *Doctors for America et al. v. Office of Personnel Management* allorché, facendo seguito ad un ordine esecutivo presidenziale, è stata ordinata la rimozione da alcuni siti *web* di tutta una serie di dati relativi alla salute, sì da rendere particolarmente impegnativa la ricerca di informazioni da parte del medico[49]. Le pagine rimosse erano relative a ricerche, studi epidemiologici, analisi dei fattori rischio in talune fasce della popolazione, quali adolescenti, soggetti in età scolare, persone vulnerabili o informazioni sui danni provocati da ambienti insalubri, HIV, contraccezione, salute riproduttiva ovvero relative all'esecuzione di trials che prevedessero l'inclusione di donne e *underrepresented populations*. Tra le righe di una motivazione ampia e articolata che, a profili procedurali affianca riflessioni sostanziali relative al danno arrecato agli stessi medici costretti ad un'attività di reperimento delle informazioni lunga e faticosa, si coglie la preoccupazione dei giudici di evitare discriminazioni in danno di "*underprivileged Americans, seeking healthcare*". Per i giudici la difficoltà di offrire cure in tempi adeguati apre al rischio "*that some individuals will not receive treatment, including for severe, life-threatening conditions. The public thus has a strong interest in avoiding these serious injuries to the public health*". Tanto, con l'av-

---

protection requirements" così in Purl, M.D. et al v. United States Department of Health and Human Services et al, No. 2:2024cv00228 - Document 34 (N.D. Tex. 2024).

[48] State of California v. U.S. Department of Health and Human Services, 3:25-cv-05536, (N.D. Cal.).

[49] Si tratta della "Initial Guidance Regarding President Trump's Executive Order Defending Women" - Memorandum from Charles Ezell, Acting Dir., OPM to the Heads & Acting Heads of Dept's & Agencies (29 gennaio 2025), in *https://www.opm.gov/media/yvlh1r3i/opm-memo-initial-guidance-regarding-trump-executive-order-defending-women-1-29-2025-final.pdf* con il quale è stato emanato l'ordine "to take down all outward facing media (websites, social media accounts, etc.) that inculcate or promote gender ideology," "[w]ithdraw any final or pending documents, directives, orders, regulations, materials, forms, communications, statements, and plans that inculcate or promote gender ideology," and "[e]nsure that all applicable agency policies and documents, including forms, use the term 'sex' and not 'gender'" (Par. 1–2).

vertenza ulteriore che rendere inaccessibili al pubblico informazioni sanitarie critiche danneggia la salute pubblica e mette a repentaglio la diagnosi e la cura delle malattie[50].

Negli Stati Uniti, in materia di dati sanitari e persone vulnerabili, la tensione tra il diritto alla riservatezza (regolato dall'HIPAA) e le politiche statali o federali che cercano di accedere o limitare la condivisione di dati sensibili per finalità di applicazione della legge, appare di complessa soluzione con un impatto diretto sulle comunità di immigrati o su quanti cercano assistenza sanitaria riproduttiva.

Per il resto, l'HIPAA[51] (*Health Insurance Portability and Accountability Act* del 1996) – come noto – non ha disposizioni specifiche per i dati raccolti al di fuori del settore sanitario. Il che vuol dire che le aziende sono libere di fare più o meno quello che vogliono con questi dati, a meno che la legislazione statale non lo vieti, (il che crea non pochi problemi in rapporto ai dati raccolti attraverso *app* per il *fitness*, *tracker, social media*[52]), creando una "zona grigia" di vulnerabilità, con tutto ciò che ne consegue in termini di *privacy*.

---

[50] Doctors For America v. Office of Personnel Management (11 febbraio 2025) United States District Court, District of Columbia, Civil Action No. 25-322 (JDB).

[51] Le PHI (*Protected health information*), alla luce dell'esigenza di tutela della riservatezza e della definizione di standard nazionali, trovano nell'HIPAA una prima regolamentazione. In discussione è l'uso delle informazioni da parte delle *Covered Entities* (i fornitori di assistenza quali medici, ospedali e compagnie di assicurazione) e dei loro *Business Associates* i quali, per contro, si occupano di servizi di fatturazione, consulenti legali, o fornitori di servizi cloud che trattano PHI). La normativa HIPAA vieta la divulgazione di informazioni sanitarie identificabili individualmente (PHI), senza il consenso del paziente (o del tutore o di altra persona responsabile), fatta eccezione per tre finalità: trattamento, pagamento o operazioni sanitarie. L'HIPAA si applica direttamente alle "entità coperte", definite come pagatori, fornitori e centri di compensazione dell'assistenza sanitaria. Dal canto suo, il più recente intervento del 2009 (*Health Information Technology for Economic and Clinical Health Act* (HITECH) a valle dell'*American Recovery and Reinvestment Act* – ARRA) estende l'applicazione delle regole in tema di sicurezza delle informazioni e *privacy* anche ai cd *Business Assiociated*, cfr., HITECH Act of 2009, 42 USC sec 139w-4(0)(2) (February 2009), subtitle D, part 1, sec 13401: *Application of security provisions and penalties to business associates of covered entities; annual guidance on security provisions.*

[52] Sul tema del tracciamento digitale e dell'uso di dati provenienti da applicazioni mobili e dispositivi intelligenti, numerosi contributi hanno messo in luce come l'esperienza pandemica abbia accelerato processi già in atto, evidenziando tanto le potenzialità quanto le criticità dei sistemi di raccolta automatizzata dei dati. In particolare, si è osservato come l'impiego di *app* e strumenti interoperabili per il *contact tracing* durante l'emergenza da SARS-CoV-2 abbia mostrato la capacità dei flussi informativi digitali di incidere sulle strategie di tutela della salute pubblica, rivelando al contempo la complessità dei relativi assetti tecnici e regolatori. Così, C. Perlingieri, *Coronavirus e tracciamento tecnologico: alcune riflessioni sull'applicazione e sui relativi sistemi di interoperabilità dei dispositivi*, in *Actual jur. iberoam.*, 2020, 12-*bis*, 836 ss. In direzione convergente, Zeno-Zencovich, *I limiti delle discussioni sulle "app" di tracciamento anti-Covid e il futuro della medicina digitale*, in *MediaLaws*, 26 maggio 2020; Corso, L*o spazio europeo dei dati sanitari. prime riflessioni sul regolamento UE 2025/327*, cit., 567.

Tanto senza considerare le possibilità di un uso secondario dei dati permesso sulla base di "deroghe" o di autorizzazioni concesse da un comitato etico (IRB), o attraverso l'uso di dati de-identificati.

Quali, all'esito di queste riflessioni, il necessario epilogo?

Nel maggio del 2017, un ormai celebre articolo di "The Economist" apriva la riflessione sulla "quarta rivoluzione industriale" con la frase di Clive Humby, matematico inglese che acutamente aveva posto l'accento sul fatto che *"Data is the new oil".* La convoluzione di mondo fisico e mondo digitale (quel "Umschlag von Quantität in Qualität" da cui si è preso le mosse) impone la creazione di un ecosistema digitale sicuro, interoperabile e trasparente. La condivisione dei dati è una realtà ma deve verificarsi nel pieno rispetto della *privacy* e dei diritti della persona.

Se si mette da parte l'esperienza americana, percorsa da ben altre vibrazioni, l'ambiziosa idea del regolatore europeo è quella di realizzare un mercato accessibile dei dati sanitari nel rispetto della dignità della persona (anche vulnerabile), creando al tempo stesso i presupposti per un "virtuoso" operare di strategie competitive. Che quello dei dati sanitari sia un mercato in forte espansione dove gli interessi delle grandi aziende farmaceutiche e degli istituti di ricerca tendono ad esitare in scontri competitivi è evidente. Così come evidente è il fatto che la competitività dipende, in questo ambito più che mai, dalla quantità di informazioni che si possiede.

La circostanza che la velocità di aggregazione dei dati e la quantità degli stessi imprima una forte accelerazione alle scoperte scientifiche e, dunque, sia funzionale al perseguimento di interessi di rilevanza pubblicistica, quale sicuramente è la salute, non cambia il discorso. Si tratta solo di capire, infatti, come addivenire a quel giusto equilibrio fra *privacy* ed innovazione che, liberandosi da logiche proprietarie, sorregga (per fini di tutela della salute o esigenze di ricerca) la circolazione dei dati.

In questo senso la vera sfida sembra destinata a giocarsi (almeno in Europa) sul terreno della razionalizzazione e coordinamento di un *frame* normativo tutt'altro che omogeneo. Aspetto, quest'ultimo, non adeguatamente ponderato da un legislatore che si è entusiasticamente incamminato sulla strada della rimozione, per dir così, "esterna" delle barriere nell'uso dei dati sanitari, senza ragionare, o meglio, rimuovere quelle "interne".

Il problema, in punto di disabilità, non è solo rappresentato dalla necessità di procedere ad un adattamento dei singoli sistemi sanitari nazionali che sia in grado di assicurare un accesso ai dati sanitari di riuso secondario e primario[53] senza creare di-

[53] Dove, Jiahong Chen, *Should consent for data processing be privileged in health research? A comparative legal analysis*, in *International Data Privacy Law*, 10, 2, 2020, 118 ss. L'art. 51 del Reg. (UE) 2025/327 individua in modo puntuale le categorie di dati sanitari elettronici che i titolari sono tenuti a mettere a disposizione per finalità di uso secondario, con l'obiettivo di garantire interoperabilità, qualità informativa e supporto alla ricerca scientifica nel rispetto dei diritti fondamentali dell'interessato. Per un'analisi sistematica della disciplina, con riguardo sia all'uso primario sia all'uso secondario dei dati sanitari, si veda Iaselli, *Le nuove regole per l'uso primario e secondario dei dati sanitari. Reg. UE 11 febbraio 2025, n. 327 (EHDS)*, Santarcangelo di Romagna (RN), 2025, 71 ss., spec. 73.

seguaglianze economiche e sociali, ma anche dalla necessità di procedere ad una armonizzazione dei sistemi giuridici di protezione. Il che rinvia ad altra considerazione che attinge al certo non nuovo dibattito sulla funzione del diritto in un'epoca nella quale l'uso del dato è condizionato dagli interessi dell'industria e dalle scienze informatiche.

Si tratta di riconsiderare il ruolo dell'azione regolativa onde evitare le derive di una "normatività digitale" che, solo in apparenza crea le condizioni per un potenziamento del controllo e la *governance* dei contenuti[54]. Il rischio, a rimanere inerti, è quello di legittimare – di là dalle buone intenzioni – una *governance* privata dei contenuti, lasciando che la discrezionalità tecnica della piattaforma si faccia perno della normazione. Tanto con buona pace di ogni discorso sulla vulnerabilità.

[54] Zuboff, *Il capitalismo della sorveglianza: Il futuro dell'umanità nell'era dei nuovi poteri*, Roma; Maestri, Manfré, *Norme e codici. La regolazione digitale tra architetture tecniche e soggettività fragili*, in *Sociologia del Diritto*, 52, 2, 2025, *passim.*