

ERMANNO CALZOLAIO

IL REGOLAMENTO SULLO SPAZIO DEI DATI SANITARI NELLA PROSPETTIVA DELLA CITTADINANZA EUROPEA

SOMMARIO: 1. Premessa. — 2. L'uso primario dei dati sanitari. — 3. La portabilità dei dati sanitari per l'uso primario. — 4. L'uso secondario dei dati sanitari. — 5. Anonimizzazione e pseudonimizzazione dei dati per l'uso secondario. — 6. Le sanzioni e il risarcimento del danno. — 7. L'entrata in vigore del Regolamento. — 8. La base giuridica del Regolamento. Riflessioni in prospettiva per un più solido fondamento della tutela del paziente/cittadino europeo.

1. PREMESSA.

Con l'approvazione del Regolamento sullo Spazio Europeo dei Dati Sanitari (European Health Data Space - EHDS) ¹, entrato in vigore nel mese di marzo 2025, si aggiunge un ulteriore tassello nella realizzazione della strategia europea per i dati, promossa dalla Commissione Europea a partire dal febbraio 2020 con l'obiettivo di costruire un mercato unico dei dati attraverso la creazione di spazi comuni europei in una serie di settori strategici, tra cui sanità, pubblica amministrazione, agricoltura, industria manifatturiera, energia, mobilità, finanza ². La cornice di riferimento per la creazione di questi 'spazi' è costituita dal cd. Data Act ³ e il primo a vedere la luce è appunto quello relativo ai dati sanitari.

¹ Il presente lavoro si inserisce nella ricerca finanziata dall'Unione Europea (NextGenerationEU Ministero Italiano dell'Università e della Ricerca - MUR) National Innovation Ecosystem grant ECS00000041 - VITALITY - CUP E13C22001060006. I punti di vista e le opinioni espresse sono dell'autore e non riflettono necessariamente quelli dell'Unione europea o della Commissione europea. Né l'Unione europea né la Commissione europea possono essere ritenute responsabili per essi.

Regolamento (UE) 2025/327 dell'11 febbraio 2025 sullo spazio europeo dei dati sanitari e che modifica la direttiva 2011/

24/UE e il regolamento (UE) 2024/2847, in GUCE, L, 5 marzo 2025, riprodotto in questo fascicolo, *infra*, p. 557.

² Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e sociale europeo e al Comitato delle Regioni. Una strategia europea per i dati (2020) COM(2020) 66 final, disponibile al link <https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52020DC0066>.

³ Regolamento (UE) 2023/2854 del 13 dicembre 2023, riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il regolamento (UE) 2017/2394 e la direttiva (UE) 2020/1828 (re-

La relativa proposta della Commissione risale al maggio 2022, all'indomani della grave crisi pandemica Covid-19, che ha evidenziato in modo drammatico le profonde differenze dei sistemi sanitari degli Stati membri e la difficoltà di condivisione di dati all'interno dell'UE. Studi approfonditi hanno consentito di verificare che il 97% dei dati acquisiti o generati negli ospedali rimangono completamente inutilizzati, ostacolando la ricerca medica e farmacologica, nonché la possibilità di reagire in tempi rapidi di fronte alle emergenze ⁴. Inoltre, l'assenza di un quadro comune per la loro acquisizione e gestione all'interno dell'Unione limita la cura dei pazienti, ad esempio quando si tratta di prestare assistenza in strutture di altri paesi, perché l'impossibilità di accedere ai dati clinici in modo immediato e agevole rende difficile l'adozione di decisioni informate, con il rischio di errori diagnostici e terapeutici.

Il Regolamento Generale sulla Protezione dei Dati (GDPR) ⁵, entrato in vigore nel 2018, si applica anche ai dati sanitari, che costituiscono forse la categoria più rilevante di dati personali. Tuttavia, esso prevede requisiti rigorosi per il loro trattamento, imponendo alle organizzazioni sanitarie di adottare misure di sicurezza avanzate e di garantire il rispetto dei diritti in materia di *privacy*. In particolare, il trattamento è assoggettato ad un regime di tutela rafforzato, in quanto l'art. 9 lo subordina al consenso esplicito dell'interessato, a meno che non sussistano motivi di interesse pubblico nel settore della salute o non sia necessario garantire la sicurezza del paziente e la continuità delle cure ⁶. Pur ponendosi in continuità con il GDPR, il Regolamento in esame introduce varie novità.

La creazione di uno Spazio Europeo dei Dati Sanitari si prefigge lo scopo di superare le barriere che limitano la condivisione e l'uso efficace delle informazioni sanitarie nei diversi Stati membri e di rafforzare i diritti dei pazienti in relazione ai loro dati elettronici sanitari, rendendo anche possibile l'accesso agli stessi a fini di ricerca, di innovazione e di politiche sanitarie. L'impianto del Regolamento contempla due possibilità di utilizzazione

golamento sui dati), in GU L, 22 dicembre 2023; cfr. E. CALZOLAIO, *From data property to data access and back again? Comparative remarks on the EU Data Act*, in lceonline (www.lceonline.eu), 1/2024, I/Saggi e contributi, p. 43 ss.

⁴ J. MOORE-Y. DIAS GUICHOT, *How to harness the power of health data to improve patient outcomes*, World Economic Forum (5 January 2024), disponibile al link <<https://www.weforum.org/agenda/2024/01/how-to-harness-health-data-to-improve-patient-outcomes-wef24/>>

⁵ Regolamento (UE) 2016/679 del 27

aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

⁶ Sulle potenzialità del GDPR in tema di trattamento dei dati ai fini della ricerca, cfr. G. COMANDÉ-G. SCHNEIDER, *Differential Data Protection Regimes in Data-Driven Research: Why the GDPR is More Research-Friendly Than You Think*, in *German Law Journal*, 2022, pp. 559 ss.

dei dati sanitari elettronici: l'uso primario riguarda il trattamento dei dati per i pazienti a fini di cura, per assicurare un accesso tempestivo ai loro dati sanitari elettronici; l'uso secondario concerne invece il trattamento dei dati da parte di ricercatori e soggetti economici pubblici e privati per scopi di interesse generale, come l'educazione o l'istruzione, la ricerca scientifica, lo sviluppo e l'innovazione.

Sono molteplici i profili che attirano l'attenzione rispetto a questa nuova iniziativa europea. Anzitutto, essa investe il settore particolarmente delicato dei dati sanitari ed è destinata ad avere un impatto rilevante, agevolandone la diffusione e il trattamento. In secondo luogo, la sua portata va ben al di là della disciplina dei dati in sé considerati, giacché incide anche su aspetti organizzativi e di gestione del paziente, imprimendo un nuovo volto al rapporto con gli operatori e le strutture sanitarie, che dovranno in qualche modo ripensare il modo con cui si relazionano con i pazienti e ne acquisiscono i dati. In terzo luogo, le nuove regole sono suscettibili di investire il settore della ricerca scientifica, che al momento attuale si muove in un contesto caratterizzato da regole contraddittorie e frammentate a livello nazionale, rendendo difficile l'acquisizione di dati sanitari. In quarto luogo, il Regolamento conferma che la disciplina dei dati è un terreno scivoloso, non solo per l'esigenza di conciliare l'utilità di un accesso e di un trattamento più agevoli con la necessità di tutelare i diritti dei singoli, ma anche per la difficoltà di trovare un solido inquadramento giuridico di un 'bene' tanto rilevante quanto sfuggente⁷. Da questo punto di vista, resta irrisolto il nodo della qualificazione dei dati, che per un verso sono considerati come 'bene' accessibile e, per altro verso, sembrano rimanere nella sfera giuridica esclusiva del loro titolare, che può impedirne la raccolta e l'uso. Vi è poi un ultimo motivo di interesse che preme porre in evidenza. Il legislatore europeo lascia ampi spazi agli Stati membri rispetto ad alcuni aspetti rilevanti che, come si vedrà, possono compromettere, se non addirittura vanificare, il tentativo di realizzare un autentico spazio europeo dei dati sanitari. Ciò significa che, lungi dal costituire un punto di arrivo, il Regolamento è piuttosto un punto di partenza, che apre una sfida che potrà essere (o *non*) raccolta.

Nelle pagine che seguono si intende fornire una prima lettura dei suoi principali contenuti, concentrandosi sull'uso primario (par. 2 e 3), sull'uso secondario (par. 4 e 5), sulle sanzioni e il risarcimento del danno (par. 6) e sull'entrata in vigore (par. 7), per poi allargare lo sguardo ad alcune considerazioni sulla base

⁷ Cfr. K. LIDDELL-D.A. SIMON-A. LUCASEN, *Patient data ownership: who owns your*

health?, in *Journal of Law and the Bio-sciences*, 2021, pp. 1 ss.

giuridica individuata dal legislatore europeo per superare l'ostacolo costituito dalle limitate competenze dell'Unione nella materia sanitaria. Ci si chiede, in particolare, se queste basi siano adeguate al fine di realizzare una autentica armonizzazione, superando le resistenze a livello nazionale. La dottrina giuridica e, in particolare, i giuristi sensibili ad un approccio comparatistico sono chiamati in causa per contribuire a fornire chiavi di lettura e ipotesi di lavoro che consentano di non disperdere il potenziale racchiuso nell'iniziativa europea.

2. L'USO PRIMARIO DEI DATI SANITARI.

Le disposizioni relative all'uso primario, contenute nel capo II, mirano a garantire ai pazienti un accesso rapido e gratuito ai propri dati sanitari elettronici, la loro agevole condivisione con gli operatori sanitari, anche oltre frontiera, nonché la possibilità di aggiungere informazioni personali sulla salute, di limitare l'accesso a parti specifiche della cartella clinica o a determinate persone, di visualizzare chi ha avuto accesso ai propri dati, di chiedere la correzione di errori riscontrati, nonché il diritto a visualizzare i dati sanitari in un formato europeo standard ⁸. Dal canto loro, gli operatori sanitari potranno avere un rapido accesso alle cartelle cliniche, avendo a disposizione anche dati acquisiti in altri paesi.

Già con la Direttiva 2011/24 EU sull'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera si prevedeva l'obbligo dell'Unione di sostenere e facilitare la cooperazione e lo scambio di informazioni tra stati membri, nel contesto di una rete volontaria tra le autorità responsabili. Tuttavia, è proprio l'approccio su base volontaria ad essersi rivelato poco fruttuoso, stante l'adesione di un numero limitato di Stati, tanto da spingere la Commissione ad emanare una raccomandazione in cui sottolineava le difficoltà derivanti dall'incompatibilità dei sistemi informatici usati in campo sanitario all'interno dell'Unione ⁹.

Il Regolamento realizza quindi un cambio di passo sostanziale, rendendo obbligatoria l'istituzione di una piattaforma per la salute digitale, che fornisce servizi per facilitare lo scambio di dati personali sanitari tra punti di contatto per la salute digitale che ogni Stato membro dovrà identificare.

Prima di analizzare più nel dettaglio il contenuto dei diritti e degli obblighi connessi all'uso primario, è bene concentrarsi brevemente sulla definizione di "dati sanitari elettronici". Essi si

⁸ Per un quadro generale sui contenuti del Regolamento, cfr. M. IASELLI, *Le nuove regole per l'uso primario e secondario dei dati sanitari*, Rimini, 2025.

⁹ Raccomandazione (EU) 2019/243 del 6 febbraio 2019.

articolano in dati personali e non personali. I dati personali sono quelli “relativi alla salute e i dati genetici che sono trattati in formato elettronico” (art. 2.2 lett. *a*), mentre quelli non personali vengono definiti come “i dati sanitari elettronici diversi dai dati sanitari elettronici personali, compresi sia quelli che sono stati anonimizzati in modo da non riferirsi più a una persona fisica identificata o identificabile (« interessato »), sia quelli che non si sono mai riferiti a una specifica persona (art. 2.2 lett. *b*).

L’art. 3 prevede che le persone fisiche possono accedere ai dati sanitari elettronici personali, scaricando gratuitamente una copia elettronica, nel formato europeo di scambio delle cartelle cliniche elettroniche. Gli Stati membri possono introdurre però delle limitazioni, ove necessarie per la tutela della persona fisica, tenendo conto della sicurezza del paziente e sulla base di considerazioni etiche, ritardando temporaneamente l’accesso fino a quando un professionista sanitario non sia in grado di comunicare e spiegare adeguatamente alla persona fisica interessata informazioni che possono avere un impatto significativo sulla sua salute.

Il Regolamento non impone l’obbligo di registrare (e consentire l’accesso *a*) tutti i tipi di dati, ma prevede alcune categorie prioritarie, elencate nell’art. 14(1). Si tratta dei profili sanitari sintetici dei pazienti, delle prescrizioni elettroniche, delle dispensazioni elettroniche, degli esami diagnostici per immagini e relativi referti di immagini, dei risultati degli esami medici (compresi i risultati di laboratorio e altri risultati diagnostici e relativi referti), nonché delle lettere di dimissione. Gli Stati membri possono prevedere l’accesso e lo scambio di ulteriori dati in base a disposizioni introdotte a livello nazionale, con il conseguente rischio di frammentazione della disciplina a seconda del paese in cui vengono raccolti i dati.

Come si è già accennato, il sistema fa perno su una piattaforma centrale di interoperabilità, denominata ‘LaMiaSalute@UE’ (*MyHealth@EU*), che fornisce servizi volti a favorire e agevolare lo scambio di dati sanitari elettronici personali tra i punti di contatto nazionali. La Commissione è tenuta a stabilire, entro il 26 marzo 2027, le specifiche tecniche relative alle categorie prioritarie di dati sanitari elettronici sanitari e il formato europeo di scambio delle cartelle cliniche. ● Ogni Stato membro è invece tenuto a designare una o più autorità di sanità digitale, il cui compito è di assicurare l’attuazione a livello nazionale delle direttive impartite dalla Commissione. I dati relativi alle categorie prioritarie devono essere inseriti in conformità al formato europeo che, in base all’art. 15(1) deve essere di uso comune, leggibile da un dispositivo automatico e tale da consentire la trasmissione di dati sanitari elettronici personali tra applicazioni software, dispositivi e prestatori di assistenza sanitaria diversi.

Una ulteriore significativa previsione del Regolamento è quella relativa alla possibilità per pazienti stessi di inserire direttamente

dati sanitari, che nella proposta era invece rimessa alla decisione dei singoli Stati membri. L'art. 5 precisa che queste informazioni devono essere chiaramente distinguibili rispetto a quelle inserite dagli operatori sanitari, che in nessun caso il paziente può modificare. La ragione è chiarita nel considerando n. 12, ove si pone in evidenza che le informazioni inserite dal paziente non possono assumere lo stesso valore di quelle inserite dagli operatori sanitari. È invece rimesso alla decisione degli Stati membri di stabilire se le informazioni inserite dal paziente possono essere rettificare o comunque modificate dagli operatori sanitari.

Tra i diritti attribuiti al paziente vi è anche quello di limitare l'accesso dei professionisti sanitari e dei prestatori di assistenza sanitaria alla totalità o a parte dei loro dati sanitari elettronici personali, senza che il limite sia visibile dal prestatore di assistenza sanitaria (art. 8). Inoltre, il paziente ha diritto di ottenere informazioni su chi ha avuto accesso ai propri dati.

Queste norme consentono quindi al paziente di controllare l'accesso e proteggere il diritto alla riservatezza della vita privata, che costituisce uno dei profili più delicati del sistema delineato dal Regolamento, dovendosi ricercare un bilanciamento tra le esigenze di tutela della salute (che si intende perseguire facilitando la registrazione e l'accesso ai dati) e il diritto di autodeterminazione del paziente, che potrebbe essere compromesso dal meccanismo obbligatorio di inclusione nella piattaforma.

A tale riguardo, nella proposta si prevedeva che i pazienti potessero restringere l'accesso ai loro dati, ma non rifiutarsi di essere inseriti nel sistema. Il testo finale consente invece agli Stati membri di prevedere il diritto di escludere l'accesso ai dati sanitari elettronici personali. In tal caso, devono essere stabilite adeguate discipline che consentano ai professionisti sanitari di accedere comunque ai dati in presenza di un trattamento necessario per tutelare gli interessi vitali del paziente anche nel caso in cui eserciti il diritto di esclusione (art. 10). Questa soluzione di compromesso si è rivelata necessaria per raggiungere un accordo, ma certamente crea il rischio di una seria frammentazione tra le discipline nazionali ed è suscettibile di pregiudicare la portata innovativa del Regolamento, laddove gli Stati si indirizzeranno nel senso di prevedere un *opt-out*.

D'altro canto, nel corso dell'*iter* che ha condotto al testo definitivo è emerso il timore che la scelta di un sistema obbligatorio di registrazione e di accesso ai dati sanitari potesse condurre ad una vera e propria dipendenza dai sistemi informatici, con effetti negativi per la stessa sicurezza dei pazienti¹⁰. In proposito, vi sono esempi che dimostrano la delicatezza del problema, stante quanto accaduto in Danimarca, ove sono state somministrate dosi errate di farmaci per questioni tecniche del software utilizzato, cagionando gravi danni ed in alcuni casi la morte degli interes-

sati¹⁰. Per questa ragione, il Regolamento prevede in modo esplicito una adeguata formazione degli operatori del settore, ivi compresa l'assistenza nella fase di registrazione dei dati (art. 83). Un profilo critico è infine costituito dal problema linguistico, giacché i dati vanno inseriti nella lingua dell'operatore, per essere poi tradotti nella lingua del paese ove vengono utilizzati, con tutti i rischi che ciò può comportare.

3. LA PORTABILITÀ DEI DATI SANITARI PER L'USO PRIMARIO.

Il diritto alla portabilità dei dati si aggiunge al diritto di accesso e consiste nella possibilità per l'interessato di gestire i dati in modo attivo e di riutilizzarli (cd. 'riuso'), che può rivelarsi in concreto difficile o addirittura impossibile in presenza di ostacoli di natura tecnica che ostacolano la circolazione.

La portabilità costituisce una delle innovazioni più significative del GDPR, il cui art. 20 del GDPR prevede che "l'interessato ha diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento". Nel sistema delineato dal GDPR, tuttavia, l'ambito di applicazione del diritto alla portabilità è circoscritto ai dati « forniti » dall'interessato al titolare del trattamento e che questo tratta sulla base del consenso o dell'esecuzione di un contratto, ricorrendo a mezzi automatizzati. Restano quindi esclusi i cd. dati inferenziali (*inferred data*), cioè quelli che il titolare del trattamento elabora sulla base dei dati grezzi forniti dall'interessato¹¹. Il GDPR accoglie una soluzione di compromesso, adottata al duplice scopo di limitare i rischi per il titolare del trattamento quando le informazioni deducibili dai dati personali trasmessi siano tali da recare vantaggi competitivi ai concorrenti e di tutelare la riser-

¹⁰ Cfr. K. O' CATHAOIR, *The EHDS and Electronic Health Records. GDPR+ or Transforming Patients' Rights?*, in S. SLOKENCERBA-K. O' CATHAOIR-M. SHABANI (cur.), *The European Health Data Space. Examining a New Era in Data Protection*, London, 2025, pp. 22 ss., a p. 27.

¹¹ Cfr. la definizione fornita dallo *European Data Protection Board* (Comitato europeo per la protezione dei dati) nelle linee guida reperibili al link <https://ec.europa.eu/newsroom/article29/items/611233>. Come è noto, l'EDPB è il gruppo di lavoro istituito dal GDPR (art. 68), che ha sostituito quello previsto dalla direttiva 95/46 e

noto come WP29 (essendo previsto appunto dall'art. 29 della direttiva europea). Si tratta di un organismo consultivo indipendente, composto da un rappresentante delle varie autorità nazionali, dal Garante europeo della protezione dei dati (EDPS), nonché da un rappresentante della Commissione. Ha il compito di assicurare che le autorità di controllo nazionali seguano interpretazioni comuni della normativa europea in materia di protezione dei dati personali, fornendo orientamenti generali e anche adottando decisioni vincolanti rivolte alle Autorità di Controllo nazionali per dirimere le controversie in sede di applicazione del GDPR.

vatezza dei terzi, quando i dati oggetto della richiesta dell'interessato comprendono informazioni che li riguardano.

Il Regolamento sui dati sanitari segna un passo in avanti. Come emerge dall'art. 7¹², il diritto di portabilità riguarda *tutti* i dati e quindi anche quelli inferenziali. La diagnosi del medico, ad esempio, è il risultato di una elaborazione di dati grezzi (le indicazioni fornite dal paziente, i risultati di analisi e via di seguito) e anch'essa rientra nel diritto di portabilità. La rilevanza degli *inferred data* è evidente ove si consideri la continua espansione della medicina digitale, che consente l'acquisizione e l'elaborazione di dati come il battito cardiaco, l'intensità dell'esercizio fisico, la dieta seguita, il ritmo sonno-veglia, ormai comunemente rilevabili attraverso specifiche applicazioni digitali¹³.

Il medesimo art. 7 al terzo comma prevede poi che la richiesta di portabilità va rivolta al prestatore di assistenza sanitaria e che essa può avere ad oggetto anche la trasmissione ad un fornitore di servizi della sicurezza sociale (si pensi alle strutture residenziali per anziani, o di recupero per tossicodipendenze). La proposta di regolamento prevedeva anche la situazione reciproca e cioè il flusso di dati verso il prestatore di assistenza sanitaria, ma questa disposizione è stata espunta dal testo definitivo. Ciò apre qualche margine di incertezza, in quanto rimette ai legislatori nazionali la decisione di stabilire se la nozione di prestatore di assistenza sanitaria ricomprende anche strutture para-sanitarie, con tutte le conseguenze del caso nell'ipotesi di richieste di trasmissione in altri stati membri¹⁴.

4. L'USO SECONDARIO DEI DATI SANITARI.

Il tema dell'uso secondario dei dati forma oggetto di una attenzione crescente, di pari passo con lo sviluppo dei sistemi di intelligenza artificiale, in specie di quelli cd. 'generativi', che si

¹² "Le persone fisiche hanno il diritto di concedere l'accesso alla totalità o a parte dei loro dati sanitari elettronici personali a un altro prestatore di assistenza sanitaria di loro scelta o di chiedere a un prestatore di assistenza sanitaria di trasmettere la totalità o parte dei loro dati sanitari elettronici a un altro prestatore di assistenza sanitaria di loro scelta immediatamente, gratuitamente e senza ostacoli da parte del prestatore di assistenza sanitaria o dei fabbricanti dei sistemi utilizzati dal prestatore di assistenza sanitaria. 2. Qualora i prestatori di assistenza sanitaria si trovino in Stati membri diversi, le persone fisiche hanno il diritto di chiedere la trasmissione dei loro dati sanitari elettronici personali nel formato europeo di scambio delle cartelle cliniche elet-

troniche di cui all'articolo 15 attraverso l'infrastruttura transfrontaliera di cui all'articolo 23. Il prestatore di assistenza sanitaria ricevente deve accettare tali dati ed è in grado di leggerli" (art. 7).

¹³ W. LI-P. QUINN, *The European Health Data Space: An expanded right to data portability?* in *Computer Law & Security Review*, 2024, pp. 1 ss. Sull'evoluzione del diritto della portabilità dei dati, cfr. S. GATTI, *Dalla portabilità alle "portabilità": l'evoluzione al plurale di un diritto (e concetto) chiave nella disciplina europea dei dati*, in *European Journal of Privacy Law and Technologies*, 2024, pp. 157 ss.

¹⁴ Sul punto, v. I rilievi di K. ●' CATHAÏR, *The EHDS and Electronic Health Records. GDPR+ or Transforming Patients' Rights?*, cit., p. 36.

nutrono proprio sulla acquisizione di una grande quantità di dati, spesso ostacolata, in un contesto come quello europeo, dalla sovrabbondanza di regole e dalle difficoltà connesse alla interoperabilità, particolarmente problematica proprio in ambito sanitario. Ad esempio, la cura di malattie rare e la ricerca di nuovi farmaci richiede l'acquisizione del maggior numero possibile di dati, ma se i ricercatori possono avere accesso solo a quelli provenienti dal proprio paese è evidente che ciò costituisce un ostacolo rilevante ¹⁵.

Prima dell'approvazione del Regolamento, la disciplina dell'uso secondario poggiava sul regime disegnato dal GDPR, in base al quale la ricerca scientifica costituisce un fondamento legittimo per l'uso secondario di dati sensibili (come quelli sanitari) anche senza il consenso dell'interessato. Secondo l'art. 9(2) il loro trattamento è ammesso per "motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale" (lett. i); nonché "a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici", purché proporzionato alla finalità perseguita e con modalità idonee a tutelare i diritti fondamentali e gli interessi della persona" (lett. j).

Tuttavia, sul significato di "ricerca" si è aperto un ampio dibattito, non essendo chiaro se per "ricerca a fini di pubblico interesse" deve intendersi solo quella condotta in ambito accademico e sanitario o anche nel settore privato, ad esempio dalle industrie farmaceutiche, biotecnologiche o assicurative. Inoltre, il GDPR lascia agli Stati membri la facoltà di introdurre condizioni ulteriori per il legittimo trattamento dei dati genetici, biometrici e, in generale, concernenti la salute (art. 9, co. 4) e le scelte adottate in sede nazionale sono tutt'altro che armonizzate. Ad esempio, in Francia sono previsti requisiti molto stringenti per l'uso di dati anonimizzati a fini di ricerca ¹⁶, in Germania è ammesso con maggiore libertà l'uso secondario ma solo nel settore pubblico, in Finlandia viene adottato un approccio molto più aperto ¹⁷. Oltre

¹⁵ Per un primo inquadramento, cfr. F. CASINI-M.A. ARCURI, *Uso secondario dei dati personali relativi alla salute: panoramica della normativa europea e nazionale*, in questa Rivista, 2024, pp. 837 ss.

¹⁶ Cfr. X. PICAN-T. DEVRED-L. ZAGGIA, *L'évolution de l'accès et de l'utilisation secondaire des données de santé. Dans quelle*

mesure les nouvelles réglementations vont-elles affecter la façon d'accéder et de réutiliser les données de santé?, in *Droit de l'immatériel*, 2024, fasc. 5, pp. 30 ss.

¹⁷ Per ulteriori riferimenti, cfr. I. SANCHEZ FRIAS, *Secondary Uses Of Health Data Under The European Health Data Space. Connections With The GDPR And The Im-*

alla distanza tra le soluzioni, va pure considerato che oltre la metà degli Stati membri sono proprio sprovvisti di specifiche discipline sul riuso di dati sanitari elettronici a fini di ricerca o di pubblico interesse ¹⁸.

Da questo punto di vista, non può che essere accolta favorevolmente l'iniziativa dal legislatore europeo che dedica l'intero capo IV del Regolamento all'uso secondario dei dati sanitari elettronici, definito come il trattamento per finalità "diverse dalle finalità iniziali per le quali tali dati sono stati raccolti o prodotti" (art. 2, par. 2, lettera e).

L'istituzione di una infrastruttura transfrontaliera obbligatoria si prefigge di facilitare la ricerca, la sicurezza dei pazienti, lo sviluppo della medicina personalizzata, nonché di consentire appropriate statistiche ufficiali e di regolamentare l'intero settore. D'altro canto, la scelta di intervenire mediante la forma del regolamento, e non della direttiva, dovrebbe limitare — almeno in teoria — il rischio di una eccessiva frammentazione tra le discipline nazionali.

Gli usi secondari riguardano gli interventi di sanità pubblica (come ad esempio la programmazione sanitaria, la prevenzione o la gestione di emergenze di salute della collettività), le attività di innovazione (tra cui quelle condotte nel settore farmaceutico o dei dispositivi medici e delle tecnologie applicate alla salute anche da parte di soggetti privati), le attività di ricerca scientifica, storica e di medicina personalizzata, le azioni per la sicurezza delle cure, le iniziative formative e didattiche e, infine, relativi a finalità di natura legislativa e politica.

L'art. 53 elenca le finalità per cui è possibile trattare i dati sanitari elettronici per l'uso secondario e prevede che gli organismi responsabili consentono l'accesso se il trattamento dei dati è necessario per finalità di pubblico interesse e di ricerca scientifica che abbia "l'obiettivo di favorire gli utenti finali" ¹⁹. Questa ampia formulazione apre lo spazio all'uso secondario dei dati al settore privato e ciò trova conferma nel considerando n. 52, ove

fact Of AI (April 10, 2024), disponibile al link <https://ssrn.com/abstract=5143418> or <http://dx.doi.org/10.2139/ssrn.5143418>

¹⁸ Sul punto si sofferma la Commissione Europea, *Assessment of the EU Member States' rules on health data in the light of GDPR*, 2021, pp. 57 ss. (disponibile al link https://health.ec.europa.eu/publications/assessment-eu-member-states-rules-health-data-light-gdpr_en).

¹⁹ "1. Gli organismi responsabili dell'accesso ai dati sanitari concedono l'accesso ai dati sanitari elettronici di cui all'articolo 51 per l'uso secondario a un utente dei dati sanitari solo se il trattamento dei

dati da parte dell'utente è necessario per una delle finalità seguenti: [...] e) *ricerca scientifica* nel settore sanitario o dell'assistenza che contribuisce alla sanità pubblica o alla valutazione delle tecnologie sanitarie o che garantisce elevati livelli di qualità e sicurezza dell'assistenza sanitaria, dei medicinali o dei dispositivi medici, *con l'obiettivo di favorire gli utenti finali*, quali i pazienti, i professionisti sanitari e gli amministratori sanitari, tra cui: i) attività di sviluppo e innovazione per prodotti o servizi; ii) attività di addestramento, prova e valutazione degli algoritmi, anche nell'ambito di dispositivi medici, dispositivi medico-

emerge la novità rispetto al regime disegnato dal GDPR, laddove si precisa che gli Stati non possono introdurre limitazioni all'accesso, ivi incluso il previo consenso degli interessati di cui all'art. 9.4 del GDPR.

Nello stesso tempo, tuttavia, il lungo *iter* che ha condotto alla adozione del Regolamento ha posto in evidenza la necessità di garantire che la circolazione dei dati avvenga in un contesto sicuro, per scopi appropriati e con garanzie adeguate circa l'accesso agli stessi. Invero, se per un verso è senz'altro auspicabile una utilizzazione dei dati sanitari per agevolare la ricerca e, in definitiva, la tutela della salute, per altro verso vanno adeguatamente salvaguardati i diritti dei singoli, evitando che la circolazione dei dati conduca a situazioni lesive dei loro interessi. Per avvedersi della rilevanza del tema, basta pensare a cosa potrebbe accadere se i dati relativi alla gravidanza entrassero nella disponibilità del proprio datore di lavoro, o se quelli relativi ad accertamenti sanitari fossero accessibili alla propria compagnia di assicurazione. Gli esempi potrebbero moltiplicarsi.

Questa esigenza è posta in evidenza nel già citato considerando n. 52, che sottolinea la necessità che la disciplina dell'uso secondario sia accompagnata da misure idonee per salvaguardare i diritti fondamentali e gli interessi delle persone fisiche, richiamando in particolare l'art. 9 del GDPR e cioè quella norma che, come si è visto, vieta il trattamento dei "dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale", ma anche quelli genetici e biometrici che consentono di identificare in modo univoco una persona fisica, nonché i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. Il considerando n. 60 precisa inoltre che la condivisione dei dati per uso secondario deve essere coerente con le disposizioni in materia di trasparenza previste dal diritto dell'UE.

Nella ricerca di un difficile equilibrio tra queste contrapposte esigenze, il Regolamento prevede un meccanismo di obiezione (opt-out) per alcune categorie particolari di dati previste dall'art. 51.1 lett. f), g), i), q), ossia i dati genetici, genomici ed epigenomici umani, altri dati molecolari umani, i dati provenienti dalle applicazioni per il benessere e i dati provenienti da biobanche e banche dati associate. In sostanza, il diritto di accesso e di portabilità riguardano anche questi dati, ma gli Stati membri potranno prevedere il diritto dell'interessato ad escludere l'accesso²⁰.

diagnostici in vitro, sistemi di IA e applicazioni di sanità digitale; [...] (corsivo aggiunto).

²⁰ Sul rapporto tra il Regolamento e il GDPR rispetto alla ricerca sanitaria, cfr.

M. KRUUS, *Opting Out of Scientific Research with Health Data: The Limits of the EHDS and the GDPR*, in *European Journal of Health Law*, 2025, pp. 1 ss, nonché D. SPAJIC, *Transforming the secondary use of*

Di ancor maggior rilievo è però l'art. 71, che introduce un diritto generale di esclusione delle persone fisiche rispetto al trattamento dei propri dati sanitari elettronici per uso secondario. Tale diritto è esercitabile in qualsiasi momento senza dover fornire una motivazione e gli Stati membri sono tenuti a garantire modalità accessibili e facilmente comprensibili, rispettando i principi di trasparenza e semplicità al fine di evitare che le persone rinuncino all'esercizio del loro diritto a causa di procedure troppo complesse. Se il diritto viene esercitato, i dati sanitari elettronici personali non potranno più essere messi a disposizione o trattati per l'uso secondario. Ciò vale però solo per il futuro, cioè l'esclusione non pregiudica i trattamenti già autorizzati prima dell'esercizio del diritto. Quindi, se i dati sono già stati utilizzati per una finalità legittima, i relativi usi rimangono validi e non possono essere vietati retroattivamente ²¹.

Come già si è osservato rispetto al diritto di esclusione per l'uso primario, anche per l'uso secondario la previsione dell'*opt-out* costituisce evidentemente un ostacolo alla realizzazione di una piena utilizzazione dei dati. Il quadro, peraltro, si complica anche in ragione del fatto che il medesimo art. 71 prevede anche una deroga al diritto di esclusione. Infatti, gli Stati membri possono introdurre nei propri ordinamenti un meccanismo che consenta di rendere comunque disponibili i dati sanitari di una persona che ha esercitato il diritto di esclusione, pur se in base a condizioni stringenti. In particolare, la richiesta di accesso deve provenire da un ente pubblico, da un'istituzione, da un organo dell'Unione Europea o da un soggetto incaricato di svolgere compiti di interesse pubblico nel settore sanitario. Il trattamento deve poi essere necessario per la protezione della salute pubblica, per la gestione di emergenze sanitarie o per la ricerca scientifica per rilevanti motivi di pubblico interesse e deve essere dimostrato che l'accesso ai dati non è possibile in altri modi. Il considerando n. 54 esplicita le ragioni di questa deroga, precisando che la possibilità per le persone fisiche di escludere i propri dati sanitari dall'uso secondario trova un limite in presenza di finalità di interesse pubblico, quali le attività di protezione da gravi minacce per la salute a carattere transfrontaliero o la ricerca per importanti motivi di interesse pubblico, come quella che risponde ad esigenze mediche insoddisfatte (ad esempio per le malattie rare) o a minacce sanitarie emergenti. In sostanza, in questi casi l'accesso

patient data in the European Health Data Space A challenge for the patient's right to medical confidentiality?, in S. SLOKENCERBA-K. ● CATHOIR-M. SHABANI (cur.), *The European Health Data Space ecc.*, cit., ove anche interessanti rilievi sulle ripercussioni

del nuovo sistema sui rapporti medico/paziente.

²¹ Sull'iter che ha condotto a questa previsione, cfr. I. SANCHEZ FRIAS, *Secondary Uses Of Health Data ecc.*, cit., p. 8.

va sempre consentito, anche relativamente ai dati di coloro che esercitano il diritto di esclusione²².

La possibilità di introdurre la deroga al diritto di esclusione è comunque rimessa alla discrezionalità degli Stati membri e ciò potrà condurre ad una disparità circa il contenuto del diritto.

5. ANONIMIZZAZIONE E PSEUDONIMIZZAZIONE DEI DATI PER L'USO SECONDARIO.

A livello giuridico e di governance, la struttura del quadro comune per l'uso secondario si basa sull'istituzione di organismi responsabili dell'accesso ai dati sanitari (*Health Data Access Body* - HDAB), disciplinati dall'art. 55, che cooperano attraverso la già citata rete *HealthData@EU*. Saranno questi organismi a fornire ai soggetti richiedenti (utenti/utilizzatori dei dati o *data user*) l'autorizzazione all'accesso per usi secondari, secondo un meccanismo rigoroso di decisione delle richieste per verificare se le finalità indicate sono conformi alle previsioni del Regolamento. Essi sono anche responsabili della sorveglianza e del monitoraggio, nel rispetto anche delle misure di sicurezza.

Tralasciando i dettagli organizzativi, giova concentrarsi sul tema relativo alla vigilanza sulla anonimizzazione e pseudonimizzazione dei dati, al fine di proteggere la riservatezza e la sicurezza delle informazioni trattati. Viene in rilievo, in proposito, l'art. 66, che rafforza l'obbligo (già previsto nel GDPR) volto a garantire che il trattamento dei dati sia sempre proporzionato e giustificato. Gli organismi responsabili devono assicurarsi che la richiesta di accesso concerna dati adeguati, pertinenti e limitati a quanto necessario per la finalità dichiarata, con una valutazione da svolgersi caso per caso. Inoltre, va accertato che il richiedente disponga delle competenze necessarie e le qualifiche professionali adeguate nei settori dell'assistenza sanitaria, della sanità pubblica o della ricerca e che operi nel rispetto delle norme etiche e legislative applicabili. Il richiedente deve anche dimostrare di aver implementato misure tecniche e organizzative adeguate per prevenire qualsiasi uso improprio dei dati e per garantire il diritto degli interessati

Un aspetto centrale è quello relativo alla modalità di accesso,

²² Cfr., anche per ulteriori riferimenti, E. SANTAMARIA ECHEVERRIA, *The European Health Data Space. A New Paradigm for Secondary Uses of Health Data for Scientific Research*, in S. SLOKENCERBA-K. O. CATTIAOIR-M. SHABANI (cur.), cit., pp. 162 ss. Attira l'attenzione sul rischio di frammentazione delle discipline nazionali rispetto all'uso secondario P. HAJDUK, *A Walk in the*

Labyrinth. Evolving EU Regulatory Framework for Secondary Use of Electronic Personal Health Data for Scientific Research (November 23, 2023), forthcoming, *18th IFIP Privacy and Identity Management 2023 - Sharing (in) a Digital World*, Springer, disponibile al link <https://ssrn.com/abstract=4673534>.

che risponde al principio della cd. minimizzazione dei dati. La norma prevede infatti che essi vengano forniti in modo anonimo, in modo da evitare il rischio di identificazione dell'interessato e limitare i problemi di riservatezza. Anche se il testo non chiarisce se ciò che si richiede è una anonimità assoluta, cioè tale da rendere rendibile impossibile la ri-identificazione, o relativa, cioè tale da renderla possibile in teoria, anche se inverosimile in pratica in ragione dei costi o del tempo necessario, va rammentato che la giurisprudenza della Corte di Giustizia sembra da tempo orientata nel senso di preferire un significato relativo ²³.

Può però accadere che per le finalità del trattamento richiesto sia necessario un accesso non in forma anonima, ma pseudonimizzata. In tal caso, il richiedente è tenuto ad indicare, ai sensi dell'art. 67, in qual modo assicura che il trattamento sarà conforme alla normativa nazionale e alla normativa UE applicabile in materia di protezione dei dati e di privacy, in particolare descrivendone la conformità al GDPR. Se l'autorizzazione viene rilasciata, i titolari di dati hanno l'obbligo di renderli disponibili, per un periodo di tempo limitato allo svolgimento delle analisi per uso secondario.

In ragione delle verifiche necessarie, l'art. 69 prevede che il tempo del procedimento è di sei mesi, un quindi periodo piuttosto lungo, che può rivelarsi di ostacolo in situazioni di emergenza sanitaria, dove l'accesso tempestivo è essenziale per adottare efficaci misure di contrasto. Ad ogni buon conto, l'art. 70 demanda alla Commissione Europea di definire i modelli da utilizzare per la presentazione delle richieste e questo dovrebbe contribuire a rendere più fluido il procedimento.

Con norma speciale (che prevale sull'art. 6 del regolamento n. 868 del 30 maggio 2022 (Data Governance Act - DGA), il Regolamento prevede la possibilità per gli organismi di accesso ai dati di imporre il pagamento di un contributo, al fine di coprire i costi della procedura per valutare le domande di accesso ai dati o di richiesta di dati, concedere, rifiutare o modificare un permesso di dati, fornire una risposta a una richiesta di dati e, eventualmente, indennizzare i costi sostenuti dal titolare dei dati sanitari per la compilazione e la preparazione dei dati sanitari elettronici da rendere disponibili per un uso secondario (art. 62).

6. LE SANZIONI E IL RISARCIMENTO DEL DANNO.

Il Regolamento delinea un articolato sistema di tutele dei diritti dei singoli. Anzitutto, qualsiasi individuo, organismo o entità che

²³ Corte Giust., C-582/14, 19 ottobre 2016, *Patrick Breyer v Bundesrepublik Deutschland*. Sul tema, cfr. R. RAK, *Anonymisation, Pseudonymisation and Secure Processing Environments Relating to the*

Secondary Use of Electronic Health Data in the European Health Data Space (EHDS), in *European Journal of Risk Regulation*, 2024, pp. 928 ss.

abbia un legittimo interesse può presentare un reclamo all'organismo responsabile dell'accesso ai dati sanitari, se ritiene che vi sia stata una violazione delle norme applicabili in materia di gestione, accesso e condivisione dei dati sanitari elettronici (art. 81). L'organismo ricevente è tenuto ad esaminare ogni reclamo, ad avviare un'indagine interna e comunicare le proprie conclusioni in un tempo ragionevole, adottando, in caso di fondatezza, la modifica delle procedure di trattamento e l'adozione di misure di sicurezza aggiuntive per prevenire ulteriori violazioni. Se non fosse soddisfatto della risposta ricevuta, l'interessato può rivolgersi all'autorità nazionale di protezione dei dati e comunque rivolgersi ai tribunali competenti per ottenere tutela per via giudiziaria.

L'art. 99 contempla poi il regime sanzionatorio per le violazioni delle disposizioni del Regolamento, con misure amministrative pecuniarie (il cui importo è commisurato alla gravità della violazione, alla sua durata e all'eventuale vantaggio economico ottenuto dal trasgressore) e non pecuniarie (che possono consistere nella sospensione temporanea o definitiva all'accesso, il ritiro delle autorizzazioni e l'adozione di provvedimenti correttivi per garantire il rispetto delle norme). Tali sanzioni sono irrogate dalle autorità nazionali competenti, che sono tenute ad informare la Commissione Europea anche al fine di consentirle di intervenire per assicurare un'uniforme applicazione delle norme in tutti gli Stati membri, evitando disparità nell'applicazione delle sanzioni tra i vari paesi.

Di particolare interesse è infine l'art. 100 che prevede che "qualsiasi persona fisica o giuridica che subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere un risarcimento, conformemente al diritto dell'Unione e nazionale". Il rinvio al diritto dell'Unione comprende ovviamente il richiamo dell'art. 82 del GDPR, che prevede una ipotesi di responsabilità oggettiva, in quanto prescinde dal dolo o dalla colpa, sicché per il danneggiato è sufficiente dimostrare l'esistenza del danno e il nesso di causalità rispetto alla violazione delle norme applicabili. Il risarcimento deve essere integrale e comprende tanto i danni materiali (ad esempio, le spese mediche derivanti dall'uso improprio dei dati, la perdita di opportunità di lavoro, ecc.) quanto quelli immateriali, come la violazione della riservatezza, della reputazione, nonché il disagio psicologico conseguente alla divulgazione di informazioni mediche in modo non conforme alla normativa.

7. L'ENTRATA IN VIGORE DEL REGOLAMENTO.

Il legislatore europeo si mostra consapevole che la complessità dell'impianto richiede un lungo percorso per diventare pienamente operativo, come emerge dall'art. 105 che, per un verso,

fissa l'entrata in vigore al 26 marzo 2025 ma, per altro verso, prevede l'avvio di un periodo di transizione per la sua concreta applicazione, prevista per il 26 marzo 2027.

Nel corso di questo periodo sia la Commissione Europea che gli Stati membri sono impegnati a svolgere numerosi adempimenti. Quanto alla Commissione, essa è chiamata ad adottare vari atti esecutivi, il principale dei quali è l'implementazione della piattaforma *MyHealth@EU*, stabilendo le specifiche tecniche relative alle categorie prioritarie di dati sanitari elettronici sanitari e il formato europeo di scambio delle cartelle cliniche. Quanto agli Stati, essi dovranno designare le autorità nazionali competenti e decidere su tutti i temi rimessi alla loro discrezionalità.

Una volta conclusa questa fase, bisognerà attendere fino al 26 marzo 2029 per l'applicazione delle norme essenziali del Regolamento e cioè, quanto all'uso primario, lo scambio del primo gruppo di categorie prioritarie di dati sanitari (profili sanitari sintetici dei pazienti, prescrizioni/dispensazioni elettroniche) e, quanto all'uso secondario, l'accesso alla maggior parte delle categorie di dati (ad esempio i dati delle cartelle cliniche elettroniche). Solo nel 2031 diverranno operativi sia lo scambio del secondo gruppo di categorie prioritarie di dati sanitari per l'uso primario (immagini mediche, risultati di laboratorio e lettere di dimissione ospedaliera), sia la parte restante delle categorie di dati per l'uso secondario (ad esempio i dati genomici). Infine, solo dal 2034 i paesi extra UE e le organizzazioni internazionali potranno chiedere di aderire a *MyHealthData@EU* per l'uso secondario.

8. LA BASE GIURIDICA DEL REGOLAMENTO. RIFLESSIONI IN PROSPETTIVA PER UN PIÙ SOLIDO FONDAMENTO DELLA TUTELA DEL PAZIENTE/CITTADINO EUROPEO.

Il quadro che si è tentato di fornire nelle pagine che precedono sui principali contenuti del Regolamento fa emergere che ci si trova di fronte ad una svolta che, almeno nelle intenzioni, può incidere profondamente sull'assetto complessivo della tutela della salute all'interno dell'Unione. Il fatto stesso che lo spazio europeo dei dati sanitari richieda un lungo periodo per la sua concreta implementazione rivela la portata delle novità, che vanno al di là della materia dei dati in sé considerati, implicando la necessità di configurare il rapporto tra le strutture, gli operatori sanitari e i pazienti in modo diverso rispetto a quello seguito nei vari paesi. Anche la ricerca scientifica è destinata ad avere un nuovo impulso, attraverso la disponibilità di un patrimonio di dati finora accessibili con difficoltà e in modo disomogeneo all'interno dell'Unione.

A fronte della ampiezza della sfida, si è visto che la versione finale presenta delle differenze di rilievo rispetto al testo proposto

dalla Commissione, la gran parte delle quali consiste in soluzioni di compromesso, resesi necessarie di fronte alle resistenze emerse. Il loro tratto comune è di aprire spazi alla discrezionalità degli Stati, che possono introdurre regimi differenziati su aspetti centrali, che vanno dalla possibilità di estendere l'accesso e lo scambio a dati ulteriori rispetto a quelli contemplati nel Regolamento, alla previsione del diritto di escludere l'accesso con un meccanismo di *opt-out*, che peraltro gli Stati stessi possono limitare, consentendo comunque l'accesso in casi particolari.

Va poi considerato che il nuovo Regolamento si inserisce in una serie impressionante di iniziative legislative che negli ultimi anni stanno interessando la disciplina dei dati, con norme non sempre tra loro coerenti e che interferiscono l'una con l'altra. Ciò rischia di appesantire e rendere farraginoso l'adeguamento, ostacolando di fatto una reale armonizzazione. Solo con il tempo si potrà verificare se prevarrà uno spirito costruttivo e collaborativo tra le istituzioni europee e gli Stati membri.

Pur in presenza di questi limiti, non può sfuggire l'importanza del tentativo compiuto. A fronte della crisi di identità che da tempo sta attraversando l'Europa, caratterizzata dalla progressiva erosione della fiducia degli Stati e delle persone verso le istituzioni europee, la recente pandemia Covid-19 è stato un evento di portata tale da porre in evidenza che la tutela della salute circoscritta in una dimensione territoriale e nazionale è fallimentare per affrontarne gli effetti disastrosi sul piano sociale ed economico. Non a caso, la Commissione Europea ha posto mano alla prima proposta di Regolamento proprio all'indomani della fase emergenziale della pandemia, quando si era toccato con mano che cosa significa la disparità tra i sistemi sanitari, confinati dentro gli angusti limiti della sovranità degli Stati, di fronte ad un microscopico virus la cui circolazione non si è certo arrestata alle frontiere.

La posta in gioco connessa alla creazione di uno spazio comune dei dati sanitari va dunque nella giusta direzione. Nel contempo, le resistenze che si sono manifestate nella fase di discussione della proposta, che hanno condotto a quelle soluzioni di compromesso cui si è fatto cenno, si prestano ad essere lette come rivelatrici di un atteggiamento di diffidenza di fronte ad un sistema percepito come un ulteriore intralcio burocratico e una minaccia alle competenze degli Stati membri.

È allora opportuno chiedersi se la base giuridica su cui si fonda l'istituzione dello spazio europeo dei dati sanitari sia adeguata per fornire un fondamento solido ad una reale armonizzazione.

Come è noto, la competenza dell'Unione Europea ad intervenire in materia di salute è piuttosto limitata. L'art. 168 TFUE, dedicato alla sanità pubblica, prevede che "nella definizione e nell'attuazione di tutte le politiche ed attività dell'Unione è garantito un elevato livello di protezione della salute umana", precisando però

che l'azione dell'Unione "completa le politiche nazionali" e si indirizza al miglioramento della sanità pubblica, alla prevenzione delle malattie e alla eliminazione dei pericoli per la salute fisica e mentale. Il secondo comma precisa che l'Unione "incoraggia la cooperazione tra gli Stati membri" e l'ultimo comma sottolinea che l'azione dell'Unione "rispetta le responsabilità degli Stati membri" nella gestione dei servizi sanitari e dell'assistenza medica, con ciò palesando che si tratta di materia sostanzialmente devoluta agli Stati stessi.

Per questa ragione, benché nel corso delle negoziazioni fosse stata avanzata l'ipotesi di fare comunque riferimento all'art. 168 TFUE²⁴, il testo definitivo del Regolamento non lo richiama e si appoggia invece sull'art. 16 TFUE, secondo cui "ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano", e sul consueto art. 114 TFUE, che consente all'Unione di intervenire per "l'instaurazione ed il funzionamento del mercato interno".

La scelta di far leva sul mercato è in linea con l'approccio che da tempo adotta il legislatore europeo quando si tratta di intervenire su materie rispetto alle quali la competenza dell'Unione può rivelarsi problematica²⁵. L'armonizzazione ai fini del funzionamento del mercato interno è una sorta di *passpartout* a cui è facile far ricorso. Senonché, la tutela della salute coinvolge diritti fondamentali della persona e non sembra certo potersi pensare e realizzare solo in funzione del mercato e degli indici di concorrenzialità. Inoltre, la prospettiva del mercato rischia di accentuare il livello di competitività tra gli Stati membri, giungendo a legittimarli a piegare gli spazi che il Regolamento rimette alla loro discrezionalità al perseguimento di obiettivi distanti dalla realizzazione di uno spazio europeo dei dati sanitari, il cui scopo è di tutelare allo stesso tempo gli interessi dei singoli e il bene comune.

Da questo punto di vista, allora, sul filo di considerazioni da tempo espresse in dottrina²⁶, una base giuridica ben più solida, le cui potenzialità appaiono ancora poco esplorate, è quella costituita dalla cittadinanza dell'Unione, che è uno degli aspetti più innovativi del TUE sottoscritto a Lisbona nel 2007: "È cittadino dell'Unione chiunque abbia la cittadinanza di uno Stato membro.

²⁴ D. FAHRAEUS-J. REICHEL-S. SLOKENBERGA, *The European Health Data Space: Challenges and Opportunities*, 2024, disponibile al link <https://sieps.se/en/publications/2024/the-european-health-data-space-challenges-and-opportunities/>, p. 3.

²⁵ Basta pensare all'imponente corpus di direttive in materia di 'diritto privato europeo'. Cfr. L. MOCCIA, *Dal "mercato" alla "cittadinanza": ovvero, dei possibili*

itinerari di diritto privato europeo, in *Riv. trim. dir. proc. civ.*, 2003, pp. 395 ss.

²⁶ L. MOCCIA, *Dal "mercato" alla "cittadinanza": ovvero, dei possibili itinerari di diritto privato europeo*, in *Riv. trim. dir. proc. civ.*, 2003, pp. 395 ss. e Id., *Cittadinanza europea e spazio di libertà, sicurezza e giustizia*, in *La cittadinanza europea*, 2010, pp. 115 ss.

La cittadinanza dell'Unione si aggiunge alla cittadinanza nazionale e non la sostituisce" (art. 9 TUE).

Il vantaggio di questo riferimento alla cittadinanza dell'Unione è dato proprio dalla sua caratteristica intrinseca di complemento della cittadinanza nazionale (ribadito dall'art. 20 TFUE). Come rilevato dall'avvocato generale Maduro, le due cittadinanze, nazionale ed europea, sono distinte ma allo stesso tempo complementari:

Si tratta di due nozioni allo stesso tempo inestricabilmente connesse e autonome. La cittadinanza dell'Unione presuppone la cittadinanza di uno Stato membro, ma è anche una nozione giuridica e politica autonoma rispetto a quella di cittadinanza nazionale. La cittadinanza di uno Stato membro non consente solo l'accesso al godimento dei diritti conferiti dal diritto comunitario, essa ci rende cittadini dell'Unione. La cittadinanza europea costituisce inoltre qualcosa in più di un insieme di diritti che, di per sé, potrebbero essere concessi anche a coloro che non la possiedono. Essa presuppone l'esistenza di un collegamento di natura politica tra i cittadini europei, anche se non si tratta di un rapporto di appartenenza ad un popolo. [...] Esso si fonda sul loro impegno reciproco ad aprire le rispettive comunità politiche agli altri cittadini europei e a costruire una nuova forma di solidarietà civica e politica su scala europea ²⁷.

La cittadinanza europea, dunque, completa ed arricchisce la dotazione dei diritti della persona ed è un valore che assorbe ed integra il mercato, come sinonimo di uno spazio e diritto 'comune'. In tal senso, allora, anche la realizzazione di uno spazio europeo dei dati sanitari può trovare nella dimensione della cittadinanza europea una prospettiva in grado di tenere insieme esigenze diverse e potenzialmente in contrasto tra loro e cioè le prerogative nazionali in materia sanitaria riconosciute dai Trattati, la tutela dei diritti del singolo all'accesso e al trattamento dei dati, il diritto alla riservatezza, la tutela della salute che richiede strumenti che trascendono i confini nazionali anche a fini di ricerca.

La limitazione dei diritti dei singoli può trovare un fondamento ragionevole proprio se si fonda sul motivo della comune cittadinanza che lega i pazienti/cittadini europei agli altri pazienti/(con)cittadini europei e che legittima la loro compressione quando è necessario salvaguardare interessi che trascendono il perimetro della sfera individuale, come la promozione della ricerca in materia sanitaria, la prevenzione, l'adeguata reazione a fenomeni (come quello pandemico) che richiedono l'adozione di misure

²⁷ Conclusioni nella causa C-135/08, *Janko Rottmann c. Freistaat Bayern*, 30 settembre 2009, punto 23.

particolari. Allo stesso modo, il riferimento alla cittadinanza può costituire il criterio da seguire nella ricerca delle modalità attraverso cui i legislatori nazionali pervengono ad identificare la disciplina dei numerosi aspetti lasciati dal Regolamento alla loro discrezionalità, plasmandole in modo tale da non vanificare il perseguimento dell'obiettivo di realizzare una comunità di cittadini tra loro uguali al livello sia nazionale che europeo ²⁸.

Abstract

Questo articolo si sofferma sul recente Regolamento dell'UE che istituisce lo Spazio europeo dei dati sanitari, promuovendo la condivisione e l'uso efficace delle informazioni sanitarie tra gli Stati membri e rafforzando i diritti dei pazienti in relazione ai loro dati sanitari elettronici, consentendo inoltre l'accesso a tali dati per scopi di ricerca, innovazione e politica sanitaria. Questa ennesima iniziativa legislativa attira l'attenzione del comparatista, in ragione dell'ampia gamma di questioni lasciate alla discrezionalità dei legislatori nazionali, che è suscettibile di compromettere un'autentica armonizzazione. La base giuridica adottata dal legislatore europeo, imperniata sull'art. 114 TFUE, si rivela poco adeguata per affrontare la tutela della salute, in quanto essa coinvolge diritti fondamentali della persona che non possono essere protetti solo nella prospettiva del mercato. La creazione di uno spazio europeo dei dati sanitari potrebbe invece trovare nella dimensione della cittadinanza europea una base più solida, capace di far convergere esigenze diverse e potenzialmente contrastanti e in particolare le prerogative nazionali, la tutela dei diritti individuali di accesso e trattamento dei dati, il diritto alla privacy.

This article dwells on the recent EU Regulation establishing the European Health Data Space, promoting the sharing and effective use of health information across Member States and strengthening patients' rights in relation to their electronic health data, while also enabling access to it for research, innovation and health policy purposes. This umpteenth legislative initiative attracts the attention from a comparative perspective, due to the wide range of issues left to the national legislators, potentially undermining an effective harmonization. The author argues that the legal basis adopted by the EU legislator, pivoting on art. 114 TFUE, is inadequate to face health protection, which involves

²⁸ Cfr. L. MOCCIA, *Cittadini Uniti d'Europa, ovvero della cittadinanza come garanzia di futuro dell'Unione*, in *lceonline*

0/2021, reperibile al link <https://www.lceonline.eu/wp-content/uploads/2021/04/L.01Moccia-saggi-1.pdf>.

fundamental personal rights that cannot be protected solely in terms the market perspective. Instead, the creation of a European health data space could find in the dimension of European citizenship a solid base, capable of bringing together different and potentially conflicting needs and in particular the national prerogatives, the protection of the individual's rights to access and process data, the right to privacy.