Comparative Law Review

Vol. 17 · No. 2
2026

REGULAR ISSUE

ISSN 2038 – 8993

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

Office address and contact details:
Email: complawreview@gmail.com

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

COMPARATIVE
LAW
REVIEW
VOL. 17/2 - 2026

Spazio europeo dei dati sanitari

SPAZIO EUROPEO DEI DATI SANITARI

USO SECONDARIO DEI DATI SANITARI E TUTELA DELL'INTERESSATO: TRA RIMEDI E SANZIONI

Mariella Cuccovillo

SOMMARIO:

The author examines the secondary use of health data under the EHDS Regulation, reconstructing the protection of the data subject, with particular attention to the so-called right of opt-out *and the complaint system. She further analyses the investigative and enforcement powers of the health data access bodies, as well as the model of civil liability and the nature of compensation, highlighting the tensions between a compensatory function and potential sanction-oriented elements within a framework aimed at protecting "personal identity."*

L'autrice esamina l'uso secondario dei dati sanitari ai sensi del Regolamento EHDS, ricostruendo la tutela dell'interessato, con particolare attenzione al cosiddetto diritto di opt-out e al sistema dei reclami. Analizza inoltre i poteri investigativi e sanzionatori degli organismi di accesso ai dati sanitari, nonché il modello di responsabilità civile e la natura del risarcimento, evidenziando le tensioni tra una funzione compensativa e potenziali elementi di natura sanzionatoria, all'interno di un quadro volto a tutelare "l'identità personale."

Keywords: Health data - secondary use - data subject - protection - damages
Dati sanitari - uso secondario - interessato - protezione - danni

I. USO SECONDARIO DEI DATI SANITARI E VALORIZZAZIONE DELLE ESIGENZE DI RICERCA: DAL REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI ALLO SPAZIO EUROPEO DEI DATI PERSONALI

La recente vicenda della Pandemia ha dimostrato lo stretto legame tra salute (anche nella declinazione meta-individuale di sanità pubblica), *privacy* e digitale. In questa prospettiva, si comprende la necessità di condivisione dei dati sanitari[1], avvertita non solo per motivi di ricerca scientifica e tutela della salute, ma anche per la gestione organizzativa dei servizi sanitari, in particolare, in occasione di eventi pandemici[2].

[1] Sulla distinzione tra la nozione più ampia "dato relativo alla salute", in cui potrebbero confluire e rientrare tutte quelle informazioni che di per sé non indicano, né rendono individuabile una condizione fisica, una patologia o uno stato morboso, e "dato sanitario", v. Cass., ord. 11 ottobre 2023, n. 28417, secondo cui l'informazione in ordine alla necessità di seguire una terapia medica (peraltro non specificata), a seguito della dimissione da un ospedale, costituirebbe un "dato relativo alla salute" (la decisione è riportata da AMARÙ-FAVA-FOSSI-MAINARDI, *La* privacy *del dato sanitario*, Milano, 2024, p.16). Sotto un diverso profilo, si è sottolineata la necessità di controllare l'esattezza e la qualità dei dati, anche in termini di comunicazione al pubblico e l'esigenza dell'adozione di sistemi di protezione sempre più avanzati e aggiornati non solo dal punto di vista delle infrastrutture informatiche, ma anche dal punto di vista formativo e organizzativo degli Enti, delle figure professionali che trattano i dati personali e gli Interessati medesimi (cfr. AMARÙ-FAVA-FOSSI-MAINARDI, *La* privacy, cit., p. 42).

[2] È evidente il riferimento all'uso della APP. IO.

L'ammissibilità dell'uso secondario dei dati personali proviene dal Regolamento generale sulla protezione dei dati 2016/679 (General Data Protection Regulation – d'ora in avanti, GDPR) che, all'articolo 5, rende possibile il trattamento dei dati sanitari personali per finalità diverse da quelle per le quali sono stati raccolti. Tra tali diverse finalità, è compresa la finalità di ricerca, a condizione che il trattamento dei dati avvenga in modo lecito, corretto e trasparente.

La disciplina più approfondita dell'utilizzo secondario dei dati si evince dal *Considerando* n.50, dall'art. 6 e dall'art. 9, paragrafo 2, del GDPR. Nello specifico, l'uso secondario dei dati, anche con riguardo a categorie particolari di dati personali, nei quali rientrano quelli sanitari, è consentito solo se le finalità che si perseguono - con questa tipologia di trattamento - sono compatibili con quelle per le quali i dati sono stati inizialmente raccolti e la base giuridica, che regola questo tipo di utilizzo, non differisce da quella che legittima l'utilizzo primario dei dati stessi.

Se l'uso secondario dei dati sanitari è compatibile con le finalità per le quali si è proceduto all'uso primario, ed è necessario per eseguire un compito di interesse pubblico o per esercitare pubblici poteri, la liceità e la compatibilità dell'ulteriore trattamento viene constatata in base alle finalità e ai compiti che possono essere stabiliti dal diritto dell'Unione Europea o degli Stati membri. Dovrebbe essere considerato lecito e compatibile l'utilizzo ulteriore dei dati sanitari per finalità di archiviazione nel pubblico interesse o di ricerca scientifica o storica o a fini statistici[3].

Al di fuori dei casi in cui il trattamento per finalità diversa da quella per la quale i dati sono stati raccolti sia basato su un consenso o su un atto legislativo dell'Unione o degli Stati membri, la compatibilità tra le finalità dell'uso secondario dei dati e quelle per le quali, invece, gli stessi sono stati raccolti sussiste se, *ex* art. 6, paragrafo 4, del GDPR, il titolare del trattamento, dopo aver soddisfatto tutti i requisiti per la liceità del trattamento originario, tiene anche conto di ogni nesso tra tali finalità e le finalità dell'ulteriore trattamento previsto; del contesto in cui i dati personali sono stati raccolti; delle aspettative dell'interessato, in base alla sua relazione con il titolare del trattamento, sull'ulteriore utilizzo dei dati; della natura dei dati personali; delle conseguenze dell'ulteriore trattamento previsto per gli interessati e dell'esistenza di garanzie adeguate sia nel trattamento originario sia nell'ulteriore trattamento previsto.

In virtù di quanto disposto dal paragrafo 4 dell'art. 9 del GDPR, che con riguardo al trattamento dei dati genetici, biometrici e relativi alla salute, prevede che ogni Stato membro possa mantenere o introdurre ulteriori condizioni, il legislatore italiano con il D.lgs 101/2018, di adeguamento della normativa nazionale al GDPR, ha arricchito il quadro di riferimento europeo, attribuendo al Garante per la Protezione dei Dati Personali il compito di fare luce su alcuni aspetti critici relativi al trattamento dei dati sanitari personali per finalità di ricerca scientifica.

Il Garante, con diversi Pareri, inizialmente aveva ritenuto fosse necessario il consenso, in caso di uso secondario dei dati sanitari personali per finalità di ricerca scientifica e, in un secondo momento, aveva previsto che, nei casi di necessarietà a procedere con una ricerca scientifica retrospettiva, nell'impossibilità di ottenere il consenso del paziente, il ricercatore dovesse ottenere motivato parere favorevole del comitato etico, una valutazione di impatto sulla protezione dei dati (DPIA) ex art. 35 GDPR (la quale è

[3] Cfr. GDPR, *Considerando* n.50.

ritenuta necessaria quando un trattamento "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche") e, infine, dovesse rivolgersi direttamente al Garante stesso tramite lo strumento della consultazione preventiva (art. 36 GDPR).
Con la legge n. 56/2024 (di conversione del D.L. n. 19/2024 cd. "Decreto PNRR bis"), entrata in vigore il 1^ maggio 2024, la consultazione preventiva del Garante scompare come adempimento obbligatorio ritornando a essere, come nelle intenzioni originarie del GDPR, un'attività da compiere solo se, all'esito della valutazione d'impatto permangano rischi residui, che il titolare del trattamento (nella fattispecie il ricercatore) non sia in grado di mitigare mediante l'adozione di adeguate misure di garanzia, così come prescritte dal Garante.
Si evince, quindi, da un lato, la promozione dell'utilizzo di strumenti tecnologicamente avanzati, che grazie all'uso secondario dei dati sanitari personali, possono dare origine a scoperte scientifiche, orientando sempre più l'assistenza sanitaria verso finalità di utilità sociale, dall'altro, la limitazione all'utilizzo generalizzato dei dati da cui possono alimentarsi, per motivi di tutela della *privacy*.
L'utilizzo dei dati sanitari personali per finalità di ricerca scientifica, che rientrano nel novero delle attività per cui si realizza un uso secondario dei dati, in Italia risulta quindi in parte limitato dal legislatore[4].
Nella cornice della normativa di recente conio e sulla scia di quanto anticipato dal GDPR, che già riconosce l'utilizzo secondario dei dati sanitari, si inserisce l'art. 50 del regolamento n. 2025/377 (European Health Data Space, d'ora in avanti EHDS) che delimita l'ambito applicativo soggettivo della normativa, esonerando dagli obblighi stabiliti nel Regolamento per la condivisione dei dati sanitari a fini di uso secondario: a) le persone fisiche, compresi i singoli ricercatori, che detengono o trattano dati sanitari per scopi personali o accademici b) le c.d. microimprese[5], in ragione della limitata capacità organizzativa[6]
La disposizione in esame è chiaramente dettata dalla necessità di evitare di gravare eccessivamente su entità con risorse limitate, scongiurando il rischio di disincentivare la partecipazione alla condivisione dei dati sanitari per scopi di ricerca e innovazione[7].
Ai sensi del diritto europeo per uso "secondario" si intende il riutilizzo dei dati sanitari a fini di ricerca, innovazione, sanità pubblica, definizione delle politiche e medicina personalizzata[8].
I dati sono analizzati con l'obiettivo di individuare le tendenze, sviluppare nuovi trattamenti e migliorare i servizi di assistenza sanitaria. Possono essere riutilizzati da

[4] Per una riflessione su digitalizzazione e tutela della privacy, cfr. da ultimo, ARCURI, *EHDS ed EDS: la tutela della salute migliora attraverso la digitalizzazione della sanità e la ricerca scientifica*, *L'uso secondario dei dati sanitari personali. Il Regolamento (UE) 2025/327 e l'Ecosistema nazionale di dati sanitari*, reperibile sul sito www.altalex.com,
[5] Cfr. art. 2, allegato della Raccomandazione 2003/361/CE della Commissione.
[6] È, tuttavia, consentito agli stati membri di stabilire, nel proprio diritto nazionale, che tali soggetti siano comunque tenuti agli obblighi previsti per i titolati dei dati sanitari,
[7] Cfr. in tal senso, IASELLI, *Le nuove regole per l'uso primario e secondario dei dati sanitari*, Rimini, 2025, p. 72.
[8] Cfr., in questo volume, M. NATALE- O. TROIANO, *L'ambito di applicazione oggettivo e soggettivo del Regolamento (UE) 2025/327 sullo Spazio Europeo dei Dati Sanitari*, § 4, e V.V. CUOCCI, *Uso secondario dei dati sanitari e interesse generale alla ricerca: riflessioni sul Regolamento sullo Spazio Europeo dei Dati Sanitari e sul Regolamento Generale sulla Protezione dei Dati Personali.*
Uso secondario dei dati sanitari e interesse generale alla ricerca: riflessioni sul Regolamento sullo Spazio Europeo dei Dati Sanitari e sul Regolamento Generale sulla Protezione dei Dati Personali, § 2.3.

ricercatori, imprese, organizzazioni di sanità pubblica o prestatori di assistenza sanitaria conformemente al regolamento sullo spazio europeo dei dati sanitari[9].

II. USO E ABUSO DEI DATI SANITARI: I DIVIETI DI UTILIZZO SECONDARIO E L'ART. 54 DELLO SPAZIO EUROPEO DEI DATI SANITARI

La normativa europea tenta di operare un equo contemperamento tra la necessità di promuovere l'innovazione e la tutela dei diritti e delle libertà fondamentali.

In quest'ottica, l'art. 54 del Regolamento EHDS vieta alcune pratiche di uso secondario dei dati sanitari elettronici, in particolare, pratiche discriminatorie e promozionali.

Sotto il primo profilo, è vietato adottare decisioni "pregiudizievoli" ovvero è previsto il divieto di:

a) adottare decisioni, in relazione a una persona fisica o a un gruppo di persone fisiche, per quanto riguarda offerte di lavoro; offrire condizioni meno favorevoli nella fornitura di beni o servizi, compresa l'esclusione di tali persone o gruppi dal beneficio di un contratto di assicurazione o di credito, la modifica dei loro contributi e premi assicurativi o le condizioni dei prestiti, o di adottare altre decisioni, in relazione a una persona fisica o a un gruppo di persone fisiche discriminatorie nei loro confronti sulla base dei dati sanitari ottenuti

b) svolgere attività pubblicitarie o di marketing; sviluppare prodotti o servizi in grado di danneggiare le persone, la sanità pubblica o la società in generale, quali droghe illecite, bevande alcoliche, prodotti del tabacco e della nicotina, armi o prodotti o servizi concepiti o modificati in modo da creare dipendenza o violare l'ordine pubblico o la moralità o causare un rischio per la salute umana;

c) svolgere attività in contrasto con le disposizioni etiche a norma del diritto nazionale.

Sotto un primo profilo, è previsto, quindi, il divieto di utilizzare i dati sanitari per l'adozione di decisioni "pregiudizievoli" ovvero in grado di produrre effetti giuridici, sociali, economici pregiudizievoli o comunque di incidere in modo significativo sulle persone fisiche. In questa prospettiva, sono vietate decisioni pregiudizievoli che afferiscano al mercato del lavoro o la fornitura di beni e servizi, compresa l'esclusione da contratti di assicurazione o la previsione 'discriminatoria" di premi assicurativi o condizioni di accesso al credito, basate su dati sanitari.

Evidente è la preoccupazione di un uso distorto dei dati sanitari da parte di aziende assicurative, finanziarie, bancarie che potrebbero discriminare individui sulla base delle condizioni fisiche[10].

---

[9] Cfr. art. 53 EHDS. L'accesso ai dati sanitari che devono essere messi a disposizione *ex* art. 51 EHDS viene consentito solo se il trattamento è necessario per specifiche finalità di interesse pubblico. Tra queste rientrano la protezione da minacce transfrontaliere, la sorveglianza della sanità pubblica, la garanzia e la qualità dell'assistenza sanitaria, compresi medicinali e dispositivi medici. Viene consentito, dunque, l'uso dei dati sanitari per la definizione delle politiche e attività regolatorie da parte di enti pubblici e organismi dell'Unione Europea. Viene, inoltre, permesso l'uso dei dati per la ricerca scientifica, allo scopo di contribuire al miglioramento della qualità dell'assistenza sanitaria (ciò include attività di sviluppo e innovazione di prodotti e servizi, nonché l'addestramento e la valutazione di algoritmi, in particolari quelli utilizzati nei sistemi di intelligenza artificiale e nelle applicazioni di sanità digitale; in senso quasi testuale, IASELLI, cit., p. 74 s.).

[10] Si ricorderà che con Legge 7 dicembre 2023, n. 193 - *Disposizioni per la prevenzione delle discriminazioni e la tutela dei diritti delle persone, che sono state affette da malattie oncologiche* è stato sancito il c.d. oblio oncologico, ovvero "il diritto delle persone guarite da una patologia oncologica di non fornire informazioni né subire

Sotto un diverso profilo, sono vietate le attività pubblicitarie o di *marketing*, ovvero un uso potremmo definire "promozionale" del dato sanitario, al fine di prevenire, in linea con il GDPR, lo sfruttamento commerciale del dato sanitario, senza un consenso informato e specifico[11].

In ultimo, con una disposizione di chiusura, è vietato lo sviluppo di prodotti o servizi che possano danneggiare le persone o la sanità pubblica, creando dipendenza o comunque violando la moralità o esponendo a rischio la salute umana[12].

Dal novero delle disposizioni che precede, emerge la significativa tutela dell'interessato o gruppi di interessati che potranno agevolmente, in caso di violazione della normativa, (e, anche attraverso la promozione di una *class action*) agire nei confronti del titolare del trattamento o del responsabile del trattamento, senza la necessità di provare dolo o colpa, secondo il modello della responsabilità oggettiva (cfr. infra §VI), chiedendo il riconoscimento di danni economici, come danni legati alla eventuale perdita di opportunità di lavoro, ma anche pregiudizi immateriali, che non comprendono solo la riparazione della violazione della riservatezza, ma anche il danno alla reputazione e il disagio psicologico derivante dalla divulgazione illecita di informazioni mediche e ogni altra forma di pregiudizio non strettamente patrimoniale[13].

III. STRUMENTI PREVENTIVI E RIMEDIALI A TUTELA DELL'INTERESSATO: IL DIRITTO DI ESCLUSIONE

La presente indagine si interroga sull'individuazione di strumenti a tutela dell'interessato, qualora si voglia utilizzare il dato sanitario per uso secondario. Se da un lato, infatti, va riconosciuta la meritevolezza delle finalità di ricerca e di politica sanitaria connesse all'uso "secondario" dei dati sanitari, dall'altro, va tutelato il principio dell'autodeterminazione informativa sancito dal GDPR. In questa prospettiva, si coglie la rilevanza degli strumenti di tutela dell'interessato, declinati in chiave preventiva e rimediale. Sotto il primo profilo, particolarmente significativo è il c.d. diritto di esclusione (c.d. *opt-out*) sancito dall'art. 71 EHDS, che stabilisce il diritto di escludere in qualsiasi momento, senza obbligo di motivazione, il trattamento dei propri dati sanitari personali per l'uso secondario, ai sensi del regolamento. Nel pieno e sostanziale rispetto del principio di autodeterminazione dell'interessato il diritto è reversibile, in qualsiasi momento, ma gli effetti dell'esclusione, nell'ipotesi in cui il diritto sia esercitato, in un secondo momento, si produrranno solo per l'avvenire[14].

---

indagini in merito alla propria pregressa condizione patologica, nei limiti indicati dalla predetta legge, per l'accesso ai servizi bancari, finanziari, di investimento e assicurativi, in sede di indagini sulla salute dei richiedenti un'adozione e per l'accesso alle procedure concorsuali e selettive, al lavoro e alla formazione professionale". (cfr. scheda informativa reperibile all'indirizzo https//www.garanteprivacy.it/temi/sanita-e-ricerca-scientifica/oblio-oncologico).

[11] Secondo un approccio prudente e garantista, Sottolinea tuttavia il rischio che tali restrizioni possano compromettere l'innovazione nel settore sanitario, in particolare per la scoperta di nuovi farmaci e trattamenti personalizzati basati su un grande volume di dati: IASELLI, *Le nuove regole,* cit., p. 76.

[12] Per la trattazione approfondita di tali aspetti, si rinvia a VV. CUOCCI, *Uso secondario dei dati sanitari e interesse generale alla ricerca: riflessioni sul Regolamento sullo Spazio Europeo dei Dati Sanitari e sul Regolamento Generale sulla Protezione dei Dati Personali*, cit., § 2.3.

[13] Cfr. IASELLI, *Le nuove regole*, cit., p. 150.

[14] La limitazione all'uso dei dati sanitari non pregiudicherà, in questo caso, i trattamenti già autorizzati e approvati prima che la persona abbia esercitato il diritto di esclusione (cfr. IASELLI, *Le nuove regole*, cit., p. 96).

La disposizione in esame riporta in capo agli stati membri la responsabilità di garantire un meccanismo di esclusione "accessibile e facilmente comprensibile", contenendo una formulazione, che, da un lato, si spiega con la necessità di "graduare" la procedura anche in rapporto a c.d. soggetti vulnerabili, così da consentire un pieno ed effettivo riconoscimento del diritto di esclusione, che rischierebbe, altrimenti, di tradursi in una mera declamazione formale, in presenza di difficoltà burocratiche o "tecniche" che ne svuotino il contenuto.

D'altro canto, l'assenza di un modello unico di riferimento si presta a generare disomogenità e frammentarietà nell'applicazione del Regolamento, frustrando l'obiettivo di creare uno "Spazio europeo dei dati sanitari", rendendo auspicabile l'adozione di una piattaforma digitale unificata, che consenta ai cittadini di gestire facilmente il consenso e l'esclusione del trattamento dei propri dati sanitari per uso secondario[15].

Lo stesso quadro disomogeneo sembra palesarsi, in relazione all'ulteriore ambito di discrezionalità riconosciuto agli Stati Membri dall'art. 71. È infatti consentito, espressamente a titolo di eccezione, rispetto al diritto di esclusione, che il singolo Stato possa prevedere meccanismi per rendere disponibili i dati per i quali sia stato esercitato il diritto di esclusione, al ricorrere delle seguenti condizioni cumulative ovvero che a) la richiesta provenga da un ente pubblico, un'istituzione o organo dell'Unione Europea o da soggetto incaricato di svolgere compiti di interesse pubblico nel settore sanitario b) che si debbano perseguire finalità specifiche come la protezione della salute pubblica, la gestione di emergenze sanitarie, o la ricerca scientifica per importanti motivi di interesse pubblico c) che i dati sanitari non possano essere ottenuti con mezzi alternativi in modo tempestivo ed efficace.

Il chiaro tenore letterale della norma esclude che sia ravvisabile in capo al singolo Stato membro un obbligo di prevedere tali meccanismi, lasciando alla prerogativa nazionale la possibilità di tutelare, secondo il massimo grado di ampiezza, il principio di autodeterminazione, senza eccezioni al diritto di esclusione.

Come opportunamente osservato, l'esercizio del diritto di esclusione non comporta necessariamente la cancellazione dei dati, che non saranno essere oggetto di trattamenti, finalizzati all'uso secondario, ma non di qualsivoglia trattamento. Il fatto che le disposizioni del regolamento sull'EHDS consentano, in casi eccezionali, l'accesso a tali dati anche a seguito dell'esercitata esclusione, significa che un trattamento, ossia almeno la raccolta e la conservazione, debba comunque avvenire. Di qui le differenze con il diritto alla cancellazione dei dati *ex* art. 17 GDPR. Mentre la cancellazione dei dati determina la cessazione di ogni trattamento di dati e la rimozione degli stessi, l'esclusione non comporta la rimozione dei dati, ma impedisce soltanto alcuni trattamenti di dati[16].

IV. (SEGUE). IL RECLAMO

Il Regolamento in esame mira a tutelare diritti fondamentali e identità dell'interessato, contemplando la possibilità di agire in sede di reclamo dinanzi al responsabile

[15] Cfr. IASELLI, *Le nuove regole*, cit., p. 97.

[16] CORSO, *Lo spazio europeo dei dati sanitari. Prime riflessioni sul Regolamento UE 2025/327*, *Le Nuove Leggi Civili Comm.*, 2025, p. 590.

dell'accesso ai dati sanitari. Resta salva la possibilità di agire in sede giurisdizionale o amministrativa, secondo la logica del doppio binario.

Agli organismi responsabili è rimesso l'obbligo di predisporre strumenti facilmente accessibili per la presentazione dei reclami. Nei *Considerando*[17] si legge che "al fine di agevolare la presentazione dei reclami, ciascuna autorità sanitaria digitale e ciascun organismo di accesso ai dati sanitari dovrebbe adottare misure quali la fornitura di un modulo di presentazione dei reclami compilabile anche elettronicamente, senza escludere la possibilità di utilizzare altri mezzi di comunicazione". Anche per la gestione dei reclami, come per il meccanismo di *opt-out* previsto per l'esercizio del diritto di esclusione *ex* art. 71 EHDS, il Regolamento insiste sull'adozione di meccanismi facilmente accessibili. L'originaria previsione di una doppia istanza, che avrebbe consentito di proporre istanza dinanzi all'Autorità indipendente, solo nell'ipotesi in cui il responsabile dell'accesso ai dati sanitari non avesse dato risposta soddisfacente, è stata eliminata.

Sebbene il sistema del doppio livello di tutela fosse stato accolto da qualcuno con interesse, argomentandosi intorno all'esclusione della necessità di intraprendere iniziative legali e costose, è da ritenere tuttavia che la possibilità "condizionata" (alla proposizione del reclamo dinanzi al Responsabile dell'accesso dei dati) avrebbe rischiato di dilatare oltremodo i tempi necessari per la tutela effettiva della violazione, specie in assenza di un termine massimo per l'adozione della decisione sul reclamo[18].

Tra le criticità sollevate, è stata correttamente evidenziata la difficoltà di gestire un elevato numero di reclami. Per ovviare a tale pericolo, è stata proposta l'adozione di meccanismi di automazione nell'esame delle segnalazioni. In proposito, non può sottacersi che, a livello globale, numerosi ordinamenti stanno sperimentando varie forme di applicazione dell'intelligenza artificiale al sistema giudiziario e si stanno confrontando con le problematiche connesse[19].

L'adozione della decisione, da parte dell'organismo responsabile dell'accesso ai dati sul reclamo, pure estranea all'ambito specificamente giurisdizionale, ha natura decisoria ed è destinata a incidere su diritti fondamentali, presumibilmente violati[20]. Sicché, le perplessità sollevate con riferimento all'ipotesi di un giudice *robot* si estendono anche a tale attività "decisoria". In particolare, si è sostenuta la difficoltà di riprodurre il ragionamento giuridico, che, peraltro, non sembra rappresentare, al momento, l'obiettivo dei sistemi di automazione impiegati in ambito giudiziario. È stato

[17] Cfr. *Considerando*, n. 99.

[18] Cfr. Cfr. IASELLI, *Le nuove regole*, cit., p. 144. Secondo l'a.: "[l]a possibilità di presentare un reclamo direttamente a un organismo responsabile dell'accesso ai dati sanitari garantisce un primo livello di tutela immediata e relativamente agile, riducendo la necessità di intraprendere azioni legali più complesse e costose. [..] il regolamento non specifica con precisione i tempi massimi entro cui l'organismo responsabile dell'accesso ai dati sanitari deve rispondere; il che potrebbe generare ritardi nell'adozione delle misure correttive necessarie. Sarebbe opportuno che il legislatore europeo introducesse termini più stringenti per garantire una gestione tempestiva dei reclami, evitando che le segnalazioni rimangano senza risposta per lunghi periodi". È pur vero che il Regolamento prevede che l'organismo responsabile dell'accesso ai dati sanitari debba informare il reclamante dello stato di avanzamento della gestione del reclamo. Si può ritenere che questi debba comunicare cioè i tempi necessari per la conclusione dell'esame della pratica.

[19] Si pensi, limitatamente all'ambito europeo, all'adozione da parte del Consiglio d'Europa nel dicembre 2018 di una Carta Europea sull'intelligenza artificiale nei sistemi giudiziari e negli ambiti connessi

[20] Cfr. Reg. (UE) 2025 327, art. 81, comma II "L'organismo responsabile dell'accesso ai dati sanitari a cui è stato presentato il reclamo informa il reclamante sui progressi fatti nel trattare il reclamo e sulla decisione adottata".

significativamente affermato che l'intelligenza artificiale sia in grado di tesaurizzare l'esperienza, ma non sia in grado di cogliere l'*aliquid* novi in ogni fattispecie al vaglio del Giudice ovvero la specificità del caso concreto. In altri termini, l'elemento di novità che indurrebbe a un possibile mutamento di indirizzo giurisprudenziale e alla base del pensiero originale dell'interprete non sarebbe "riconoscibile" dall'IA[21].

In più, vi è da aggiungere che, l'affidabilità e la qualità dei modelli futuri di IA potrebbe degradarsi progressivamente, in ragione della loro propensione ad apprendere da dati contaminati in precedenza. Il fenomeno è noto come "*model collapse*" e allude alla circostanza per cui i c.d. "dati puliti" creati da essere umani che, un tempo rappresentavano il tessuto fondamentale del *machine learning*, stanno progressivamente per essere sepolti da strati di contenuti sintetici, che renderanno sempre più difficile addestrare nuovi modelli senza errori ricorsivi[22]. D'altro canto, il richiamo all'obbligo in capo all'organismo responsabile di informare il reclamante sullo stato di avanzamento dell'esame della richiesta è una previsione che si giustifica, escludendo la possibilità di una decisione automatizzata che interverrebbe in tempo reale sul reclamo.

Al fine di garantire l'efficace tutela dei diritti fondamentali è, forse, auspicabile una gestione collettiva del reclamo, con la possibilità di conferire l'incarico a associazioni secondo la gestione della *class action* oppure a un rappresentante a ciò designato.

Nell'intento di garantire una più efficace tutela dei soggetti interessati e qualora la persona fisica ritenga che siano violati i diritti riconosciuti dal Regolamento, è, infatti, contemplata "la possibilità di designare un rappresentante ovvero un'organizzazione o associazione, privi di finalità di lucro, costituti in conformità del diritto nazionale con obiettivi statutari di pubblico interesse e attivi nel settore della protezione dei dati personali"[23] per proporre reclamo innanzi all'Autorità competente.

Dal tenore letterale della norma, che espressamente riconosce alla persona fisica il diritto di "dare mandato a un organismo, organizzazione o associazione" si deduce che il rapporto giuridico tra interessato e rappresentante dovrebbe essere inquadrato in termini di mandato, delineando profili di responsabilità in capo al mandatario, nel caso di inadempienze più o meno gravi (come nel caso, di violazione dell'obbligo di riservatezza e divulgazione dei dati personali).

Il mandato, che può essere proposto anche da più interessati, alla luce della formulazione del Regolamento che riconosce alle persone fisiche e giuridiche di proporre un reclamo "anche collettivamente" a un organismo responsabile dell'accesso ai dati sanitari, potrà essere conferito esclusivamente in favore di un ente "organismo o organizzazione o associazione". Sembrerebbe, dunque, esclusa la possibilità di conferire mandato a favore di una persona fisica, forse in ragione delle maggiori garanzie, in termini di competenza

[21] Cfr. R. MESSINETTI, *Brevi note sulla certezza del diritto nella società algoritmica*, in *Contr. e impr.*, 2024, p. 283 ss.

[22] SHUMAILOV, I., SHUMAYLOV, Z., ZHAO, Y., AI models collapse when trained on recursively generated data, *Nature*, 755–759 (2024); https://doi.org/10.1038/s41586-024-07566-y. Sul tema affine del ruolo dell'IA in ambito sanitario e delle sue criticità applicative, v. CIANCIMINO, *Protezione e controllo dei dati in ambito sanitario e intelligenza artificiale*, Napoli, 2020, p.65 ss.

[23] v. Reg. (UE) 2025/327, art. 101 "Qualora una persona fisica ritenga che siano stati violati i diritti di cui gode a norma del presente regolamento, ha diritto di dare mandato a un organismo, un'organizzazione o un'associazione che non abbiano scopo di lucro, costituiti in conformità del diritto nazionale, con obiettivi statutari di pubblico interesse e attivi nel settore della protezione dei dati personali, per proporre reclamo per suo conto o esercitare i diritti di cui agli artt. 21 e 81"

specifica e solidità patrimoniale che un'organizzazione sembra, almeno apparentemente, offrire. Nel delineare le caratteristiche del mandatario, il Regolamento sembra sorvolare sulla tipologia specifica di ente, soffermandosi invece sulla finalità non lucrativa e sull'obiettivo di pubblico interesse.

Nel panorama nazionale, sarebbe, dunque, chiaro il riferimento agli enti di cui al libro I del codice civile o, comunque, a un ente del c.d. terzo settore[24], esclusa la possibilità di conferire mandato a una struttura societaria con scopo lucrativo, mentre tra le finalità spiccatamente statutarie (interesse pubblico) non è contemplata espressamente la finalità di tutela dei dati personali, ambito in cui il Regolamento si limita a richiedere che i soggetti incaricati "siano attivi".

L'EHDS sembra indifferente all'aspetto strutturale dell'ente, limitando ad esigere determinate finalità. L'esclusione della finalità lucrativa, si può comprendere per il timore di una contaminazione tra diritti e libertà fondamentali della persona che il Regolamento mira a tutelare e un uso improprio dei dati personali che potrebbe degenerare in abuso[25]. La logica "funzionale" adottata dal Regolamento è chiaramente dettata dalla necessità di una protezione efficace e sostanziale dell'interessato, mirando a scongiurare il pericolo di una commercializzazione, se non addirittura mercificazione del dato sanitario, in relazione della profonda connessione con gli aspetti identitari della persona. In questa prospettiva, si comprende la necessità di ristorare adeguatamente il pregiudizio non patrimoniale, nel caso di violazione dell'obbligo di riservatezza, che si ripercuota sulla identità personale. Si possono comprendere agevolmente i danni significativi sull'identità già fragile della persona che sia affetta, a titolo esemplificativo, da malattie mentali, nell'ipotesi in cui fosse violato il divieto di re-identificazione per le inevitabili ricadute sulla vita del paziente, in ragione dello stigma sociale cui sarà soggetto.

---

[24] Sulla distinzione fra enti c.d. "non profit" e "enti for profit", v. per tutti, PONZANELLI, *Gli enti collettivi senza scopo di lucro*, II ed. Torino, 2000 p, 85 s.s.; BASILE, *Le persone giuridiche*, in *Trattato di diritto privato Iudica-Zatti*, Milano, 2003, p. 71 ss. (ivi ulteriori riferimenti bibliografici); si ricorderà che con la legge delega 6 giugno 2016, n. 106 ,« delega al Governo per la riforma del terzo settore, dell'impresa sociale e per la disciplina del servizio civile universale », il legislatore italiano ha inteso riformare la disciplina degli enti non profit con finalità di interesse generale. Successivamente, la legge delega è stata attuata con il d. lgs. 3 luglio 2017, n. 112 « Revisione della disciplina in materia di impresa sociale »: c.d. decreto sull'impresa sociale e con il d. lgs. 3 luglio 2017, n. 117 (« codice del terzo settore »). In argomento, v. R. PATTI, *La disciplina del terzo settore in Italia dopo la riforma: profili ricostruttivi e problemi aperti*, in *Diritto di Famiglia e delle Persone* (Il), 2021, pag. 862 ss. Nel superare la tradizionale riconduzione della disciplina positiva sulle società senza scopo di lucro al novero della eccezione rispetto alla regola della società lucrativa, la riforma del terzo settore appare ispirata al principio della c.d. "neutralità teleologica", della società, dal momento che, al pari dell'associazione e della fondazione, la forma societaria è considerato un puro assetto organizzativo funzionale allo svolgimento di un'attività di impresa di interesse generale (sul punto, cfr. *amplius*, ARRIGONI**,** *La riforma del terzo settore e la nuova disciplina dell'impresa sociale. Alcune implicazioni sistematiche*, in *Riv. soc.*, 2019, p.79 SS.). Secondo il legislatore della riforma sono Enti del terzo settore (cd. ETS) alcuni enti disciplinati in precedenza dalla legislazione speciale (per esempio le organizzazioni di volontariato, le associazioni di promozione sociale e le imprese sociali) e tutti gli altri enti di diritto privato diversi dalle società che, senza scopo di lucro, perseguano finalità civiche, solidaristiche e di utilità sociale, mediante una o più attività di interesse generale e siano iscritti nel registro unico nazionale del terzo settore.

[25] La preoccupazione è colta da IASELLI, *Le nuove regole*, cit., p. 146, al fine di "prevenire abusi nell'uso delle informazioni sanitarie, specialmente da parte di soggetti commerciali o organizzazioni che potrebbero avere interesse a trattare i dati sanitari elettronici per finalità diverse da quelle autorizzate dall'interessato".

V. POTERI DI INDAGINE E SANZIONATORI DELL'ORGANISMO DI ACCESSO AI DATI SANITARI

Nello svolgimento dei compiti di monitoraggio e vigilanza[26], L'EHDS riconosce agli organismi di accesso ai dati sanitari poteri ispettivi e sanzionatori, prevedendo, sotto il primo profilo, il diritto di chiedere e ottenere da utenti e titolari dei dati sanitari, le informazioni necessarie, per verificarne la conformità secondo la normativa in esame.

Sotto il profilo sanzionatorio, gli organismi di accesso ai dati sanitari hanno il potere di revocare l'autorizzazione all'accesso ai dati rilasciata ai sensi dell'articolo 68 EHDS, di interrompere, senza indebito ritardo, l'operazione di trattamento dei dati sanitari elettronici, effettuata dall'utente dei dati sanitari e adottano misure appropriate e proporzionate volte a garantire un trattamento conforme da parte dell'utente dei dati sanitari.

Nell'ambito di tali misure, gli organismi di accesso ai dati sanitari possono anche, ove opportuno "escludere o avviare procedimenti per escludere, in conformità al diritto nazionale, l'utente dei dati sanitari interessato da qualsiasi accesso ai dati sanitari elettronici nell'ambito dell'EHDS nel contesto dell'uso secondario per un periodo massimo di cinque anni"[27].

Il procedimento che conduce all'irrogazione della misura è assistito da particolari garanzie in favore dell'utente (o titolare dati sanitari), in presenza dell'obbligo a carico dell'organismo di accesso di "comunicare senza indugio" le misure adottate, nonché le motivazioni su cui si basano, stabilendo un periodo di tempo ragionevole entro il quale l'utente o il titolare dei dati sanitari dovrà conformarsi a tali misure[28].

Alle misure sanzionatorie citate si accompagnano le sanzioni amministrative pecuniarie irrogabili da parte degli organismi di accesso ai dati sanitari.

---

[26] Cfr. Reg. (UE) 2025/327, art. 57. Cfr. M.I. NIGRO DI GREGORIO – A.P. MANGIACOTTI*, Il sistema sanzionatorio dell'European Health Data Space: tra armonizzazione e frammentazione normativa*, § 1.

[27] Cfr. Reg. (UE) 2025/327, art. 57: "[..]Per quanto riguarda l'inadempienza da parte dei titolari di dati sanitari, qualora un titolare di dati sanitari neghi i dati sanitari elettronici agli organismi di accesso ai dati sanitari con la manifesta intenzione di ostacolare l'uso dei dati sanitari elettronici, o non rispetti i termini di cui all'articolo 60, paragrafo 2, l'organismo di accesso ai dati sanitari ha il potere di comminare al titolare di dati sanitari una sanzione amministrativa pecuniaria per ogni giorno di ritardo, che deve essere trasparente e proporzionata. L'importo delle sanzioni è stabilito dall'organismo di accesso ai dati sanitari in conformità al diritto nazionale. In caso di ripetute violazioni da parte del titolare di dati sanitari dell'obbligo di cooperazione con l'organismo di accesso ai dati sanitari, tale organismo può escludere o avviare un procedimento per escludere, in conformità al diritto nazionale, il titolare di dati sanitari interessato dalla presentazione di domande di accesso ai dati sanitari ai sensi del presente capo per un periodo massimo di cinque anni. Durante il periodo di tale esclusione, il titolare di dati sanitari rimane tenuto a rendere i dati accessibili ai sensi del presente capo, ove applicabile".

[28] Cfr. Reg. (UE) 2025/327, art. 57, par VI e VII. Spiccata rilevanza sarà attribuita allo strumento informatico impiegato per la notifica di tutte le misure di esecuzione adottate agli altri organismi di accesso dei dati sanitari, strumento, la cui architettura informatica sarà definita nell'ambito dell'infrastruttura di HealthData@EU di cui all'articolo 75: " Tutte le misure di attuazione adottate dall'organismo di accesso ai dati sanitari ai sensi del paragrafo 3 sono notificate agli altri organismi di accesso ai dati sanitari tramite lo strumento informatico di cui al paragrafo 7. Gli organismi di accesso ai dati sanitari possono rendere tali informazioni disponibili al pubblico sui propri siti web. La Commissione, mediante atti di esecuzione, definisce l'architettura di uno strumento informatico, nell'ambito dell'infrastruttura di HealthData@EU di cui all'articolo 75, volto a supportare e rendere trasparenti agli altri organismi di accesso ai dati sanitari le misure di esecuzione di cui al presente articolo, in particolare le sanzioni per la reiterazione dell'inadempimento, la revoca delle autorizzazioni e le esclusioni. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 98, paragrafo 2.".

Tra le condizioni per l'irrogazione di una sanzione amministrativa pecuniaria, complementare o sostitutiva delle misure di esecuzione di cui all'articolo 63, paragrafi 3 e 4, EHDS, è previsto che sia "efficace, proporzionata e dissuasiva" in ogni singolo caso.
Tra le condizioni per l'irrogazione di una sanzione amministrativa pecuniaria, complementare o sostitutiva delle misure di esecuzione di cui all'articolo 63, paragrafi 3 e 4, EHDS, è previsto che sia "efficace, proporzionata e dissuasiva" in ogni singolo caso.
Il relativo importo è determinato, limitatamente al caso, in relazione alla natura, entità, durata della violazione e alla condotta dell'autore della violazione. A tal fine viene considerato,

(a) se sono già state irrogate sanzioni o sanzioni amministrative da altre autorità competenti per la stessa violazione;

(b) il carattere intenzionale o negligente della violazione;

(c) qualsiasi azione intrapresa dal titolare dei dati sanitari o dall'utente dei dati sanitari per attenuare il danno causato;

(d) il grado di responsabilità dell'utilizzatore dei dati sanitari, tenendo conto delle misure tecniche e organizzative attuate da tale utilizzatore dei dati sanitari ai sensi dell'articolo 67(2), lettera g), e dell'articolo 67(4);

(e) eventuali precedenti violazioni rilevanti da parte del titolare dei dati sanitari o dell'utente dei dati sanitari;

(f) il grado di cooperazione del titolare dei dati sanitari o dell'utente dei dati sanitari con l'organismo di accesso ai dati sanitari per quanto riguarda la riparazione della violazione e l'attenuazione dei suoi possibili effetti negativi;

(g) le modalità con cui l'organismo di accesso ai dati sanitari è venuto a conoscenza della violazione, in particolare se e in quale misura l'utente dei dati sanitari gli ha notificato la violazione;

(h) la conformità a tutte le misure esecutive di cui all'articolo 63, paragrafi 3 e 4, che sono state ordinate in precedenza nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto;

(i) qualsiasi altro fattore aggravante o attenuante applicabile alle circostanze del caso, quali i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, attraverso la violazione.

L'EHDS determina l'ammontare massimo della sanzione pecuniaria, elevabile nel caso di violazioni ritenute particolarmente gravi, come l'impiego dei dati sanitari per le finalità vietate dall'art. 68; l'estrazione dei dati sanitari da ambienti di elaborazione sicuri; la violazione del divieto di re-identificazione delle persone fisiche cui si riferiscono i dati sanitari; l'inosservanza delle misure di esecuzione *ex* art 63, par. 3 e 4[29].

[29] Cfr. Reg. (UE) 2025/327, art. 64, par. IV e V: "Conformemente al paragrafo 2 del presente articolo, le violazioni degli obblighi del titolare o dell'utilizzatore dei dati sanitari ai sensi dell'articolo 60 e dell'articolo 61, paragrafi 1, 5 e 6, sono soggette a sanzioni amministrative pecuniarie fino a un massimo di 10 000 000 di EUR o, nel caso di un'impresa, fino a un massimo del 2% del suo fatturato mondiale totale annuo dell'esercizio finanziario precedente, se superiore.

Conformemente al paragrafo 2, le seguenti violazioni sono soggette a sanzioni amministrative pecuniarie fino a un massimo di 20 000 000 di EUR o, per un'impresa, fino a un massimo del 4% del suo fatturato mondiale totale annuo dell'esercizio finanziario precedente, se superiore:

(a) utenti di dati sanitari che trattano dati sanitari elettronici ottenuti tramite un'autorizzazione all'immissione in commercio rilasciata ai sensi dell'articolo 68 per gli usi di cui all'articolo 54;

(b) utenti di dati sanitari che estraggono dati sanitari elettronici personali da ambienti di elaborazione sicuri;

VI. IL RISARCIMENTO DEL DANNO FRA FUNZIONE COMPENSATIVA E CURVATURA SANZIONATORIA

Lo strumento di tutela dell'interessato *par exellence*, da esercitare, tuttavia, successivamente alla produzione del danno, è il risarcimento del danno che l'art. 100 del Regolamento riconosce in favore delle persone fisiche e giuridiche che abbiano subito "un danno materiale o immateriale" causato da una violazione dell'EHDS.

Sul piano storico-sistematico, la norma si pone in continuità con l'art. 82 GDPR, a sua volta erede dell'art. 23 dir. 95/46/CE. Pur ribadendo la legittimazione attiva in favore di chiunque lamenti un danno a causa della violazione del regolamento, la norma non limita espressamente la legittimazione passiva "al titolare e al responsabile del trattamento", come il suo antecedente storico[30], consentendo di includere, in linea con l'indicazione offerta dalla lettura del *Considerando* n.101, nel novero degli autori del danno, anche nuovi soggetti come l'autorità di sanità digitale e gli organismi responsabili dell'accesso ai dati sanitari, destinatari di prescrizioni nel Regolamento.

Alla mancata esplicita estensione dei soggetti tenuti al risarcimento, che schiude a una gamma indeterminata e sfuggente di responsabili, si accompagna l'assenza di previsioni sull'eventuale rapporto tra coloro, che, a vario titolo, abbiano violato l'EHDS, sulla eventuale prova liberatoria e sulla solidarietà o meno dell'obbligo risarcitorio, sulla rivalsa e sul foro competente. Tutti questi aspetti sono disciplinati dall'art. 82 GDPR[31], circostanza che rende ancora più complessa e ambiziosa l'opera dell'interprete che dovrà necessariamente conformarsi con l'attività della Corte di Giustizia europea, come indicato dal *Considerando* n.101.

In più occasioni, si è segnalato che, specie nelle ipotesi in cui il legislatore europeo intervenga con lo strumento dell'uniformazione, ovvero con l'adozione di regolamenti, eventuali vuoti di disciplina non potrebbero essere colmati, facendo ricorso a regole, principi o moduli interpretativi desunti dai singoli ordinamenti nazionali, il cui richiamo condurrebbe inevitabilmente a un esito di frammentazione, opposto all'esigenza, sottesa all'adozione di regolamenti, di uniformazione[32].

In questa prospettiva, la disciplina dell'EHDS, nel solco della regolamentazione del GDPR, si presta a rappresentare un significativo tassello, nella costruzione di un sistema eurounitario della responsabilità civile[33]. Tuttavia, nell'edificazione di uno statuto unionale

(c) reidentificare o tentare di reidentificare le persone fisiche a cui si riferiscono i dati sanitari elettronici ottenuti dagli utenti dei dati sanitari sulla base di un'autorizzazione dati o di una richiesta di dati sanitari ai sensi dell'articolo 61(3);

(d) inosservanza delle misure di attuazione adottate dall'organismo di accesso ai dati sanitari ai sensi dell'articolo 63(3) e (4).

30 Cfr. art. 82 GDPR

31 CORSO, *Lo spazio europeo dei dati sanitari*,cit, p. 592.

32 SCOGNAMIGLIO, *Danno e risarcimento nel sistema del Rgpd: un primo nucleo di disciplina eurounitaria della responsabilità civile?,* in *Nuova giur. civ.*, II, p. 1152; sul punto anche, PAGLIANTINI, *Un altro palcoscenico della guerra tra le Corti: il danno (immateriale) bagatellare dell'art. 82 GDPR,* nota a Corte Giust. UE, 4 maggio 2003, causa C-300/21, in *Foro it.,* 2023, 286 s.; sulla necessità di escludere l'applicazione delle categorie della responsabilità civile proprie del diritto nazionale, sul presupposto che in esame sia una norma di diritto eurounitario: CORSO, *Lo spazio europeo dei dati sanitari*,cit, p. 594.

33 "Costituisce un assunto sufficientemente condiviso quello secondo il quale, in materia di responsabilità civile, l'incidenza della regolazione di fonte eurounitaria si presenta assai meno significativa di quanto non

della responsabilità civile, non si potrebbe prescindere dal riferimento alle categorie nazionali. Lo stesso art. 100 EHDS prevede che il risarcimento del danno sia sancito conformemente "al diritto dell'Unione e nazionale", suggerendo la necessaria contaminazione fra le categorie giuridiche nazionali e eurounitarie e confermando la lettura della più autorevole dottrina che sostiene l'opportunità di muovere dagli ordinamenti giuridici nazionali per l'opera di concettualizzazione giuridica nella cornice euro-unitaria[34].

Quanto alla natura della responsabilità, il tenore letterale della norma sembrerebbe suggerire la rilevanza oggettiva della violazione del Regolamento, svincolato da criteri di imputazione, che, pure articolati, secondo la tecnica dell'esimente, sono previsti nell'art. 82 GDPR[35], ma non risultano riprodotti nell'art. 100 EHDS. Si potrebbe trarre in proposito l'idea della natura oggettiva della responsabilità nel caso di uso (primario e secondario) dei dati sanitari, a differenza del modello di responsabilità adottato dal GDPR, che presupporrebbe un'attività pericolosa, solo in via eventuale.

La pericolosità del trattamento dei dati personali, nell'ottica del GDPR sarebbe solo eventuale e non sistematica, come emerge, dalla regola che prevede che un rischio elevato possa talvolta emergere, a seguito di valutazione d'impatto (art. 35 e 36 GDPR). L'uso dei dati sanitari sarebbe declinato, invece, in termini di attività pericolosa[36].

D'altro canto, l'eventuale qualificazione in termini di attività pericolosa non esime dalla prova del danno, che non può ritenersi *in re ipsa* assorbita dalla violazione della norma regolamentare. In tale direzione si è espressa, la Corte di Giustizia Europea con riferimento alla fattispecie contemplata dall'art. 82 GDPR[37], le cui considerazioni possono essere estese all'ipotesi di responsabilità prevista dall'art. 100 EHDS. Sarebbero, dunque, tre i presupposti per accordare io risarcimento del danno: la violazione delle disposizioni del Regolamento, il nesso di causalità tra la stessa e il danno, il danno stesso. A conferma di tale conclusione, la Corte di giustizia ha richiamato l'argomento letterale, ovvero la distinzione tra violazione del regolamento e danno, nella previsione regolamentare, altrimenti superflua, e l'argomento sistematico, ovvero la presenza di ulteriori tecniche rimediali, con finalità punitiva, svincolate dal requisito del danno.

Il danno rilevante per attingere al rimedio risarcitorio potrà essere anche immateriale, indipendentemente dal raggiungimento di una determinata soglia di gravità. Coerentemente con la necessità di ricostruire la nozione di danno all'interno della cornice eurounitaria, sostenuta dallo stesso *Considerando* n.101[38], che suggerisce di far ricorso alla nozione ampia di danno elaborata dalla Corte di Giustizia europea, non è previsto un

sia dato constatare in altre aree della legislazione di diritto privato, a cominciare dal diritto dei contratti" (così, SCOGNAMIGLIO, *Danno e risarcimento*, cit., p. 1150).

[34] Cfr. PARADISO, *Il risarcimento del danno. Verso un sistema di responsabilità civile europea*?, in *Danno e resp.*, p. 305, nt. 13, ove riferimenti ai contributi di Falzea e Castronovo.

[35] Cfr. SALANITRO, *Illecito trattamento dei dati personali e risarcimento del danno nel prisma della Corte di Giustizia*, in *Riv. dir. civ.,* 2023, p. 433.

[36] Cfr. SALANITRO, *Illecito trattamento*, cit., p. 445.

[37] Cfr. Corte Giust., UE, 4 maggio 2023, causa C-300/21, in *Foro it.*, 2023, c.286 ss.

[38] Cfr. *Considerando* EHDS, n. 102: "Per rafforzare il rispetto delle norme del presente regolamento dovrebbero essere imposte sanzioni, comprese sanzioni amministrative pecuniarie, per violazione del regolamento, in aggiunta o in sostituzione di misure appropriate imposte dagli organismi responsabili dell'accesso ai dati sanitari ai sensi del presente regolamento. L'imposizione di sanzioni, comprese sanzioni amministrative pecuniarie, dovrebbe essere soggetta a garanzie procedurali appropriate in conformità dei principi generali del diritto dell'Unione e della Carta dei diritti fondamentali dell'Unione europea, inclusi l'effettiva tutela giurisdizionale e il giusto processo".

filtro selettivo del danno non patrimoniale, incentrato sul superamento di una determinata soglia di gravità, circostanza che schiude la prospettiva del risarcimento dei danni c.d. bagatellari[39].

Rimane dubbia la riconoscibilità di risarcimenti ultra-compensativi, che solleva il quesito dell'ammissibilità dei risarcimenti punitivi e, in ultima analisi, delle funzioni della responsabilità civile nella cornice eurounionale. Se da un lato l'argomento letterale, dedotto dalla lettura dei *Considerando*, milita nel senso del riconoscimento di una funzione esclusivamente compensativa della responsabilità civile, stabilendo che le persone fisiche dovrebbero ottenere un risarcimento "pieno ed effettivo" del danno subito, sempre dalla lettura dei *Considerando*, si evince la presenza di un invito a imporre sanzioni "al fine di rafforzare l'applicazione delle norme del presente regolamento, comprese sanzioni amministrative pecuniarie, per qualsiasi violazione del presente regolamento, in aggiunta o in sostituzione delle misure appropriate imposte dagli organismi preposti all'accesso ai dati sanitari ai sensi del presente regolamento", lettura di per sé compatibile con una curvatura sanzionatoria del rimedio risarcitorio, nonostante l'iniziale divaricazione tra l'irrogazione di sanzioni amministrative, indipendenti dalla produzione del danno, e rimedi risarcitori ancorati alla ricorrenza del danno.

Come opportunamente segnalato da più voci, lo statuto unionale della responsabilità civile è in divenire e procede di pari passo con la costruzione di un articolato sistema di tutela dell'interessato, che offre mezzi di tutela esercitabili ex ante (come il diritto *opt-out*), nonché strumenti rimediali e risarcitori, accanto a una serie di sanzioni, declinabili anche in chiave pecuniaria.

A fondamento della tutela dell'interessato, si coglie la centralità della lesione alla riservatezza e all'identità della persona, che opera, evidentemente, nella direzione di escludere l'assimilazione tra persona e dati sanitari. La tutela dell'identità personale[40], declinabile in molteplici sfumature, opera con tutta evidenza, oltre che in chiave positiva, tutelando il patrimonio identitario della persona (nella direzione della tutela della propria identità sessuale, della propria storia, anche familiare, e delle proprie scelte di vita) anche in chiave negativa, escludendo il carattere identitario della malattia nell'individuazione del significato unico e più profondo della persona[41].

In questa prospettiva, sempre più manifesto è il mutamento del ruolo del diritto, chiamato a tutelare non tanto ciò che l'individuo è, nella percezione sociale, ma ciò che sente e sceglie di essere, pure nella necessaria ottica di bilanciamento con la tutela di interessi generali, come la prevenzione e la salute pubblica[42].

---

[39] Cfr. Corte Giust. UE 20 giugno 2024, causa riunite C-182/22 e C-189/22; Corte Giust. UE 14 dicembre 2023, causa C-456/22

[40] Si ricorderà il caso Veronesi, ovvero la storica sentenza degli anni Ottanta, all'origine del riconoscimento giurisprudenziale del diritto alla tutela della identità personale. In questo caso fu accertato che un inserto pubblicitario aveva usato indebitamente il nome dell'oncologo Veronesi, distorcendo il patrimonio culturale e professionale, l'"immagine" nella proiezione sociale, del noto medico (Cass. 22 giugno 1985, n. 3769, in *Foro it.*, 1985, I, 2211). Sul contenuto del diritto all'identità personale, v. PINO, *Il diritto all'identità personale. Interpretazione costituzionale e creatività giurisprudenziale*, Bologna, 2003.

[41] "Io non sono la mia malattia" è lo slogan ricorrente nei titoli di numerosi libri e diffusa da diverse associazioni che la utilizzano per campagne di sensibilizzazione e per dare voce ai pazienti. Tale messaggio intende affermare che l'identità di una persona va oltre la propria condizione di salute ed esprime un atto di ribellione contro la tendenza a categorizzare le persone, unicamente in relazione alle loro malattie.

[42] Tale passaggio è avvertito in particolare, nelle più recenti applicazioni giurisprudenziali, che hanno riconosciuto la tutela dell'identità di genere, ovvero quella auto-percepita dalla persona, pure in presenza di

un disallineamento tra il sesso biologico, attribuito alla nascita su base morfologico-genotipica, e l'identità sessuale, percepita dall'individuo nello sviluppo della sua personalità. La giurisprudenza costituzionale, cosi, ha riconosciuto la rettificazione di stato civile prevista dalla l. 164/1982 non solo nel caso di intervento chirurgico demolitorio o ricostruttivo di modifica dei caratteri sessuali, "purché la serietà ed univocità del percorso scelto e la compiutezza dell'approdo finale siano oggetto di accertamento anche tecnico in sede giudiziale", escludendo la sufficienza dell'elemento volontaristico (cfr. Corte Cost., 5 novembre 2015, n. 221; Corte Cost., 13 luglio 2017, n. 180). In relazione al riconoscimento di un terzo genere, va osservato, che non pochi ordinamenti europei – da ultimo quello tedesco, con la recente legge sull'autodeterminazione in materia di registrazione del sesso («*Gesetz über die Selbstbestimmung in Bezug auf den Geschlechtseintrag SBGG*») – hanno riconosciuto e disciplinato l'identità non binaria e la Corte costituzionale belga ha censurato la delimitazione binaria della disciplina legislativa della transizione di genere, stigmatizzando l'ingiustificata disparità di trattamento fra chi sente di appartenere al sesso maschile o femminile e chi invece non si identifica in alcuno dei predetti generi (arrêt n° 99/2019 del 19 giugno 2019). Lo stesso diritto dell'Unione europea, pur con segnali contraddittori, da tempo sembrerebbe evolvere in tal senso, e infatti, per favorire la circolazione dei documenti pubblici tra gli Stati membri, il regolamento (UE) 2016/1191 del 6 luglio 2016, che promuove la libera circolazione dei cittadini semplificando i requisiti per la presentazione di alcuni documenti pubblici nell'Unione europea e che modifica il regolamento (UE) n. 1024/2012, presenta moduli standard recanti alla voce «sesso» non due diciture, ma tre, «femminile», «maschile» e «indeterminato». Nonostante tali indicazioni, la Corte Costituzionale ha ritenuto, tuttavia, di non riconoscere un terzo genere di identità (non binaria), ai fini della registrazioni di stato civile, lasciando il relativo compito di intervenire eventualmente, al legislatore, "primo interprete della sensibilità sociale".(cfr. Cass., 23 luglio 2024, n. 143).