LA RESPONSABILITÀ CIVILE DEI SOGGETTI CHE OPERANO NEGLI SPAZI DI CONDIVISIONE DEI DATI SANITARI SECONDO IL REGOLAMENTO EHDS.

Di Stefano Faillace

SOMMARIO*: 1. Lineamenti generali della disciplina prevista dal Regolamento EHDS. – 2. La responsabilità civile all'interno dell'architettura per la condivisione di dati sanitari disegnata dal regolamento EHDS. – 3. Segue. I profili patologici della relazione tra il data user e l'Organismo di accesso ai dati sanitari.*

ABSTRACT. *Il Regolamento UE n. 327/2025 istituisce lo Spazio Europeo dei Dati Sanitari (EHDS) per facilitare l'accesso e la condivisione dei dati sanitari nell'Unione Europea, rafforzando i diritti dell'interessato nell'uso primario e prevedendo organismi pubblici responsabili dell'autorizzazione e del controllo dell'accesso ai dati per l'uso secondario. In tale sistema, l'art. 100 del regolamento disciplina la responsabilità civile, riconoscendo il diritto al risarcimento per danni materiali e immateriali derivanti da violazioni di tale norma. Si tratta di una disposizione generica e lacunosa, che rinvia al diritto nazionale e unionale, creando il rischio di applicazioni non uniformi tra Stati membri. In assenza di una disciplina dettagliata, al fine di garantire coerenza applicativa, un ruolo centrale nell'interpretazione sarà svolto dalla Corte di Giustizia dell'Unione Europea.*

Regulation (EU) n.327/2025 establishes the European Health Data Space (EHDS) with the objective of facilitating access to and the sharing of health data within the European Union. It enhances data subjects' rights in relation to the primary use of health data and provides for the establishment of public bodies responsible for authorising and supervising access to data for secondary use. Within this framework, Article 100 of the Regulation sets out the rules on civil liability, expressly recognising the right to compensation for both material and non-material damage arising from infringements of its provisions. However, the provision is formulated in broad and indeterminate terms. It refers to national and EU law for the definition of the applicable conditions and modalities of redress, thereby creating the potential for divergent interpretations and uneven levels of protection among Member States. In the absence of a comprehensive harmonised framework, the Court of Justice of the European Union is likely to play a pivotal role in clarifying the scope, conditions, and practical implications of the liability regime, thereby ensuring uniformity and coherence in its application across the Union.

ISSN 2239-8570

1. Lineamenti generali della disciplina prevista dal Regolamento EHDS.

Il Regolamento UE n. 327/2025, di recente entrato in vigore[1], è nato con l'obiettivo di facilitare l'accesso e la condivisione dei dati sanitari all'interno dell'Unione Europea[2]. L'idea del legislatore europeo è maturata sulla base di esperienze pregresse, episodiche ma determinanti, che hanno dimostrato l'efficacia per la salute collettiva dello sviluppo di piattaforme di dati sanitari[3].

La disciplina prevista da questo nuovo regolamento consentirà ai pazienti di accedere ai propri dati sanitari in formato elettronico, anche se generati in uno Stato membro diverso da quello di residenza, e permetterà agli operatori sanitari di consultare le cartelle cliniche dei propri pazienti, previo loro consenso, anche da altri Paesi dell'Unione europea, facilitando così la continuità delle cure. Viene regolamentato il ruolo del fornitore di servizi di condivisione di dati, i formati che garantiscono la portabilità dei dati sanitari, le norme di cooperazione per l'altruismo dei dati nel settore sanitario e l'accesso a dati privati per l'uso secondario. L'EHDS fornisce regole *standard*, infrastrutture e un quadro di *governance* sia per l'uso primario (l'utilizzo di dati sanitari elettronici personali per fornire servizi all'individuo)[4], che per l'uso secondario dei dati sanitari (l'utilizzo di dati sanitari elettronici per esigenze più ampie come la ricerca sanitaria o le poli-

[1] È stato pubblicato nella Gazzetta ufficiale dell'Unione Europea in data 5 marzo 2025.

[2] Per un approfondimento sul Regolamento EHDS, mi si consenta il rinvio a S. FAILLACE, *Prospettive civilistiche in ordine agli spazi di condivisione di dati sanitari alla luce del Regolamento EHDS*, Milano, 2025. Vedi anche A. MORACE PINELLI (a cura di) *Sanità digitale. Regolamento "EHDS" (UE 2025/327) sullo spazio europeo dei dati sanitari. I Uso dei dati e assetti organizzativi*, Pisa, 2025; C. DE MENECH e M. FOGLIA (a cura di), *Autodeterminazione, cura e ricerca nell'era digitale*, Torino, 2026; S. CORSO, *Autodeterminazione e dati sanitari*, Torino, 2025; S. CORSO, *Lo spazio europeo dei dati sanitari. Prime riflessioni sul Regolamento UE 2025/327*, in *Nuove leggi civ. comm.*, 2025, 563 ss.; S. SLOKENBERGA, K. Ó CATHAOIR, M. SHABANI, *The European Health Data Space. Examining A New Era in Data Protection*, Abingdon-New York, 2025. Sulla proposta di Regolamento, vedi M. SHABANI, *Will the European Health Data Space change data sharing rules?* in *Science,* 2022, 1357 ss., consultabile in *https://doi.org/10.1126/science.abn4874*; I. RAPISARDA, *Sul costituendo spazio europeo dei dati sanitari*, in *Resp. medica*, 2023, 413 ss.; P. TERZIS e E. SANTAMARIA ECHEVERRIA, *Interoperability and governance in the European Health Data Space regulation*, in *Medical Law International*, in *journals.sagepub.com*, 24 aprile 2023. In tema, vedi pure F. CASCINI e A. ARCURI, *Uso secondario dei dati personali relativi alla salute: panoramica della normativa europea e nazionale*, in *Dir. inform.*, 2024, 837 ss.

[3] Ci si riferisce alla *European COVID-19 Data Platform*, ossia la piattaforma europea di dati sul COVID-19, che ha avuto lo scopo, a far data dall'aprile 2020 e su iniziativa della Commissione Europea, all'interno del piano d'azione «ERAvsCorona Action Plan», di consentire la rapida raccolta e condivisione dei dati di ricerca disponibili per apprestare le migliori soluzioni sul piano terapeutico ed epidemiologico.

[4] Secondo l'art. 1 lett. d) del Regolamento EHDS, si intende, per «uso primario», il trattamento dei dati sanitari elettronici per la prestazione di assistenza sanitaria, al fine di valutare, mantenere o ripristinare lo stato di salute della persona fisica cui si riferiscono tali dati, comprese la prescrizione, la dispensazione e la fornitura di medicinali e dispositivi medici, nonché per i pertinenti servizi sociali, amministrativi o di rimborso.

ISSN 2239-8570

tiche pubbliche)[5]. Il diritto dell'Unione impone, quindi, alle autorità nazionali degli Stati membri di cooperare nella gestione e nello scambio dei dati sanitari, al fine di assicurare un livello coerente ed elevato di protezione delle persone fisiche e rimuovere gli ostacoli alla circolazione dei dati sanitari all'interno dell'Unione, creando un livello di protezione dei diritti e delle libertà equivalente in tutti gli Stati membri.

Il Legislatore unionale rafforza, pertanto, il controllo dei pazienti sui propri dati e stabilisce norme per i sistemi di cartelle cliniche elettroniche, al fine di promuoverne l'affidabilità, la sicurezza e l'interoperabilità e consentire lo scambio per uso primario dei dati dei pazienti attraverso la piattaforma europea LaMiaSalute@UE (MyHealth@EU)[6].

Per quel che concerne l'uso primario dei dati sanitari elettronici, nello specifico, il Regolamento EHDS prevede l'integrazione e il potenziamento di diritti dell'interessato, quali il diritto di accesso, il diritto alla portabilità, il diritto di rettifica, il diritto di inserimento di dati sanitari elettronici[7].

Nello scenario progettato dal legislatore europeo con riferimento all'uso secondario, invece, i titolari dei dati dovranno mettere a disposizione i dati in loro possesso ad un Organismo di accesso ai dati sanitari, sulla base di un'autorizzazione o di una richiesta inoltrata da un utente dei dati[8].

---

[5] Secondo l'art. 1 lett. e) reg. EHDS, per «uso secondario dei dati sanitari elettronici», si intende il trattamento dei dati sanitari elettronici per le finalità indicate al capo IV del presente regolamento, che sono diverse dalle finalità iniziali per le quali tali dati sono stati raccolti o prodotti.

[6] Quest'ultima è un'infrastruttura volontaria, già esistente ed attualmente funzionante in undici stati membri (tra cui l'Italia), attraverso cui gli Stati membri offrono alle persone fisiche la possibilità di condividere i loro dati sanitari elettronici personali con prestatori di assistenza sanitaria in occasione di viaggi all'estero. Secondo il Considerando n. 33, Reg. EHDS, per sostenere ulteriormente tali possibilità, la partecipazione degli Stati membri a LaMiaSalute@UE (*MyHealth@EU*) quale stabilita dal presente regolamento dovrebbe essere obbligatoria. Gli Stati membri dovrebbero essere tenuti ad aderire a LaMiaSalute@UE (*MyHealth@EU*), rispettarne le specifiche tecniche e provvedere al collegamento di prestatori di assistenza sanitaria, comprese le farmacie, in quanto ciò è necessario per consentire alle persone fisiche di esercitare i propri diritti ai sensi dal presente regolamento ad accedere ai propri dati sanitari elettronici personali e a utilizzarli indipendentemente dallo Stato membro in cui si trovano.

[7] Cfr. S. FAILLACE, *I diritti dell'interessato nell'uso primario dei dati sanitari elettronici secondo il nuovo Regolamento EHDS*, in *Contratto e impresa*, 2025, 379 ss.; e, con riferimento specifico alla portabilità, vedi F. BRAVO, *Intermediazione di dati sanitari e diritto alla portabilità*, in A. MORACE PINELLI (a cura di), *Sanità digitale. Regolamento "EHDS" (UE 2025/327) sullo spazio europeo dei dati sanitari. I Uso dei dati e assetti organizzativi*, Pisa, 2025, 36 ss.; F. BRAVO, *L'intermediazione dei dati e la sua evoluzione dal settore privato a quello pubblico / Data intermediation and its evolution from the private to the public sector*, in *Riv.it. inf. dir.*, 2025, 17 ss.

[8] A tal proposito, il Considerando n. 59 del Reg. EHDS ricorda, che «i soggetti pubblici o privati ricevono spesso finanziamenti pubblici, da fondi nazionali o dell'Unione, per raccogliere e trattare dati sanitari elettronici per la ricerca, le statistiche sia ufficiali che non ufficiali, o altre finalità simili, anche in ambiti in cui la raccolta di tali dati è frammentata o difficile, quali quelli relativi alle malattie rare o al cancro. Tali dati, raccolti e trattati dai titolari dei dati sanitari con il sostegno di finanziamenti pubblici nazionali o dell'Unione, dovrebbero essere messi a disposizione degli organismi responsabili dell'accesso ai dati sanitari al fine di massimizzare l'impatto dell'investimento pubblico e sostenere la ricerca, l'innovazione, la sicurezza dei pazienti o la definizione delle politiche, a beneficio della società». Si intende per «titolare dei dati sanitari», una persona fisica o giuridica, un'autorità

ISSN 2239-8570

Quest'organo decide di concedere l'accesso ai dati sanitari solo se la finalità descritta nella domanda è tra quelle considerate lecite dal regolamento[9]; se i dati richiesti sono necessari, adeguati e proporzionati alle finalità descritte; se il richiedente possiede competenze adeguate, proponendo misure tecniche e organizzative sufficienti per prevenire l'uso improprio dei dati e per tutelare i diritti e gli interessi del titolare dei dati e delle persone fisiche interessate.

Gli organismi responsabili di accesso ai dati sanitari (ai sensi degli art. 66 e 67, reg. EHDS) decidono se i dati debbano essere resi accessibili in forma anonimizzata o pseudonimizzata, sulla base di una valutazione approfondita dei motivi addotti dal richiedente. Poi, a loro volta, tali organismi richiedono i dati sanitari elettronici ai titolari; trattano i dati sanitari elettronici; monitorano e vigilano sul rispetto delle prescrizioni stabilite nel regolamento da parte degli utenti e dei titolari di dati sanitari; mettono, infine, i dati sanitari elettronici pertinenti a disposizione degli utenti in un ambiente di trattamento sicuro e conservandoli per il periodo stabilito nell'autorizzazione concessa. Nel fornire l'accesso a una serie di dati, anonimizzata o pseudonimizzata, l'organismo per l'accesso ai dati sanitari deve poi utilizzare tecnologie e norme all'avanguardia, garantendo per quanto possibile che le persone fisiche non possano essere reidentificate dagli utenti dei dati sanitari[10].

---

pubblica, un'agenzia o un altro organismo del settore dell'assistenza sanitaria o delle cure assistenziali, compresi, ove necessario, i servizi di rimborso, nonché una persona fisica o giuridica che sviluppi prodotti o servizi destinati al settore sanitario, dell'assistenza sanitaria o delle cure assistenziali, sviluppi o fabbrichi applicazioni per il benessere, svolga attività di ricerca in relazione al settore dell'assistenza sanitaria o delle cure assistenziali o funga da registro della mortalità, nonché un'istituzione, un organo o un organismo dell'Unione che abbia: i) il diritto o l'obbligo, conformemente al diritto dell'Unione o nazionale applicabile e in qualità di titolare o contitolare del trattamento, di trattare dati sanitari elettronici personali per la prestazione di assistenza sanitaria o cure assistenziali o a fini di sanità pubblica, rimborso, ricerca, innovazione, definizione delle politiche, statistiche ufficiali o sicurezza dei pazienti o a fini di regolamentazione; o ii) la capacità di rendere disponibili dati sanitari elettronici non personali, mediante il controllo della progettazione tecnica di un prodotto e dei servizi correlati, anche in termini di registrazione, fornitura, limitazione dell'accesso o scambio. Alla definizione di «titolare dei dati», francamente troppo estesa, ne corrisponde una altrettanto ampia di «utente dei dati sanitari», indicato come una persona fisica o giuridica, comprese le istituzioni, gli organi o gli organismi dell'Unione, cui è stato concesso l'accesso legittimo ai dati sanitari elettronici ai fini dell'uso secondario in virtù di un'autorizzazione ai dati, di un'approvazione di una richiesta di dati sanitari o di un'approvazione di accesso da parte di un partecipante autorizzato alla piattaforma DatiSanitari@UE (HealthData@EU) (reg. EHDS art. 2 lett. u).

[9] Le finalità per le quali i dati sanitari possono essere trattati per usi secondari (cfr. art. 53 del Regolamento EHDS) riguardano compiti svolti da organismi pubblici, quali l'esercizio di funzioni pubbliche, compresi la sorveglianza sanitaria pubblica, i compiti di pianificazione e comunicazione, l'elaborazione delle politiche sanitarie, la garanzia della sicurezza dei pazienti, la qualità dell'assistenza e la sostenibilità dei sistemi sanitari, la ricerca scientifica.

[10] Quando rilascia un'autorizzazione ai dati, l'organismo per l'accesso ai dati sanitari stabilisce le condizioni generali applicabili all'utente dei dati sanitari. L'autorizzazione ai dati deve contenere i seguenti elementi: (a) le categorie, la specifica e il formato dei dati sanitari elettronici a cui accedere contemplati dall'autorizzazione ai dati, comprese le relative fonti e, l'eventuale indicazione che l'accesso ai dati sanitari elettronici dovrà essere effettuato in forma pseudonimizzata nell'ambiente di trattamento sicuro; b) una descrizione dettagliata

2. La responsabilità civile all'interno dell'architettura per la condivisione di dati sanitari disegnata dal regolamento EHDS

A fronte di tale disciplina piuttosto complessa e multiforme, in caso di violazione dei precetti ivi previsti, accanto alla previsione di sanzioni amministrative, vi è una norma che regola la responsabilità civilistica, l'art. 100, che, inevitabilmente, dovrà essere confrontata con quanto previsto dalla norma omologa di cui all'art. 82, GDPR. Essa afferma 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». Per quanto riguarda l'ambito di applicazione soggettivo, balza subito all'occhio la presenza della persona giuridica, quale soggetto suscettibile di subire un danno. Il regolamento EHDS, del resto, prevede una serie di obblighi di condotta o prescrizioni che, direttamente o indirettamente, tutelano pure gli utenti dei dati sanitari e i titolari di dati sanitari, che ben possono essere persone giuridiche, che si rapportano con l'Organismo di accesso ai dati sanitari o l'autorità sanitaria digitale, e subire un pregiudizio da un comportamento scorretto o in conseguenza della violazione di una norma da parte di quest'ultimi[11].

L'art. 100, reg. EHDS, poi, a differenza di quanto previsto nel GDPR, non individua esplicitamente i soggetti su cui grava l'obbligo risarcitorio. Il Considerando n. 101, all'uopo, soccorre l'interprete, precisando che a risarcire i danni dovrebbero essere «l'autorità di sanità digitale, l'organismo responsabile dell'accesso ai dati sanitari, il titolare dei dati sanitari o l'utente dei dati sanitari»[12]. Viene però da chiedersi se tale elencazione vada consi-

della finalità della messa a disposizione dei dati sanitari elettronici; c) qualora sia previsto un meccanismo di attuazione di un'eccezione e questo sia applicabile a norma dell'articolo 71, paragrafo 4, informazioni che indichino se è stata applicato e il motivo della relativa decisione; d) l'identità delle persone autorizzate, in particolare l'identità del ricercatore principale, con il diritto di accedere ai dati sanitari elettronici nell'ambiente di trattamento sicuro; e) durata dell'autorizzazione ai dati; f) informazioni sulle caratteristiche tecniche e sugli strumenti a disposizione dell'utente dei dati sanitari nell'ambiente di trattamento sicuro; g) tariffe a carico dell'utente dei dati sanitari; h) eventuali condizioni specifiche.

[11] Una questione molto complessa da valutare è se le regole del regolamento EHDS si applichino anche alla responsabilità derivante dai danni provocati dai sistemi di cartelle cliniche elettroniche e dai *software* collegati, le quali sono considerate rischiose per la salute, la sicurezza, i diritti delle persone fisiche, la protezione dei dati personali. Sorge in particolare il problema se, rispetto a questo corpo normativo, le regole di responsabilità vadano integrate dal GDPR ovvero dalla disciplina della responsabilità del produttore, la quale ultima, pur essendo posta da una direttiva europea, sul piano delle fonti è disciplina nazionale. Il problema si pone perché la disciplina del regolamento EHDS disciplina direttamente la fabbricazione e la messa in circolazione di questo prodotto elettronico, imponendo al fabbricante di adottare le misure appropriate per garantire che il sistema non metta a rischio dati e persone. (Cfr., in argomento U. SALANITRO, *La tutela risarcitoria tra GDPR e EHDS: appunti per una ricerca*, in A. MORACE PINELLI (a cura di), *Sanità digitale. Regolamento "EHDS" (UE 2025/327) sullo spazio europeo dei dati sanitari I Uso dei dati e assetti organizzativi*, Pisa, 2025, 381 ss.

[12] Come noto, al fine di accertare le responsabilità per un eventuale trattamento di dati sanitari non conforme, occorre individuare preliminarmente il titolare del trattamento, nella de-

ISSN 2239-8570

derata o meno esaustiva, considerato che la stessa trascura di menzionare diversi altri soggetti che potrebbero commettere una violazione del Reg. 2025/327/UE, quali, per esempio, i professionisti sanitari (considerati come persone fisiche nell'ambito dell'uso primario dei dati) o i produttori di cartelle cliniche elettroniche e applicazioni per il benessere[13].

Vista la mancanza di un qualsiasi accenno alla natura della responsabilità, si ripropongono in questa sede alcuni interrogativi sulla medesima già venuti alla luce per l'art. 82 GDPR[14]. Ciò consapevoli del fatto che l'art.

finizione di cui all'art. 4 GDPR. A riguardo, non può che rinviarsi alle Linee guida EDPB 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento, ai sensi del GDPR, versione 2.0, adottate il 7 luglio 2021, nelle quali si ricorda che i concetti di titolare del trattamento, di contitolare del trattamento e di responsabile del trattamento sono funzionali, in quanto mirano a ripartire le responsabilità in funzione dei ruoli effettivi delle parti, e autonomi, nel senso che dovrebbero essere interpretati principalmente ai sensi del diritto dell'UE in materia di protezione dei dati. Opportunamente, il Considerando n. 79 reg. EHDS definisce nel dettaglio i ruoli del trattamento nelle varie fasi del procedimento volto alla circolazione dei dati sanitari per uso secondario. Esso precisa che, nell'ambito di un trattamento di dati sanitari elettronici, in base ai rispettivi ruoli svolti per una specifica parte del processo, devono essere considerati titolari dei dati sanitari gli organismi responsabili dell'accesso ai dati sanitari e gli utenti dei dati sanitari. Ai sensi dell'art. 74 reg. EHDS, il titolare dei dati sanitari è considerato titolare del trattamento per la messa a disposizione dell'organismo responsabile dell'accesso ai dati sanitari dei dati sanitari elettronici personali richiesti. L'organismo responsabile dell'accesso ai dati sanitari è indicato, invece, titolare del trattamento dei dati sanitari elettronici personali nello svolgimento dei suoi compiti. L'organismo responsabile dell'accesso ai dati sanitari agisce, poi, in qualità di responsabile del trattamento per conto dell'utente dei dati sanitari, per la produzione di una risposta, se quest'ultimo titolare del trattamento dei dati sanitari elettronici personali, ai sensi di un'autorizzazione o una richiesta ai dati. Se questi sono punti fermi, rimane non del tutto chiaro il rapporto del Reg. EHDS n. 327/2025 con l'erigendo Ecosistema dei dati sanitari, per il quale la titolarità dei dati è in capo al Ministero della Salute. Pare potersi dire però che fino al trasferimento dei dati all'Organo di accesso, il Ministero della Salute sia da considerare titolare del trattamento, trasferendo poi tale qualifica ai suddetti enti.

[13] La risposta parrebbe dover essere di segno negativo, se è vero che secondo la Corte di giustizia UE i Considerando, pur rivestendo un importante valore interpretativo utile a precisare il significato degli atti normativi dell'Unione, non possono essere invocati per derogarvi o interpretarli in un senso manifestamente contrario al loro tenore letterale. Lo ricorda M. FACCIOLI, *La responsabilità civile per violazione della disciplina sull'utilizzo dei dati sanitari elettronici nell'European health data space (art. 100, reg. 2025/327/UE)*, in *Resp. civ. prev.*, 2025, 1450. Per una riflessione sulla rilevanza interpretativa dei numerosi e articolati considerando del GDPR, vedi V. CUFFARO, *Il diritto europeo sul trattamento dei dati personali*, in *Contratto e impresa*, 2018, 1107 ss.

[14] Tra i contributi più recenti a riguardo, vedi, C. SCOGNAMIGLIO, *Danno e risarcimento nel sistema del Rgpd: un primo nucleo di disciplina eurounitaria della responsabilità civile?*, in *Nuova giur. civ. comm.*, 2023, 1151; V. CUFFARO, voce *Risarcimento del danno e trattamento dei dati personali*, in *Enc. dir.*, *I tematici*, VII, *Responsabilità civile*, diretto da C. SCOGNAMIGLIO, Milano, 2024, 1360 ss.; B. PARENZO, *Note sparse in tema di responsabilità da illecito trattamento dei dati personali (a partire da due premesse)*, in *Rass. dir. civ.*, 2024, 870 ss.; U. SALANITRO, *Illecito trattamento dei dati personali e risarcimento del danno nel prisma della Corte di giustizia*, in *Riv. dir. civ.*, 2023, 426 ss. Nell'ambito di una configurazione della natura extracontrattuale della responsabilità ex art. 82 GDPR, è discusso se la regola attuale dell'imputazione si ponga sul piano della dimostrazione della mancanza di colpa (presunzione di colpa) (in tal senso, tra gli altri, vedi M. GAMBINI, *Responsabilità e risarcimento nel trattamento dei dati personali*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, 1048 ss.; E. PALMERINI, *sub* art. 82 GDPR, in E. NAVARRETTA (a cura di), *Codice della respon-*

100, reg. EHDS, è, come l'art. 82 GDPR, norma di fonte europea, ma con la precisazione, per la prima disposizione normativa, che «il diritto ad ottenere il risarcimento del danno è sancito conformemente al diritto dell'Unione e nazionale»[15]. Questa specificazione non significa che venga meno l'unità

sabilità civile, Milano, 2021, 2497 ss.; R. CATERINA e S. THOBANI, *Il diritto al risarcimento dei danni*, in *Giur. it.*, 2019, 2807 s.) ovvero richieda un evento estraneo al rischio tipico di impresa (responsabilità oggettiva per rischio). Vedi, a riguardo, S. SICA, *Verso l'unificazione del diritto europeo alla tutela dei dati personali*, in S. SICA, V. D'ANTONIO, G.M. RICCIO (a cura di), *La nuova disciplina europea della privacy*, Milano, 2016, 893; E. TOSI, *Diritto privato delle nuove tecnologie digitali*, Milano, 2021, 599, che individua una «responsabilità oggettiva per rischio d'impresa derivante dall'attività di trattamento di dati personali in violazione delle regole di condotta conformative, protettive dell'interessato-danneggiato»; C. CAMARDI, *Illecito trattamento dei dati e danno non patrimoniale. Verso una dogmatica europea*, in *Nuova giur. civ. comm.*, 2023, 795 ss., che si esprime in termini di responsabilità oggettiva e nega che il titolare del trattamento possa limitarsi a dimostrare la propria diligenza; esprime il dubbio se la norma si riferisca alla mancanza del nesso causale o ad una esimente di tipo oggettivo. In tale dibattito, si è di recente inserita la Corte di Giustizia europea, che accredita la tesi che ricostruisce l'imputazione della responsabilità, al titolare o al responsabile del trattamento, come fondata su un «meccanismo di responsabilità per colpa accompagnato da un'inversione dell'onere della prova» (CGUE, III sez., 21.12.2023, ZQ c. *Medizinischer Dienst der Krankenversicherung Nordrhein, Körperschaft des öffentlichen Rechts*, C-667/21, in *www.curia.europa.eu;* CGUE, III Sez., 25.1.2024, MediaMarktSaturn, C-687/21, § 52; CGUE, III Sez., 20.6.2024, Scalable Capital, C-182/22 e C189/22, § 28.). Non spetterebbe, dunque, al danneggiato provare il dolo o un profilo di negligenza nell'attività di trattamento, essendo questi aspetti "soggettivi" presunti sino a prova contraria, per il fatto che vi è stata un'attività di trattamento violativa del GDPR dannosa. Tale orientamento sarebbe suffragato sia «dal contesto in cui si inserisce tale articolo 82» sia «dagli obiettivi perseguiti dal legislatore dell'Unione» con l'emanazione del GDPR. Dal primo punto di vista, si è aggiunto che gli artt. 24 e 32 del Regolamento «si limitano ad imporre al titolare del trattamento di adottare misure tecniche e organizzative destinate ad evitare, per quanto possibile, qualsiasi violazione di dati personali» e che «un tale obbligo sarebbe messo in discussione se il titolare del trattamento fosse tenuto, in un secondo momento, a risarcire qualsiasi danno causato da un trattamento effettuato in violazione» del GDPR. Sotto il secondo profilo, è stato evidenziato come dalle considerazioni contenute nei Considerando da 4 a 6 del regolamento traspaia che il medesimo «è volto a realizzare un equilibrio tra gli interessi dei titolari del trattamento di dati personali e i diritti delle persone i cui dati sono oggetto di trattamento» e che «un meccanismo di responsabilità per colpa accompagnato da un'inversione dell'onere della prova [...] consente proprio di garantire un siffatto equilibrio», mentre «un regime di responsabilità oggettiva non garantirebbe la realizzazione dell'obiettivo di certezza giuridica perseguito dal legislatore», come si evince dal considerando 7 del GDPR stesso.

[15] Cfr., riguardo all'art. 82 GDPR ed al fatto che esso debba essere interpretato secondo gli orientamenti unionali, G. FINOCCHIARO, *Introduzione al regolamento europeo sulla protezione dei dati*, in *Nuove leggi civ. comm.*, 2017, 1 ss.; U. SALANITRO, *Illecito trattamento dei dati personali e risarcimento del danno nel prisma della Corte di Giustizia*, in *Riv. dir. civ.*, 2023, 430, per il quale occorre abbandonare l'impostazione localista e porsi alla ricerca del sistema e delle categorie a livello sovranazionale per cogliere le peculiari caratteristiche di un sistema europeo della responsabilità; G. NAVONE, *Ieri, oggi e domani della responsabilità civile da illecito trattamento dei dati personali*, in *Nuove leggi civ. comm.* 2022, 132 ss. Quest'ultimo Autore sottolinea che le decisioni della Corte lussemburghese, per comune consenso munite di autorità di cosa interpretata *ultra partes,* sono le sole idonee a disciplinare i profili trascurati dalla regola scritta, e i *dicta* resi in sede di rinvio pregiudiziale, vincolanti per tutti i giudici nazionali cui venga sottoposta un'analoga questione, introdurrebbero gocce di diritto uniforme che s'insinuano negli spazi lasciati vuoti dalla fonte regolamentare, colmandoli. Come noto, infatti, alle sentenze della Corte di Giustizia va attribuito il valore di ulteriore fonte del diritto comunitario, non nel senso che esse crei-

ISSN 2239-8570

della nozione nel diritto dell'Unione, anzi la sua esistenza trova conferma nel richiamo successivo all'opera interpretativa della Corte di Giustizia per quanto riguarda il concetto di «danno»[16]. È però evidente che una norma così generica non aiuti la costruzione di una responsabilità civile europea, dovendosi appoggiare la medesima alla stampella dei diritti nazionali, finchè non vi saranno interventi chiarificatori della Corte di Bruxelles. E di qui sorge il rischio di un'eterogeneità di tutele, ancor più grave, dato che la materia trattata dal regolamento EHDS si riferisce a rapporti perlopiù extradomestici[17].

Considerata la maggiore complessità, rispetto al GDPR, della disciplina dello spazio europeo dei dati sanitari – in termini di infrastrutture, funzioni, attori coinvolti e tecnologia impiegata (che implica l'impego di sistemi di

---

no "*ex novo*" norme comunitarie, ma in quanto ne indicano il significato ed i limiti di applicazione, con efficacia "*erga omnes*" nell'ambito della Comunità (Cfr. Corte Giustizia UE 9.6.2016, in causa C-586/14, Budisan, § 45. Nella giurisprudenza interna, fin da Cass. 30.12.2003, n. 19842, la Suprema Corte ha riconosciuto alle pronunce della Corte UE "valore normativo" ed efficacia retroattiva, essendo a tale organo giurisdizionale affidato il compito di fornire un'interpretazione autentica del diritto dell'Unione. Vedi poi, tra le ultime, nello stesso senso, Cass. 2.5.2024, n. 11760; Cass. 21.5.2024 n. 14089; Cass. Ord. 29.1.2024 n. 2674; Cass. Ord. 12.12.2023 n. 34743; Cass. 17.5.2019 n. 13425; Cass. 11.12.2012, n. 22577; cfr., analogamente, la Corte Costituzionale con la sentenza 13.7.2007 n. 284, tutte consultabili in *Dejure*). In questo quadro, sembra potersi ravvisare il progressivo tramonto della contrapposizione tra sistemi di *civil law* e sistemi di *common law,* oltre che il superamento del positivismo giuridico (Cfr., a riguardo, le parole di F. GALGANO, *Democrazia politica e legge della ragione*, in *Contratto e impresa*, 2007, 410 ss.). In argomento, vedi anche G. VETTORI, *La giurisprudenza come fonte del diritto privato*, in *Persona e mercato*, 2017, 137 ss.; G. ALPA, *La dialettica fra legislatore e interprete. Dai codici francesi ai codici dell'Italia unita: riflessioni in prospettiva storica nella recente letteratura*, in *Contratto e impresa*, 2015, 646; E. CALZOLAIO, *Il valore di precedente delle sentenze della Corte di Giustizia*, in *Riv. crit. dir. priv*., 2009, 41 ss.; N. LIPARI, *Per un ripensamento delle fonti-fatto nel quadro del diritto europeo*, in *Riv. trim. dir. e proc. civ*., 2013, 1217; A. RICCIO, *La giurisprudenza fonte del diritto*, in *Contratto e impresa*, 2017, 857 ss.; S. PATTI, *L'interpretazione, il ruolo della giurisprudenza e le fonti del diritto privato*, in *Foro it*., 2014, c. 113 ss.. Non esita a definire la Corte come il vero "legislatore comunitario", C. NOURISSAT, *La jurisprudence de la Cour de justice des Communautés européennes: Un regard privatiste à partir de l'actualité*, in *Archives de Philosophie du Droit,* 50, 2007, 245 ss.. Degna di nota pure la posizione di chi, pur riconoscendo la centralità della Corte di Giustizia nel «processo di armonizzazione degli ordinamenti nazionali» e nella messa a punto delle «tecniche grazie alle quali il primato del diritto europeo, una volta proclamato *in apicibus*, è andato progressivamente guadagnando di effettività», dubita dell'idea «oggi molto diffusa, che la giurisprudenza della Corte di Giustizia possieda dignità di fonte del diritto». Tale Autore ritiene, infatti, che la straordinaria concentrazione di potere in capo alla Corte del Lussemburgo (i cui Giudici sono nominati di comune accordo dai governi degli Stati membri, senza il coinvolgimento del Parlamento europeo e di quelli nazionali), susciti più di una perplessità in ordine alla legittimità democratica di questo «inedito e "complesso" demiurgo» (L. NIVARRA, *Il disordine delle fonti e l'ordine del diritto*, in *Riv. crit. dir. priv.*, 2021, 158 s.).

[16] Nello stesso senso, vedi S. CORSO, *Lo spazio europeo dei dati sanitari. Prime riflessioni sul regolamento UE 2025/327*, cit., 595.

[17] Sulla frammentarietà e incompletezza del formante legislativo europeo, si rinvia agli studi di H.W. MICKLITZ, *Il fascino del diritto privato europeo*, in *Contratto e impresa/Europa*, 2021, 103 ss. Cfr. nello stesso senso, M. FACCIOLI, *La responsabilità civile per violazione della disciplina sull'utilizzo dei dati sanitari elettronici nell'European Health Data Space (art. 100, reg. 2025/327/UE)*, in *Resp. civ. prev*., 2025, 1450 ss.

ISSN 2239-8570

AI) –, la configurazione dei profili di responsabilità per i danni occorsi a livello di spazio europeo dei dati sanitari sembra doversi riferire ad una pluralità di modelli rimediali e la polarizzazione dei criteri di imputazione secondo la secca alternativa colpa/responsabilità oggettiva non si rivela esaustiva. Rinunciando a prevedere anticipatamente e disciplinare nel dettaglio tutte le vicende di responsabilità civile che potrebbero essere potenzialmente innescate da una violazione della disciplina dell'EHDS, l'art. 100, Reg. 2025/327/UE, effettua dunque un generico rinvio alle disposizioni del diritto dell'Unione Europea e degli ordinamenti nazionali che saranno di volta in volta più confacenti al caso di specie[18].

In linea generale, e in mancanza di chiari riferimenti in un senso o nell'altro, la disciplina della responsabilità contrattuale o di quella extracontrattuale dovrà comunque essere scelta, distinguendo i casi, a seconda dell'inquadramento che si dà del rapporto tra le parti. Si tratta di una valutazione ermeneutica necessaria e doverosa, considerando che manca una puntuale regolamentazione di aspetti rilevanti in materia di responsabilità, come un qualsivoglia accenno all'elemento soggettivo, all'atteggiarsi della causalità [19], alla prova liberatoria, al termine di prescrizione dell'azione risarcitoria e al perimetro della risarcibilità del danno (e tale laconicità testuale, lo si ripete, appare uno dei motivi del riferimento ancillare al diritto degli Stati membri).

Nell'ambito di una qualificazione del rapporto come extracontrattuale, occorre valutare se sia sufficiente, per ritenersi sussistente un danno, la sola condotta, vale a dire, la «violazione del Regolamento», oppure se sia altresì necessaria l'individuazione di una specifica lesione di un interesse giuridicamente protetto, come previsto dal nostro art. 2043 c.c. Secondo l'interpretazione preferibile dell'art. 82 GDPR, traslabile in questo contesto,

---

[18] Cfr. M. FACCIOLI, *La responsabilità civile per violazione della disciplina sull'utilizzo dei dati sanitari elettronici nell'European Health Data Space (art. 100, reg. 2025/327/UE)*, in *Resp. civ. prev.*, 2025, 1450 ss., che conseguentemente afferma che, per esempio, qualora la trasgressione del Reg. 2025/327/UE comporti la violazione di uno (o più) dei diritti delle persone fisiche interessate riconosciuti nel GDPR o la compromissione di dati sanitari elettronici di natura personale, la responsabilità conseguente sarà da ricondurre all'ambito applicativo dell'art. 82, Reg. 2016/679/UE. Nell'ipotesi in cui venga in rilievo l'inosservanza dei requisiti stabiliti dal Reg. 2025/327/UE per la produzione e la messa in commercio di sistemi di cartelle cliniche elettroniche, è verosimile, invece, che la vicenda risarcitoria sia disciplinata dalla Direttiva 2024/2853/UE sulla responsabilità per danno da prodotti difettosi. Se l'inottemperanza dovesse riguardare uno degli «accordi contrattuali tra i titolari dei dati sanitari e gli utenti dei dati sanitari per la condivisione di dati contenenti informazioni o contenuti protetti da diritti di proprietà intellettuale o da segreti commerciali» conclusi ai sensi dell'art. 52, par. 4, del Regolamento in esame, si dovrà dare spazio alla disciplina della responsabilità contrattuale prevista dagli ordinamenti nazionali degli Stati membri. E così, per ciascuna delle varie fattispecie di responsabilità occasionate dalla violazione dell'EHDS, potranno venire in rilievo diverse discipline, potenzialmente anche molto differenti tra loro per quanto concerne l'ambito di applicazione soggettivo, il criterio di imputazione, l'onere della prova, il danno risarcibile, la prescrizione, la natura contrattuale o aquiliana.

[19] Cfr. N. MUCCIOLI, *Spazio europeo dei dati sanitari: nuovi danni e profili di responsabilità civile*, in *Accademia*, 2025, 851 ss., che si interroga, quindi, sulla rilevanza del comportamento di terzi nella produzione del danno (si pensi al caso dell'attacco *hacker*) nell'escludere la responsabilità del titolare e del responsabile del trattamento.

ISSN 2239-8570

pur non essendo il danno qualificato come ingiusto, la sola violazione di una disposizione del Regolamento non può aprire, di per sé sola, le porte al risarcimento, giacché la funzione selettiva dei danni risarcibili, svolta dalla clausola dell'ingiustizia, è sostituita dagli esiti selettivi dell'eventuale bilanciamento tra ragioni della persona e ragioni pubblicistiche/solidaristiche e/o del mercato[20]. Anche in caso di responsabilità contrattuale, non ogni violazione sarà qualificabile alla stregua di inadempimento di un obbligo specificamente connotante il rapporto obbligatorio tra le parti, giacché non ogni regola di condotta prevista nell'impianto regolamentare corrisponde a una prestazione *ex lege* imposta per l'immediata soddisfazione dell'interesse che vanta il soggetto leso.

Ciò considerato, il regolamento EHDS, in ordine all'uso secondario dei dati, disegna il formarsi di un rapporto che prevede la presenza di quattro parti: chi genera i dati (l'interessato), chi li detiene per fini di cura (titolare dei dati), chi ne gestisce l'accesso (l'autorità per l'accesso ai dati) e chi ne chiede e poi ne ottiene la disponibilità per fini di riutilizzo (utente dei dati). Profili di responsabilità si possono verificare nelle deviazioni rispetto ai termini e alle condizioni di accesso e riuso del flusso di dati ovvero laddove si verifichi una violazione nel trattamento dei dati personali (accesso non autorizzato, perdita o alterazione delle informazioni). In questo contesto, si può configurare alla base un rapporto *lato sensu* contrattuale sia tra l'interessato e il titolare dei dati, che tra l'interessato e l'Organismo per l'accesso ai dati sanitari.[21] Appare palese, infatti, che si instauri, anche al di fuori di una vera relazione contrattuale, un rapporto di fiducia tra le parti sopramenzionate, fiducia che è uno dei principali obiettivi dichiarati di questa normativa. Tale fiducia è puntellata e rafforzata sia dalla posizione di soggetto pubblico, che da una serie di obblighi indicati dalla normativa europea a carico sia del titolare dei dati sanitari, che dell'Organismo per l'accesso ai dati sanitari, che proiettano tali relazioni nella dimensione del rapporto obbligatorio. In queste ipotesi, quindi, la responsabilità sarà disciplinata dall'art. 1218 c.c., che disciplina l'inadempimento di obblighi di na-

[20] Cfr., in modo analogo, con riferimento alla disciplina di cui all'art. 82 GDPR, C. CAMARDI, *Illecito trattamento dei dati e danno non patrimoniale,* in *Nuova giur. civ. comm.,* 2023, 1141.

[21] Quando si fa riferimento alla natura «contrattuale» della responsabilità di cui all'art. 1218 c.c., in realtà, si utilizza una semplificazione del linguaggio giuridico, in quanto – a ben guardare – si tratta di una responsabilità diversa da quella aquiliana e che ha come presupposto la violazione di un'«obbligazione» o di un altro «obbligo» di eseguire una «prestazione» non necessariamente di fonte contrattuale (cfr. M. BIANCA, *Diritto civile*, 5, *La responsabilità*, Milano, 2012, 1, ove si precisa che «la responsabilità per inadempimento è detta contrattuale a prescindere dalla fonte contrattuale o non contrattuale dell'obbligazione inadempiuta». Nello stesso senso, anche G. VISINTINI e L. CABELLA PISU, *L'inadempimento delle obbligazioni*, in *Tratt. dir. priv.*, diretto da P. RESCIGNO, vol. 9, *Obbligazioni e contratti*, tomo I, Torino, 1984, 155, per le quali la regola generale in materia di responsabilità del debitore, contenuta nell'art. 1218 c.c., viene «preferibilmente definita "contrattuale" dalla dottrina a causa del prevalere delle obbligazioni derivanti da contratto e rappresenta il tentativo del legislatore di riassumere in una disciplina uniforme una casistica, a dire il vero, molto varia a causa della diversa natura dei contratti e dei diversi modi di inadempimento»).

ISSN 2239-8570

tura contrattuale[22]. Del resto, nella logica dell'*accountability*, la frontiera della responsabilità è spostata *ex ante* ed incentrata sul binomio sicurezza e prevenzione, garantite dal rispetto di regole dettate da leggi, norme armonizzate, codici di condotta, protocolli e linee guida, che impongono doveri positivi la cui violazione è sanzionata anche a livello amministrativo. Profili di responsabilità di natura extracontrattuale, invece, non rinvenendosi un previo rapporto tra le parti, sono attribuibili al *data user* nei confronti dell'interessato, se si verifichi una sua violazione volontaria o colposa nel trattamento dei dati da cui derivi una fuga di dati potenzialmente o concretamente capace di re-identificare l'interessato medesimo, condotta esplicitamente vietata dal regolamento UE, in coerenza con la tutela dei diritti fondamentali tutelati dal GDPR. Ad essa potrà affiancarsi, in concorso, una responsabilità dell'Organismo per l'accesso ai dati sanitari, che, in fase di richiesta di autorizzazione, male abbia valutato le capacità dell'utente dei dati, anche dal punto di vista della sicurezza dell'ambiente proposto. Sarà da valutare pure un'eventuale responsabilità dell'Autorità sanitaria digitale per omesso controllo.

Per quanto riguarda, poi, il concetto di danno risarcibile, esso dovrebbe essere interpretato in senso lato, alla luce della giurisprudenza della Corte di giustizia, in modo da rispecchiare pienamente gli obiettivi del regolamento EHDS (Cfr. Considerando 101 EHDS), sempre facendo salve le eventuali richieste di risarcimento danni derivanti dalla violazione di altre norme del diritto dell'Unione o nazionale[23]. Le persone fisiche dovrebbero, quindi, ot-

[22] *Amplius*, sulla natura «contrattuale» di tale tipo di rapporti nell'ambito della protezione dei dati personali, mi si consenta il rinvio a S. FAILLACE, *La controversa categoria delle obbligazioni ex lege*, Milano, 2023, 177 ss.; ID., *La natura e la disciplina delle obbligazioni di cui all'art. 25 del GDPR, espressione dei principi di privacy by design e di privacy by default*, in *Contratto e impresa*, 2022, 1123 ss. Ma in tal senso, vedi anche F. BRAVO, *L'«architettura» del trattamento e la sicurezza dei dati e dei sistemi*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, 775 ss.. Vedi pure F. PIRAINO, *Il regolamento generale sulla protezione dei dati personali e i diritti dell'interessato*, in *Le nuove leggi civ. comm.*, 2017, 390; B. PARENZO, *Note sparse in tema di responsabilità da illecito trattamento dei dati personali (a partire da due premesse)*, in *Rass. dir. civ.*, 2024, 882. Tale posizione origina dalla nota teoria di Carlo Castronovo (a partire da C. CASTRONOVO, *L'obbligazione senza prestazione, ai confini tra contratto e torto*, in *Le ragioni del diritto. Scritti in onore di L. Mengoni*, Milano, 1995, I, 148 ss.). In argomento, di recente vedi per tutti A. NICOLUSSI, *Responsabilità da contatto sociale qualificato*, in *Enc. dir.*, *I tematici*, VII, *Responsabilità civile*, diretto da C. SCOGNAMIGLIO, Milano, 2024, 1076 ss.

[23] La Corte Ue con sentenza 4.5.2023 (causa C-300/21), in *Foro it.*, 2023, IV, c. 268 ss., con note di A. PALMIERI e R. PARDOLESI, *Mai futile il danno non patrimoniale da violazione della privacy (purché lo si provi!)*; C. SCOGNAMIGLIO, *Danno e risarcimento nel sistema del Rgpd: un primo nucleo di disciplina eurounitaria della responsabilità civile?*, in *Nuova giur. civ. comm.*, 2023, 1150 ss., ha rimarcato come l'art. 82 GDPR non subordini la risarcibilità del danno al superamento di una determinata soglia di gravità e una tale subordinazione «(…) rischierebbe di nuocere alla coerenza del regime istituito dal GDPR, poiché la graduazione di una siffatta soglia, da cui dipenderebbe la possibilità o meno di ottenere detto risarcimento, potrebbe variare in funzione della valutazione dei giudici aditi(...)». La Corte Europea, quindi, stigmatizza quegli orientamenti nazionali, sino ad oggi seguiti anche dalla giurisprudenza italiana, secondo cui il risarcimento del danno in discorso dovrebbe essere bilanciato col principio di solidarietà che implica di verificare, ai fini della risarcibilità, il superamento di un non meglio identificato limite di tollerabilità della lesione. Infine,

tenere pieno ed effettivo risarcimento per il danno subito, ad esempio, in caso di fatti che abbiano come effetto quello della re-identificazione di persone fisiche, del trasferimento di dati sanitari personali al di fuori dell'ambiente di trattamento sicuro e in caso di trattamento dei dati per usi vietati o al di fuori di un'autorizzazione. Peraltro, qualora le autorità di sanità digitale, gli organismi responsabili dell'accesso ai dati sanitari, i titolari dei dati sanitari o gli utenti dei dati sanitari siano coinvolti nello stesso trattamento, ogni attore dovrebbe rispondere per la totalità del danno. Tuttavia, qualora essi siano riuniti negli stessi procedimenti giudiziari, conformemente al diritto degli Stati membri, dovrà essere possibile ripartire il risarcimento in base alla responsabilità che ricade su ognuno di questi attori, a condizione che sia assicurato il pieno ed effettivo risarcimento della persona fisica che ha subito il danno. Dovrà pure considerarsi ammissibile, *ex* art. 2055 c.c., anche in assenza di indicazioni normative unionali in tal senso, un'azione di regresso in favore dei soggetti sopra individuati che abbiano corrisposto l'intero risarcimento del danno nei confronti degli altri soggetti coinvolti nel medesimo trattamento, laddove vi siano responsabilità concorrenti.

3. Segue. I profili patologici della relazione tra il data user e l'Organismo di accesso ai dati sanitari.

La relazione tra il *data user* che formuli richiesta di utilizzo e l'Organismo di accesso ai dati sanitari, che dovrebbe autorizzare il trattamento, merita un approfondimento particolare.

Per «autorizzazione ai dati», secondo il reg. Ue EHDS (art. 2, par. 2, lett. v), si intende «una decisione amministrativa emessa nei confronti di un

il Giudice Europeo, vista l'assenza di norme unionali sul punto del *quantum* risarcibile, ne rimanda all'ordinamento giuridico di ciascuno Stato membro l'individuazione, nel rispetto dei principi di equivalenza e di effettività del diritto dell'Unione. Dunque, in base all'art. 82, GDPR e al considerando 146, deve essere garantito un «(...) pieno ed effettivo risarcimento per il danno subito (...)» che, «tenuto conto della funzione compensativa del diritto al risarcimento previsto dall'art. 82 del GDPR (...)», valga a «(...)compensare integralmente il danno concretamente subito a causa della violazione di tale regolamento (...)».Cfr., da ultimo, CGUE, 4 settembre 2025, C-655/23, secondo la quale "la nozione di «danno immateriale» contenuta in tale disposizione include sentimenti negativi provati dalla persona interessata a seguito di una trasmissione non autorizzata dei suoi dati personali ad un terzo, quali il timore o l'insoddisfazione, che sono suscitati da una perdita di controllo su tali dati, da una potenziale utilizzazione abusiva di questi ultimi o da un pregiudizio alla sua reputazione, purché detto interessato dimostri che prova sentimenti siffatti, con le loro conseguenze negative, a causa della violazione de qua del regolamento suddetto". Insomma, il danno immateriale, anche se lieve, persino il timore di un danno futuro, si candidano a trovare ristoro, laddove si riesca a dimostrarne in giudizio l'essenza. In senso critico rispetto all'orientamento della Cassazione, che, ai fini della liquidazione di un danno non patrimoniale, adotta i filtri selettivi della «gravità della lesione» e della «serietà del danno», ed utilizza in maniera distorta il principio di solidarietà, vedi F BRAVO, *Il principio di solidarietà in materia di protezione dei dati personali nelle decisioni del Garante e della Corte di Cassazione*, in *Contratto e impresa*, 2023, 426 ss. e ID., *Il principio di solidarietà*, in F. BRAVO (a cura di), *Dati personali. Protezione, libera circolazione e Governance. 1. Principi*, Pisa, 2023, 598 ss.

ISSN 2239-8570

utente dei dati sanitari da un organismo responsabile dell'accesso ai dati sanitari per il trattamento di determinati dati sanitari elettronici specificati nell'autorizzazione di cui trattasi per finalità specifiche correlate all'uso secondario, sulla base delle condizioni stabilite al capo IV del presente regolamento». In linea generale, l'autorizzazione si può definire come un atto provvedimentale volto a definire presupposti, limiti e condizioni per l'avvio e per il successivo svolgimento di un'attività privata in maniera rispondente alle esigenze degli interessi pubblici coinvolti[24]. Più nel dettaglio, alle autorizzazioni preesiste un diritto soggettivo, allo stato, puramente potenziale, che potrà essere esercitato solo quando la pubblica amministrazione riterrà sussistenti i presupposti fissati dalla legge, in relazione all'interesse pubblico coinvolto. L'autorizzazione risponde, dunque, essenzialmente ad una funzione di tutela e conservatrice dell'interesse pubblico, di talché i limiti posti dalle norme di legge allo svolgimento di determinate attività vengono rimossi, perché le condizioni della persona richiedente, e dell'atto od opera che essa vuol compiere, danno sufficiente garanzia che tutte le esigenze giuridiche e sociali, in nome delle quali quei limiti furono posti all'attività individuale, saranno rispettate. L'autorizzazione viene quindi ricondotta all'interno della categoria dei provvedimenti di carattere accrescitivo o migliorativo delle posizioni giuridiche dei destinatari, e, in particolare, dei diritti soggettivi, non creandoli *ex novo*, poiché essi originano e si radicano nella Costituzione, bensì consentendo alle facoltà in essi potenzialmente insite di essere esercitate in atto e in concreto[25].

---

[24] Cfr. R. VILLATA, *Autorizzazioni amministrative e iniziativa economica privata*, Milano, 1974, 34, che su questo punto si pone in coerenza con la ricostruzione del Ranelletti (O. RANELLETTI, *Scritti giuridici scelti*, a cura di E. FERRARI, B. SORDI, Napoli, 1992, III, 37 ss., 77 ss., 235 ss.) e degli altri studiosi dell'istituto autorizzatorio. Cfr. anche G. ZANOBINI, *Corso di diritto amministrativo*, Milano, 1958, I, 262; A. SANDULLI, *Notazioni in tema di provvedimenti autorizzativi*, in *Riv. trim. dir. pubbl.*, 1957, 784 ss.; ID., *Abilitazioni, autorizzazioni, licenze*, in *Rass. dir. pubbl.*, 1958, 3 ss.; F. FRANCHINI, *Le autorizzazioni amministrative costitutive di rapporti giuridici fra l'amministrazione e i privati*, Milano, 1957, nonché, più di recente, F. FRACCHIA, *Autorizzazione amministrativa e situazioni giuridiche soggettive*, Napoli, 1996; ID., *Autorizzazioni amministrative*, in S. CASSESE (a cura di), *Dizionario di diritto pubblico*, Milano, 2006, I, 598 ss., e gli ampi riferimenti dottrinali e giurisprudenziali ivi contenuti. Vedi poi A. ORSI BATTAGLINI, che fonda la propria ricostruzione innanzitutto sul considerare – come già Villata – una contraddizione il fatto che l'attività di un privato possa essere oggetto di un diritto soggettivo e, al tempo stesso, contraria all'ordinamento (e spesso addirittura penalmente illecita) se posta in essere in assenza o in contrasto con un atto amministrativo «permissivo» (cfr. Cfr. A. ORSI BATTAGLINI, *Autorizzazione amministrativa*, in *Dig. Disc. Pubbl.*, II, Torino, 1987, 1 ss.).

[25] Si consideri che l'Unione europea ha disciplinato direttamente, tramite regolamenti o più frequentemente tramite direttive, alcune delle autorizzazioni o atti di assenso (la distinzione non assume particolare rilievo nell'ottica eurounitaria) funzionali alla cura e alla tutela di interessi pubblici diversi da quelli economici e commerciali, eppure ritenuti fondamentali dallo stesso ordinamento eurounitario, quali ad esempio gli interessi ambientali. A questo riguardo basti pensare alle valutazioni ambientali (valutazione ambientale strategica, valutazione di impatto ambientale, valutazione di incidenza sugli habitat e sulle specie prioritari), all'autorizzazione integrata ambientale, alle autorizzazioni alle emissioni industriali. La normazione eurounitaria, e, in particolare la Direttiva 2006/123/CE sulla libera circolazione dei servizi e il diritto di stabilimento (la c.d. «Direttiva Bolkestein»), elabora una nozione amplissima e sostanzialmente neutra di autorizzazione, come si evince dal Considerando 39, secondo cui «la nozione di regime di autorizzazione dovrebbe comprendere, in partico-

Come noto, il diritto alla protezione dei dati personali è diritto fondamentale, ma nel contesto giuridico europeo vive in relazione con altri diritti di pari livello, va con essi bilanciato e pertanto non è predicabile una sua aprioristica prevalenza, tale da imporlo ad altre situazioni soggettive.

Ciò emerge anche dal Considerando n. 4, GDPR, secondo il quale il diritto alla protezione dei dati personali «non è una prerogativa assoluta ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità».

L'autorizzazione all'utilizzo di dati sanitari, normata dal Regolamento EHDS, si configura come un provvedimento che, verificate previamente tutte le condizioni tecniche e giuridiche, facoltizza il *data user* ad utilizzare i dati sanitari elettronici dell'interessato. Si contrappone, quindi, il diritto e/o il potere dell'utente dei dati di svolgere operazioni di trattamento (diritto radicato, nel nostro ordinamento all'art. 41 della Costituzione, relativo all'iniziativa economica privata, all'art. 33, che introduce il principio di libertà della scienza, e all'articolo 9, che stabilisce « l'obbligo » della Repubblica di promuovere «lo sviluppo della cultura e della ricerca scientifica e tecnica»), nonché le implicazioni che il riconoscimento di tale diritto o potere ha, con il concorrente diritto dell'interessato a veder protetti i propri dati personali, con le conseguenti necessità di bilanciamento tra i relativi interessi giuridicamente rilevanti, che si confrontano però secondo logiche non (necessariamente) antagoniste[26]. Il *data user*, ottenuta l'autorizzazione, ac-

---

lare, le procedure amministrative per il rilascio di autorizzazioni, licenze, approvazioni o concessioni, ma anche l'obbligo, per potere esercitare l'attività, di essere iscritto in un albo professionale, in un registro, ruolo o in una banca dati, di essere convenzionato con un organismo o di ottenere una tessera professionale [...]», nozione pienamente avallata dalla Corte di Giustizia dell'Unione Europea, che vi ha ricondotto addirittura le concessioni di beni demaniali marittimi, lacuali e fluviali. La medesima Direttiva però ammette regimi di tipo autorizzatorio (nell'accezione ampia e neutra appena riferita) solo qualora siano necessari per "motivi imperativi di interesse generale", tra i quali non possono rientrare ragioni di tipo economico, e comunque nel rigoroso rispetto dei principi di proporzionalità e di non discriminazione.

[26] La natura delle posizioni giuridiche soggettive nascenti dalla disciplina europea sulla protezione dei dati personali è stata ampiamente dibattuta in dottrina, specie in campo privatistico, già alla luce della disciplina di cui alla Direttiva 95/46/CE, al punto che si è sostenuta la tesi dell'interesse legittimo anche nei rapporti tra soggetti privati (Cfr., a riguardo, G. RESTA, *Revoca del consenso ed interesse al trattamento nella legge sulla protezione dei dati personali*, in *Riv. crit. dir. priv.*, 2000, 329, il quale parla appunto di «interesse legittimo di diritto privato», rievocando istituti oggetto di studi meno recenti quali quelli di L. BIGLIAZZI GERI, *Contributo ad una teoria dell'interesse legittimo nel diritto privato*, Milano, 1967). Nei rapporti con le pubbliche autorità, nei casi di trattamento dei dati personali, a favore della figura dell'interesse legittimo, cfr. G. CIRILLO, *Trattamento pubblico dei dati personali e responsabilità civile della P.A.*, in *Foro amm.*, 1999, 3 ss., secondo cui: « essendo l'attività di "trattamento" attività pubblicistica in senso stretto, la posizione dell'interessato, almeno secondo il sistema ricevuto, è di interesse legittimo, almeno che non vi sia una espressa eccezione posta dal legislatore medesimo. Eccezione che non può essere rinvenuta semplicemente nel fatto che sia stata utilizzata la parola diritto». In tal senso, parrebbe propendere anche F. MIDIRI, *Il diritto alla protezione dei dati personali. Regolazione e tutela*, Napoli, 2017, 126, che riconosce che «la situazione soggettiva (*de qua*) non è strutturalmente dissimile dall'interesse legittimo», salvo poi affermare che «il diritto alla protezione dei dati personali pare assimilabile alla categoria dei diritti nella quale parte della dottrina amministrativistica dissolve l'interesse legittimo». In argomento, vedi anche

ISSN 2239-8570

quisirà la facoltà propria del titolare di effettuare il trattamento per finalità legittime (attività di ricerca e per il perseguimento di interessi meritevoli di tutela), di gestire il trattamento e conformarlo alle proprie esigenze, nonché di trarre utilità anche economica dalle operazioni di trattamento sui dati, qualora ciò sia rispondente alla cornice delineata dalle condizioni di liceità del trattamento e dalle finalità con esso legittimamente perseguite. Ove l'Organismo si rifiuti di rilasciare un'autorizzazione ai dati, tale ente dovrà motivare il proprio diniego (vedi art. 68, par. 9, reg. EHDS) e la motivazione dovrà indicare i presupposti di fatto e le ragioni giuridiche che hanno determinato la decisione, anche in relazione alle risultanze dell'istruttoria, *ex* art.3, legge 241/1990.

In questo quadro, deve poter sempre essere risarcibile (sussistendone i presupposti concreti, naturalmente) il danno derivante dall'illegittimo diniego o dall'annullamento in autotutela dell'atto autorizzatorio da parte dell'Organismo di accesso ai dati sanitari, ovverosia la lesione consistente nell'illegittimo impedimento all'espansione del relativo diritto soggettivo[27]. Così dovrà essere pure ove si volesse addivenire alla configurazione di un rapporto "contrattuale" tra Organismo di accesso ai dati sanitari e *data user*, sulla base dell'individuazione di un "contatto sociale" o di un "contatto amministrativo qualificato" tra queste due parti, considerato l'elemento della fiducia che viene decantato dal regolamento EHDS in più occasioni e che pare confermare la nascita di una relazione molto stretta tra le parti dei rapporti che si instaurano ai sensi di questa normativa[28]. E del resto, anche la giurisprudenza più recente della Suprema Corte accoglie questa impostazione, laddove vi sia una lesione del legittimo affidamento del privato in ordine ad un provvedimento della P.A. ampliativo della di lui posizione[29].

G. CARULLO, *Trattamento di dati personali da parte delle pubbliche amministrazioni e natura del rapporto giuridico con l'interessato*, in *Riv. it. dir. pubbl. com.*, 2020, 131.

[27] Fin da A. SANDULLI, *Lesione di interessi legittimi e obbligazione risarcitoria della pubblica amministrazione*, in *Riv. trim. dir. proc. civ.*, 1963, 1293 ss.

[28] Si veda, ad esempio, il Considerando 4, reg. EHDS, secondo cui, «vista la sensibilità dei dati sanitari elettronici personali, il presente regolamento intende fornire garanzie sufficienti sia a livello dell'Unione sia a livello nazionale per assicurare un elevato livello di protezione, sicurezza, riservatezza e uso etico dei dati. Tali garanzie sono necessarie per promuovere la fiducia nella gestione sicura dei dati sanitari elettronici delle persone fisiche per l'uso primario e per l'uso secondario quali definiti nel presente regolamento.» In ordine all'impostazione "contrattuale" di cui al testo, non possono non menzionarsi gli scritti di Carlo Castronovo, il quale, dall'idea di un diritto amministrativo paritario, getta le premesse per una riconsiderazione della responsabilità della p.a. su basi relazionali. (cfr. C. CASTRONOVO, *Responsabilità civile per la Pubblica Amministrazione*, in *Jus*, 1998, 647 ss.; ID., *La civilizzazione della p.a.*, in *Europa dir. priv.,* 2013, 637 ss.; ID, *L'obbligazione senza prestazione, ai confini tra contratto e torto*, in *Le ragioni del diritto*, *Scritti in onore di L. Mengoni*, Milano, 1995, I, 148 ss.; ID., *La nuova responsabilità civile*, Milano, 2006, 443 ss.; vedi pure A. IULIANI, *La responsabilità civile della pubblica amministrazione; alcune riflessioni intorno all'interesse legittimo dalla prospettiva dei rimedi*, in *Contratto e impresa*, 2016, 1196 ss.

[29] Cfr., in tal senso, Cass. civ. 19.5.2025, n. 13289, in *Dejure*. Nel caso di specie, una società aveva presentato un'istanza per ottenere il certificato di compatibilità ambientale e l'autorizzazione per costruire e gestire un impianto microidroelettrico. Nel decidere la controversia, la Cassazione ha confermato l'orientamento per cui la responsabilità della pubblica amministrazione per lesione dell'affidamento incolpevole del privato non è qualificabile né come extracontrattuale, né come contrattuale in senso proprio. Si configura, piuttosto,

Dal canto suo, il *data user*, oltre ad osservare un generale impegno a trattare il flusso di dati in conformità con il quadro etico-giuridico applicabile e a rendicontare – in termini di *accountability* – la conformità del riuso dei dati rispetto a quanto dichiarato in sede di richiesta di accesso, assume l'impegno specifico di rendere pubblici i risultati o gli esiti dell'uso secondario dei dati sanitari elettronici, comprese le informazioni pertinenti per la prestazione di assistenza sanitaria, entro 18 mesi dal completamento del trattamento dei dati sanitari elettronici. Il risultato, inoltre, deve essere reso pubblico nelle sintesi divulgative [30]. Una deviazione o un vero e proprio inadempimento da tali obblighi creerà, oltre all'irrogazione di sanzioni amministrative, una responsabilità da fatto illecito nei confronti dell'interessato.

In definitiva, si può affermare, vista la genericità delle disposizioni di cui all'art. 100 reg. EHDS, che occorrerà, *in primis*, verificare, caso per caso, l'applicabilità delle legislazioni di settore di derivazione europea, quali, oltre al GDPR, quella relativa all'utilizzo dell'intelligenza artificiale, se e quando la stessa sarà oggetto di una disciplina specifica in ordine alla responsabilità [31] o quella relativa alla responsabilità del produttore, con le op-

---

come una responsabilità di tipo relazionale o da «contatto sociale qualificato». In motivazione, si legge, in continuità con Cass. Sez. un., 19.1.2023 n. 25324 (in *Dejure*), che «il pregiudizio non deriva dalla violazione delle regole di diritto pubblico sull'esercizio della potestà amministrativa, bensì, in una più complessa fattispecie, dalla violazione dei principi di correttezza e buona fede, che devono governare il comportamento dell'amministrazione e si traducono in regole di responsabilità, non di validità dell'atto; pertanto, l'affidamento incolpevole, la cui lesione potrebbe determinare la responsabilità risarcitoria della P.A. è «una situazione autonoma, tutelata in sé, e non nel suo collegamento con l'interesse pubblico, come affidamento incolpevole di natura civilistica, che si sostanzia, secondo una felice sintesi dottrinale, nella fiducia, nella delusione della fiducia e nel danno subito a causa della condotta dettata dalla fiducia mal riposta: si tratta, in sostanza, di un'aspettativa di coerenza e non contraddittorietà del comportamento dell'amministrazione fondata sulla buona fede».

[30] Secondo l'art. 63 reg. EHDS, quando svolgono i compiti di monitoraggio e controllo a norma dell'articolo 57, paragrafo 1, lettera a), punto ii), gli organismi responsabili dell'accesso ai dati sanitari hanno il diritto di chiedere e ricevere dagli utenti dei dati sanitari e dai titolari dei dati sanitari tutte le informazioni necessarie per verificare la conformità al presente capo. Qualora concludano che un utente dei dati sanitari o un titolare dei dati sanitari non rispetta le prescrizioni del presente capo, gli organismi responsabili dell'accesso ai dati sanitari ne informano immediatamente l'utente dei dati sanitari o il titolare dei dati sanitari e adottano misure appropriate. L'organismo responsabile dell'accesso ai dati sanitari interessato dà all'utente dei dati sanitari o al titolare dei dati sanitari interessato la possibilità di esprimere il proprio parere entro un termine ragionevole che non deve superare le quattro settimane. Qualora l'accertamento della non conformità riguardi una possibile violazione del regolamento (UE) 2016/679, l'organismo responsabile dell'accesso ai dati sanitari interessato informa immediatamente le autorità di controllo a norma dello stesso e fornisce loro tutte le informazioni pertinenti in merito a tale risultanza. Per quanto riguarda la non conformità da parte degli utenti dei dati sanitari, gli organismi responsabili dell'accesso ai dati sanitari hanno il potere di revocare l'autorizzazione ai dati rilasciata a norma dell'articolo 68 e di interrompere senza indebito ritardo il trattamento dei dati sanitari elettronici interessato da parte dell'utente dei dati sanitari, e adottano misure adeguate e proporzionate volte a garantire un trattamento conforme da parte.

[31] Si ricorda che, in data 28 settembre 2022, la Commissione UE aveva presentato una proposta di Direttiva relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale (Cfr. E. BELLISARIO, *Il pacchetto europeo sulla responsabilità per danni da prodotti e da intelligenza artificiale. Prime riflessioni sulle*

ISSN 2239-8570

portune modifiche di cui alla Direttiva (UE) 2024/2853, in via di recepimento nel nostro paese. Diversamente, in mancanza di una regolamentazione puntuale della materia, la Corte di Giustizia europea dovrà fare valere, nel tempo, la propria posizione di organo dal ruolo centrale all'interno degli equilibri unionali, interpretando le scarne disposizioni esistenti, con il rischio però che, *medio tempore*, si evidenzino pericolose criticità ermeneutiche, anche alla luce del richiamo fatto dall'art. 100 reg. EHDS al diritto nazionale.

Proposte della Commissione, in *Danno resp.*, 2023, 153 ss.; R. GELLERT, A. JANSENN, *The impact of artificial intelligence on european tort law: taking stock of an ongoing process*, in A. JANSSEN, M. LEHMANN, R. SCHULZE (eds), *The future of European Private Law, Hart Nomos*, 2023, 185 ss.). Tale proposta– che si inseriva nel quadro più ampio della regolamentazione dell'intelligenza artificiale nell'UE, accanto ad altre normative quali, *in primis*, il Regolamento UE n. 2024/1689 sull'intelligenza artificiale (cd. IA Act), nonché la revisione delle norme (settoriali e orizzontali) in materia di sicurezza dei prodotti– si prefiggeva l'obiettivo di promuovere la diffusione di un'IA affidabile, affinché fosse possibile sfruttarne appieno i vantaggi per il mercato interno, e si proponeva di conseguirlo garantendo a coloro che hanno subito danni causati dall'IA una protezione equivalente a quella di cui beneficiano quanti subiscono danni causati da altri prodotti. La Proposta si applicava alle azioni civili di responsabilità extracontrattuale promosse successivamente alla data di recepimento della direttiva da parte di:– soggetti direttamente danneggiati dall'IA; soggetti subentrati/surrogati nei diritti del danneggiato dall'IA (es. eredi; compagnia assicurativa);– soggetti che agiscono per conto di uno o più danneggiati (azioni rappresentative), al fine di ottenere il risarcimento del danno causato dall'output di un sistema di IA o dalla mancata produzione di un output (che avrebbe dovuto essere prodotto da tale sistema) nell'ambito di regimi di responsabilità per colpa. L'obiettivo principale della direttiva era, dunque, quello di introdurre semplificazioni dell'onere della prova per qualunque soggetto instaurasse un'azione per danni causati da sistemi di IA in uno Stato membro. In tale ottica, la proposta introduceva il diritto per il danneggiato/attore di ottenere in sede giudiziale elementi di prova sul sistema di IA c.d. «ad alto rischio», mediante un ordine giudiziale di divulgazione di tali elementi: tale provvedimento costituisce, infatti, un oggettivo mezzo efficace per l'identificazione delle persone responsabili, e delle relative prove, al netto, tuttavia, di eventuali limiti intrinseci, quali, in primis, la protezione dei segreti commerciali e delle informazioni riservate. A tal riguardo, la direttiva mirava, altresì, a fornire una base efficace per le domande di risarcimento in relazione alla colpa consistente nella non conformità a un obbligo di diligenza a norma del diritto dell'unione o nazionale: sul punto, era stata, dunque, prevista, all'art. 4 paragrafo 1) della direttiva, una presunzione relativa in relazione, appunto, al nesso di causalità tra la non conformità e l'output prodotto dal sistema di IA o la mancata produzione di un output da parte del medesimo sistema di IA che ha cagionato un danno. Risultava, infine, degno di attenzione il suggerimento, inserito nella relazione complementare alla direttiva, circa l'introduzione di un cd. regime misto, che combinasse elementi di responsabilità basata sulla colpa e di responsabilità oggettiva: nello specifico, la prima sarebbe rimasta applicabile in generale, mentre la seconda sarebbe stata riservata ai casi di danni causati da sistemi di IA ad alto impatto o cd. general-purpose (es. sanità). La Commissione europea ha motivato il ritiro di tale proposta di direttiva con l'obiettivo di evitare un eccesso di regolamentazione che incidesse negativamente sulla competitività delle imprese europee. L'adozione di criteri più stringenti per l'imputazione della responsabilità in caso di danni derivanti dall'impiego di sistemi autonomi avrebbe, secondo la Commissione, comportato un incremento degli oneri regolatori, con ripercussioni sullo sviluppo tecnologico e sull'attrattività del mercato europeo per gli investitori. (cfr. F. NIOLA, *Responsabilità civile per l'AI: gli effetti del ritiro della proposta di direttiva*, in *Cybersecurity360.it*, pubblicato in data 28 febbraio 2025).

ISSN 2239-8570