Spazio europeo dei dati sanitari: nuovi danni e profili di responsabilità civile

Nicoletta Muccioli
Ricercatrice dell'Università di Roma Tor Vergata

Quanto all'individuazione dell'*incipit* del discorso, il compito assegnatomi – di trattare, con il dovuto sforzo di sintesi, dei profili di responsabilità collegati all'istituzione ed all'operatività (ancora *in fieri*) dello spazio europeo dei dati sanitari[1] – è favorito dall'esistenza, nel corpo del regolamento EHDS, di una specifica disposizione, contenuta all'art. 100, a mente della quale "*Qualsiasi persona fisica o giuridica che subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere un risarcimento, conformemente al diritto dell'Unione e nazionale*".

Il tenore della norma appena citata rende altrettanto agevole prospettare il successivo passaggio del discorso, indirizzando verso la lettura, in chiave sinottica, di un'altra disposizione di stile e contenuto analoghi. Mi riferisco ovviamente all'art. 82 GDPR, che recita: "*Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento*".

L'analogia tra le due norme è manifesta (tanto da aver fatto persino dubitare della necessità di quella che, *prima facie*, appare una mera duplicazione); analogia, peraltro, rafforzata dalla circostanza che entrambe le norme trovano collocazione all'interno di plessi regolamentari, di rango europeo, deputati alla disciplina della protezione e della circolazione dei dati[2].

---

[1] Il presente scritto riproduce la relazione, integrata con note bibliografiche e di approfondimento, presentata al Convegno in tema di "Spazio europeo dei dati sanitari e sanità digitale", tenutosi il 28 ottobre 2025 presso il Dipartimento di Giurisprudenza dell'Università di Foggia.

[2] Cfr. Ricciuto, *Base giuridica del trattamento del dato sanitario nel contesto dell'EHDS*, in 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, 9 ss.; Faillace, *I diritti dell'interessato nell'uso primario dei dati sanitari elettronici secondo il nuovo regolamento EHDS*, in *Contr. e impr.*, 2025, 379 ss., per un raffronto tra GDPR e regolamento EHDS, quale "approfondimento normativo «vertica-

Come noto, l'interpretazione dell'art. 82 GDPR ha costituito, di recente, l'oggetto di un ampio dibattito, non solo dottrinale[3]. Il biennio 2023-2024 (tempistica perfettamente coerente con l'entrata in vigore, nel 2018, del GDPR) ha visto, infatti, susseguirsi una serie di pronunce della CGUE in materia, tutte accomunate dall'intento di tratteggiare, su un piano sistematico, lo schema della fattispecie risarcitoria *ex* art. 82, con riguardo alla funzione, ai presupposti e criteri di imputazione e, soprattutto, alla perimetrazione del danno risarcibile.

Vi è allora da chiedersi se, in virtù della segnalata affinità, le acquisizioni della Corte europea siano estensibili al rimedio risarcitorio di cui all'art. 100 regolamento EHDS.

Oppure si tratta di "falsi amici" (*false friends*), come quelle parole di una lingua straniera che si assomigliano nella forma (scrittura o pronuncia) ma hanno significati completamente differenti?

Qualche sovrapponibilità risulta, in effetti, predicabile. La similitudine, come si diceva, investe, senza dubbio, lo stile, cui si associa la coincidenza, invero solo parziale, dell'ambito applicativo (i.e. la materia dei dati).

La nuova normativa introduce, come noto, un sistema organico di regole, deputato a gestire, in modo sicuro, etico, interoperabile e in un'ottica di *governance* digitale unificata a livello UE, la condivisione, supportata da un'infrastruttura digitale europea[4], dei dati sanitari elettronici a fini di cura (uso primario) e di ricerca (uso secondario)[5]. Si trat-

---

le» o «settoriale» del Data Governance Act" (382).

[3] A mo' di mero compendio della vastissima letteratura, Salanitro, *Illecito trattamento dei dati personali e risarcimento del danno nel prisma della Corte di giustizia*, in *Riv. dir. civ.*, 2023, 438 ss.; Scognamiglio, *Danno e risarcimento nel sistema del Rgpd: un primo nucleo di disciplina eurounitaria della responsabilità civile?*, in *NGCC*, 2023, 1150 ss.; Baldini, *Responsabilità da trattamento illecito dei dati personali: verso uno statuto unionale*, in *Danno e resp.*, 2025, 49 ss.; Cuffaro, voce *Risarcimento del danno e trattamento dei dati personali*, in *Enc. dir.*, *I tematici*, VII, *Responsabilità civile*, diretto da Scognamiglio, Milano, 2024, 1360 ss.; ID., *Il diritto europeo sul trattamento dei dati personali*, in *Contr. impr.*, 2018, 1098 ss; Gambini, *Responsabilità e risarcimento nel trattamento dei dati personali*, in Cuffaro, D'orazio, Ricciuto, *I dati personali nel diritto europeo*, Torino, 2019, 1017 ss.

[4] Si tratta, quanto all'uso primario, della piattaforma europea LaMiaSalute@UE (MyHealth@EU), già operativa in alcuni stati membri (tra i quali l'Italia); per l'uso secondario, di HealthData@eu. La Commissione è ora tenuta a istituire MyHealth@EU come piattaforma di interoperabilità per la salute digitale. La piattaforma fornirà servizi per supportare e facilitare lo scambio di dati sanitari personali tra i punti di contatto nazionali per la salute digitale. Ogni Stato membro designerà un punto di contatto nazionale, che consentirà lo scambio di dati sanitari personali (EHD) sulla base del formato di scambio europeo, ora obbligatorio. Gli Stati membri potranno fornire servizi e infrastrutture sanitarie digitali transfrontalieri supplementari (art. 24).

[5] Cfr. Morace Pinelli, *Riflessioni introduttive sul Regolamento c.d.* EHDS, in Morace Pinelli (a cura di), *Sanità digitale. Regolamento "EHDS" (UE 2025/327) sullo spazio europeo dei dati sanitari*, cit., I; Orlando, *Il regolamento EHDS nel sistema del nuovo diritto europeo dei dati*, ivi, 81 ss.; Corso, *Lo spazio europeo dei dati sanitari. Prime riflessioni sul regolamento UE 2025/327*, in *NLCC*, 2025, 563 ss.; Sandulli, *Introduzione*, in Thiene e Corso (a cura di), *La protezione dei dati sanitari. Privacy e innovazione tecnologica tra salute pubblica e riservatezza*, Napoli, 2023, 1 ss.

ta, quindi, di un *framework* europeo pensato per favorire ricerca, innovazione e *policy-making*.

Sicché, sin da principio pare possibile affermare che il legame tra regolamento EHDS e GDPR è definibile in termini di integrazione[6]: il primo amplia il secondo, foriero di nuove opportunità, ma anche di nuovi rischi e conseguenti responsabilità.

Il regolamento EHDS conforma i diritti già regolati nel GDPR, specificandone le prerogative per adattarli al contesto dello spazio europeo dei dati sanitari[7]; allo stesso tempo, ne introduce alcuni nuovi[8] ed affronta nuove questioni correlate alla circolazione dei dati, quali ruolo e peso dell'autonomia e delle scelte dell'interessato con riguardo agli aspetti *procedimentali* dell'uso primario. Quanto all'uso secondario, in una cornice di bilanciamento tra dimensione individuale e interessi generali, il regolamento articola la disciplina della condivisione e dell'accesso ai dati sanitari, e "lascia impregiudicato l'accesso ai dati sanitari elettronici per l'uso secondario concordato nel quadro di accordi contrattuali o amministrativi tra soggetti pubblici o privati" (art. 1 comma 8).

Una lettura appena più attenta del contenuto delle disposizioni in questione disvela, però, come la fattispecie di cui all'art. 82 GDPR sia tratteggiata, almeno tendenzialmente[9], in modo da poter essere autosufficiente, a differenza di quella di cui all'art. 100

---

[6] Cfr. Faillace, *op. cit.*, 383 ss.

[7] Cfr. Ó Cathaoir, *The EHDS and Electronic Health Records. GDPR+ or Transforming Patients' Rights?*, in Slokenberga, Ó Cathaoir, Shabani (*edited by*), *The European Health Data Space. Examining A New Era in Data Protection*, London and New York, 2025, 22 ss.: "*the European Health Data Space (EHDS) aims to revolutionise individuals' access to and control over their EHD. The Regulation supports the European Commission's ambitious vision to grant all European Union (EU) residents' access to their EHR by 2030. It concretises the rights provided for under the GDPR and transforms the voluntary provisions in Article 14 of the Patients' Rights Directive into binding obligations across the Union*"; Solinas, *Dal diritto d'accesso dell'interessato nel GDPR al diritto all'accesso del paziente e del personale sanitario nell'EHDS*, in Morace Pinelli (a cura di), *Sanità digitale. Regolamento "EHDS" (UE 2025/327) sullo spazio europeo dei dati sanitari*, cit., 121 ss. Come osserva Caggiano, *Interessi e norme nell'ecosistema europeo dei dati sanitari*, ivi, 23, «appare evidente come nel quadro della tecno-regolazione che è tecnica normativa ormai non evitabile in una realtà completamente digitalizzata, i diritti prendano forma sugli artefatti tecnologici, i quali condizionano in maniera diretta ciò che le persone possono o non possono fare e che quindi sono pre-condizione per l'attribuzione di diritti».

[8] Ad esempio, ai sensi dell'art. 5, le persone fisiche o i loro rappresentanti hanno il diritto di inserire informazioni nella propria cartella clinica elettronica attraverso servizi o applicazioni di accesso ai dati sanitari elettronici collegati a tali servizi (diritto di inserimento, corredato dalla previsione che le informazioni inserite dall'interessato dovranno essere chiaramente distinguibili come tali); ai sensi dell'art. 8, le persone fisiche hanno il diritto di limitare l'accesso dei professionisti sanitari e dei prestatori di assistenza sanitaria alla totalità o a parte dei loro dati sanitari elettronici personali (diritto di esclusione). Cfr. Grisafi, *Il diritto di opporsi ed escludere il trattamento dei dati personali sanitari per uso secondario*, in Morace Pinelli (a cura di), *Sanità digitale. Regolamento "EHDS" (UE 2025/327) sullo spazio europeo dei dati sanitari*, cit., 295 ss.

[9] È ricorrente, del resto, l'affermazione che l'art. 82 GDPR "somiglia ad un frammento di norma" (Pagliantini, *Un altro palcoscenico della «guerra» tra le corti: il danno (immateriale) bagatellare dell'art. 82 GDPR*, in *Foro it.*, 2023, IV, 285, commento a CGUE 4 maggio 2023, causa C-300/21); un

regolamento EHDS, che è invece connotata dall'espresso rinvio al diritto dell'Unione, preso in considerazione nel suo complesso[10], ed al diritto dei singoli stati.

Ed invero, la fondamentale premessa ermeneutica dalla quale, in tutte le suddette pronunce relative all'art. 82 GDPR, la Corte Europea prende le mosse è proprio nel senso che, in mancanza di un esplicito rinvio al diritto degli Stati membri, il significato di una disposizione di un regolamento europeo deve essere ricavato procedendo ad una interpretazione uniforme e autonoma della stessa, quale emergente dalla normativa dell'UE e dalla giurisprudenza della Corte di Giustizia. A dire della Corte, una volta consacrata la singola regola a livello europeo, la stessa deve essere immediatamente fatta propria dall'ordinamento interno – in virtù del primato del diritto dell'Unione – a prescindere dalla sua disarmonia rispetto al modello municipale.

Nonostante la consistenza "sdogmatizzata" (come l'ha, assai bene, descritta Carmelita Camardi[11]) della struttura dell'art. 82, dalla lettura di queste prime pronunce, può ricavarsi una – seppur ancora embrionale ed appena abbozzata – istanza sistematica.

Una acquisizione che emerge in modo univoco dalle pronunce della CGUE è la struttura tripartita dell'illecito ai sensi dell'art. 82, costituito *i)* dalla violazione del regolamento, *ii)* dal danno, materiale o immateriale e *iii)* dal nesso di causalità tra violazione e danno[12].

"testo senza contesto", secondo Navone, *Ieri, oggi e domani della responsabilità civile da trattamento illecito dei dati personali*, in *NLCC*, 2022, 158.

[10] È appena il caso di rammentare come il regolamento EHDS sia collegato a già esistenti ed in via di messa a punto soluzioni legislative europee in materia di dati, di dispositivi medici, di AI e di *cybersecurity*.

[11] Camardi, *Note critiche in tema di danno da illecito trattamento dei dati personali*, in *Jus civile*, 2020, 789 ss., spec. 791.

[12] Cfr. Patti, *Il risarcimento del danno immateriale secondo la Corte di Giustizia*, in *NGCC*, 2023, 1146 ss.

Con ciò vuol dirsi che, una volta accertata la violazione del regolamento, il danno, materiale e/o immateriale, causato da detta violazione è risarcibile in quanto sussistente, imputabile e causalmente collegato alla violazione del regolamento. La sola violazione non è ritenuta sufficiente in sé a far nascere il diritto al risarcimento, bensì è necessario che l'offeso abbia subito un danno materiale o immateriale e che possa provarlo in giudizio. Pertanto, ad avviso della Corte europea, per stabilire un diritto concreto al risarcimento, occorre che il reclamante fornisca prove dell'effettivo pregiudizio subito come risultato diretto della non conformità al regolamento: non sussiste il danno *in re ipsa*. In stretto collegamento logico con l'affermazione della necessaria sussistenza di un danno, sia esso materiale o immateriale, sta l'attestazione ricorrente per cui l'articolo 82 del RGPD deve essere interpretato nel senso che il diritto al risarcimento previsto a tale disposizione svolge una funzione compensativa, laddove il risarcimento pecuniario fondato su detta disposizione è volto a compensare integralmente il danno concretamente subito a causa della violazione di tale regolamento, e non una funzione punitiva. A questo proposito, la Corte ribadisce che l'articolo 82 riveste una funzione non afflittiva, bensì compensativa, contrariamente ad altre disposizioni di tale regolamento del pari contenute al capo VIII di quest'ultimo, ossia i suoi articoli 83 e 84, che svolgono, dal canto loro, una finalità sostanzialmente punitiva, dato che consentono di infliggere, rispettivamente, sanzioni amministrative pecuniarie ed altre sanzioni. L'articolazione tra le norme sancite in detto articolo 82 e quelle sancite in detti articoli 83 e 84 dimostra che esiste una differenza tra queste due categorie

Più specificamente, la Corte è stata chiamata a pronunciarsi su quello che Stefano Pagliantini ha definito il "quesito che ammalia"[13], ovvero: se l'art. 82 GDPR "codifichi un limite minimo di offensività e gravità della condotta illecita oppure se ogni danno immateriale, e quindi pure il timore di aver perduto il controllo sui propri dati, sia meritevole, quale che sia la sua entità, di una tutela risarcitoria".

La Corte, sul punto, ha rilevato come la nozione di danno (materiale o immateriale) non sia ulteriormente qualificata dall'art. 82 GDPR e che, pertanto, non è richiesto il superamento di una determinata soglia di gravità. Si osserva, peraltro, come subordinare il risarcimento al raggiungimento di un determinato livello di gravità del danno rischierebbe di pregiudicare gli obiettivi di uniformazione giuridica del Regolamento, determinando una indesiderabile frammentazione nell'applicazione del rimedio a causa della diversa valutazione ad opera delle corti municipali.

Ai fini, dunque, dell'art. 82 GDPR, espressione di un autonomo e autosufficiente formante eurounitario, non si pone un problema di selezione dei danni risarcibili (con criteri quali l'ingiustizia e la gravità), quanto piuttosto un problema di sussistenza, che porta con sé le questioni della prova e della quantificazione, entrambe rimesse ai giudici nazionali.

Sicché, provando a tirare le fila, 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. La declamazione è nel senso che ogni danno, materiale o immateriale, non importa quanto piccolo, è suscettibile di riparazione[14].

---

di disposizioni, ma anche una complementarità, in termini di incentivo a rispettare il RGPD, fermo restando che il diritto di chiunque a chiedere il risarcimento di un danno rafforza l'operatività delle norme di protezione previste da tale regolamento ed è atto a scoraggiare la reiterazione di comportamenti illeciti. Sul punto, cfr. Scognamiglio, *I nuovi percorsi del risarcimento del danno, tra diritto nazionale e disciplina eurounitaria della responsabilità civile*, in *www.lavorodirittieuropa.it*, 2024, 10 ss.

[13] Pagliantini, *op. cit*., 286. Cfr. anche, sempre a margine di CGUE 4 maggio 2023, causa C-300/21, Federico, *«La tempesta perfetta»: ultime dalla Corte di Lussemburgo su danno (non patrimoniale) da illecito trattamento dei dati personali e possibili risvolti in tema di tutela collettiva*, in *Foro it.*, 2023, IV, 293, per l'interessante rilievo nel senso che "la pronuncia che si riporta, pur avendo avuto origine a partire da una controversia individuale, sembra essere particolarmente importante nell'ottica della costruzione di un sistema di ricorsi collettivi a tutela degli interessati. Proprio l'aggregazione dei danni «irrisori» è una delle finalità principali delle azioni di gruppo. Queste, difatti, riescono a garantire le pretese individuali di piccola entità che, altrimenti, rimarrebbero sprovviste di protezione, in quanto i costi e le tempistiche necessarie ad intentare un processo in via individuale supererebbero di gran lunga l'ammontare dell'eventuale risarcimento del danno. Alla luce della sentenza della Corte di Lussemburgo, poiché l'irrisorietà del danno, nel caso di una lesione al diritto alla protezione dei dati personali, non osta ad ottenere un risarcimento, è ragionevole ritenere che ciò potrebbe facilitare la possibilità di dedurre in giudizio numerose pretese individuali, anche se di piccola entità, mediante i ricorsi collettivi".

[14] 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 poten-

Insomma: mai futile il danno non patrimoniale da violazione della *privacy*, purché lo si provi[15]!

Non è evidentemente questa la sede per sviluppare il tema del danno immateriale di matrice europea. Basti qui sottolineare che, per la prima volta a chiare lettere, si afferma che le nozioni di danno e di risarcimento debbano essere considerate quali nozioni autonome del diritto dell'Unione[16].

Se così è, mi sembra che il concetto di danno immateriale asseverato dalla corte europea potrebbe valere anche in sede di spazio europeo dei dati sanitari (come del resto è espressamente affermato al considerando 101 del regolamento EHDS: "Il concetto di danno dovrebbe essere interpretato in senso lato alla luce della giurisprudenza della Corte di giustizia dell'Unione europea in modo tale da rispecchiare pienamente gli obiettivi del presente regolamento").

L'art. 82 GDPR si compone, invero, di altri commi che danno maggior compiutezza alla disciplina del rimedio risarcitorio.

---

ziale 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".

A meglio definire l'orientamento della corte europea, merita, inoltre, menzione la pronuncia della CGUE del 25 gennaio 2024 C-687/21. Di particolare interesse la formulazione del relativo quesito: "Se sussista un danno morale ai sensi dell'articolo 82 del RGPD anche allorché il terzo, che aveva ricevuto il documento con i dati personali, non sia venuto a conoscenza di tali dati prima della restituzione della documentazione cartacea contenente le informazioni, oppure se a tal fine sia sufficiente il disagio del soggetto i cui dati personali erano stati trasmessi illegalmente, in quanto in ogni caso di rivelazione non autorizzata di dati personali non è possibile escludere l'eventualità che i dati vengano ulteriormente diffusi a un numero di soggetti non identificati o addirittura utilizzati in modo improprio". La Corte qui, citando i precedenti del 2023, ha affermato che il timore di un potenziale utilizzo abusivo dei suoi dati personali da parte di terzi che un interessato nutre a seguito di una violazione del regolamento può, di per sé, costituire un «danno immateriale», ai sensi dell'art. 82, che dà diritto al risarcimento, a condizione che si dimostri di aver effettivamente subito un simile danno, per quanto minimo, tenendo presente che la mera violazione delle disposizioni di detto regolamento non è sufficiente a dare fondamento alla pretesa risarcitoria. Ad avviso della Corte, resta il fatto che chi esercita un'azione di risarcimento fondata sull'articolo 82 GDPR ha l'onere di dimostrare l'esistenza di un danno del genere. In particolare, un rischio puramente ipotetico di utilizzo abusivo da parte di un terzo non autorizzato, come nel caso in cui nessun terzo sia venuto a conoscenza dei dati personali di cui trattasi, non può dare luogo a un risarcimento.

[15] Citando l'efficace titolo del commento alla decisione della CGUE 4 maggio 2023, causa C-300/21 a firma di Palmieri, Pardolesi, *Mai futile il danno non patrimoniale da violazione della privacy (purché lo si provi!)*, in *Foro it*., 2023, IV, 278.

[16] Nel commentare CGUE 4 maggio 2023, causa C-300/21, è stato riconosciuto alla decisione di aver posto "le direttive per una dogmatica europea della responsabilità civile per la causazione di un danno non patrimoniale, quantomeno nel campo della lesione dei diritti della persona per trattamento illecito dei dati personali" (Camardi, *Illecito trattamento dei dati e danno non patrimoniale. Verso una dogmatica europea*, in *NGCC*, 2023, 1136).

In particolare, al comma 3, si prevede che "Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, (...) se dimostra che l'evento dannoso non gli è in alcun modo imputabile".

Malgrado la scarnificazione concettuale della sua struttura, dall'art. 82 GDPR affiora, dunque, un modello di responsabilità incentrato sulla "violazione del regolamento" cui è abbinato un criterio di imputazione, che viene declinato in guisa di esimente (di esonero dalla responsabilità) e formulato in termini assolutamente generici ("in alcun modo imputabile")[17].

Nulla si dice circa la natura della responsabilità (ritenuta dai più extracontrattuale) e della relativa disciplina, lasciando all'interprete il compito di interrogarsi su questioni cruciali quali il criterio soggettivo dell'imputazione (se oggettiva o per colpa), l'atteggiarsi della causalità, e, di conseguenza, la 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, nonché la determinazione della responsabilità del titolare del trattamento (se vicaria, in virtù del rapporto organico, o per colpa – *in eligendo* e/o *in vigilando* – seppure presunta) per errore di un dipendente[18]. Quanto agli oneri probatori ed ai criteri di valutazione, nell'ermeneusi compiuta dalla CGUE, vien fatto rinvio alle soluzioni normative (e giurisprudenziali) dei singoli stati membri.

Si ricava, innanzitutto, dalla norma che si tratta di una responsabilità determinata dalla inosservanza delle prescrizioni regolamentari. Nella imputazione del danno al candidato responsabile, si prende in considerazione un dato che "sporge" oltre il mero nesso causale di derivazione del danno dalla condotta, consistente nella difformità della medesima da regole cautelari generali e/o specifiche, in vista del bilanciamento tra la tutela del danneggiato e l'esigenza di non inibire lo svolgimento di attività ritenute economicamente e socialmente meritevoli ed in linea con un utilizzo efficiente, in una prospettiva di sistema, dello strumento risarcitorio.

In prima approssimazione, potrebbe, allora, affermarsi che siamo di fronte ad una responsabilità per colpa, salvo poi intendersi sul contenuto da attribuire a tale criterio di imputazione.

In dottrina, la previsione della possibilità di difesa del candidato responsabile mediante la dimostrazione della non imputabilità «in alcun modo» del danno medesimo, ha orientato due opposte letture della regola di imputazione, l'una in chiave oggettiva[19]; l'al-

---

[17] Salanitro, *Illecito trattamento dei dati personali e risarcimento del danno nel prisma della corte di giustizia*, cit., 433.

[18] Su tali questioni, di recente, diffusamente, Locatello, *Adeguata gestione del rischio e presunzione di colpa nell'imputazione del danno da illecito trattamento di dati personali*, in *Contr. impr.*, 2024, 1215 ss., 1220 ss.

[19] Ed invero, anche laddove il criterio di imputazione viene espresso in termini di responsabilità oggettiva, si attribuisce rilevanza alla mancata dimostrazione dell'adozione delle misure adeguate ad evitare il danno, dando rilievo alla condotta del candidato responsabile, così da stemperare la valutazione della imputazione della responsabilità in termini di *secco* causalismo. Cfr. Camardi, *Note critiche*

tra, nei termini di una presunzione di colpa[20], con aggravamento (secondo taluni) della misura di diligenza esigibile (ricorre, infatti, l'espressione "colpa aggravata"[21]).

Eccentrica rispetto a tale ripartizione, che, per vero, annovera (tanto nell'uno quanto nell'altro versante) posizioni più sfumate e vere e proprie "zone grige", l'idea, pure avanzata in dottrina, di fare riferimento al modello di responsabilità di cui all'art. 1218 c.c., facendo perno sull'elemento della violazione del GDPR, intesa quale inadempimento di un'obbligazione di fonte legale[22].

Più articolata, ed incline a valorizzare il tratto originale della norma europea, è la ricostruzione che ravvisa una sorta di coesistenza, nell'alveo della stessa disposizione (l'art. 82), di diversi criteri di imputazione, la cui applicabilità dipenderebbe dal grado di rischio e pericolo della singola attività di trattamento[23].

---

in tema di danno da illecito trattamento dei dati personali, cit., 797, nel senso che "il titolare risponderà dei danni derivanti dalla mancata adozione di (altre) misure tecnicamente possibili e proporzionate alle risultanze di quella valutazione, e non risponderà dei danni che erano stati esclusi da quella valutazione, se correttamente svolta, in quanto non prevedibili o altamente improbabili o non rimediabili allo stato dell'arte. Egli, dunque, non risponde del fortuito, classicamente inteso (ad esempio, un attacco *hacker* grave e generalizzato"; si interroga circa la portata dell'esimente prevista dalla norma, se essa implichi la prova della mancanza del nesso causale o di altra circostanza, con effetto liberatorio, di tipo oggettivo, Lucchini Guastalla, *Il nuovo regolamento europeo sul trattamento dei dati personali*, in *Contr. impr*., 2018, 124 s. Il Maestro della responsabilità da rischio di impresa nella prospettiva di analisi economica del diritto, specifica, del resto, come, a fronte di attività socialmente e/o economicamente utili sebbene intrinsecamente pericolose, sia opportuno limitare la responsabilità prevedendone l'esclusione per i danni derivanti da un rischio incalcolabile, assolutamente eccezionale e imprevedibile (Trimarchi, *La responsabilità civile: atti illeciti, rischio, danno*, Milano, 2021, 275 s.). Per una nozione di caso fortuito coincidente con un fatto non evitabile con l'ordinaria diligenza: Patti, *Il declino della responsabilità oggettiva (a margine del 2051 c.c.)*, in *Riv. dir. civ.*, 2019, 977 ss. In tema, anche Scoditti, voce *Danno da cose in custodia*, in *Enc. dir*., *I tematici*, VII, *Responsabilità civile*, diretto da Scognamiglio, Milano, 2024, 281 ss.

[20] Cfr. Gambini, *Responsabilità e risarcimento nel trattamento dei dati personali*, cit., 1048 s.; Caterina, Thobani, *Il diritto al risarcimento dei danni*, in *Giur. it.*, 2019, n. 12, 2807.

[21] Cfr. le conclusioni dell'Avvocato Generale Giovanni Pitruzzella, del 27 aprile 2023 Causa C-340/21: "Il danno da violazione dei dati personali può configurarsi quale conseguenza colposa della mancata adozione delle misure tecniche e organizzative ragionevoli e comunque adeguate a scongiurarlo, tenuto conto dei rischi per i diritti e le libertà delle persone connessi all'attività di trattamento. Tali rischi rendono l'obbligo di prevenire ed evitare il danno più rigoroso, ampliando il dovere di diligenza incombente sul titolare del trattamento. Pertanto, dalla lettura coordinata degli obblighi di condotta in capo ai titolari del trattamento e della previsione sulla prova liberatoria posta a carico del danneggiante, è possibile trarre argomento in favore del riconoscimento della natura di responsabilità aggravata per colpa presunta alla fattispecie di responsabilità da illecito trattamento di dati personali disegnata dall'articolo 82 del Regolamento».

[22] Bravo, *Riflessioni critiche sulla natura della responsabilità da trattamento illecito dei dati personali*, in Zorzi, Galgano (a cura di), *Persona e mercato dei dati. Riflessioni sul GDPR*, Padova, 2019, 383; Zecchin, *Molteplicità delle fonti e tutela dei diritti. Il danno non patrimoniale nella lesione della proprietà e dei dati personali*, in *Eur. e dir. priv*., 2022, 517 ss.

[23] Per tale impostazione, vd. Salanitro, *Illecito trattamento dei dati personali e risarcimento del danno nel prisma della corte di giustizia*, cit., 429 nt. 9 e 445 ss.

Venendo alla soluzione della corte europea, discostandosi dalle conclusioni dell'Avv. Campos Sánchez-Bordona – che esplicitamente propendeva per una imputazione di tipo oggettivo[24] – la CGUE[25] ha ravvisato, altrettanto chiaramente, nell'art. 82 una fattispecie fondata su un «meccanismo di responsabilità per colpa accompagnato da un'inversione dell'onere della prova» (§ 98). Il danneggiato non sarà, pertanto, tenuto a provare il dolo o altra negligenza nell'attività di trattamento, essendo questi aspetti presunti sino a prova contraria, per il fatto che v'è stata un'attività di trattamento violativa del GDPR e produttiva di danno.

Ebbene, mi sembra che, specie avuto riguardo alla 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 AI) –, la configurazione dei profili di responsabilità per i danni occorsi a livello di spazio europeo dei dati sanitari debba piuttosto riferirsi ad una pluralità di modelli rimediali e che la polarizzazione dei criteri di imputazione secondo la secca alternativa colpa/responsabilità oggettiva non si riveli esaustiva[26].

Senza dubbio, tanto nel GDPR, che rappresenta il prototipo, quanto nel regolamento EHDS è possibile cogliere la medesima ottica di riduzione al minimo di falle organizzative ed eventi avversi, in linea con il sempre più sentito approccio, ispirato al *Risk Management*, in termini di "responsabilità c.d. proattiva" (di *accountability*)[27].

---

[24] Conclusioni presentate il 25 maggio 2023, spec. §§ 93 ss.

[25] In particolare, cfr. CGUE 21 dicembre 2023, C-667/21, in *Riv. Dir. Internaz. Priv. e Proc.*, 2024, IV, 1367, in cui la Corte afferma che la responsabilità per trattamento illecito dei dati personali è da intendersi come una responsabilità per colpa per due ragioni. Da un lato, questa conclusione si evince dal contesto in cui si colloca l'art. 82 GDPR, poiché gli artt. 24 e 32 dello stesso atto normativo prevedono che il titolare del trattamento sia tenuto ad *evitare* l'evento dannoso, *per quanto possibile*, adottando delle misure adeguate al tipo di trattamento svolto e al rischio che ne scaturisce. Sarebbe quindi illogico, a detta di questa pronuncia, imporre poi allo stesso soggetto di risarcire *qualsiasi* danno provocato dalla sua attività, a prescindere da ciò che egli ha fatto per limitare le probabilità che questo venisse ad esistenza. La seconda ragione per cui il fondamento della responsabilità viene individuato nella colpa è che questa viene concepita come la soluzione più adeguata a perseguire l'obiettivo di bilanciare l'interesse di chi svolge il trattamento dei dati con quello degli interessati, poiché l'adozione di un sistema di responsabilità oggettiva propenderebbe troppo a favore di questi ultimi. Sulla medesima linea, CGUE 25 gennaio 2024 C-687/21, § 52; CGUE 20 giugno 2024 C-182/22 e C189/22, § 28. Quanto ai rimedi concreti, cfr. CGUE 4 ottobre 2024 C-507/23, con commento di Venchiarutti, *Ancora sulla responsabilità per violazione del Rgpd: la presentazione di scuse come risarcimento del danno non patrimoniale*, in *NGCC*, 2025, 107 ss.

[26] Più in generale, per una rivisitazione critica della contrapposizione tra responsabilità per colpa e responsabilità per rischio volta ad evidenziare un quadro più mosso dei criteri di imputazione, cfr. Salvi, *La responsabilità civile*, Milano, 2019, 3° ed., 160 ss.; Castronovo, *Diritto positivo, dogmatica e teoria generale nella responsabilità oggettiva*, in *Eur. dir. priv*., 2021, 684 ss. Cfr., da ultimo, Salanitro, *I criteri di imputazione della responsabilità civile alla luce del quadro normativo eurounitario*, in *Riv. dir. civ.*, 2025, 896 ss. part. 903 ss.

[27] Cfr. Finocchiaro, *Il principio di* accountability, in *Giur. it.*, 2019, n. 12, 2778 ss.

Nella logica della *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 (a livello amministrativo) indipendentemente dal verificarsi di un danno.

Ed è innegabile che tale rilievo della *accountability* (*ex ante*) si rifletta sul piano della responsabilità per i danni (*ex post*, intesa come *liability*)[28].

Come si ricava dalle argomentazioni della CGUE, la colpa, quale criterio di imputazione della responsabilità, sembra godere di una crescente vitalità. Ebbene, proprio la colpa, che aveva perso la centralità riconosciutale dall'ottocentesca ricostruzione jheringiana a fronte delle istanze della società industriale, riceve, nell'attuale era della tecnica, nuova linfa, quale criterio di imputazione meglio in grado di coniugare le diverse istanze di tutela; istanze tutte, anche quelle della persona, declinate, nel momento storico attuale, secondo una logica promozionale dell'uso della tecnologia e della AI (che non possono fare ameno di un uso sempre più massivo di dati e della loro condivisione). La colpa indossa allora la veste del difetto di adeguata organizzazione in capo a chi è tenuto a prevenire e mitigare i rischi connessi all'esercizio di una determinata attività[29].

Nella concretizzazione della colpa, in tale accezione *oggettiva* e *normativa*[30], si pone allora la questione di comprendere se la dimostrazione della *compliance* a standard di sicurezza e prevenzione sia sufficiente ad integrare la prova liberatoria nei termini di cui al comma 3 dell'art. 82, oppure se, in virtù della valorizzazione della colpa/diligenza parametrata allo specifico contesto applicativo, la corretta messa in opera delle cautele

---

[28] Cfr. Bernes, D*alla responsabilità civile alla responsabilità sociale d'impresa nella protezione dei dati personali: alla ricerca del rimedio effettivo*, in *Actualidad Jurídica Iberoamericana*, 2023, 658 ss. part. 665 ss.

[29] Una siffatta impostazione è condivisa anche nella sfera propria della responsabilità penale, laddove la colpa viene è stata definita come "il *calco di una valutazione giuridica*: ovvero *la risultante di una sequenza diagnostica incentrata su norme*: o meglio ancora l'*ordinata riproduzione delle condizioni imputative previste dall'ordinamento* per poter ascrivere un danno involontario a un individuo". Cfr. Micheletti, *Il criterio della competenza sul fattore di rischio concretizzatosi nell'evento. L'abbrivio dell'imputazione colposa*, in *Criminalia*, 2015, 510-511, il quale concilia tale concezione oggettiva della colpa con il principio di personalità della responsabilità penale, specificando come "la genesi personalistica del fatto colposo meglio è garantita dal criterio della competenza, e quindi dalla preliminare determinazione del soggetto che doveva e poteva esercitare una controspinta ostativa alla verificazione dell'evento offensivo. Un siffatto approccio non può prescindere infatti dalla titolarità dei doveri e dalla effettività dei connessi poteri di gestire il rischio che si è materializzato nella storia, in ragione del *ruolo* svolto dal singolo soggetto e degli *obblighi* che ne discendono. È dunque la «doverosa dominabilità del fattore di rischio» – anziché l'anodino riscontro causale – sul quale dovrebbe farsi affidamento per congegnare un modello d'imputazione colposa autenticamente conforme al principio di personalità".

[30] Cfr., con specifico riguardo alla responsabilità contrattuale, ma con ricchezza di spunti sulla concezione della colpa in diritto civile, D'amico, *La colpa contrattuale*, in *Contratti*, 2025, 393 ss., ove, in più passaggi, *dialoga* con Piraino, voce *Dolo e colpa (responsabilità civile)*, in *Enc. dir*., *I tematici*, VII, *Responsabilità civile*, diretto da Scognamiglio, Milano, 2024, 554 ss. part. 564.

nello specifico caso concreto dovrà essere oggetto di vaglio nel corso del giudizio di responsabilità, onde evitare di rendere l'incombente un mero adempimento burocratico/formale pure inficiato dal vizio di autoreferenzialità[31].

Poiché, nella logica del GDPR, al titolare del trattamento è rimessa la determinazione e l'implementazione degli strumenti di prevenzione adeguati, tenendo conto del livello di rischio e degli interessi in gioco, è apparso preferibile, nondimeno, ritenere che sia riservata al giudice ("sollecitato dalle allegazioni motivate dell'attore") la sindacabilità circa la sussistenza e l'adeguatezza di dette misure preventive, avendo particolare riguardo alla corretta determinazione del "punto di equilibrio" delle diverse istanze, da individuarsi in base ai parametri, espressamente specificati nel GDPR, della natura, dell'ambito di applicazione, del contenuto e delle finalità, nonché dei rischi o dello stato dell'arte e dei costi di attuazione (artt. 5, 24, 25 e 32 GDPR)[32].

Vi è allora di chiedersi se una siffatta impostazione, condivisa, come si diceva dalla CGUE con riguardo all'art. 82 GDPR, possa essere predicata anche per i danni occorsi nell'ambito dello spazio europeo dei dati sanitari.

Occorre, al riguardo, mettere a tema alcune considerazioni.

In primo luogo, viene in rilievo il peculiare statuto dei dati sanitari[33], la cui *governance* richiede, non solo un *surplus* di cautele in via preventiva, ma anche un elevato *grado di tutela*, e che, pertanto, potrebbe sospingere verso la rievocazione della figura del *danno in re ipsa*, o, comunque, ferma restando la necessità di provare la sussistenza della lesione, potrebbe alimentare il dibattito "nostrano" circa il superamento della dicotomia danno evento/danno conseguenza, specie nel caso in cui dalla violazione del regolamen-

---

[31] Quello della concretizzazione, alla luce della logica dell'*accountability*, della colpa /diligenza nel giudizio di responsabilità per danni è, del resto, un tema delicato. Si è, infatti, condivisibilmente, osservato che "in una prospettiva critica, l'idea di *compliance*, intesa come conformità preventiva e tecnico-organizzativa a un insieme di obblighi normativi o para-normativi, sembra porsi in tensione con una concezione del diritto come espressione e regolazione del conflitto sociale"; e che "sembra in ogni caso imporsi la visione di un diritto che non nasce più dal conflitto, ma dall'adattamento, e che rischia perciò di svuotare la sua dimensione emancipativa e trasformativa, che per molto tempo si è giovata in maniera peculiare degli strumenti della responsabilità civile" (Viglione, *Diritto privato europeo transnazionale? Il caso della responsabilità civile*, in *Riv. dir. civ.*, 2025, 893 e 894).

[32] In tale ottica si pone l'analisi di Barcellona, *La Responsabilità civile*, vol. VI, *Le fonti delle obbligazioni diverse dal contratto*, tomo I, 2° ed. 2025, in *Trattato di diritto privato* diretto da Mazzamuto, 2025, 108-109, il quale chiosa: "Dunque, il dispositivo della presunzione, disponendo che il titolare debba provare di aver adottato «misure tecniche e organizzative adeguate/appropriate», lo sottopone al giudizio di mancato assolvimento dell'onere probatorio quando si possa ritenere che non abbia fatto buon uso del potere di determinare il punto di equilibrio normativo e/o di non aver osservato rispetto a tale punto di equilibrio il criterio della adeguatezza/appropriatezza delle misure da adottare. Quella che il GDPR pone a suo carico, perciò, non è la prova di avere adottato misure, ma la prova di aver determinato correttamente il *punto di equilibrio* al quale le norme impongono di commisurare le misure da adottare e l'ulteriore prova dell'*adeguatezza* delle misure adottate rispetto a siffatto indisponibile imperativo punto di equilibrio/bilanciamento". Cfr. anche Bernes, *op. cit.*, 667.

[33] Sulla differenza tra "dati sanitari elettronici" e "dati relativi alla salute", cfr. Corso, *op. cit.*, 571 ss.

to derivi l'offesa di diritti e libertà fondamentali travalicante la mera dimensione della protezione dei dati personali[34].

Mi chiedo, peraltro, se, proprio tenuto conto della delicatezza degli interessi (non solo individuali) messi a rischio, oltre allo sviluppo delle tutele in forma collettiva già esistenti, non si possa giungere, *in fieri*, a pensare a modelli di tutela *no fault*, congiunti a forme di copertura assicurativa.

In secondo luogo, può osservarsi come il regolamento EHDS riguardi un ampio spettro di attori pubblici e privati che operano nella raccolta, conservazione o utilizzo dei dati sanitari:

- Aziende sanitarie pubbliche e private, ospedali, ASL, case di cura, laboratori analisi, RSA e poliambulatori (e con essi i DPO e i vari referenti della *compliance* GDPR), che dovranno ripensare modelli e prassi in attuazione dello spazio europeo dei dati sanitari, nonché procedere a nuove valutazioni di impatto, revisione delle informative, classificazione dei trattamenti e valutazione dei fornitori, garantire l'adozione di sistemi di cartelle cliniche interoperabili, applicare nuove modalità di consenso e implementare sistemi per la condivisione sicura dei dati, in modo che possano essere facilmente integrati da diverse fonti, con modalità di accesso conformi ai principi FAIR, ormai famosi, per cui i dati sanitari devono essere reperibili, accessibili, interoperabili e riutilizzabili.
- Fornitori di *software*, ovvero coloro che sviluppano *software* sanitari[35] (cartelle cliniche elettroniche, telemedicina, applicazioni di AI in sanità), per i quali si potrebbe configurare l'eventualità di essere chiamati in causa in veste di produttori.
- Centri di Ricerca che accedano all'uso secondario dei dati clinici per la ricerca, che dovranno, ad es., rispettare requisiti di anonimizzazione, o quanto meno di pseudonimizzazione avanzata, e dimostrare finalità legittime nei progetti di analisi.

---

[34] Mentre la CGUE, con riguardo all'art. 82, ha mantenuto, come si detto, un coeso atteggiamento contrario alla configurabilità di danni *in re ipsa*, l'operatività dello spazio europeo dei dati sanitari potrebbe, plausibilmente, dare nuovo impulso a quelle posizioni dottrinali secondo le quali, posto che per alcuni danni non patrimoniali lo stesso accertamento mediante presunzioni risolve i medesimi in danni *in re ipsa*, giungono ad affermare che, almeno con riguardo ad alcuni diritti fondamentali, la distinzione danno-evento danno-conseguenza andrebbe superata attribuendo rilevanza alla lesione in sé. Cfr. sul tema, più in generale, Alpa, *Danno* in re *ipsa e tutela dei diritti fondamentali (Diritti della personalità e diritto di proprietà)*, in *Resp. civ. e prev*., 2023, 6; con riguardo specifico al danno da illecito trattamento dei dati, Camardi, *Illecito trattamento dei dati e danno non patrimoniale*, cit., 1144, che, senza mezzi termini, afferma: "Riteniamo infatti che la lesione dei diritti fondamentali costituzionalmente rilevanti, attinenti alla persona in quanto tale, alla sua dignità o libertà, alla sua identità, al suo onore, non abbisogni che di essere provata in quanto tale, senza ulteriori allegazioni di danni «conseguenza»"; per interessanti spunti, v. già Thiene, *Segretezza e riappropriazione di informazioni di carattere personale: riserbo e oblio nel nuovo regolamento europeo, in NGCC, 2017,* 441 s. Sebbene in un diverso contesto di fattispecie, sia consentito il rinvio a Muccioli, *In tema di danno da ritardata diagnosi*, in *NGCC*, 2022, 359 ss. part. 363.

[35] Il capo III del regolamento è dedicato alle cartelle cliniche elettroniche e alle applicazioni di benessere.

A ciò si aggiunga che, come innanzi accennato, la gestione delle piattaforme nell'ambito dello spazio europeo dei dati sanitari è strutturata su due livelli principali, uno nazionale e uno europeo.

Ogni Stato membro dell'UE è tenuto alla designazione di specifiche autorità e organismi per gestire le piattaforme a livello nazionale, quali, ad esempio, gli organismi di accesso ai dati sanitari per l'uso secondario (art. 55), incaricati di svolgere i compiti di cui all'art. 57 e rispettare gli obblighi, previsti nei confronti delle sole persone fisiche, di cui all'art. 58; l'autorità di vigilanza del mercato dei sistemi di cartelle cliniche elettroniche (artt. 43, 44, 45 e art. 47 comma 7 con riguardo alle applicazioni per il benessere). Gli Stati membri sono, inoltre, tenuti all'implementazione delle infrastrutture tecniche (nodi nazionali) che si collegheranno alle infrastrutture transfrontaliere MyHealth@EU e HealthData@EU per consentire lo scambio di dati.

La *governance* e il coordinamento generale sono garantiti dalla Commissione Europea, che supervisiona l'implementazione e lo sviluppo del quadro normativo e delle infrastrutture comuni. In sintesi, la gestione operativa delle piattaforme è decentralizzata a livello dei singoli Stati membri attraverso le autorità nazionali designate, mentre la Commissione Europea e gli organismi correlati assicurano un quadro comune e l'interoperabilità a livello dell'intera UE.

Se quello sommariamente tratteggiato è il quadro operativo nel quale si inscrive la norma di cui all'art. 100 regolamento EHDS, appare evidente come la sfera applicativa di quest'ultima include, rispetto alla previsione di cui all'art. 82 GDPR, nuovi potenziali danneggiati, nuovi candidati responsabili, nuovi rischi e possibili danni (quelli derivanti, non solo dall'uso illecito dei dati, ma anche, ad esempio, dalla loro inaffidabilità ed erroneità che può tradursi in scelte discriminatorie o lesive di altri diritti fondamentali della persona).

Tra i potenziali danneggiati, l'art. 100 regolamento EHDS annovera anche le *legal persons*, come, ad esempio, le strutture sanitarie persone giuridiche, che hanno messo a disposizione degli utenti i dati di cui sono titolari per gli usi secondari, nonché gli stessi utenti dei dati sanitari (sovente persone giuridiche), che possono subire danni a causa delle mancate autorizzazioni da parte delle autorità competenti o per la fornitura incompleta o erronea dei dati da parte dei titolari dei dati sanitari[36].

Quanto ai responsabili, è utile la lettura del considerando 101, laddove l'autorità di sanità digitale (ad es. per omesso controllo), l'organismo responsabile dell'accesso ai dati sanitari, il titolare dei dati sanitari o l'utente dei dati sanitari vengono espressamente designati quali possibili candidati a risarcire i danni subiti da una persona fisica o giuridica a causa di violazioni del regolamento.

E ciò, già in prima battuta, dà il senso della complicatezza – per il soggetto eventualmente leso – del contesto da affrontare per ottenere giudizialmente il ristoro dei dan-

[36] Cfr. Salanitro, *La tutela risarcitoria tra GDPR e EHDS: appunti per una ricerca*, in Morace Pinelli (a cura di), *Sanità digitale. Regolamento "EHDS" (UE 2025/327) sullo spazio europeo dei dati sanitari*, cit., 382.

ni subiti[37]. Contesto nel quale il numero dei soggetti coinvolti, nonché la prefigurabile transnazionalità di alcuni di essi, potrebbero verosimilmente incidere non solo sulla stessa giurisdizione territoriale competente, ma anche sui costi dei meccanismi di attività processuale (basti pensare a possibili notifiche transfrontaliere), sulle tecniche difensive adottabili (ad esempio domande di manleva, a scopo magari solo dilatorio), e sui tempi di emissione di una decisione[38].

La dinamica di condivisione e di riuso dei dati potrebbe farsi a tal punto articolata da sospingere verso l'oblio i singoli *players*, con il conseguente rischio del verificarsi di "danni anonimi".

In assenza di un candidato responsabile gravato da responsabilità *vicaria* (individuabile, in base a previsione normativa, quale legittimato passivo in caso di danni), e se si considera che il ricorso (in favore del danneggiato) alla regola della solidarietà, pur astrattamente invocabile sulla base della unicità dell'evento lesivo, potrebbe risultare in concreto difficilmente praticabile, in quanto presuppone già identificata la platea dei responsabili (salvo poi coglierne il rispettivo contributo in sede di regresso)[39], si lascia al

---

[37] Incisivamente, Corso, *Lo spazio europeo dei dati sanitari*, cit., 592, chiosa: "l'EHDS si tramuta così in un agone di agenti dai più svariati connotati, per i quali non è prevedibile il tipo di rapporto che li leghi e che li relazioni con la persona che, dalla loro condotta, abbia subito un danno".

[38] Un correttivo per tali criticità può essere costituito dalle azioni collettive come reazioni nel caso dei *data breaches,* nonché di altre condotte di illecito trattamento dei dati offensive di una pluralità di diritti omogenei. Si pensi all'art. 80 del GDPR, che abilita gli enti rappresentativi muniti dei caratteri richiesti dalla legge, di far valere in giudizio le istanze degli interessati, con o senza mandato. Si pensi, inoltre, alla normativa di derivazione europea sulle azioni rappresentative, che possono essere nazionali o transfrontaliere, a tutela degli interessi collettivi dei consumatori (Dir. UE/2020/1828), che espressamente rinvia al GDPR, posto che la qualifica di consumatore e quella di interessato tendono talora a coincidere. Nell'ordinamento italiano, i rimedi collettivi sono costituiti dall'azione rappresentativa prevista agli artt. 140-*ter* ss. cod. cons., attuativi la Direttiva europea, e dai procedimenti collettivi, di cui agli artt. 840-*bis* ss. c.p.c. Con specifico riguardo al regolamento GDPR, cfr. Corso, *op. cit*., 597 ss. In tema, di recente, il puntuale studio di M. Federico, *Protezione dei dati personali e tutela collettiva. Itinerari di comparazione fra Europa e Stati Uniti*, Torino, 2024.; ma già Bernes, *op. cit*., 678 ss. Parrebbe, in effetti, essere in crescita il numero e l'efficacia delle azioni collettive avviate in seguito alla riforma varata nel 2019 (entrata in vigore il 19 maggio 2021) – che ha modificato la precedente *class action* (poco usata) e l'ha resa uno strumento di tutela generale, ampliando la platea dei ricorrenti e l'ambito d'azione – e dopo che, nel 2023, con il recepimento della direttiva UE 2020/1828, sono state introdotte le azioni rappresentative. La tendenza positiva innescata dalle nuove regole sta concretizzandosi nella risoluzione in via transattiva di molti procedimenti laddove le imprese valutano il rischio di una sentenza negativa.

[39] Ferme restando, ovviamente, le previsioni dei commi 4 ("Qualora più titolari del trattamento o responsabili del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano, ai sensi dei paragrafi 2 e 3, responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato") e 5 (Qualora un titolare del trattamento o un responsabile del trattamento abbia pagato, conformemente al paragrafo 4, l'intero risarcimento del danno, tale titolare del trattamento

danneggiato la problematica individuazione a monte del responsabile o dei responsabili cui indirizzare l'azione risarcitoria, in un contesto nel quale non sarà agevole identificare, con elevato grado di affidabilità, lo svilupparsi delle differenti serie causali riferibili ai soggetti coinvolti.

Altra ipotesi da considerare è, poi, quella in cui lo stesso interessato agisca in modo da comprometterne la sicurezza dei dati, omettendo, ad esempio, di proteggere le credenziali personali e consentendo, in tal modo, l'accesso a soggetti non autorizzati; in casi simili, all'interessato/paziente potrebbe attribuirsi una quota di responsabilità collegata all'onere/dovere di controllo (periodico e regolare) della propria posizione e dei propri dati che comunque gli si affigge (cfr. considerando 12 e 13)[40].

Oltre ai già menzionati profili di eventuale concorrenza degli strumenti di tutela di fonte unionale e nazionale, rispetto ai quali occorre mettere a punto l'analisi dei presupposti e delle modalità di applicazione, penso, quali ulteriori temi di approfondimento, a quello relativo alla responsabilità civile delle *authorities* e degli organismi di vigilanza[41],

---

o responsabile del trattamento ha il diritto di reclamare dagli altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno conformemente alle condizioni di cui al paragrafo 2) dell'art. 82 GDPR, è evidente che le medesime, connotate come sono da una sfera applicativa limitata specialmente quanto ai soggetti evocati ed astretti al vincolo della solidarietà, non siano idonee a coprire tutte le possibili ipotesi di danni derivanti dalla violazione del regolamento EHDS.

Interessa notare, peraltro, che la regola della solidarietà è espressamente sancita lungo tutta la catena del valore in caso di responsabilità da difetto del prodotto, ai sensi dell'art. 12 della Direttiva 2024/2853, a mente del quale, in caso di pluralità di operatori economici responsabili, "Fatto salvo il diritto nazionale in materia di diritto di rivalsa, qualora due o più operatori economici siano responsabili dello stesso danno a norma della presente direttiva, gli Stati membri provvedono affinché essi possano essere ritenuti responsabili in solido", specificandosi che "il fabbricante che integri un software quale componente in un prodotto non ha diritto di rivalsa nei confronti del fabbricante di un componente software difettoso che causa danni se: a) il fabbricante del componente software difettoso era, al momento dell'immissione sul mercato del componente software, una microimpresa o una piccola impresa, (...); e b) il fabbricante che ha integrato il componente software difettoso nel prodotto ha concordato contrattualmente con il fabbricante del componente software difettoso di rinunciare a tale diritto".

[40] Cfr. Solinas, *Diritto alla salute del paziente e uso primario dei dati sanitari elettronici personali*, *EJPLT Special Issue* 2025, DOI: https://doi.org/10.57230/EJPLT25SIBCS, 11 ss. e part. 15, nel senso che "l'Unione europea non solo mira a «trasformare» i rapporti sociali ed economici in senso digitale, ma concepisce il destinatario dei servizi sempre più come un soggetto attivo nella soddisfazione del proprio bisogno. La persona è concepita quale tassello essenziale del complessivo servizio; essa è resa, laddove possibile, autonoma nella cura del proprio interesse e, dunque, del proprio diritto (...) Non fa eccezione il settore della cura della salute, in cui la persona è individuata e concepita dall'ordinamento come la prima figura che possa occuparsi del proprio benessere e della propria salute".

[41] Ad esempio, ai sensi dell'art. 19 regolamento EHDS, tra i compiti di *governance* relativa all'uso primario, ciascuna autorità di vigilanza digitale è tenuta a "garantire l'attuazione a livello nazionale del formato europeo di scambio delle cartelle cliniche elettroniche, in cooperazione con le autorità nazionali e i portatori di interessi" (lett. *g*), a "contribuire a livello dell'Unione allo sviluppo

riconducibile, secondo una ricostruzione già da tempo vagliata in dottrina e giurisprudenza, al modello della responsabilità da *status*, che potrebbe riportare in auge la discussione intorno alla figura degli obblighi/doveri di protezione[42]; a quello relativo alla *cybersecurity*, anch'esso oggetto di costante attenzione legislativa, a livello europeo e nazionale[43]; a quello

---

del formato europeo di scambio delle cartelle cliniche elettroniche, all'elaborazione di specifiche comuni, in conformità dell'articolo 36, per far fronte alle preoccupazioni in materia di qualità, interoperabilità, sicurezza, facilità d'uso, accessibilità, non discriminazione o diritti fondamentali e all'elaborazione delle specifiche della banca dati UE per la registrazione dei sistemi di cartelle cliniche elettroniche e delle applicazioni per il benessere di cui all'articolo 49" (lett. *h*), a "cooperare con le autorità di vigilanza del mercato, partecipare alle attività relative alla gestione dei rischi posti dai sistemi di cartelle cliniche elettroniche e degli incidenti gravi e vigilare sull'attuazione di misure correttive conformemente all'articolo 44" (lett. *k*).

[42] Si tratterebbe, per vero, nella specie, di obblighi aventi fonte legale nelle disposizioni del regolamento EHDS. Cfr. Mazzamuto, *Rimedi specifici e responsabilità*, 2° ed., Napoli, 2024, 771 ss.; Thiene, *Nuovi percorsi della responsabilità civile. Dalla condotta allo* status, Padova, 2006, *passim* e part. 168 e ss.

[43] Il panorama della *cybersecurity* si presenta come un contesto in rapida evoluzione, influenzato da dinamiche geopolitiche, innovazioni tecnologiche, sfide legislative e la crescente interconnessione delle infrastrutture digitali. Protezione dei dati e *cybersecurity* sono ormai inseparabili, in ragione della crescente dipendenza dai *software* e dalle infrastrutture digitali. Senza adeguate misure di sicurezza informatica, la conformità normativa non può essere pienamente realizzata. Il GDPR deve essere, pertanto, integrato con le normative sulla sicurezza informatica. La direttiva NIS2, recepita con il d. lgs. 4 settembre 2024, stabilisce obblighi specifici sulla sicurezza delle reti e dei sistemi informativi, coinvolgendo, oltre alle infrastrutture più critiche nei comparti dell'energia, della sanità e dei trasporti (soggetti essenziali), anche settori quali quelli alimentare, chimico, farmaceutico e telecomunicazioni (soggetti importanti). In data 20 novembre 2024 è entrato in vigore il Regolamento (UE) 2024/2847 del 23 ottobre 2024 *"relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828"* (regolamento sulla ciber-resilienza). L' ambito di applicazione del Regolamento (v. art. 2) riguarda, salvo specifiche esclusioni, i prodotti con elementi digitali messi a disposizione sul mercato la cui finalità prevista o il cui utilizzo ragionevolmente prevedibile include una connessione dati logica o fisica diretta o indiretta a un dispositivo o a una rete. Quanto al rapporto con il regolamento EHDS, e con particolare riguardo alle CCE, al considerando (112) è specificato che "Il presente regolamento integra i requisiti essenziali di cibersicurezza stabiliti dal regolamento (UE) 2024/2847. I sistemi di cartelle cliniche elettroniche che sono prodotti con elementi digitali ai sensi del regolamento (UE) 2024/2847 dovrebbero pertanto essere conformi ai requisiti essenziali di cibersicurezza stabiliti in tale regolamento. I fabbricanti dei sistemi di cartelle cliniche elettroniche dovrebbero dimostrare la conformità dei loro sistemi secondo quanto disposto dal presente regolamento. Per facilitare tale conformità, i fabbricanti dovrebbero essere autorizzati a redigere un'unica documentazione tecnica contenente gli elementi richiesti da entrambi gli atti giuridici. Dovrebbe essere possibile dimostrare la conformità dei sistemi di cartelle cliniche elettroniche ai requisiti essenziali di cibersicurezza stabiliti dal regolamento (UE) 2024/2847 mediante il quadro di valutazione previsto dal presente regolamento. Tuttavia, le parti della procedura di valutazione della conformità a norma del presente regolamento relative all'uso di ambienti di prova non dovrebbero essere applicate, in quanto gli ambienti di prova non consentono una valutazione della conformità ai requisiti essenziali di cibersicurezza. Poiché il regolamento (UE)

della tutela della proprietà intellettuale e dei brevetti industriali, nonché al tema del diritto *sui generis* sulle banche dati[44] ed alle biobanche[45].

Nel raffronto con l'art. 82 GDPR, non può, inoltre, ignorarsi il dato testuale dell'art. 100, che fa espresso rinvio al diritto dell'Unione (del quale il GDPR, deputato alla disciplina di una specifica materia, è solo una parte) e nazionale. Mi sembra, come già anticipato, che, specie avuto riguardo alla maggiore complessità dello scenario dello spazio europeo dei dati sanitari rispetto al mero trattamento dei dati investito dal GDPR, la configurazione dei profili di responsabilità per i danni debba riferirsi ad una pluralità di modelli rimediali, che potranno essere invocati anche in alternativa tra loro[46] [penso alla responsabilità da prodotto difettoso[47], ma anche alle norme di diritto domestico, ascrivibili, a seconda dei casi, tanto al versante extracontrattuale (in base ai diversi criteri di imputazione racchiusi nella disciplina aquiliana[48]) quanto al versante della responsabilità da inadempimento *ex* art. 1218 c.c.].

2024/2847 non contempla direttamente il servizio a livello di software (*Software as a Service* - SaaS) in quanto tale, i sistemi di cartelle cliniche elettroniche offerti attraverso il modello di concessione e fornitura di licenze SaaS non rientrano nell'ambito di applicazione di tale regolamento. Analogamente, i sistemi di cartelle cliniche elettroniche sviluppati e utilizzati internamente non rientrano nell'ambito di applicazione di tale regolamento, in quanto non sono immessi sul mercato".

[44] Cfr. Ricci, *Introduzione al Regolamento europeo sull'accesso equo ai dati e sul loro utilizzo*, in *NLCC*, 2024, 799 part. 810 ss.

[45] Ai sensi dell'art. 51 comma 4, gli Stati membri possono introdurre misure più rigorose e garanzie supplementari a livello nazionale intese a tutelare la sensibilità e il valore dei dati genetici, epigenomici e genomici umani; degli altri dati molecolari umani, quali quelli provenienti dalla proteomica, dalla trascrittomica, dalla metabolomica, dalla lipidomica e altri dati omici; dei dati provenienti dalle applicazioni per il benessere; dei dati sanitari provenienti da biobanche e banche dati associate. In materia di biobanche, cfr. Corti, *La sorte (incerta) della ricerca sui campioni biologici umani all'indomani della decisione Shardna*, in *NGCC*, 2022, I, 594, in nota a Cass. 7 ottobre 2021 n. 27325; Perlingieri, *Transizione digitale nella sanità ed ecosistema dei dati sanitari: profili ricostruttivi del fenomeno circolatorio e implicazioni sui dati genetici*, in *Tecnologie e diritto*, 2024, 485 ss., e ora in EAD., *Innovazione tecnologica e diritto civile. Saggi*, Napoli, 2025, 159 ss.; Bernes, *La protezione dei dati personali nell'attività di ricerca scientifica*, in *NLCC*, 2020, 175 ss.

[46] La questione del concorso dei rimedi è assai dibattuta e particolarmente spinosa. Per una messa a punto dei rapporti tra la tutela aquiliana e la responsabilità da prodotto difettoso, cfr. Cass. 28 marzo 2025 n. 8224, in *Foro it.*, 2025, I, 1806, con nota di Bitetto, *Responsabilità per vaccino difettoso: no al* patchwork *di regole!*; in *Riv. it. med. leg.*, 2025, 365 ss., con nota di Musto, *Risarcimento del danno da vaccino: la via del "cumulo senza commistione" dei diversi regimi di responsabilità*.

[47] Recentemente riformata dalla Direttiva 2024/2853/UE (che sostituisce la precedente Direttiva 85/374/CEE per i prodotti immessi in commercio nell'Unione a partire dal 9 dicembre 2026), sulla quale, Bellisario, voce *Responsabilità per i prodotti difettosi*, in *Enc. dir.*, *I tematici*, VII, *Responsabilità civile*, diretto da Scognamiglio, Milano, 2024, 1240 e part. 1279; Afferni, *La nuova direttiva sulla responsabilità per danno da prodotti difettosi: una analisi economica*, in *Resp. civ. e prev.*, 2025, 351 ss.; Fusaro, *Intelligenza artificiale e responsabilità da prodotti difettosi: la direttiva 2024/2853*, in *NGCC*, 2025, II, 488 ss.

[48] La regola di imputazione di cui all'art. 2050 c.c. potrebbe, ad esempio, essere invocata nei casi di danni derivanti dalla interazione con sistemi di AI ad alto rischio. Il tema richiede eviden-

Alla luce di quanto sin qui osservato, pare, dunque, che, nonostante la vocazione tendenzialmente unificatrice dell'art. 100, l'operatività dello spazio europeo dei dati sanitari apra, in punto di danni e profili di responsabilità, una pluralità di scenari che daranno luogo all'incardinarsi di diversi filoni di indagine.

Quel che si ricava è che, mentre l'art. 82 GDPR è dotato di una sua forza autoevocativa sul piano rimediale, l'art. 100 regolamento EHDS non fonda un modello di tutela autonomo, bensì rappresenta una norma di *raccordo* tra la disciplina dello spazio europeo dei dati e i vari strumenti di tutela previsti in altre norme, europee e nazionali.

Non si tratta, tuttavia, mi pare, di un mero rinvio pleonastico. Nella formulazione dell'art. 100, l'accento non è sul rimedio (dove la tecnica normativa utilizzata è quella del rinvio all'esistente); ciò che risalta è piuttosto il monito all'interprete di tener conto del "nuovo universo" *creato* dal regolamento, dove è tratteggiato il copione cui gli attori dello spazio europeo dei dati devono attenersi.

---

temente maggiore approfondimento rispetto a quanto possibile in questa sede. Basti qui rinviare a Scognamiglio, *Responsabilità civile ed intelligenza artificiale: quali soluzioni per quali problemi?*, in *Resp. civ. e prev.*, 2023, 1073 ss., il quale invita a privilegiare il criterio di imputazione dell'art. 2050 c.c., specificando come "se è certamente vero che anche quello contenuto nell'art. 2050 è ritenuto prevalentemente un criterio di imputazione di responsabilità oggettiva, è anche vero che questo esito applicativo risulta essere assai più il frutto del modo, particolarmente rigoroso, in cui viene inteso, nella elaborazione giurisprudenziale della materia, l'onere della prova liberatoria a carico dell'esercente l'attività pericolosa, che non la conseguenza di una scelta del legislatore, immediatamente desumibile dall'enunciato della disposizione: ed infatti il riferimento alla prova di avere adottato tutte le misure idonee ad evitare il danno sembra effettivamente evocare più un modello di responsabilità dove la colpa del candidato responsabile comunque rilevi, sia pure con un onere della prova invertito rispetto a quello della norma generale dell'art. 2043 c.c.". La differenza tra l'art. 2050 c. c e 82 GDPR (il primo più *severo* del secondo nel fissare l'ascrizione della responsabilità) è rimarcata da Barcellona, *op, cit*., 108, che sottolinea come l'art. 82 GDPR, nel consentire al titolare del trattamento di tener conto, nell'adozione delle misure di prevenzione, della natura, dell'ambito di applicazione, del contesto e delle finalità, nonché dei rischi, "lascia intendere che misure più accentuate (di quelle adottate) in grado di giungere a scongiurare del tutto il verificarsi del danno lamentato dall'attore possano non essere dovute per il peso di uno (o più) di tali elementi di giudizio".

La duttilità della regola di cui all'art. 20250 c.c., laddove consente di configurare una responsabilità per i danni cagionati da un prodotto "conforme", ossia rispettoso delle norme tecniche armonizzate che ne definiscono le caratteristiche, rende, peraltro, il rimedio aquiliano generale possibile *competitor* della disciplina della responsabilità da prodotto difettoso, in quanto, sulla scorta della (pur non sempre agevole) distinzione tra prodotto difettoso e prodotto pericoloso, consente di apprestare una tutela più incisiva del consumatore-danneggiato rispetto a quella recata dagli artt. 117-124 cod. cons. In tema, cfr. Cioni, *L'influenza indiretta del diritto europeo: il caso dei danni cagionati dai prodotti pericolosi. Spunti per una riscoperta dell'articolo 2050 c.c.*, in *Riv. dir. civ.*, 2023, 956; Montinaro, *Responsabilità da prodotto difettoso e tecnologie digitali tra* soft law *e* hard law, in *Pers. merc*., 2020, 350 ss.

Se le sollecitazioni e le criticità con le quali gli interpreti dovranno confrontarsi sono parecchie e di ampio spettro, dovendo avviarmi alla conclusione, vorrei congedarmi con una notazione positiva.

Con sentenza 26 ottobre 2023 C-307/22, la CGUE è stata investita di questione pregiudiziale relativa ad una causa tedesca dove una paziente, che aveva chiesto alla sua dentista copia della propria cartella clinica al fine di farne valere la responsabilità per *malpractice*, veniva a sua volta richiesta dalla professionista di farsi carico delle spese relative alla fornitura della copia, come previsto dal diritto tedesco. La Corte federale tedesca, rilevata la dipendenza della soluzione della controversia dalla interpretazione delle disposizioni del GDPR, si rivolgeva alla CGUE. La corte europea ha, così, avuto modo di ribadire che il GDPR sancisce il diritto del paziente di avere copia della cartella clinica senza spese, anche al fine di intentare una causa civile nei confronti del professionista. Sicché le norme nazionali non possono porre a carico del paziente spese per ottenere la prima copia della propria cartella sanitaria[49].

A differenza del GDPR, dove è previsto che il titolare del trattamento ha un mese di tempo per rispondere a una richiesta dell'interessato, il regolamento EHDS garantisce ai pazienti, o ai loro rappresentanti, il diritto di accedere direttamente a un insieme minimo di dati, indipendentemente dal luogo in cui vengono elaborati, dal tipo di fornitore di assistenza sanitaria, dalle fonti dei dati o dal paese di affiliazione (art. 3).

Ed ecco, dunque, la buona notizia. Se il Regolamento EHDS fosse già stato applicabile, la paziente o il suo avvocato avrebbero potuto selezionare personalmente i documenti utili a supportare la richiesta di risarcimento per negligenza medica e ottenerne una copia senza dover sostenere alcun costo (cfr. art. 3 e 4 regolamento EHDS).

Abstract

L'art. 100 del regolamento EHDS è dedicato alla responsabilità per danni. Nonostante la vocazione unificatrice, l'art. 100 non istituisce un modello di tutela autonomo, bensì pone una norma di raccordo tra la disciplina europea e gli strumenti di tutela previsti in altre norme, europee e nazionali. L'enfasi non è sul rimedio (dove opera il rinvio all'esistente); risalta piuttosto il monito all'interprete di tener conto del "nuovo universo" creato dal regolamento, dove è tratteggiato il copione cui gli attori dello spazio europeo dei dati devono attenersi.

Article 100 EHDS Regulation is devoted to liability for damages. While aiming to unify the legislation, Article 100 does not establish an autonomous model; rather, it represents a connecting rule that links European legislation to the various protection instruments provided

[49] Cfr. Di Federico, F*rom dusk till dawn. the case of F.T. v D.W. and the right to access electronic medical records in light of the future European Health Data Space regulation*, in *European Papers*, Vol. 9, 2024, No 2, 463-477.

by other European and national legislation. The emphasis is not on the remedy (with reference to existing legislation); rather, what stands out is the warning to take into account the "new universe" created by the regulation, which outlines the script that the actors in the European data space must play.