Intervista al Dott. Stefano Corso, la Prof.ssa Simona Cacace ed il Prof. Massimo Foglia. La sanità digitale e il trattamento dei dati dei pazienti fra teoria e prassi applicative

27 GIUGNO 2025 Redazione DIMT

In occasione dell'incontro *"La sanità digitale e il trattamento dei dati dei pazienti fra teoria e prassi applicative"*, tenutosi lo scorso 16 maggio, abbiamo raccolto le riflessioni di tre relatori: Stefano Corso, Simona Cacace e Massimo Foglia. Le loro risposte offrono, da prospettive complementari, un'analisi approfondita su alcuni dei temi centrali legati alla protezione dei dati sanitari, al Fascicolo Sanitario Elettronico e al nuovo

Regolamento UE 2025/327 sullo spazio europeo dei dati sanitari (EHDS).

Il Dott. **Stefano Corso** è assegnista di ricerca in Diritto privato, Dottore di ricerca in Diritto internazionale e Diritto privato e del lavoro dell'Università di Padova, nonché Cultore in Diritto privato, nel Dipartimento di Giurisprudenza dell'Università di Ferrara. È membro del Comitato editoriale della *Nuova giurisprudenza civile commentata*, della Redazione di *Responsabilità medica. Diritto e pratica clinica*, nonché del Comitato di ricerca del Centro interdisciplinare di studi sul diritto sanitario (CeSDirSan).

Simona Cacace è Professoressa aggregata di Biodiritto presso il Dipartimento di Giurisprudenza dell'Università degli Studi di Brescia, abilitata al ruolo di professore di seconda fascia. È membro del Collegio docenti del Dottorato *Intelligenza Artificiale in Medicina e Innovazione nella Ricerca clinica e metodologica* e del Consiglio scientifico del Master di II livello *Intelligenza artificiale, mente e impresa* (UniBS). Insegna *Emerging Technologies Law* nel dottorato nazionale in Intelligenza Artificiale (coordinamento Sapienza). È Presidente del Comitato Etico per la Ricerca di Ateneo, coordinatrice

dell'Osservatorio di Biodiritto di Brescia e co-fondatrice del TRAIL – Trustworthy AI Lab.

Massimo Foglia è professore associato di Diritto privato presso il Dipartimento di Giurisprudenza dell'Università degli studi di Bergamo, dove insegna Diritto privato e Scrittura giuridica. Ha conseguito il titolo di Dottore di ricerca in Diritto privato nella dimensione europea nell'Università di Padova. È avvocato iscritto all'Ordine degli Avvocati di Bergamo (elenco speciale dei Professori e Ricercatori universitari a tempo pieno). Ha svolto studi di perfezionamento presso università e istituti di ricerca all'estero. È relatore in convegni e seminari di studio in Italia e all'estero. È autore di pubblicazioni dedicate principalmente alle materie delle obbligazioni, dei contratti, della responsabilità civile e dei diritti della persona, anche nel contesto delle nuove tecnologie.

Dott. Corso, quali sono le principali sfide che il GDPR pone nel trattamento dei dati sanitari, in particolare nell'ambito del Fascicolo Sanitario Elettronico?

Il GDPR si connota per la sua duplice finalità di tutelare la persona fisica rispetto al trattamento di dati personali e di assicurare la circolazione stessa dei dati. Questo aspetto si riscontra anche con riferimento al trattamento dei dati sanitari, che è certo in grado di mettere a rischio le libertà e i diritti fondamentali della persona, ma al contempo è funzionale ed essenziale per scopi di carattere pubblico o collettivo. Il trattamento di particolari categorie di dati personali – i c.d. dati sensibili, tra cui rientrano i dati relativi alla salute – è in linea generale vietato dall'art. 9, par. 1, GDPR. Ma le deroghe al divieto, sancite dal par. 2 dell'art. 9, consentono che dati relativi alla salute siano trattati a prescindere dal consenso dell'interessato, purché ne ricorrano i presupposti. È sulla base di ciò che l'alimentazione del Fascicolo Sanitario Elettronico si è resa automatica, con il d.l. n. 34 del 2020.

Il FSE è strumento centrale della digitalizzazione della sanità e la sua stessa regolamentazione rappresenta una delle più grandi sfide di oggi. Disciplinato principalmente dal d.l. n. 179/2012, all'art. 12, e dal d.m. 7 settembre 2023, deve coordinarsi con le varie altre realtà della sanità digitale, una su tutte l'Ecosistema Dati Sanitari, regolato dal d.m. 31 dicembre 2024.

L'impiego di tali strumenti è orientato non solo alla cura, ma anche alla ricerca e al governo della sanità. È necessario quindi coniugare i diversi interessi sottesi, da un punto di vista tanto teorico quanto pratico e operativo, attraverso un'opera attenta di bilanciamento.

Quali misure di sicurezza ritiene indispensabili per garantire la protezione dei dati personali nel contesto della sanità digitale a Suo avviso Dott. Corso?

L'art 2 septies del Codice della privacy prevede che il trattamento dei dati relativi alla salute, genetici e biometrici avvenga nel rispetto non solo delle disposizioni del GDPR e del d.lgs. n. 196/2003, ma anche delle misure di garanzia adottate dal Garante per la protezione dei dati personali. Il provvedimento recante le misure di garanzia, non ancora emanato, individuerà le misure di sicurezza per garantire la protezione dei dati e queste varranno anche per il contesto sanitario. Alcune misure di sicurezza sono già menzionate dalla disposizione, ad esempio le tecniche di cifratura e pseudonimizzazione.

La sicurezza con riferimento alla protezione dei dati sanitari dipende necessariamente dal contesto dell'ambiente digitale, in termini di struttura dell'architettura informatica. L'attuazione dei principi e delle regole giuridiche avviene quindi attraverso la tecnologia stessa. Garantire la sicurezza è in ogni caso un obbligo per il titolare del trattamento. Con riguardo all'ambito sanitario, sarà soprattutto un obbligo della pubblica amministrazione.

Resta cruciale il ruolo di controllo, consultazione e promozione svolto dal Garante per la protezione dei dati personali, cui si affianca oggi quello di AGENAS, in qualità di Agenzia nazionale per la sanità digitale. A questi si aggiungeranno le funzioni dell'Autorità di sanità digitale e dell'Organismo responsabile dell'accesso – rispettivamente per l'uso primario e l'uso secondario di dati sanitari elettronici – nel quadro normativo tracciato dal Regolamento 2025/327, sullo spazio europeo dei dati sanitari (c.d. EHDS).

Prof.ssa Cacace, quali innovazioni introduce il Regolamento UE 2025/327 riguardo allo spazio europeo dei dati sanitari?

L'art. 3, comma terzo, del Regolamento UE 2025/327 prevede la possibilità, per gli Stati membri, di limitare il diritto delle persone fisiche all'accesso ai dati sanitari elettronici personali che le riguardano e di limitare altresì il diritto delle medesime di scaricarne gratuitamente una copia elettronica. L'uso primario dei dati sanitari – trattati ai fini della prestazione di assistenza sanitaria – potrebbe essere interessato da tale limitazione, predisposta dal legislatore nazionale, allorché necessaria per tutelare la persona fisica, «tenendo conto della sicurezza del paziente e sulla base di considerazioni etiche». L'esigenza di un'informazione comunicata all'interessato direttamente dal medico, con un'adeguata spiegazione e in occasione di un incontro e di un colloquio orale, giustificherebbe il temporaneo differimento della possibilità di accedere ai dati, così evitando che notizie di particolare impatto per la salute del paziente vengano semplicemente veicolate per il tramite della tecnologia e in un contesto avulso dalla relazione di cura e di fiducia. In questo caso, dunque, all'esito di un bilanciamento fra il diritto di conoscere certe informazioni e l'esigenza che tale consapevolezza si formi con modalità deontologicamente conformi e nel rispetto del benessere della persona malata, il momento della visibilità del dato per l'utente finisce per non corrispondere, sotto il profilo strettamente temporale, con il momento del suo inserimento e registrazione nel sistema di cartelle cliniche elettroniche.

La limitazione di cui al comma terzo dell'art. 3 del Regolamento non deve certo ritenersi, dunque, quale reviviscenza di una modalità paternalistica d'intendere il rapporto fra medico e paziente, sulla scorta della quale a quest'ultimo potrebbe tacersi la verità sulle sue condizioni di salute allorché sia giudicato incapace di accettarla, sostenerla o persino comprenderla, dal punto di vista psicologico, emotivo, intellettuale o culturale. Tutt'al contrario, la restrizione del diritto di accesso così disciplinata risponde – e in questo senso soltanto deve essere letta – all'esigenza di consentire l'adeguato svolgimento della relazione di cura e di fiducia intercorrente fra medico e paziente, descritta e disciplinata dalla legge n. 219/2017.

Il paziente, Prof.ssa Cacace, può a sua volta scegliere di oscurare i dati che lo riguardano?

L'art. 8 del Regolamento prevede il diritto di oscurare la totalità o una parte dei propri dati sanitari elettronici personali, che il titolare può esercitare una volta informato circa le possibili conseguenze negative di tale scelta sulla qualità del servizio erogato e sul buon esito della prestazione sanitaria, nonché, in definitiva, sulla sua stessa sicurezza e integrità psico-fisica. Soltanto una volta acquisita una consapevolezza in questi termini il paziente è in grado di opporre un diniego giuridicamente valido alla visibilità dei propri dati, assumendosi la responsabilità del fatto che il medico non potrà tenerne conto nelle sue valutazioni e nel suo operato.

In ordine a questa possibilità di condivisione selettiva, al 'considerando' diciassette si fa riferimento a questioni relative, per esempio, alla salute mentale o sessuale, a procedure sensibili quali l'aborto o a dati riguardanti l'assunzione di medicinali specifici, suscettibili di rivelare altre e ulteriori informazioni sensibili.

Benché una decisione in questo senso non sia in alcun modo visibile al personale sanitario, l'art. 11 introduce una deroga

alla facoltà di tenere celati i propri dati, ai quali il medico potrebbe comunque accedere «se necessario per la salvaguardia degli interessi vitali dell'interessato», per non mettere a repentaglio la vita del suo assistito in situazioni di emergenza, lasciando di tale accesso traccia chiara e comprensibile per il paziente.

Dalla previsione di una deroga in questi termini scaturiscono, tuttavia, diverse perplessità.

Infatti, a fronte di un bilanciamento fra beni giuridici riconducibili unicamente a un medesimo titolare, non si vede come la riservatezza pretesa dal paziente possa soccombere in nome della migliore cura possibile, in un ordinamento che riconosce il principio di volontaria sottoposizione ai trattamenti sanitari, a prescindere dal danno che all'integrità psicofisica della persona derivi dal rispetto della sua autodeterminazione, secondo quanto chiaramente enunciato dall'art. 32 Cost. e dall'art. 1 della legge n. 219/2017.D'altro canto, poiché non v'è modo di sapere prima se la persona abbia deciso di oscurare alcunché, il rischio è che, nel dubbio, il personale sanitario opti sistematicamente per un accesso indiscriminato, in nome di un interesse vitale o di un preteso stato di necessità. Una violazione in tal senso si pone in palese contraddizione con la pacifica vincolatività, ai sensi degli artt. 4 e 5 della legge n. 219/2017, delle indicazioni contenute nelle disposizioni anticipate di trattamento o in una pianificazione condivisa delle cure, anche e proprio al ricorrere di condizioni d'urgenza.

Prof. Foglia, come si è evoluta la responsabilità civile nell'ambito del trattamento illecito dei dati sanitari secondo la giurisprudenza più recente?

La giurisprudenza più recente ha rafforzato l'idea che la lesione della riservatezza dei dati sanitari costituisca una violazione autonoma dei diritti della persona, capace di generare responsabilità civile anche in assenza di un danno patrimoniale quantificabile. I giudici riconoscono sempre più spesso la tutela

risarcitoria del danno non patrimoniale, qualificandolo come compromissione della sfera più intima dell'individuo, con particolare attenzione alla dignità, alla vita relazionale e alla libertà di autodeterminazione. Non è quindi più necessario dimostrare un pregiudizio materiale o economico: è sufficiente che il trattamento avvenga in modo illecito – ad esempio per carenza di base giuridica, eccessiva diffusione, o violazione dei principi di minimizzazione e proporzionalità – per far scattare il diritto al risarcimento. Il danno alla privacy è valutato anche in termini di stress, disorientamento e disagio psico-emotivo.

A Suo avviso, Prof. Foglia, quali criteri adottano i tribunali per valutare la responsabilità civile in questi casi e quali implicazioni possono avere per gli operatori sanitari?

I tribunali si orientano sulla base di criteri ispirati al Regolamento generale sulla protezione dei dati (GDPR) e ai principi generali del diritto civile. In particolare, vengono considerati: la natura e la sensibilità dei dati trattati (es. informazioni sulla salute, patologie, trattamenti); la legittimità della base giuridica del trattamento; la chiarezza e adeguatezza dell'informativa resa agli interessati; il rispetto dei principi di correttezza, trasparenza e minimizzazione; l'impatto del trattamento sulla vita privata e sulle relazioni personali del soggetto coinvolto. Per gli operatori sanitari ciò comporta un'importante responsabilità, anche quando non siano direttamente responsabili del trattamento: devono assicurarsi che i dati siano trattati nel rispetto delle regole, che siano protetti con adeguate misure di sicurezza e che ogni attività sia conforme alla finalità terapeutica. La non osservanza di tali doveri può esporre non solo le strutture sanitarie, ma anche i singoli professionisti, a conseguenze risarcitorie e disciplinari. L'adozione di procedure corrette e l'aggiornamento costante su normativa e buone pratiche rappresentano quindi oggi una componente essenziale della diligenza professionale.

a cura di Valeria Montani

Condividi

Redazione DIMT

Articoli correlati

LinkedIn, dal 3 novembre i dati pubblici degli utenti usati per l'IA: il Garante privacy invita a esercitare il diritto di opposizione

Il Garante per la protezione dei dati personali richiama l'attenzione degli utenti LinkedIn su una…

Pump&dump, Consob avverte i risparmiatori: "Attenzione alle truffe via social e WhatsApp"

La Consob torna a puntare i riflettori sulle truffe finanziarie che circolano sui social network…

"Il diritto ed i robot": al Young International Forum un confronto sulle nuove sfide dell'intelligenza artificiale per il diritto

Nell'ambito dello Young International Forum (YIF), evento aperto dal 21 al 23 ottobre 2025 a…

« Quotazione dei fondi: la Consob avvia una consultazione per semplificare l'accesso al mercato italiano

La Commissione Europea rilancia l'innovazione IA a Roma con l'evento "La Rivoluzione dell'IA: dalle parole ai fatti" »