UNIVERSITA' DEGLI STUDI DI ROMA TOR VERGATA

***European Digital Law of the Person, of the Contract and of the Technological Marketplace* - EUDILA**
Cattedra Jean Monnet del Progetto ERASMUS +

La tutela dei dati sanitari nell'era digitale:
Accesso, interoperabilità e riservatezza tra GDPR ed EHDS

Sara Cecchetti

Anno accademico 2024/2025

1. Introduzione

- Contesto e centralità dei dati sanitari nel digitale
- Il dilemma tra accessibilità e privacy
- Obiettivi della tesina

2. Dati sanitari: definizione e rischi

- Dati personali sensibili
- Tipologie di dati sanitari e loro implicazioni
- Rischi di un uso improprio

3. Verso l'accessibilità: valorizzazione pubblica dei dati sanitari

- Cartelle cliniche elettroniche e Fascicolo Sanitario Elettronico (FSE)
- Big Data Sanitari e data altruism
- L'European Health Data Space: il modello europeo di interoperabilità (EHDS)

4.Il GDPR e strumenti per la tutela dell'individuo

- Il Regolamento Generale sulla Protezione dei Dati (GDPR)
- Anonimizzazione, pseudonimizzazione e consenso granulare
- Prevenzione delle discriminazioni e tutela del paziente: La legge 193 sull'oblio oncologico
- Ruolo del Garante della Privacy

5. Conclusioni

- Sintesi dei rischi e delle opportunità
- Verso un equilibrio tra innovazione e diritti
- Riflessioni finali sul valore del dato sanitari

1. Introduzione

In un'epoca in cui ogni aspetto della nostra vita quotidiana è progressivamente digitalizzato, anche la salute, l'ambito più intimo e personale dell'individuo, è diventata oggetto di raccolta, trattamento e analisi dati. Esami clinici, referti, prescrizioni, accessi al pronto soccorso e perfino i parametri fisiologici rilevati tramite smartwatch e app di benessere generano ogni giorno una mole crescente di informazioni. Se correttamente gestiti, questi dati possono offrire benefici concreti al singolo paziente e contribuire al miglioramento dell'intero sistema sanitario.

Tuttavia, questa centralità del dato sanitario apre scenari complessi che vanno ben oltre la semplice efficienza tecnologica. Il corpo umano, attraverso le sue fragilità e vulnerabilità, si traduce in informazione sensibile: preziosa, ma anche estremamente delicata. Non si tratta più soltanto di curare un paziente, ma di stabilire chi può accedere a questi dati, con quali garanzie e per quali finalità. Il rischio è che la persona venga ridotta a "dato", perdendo così parte della propria dignità e riservatezza.

Negli ultimi anni, le politiche europee e nazionali hanno spinto verso una sempre maggiore digitalizzazione del settore sanitario, riconoscendone il potenziale nel migliorare la qualità dell'assistenza, semplificare l'accesso alle cure e ottimizzare la gestione delle risorse pubbliche. L'introduzione della cartella clinica elettronica, l'interoperabilità tra sistemi regionali, lo sviluppo dell'European Health Data Space (EHDS) e il potenziamento delle infrastrutture digitali sono esempi concreti di questa trasformazione. Tali strumenti, se ben regolati, offrono opportunità rilevanti per la medicina personalizzata, la prevenzione e la ricerca scientifica.

A fronte di questi vantaggi, emergono però rischi significativi per la protezione dei diritti fondamentali della persona, a partire dal diritto alla privacy. Il progresso tecnologico, se non accompagnato da regole chiare e strumenti di controllo efficaci, può diventare veicolo di sorveglianza, esclusione o discriminazione. La questione,

quindi, non è più soltanto tecnica, ma profondamente giuridica ed etica: come garantire che l'innovazione non comprometta la centralità della persona?

Il Regolamento Generale sulla Protezione dei Dati (GDPR) attribuisce ai dati sanitari lo status di "categorie particolari di dati personali", prevedendo condizioni rigorose per il loro trattamento. È consentito raccoglierli solo in presenza di una base giuridica solida e per finalità determinate, come la cura del paziente o la ricerca scientifica, nel rispetto dei principi di necessità e proporzionalità.

Un ruolo sempre più strategico è affidato anche al progetto europeo dell'European Health Data Space (EHDS), pensato per promuovere l'accesso, l'interoperabilità e l'uso dei dati sanitari su scala europea. L'obiettivo è ambizioso: costruire un'infrastruttura digitale comune che permetta a cittadini, operatori sanitari e ricercatori di accedere in modo sicuro e regolato a informazioni sanitarie rilevanti, favorendo un approccio coordinato alla salute digitale.

Perché ciò avvenga senza sacrificare i diritti individuali, è necessaria una governance attenta e bilanciata. Le autorità di controllo, come il Garante per la protezione dei dati personali, giocano un ruolo essenziale nel garantire che l'innovazione non prevalga sulla tutela dei diritti, e che l'individuo mantenga sempre il controllo consapevole sui propri dati.

Questa tesina si propone di esplorare come la gestione dei dati sanitari, in un contesto sempre più digitale, possa essere compatibile con il rispetto dei diritti fondamentali. Partendo dal quadro normativo vigente, il lavoro analizzerà sia le opportunità offerte da una sanità più connessa e intelligente, sia le criticità legate alla privacy, alla sicurezza e all'etica dell'uso dei dati personali.

2. Dati sanitari: definizione e rischi

Nel contesto giuridico europeo, il dato sanitario rientra a pieno titolo nella categoria dei dati personali ai sensi dell'articolo 4 del Regolamento 2016/679 (GDPR), che definisce come dato personale "qualsiasi informazione riguardante una persona fisica identificata o identificabile". I dati che descrivono lo stato di salute fisico o mentale di un individuo, comprese diagnosi, trattamenti, informazioni genetiche o biometriche, sono pertanto dati personali, in quanto riferiti a una persona identificata o identificabile.

Ma la rilevanza del dato sanitario non si esaurisce qui. Esso appartiene alla sottocategoria dei dati particolari (art. 9 GDPR), anche detti "dati sensibili", che godono di una tutela rafforzata proprio a causa del loro contenuto profondamente intimo e del potenziale rischio per i diritti e le libertà fondamentali dell'interessato in caso di trattamento improprio. Il GDPR vieta in linea generale il trattamento di questi dati, salvo che ricorrano specifiche condizioni di liceità.

Possiamo distinguere i dati sanitari in dati diretti e indiretti; i primi comprendono tutte le informazioni esplicitamente legate alla salute di un individuo, come diagnosi, terapie, esiti clinici, referti, esami strumentali, cartelle cliniche digitali e certificati medici. I secondi, invece, sono dati che, pur non essendo prodotti in ambito strettamente sanitario, possono rivelare informazioni sensibili sullo stato di salute, come i dati biometrici, genetici, quelli provenienti da app per il fitness o l'analisi di comportamenti digitali.

L'elevato valore informativo dei dati sanitari rende questi ultimi particolarmente vulnerabili a usi impropri, che possono assumere forme diverse e generare conseguenze gravi sia per l'individuo sia per l'intera collettività. Il rischio più immediato riguarda le violazioni della riservatezza: accessi non autorizzati, fughe di dati o attacchi informatici possono esporre informazioni sensibili, mettendo a rischio la privacy, la reputazione e la dignità delle persone coinvolte.

In ambito sanitario, le violazioni non sono soltanto una questione di sicurezza informatica, ma possono tradursi in discriminazioni concrete, ad esempio in ambito lavorativo, assicurativo o creditizio. L'accesso, anche parziale, a dati clinici può essere utilizzato per profilare gli individui, escluderli da opportunità o trattarli in modo sfavorevole. Particolarmente critico è l'uso dei dati in settori dove le decisioni sono sempre più affidate ad algoritmi: in assenza di trasparenza e controllo, l'elaborazione automatica di informazioni sanitarie può rafforzare pregiudizi esistenti e determinare scelte poco chiare o ingiuste.

Un altro rischio rilevante riguarda la strumentalizzazione dei dati per finalità estranee a quelle dichiarate, come la loro vendita a terzi per attività di marketing sanitario, profilazione commerciale o addirittura sorveglianza. Anche quando il trattamento avviene all'interno di contesti legittimi, come la ricerca scientifica o la governance pubblica, l'assenza di un chiaro consenso informato o di adeguati meccanismi di controllo può generare una perdita di fiducia da parte dei cittadini, compromettendo l'efficacia di iniziative basate sulla condivisione dei dati.

Infine, l'uso improprio può derivare anche da carenze organizzative e mancanza di formazione, sia nel settore pubblico che in quello privato. Personale non adeguatamente sensibilizzato o protocolli deboli possono tradursi in errori, esposizione accidentale di dati, o uso inappropriato di strumenti digitali. Questo dimostra come la protezione dei dati sanitari non possa limitarsi a soluzioni tecnologiche, ma debba essere accompagnata da una solida cultura della responsabilità e della consapevolezza.

3. Verso l'accessibilità: valorizzazione pubblica dei dati sanitari

Affinché i dati sanitari possano assumere un valore concreto per la collettività, è imprescindibile che essi siano resi accessibili, strutturati e interoperabili. Questo processo passa inevitabilmente dalla loro digitalizzazione, intesa non solo come semplice trasposizione dei dati in formato elettronico, ma anche come condizione abilitante per la loro condivisione, analisi e utilizzo a fini clinici, organizzativi e di ricerca.

Al momento le cartelle cliniche elettroniche (CCE) e i database sanitari centralizzati rappresentano l'evoluzione più avanzata nel trattamento dei dati sanitari. Le CCE sono strumenti informatici adottati all'interno di strutture ospedaliere e studi medici per tracciare in tempo reale diagnosi, terapie, esami e anamnesi del paziente. A differenza della versione cartacea, offrono vantaggi tangibili: accesso immediato ai dati, riduzione degli errori dovuti alla trascrizione manuale, tracciabilità delle modifiche e supporto per decisioni cliniche tempestive.

Oltre alle CCE, esistono anche sistemi più ampi che aggregano i dati sanitari a livello regionale o nazionale, creando veri e propri database in grado di accompagnare il paziente lungo tutto il suo percorso di cura. Questi strumenti, se ben progettati, favoriscono la continuità assistenziale, agevolano il lavoro dei professionisti e aprono nuove possibilità per la ricerca scientifica e la prevenzione.

In Italia, un esempio concreto di questo processo è rappresentato dal Fascicolo Sanitario Elettronico (FSE). L'FSE, introdotto in Italia dal D.L. n. 179/2012, punta a integrare queste cartelle in un livello sovraregionale e multidisciplinare. Al suo interno confluiscono referti, lettere di dimissione, prescrizioni, vaccini, taccuino personale e persino dati da dispositivi indossabili. Grazie all'interoperabilità, un medico in Piemonte può accedere a dati sanitari generati in Basilicata o viceversa.

Vantaggi concreti emergono nella continuità assistenziale, nella partecipazione attiva del paziente e nel supporto decisionale: ad esempio, allarmi automatici su interazioni farmacologiche o cambiamenti insoliti nei valori biologici del paziente. Dal punto di vista sociale, l'aggregazione di milioni di fascicoli in un database pseudonimizzato favorisce la ricerca clinica, la prevenzione delle epidemie e la pianificazione sanitaria, purché siano rispettati protocolli di anonimizzazione e trattamento.

Tuttavia, i limiti non mancano. Sul piano tecnico, l'attuazione del FSE è ancora disomogenea: da una parte, alcune regioni hanno adattato pienamente i documenti, raggiungendo fino al 95 % della disponibilità, dall'altra regioni più arretrate rimangono sotto il 30 % . Gli standard per codifica, metadati e interoperabilità non sono uniformi, ostacolando l'uso analitico dei dati.

Sul piano della sicurezza, i rischi di accessi non autorizzati, data breach e attacchi informatici restano elevati. Per ottemperare a ciò vengono imposti l'uso di autenticazione multilivello, crittografia, autorizzazioni differenziate e procedure periodiche di verifica.

Infine, il rischio culturale: un database sanitario è efficace solo se i cittadini vi riconoscono affidabilità. Tuttavia, studi indicano che meno della metà della popolazione conosce l'esistenza del FSE, e solo circa il 33 % lo utilizza attivamente; la scarsa alfabetizzazione digitale e la mancanza di fiducia nel sistema rappresentano ostacoli reali alla piena efficacia di questi strumenti.

Parallelamente alla diffusione dei database sanitari, l'utilizzo dei Big Data sta rivoluzionando la ricerca medica e la governance della salute pubblica. L'enorme quantità di dati generati ogni giorno da dispositivi medici, applicazioni mobili e piattaforme sanitarie consente di individuare pattern, anticipare epidemie, personalizzare trattamenti e rendere i sistemi sanitari più efficienti e predittivi. I sistemi di intelligenza artificiale applicati ai dati sanitari sono in grado di individuare

correlazioni invisibili all'occhio umano, aprendo la strada a una medicina di precisione sempre più sofisticata.

In questo scenario, assume crescente rilevanza il concetto di "data altruism", introdotto nel Regolamento europeo sulla governance dei dati (Data Governance Act). Il data altruism si riferisce alla condivisione volontaria e gratuita dei propri dati da parte degli individui, per finalità di interesse generale come la ricerca scientifica, la sanità pubblica o la gestione delle emergenze. Questo approccio si fonda su una logica collaborativa e solidale, in cui il cittadino diventa parte attiva del progresso collettivo, mettendo a disposizione i propri dati in modo consapevole e regolato. Tuttavia, il passaggio da una logica di "protezione" a una logica di "condivisione responsabile" richiede strumenti giuridici e tecnologici affidabili. Il consenso al data altruism deve essere espresso in modo libero, informato, specifico e revocabile, nel pieno rispetto del GDPR. Sono necessari intermediari certificati, gli "organismi di altruismo dei dati", che garantiscano la trasparenza delle finalità, la sicurezza delle modalità di trattamento e l'effettiva destinazione dei dati agli scopi dichiarati. In ambito sanitario, ciò implica una delicata gestione dell'equilibrio tra libertà individuale e interesse collettivo.

L'introduzione di questi meccanismi rappresenta un potenziale cambio di paradigma: da cittadini soggetti a profilazione e rischio di esposizione, a protagonisti consapevoli di un ecosistema etico di dati condivisi. Ma affinché il data altruism possa realizzarsi su larga scala, è necessario colmare il divario informativo tra cittadini e istituzioni, rafforzare la fiducia nelle infrastrutture di protezione dei dati e garantire una reale inclusività, che non escluda chi è meno digitalizzato o consapevole.

Se gli strumenti finora descritti rappresentano l'infrastruttura attuale su cui si fonda la gestione e l'accessibilità dei dati sanitari in Italia, a livello europeo si sta delineando una prospettiva più ampia e ambiziosa. Il progetto dell'European Health Data Space (EHDS) si inserisce proprio in questa visione di lungo periodo, mirando a costruire un ecosistema digitale integrato e interoperabile tra tutti gli Stati membri.

L'obiettivo è duplice: da un lato, facilitare l'accesso primario ai dati per migliorare la qualità delle cure fornite ai pazienti ovunque si trovino nell'UE; dall'altro, consentire un accesso secondario per finalità di ricerca scientifica, pianificazione delle politiche sanitarie, innovazione e sviluppo di tecnologie mediche.

L'European Health Data Space (EHDS) si basa su una struttura di governance a più livelli, pensata per rendere più semplice e sicuro l'utilizzo dei dati sanitari in tutta Europa. Prevede regole condivise, strumenti tecnici per far dialogare i diversi sistemi digitali e certificazioni che garantiscano il rispetto di standard elevati da parte delle piattaforme che gestiscono queste informazioni. Grazie a questo sistema, ogni cittadino europeo potrà accedere facilmente ai propri dati sanitari elettronici – come cartelle cliniche, prescrizioni, immagini diagnostiche e referti – anche quando provengono da paesi diversi. Si tratta di un importante passo avanti verso una sanità europea davvero connessa.

Contestualmente, l'EHDS introduce un quadro regolatorio per l'accesso secondario ai dati, prevedendo che enti pubblici, ricercatori e industrie farmaceutiche possano utilizzare i dati sanitari – rigorosamente anonimizzati – per finalità diverse dalla cura diretta. L'uso secondario sarà però soggetto a una procedura di autorizzazione rigorosa da parte di organismi appositi al fine di garantire trasparenza, equità e sicurezza. Tali autorizzazioni saranno rilasciate solo per progetti che dimostrino una chiara finalità di interesse pubblico, escludendo l'uso commerciale diretto o la profilazione individuale.

Un elemento chiave della proposta è il principio di interoperabilità: affinché lo scambio dei dati sia efficace, è necessario che i sistemi informativi sanitari parlino la stessa lingua, condividano formati, codifiche e standard comuni. A tal fine, l'EHDS promuove l'adozione di standard tecnici vincolanti e la creazione di un'infrastruttura europea federata, che metta in comunicazione piattaforme e banche dati, pur mantenendo il controllo locale sui flussi informativi. La sicurezza rappresenta un pilastro essenziale dell'intero impianto: il regolamento prevede l'adozione di misure

avanzate di protezione informatica per garantire la massima tutela della privacy dei pazienti.

Tuttavia, il progetto solleva anche alcune criticità. La prima riguarda l'armonizzazione normativa: gli Stati membri partono da contesti legislativi e tecnologici profondamente diversi, e l'applicazione uniforme delle nuove regole richiederà uno sforzo di coordinamento significativo. Un'altra questione importante è il rapporto tra l'EHDS e il GDPR; mentre il regolamento generale sulla protezione dei dati si fonda sul principio del consenso e della limitazione delle finalità, l'EHDS introduce deroghe e meccanismi autonomi di gestione dell'accesso secondario, che potrebbero generare incertezze giuridiche. Altre sfide riguardano l'adozione di standard tecnici condivisi e l'effettiva interoperabilità dei sistemi, ancora oggi frammentata a livello nazionale.

In definitiva, lo Spazio Europeo dei Dati Sanitari rappresenta una delle iniziative più ambiziose dell'UE nel campo della sanità digitale. Il suo successo dipenderà dalla capacità di bilanciare innovazione tecnologica e garanzie giuridiche, promuovendo un modello europeo che ponga la persona al centro, nel rispetto della sua dignità, autonomia e riservatezza.

4. Il GDPR e strumenti per la tutela dell'individuo

La crescente digitalizzazione del settore sanitario e la centralità dei dati personali nelle dinamiche di cura, ricerca e prevenzione pongono la necessità di garantire la protezione dei diritti fondamentali degli individui. In questo contesto, il quadro giuridico europeo, e in particolare il Regolamento generale sulla protezione dei dati (GDPR), definisce principi e diritti essenziali che rappresentano la base per una gestione responsabile dei dati sanitari.

All'interno del quadro normativo europeo, il GDPR (Regolamento UE 2016/679) rappresenta il pilastro per la protezione dei dati personali, con un'attenzione particolare ai dati sensibili, come quelli sanitari. Il trattamento di tali dati è ammesso solo se avviene nel rispetto di alcuni principi fondamentali: la liceità, la correttezza e la trasparenza richiedono che l'interessato sia informato in modo chiaro sulle finalità e modalità del trattamento; il principio di minimizzazione impone che vengano raccolti solo i dati strettamente necessari; quello di limitazione della finalità vieta usi diversi da quelli dichiarati.

Poiché i dati sanitari sono particolarmente delicati, il GDPR impone garanzie elevate di integrità e riservatezza, introducendo obblighi tecnici e organizzativi per prevenire accessi non autorizzati o trattamenti illeciti. Inoltre, il principio di responsabilizzazione (accountability) impone al titolare del trattamento non solo di rispettare le regole, ma anche di dimostrare in ogni momento la conformità al regolamento.

Nel contesto sanitario, la base giuridica più comune per il trattamento dei dati è il consenso dell'interessato, che deve essere libero, specifico, informato ed esplicito. Tuttavia, il GDPR ammette anche eccezioni: per esempio, in caso di sanità pubblica, diagnosi mediche o obblighi legali, il trattamento può avvenire senza consenso, purché siano rispettate precise condizioni di sicurezza e legittimità.

Il regolamento rafforza anche i diritti dell'interessato: è possibile accedere ai propri dati, chiederne la rettifica o la cancellazione, limitarne il trattamento o opporsi, nei casi previsti. Il diritto alla portabilità consente inoltre di ricevere i propri dati in un formato strutturato e trasferirli a un altro titolare.

In ultima analisi, il GDPR ha promosso un vero cambio di paradigma, trasformando la protezione dei dati in un elemento strutturale della relazione tra paziente e sistema sanitario. La logica non è più solo quella del rispetto formale delle norme, ma quella di una tutela integrata e preventiva, che si realizza anche attraverso strumenti progettuali come la privacy by design.

Proprio a partire da questi principi, è possibile identificare una serie di strumenti e misure operative che rafforzano la tutela dei dati sanitari e la protezione dell'individuo nella società digitale.

L'anonimizzazione rappresenta una delle misure più incisive in tal senso: consiste in un processo di trasformazione del dato volto a impedire, in maniera definitiva, l'identificazione dell'interessato. Una volta anonimizzato, il dato non è più riconducibile a una persona fisica, neppure attraverso l'incrocio con altre informazioni, e quindi non è più soggetto alla normativa sulla protezione dei dati personali. Tuttavia, questa soluzione risulta spesso poco funzionale in ambito sanitario, dove il collegamento con l'identità del paziente può essere necessario per garantire la continuità delle cure o per finalità di ricerca.

Per questo motivo si ricorre frequentemente alla pseudonimizzazione, ovvero a una tecnica che consente di "mascherare" l'identità dell'interessato sostituendo gli elementi identificativi diretti con codici o altri riferimenti indiretti. A differenza dell'anonimizzazione, la pseudonimizzazione è reversibile e permette di risalire all'identità solo tramite informazioni aggiuntive conservate separatamente e protette. Essa offre un compromesso tra tutela della privacy e utilità del dato,

risultando particolarmente utile nei progetti di ricerca scientifica e nell'elaborazione dei dati a fini statistici.

Un ulteriore strumento di tutela è rappresentato dal consenso granulare, che consente agli interessati di esercitare un controllo più preciso e consapevole sull'uso dei propri dati. Invece di un consenso generico e indistinto, questa modalità permette di decidere in modo selettivo a quali trattamenti acconsentire, per quali finalità, e da parte di quali soggetti. Si tratta di un passo importante verso una gestione più trasparente e responsabile dei dati, che mira a rafforzare il ruolo attivo del cittadino nel processo decisionale legato alla propria identità digitale.

In questo contesto di crescente digitalizzazione della sanità, la prevenzione delle discriminazioni legate allo stato di salute o alla storia clinica assume un ruolo centrale nella tutela della persona. La disponibilità e l'accessibilità dei dati sanitari, se non correttamente regolata, può infatti alimentare dinamiche discriminatorie, sia nel settore pubblico che in quello privato, in ambiti come il lavoro, l'istruzione, le assicurazioni o l'accesso a determinati servizi.

Garantire la non discriminazione significa non solo vietare l'uso improprio del dato, ma costruire un sistema in cui ogni paziente sia posto al centro, rispettato nella sua integrità e protetto da trattamenti differenziati ingiustificati. Questo obiettivo richiede politiche attive e strumenti giuridici efficaci, ma anche un'evoluzione culturale che riconosca la persona al di là del suo stato di salute, presente o passato.

La tutela del paziente, in una società digitale, non può più limitarsi alla sola protezione del dato, ma deve estendersi alla gestione dei processi decisionali che utilizzano tali dati. Occorre rafforzare la trasparenza degli algoritmi, garantire la possibilità di intervento umano nelle decisioni automatizzate e prevedere strumenti di ricorso efficaci in caso di trattamenti discriminatori. A tal fine, risulta fondamentale il ruolo di organismi di vigilanza e garanzia, ma anche il

coinvolgimento attivo dei cittadini, che devono poter esercitare i propri diritti in modo consapevole, informato e tempestivo.

Un esempio significativo è dato dalla legge 15 dicembre 2023, n. 193 sull'oblio oncologico. La normativa sancisce il diritto per le persone guarite da una patologia oncologica a non essere discriminate sulla base del proprio passato clinico, soprattutto in contesti delicati come la stipula di contratti assicurativi, l'adozione di minori e l'accesso a concorsi o selezioni lavorative.

Il principio cardine della legge è che, trascorsi dieci anni dalla fine del trattamento attivo (cinque se la diagnosi è avvenuta prima dei 21 anni), il cittadino ha diritto a non fornire informazioni relative alla pregressa malattia oncologica e, soprattutto, che tali dati non possano essere utilizzati a suo svantaggio. Questo rappresenta un passaggio epocale non solo sul piano sociale e culturale, ma anche sotto il profilo giuridico e digitale, in quanto impone una nuova riflessione sulla gestione dei dati sanitari nel lungo periodo.

I sistemi sanitari e le infrastrutture digitali devono essere in grado di garantire che il dato non venga usato oltre i limiti di tempo previsti dalla legge e che, laddove richiesto, possa essere "oscurato" rispetto a specifiche finalità. La sfida, in questo senso, è duplice: da un lato tecnica, perché richiede meccanismi di controllo flessibili; dall'altro culturale, perché invita a superare stereotipi e pregiudizi ancora radicati nel rapporto tra salute e identità.

Si tratta, quindi, di un'ulteriore conferma di come il diritto alla salute digitale non sia soltanto una questione di tecnologie, ma un terreno di giustizia sostanziale, in cui il rispetto della dignità della persona si misura anche nella capacità del sistema di "dimenticare" ciò che non deve più essere ricordato.

In questo contesto, il ruolo delle autorità di controllo nazionali, in particolare del Garante per la protezione dei dati personali, diventa cruciale per assicurare che i principi delineati dal GDPR vengano effettivamente rispettati. Il Garante opera come

organismo indipendente e ha il compito di vigilare sul trattamento dei dati sanitari, intervenendo in caso di violazioni e fornendo linee guida per l'applicazione uniforme delle regole.

Tra le sue prerogative rientrano l'autorizzazione di trattamenti particolarmente delicati, la valutazione d'impatto sui diritti e le libertà degli interessati, e l'adozione di misure correttive nei confronti di soggetti pubblici e privati che non rispettano le norme. Il Garante può imporre limitazioni o blocchi al trattamento oppure applicare sanzioni amministrative. In ambito sanitario, ha un'importante funzione di guida interpretativa, offrendo chiarimenti su temi complessi come l'utilizzo dei dati per scopi scientifici, la loro conservazione prolungata e l'eventuale accesso da parte di terzi.

A ciò si affiancano i meccanismi interni di controllo che ogni titolare del trattamento è tenuto a predisporre: dal registro delle attività di trattamento alla nomina del Responsabile della Protezione dei Dati (DPO), dalle procedure di gestione delle violazioni di dati personali (data breach) alle valutazioni d'impatto sulla protezione dei dati (DPIA). Questi strumenti, oltre a garantire la conformità normativa, costituiscono un presidio essenziale per prevenire rischi e rafforzare la fiducia dei cittadini nel sistema sanitario digitale. La trasparenza, la tracciabilità degli accessi e la responsabilizzazione degli attori coinvolti rappresentano elementi indispensabili per costruire un ecosistema in cui l'innovazione tecnologica non sia in contraddizione con i diritti fondamentali della persona, ma ne diventi piuttosto un veicolo di tutela e valorizzazione.

5. Conclusione

La digitalizzazione dei dati sanitari apre prospettive straordinarie, potenziando diagnosi, cura e prevenzione attraverso strumenti intelligenti come cartelle cliniche elettroniche, Big Data e spazi di condivisione come l'EHDS. Questi dati alimentano nuove modalità di ricerca e miglioramento delle politiche sanitarie, favorendo una sanità predittiva e personalizzata, con risparmi stimati in decine di miliardi nel prossimo decennio.

Allo stesso tempo, emergono rischi rilevanti legati alla privacy, alla sicurezza e alla discriminazione. Accessi non autorizzati, utilizzi impropri, gap normativi tra sistemi e difficoltà nell'anonimizzazione pongono sfide complesse. L'adozione del GDPR ha introdotto strumenti essenziali, ma serve una coerente implementazione a livello nazionale per garantire tutele effettive.

Per trasformare le opportunità in risultati concreti e sicuri, è necessario un approccio integrato: infrastrutture interoperabili, regole uniformi, etica informatica e alfabetizzazione digitale dei cittadini. Solo così il dato sanitario potrà diventare una leva di progresso senza compromettere la dignità e i diritti dell'individuo.

La sfida non è solo tecnica o normativa, ma profondamente umana: si tratta di creare un ecosistema in cui l'innovazione sostenga la persona, ponendo fiducia, consapevolezza e partecipazione al centro della sanità del futuro. Non si deve scegliere tra progresso e privacy, ma renderli compatibili. Le tecnologie possono diventare alleate dei diritti, se progettate con trasparenza, controllo individuale e equità d'accesso.

In questa prospettiva, strumenti come il consenso granulare, l'anonimizzazione forte, l'accesso controllato e la certificazione delle piattaforme assumono un ruolo centrale. Fondamentale è anche il coinvolgimento attivo di tutti gli attori —

cittadini, professionisti sanitari, istituzioni e sviluppatori — per costruire un sistema basato su responsabilità condivisa.

Il diritto deve restare un argine e una guida, capace di accompagnare l'innovazione senza irrigidirla e di proteggerla da abusi o discriminazioni. Costruire questo equilibrio non è un traguardo raggiunto, ma un processo continuo, da monitorare e aggiornare.

Nel cuore della trasformazione digitale della sanità si colloca il dato: fragile e potente allo stesso tempo, individuale ma con un potenziale collettivo enorme. La sua gestione richiede una visione integrata e consapevole, lontana da approcci meramente tecnici o burocratici.

Valorizzare il dato sanitario significa saperlo proteggere, ma anche impiegarlo per migliorare la cura, prevenire malattie e sviluppare politiche pubbliche più efficaci. È un valore che cresce se ne garantiamo l'integrità, la condivisione sicura e la trasparenza verso i cittadini.

Nel bilanciamento tra tutela e sviluppo, tra protezione e apertura, si gioca il futuro di una sanità capace di affrontare le nuove sfide restando sempre al servizio della persona.

Bibliografia

Autorità Garante per la protezione dei dati personali. (2022). *Relazione annuale 2022*. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9896236

European Commission. (2022, May 3). *Proposal for a Regulation on the European Health Data Space* (COM(2022) 197 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0197

Ministero della Salute. (2023). *Fascicolo Sanitario Elettronico – FSE 2.0*. https://www.salute.gov.it/portale/fse/homeFSE.jsp

Ministero della Salute. (2023). *Sanità digitale: scenari e prospettive*. https://www.salute.gov.it

Parlamento italiano. (2023). *Legge 7 dicembre 2023, n. 193: Disposizioni in materia di oblio oncologico*. Gazzetta Ufficiale n. 289 del 12 dicembre 2023. https://www.gazzettaufficiale.it/eli/id/2023/12/12/23G00197/sg

Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (GDPR). *Gazzetta ufficiale dell'Unione europea*, L 119, 4.5.2016. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Unione Europea. (2022). *European Health Data Space – Fact Sheet*. https://health.ec.europa.eu/system/files/2022-05/ehealth_factsheet_en_0.pdf