

IL DATO SANITARIO COME ELEMENTO FONDANTE DELL'INTELLIGENZA ARTIFICIALE AL SERVIZIO DEL PAZIENTE E DELLA RICERCA

Paco D'Onofrio

I. BLOCKCHAIN, TELEMEDICINA E GARANZIE COSTITUZIONALI NELLA GESTIONE DEI DATI SANITARI: MODELLI INNOVATIVI E CRITICITÀ GIURIDICHE

L'irruzione della tecnologia blockchain nell'ambito sanitario non costituisce un mero passo avanti sul piano tecnico-informatico, bensì segna un vero spartiacque concettuale ed operativo nella configurazione giuridica della gestione dei dati sanitari e, più in generale, nei modelli di erogazione delle prestazioni assistenziali¹. L'interazione sempre più stretta tra sanità digitale, intelligenza artificiale e architetture distribuite chiama oggi il diritto a confrontarsi con una dimensione inedita, nella quale le tradizionali categorie dogmatiche risultano messe alla prova da esigenze di efficienza, sicurezza e rispetto delle libertà fondamentali². Si assiste così ad una tensione, tanto feconda quanto problematica, fra l'innovazione tecnologica e il presidio dei diritti, fra l'urgenza della semplificazione operativa e la complessità della tutela giuridica, in un equilibrio che, *ictu oculi*, appare ancora instabile. In questo contesto, blockchain e telemedicina si impongono non solo come strumenti tecnici, ma come autentici dispositivi regolativi, capaci di ridefinire le responsabilità giuridiche, le relazioni istituzionali e le forme normative attraverso cui si struttura il governo del dato sanitario³.

La blockchain, nella sua essenza di registro distribuito e immutabile, si configura quale infrastruttura decentralizzata per l'archiviazione e la gestione dell'informazione,

¹ E. CATELANI, *Nuove tecnologie a tutela del diritto della salute: potenzialità e limiti dell'uso della Blockchain*, in *Federalismi.it*, 2022; E. SIGNORINI, F. ZAMBARDINO, *La blockchain e la telemedicina: quali opzioni per la sicurezza e l'integrità dei dati sanitari*, in *Federalismi.it*, 27, 2024, p. 205 ss.

² F. APERIO BELLA, *L'accesso alle tecnologie innovative nel settore salute tra universalità e limiti organizzativi (con una postilla sull'emergenza sanitaria)*, in *Persona e Amministrazione*, 2020, p. 220.

³ G. CHIARINI, *Telemedicina, attenzione ai profili di responsabilità*, 2024, in *www.sanita24.ilsole24ore.com*; M. FACCIOLI, *La responsabilità sanitaria in telemedicina*, 2021, in *Resp. Civ. Prev.*, pp. 740-755.

nella quale ogni nodo della rete detiene copia integrale delle transazioni e partecipa alla loro validazione tramite meccanismi di consenso condiviso. Tale architettura, per sua natura, si oppone strutturalmente ad ogni tentativo di manipolazione arbitraria, garantendo integrità, trasparenza e tracciabilità dell'informazione. Tali caratteristiche assumono un rilievo dirimente nel settore sanitario, connotato da un'elevatissima sensibilità dei dati trattati e da una fitta rete di relazioni tra pazienti, operatori sanitari, enti pubblici e soggetti privati. In siffatto ambito, l'innovazione in parola assurge a strumento fiduciario, in grado di assicurare la verificabilità e la sicurezza degli scambi informativi, nel rispetto del principio di *accountability* che rappresenta uno dei pilastri del trattamento, legittimo, dei dati.

Il connubio tra blockchain e telemedicina produce effetti dirompenti sul piano sistemico, amplificando la portata trasformativa delle tecnologie digitali. La telemedicina, quale forma di assistenza erogata a distanza, si pone al crocevia tra accessibilità, sostenibilità ed innovazione, sfidando i modelli tradizionali di presa in carico del paziente. L'integrazione tra questi strumenti consente la costruzione di un ecosistema sanitario connesso, ove la raccolta, l'elaborazione e la condivisione dei dati diventano processi continui e dinamici, idonei a promuovere una medicina predittiva e personalizzata. In tal modo, si afferma una nuova centralità del paziente, che da oggetto di cura si trasforma in soggetto attivo del proprio percorso terapeutico, secondo una logica che potrebbe dirsi, *rectius*, partecipativa. L'impiego di apparecchi *wearable*, sensori biometrici, piattaforme di telemonitoraggio, intelligenze artificiali clinicamente addestrate e dispositivi ingeribili marca, in questo senso, un punto di svolta nell'architettura della relazione di cura.

In tale quadro, la blockchain assume una funzione strutturante nella protezione dell'informazione, assicurando la tracciabilità delle transazioni, la protezione contro accessi non autorizzati e la possibilità di ricostruzione dell'intera filiera informativa⁴. Il modello peer-to-peer, privo di un'autorità centrale, riduce la vulnerabilità tipica dei sistemi accentrati, notoriamente esposti a cyberattacchi e disservizi. Ogni blocco della catena contiene il riferimento al precedente, in un *continuum* che rende impossibili modifiche retroattive, garantendo un controllo diffuso, secondo una logica di sorveglianza orizzontale. Il dato, così strutturato, assume valore probatorio potenzial-

⁴ F. FAINI, *Blockchain e diritto. La "catena del valore" tra documenti informatici, smart contracts e data protection*, in *Responsabilità civile e previdenza*, 2020, I, pp. 297-316; ID., *Il diritto nella tecnica: tecnologie emergenti e nuove forme di regolazione*, in *federalismi.it*, 2020, XVI, pp. 79-117; ID., *Data society. Governo dei dati e tutela dei diritti nell'era digitale*, Milano, 2019; B. CAPIELLO, G. CARULLO, *Blockchain, Law and Governance*, Cham, 2020; R. BRUSCHI, *Le applicazioni delle nuove tecnologie: criptovalute, blockchain e smart contract*, in *Il Diritto industriale*, 2020, II, pp. 162-164; M. CASTELLANI, P. POMI, C. TIBERTI, A. TURATO, *Blockchain. Guida pratica tecnico giuridica all'uso*, Firenze, 2019; R. BASHIR, *Mastering Blockchain. Distributed ledger technology, decentralization, and smart contracts explained*, Birmingham, 2018; M. FINK, *Blockchains and Data Protection in the European Union*, in *European Data Protection Law Review*, 2018, IV, pp. 17-35.

mente rilevante, in linea con la tendenza giurisprudenziale a valorizzare le tecnologie come strumenti di tracciabilità giuridicamente rilevante.

Tra le applicazioni più promettenti vi è certamente quella relativa alla gestione del consenso informato. In un ecosistema sanitario fondato sulla centralità del dato, è imprescindibile garantire modalità di acquisizione del consenso che siano trasparenti, verificabili e reversibili. La blockchain consente di registrare il consenso dell'interessato in forma immutabile, conferendogli un valore giuridico (quindi, in prospettiva, anche processuale) rafforzato, capace di soddisfare al contempo le esigenze di prova e di autodeterminazione informativa. L'interessato può, in ogni momento, conoscere chi ha avuto accesso ai suoi dati, in quale circostanza e per quali finalità, nel rispetto del principio di trasparenza, che *ex lege* ispira l'intero assetto normativo del GDPR. Si realizza così una sintesi equilibrata fra efficienza e garanzia, fra fluidità operativa e protezione dei diritti.

Tuttavia, una tale applicazione in ambito sanitario solleva interrogativi complessi di compatibilità normativa, specie in relazione ai principi posti dal Regolamento (UE) 2016/679. L'immutabilità del registro, elemento costitutivo della blockchain, mal si concilia con i diritti alla rettifica ed alla cancellazione dei dati personali, previsti *in primis* dagli artt. 16 e 17 del GDPR. Analoga problematicità emerge sul fronte dell'individuazione del titolare del trattamento, reso opaco dalla struttura distribuita del sistema. Ciò impone un ripensamento dell'intero paradigma regolativo, alla luce di una ricostruzione sistematica che, senza abdicare ai principi fondanti dell'ordinamento europeo, sia in grado di integrare le nuove tecnologie nel tessuto giuridico esistente.

Al contempo, l'interazione tra blockchain, intelligenza artificiale e telemedicina impone una riflessione rinnovata sulla responsabilità sanitaria. In un ambiente in cui le decisioni cliniche sono supportate da strumenti algoritmici e l'informazione è condivisa in modalità decentralizzata, occorre ridefinire i confini della colpa medica, degli obblighi informativi e delle garanzie assicurative. L'uso integrato di dati eterogenei – genetici, comportamentali, ambientali – apre scenari diagnostici inediti, ma espone anche a nuove forme di discriminazione, che vanno arginate con strumenti normativi ispirati al principio di precauzione. Non si tratta di erigere nuove barriere, ma di governare la complessità secondo una logica di equilibrio dinamico tra tutela ed innovazione.

In tale orizzonte, il Fascicolo Sanitario Elettronico (FSE) rappresenta il primo banco di prova dell'incontro tra innovazione digitale e garanzie giuridiche⁵. Esso condensa le tensioni tra interoperabilità e sicurezza, tra centralità della persona e uniformità dei protocolli, tra apertura dei dati e riservatezza. L'implementazione della blockchain potrebbe favorire la nascita di un'infrastruttura unitaria, interoperabile e trasparente, in cui le informazioni siano consultabili in tempo reale da soggetti

⁵ M. FARINA, *Blockchain e tutela della salute: verso la riorganizzazione dei sistemi sanitari?* in *Federalismi.it*, 2020, p. 173.

autorizzati, nel rispetto del principio di minimizzazione e con idonei meccanismi di controllo da parte dell'interessato. Si tratta di un'evoluzione non solo tecnologica, ma eminentemente giuridica, che richiama l'esigenza di un governo pubblico della trasformazione digitale.

Non va sottovalutato, peraltro, che l'adozione di soluzioni come la telemedicina e, ancor più, della blockchain, implica un radicale mutamento culturale e organizzativo. La *digital literacy*, vale a dire la competenza digitale degli utenti, si configura come prerequisito indefettibile per un accesso equo e consapevole alle cure. Occorre, *in re ipsa*, accompagnare tale transizione con percorsi formativi rivolti tanto ai cittadini quanto agli operatori sanitari, chiamati ad acquisire nuove abilità tecniche, deontologiche e giuridiche. L'assenza di tali strumenti rischierebbe di generare nuove forme di esclusione e disuguaglianza, in contraddizione con il mandato inclusivo proprio della sanità pubblica.

Un segnale in tale direzione proviene dal legislatore nazionale, che con la legge n. 33/2023 e il d.lgs. n. 29/2024 ha inteso rafforzare il ruolo della telemedicina e dell'assistenza digitale domiciliare, anche mediante il sostegno offerto dal Piano Nazionale di Ripresa e Resilienza (PNRR). In particolare, è stato previsto che l'accesso ai servizi digitali avvenga previa valutazione dell'eleggibilità clinica, tecnologica e sociale dell'assistito, secondo criteri fissati da AGENAS. Si tratta di un primo tentativo, certo ancora perfezionabile, di coniugare l'innovazione tecnologica con l'imperativo costituzionale dell'uguaglianza sostanziale.

Non meno rilevante è il contributo che la blockchain può offrire sul versante della tracciabilità dei farmaci e del contrasto alle frodi assicurative. La possibilità di attestare l'autenticità, la provenienza e la correttezza prescrittiva dei medicinali consente, *a fortiori*, di tutelare il paziente e razionalizzare la spesa sanitaria. L'utilizzo di *smart contracts* e algoritmi predittivi può semplificare la gestione dei sinistri e dei rimborsi, a condizione che vengano predisposti presidi efficaci di trasparenza, controllo e attribuzione della responsabilità⁶.

In definitiva, il nesso tra blockchain, telemedicina e trattamento dei dati sanitari interpella il diritto nella sua capacità di governare la modernità. Da un lato, s'impone la necessità di predisporre regole chiare e coerenti, che prevengano abusi e rafforzino la fiducia dei cittadini; dall'altro, si apre la possibilità di utilizzare le tecnologie per dare attuazione concreta ai principi costituzionali di solidarietà, efficienza e inclusione. *Tertium non datur*: il diritto, in una prospettiva normativa fluida deve porsi come garante dell'innovazione, o finirà fatalmente per esserne un ostacolo, potendo contribuire a costruire un sistema sanitario orientato alla persona e capace di reggere la complessità del tempo presente. La blockchain, in quest'ottica, non è più solo uno strumento tecnico,

⁶ M. GIULIANO, *La blockchain e gli smart contracts nell'innovazione del diritto nel terzo millennio*, in *Dir. Inform.*, 2018, p. 996.

ma diventa lo spazio in cui il diritto è chiamato a reinventare sé stesso, coniugando la dignità della persona e l'efficienza dei processi in un nuovo patto giuridico sulla salute.

2. IL GOVERNO NORMATIVO DEI DATI SANITARI TRA CONSERVAZIONE E SICUREZZA

La gestione e la conservazione dei dati sanitari rappresentano, nell'attuale ecosistema digitale, una delle sfide più complesse e controverse del diritto pubblico dell'innovazione. Essi si collocano al crocevia tra l'istanza di efficienza ed accessibilità dei servizi sanitari, da un lato, e la necessità di salvaguardare la riservatezza, l'integrità e la disponibilità di informazioni ad alta densità sensibile, dall'altro. Il tessuto normativo vigente, nondimeno, appare talvolta inadeguato a sostenere la portata di tale complessità: come ha rilevato una parte della dottrina, permane un *vulnus* regolativo, tanto nell'ordinamento nazionale quanto in quello sovranazionale, che genera effetti distorsivi sulla sicurezza dei dati, sulla loro conservazione prolungata e sul pieno rispetto dei diritti dell'interessato⁷. L'assenza di una cornice normativa organica rischia di compromettere l'attuazione del principio di *accountability*, esponendo il sistema sanitario ad un'instabilità strutturale che, *rebus sic stantibus*, può minare la legittimazione stessa del processo di digitalizzazione.

I dati sanitari, come noto, rientrano tra le informazioni qualificabili *ex lege* come “*particolari*”, ai sensi dell'art. 9 del Regolamento (UE) 2016/679 (GDPR), e la loro gestione impone l'adozione di tutele rafforzate in ogni fase del trattamento. La definizione offerta dall'art. 4, par. 15, del medesimo Regolamento, che include qualsiasi informazione relativa alla salute fisica o mentale della persona, estende l'oggetto della protezione ben oltre i dati clinici in senso stretto, includendo anche elementi potenzialmente idonei a rivelare indirettamente lo stato di salute. In un contesto in cui la medicina evolve verso modelli predittivi e personalizzati, e in cui le distinzioni tra dato, informazione e conoscenza tendono a sfumare, diventa dirimente assicurare che le modalità di conservazione siano non solo conformi alle più aggiornate tecnologie, ma anche rispondenti ai principi generali dell'ordinamento, primi fra tutti quelli di liceità, minimizzazione, integrità e correttezza⁸.

Una delle criticità maggiormente evidenziate in sede scientifica riguarda l'assenza di criteri chiari ed uniformi per la conservazione a lungo termine dei dati digitali in ambito sanitario. Tale carenza finisce con l'indebolire il valore giuridico delle in-

⁷ E. SORRENTINO, *Gestione e conservazione dei dati sanitari. Il vulnus normativo che impatta su sicurezza e data protection*, in *Federalismi.it*, 29, 2024, p. 137 ss.

⁸ F. DI CIOMMO, *Il trattamento dei dati sanitari tra interessi individuali e collettivi*, in *Danno e resp.*, 2002, 2, 121; S. MELCHIONNA, F. CECAMORE, *Le nuove frontiere della sanità e della ricerca scientifica*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 679/2016 e al d.lgs. 101/2018*, Giuffrè, Milano, 2019, p. 585 e ss.

formazioni e con il compromettere la qualità del percorso assistenziale. Il Fascicolo Sanitario Elettronico (FSE), che dovrebbe costituire il cardine del sistema, appare ancora oggi afflitto da disomogeneità regionali, difficoltà di interoperabilità e carenze nell'indicizzazione univoca dei documenti. Nonostante l'apparato normativo di riferimento, costruito a partire dal d.l. n. 179/2012 e rafforzato dal d.p.c.m. n. 178/2015 e le spinte provenienti dal PNRR, l'implementazione concreta del FSE presenta criticità tali da ostacolare la trasformazione del dato in conoscenza clinicamente utile. Di conseguenza, il diritto del paziente a una cura informata, tempestiva ed efficace rischia di rimanere inattuato.

La mancata definizione di standard condivisi si pone altresì in contrasto con quanto prescritto dall'art. 44, comma 1-*ter*, del Codice dell'Amministrazione Digitale (d.lgs. n. 82/2005), che impone ai sistemi di conservazione dei documenti informatici il rispetto di requisiti di autenticità, leggibilità e affidabilità. Tradurre questi parametri nella realtà del dato sanitario implica un profondo ripensamento delle architetture informative, nonché un investimento strategico nelle competenze archivistiche e nei modelli organizzativi. In assenza di tali condizioni, il rischio è quello di generare una documentazione clinica fragile, esposta a fenomeni di obsolescenza, disallineamento semantico e compromissione del valore medico-legale.

A rendere ancora più articolato il quadro, si aggiunge la problematica dell'uso secondario dei dati sanitari, vale a dire il loro trattamento per finalità ulteriori rispetto a quelle originarie. Tra le più ricorrenti vi sono la ricerca biomedica, la programmazione sanitaria, le statistiche pubbliche, fino alla messa a punto di modelli predittivi. Tuttavia, l'ampiezza degli interessi pubblici in gioco non può legittimare deroghe indiscriminate ai diritti dell'interessato: si impone *ex necessitate* un bilanciamento ponderato tra la valorizzazione del patrimonio informativo e la protezione della sfera personale. Il Regolamento europeo sullo Spazio dei Dati Sanitari (EHDS) tenta di individuare una sintesi, prevedendo il riutilizzo di dati anonimizzati o pseudonimizzati, pur restando pendenti numerose criticità, in particolare sul fronte della trasparenza, del consenso e della valutazione d'impatto. Il parere congiunto dell'EDPB e del GEPD ha opportunamente richiamato la necessità di salvaguardare l'equilibrio fra finalità collettive e diritti individuali, ribadendo che l'innovazione normativa non può prescindere dal rigoroso rispetto del GDPR.

Un passaggio fondamentale verso un sistema più coerente è rappresentato dall'applicazione dei principi FAIR (*Findable, Accessible, Interoperable, Reusable*), già noti nel campo della ricerca scientifica. Questi principi mirano a strutturare il dato in modo che esso sia realmente fruibile, condivisibile e riutilizzabile, anche in contesti eterogenei. Tuttavia, *non omittendum*, la loro trasposizione nel settore sanitario richiede un'opera di adattamento profondo, che tenga conto della natura particolare del dato clinico e dei rischi di re-identificazione. Occorre quindi integrare i principi FAIR con una cornice normativa ispirata alla precauzione, ancorata ai valori costituzionali di dignità e autodeterminazione.

Il Garante per la protezione dei dati personali, nel valutare l'impianto normativo dell'Ecosistema Dati Sanitari (EDS), ha formulato osservazioni puntuali e severe, evidenziando profili di carenza sostanziale e procedurale. In particolare, l'Autorità ha sottolineato il pericolo di una concentrazione eccessiva delle informazioni cliniche, con il rischio di accessi impropri, utilizzi distorti e perdita del controllo da parte del titolare del dato. La duplicazione dei dati già presenti nel FSE, in assenza di una base giuridica chiara e di una valutazione d'impatto *ex art. 35 GDPR*, rafforza le perplessità circa la legittimità dell'intervento. Il Garante, tuttavia, non assume una posizione di "opposizione tecnologica", bensì svolge un ruolo di presidio critico, volto a garantire che l'innovazione si sviluppi nel rispetto dell'architettura dei diritti.

In un simile contesto, il principio di *privacy by design and by default*, previsto all'art. 25 GDPR, si conferma come uno strumento imprescindibile⁹. Esso impone che ogni progetto informatico incorpori *ab origine* le garanzie necessarie alla protezione del dato. Nella pratica della sanità digitale, ciò significa disegnare sistemi che proteggano automaticamente l'informazione sensibile, anche a costo di sacrificare, in via temporanea, alcuni margini di efficienza. La sostenibilità giuridica del sistema non può essere disgiunta dalla sua legittimità democratica: una sanità digitale priva di presidi normativi efficaci tradirebbe il patto fiduciario che deve legare cittadino ed istituzioni.

Non si tratta, pertanto, di una questione meramente tecnica. La riflessione giuridica è chiamata a compiere un salto di scala, elaborando una teoria costituzionale dell'informazione sanitaria, che ne riconosca la natura non neutrale. Il dato clinico, in quanto riflesso della persona, ha una valenza ontologica e simbolica ulteriore: custodirlo significa proteggere la memoria biografica, l'identità e la dignità del soggetto. In questa prospettiva, il legislatore non può limitarsi a regolare procedure, ma deve farsi promotore di una cultura pubblica della protezione dei dati, ispirata all'etica della cura ed alla responsabilità collettiva.

Il prefato argomento merita, infine, una puntualizzazione terminologica tutt'altro che irrilevante: la distinzione tra *data retention* e *data preservation*, spesso utilizzate in modo intercambiabile, in realtà risponde a logiche giuridiche differenti. La *retention* implica una conservazione a tempo determinato, funzionale alla finalità del trattamento; la *preservation*, invece, mira ad una custodia di lungo periodo, motivata da esigenze di interesse pubblico, quali la continuità terapeutica, la documentazione medico-legale o la ricerca. *In claris non fit interpretatio*: in ambito sanitario la necessità di garantire la permanenza del dato nel tempo deve accompagnarsi a misure di protezione rafforzata, ad una chiara individuazione delle finalità e ad una valutazione rigorosa della proporzionalità degli strumenti adottati.

In conclusione, il tema della conservazione dei dati sanitari rivela tutta la tensione tra diritto e tecnica, tra innovazione e tutela. Il vuoto normativo cui si è fatto

⁹ S. CALZOLAIO, *Privacy by design. Principi, dinamiche, ambizioni del nuovo Reg. UE 2016/679*, in *Federalismi.it*, 24, 2017, pp. 1-21.

riferimento non è solo una lacuna regolativa, ma il sintomo di un'incapacità più profonda di governare il cambiamento secondo principi di razionalità giuridica e rispetto della persona. Superarlo implica un'azione coordinata, multidisciplinare e costituzionalmente orientata, capace di fondare un nuovo modello di *governance* dei dati, rispettoso delle garanzie e aperto all'innovazione. La salute digitale deve diventare lo spazio in cui dignità, trasparenza e cura si saldano in un orizzonte condiviso, senza che tuttavia lo scenario di incertezza porti ad una rigidità burocratizzazione in chiave irragionevolmente prudente, con il rischio che la mancata circolazione dei dati rallenti la ricerca scientifica e vulneri il prezioso sostegno del *machine learning*¹⁰.

3. OLTRE LA PROTEZIONE: DATI SANITARI, MERCATI INFORMATIZIONALI E SFIDE GIURIDICHE DELLA MONETIZZAZIONE

Dunque, nel panorama della società digitale, i dati personali ed in particolar modo quelli sanitari assumono una centralità strategica che travalica la dimensione protettiva per accedere a quella propriamente economica e conoscitiva. Essi si impongono non solo come oggetto di tutela costituzionale, ma altresì come asset informativo capace di alimentare modelli di sviluppo scientifico, progresso biotecnologico ed innovazione terapeutica. La possibilità di impiegare e valorizzare, anche economicamente, tali dati, se adeguatamente anonimizzati, non si presenta più come un tabù etico o giuridico, bensì come un imperativo di sistema, volto a coniugare il progresso della medicina con l'efficienza e l'equità dei servizi sanitari pubblici¹¹. L'impiego di tecnologie emergenti, come l'intelligenza artificiale e il *machine learning*, rappresenta, in tale prospettiva, non un fine, ma un mezzo di razionalizzazione virtuosa, che trova nei dati la linfa vitale della sua operatività.

Il dato sanitario cessa, dunque, di essere concepito esclusivamente quale elemento soggettivamente "intangibile" e si configura piuttosto come risorsa comune, da valo-

¹⁰ F. PIRAINO, *I "diritti dell'interessato" nel Regolamento generale sulla protezione dei dati personali*, in *Giur. it.*, 2019, XII, 2777; R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole di mercato. Commentario al Reg. UE n. 2016/679 (GDPR) e al novellato D.lgs. n. 196/2003*, Milano, 2019; F. SENIGAGLIA, *Reg. UE 2016/679 e il diritto all'oblio nella comunicazione telematica. Identità, informazione e trasparenza nell'ordine della dignità personale*, in *Leggi Civ. Comm.*, 2017, p. 1023 ss.; R. TORINO, *Il diritto di opposizione al trattamento dei dati personali e il diritto a non essere sottoposti a decisioni basate su trattamenti automatizzati e alla profilazione nel Regolamento (UE) 2016/679*, in *Cittadinanza eur.*, 2018, p. 45 ss.; P. PERLINGIERI, *Privacy digitale e protezione dei dati personali*, cit., pp. 483-484; ID., *Principio personalista, dignità umana e rapporti civili*, in *Annali della SISDIC*, 2020, p. 1 ss.; E. TOSI (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice privacy*, Milano, 2019.

¹¹ L.M. LUCARELLI TONINI, *La monetizzazione dei dati personali: applicazione e rischi relativi al trattamento dei dati inerenti la salute*, in *Dirittifondamentali.it*, n. 2, 2022.

rizzare secondo logiche di utilità collettiva. La sua circolazione in forma anonimizzata, lungi dal porsi in antitesi con la protezione dei diritti fondamentali, appare oggi funzionale alla creazione di una medicina predittiva, personalizzata e proattiva. La cessione regolata e trasparente di tali informazioni, in forma aggregata, contribuisce allo sviluppo di algoritmi diagnostici e modelli decisionali che innalzano il livello qualitativo dell'intervento clinico e favoriscono l'allocazione efficiente delle risorse.

Tale mutamento di paradigma impone, *de iure condendo*, una revisione dell'inquadramento giuridico dei dati sanitari anonimizzati, che non può più essere rigidamente ancorato all'alveo dei diritti soggettivi, ma deve orientarsi verso la sfera degli interessi legittimi. Tale riconfigurazione, lungi dal depotenziare le garanzie dell'individuo, consente un bilanciamento più equilibrato tra tutela personale e finalità di ricerca, rendendo possibile un utilizzo dei dati coerente con i principi di proporzionalità e ragionevolezza. In ciò risiede la premessa per un nuovo patto tra diritto e scienza, capace di sostenere l'innovazione senza arretramenti sul fronte delle garanzie.

La disciplina europea, pur nata all'insegna della protezione individuale, non preclude la valorizzazione dei dati sanitari a fini scientifici e commerciali, purché tale impiego avvenga nel rispetto delle condizioni previste. L'uso secondario dei dati anonimizzati, se diretto a finalità di ricerca, innovazione terapeutica o pianificazione pubblica, è ritenuto compatibile con l'etica medica e con l'impianto regolativo del GDPR. Il requisito dell'anonimizzazione effettiva, in tale ambito, rappresenta condizione dirimente, pena la trasformazione di uno strumento di progresso in un potenziale strumento di sorveglianza.

Le imprese private e le piattaforme tecnologiche non devono, dunque, essere demonizzate, piuttosto riconosciute come attori essenziali di un ecosistema complesso, nel quale pubblico e privato collaborano alla produzione di valore scientifico. Il loro apporto è determinante per integrare, standardizzare e armonizzare dati sanitari provenienti da fonti eterogenee, rendendoli disponibili per l'elaborazione algoritmica e la sperimentazione clinica. È *in re ipsa* che tale cooperazione impone l'adozione di presidi regolatori solidi, che garantiscano trasparenza, *accountability* e tracciabilità dell'intero processo di trattamento.

La disponibilità crescente di dati anonimizzati consente, inoltre, di perseguire obiettivi di sostenibilità economica del sistema sanitario, attraverso una programmazione fondata su evidenze reali ed una gestione oculata delle risorse. La possibilità di anticipare bisogni clinici, evitare sprechi e migliorare l'efficacia degli interventi è strettamente legata alla qualità e quantità dei dati disponibili, ed alla loro corretta utilizzazione. In tal senso, la valorizzazione del dato diventa leva di razionalizzazione e giustizia allocativa.

Secondo le stime più recenti, il mercato dei dati sanitari è destinato a raggiungere valori significativi nei prossimi anni, con un impatto crescente sul PIL delle economie avanzate. In tale contesto, l'Italia, forte di un sistema sanitario universalistico e di

un vasto patrimonio informativo, può aspirare ad un ruolo da protagonista. Per farlo, tuttavia, è necessario uno sforzo di coordinamento istituzionale, capace di promuovere sinergie tra ricerca pubblica e iniziativa privata, nonché di attrarre investimenti eticamente sostenibili in settori strategici della medicina del futuro.

Tale evoluzione richiede, fatalmente un aggiornamento del quadro giuridico, non solo in termini di adeguamento normativo, ma anche sul piano concettuale. Occorre abbandonare l'approccio difensivo, incentrato su logiche meramente limitative, per adottare una visione proattiva che riconosca esplicitamente il valore economico-sociale del dato. In questo contesto, la transizione da una titolarità soggettiva assoluta verso un interesse legittimo a contenuto collettivo si presenta come una soluzione giuridicamente fondata e moralmente doverosa.

L'analisi delle dinamiche di mercato mostra un'espansione costante del settore della sanità digitale, sostenuta da normative europee come l'EHDS e da iniziative nazionali tese ad incentivare la valorizzazione del dato. Questo scenario di grande fermento espone però a rischi tangibili: tra essi, la gestione opaca del consenso, la perdita di controllo da parte dell'interessato, la profilazione algoritmica e l'utilizzo non autorizzato delle informazioni per finalità diverse da quelle originarie. Si tratta di *pericula in mora*, che impongono l'adozione di misure rigorose di vigilanza, informazione e controllo.

Il mercato si articola in filiere complesse: assicurazioni, industria farmaceutica, ricerca clinica e *health tech* rappresentano ambiti ad altissima intensità informativa, e in particolare, il comparto assicurativo evidenzia una crescente domanda di dati per la personalizzazione delle polizze, tramite algoritmi capaci di calcolare il rischio individuale sulla base di parametri biometrici e comportamentali tipizzati¹². Pur se funzionale ad una maggiore equità, tale pratica espone, altresì, ad evidenti rischi di discriminazione sanitaria e selezione avversa, soprattutto nei confronti dei soggetti fragili. Si pone quindi l'esigenza di un presidio regolativo che impedisca derive escludenti e garantisca il rispetto del principio di uguaglianza sostanziale.

Analogamente, il settore farmaceutico e biotecnologico fa sempre più affidamento su database clinici anonimizzati, indispensabili per velocizzare sperimentazioni e approvazioni. La riduzione dei costi e dei tempi di accesso al mercato è, in questo caso, il riflesso di una nuova metodologia, *data-driven* e flessibile. Tuttavia, qualora l'anonimizzazione risulti imperfetta o le finalità dichiarate vengano aggirate, si rischia una sostanziale elusione dei diritti dell'interessato. Il principio di finalità, sancito dal GDPR, deve essere il *punctum pruriens* di ogni valutazione giuridica sull'uso dei dati sanitari in ambito industriale.

L'impiego a fini statistici e scientifici, pur promosso dalle politiche europee, solleva questioni di controllo democratico e trasparenza. La progressiva centralizzazione

¹² E. BATTELLI, *Big data e algoritmi predittivi nel settore assicurativo: vantaggi e rischi*, in *Il Corriere giuridico*, 12, 2019, p. 1517 ss.

dei dati, se non adeguatamente presidiata, può trasformarsi in uno strumento opaco di concentrazione informativa, sottraendo al cittadino il potere effettivo di disporre del proprio patrimonio digitale. Il rischio di una deriva panottica, seppur latente, impone l'adozione di misure di controllo multilivello, ispirate a principi di legalità, proporzionalità e partecipazione informata.

In tale quadro, il diritto è chiamato a svolgere una funzione regolativa di alto profilo, che superi l'ottica emergenziale e si traduca in un disegno normativo compiuto. Il GDPR, pur rappresentando un riferimento imprescindibile, non basta più: occorrono discipline settoriali specifiche, capaci di delineare confini netti tra uso legittimo e abuso, nonché di costruire un nuovo equilibrio tra interesse generale alla salute pubblica e tutela dei diritti individuali. Il rapporto tra pubblico e privato deve essere ridefinito in chiave cooperativa, ma senza rinunciare a un presidio pubblico forte e autorevole.

Un modello virtuoso passa, inevitabilmente, attraverso la responsabilità sociale d'impresa. Le imprese devono farsi carico di un'etica della trasparenza, dell'equità algoritmica e della tracciabilità. Il principio di *accountability*, inteso come dovere di rendicontazione sostanziale, deve diventare l'asse portante di ogni intervento normativo e operativo. Strumenti come gli audit indipendenti, le certificazioni di conformità e i codici di condotta assumono, in tale ottica, un ruolo sistemico.

Ultimo, ma non per importanza, è il ruolo della cittadinanza informata. Un'effettiva emancipazione digitale richiede campagne educative, strumenti semplici di gestione del consenso e una nuova cultura della protezione dei dati¹³. Il cittadino deve poter esercitare una signoria informativa effettiva, consapevole e non subordinata a meri formalismi.

In conclusione, il mercato dei dati sanitari costituisce una delle prove più complesse del diritto contemporaneo. Il compito dell'interprete è quello di costruire, passo dopo passo, un ordinamento capace di integrare innovazione e diritti, efficienza e dignità, progresso tecnologico e solidarietà. Solo attraverso una rinnovata architettura regolativa, radicata nella Costituzione ma contemporaneamente aperta al futuro, sarà possibile trasformare il dato sanitario in uno spazio di libertà, conoscenza e giustizia condivisa.

¹³ C. IRTI, *Consenso negoziato e circolazione dei dati personali*, Torino, Giappichelli, 2021, pp. 50-56.