LA BLOCKCHAIN NELLA SANITÀ DIGITALE*:* IL GOVERNO DELL'INNOVAZIONE SANITARIA TRA IMMUTABILITÀ TECNICA E DIRITTI DELLA PERSONA

Gianluca Attademo[*], Ilaria Amelia Caggiano[**], Christiancarmine Esposito[***]

SOMMARIO: 1.- Introduzione - Autodeterminazione e paradigma "blockchain" in sanità; 2.-Nuove regole per l'Intelligenza Artificiale: le indicazioni europee e le raccomandazioni italiane; 3.- La responsabilità civile per i danni cagionati da sistemi di Intelligenza Artificiale ad applicazione medica; 4.- Architetture della sovranità: il modello paziente-centrico; 5.- La filiera del bene pubblico: il caso studio "BloodChain"; 6.- Il trilemma della ricerca: "big data", "data harms" e risposte della "blockchain"; 7.- Proprietà e partecipazione: la condivisione dei dati genomici; 8.- Il fattore umano: limiti sociali e organizzativi all'innovazione tecnologica; 9.- Progettare la responsabilità: principi per una "blockchain" etica in sanità; 10.- Conclusioni. La "costituzionalizzazione" della "blockchain" come governo dell'innovazione.

1.- **Introduzione - Autodeterminazione e paradigma "blockchain" in sanità.**

La trasformazione digitale del settore sanitario, accelerata dalla diffusione dell'intelligenza artificiale e dall'impiego dei "big data", impone un difficile bilanciamento tra l'efficienza tecno-scientifica e la tutela dei diritti fondamentali della persona. Tale innovazione pone al centro del dibattito giuridico ed etico-filosofico il principio di autodeterminazione informativa, inteso come diritto fondamentale dell'individuo a disporre liberamente delle proprie informazioni personali. Questa nozione, già delineata dalla giurisprudenza costituzionale tedesca con la celebre sentenza del Bundesverfassungsgericht del 1983 sul "censimento di massa" (Volkszählungsurteil), è stata progressivamente recepita nell'ordinamento europeo, trovando infine compiuta espressione nel Regolamento (UE) 2016/679 (GDPR). Tale principio, tuttavia, nel contesto digitale contemporaneo, si configura come una facoltà complessa che implicherebbe la possibilità di conoscere, controllare e indirizzare i flussi informativi che riguardano la persona. Sono proprio le logiche operative delle nuove tecnologie a complicare questo paradigma tradizionale. Tecniche di "machine learning" e "deep learning" operano infatti su vasti insiemi di dati eterogenei, spesso al di fuori della sfera di consapevolezza dell'interessato, ampliando il rischio di profilazione occulta e di inferenze non desiderate. L'impiego di algoritmi predittivi comporta la generazione di nuovi dati per inferenza, con un impatto diretto sulla libertà e sulla costruzione identitaria del soggetto. In assenza di adeguati presidi di trasparenza e "explainability", l'esercizio del diritto all'autodeterminazione rischia di ridursi a una finzione giuridica, poiché l'interessato non è posto nelle condizioni di comprendere effettivamente né le logiche né le finalità del trattamento.

La centralità del principio di autodeterminazione informativa non esaurisce le problematiche poste dalle tecnologie di intelligenza artificiale e dall'economia dei "big data" nell'ambito sanitario. Emergono infatti rilevanti questioni etiche e giuridiche, che riguardano gli effetti delle decisioni algoritmiche sui diritti e la vita delle persone.

[*]Gianluca Attademo è Assegnista di Ricerca presso il Dipartimento di Informatica dell'Università degli Studi di Salerno.
[**] Christiancarmine Esposito è Professore Associato presso il Dipartimento di Informatica dell'Università degli Studi di Salerno.
[***] Ilaria Amelia Caggiano è Professore Ordinario presso l'Università degli Studi Suor Orsola Benincasa.

Anzitutto, si pongono problemi di discriminazione, giustizia distributiva e di equità dato che gli algoritmi di "machine learning" apprendono da basi dati che riflettono pregiudizi, discriminazioni e squilibri presenti nella società; di conseguenza, il rischio è che l'IA amplifichi "bias" sistemici, incidendo in modo sproporzionato su categorie vulnerabili. In tale prospettiva, appare necessaria un'etica della responsabilità algoritmica. In secondo luogo, l'opacità delle logiche decisionali dei sistemi di IA solleva questioni legate al principio di trasparenza e alla spiegabilità delle decisioni. Ciò richiama l'esigenza etica, oltre che giuridica, di garantire la comprensibilità e l'auditabilità degli algoritmi.

Infine, si evidenzia il problema della responsabilità: in scenari caratterizzati da processi decisionali automatizzati, è spesso arduo stabilire chi sia effettivamente responsabile di una violazione dei diritti o di un danno arrecato. Da più parti è stata sollevata l'esigenza di ripensare i modelli di "accountability", prevedendo forme di responsabilità condivisa e multilivello che riflettano la complessità delle filiere tecnologiche.

La governance di questi processi, con riguardo ai dati sanitari, fa emergere la tensione tra l'esigenza di garantire a ogni individuo la sovranità sul proprio "corpo elettronico", su quella proiezione digitale di sé costituita dal flusso incessante di dati personali[1] accanto alla valorizzazione dei dati sanitari, che è un obiettivo strategico, sia in termini di miglioramento dell'assistenza clinica, sia come risorsa per la ricerca scientifica e l'innovazione. La dottrina ha più volte sottolineato come l'utilizzo secondario dei dati sanitari[2], se ben regolato, rappresenti un potente strumento per lo sviluppo di politiche di sanità pubblica basate sull'evidenza, per la medicina personalizzata e per la prevenzione. Tuttavia, questa prospettiva pone problematiche giuridiche ed etiche. Sul piano giuridico, vi è il rispetto i principi del GDPR in tema dati particolari, relativi alla salute. Ciò significa che ogni processo di raccolta, analisi e riuso dei dati deve avere una base giuridica (art. 9 GDPR, tra le quali vi è il consenso informato) ed essere accompagnato da garanzie stringenti di trasparenza, minimizzazione e tracciabilità (art. 5 GDPR). Sul piano etico, la questione riguarda il rischio di un'asimmetria di potere tra i soggetti che generano i dati (i pazienti) e coloro che li utilizzano (istituzioni, aziende farmaceutiche, piattaforme tecnologiche).

La questione è anche di politica sanitaria: la fiducia del cittadino nel sistema sanitario dipende in larga misura dalla percezione di controllo sul proprio dato e dalla garanzia che l'uso a fini collettivi non comprometta la tutela individuale. Inoltre, i dati sanitari, se aggregati e gestiti in grandi piattaforme di *data sharing*, pongono problemi di equità e non discriminazione: algoritmi di IA mal calibrati possono infatti generare bias clinici, con conseguenze dirette sulla qualità delle cure erogate. In questa prospettiva, la valorizzazione dei dati sanitari non può essere intesa in termini meramente economici o tecnologici, ma deve essere accompagnata da una cornice etico-giuridica che ne orienti l'uso verso finalità di interesse generale, garantendo al contempo il rispetto della dignità e dei diritti fondamentali della persona.

Ciò richiede un equilibrio dinamico tra tre poli: utilità collettiva, tutela individuale e responsabilità etica, secondo un approccio che si sta consolidando sia nella dottrina bio-giuridica sia nelle più recenti iniziative normative europee (EHDS, AI Act). Nella condizione "onlife"[3] è la stessa salute degli individui a costituire a sua volta un fenomeno informazionale. I sistemi sanitari tradizionali, per molti

[1] Cfr. S. Rodotà, *Il diritto di avere diritti*, Roma-Bari 2012.
[2] Cfr. F. Cascini, Secondary Use of Electronic Health Data, Cham 2025.
[3] Cfr. L. Floridi (cur.), The Onlife Manifesto: Being Human in a Hyperconnected Era, Cham 2015.

versi, risultano strutturalmente inadeguati a governare questa nuova realtà. Edificati su architetture centralizzate, caratterizzati da frammentazione in silos proprietari, scarsa interoperabilità e una cronica opacità gestionale, perpetuano, secondo diversi interpreti[4], un modello paternalistico che espropria il paziente della sovranità sui propri dati, i quali vengono identificati non come un bene personale da custodire fiduciariamente, ma come un asset strategico e finanziario da controllare.

In questo quadro, la "blockchain" è stata proposta come infrastruttura innovativa per la gestione dei dati sanitari, poiché consente di registrare le transazioni in maniera immutabile e verificabile, garantendo tracciabilità e resistenza a manomissioni. Essa può sollecitare una ridefinizione paradigmatica della gestione dei dati.

Sul piano giuridico, la "blockchain" può rappresentare uno strumento idoneo a rafforzare il principio di autodeterminazione informativa. Attraverso meccanismi di consenso distribuito e l'impiego di "smart contracts", si cerca di garantire che il paziente eserciti un controllo effettivo sull'accesso ai propri dati, definendo chi può consultarli, per quali finalità e per quanto tempo. Ciò appare in linea con le garanzie previste dal GDPR, in particolare con i principi di "accountability", "privacy by design" e "by default".

Tuttavia, emergono numerosi chiaroscuri: l'immutabilità della "blockchain" può confliggere con diritti come la rettifica e la cancellazione (artt. 16 e 17 GDPR), richiedendo soluzioni tecniche ibride (ad es. "off-chain storage" con "hash" su "blockchain"). Dal punto di vista della valorizzazione dei dati sanitari, la "blockchain" può abilitare modelli di *data sharing* fiduciario: i dati restano sotto il controllo dell'individuo, ma possono essere condivisi in forma sicura per finalità di ricerca, innovazione e sanità pubblica, riducendo i rischi di usi impropri. In questo senso, la "blockchain" può costituire una tecnologia "abilitante" per rafforzare la fiducia sociale nell'uso secondario dei dati, tracciando in modo verificabile chi ha avuto accesso ai dati e a quale scopo[5]. Ancora, l'adozione della "blockchain" può generare nuove forme di asimmetria digitale, penalizzando soggetti meno alfabetizzati sul piano tecnologico. Inoltre, il decentramento delle responsabilità tipico delle reti "blockchain" pone una complessa sfida in termini di *accountability*, rendendo ardua l'attribuzione della responsabilità giuridica per un eventuale trattamento illecito in un sistema distribuito. Infine, vi è il rischio che l'uso della "blockchain" venga percepito come una "tecnologia salvifica", senza adeguata valutazione dei suoi limiti, come la scalabilità o l'impatto ambientale delle soluzioni "proof-of-work". Per questi motivi, numerosi autori hanno evidenziato come non si tratti semplicemente di una tecnologia, quanto di un'architettura sociotecnica e normativa che incarna una differente filosofia della fiducia, della governance e della "stewardship" del dato[6]. In tale architettura sostituendo l'autorità centrale garante con un sistema di validazione distribuita, crittograficamente sicura e

[4] Cfr. J. Bautista, M. Usman, D. Harrell, E. Meyer, A. Khurshid, Clinical, organizational and regulatory, and ethical and social (CORES) issues and recommendations on "blockchain" deployment for healthcare: Evidence from experts, in"blockchain" in Healthcare Today 5 (2022) 1-14.

[5] Cfr. G. Rubeis, Ethical implications of "blockchain" technology in biomedical research, in Ethik in der Medizin 36 (2024) 493-506.

[6] Cfr. M. Wong, K. Yee, C. Nohr, Socio-technical consideration for "blockchain" technology in healthcare: the technological innovation needs clinical transformation to achieve the outcome of improving quality and safety of patient care, in Studies in health technology and informatics 247 (2018) 636-640; vedi anche M. Shabani,"blockchain"-based platforms for genomic data sharing: A de-centralized approach in response to the governance problems?, in J. Am. Med. Inform. Assoc. 26.1 (2019) 76-80.

consensuale, la "blockchain" offrirebbe la promessa di un ecosistema informativo nel quale la trasparenza e l'immutabilità emergono quali proprietà intrinseche del sistema stesso.
Il presente contributo si propone di analizzare come l'introduzione della tecnologia "blockchain" nel settore sanitario determini un'articolata ed ampia riflessione etico-giuridica. La rassegna di dottrina in esso contenuta evidenzia come, lungi dall'offrire una soluzione tecnica neutrale, l'adozione di tale tecnologia può innescare tensioni con i principi fondamentali dell'ordinamento. Il punto cruciale che si intende evidenziare è che l'utilizzo della "blockchain" in ambito sanitario possa valorizzare il controllo del paziente sui propri dati sanitari ma allo stesso tempo vada confrontato con la garanzia dei diritti fondamentali del paziente e il rischio di nuove forme di esclusione sociale[7].
Il saggio traccerà una mappa del confronto tra queste implicazioni: dopo un'analisi dei fondamenti della tecnologia, verranno discussi criticamente i modelli applicativi, evidenziando l'impatto dell'immutabilità della catena sui diritti alla cancellazione e rettifica sanciti dal GDPR. Successivamente, l'attenzione si sposterà sulle sfide sociotecniche, come il divario digitale, per poi esaminare alcuni snodi della risposta regolatoria europea. Si argomenterà, infine, come la realizzazione di un ecosistema sanitario rispondente ai principi e valori fondamentali dell'ordinamento dipenda dalla capacità di integrare sin dalla progettazione ("by design") presìdi di tutela per la persona in un processo di continua negoziazione tra innovazione e valori democratici.

2.- **Fondamenti della tecnologia "blockchain".**

Per cogliere le implicazioni etico-filosofiche e giuridiche della "blockchain", è imprescindibile una disamina delle sue fondamenta tecniche. Una piattaforma "blockchain" realizza un'istanza delle cosiddette "Distributed Ledger Technologies" (DLT), ovvero sistemi basati su un registro distribuito e condiviso tra i nodi di una rete "peer-to-peer". Nello specifico, le DLT rappresentano l'evoluzione contemporanea di un istituto antico: il registro delle transazioni. Già nel Medioevo, le banche mercantili italiane si servivano di registri per annotare crediti, debiti e movimenti finanziari, garantendo continuità e affidabilità ai rapporti economici. Tali registri, spesso redatti con tecniche di doppia scrittura, costituivano strumenti di certezza giuridica, poiché erano considerati prova documentale delle transazioni nei tribunali mercantili e nelle corti cittadine. La DLT riprende questa logica di fondo, ma la trasforma radicalmente grazie alla tecnologia: il registro non è più custodito centralmente da un banchiere o da un notaio, bensì distribuito tra più nodi della rete, ciascuno dei quali conserva una copia sincronizzata e validata mediante algoritmi di consenso. In questo modo, l'affidabilità del registro non deriva più dalla reputazione di un singolo custode, ma dalla struttura stessa del sistema distribuito, che rende estremamente difficile la falsificazione o la manipolazione unilaterale delle scritture. Questa continuità/discontinuità storica evidenzia il carattere ibrido delle DLT: da un lato, esse rappresentano la prosecuzione di una funzione giuridico-economica millenaria (la registrazione certa delle transazioni), dall'altro, introducono elementi dirompenti che ridisegnano le categorie classiche del diritto della prova, della responsabilità e della circolazione dei beni. In particolare, la immutabilità delle scritture distribuite richiama l'antica funzione probatoria dei registri bancari medievali, ma la potenzia fino a sollevare questioni di compatibilità con i diritti fondamentali moderni (ad es. diritto all'oblio o alla rettifica dei dati). Si realizza sulla base della fiducia tecnologica

[7] Cfr. P. De Filippi, A. Wright, *"blockchain" and the Law: The Rule of Code*, Harvard University Press, Cambridge (MA) 2018.

e algoritmica, fondata su crittografia, consenso distribuito e immutabilità delle registrazioni. Inoltre, la decentralizzazione rompe il legame tradizionale tra registro e autorità, ponendo nuove sfide per la regolazione e la governance giuridica.

Questa architettura distribuita rappresenta il primo pilastro: eliminare i singoli punti di fallimento ("single points of failure") e di controllo, creando un sistema intrinsecamente resiliente e democratico[8]. Le informazioni sono raggruppate in "blocchi" che, una volta validati, vengono aggiunti alla catena. Ogni blocco contiene un marcatore temporale e, soprattutto, un hash crittografico del blocco che lo precede. L'*hash* è l'impronta digitale del blocco; collegando ogni nuovo blocco all'impronta del precedente, si crea una catena retroattivamente sigillata. Questa struttura rende il registro "append-only" (si possono solo aggiungere nuovi dati) e immutabile: la modifica di un blocco pregresso altererebbe il suo "hash", invalidando a cascata l'intera catena successiva e rendendo la manomissione palese e rigettata dalla rete. La validazione di nuovi blocchi è, a sua volta, affidata a un algoritmo di consenso. Il meccanismo originario, la "Proof-of-Work", pur garantendo un'elevatissima sicurezza nelle reti pubbliche e anonime come Bitcoin, comporta un significativo dispendio energetico e limita la velocità delle transazioni, sollevando questioni etiche di sostenibilità che un'etica dell'innovazione, come quella proposta, tra gli altri, dal filosofo Luciano Floridi, non può ignorare[9].

Nel settore sanitario, si privilegiano le "blockchain" private o "permissioned": in queste reti, l'accesso è riservato a partecipanti noti e autorizzati (es. ospedali, laboratori, pazienti), la cui identità è verificata. Ciò permette di utilizzare algoritmi di consenso più efficienti (es. "Byzantine Fault Tolerance" - BFT), che si basano sulla fiducia governata tra un numero definito di attori, e garantisce un livello di accountability impossibile nelle reti anonime. La scelta di un'architettura "permissioned" è, dunque, una scelta giuridica prima ancora che tecnica, in quanto risponde alla necessità di identificare chiaramente i soggetti responsabili del trattamento dei dati.

L'elemento che trasforma la "blockchain" da semplice database a piattaforma per la governance è lo "smart contract". Definito come un programma auto-eseguibile che traspone in codice le clausole di un accordo[10], esso si attiva autonomamente al verificarsi di condizioni predefinite (es. "se il paziente firma digitalmente il consenso, allora concedi l'accesso al dato X al medico Y per 24 ore"). Questa capacità di automatizzare regole e consensi senza intermediari si pone come la chiave di volta per la realizzazione tecnica di un sistema che contemperi i principi dell'autodeterminazione, trasformando il consenso da un atto burocratico a un processo dinamico e granulare. Lo "smart contract" rappresenterebbe un 'assioma algoritmico' che, se da un lato promette oggettività e imparzialità, dall'altro solleva interrogativi sulla sua rigidità e sulla gestione degli errori, problemi centrali anche nell'etica dell'intelligenza artificiale.

3.- **Scenari di utilizzo della "blockchain" in ambito sanitario.**

Le proprietà uniche della "blockchain" stanno trovando applicazione in un'ampia gamma di applicazioni teoriche e sperimentali volte a risolvere alcune delle più annose problematiche del settore

[8] Cfr. Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, *"Blockchain" challenges and opportunities: A survey*, in *International Journal of Web and Grid Services* 14.4 (2018) 352-375.

[9] L. Floridi, *Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide*, Milano 2022.

[10] Cfr. W. Zou, D. Lo, P. Kochhar, X. Le, X. Xia, Y. Feng, Z. Chen, B. Xu, *Smart contract development: Challenges and opportunities*, in *IEEE Transactions on Software Engineering* 47.10 (2019) 2084-2106.

sanitario. Ciascuna di queste applicazioni, al di là del suo valore tecnico, solleva interrogativi di governance locale e globale dei dati in particolare per quanto riguarda l'inedito grado di controllo sui dati che verrebbe restituito ai pazienti[11].

La gestione delle Cartelle Cliniche Elettroniche (EHRs) è sicuramente tra gli ambiti più discussi. I modelli attuali presentano di regola una "balcanizzazione" dell'informazione sanitaria: i dati degli individui sono conservati in una moltitudine di database proprietari, non comunicanti tra loro, appartenenti a ospedali, medici di base, laboratori e specialisti. Questa frammentazione non è solo una fonte di inefficienza, può costituire un limite alla continuità della cura e alla sicurezza del paziente. La "blockchain" potrebbe operare come coordinamento e di controllo degli accessi distribuito. In questo modello, i dati clinici potrebbero rimanere fisicamente dove si trovano (nei sistemi degli ospedali, dei laboratori, ecc.), ma la "blockchain" fungerebbe da "master index" immutabile e controllato dal paziente. Ogni record sanitario viene referenziato sulla catena tramite un puntatore crittografico e il paziente, attraverso la propria identità digitale e la propria chiave privata, diventa, a seconda dei modelli, l'unico soggetto in grado di autorizzare l'accesso a questi puntatori. Uno "smart contract" potrebbe, dunque, ad esempio, concedere a un medico specialista l'autorizzazione a "vedere" e aggregare i referti provenienti da tre diverse istituzioni per la durata di una singola consultazione. In questo modo, il paziente potrebbe esercitare un controllo effettivamente 'granulare', revocabile e completamente tracciabile, realizzando una forma concreta di sovranità sul proprio "corpo elettronico". La filiera farmaceutica rappresenta un ulteriore settore di impatto cruciale, dove la trasparenza si traduce direttamente in sicurezza per la vita umana. La circolazione di farmaci contraffatti è, infatti, una piaga globale che causa innumerevoli decessi e mina la fiducia nei sistemi sanitari. La "blockchain" offre, in questo scenario, la concreta possibilità di creare una "catena di custodia" digitale ed inviolabile per ogni singola confezione di farmaco. Dal momento in cui un lotto venisse prodotto, ogni spostamento e passaggio di mano – dal produttore al grossista, dal distributore alla farmacia – verrebbe registrato come una transazione immutabile sulla catena. Ogni singolo attore della filiera, scansionando un codice univoco sulla confezione, potrebbe verificare in tempo reale l'intera storia del prodotto, confermandone l'autenticità. Questo meccanismo non solo rappresenterebbe un'importante misura contro la contraffazione, ma potrebbe al contempo garantire altri aspetti di integrità come per la catena del freddo o il rapido ritiro dal mercato in caso di problemi. La 'fiducia' cambia forma, non è più (solo) riposta nella dichiarazione di un intermediario, ma diventa verificabile matematicamente grazie al registro distribuito.

Anche nell'ambito della ricerca clinica, la tecnologia "blockchain" può agire come un potente garante dell'integrità scientifica e dei diritti dei partecipanti. La cosiddetta "crisi di riproducibilità" che affligge molti settori della scienza è spesso legata a una gestione opaca dei dati e dei protocolli di ricerca[12]. La "blockchain" in questo scenario potrebbe essere impiegata per creare un registro immutabile e marcatempo di ogni fase di una sperimentazione clinica: dalla registrazione del protocollo iniziale, al consenso informato dei partecipanti, alla raccolta dei dati grezzi, fino all'analisi statistica e alla pubblicazione dei risultati. Qualsiasi modifica o tentativo di manipolazione a posteriori risulterebbe immediatamente tracciabile. In questo modo non solo aumenterebbe la robustezza e la credibilità dei risultati scientifici, ma sarebbe rafforzata la stessa tutela dei

[11] Cfr M. Hölbl, M. Kompara, A. Kamišalić, L. Nemec Zlatolas, *A systematic review of the use of blockchain in healthcare*, in Symmetry 10.10 (2018) 470.
[12] Rubeis, *Ethical* cit. 500.

partecipanti, grazie ad una gestione 'dinamica' del consenso ed alle metodiche di pseudonimizzazione garantite dalla piattaforma.

Infine, la "blockchain" viene proposta come l'infrastruttura ideale per una gestione sicura dell'identità digitale dei pazienti e per articolare il consenso informato in un insieme di regole operativamente efficaci, giuridicamente vincolanti e immutabilmente verificabili. Superando il modello obsoleto di un'identità frammentata e controllata da terzi, la "blockchain" guarda alla creazione di identità digitali sovrane ("Self-Sovereign Identity"), in cui l'individuo è l'unico custode delle proprie credenziali[13]. In questo modello puramente teorico il paziente potrebbe interagire con un qualsiasi fornitore di servizi tramite un'identità digitale verificabile che non dovrebbe dipendere da un'autorità centrale. Su questa base, gli "smart contracts" potrebbero trasformare il consenso da un documento cartaceo statico, firmato una volta e poi archiviato, in un processo vivo e granulare. Il paziente, potrebbe, ad esempio, autorizzare l'uso dei propri dati anonimizzati per un progetto di ricerca specifico, ponendo condizioni precise (es. solo per la ricerca sul diabete, per un periodo di due anni, escludendo l'uso da parte di aziende private), con la certezza che lo "smart contract" ne garantisca l'applicazione e con la possibilità di revocare tale consenso in qualsiasi momento, lasciando una traccia indelebile della propria decisione.

L'espansione dei servizi digitali basati su "blockchain" e "distributed ledger" solleva, inoltre, complesse questioni di giurisdizione e competenza regolatoria, in particolare quando le società presentano una struttura organizzativa transnazionale. Guardtime, registrata in Svizzera, con sede operativa principale in Estonia e attiva anche nel Regno Unito, offre un esempio paradigmatico[14] delle tensioni che si creano tra diritto societario, diritto della protezione dei dati e regolamentazione delle tecnologie emergenti. In primis, la registrazione in Svizzera implica che, sotto il profilo del diritto societario e della personalità giuridica, Guardtime sia soggetta alla legislazione elvetica e alla vigilanza delle autorità svizzere competenti (ad esempio, l'Handelsregister e, per specifici settori, l'Autorità federale di vigilanza sui mercati finanziari – FINMA). Pertanto, questioni come la governance societaria, gli obblighi contabili e la responsabilità degli amministratori ricadono in prima battuta nell'ordinamento svizzero. La presenza di una sede operativa in Estonia rileva ai fini dell'applicazione del diritto estone, in particolare per quanto attiene agli obblighi fiscali, al diritto del lavoro e alle normative settoriali in materia di sicurezza informatica e protezione dei dati. Inoltre, l'Estonia, in quanto Stato membro dell'UE, assoggetta Guardtime al rispetto del GDPR per i trattamenti di dati personali effettuati nell'Unione. Le autorità competenti in questo caso sono l'Estonian Data Protection Inspectorate e, per attività trasfrontaliere, il Comitato europeo per la protezione dei dati (EDPB) attraverso il meccanismo di one-stop-shop. Infine, l'operatività nel Regno Unito introduce un ulteriore livello di complessità. Dopo il Brexit, il Regno Unito ha adottato l'UK GDPR, che ricalca il GDPR europeo ma sotto la supervisione dell'Information Commissioner's Office (ICO). Pertanto, per i trattamenti di dati effettuati nel Regno Unito o rivolti a interessati britannici, Guardtime deve rispettare la normativa locale ed è soggetta alla vigilanza dell'ICO. Questo intreccio produce un conflitto potenziale di giurisdizioni, e l'esistenza di più fori competenti comporta che eventuali controversie (ad es. "data breach", violazioni contrattuali o responsabilità in materia di

[13] F. Wang, P. De Filippi, Self-sovereign identity in a globalized world: Credentials-based identity systems as a driver for economic inclusion, in Frontiers in blockchain 2 (2020) 28.

[14] Cfr. M. Mettler, Blockchain technology in healthcare: The revolution starts here, in 2016 IEEE 18th international conference on e-health networking, applications and services (Healthcom), Munich 2016.

"blockchain" sanitaria) possano essere oggetto di diverse pretese giurisdizionali. La determinazione dell'autorità competente dipende quindi da criteri di collegamento: il luogo di stabilimento, il mercato di riferimento degli interessati, la legge scelta contrattualmente, nonché le regole europee e internazionali di diritto internazionale privato (Reg. Bruxelles I-bis nell'UE; Convenzione di Lugano con la Svizzera). Il caso Guardtime dimostra che, in contesti tecnologici transnazionali, non esiste un'unica autorità di riferimento. Al contrario, si delinea una pluralità di competenze parallele: l'autorità societaria svizzera, l'autorità di protezione dei dati estone (coordinata a livello UE), e l'ICO britannico. Ciò impone alle imprese di adottare un approccio di compliance multilivello, in grado di integrare i diversi regimi giuridici, anticipando possibili conflitti normativi e riducendo il rischio di "forum shopping" o di esposizione a sanzioni in più ordinamenti.

L'impiego della "blockchain" nella gestione e valorizzazione dei dati sanitari solleva questioni inedite di proprietà intellettuale (IP) e di responsabilità ("liability"), che si intrecciano con i principi di autodeterminazione informativa, trasparenza e tutela della persona. L'adozione di soluzioni "blockchain" in sanità implica la registrazione, la condivisione e l'elaborazione di dati clinici, spesso aggregati a fini di ricerca o innovazione. Ciò genera tre ordini di problematiche. In primis, riguardo la titolarità dei dati e delle informazioni: benché i dati sanitari non siano qualificabili come "proprietà" in senso civilistico, il loro utilizzo secondario può implicare conflitti tra diritti del paziente, diritti del titolare del trattamento (ospedali, centri di ricerca) e interessi commerciali di soggetti terzi (industria farmaceutica, piattaforme tecnologiche). La "blockchain", garantendo tracciabilità e immutabilità, rafforza la prova delle operazioni, ma non risolve la questione della titolarità giuridica del dato. Inoltre, sussistono i diritti di proprietà intellettuale sul software e sugli "smart contracts": le piattaforme "blockchain" in sanità si fondano su codici sorgente, protocolli e "smart contracts", suscettibili di tutela brevettuale o autoriale. Sorge quindi il problema della compatibilità tra un'infrastruttura "open source" (tipica di molte "blockchain") e la protezione IP rivendicata da sviluppatori o fornitori privati. Infine, ci sono innovazioni derivate dai dati: i risultati della ricerca condotta su dati sanitari condivisi tramite "blockchain" (ad es. nuovi algoritmi diagnostici, farmaci personalizzati) pongono il problema della ripartizione dei diritti IP tra pazienti, ricercatori, istituzioni sanitarie e imprese. In questo contesto, la "blockchain" può fungere da registro probatorio per stabilire priorità e contributi, ma non elimina le tensioni sui diritti di sfruttamento economico. Il tema della responsabilità assume una rilevanza cruciale nei sistemi "blockchain" applicati alla sanità, a causa della natura decentralizzata delle reti e della delicatezza dei beni giuridici coinvolti (la salute e i dati personali). Il primo problema è la responsabilità per malfunzionamenti tecnologici: un errore nello "smart contract" che gestisce consensi sanitari, oppure un bug nella piattaforma "blockchain", può determinare trattamenti illeciti di dati o bloccare l'accesso a informazioni vitali per la cura.

Il secondo problema è la responsabilità per "data breach" o usi impropri: sebbene la "blockchain" garantisca immutabilità, non è immune da violazioni di sicurezza (ad es. nelle interfacce "off-chain"). In caso di divulgazione indebita di dati sanitari, si applicano le regole del GDPR e del diritto civile, che richiedono l'individuazione di un titolare/responsabile del trattamento. La natura distribuita della "blockchain" rende difficile identificare un unico soggetto responsabile. L'ultimo problema riguarda la Liability 'diffusa' e l'"accountability": l'assenza di un'autorità centrale implica che la responsabilità possa dover essere ripartita lungo la filiera (sviluppatori, operatori sanitari, fornitori di servizi cloud, nodi della rete). Ciò sollecita un ripensamento dei modelli tradizionali di responsabilità, avvicinandoli a una logica di responsabilità collettiva o solidale, come già proposto nel dibattito

sull'AI Act e sulle tecnologie autonome. La "blockchain" in ambito sanitario offre strumenti promettenti per garantire trasparenza, tracciabilità e fiducia nell'uso dei dati. Tuttavia, i problemi legati alla proprietà intellettuale (sui dati, sugli algoritmi e sulle innovazioni derivate) e alla responsabilità civile (in caso di errori, violazioni o malfunzionamenti) mostrano come l'infrastruttura tecnologica, da sola, non basti a tutelare i diritti fondamentali. È necessaria una cornice giuridica multilivello, capace di chiarire la titolarità dei diritti e di stabilire regimi di responsabilità certi, bilanciando l'innovazione con la protezione della persona e con i principi etici di equità e giustizia.
Nel dibattito giuridico e tecnologico sull'uso della "blockchain" in sanità le ricerche seminali[15] di De Filippi e Wright hanno proposto la necessità di distinguere due piani concettuali complementari: la governance by "blockchain" e la governance of "blockchain". La governance "by blockchain" si riferisce all'impiego della tecnologia stessa come strumento di governo dei processi sanitari. In questa prospettiva, la "blockchain" non è soltanto un'infrastruttura tecnica, ma un meccanismo regolativo in grado di garantire tracciabilità, trasparenza e immutabilità nelle operazioni sui dati sanitari. Ad esempio, attraverso l'uso di "smart contracts", è possibile automatizzare la gestione dei consensi informati, assicurando che i dati di un paziente vengano utilizzati esclusivamente per le finalità autorizzate e con tempi di conservazione prestabiliti. Allo stesso modo, la "blockchain" può fungere da registro verificabile per la condivisione dei dati a fini di ricerca, consentendo al paziente di esercitare un controllo diretto e continuo, rafforzando così l'autodeterminazione informativa. In tal senso, la governance by "blockchain" introduce un modello di regolazione tecnologica che tradurrebbe i principi giuridici in regole auto-esecutive, riducendo i margini di discrezionalità e aumentando la fiducia degli utenti nel sistema. La governance "of blockchain", invece, riguarda il modo in cui la stessa infrastruttura tecnologica viene regolata, controllata e legittimata. Questo piano si concentra sulle regole di funzionamento della rete, sugli attori che partecipano al consenso distribuito e sulle modalità di gestione delle responsabilità. In ambito sanitario, ciò si traduce nella necessità di definire chi amministra la "blockchain", chi ha il potere di validare i blocchi, come vengono garantiti i requisiti di sicurezza e di conformità normativa (ad es. con il GDPR e l'EHDS) e quali siano i meccanismi di risoluzione delle controversie in caso di errore o malfunzionamento. A differenza della governance "by blockchain", qui non è la tecnologia che disciplina i processi sanitari, ma è l'insieme di norme giuridiche, policy istituzionali e decisioni organizzative che stabilisce come la "blockchain" deve essere progettata, implementata e utilizzata in un contesto sanitario. La distinzione tra "governance by" e "governance of blockchain" evidenzia una tensione cruciale: da un lato, la "blockchain" promette di rafforzare la fiducia nei processi sanitari rendendo automatico e verificabile il rispetto delle regole; dall'altro, la stessa tecnologia necessita di una cornice di governance esterna che ne garantisca la legittimità democratica, l'allineamento con i diritti fondamentali e la compatibilità con i sistemi sanitari nazionali ed europei.

4.- **Architetture della sovranità: il modello paziente-centrico.**

Duong-Trung, Le, Son e Phan intervengono nel dibattito contemporaneo sulla trasformazione dei sistemi sanitari, postulando la necessità di un ripensamento architetturale fondato su principi etico-

[15] De Filippi, Wright, *Blockchain* cit. 171ss.

giuridici di centralità del paziente[16]. La loro analisi parte dalla rilevazione di un cambiamento paradigmatico che sarebbe in corso: il passaggio da un modello di cura basato sul volume ("volume-based care"), in cui la remunerazione è proporzionale alla quantità di prestazioni erogate, a un modello basato sul valore ("value-based care"), che promuoverebbe una cura incentrata sul paziente e di qualità superiore[17]. Questo nuovo paradigma filosofico-giuridico implica una ridefinizione radicale del ruolo del paziente, che da destinatario passivo del processo di cura viene ad essere riconosciuto quale soggetto attivo e informato, pienamente coinvolto nel processo decisionale clinico. In un tale modello, il paziente acquisirebbe la facoltà di integrare nella propria anamnesi dati autoprodotti, come le misurazioni raccolte tramite dispositivi personali. La possibilità per il paziente di accedere a una visione completa e unificata della propria storia clinica costituirebbe dunque un antidoto essenziale alla frammentazione informativa e gli errori di coordinamento, migliorando conseguentemente la continuità e la qualità delle cure[18]. Si assiste, pertanto, ad un'evoluzione profonda verso un paradigma di sanità personalizzata, che si fonda sull'impiego congiunto di *big data*, intelligenza artificiale e biotecnologie al fine di adattare prevenzione, diagnosi e terapie alle caratteristiche uniche del singolo paziente. Mentre nel modello tradizionale vengono definiti protocolli uniformi per categorie generiche di pazienti, la medicina personalizzata mira ad integrare dati clinici, genomici, ambientali e comportamentali, con l'obiettivo di ottimizzare gli esiti clinici e ridurre effetti collaterali. La crescente valorizzazione dei dati sanitari, promossa a livello europeo grazie all'istituzione dell'European Health Data Space (EHDS)[19], sintetizza queste dinamiche che favoriscono l'uso primario e secondario dei dati per la cura individuale e per la ricerca scientifica.

L'istanza giuridica fondamentale che emerge da questa visione configura un diritto del paziente di controllare quando, a chi e quali dati sanitari vengono condivisi[20]. Tuttavia, l'intento degli autori è la messa in luce di una 'lacuna' nei sistemi sanitari attuali, i quali, appunto, non consentirebbero al paziente gli strumenti per modificare o revocare l'accesso ai propri dati da parte degli operatori sanitari. Di conseguenza, una volta che un dato venga acquisito, esso rimarrebbe teoricamente in possesso permanente del fornitore, che può condividerlo con altre organizzazioni senza un consenso esplicito e verificabile, in assenza di un meccanismo che vincoli o verifichi tali transazioni. Questa incontrollata diffusione dei dati attraverso molteplici siti e applicazioni, ciascuno con i propri standard di sicurezza, non fa che aumentare esponenzialmente il rischio di violazioni, un'eventualità che non solo presenta profili problematici sul piano etico, ma espone le istituzioni a severe conseguenze legali ed economiche.

La proposta di Duong-Trung e colleghi[21], dunque, è volta all'identificazione degli ostacoli strutturali alla realizzazione di un sistema sanitario interoperabile e genuinamente incentrato sul paziente. Il primo sarebbe costituito dalla sicurezza e la privacy delle informazioni: la necessità di condividere i

[16] N. Duong-Trung, H. Le, H. Son, T. Phan, Smart Care: Integrating blockchain technology into the design of patient-centered healthcare systems, in *Proceedings of the 2020 4th International Conference on Communication Software and Networks (ICCSP 2020)*, Nanjing 2020, 1-10.

[17] P. Zhang, D. Schmidt, J. White, G. Lenz, Blockchain technology use cases in healthcare, in Advances in Computers 111 (2018) 1-41.

[18] J. Ash, M. Berg, E. Coiera, Some unintended consequences of information technology in health care: The nature of patient care information system-related errors, in J. Am. Med. Inform. Assoc. 11.2 (2004) 104-112.

[19] J. S. Marcus, B. Martens, C. Carugati, A. Bucher, I. Godlovitch, *The European health data space*, Bruxelles 2022.

[20] G. Preite, L'habeas data sanitario come diritto all'autodeterminazione digitale del paziente, in Rivista elettronica di diritto, economia, management 3 (2014) 106.

[21] Duong-Trung et al., *Smart Care* cit. 7.

dati per garantire cure collaborative si scontra con il rischio di violazioni in assenza di un'infrastruttura altamente sicura. Il secondo ostacolo sarebbe rappresentato dalla mancanza di fiducia ("lack of trust") tra i diversi fornitori di servizi sanitari; questi ultimi necessitano, infatti, di meccanismi affidabili per identificare e fidarsi delle controparti prima di ogni comunicazione, un problema particolarmente acuto al di fuori di reti ospedaliere chiuse. Il terzo riguarderebbe principalmente la scalabilità, ovvero la difficoltà tecnica di condividere istantaneamente "dataset" di grandi dimensioni, come ad es. le immagini mediche, specialmente in contesti con limitazioni di banda o infrastrutturali. Per superare queste criticità tramite le potenzialità della tecnologia "blockchain" secondo gli autori, in dialogo con Wong, Yee e Nohr[22] sarebbe, pertanto, necessario il passaggio concettuale da un focus sull'informazione a un focus sul valore e sulla fiducia.

Da questa svolta fondamentale procede il sistema presentato nel saggio 'Smart Care: Integrating blockchain Technology into the Design of Patient-centered Healthcare Systems' del 2020[23]. "Smart Care" è un'architettura che utilizza la tecnologia "blockchain" e gli "smart contracts" per realizzare un modello sanitario autenticamente paziente-centrico. Il sistema è stato progettato attorno a cinque gruppi di utenti con ruoli e permessi rigorosamente definiti: pazienti, medici, personale sanitario ausiliario ("medical men"), infermieri e personale assicurativo[24] (Duong-Trung et al., 2020, p. 3). Ciascun utente è identificato da un ID univoco e dall'appartenenza a una collezione che ne definisce il gruppo e, di conseguenza, le autorizzazioni. In questo senso l'innovazione non è semplicemente tecnica ma a tutti gli effetti normativa e risiede nell'assoluta centralità conferita al paziente. A differenza degli altri attori, il paziente non solo ha il diritto di inizializzare le proprie informazioni anagrafiche e di interrogare i propri dati clinici e farmacologici, ma è l'unico ("the exclusive group") a cui è concesso il potere di supervisione totale. Il paziente può tracciare ogni singola interazione avvenuta con i propri dati: può sapere chi vi ha avuto accesso, quando, da quale indirizzo IP e per quale scopo (semplice interrogazione o modifica). Si realizzerebbe dunque pienamente la transizione da un paziente quale soggetto passivo, che vede i propri dati gestiti da altri, a controllore attivo e «auditore della propria sfera informativa»[25]. Le azioni degli altri utenti vengono, infatti, subordinate a questa architettura di controllo. I medici, ad esempio, possono inizializzare e aggiornare le cartelle cliniche e le informazioni sui farmaci, ma ogni loro interazione viene immutabilmente annotata nel registro distribuito, e, in questo modo, diviene trasparente e verificabile dal paziente. Allo stesso modo, il personale sanitario ausiliario può solo interrogare le cartelle cliniche e gli infermieri possono interrogare e tracciare le informazioni inserite dai medici, mentre il personale assicurativo può accedere esclusivamente alle informazioni sulle spese ospedaliere. Ogni azione di qualsiasi utente è preceduta da un rigoroso processo di autenticazione che verifica l'ID e l'appartenenza al corretto gruppo ("collection"), e ogni transazione viene registrata con uno stato ("QUERY" o "MODIFY") e metadati precisi (ID utente, ora, IP del dispositivo). In questo modo, il sistema "Smart Care" non si limita a proporre una soluzione tecnologica, ma delinea un vero e proprio ordinamento di *governance*

[22] M. Wong, K. Yee, C. Nohr, Socio-technical consideration for blockchain technology in healthcare: The technological innovation needs clinical transformation to achieve the outcome of improving quality and safety of patient care, in Studies in Health Technology and Informatics 247 (2018) 636-640.
[23] Cfr. Duong-Trung et al., Smart Care cit.
[24] Duong-Trung et al., Smart Care cit. 3.
[25] Duong-Trung et al., Smart Care cit. 6.

dei dati sanitari, basato su diritti, permessi e responsabilità chiaramente definiti e tecnicamente applicati ("enforced") tramite "smart contracts".

Posizionando il paziente al centro del sistema, l'architettura proposta affronta simultaneamente, dunque, i tre ostacoli principali identificati: garantisce la sicurezza e la privacy attraverso un controllo effettivo e granulare degli accessi; risolve la mancanza di fiducia tra gli operatori fornendo un registro trasparente e immutabile delle interazioni; e promuove la scalabilità dell'interoperabilità sanitaria. Duong-Trung e colleghi (2020) argomentano in difesa di questo approccio centrato sul paziente quale "soluzione sostenibile" ("tenable solution") per il complesso problema del controllo e del mantenimento della privacy nei meccanismi di transazione clinica. Inoltre, l'impegno a rendere pubblica l'intera soluzione di codice sul loro repository *GitHub* rafforza ulteriormente la natura pragmatica del contributo, coinvolgendo, non solo idealmente, la comunità scientifica per ulteriori sviluppi e una piena riproducibilità[26]. L'auspicio degli autori riguarda la delineazione di un percorso da un sistema opaco e basato sul possesso dei dati da parte delle istituzioni, a un 'nuovo' paradigma fondato su una "stewardship" dei dati trasparente, verificabile e, soprattutto, governata dal paziente stesso.

Si delinea una governance coerente con il tema dell'"habeas data", il diritto fondamentale di conoscere e controllare il destino delle proprie informazioni personali[27]; parallelamente, un altro interessante lavoro[28] di Duong-Trung prova ad applicare i principi della "blockchain" alla gestione della filiera del sangue, un bene pubblico non commerciabile, per instaurare una "fiducia nella matematica" che garantisca la qualità e la tracciabilità di una "risorsa vitale". L'idea di una "restituzione biopolitica" dell'atto della donazione, attraverso la quale il donatore può ricevere informazioni sul proprio stato di salute, illustra come la tecnologia possa riconfigurare il significato etico e sociale delle pratiche sanitarie, trasformando un atto di generosità in un ciclo informativo virtuoso. Entrambi i modelli, quantomeno sul piano concettuale, delineano la figura di un paziente pienamente sovrano, dotato di strumenti tecnici per l'esercizio effettivo della propria autodeterminazione[29]. Questa prospettiva traduce in termini architetturali la descrizione delle reti distribuite che, come notato da Philippakis e colleghi, «permette a ciascun database di essere autonomo rispetto al proprio schema di dati, di mantenere un controllo continuo sui propri dati e di innovare costantemente al proprio ritmo»[30].

5.- **La filiera del bene pubblico: il caso studio "BloodChain".**

Nel lavoro già introdotto sul tema della circolazione dei tessuti gli autori muovono dalla premessa che il sangue, risorsa vitale per l'essere umano e bene non soggetto a commercializzazione, soffre di catene di approvvigionamento inefficienti e di una fondamentale asimmetria informativa. Nei sistemi tradizionali, i riceventi non disporrebbero di alcuna informazione verificabile circa la qualità e l'origine del sangue che ricevono per trattamenti medici, e per le stesse istituzioni sanitarie l'intreccio

[26] Duong-Trung et al., Smart Care cit. 11ss.
[27] Rodotà, *Il diritto* cit. 315ss.
[28] H. Le, T. Nguyen, T. Nguyen, X. Ha, N. Duong-Trung, BloodChain: A Blood Donation Network Managed by Blockchain Technologies, in Network 2 (2022) 21 ss.
[29] Cfr. N. Rose, La politica della vita: biomedicina, potere e soggettività nel XXI secolo, a cura di P. B. T. M. M. De L., Torino 2008.
[30] A. Philippakis, D. Azzariti, S. Beltran et al., The Matchmaker Exchange: A platform for rare disease gene discovery, in Human Mutation 36.10 (2015) 919.

tra domanda ed offerta dei tessuti rappresenta una sfida costante in termini di efficienza, specialmente in un contesto demografico caratterizzato da un aumento della richiesta[31]. Sebbene esistano linee guida internazionali, come quelle dell'OMS, sulla gestione e conservazione del sangue, e sistemi nazionali, le (sempre limitate) risorse vengono impiegate in larga misura per la raccolta e la distribuzione spostando in secondo piano la tracciabilità completa e trasparente.

Di fronte a queste criticità che investono tanto la sicurezza sanitaria quanto la stessa fiducia nel sistema, gli autori hanno proposto l'adozione di un modello basato su "blockchain", quale «fondamento per un'architettura basata sulla fiducia, la trasparenza e l'immutabilità dei dati»[32]. L'obiettivo è stato, appunto, la realizzazione di un sistema, denominato "BloodChain", in cui la tracciabilità e la rintracciabilità dei dati permettessero di chiarificare ogni dettaglio della filiera, garantendo ai pazienti l'accesso alle informazioni necessarie senza violazioni della *privacy* e fornendo alle istituzioni uno strumento robusto per la gestione. La *Weltanschauung* soggiacente consisterebbe nella transizione, invero, non esente da problemi e da una certa naïveté vetero-positivista, dalla fiducia negli attori umani alla fiducia in un protocollo matematico, immutabile e verificabile da tutte le parti autorizzate[33]. Il fondamento architetturale di *BloodChain* si basa su una scelta tecnologica precisa ed eticamente rilevante: l'adozione di una "blockchain" di tipo "permissioned" (privata), in contrapposizione ai modelli "permissionless" (pubblici) come quello di *Bitcoin*. Gli autori argomentano che, mentre una rete permissionless è aperta a chiunque e si basa sull'anonimato e su costosi meccanismi di consenso come il "Proof of Work" per stabilire la fiducia, una rete "permissioned" opera come un consorzio di partecipanti noti, identificati e spesso verificati, che agiscono all'interno di un modello di governance predefinito.

Nel dibattito in corso merita menzione l'argomento secondo il quale questa scelta rappresenterebbe la via obbligata per il contesto sanitario. In un ecosistema che coinvolge ospedali, banche del sangue e centri medici, la fiducia non può (e non deve secondo gli autori) basarsi sull'anonimato, ma sulla responsabilità e sull'identità verificata degli attori. L'adozione di un'architettura "permissioned" permetterebbe, pertanto, di utilizzare protocolli di consenso più efficienti (come il *Crash Fault*-Tolerant o il Byzantine Fault-Tolerant) e, soprattutto, di mitigare intrinsecamente il rischio di azioni malevole. Proprio perché ogni partecipante è noto, ogni azione, dalla sottomissione di una transazione all'implementazione di uno "smart contract", verrebbe registrata in modo immutabile sul registro distribuito, rendendo l'attore responsabile facilmente identificabile e soggetto alle regole di governance del consorzio[34]. Per l'implementazione concreta di questo paradigma, gli autori hanno scelto la piattaforma Hyperledger Fabric, un progetto "open-source" di livello "enterprise". La scelta deriva dalle caratteristiche principali di questa risorsa: la sua architettura modulare, che separa la logica di business (*chaincode*), l'ordinamento delle transazioni e la loro validazione, ottimizzando performance e scalabilità; il supporto ai "canali" (*channels*), che permettono di creare delle sotto-reti private per partizionare i dati e garantire che le informazioni sensibili siano condivise solo con le parti autorizzate secondo un principio di "*need-to-know*"; e infine, la sua gestione di un registro immutabile che traccia ogni singola transizione di stato, garantendo un *audit trail* completo e inalterabile.

[31] Le et al., *BloodChain* cit. 22.
[32] Le et al., *BloodChain* cit. 22.
[33] Le et al., *BloodChain* cit. 23.
[34] Cfr. L. Feng, H. Zhang, Y. Chen, L. Lou, Scalable dynamic multi-agent practical byzantine fault-tolerant consensus in permissioned blockchain, in Applied Sciences 8.10 (2018) 1919.

L'architettura del sistema *BloodChain* è stata concepita per tradurre questi principi in un flusso operativo concreto, che crea una catena di custodia digitale e immutabile per ogni unità di sangue. Il modello identifica cinque attori principali: il donatore, il paziente, il personale medico, l'addetto al trasporto e il registro distribuito (l*edger*) stesso, che funge da garante e memoria storica del processo. Il flusso operativo, articolato in sette passaggi, inizia con la donazione di sangue da parte di un volontario e si chiude con l'utilizzo finale dell'unità di sangue per una trasfusione a un paziente. La "visibilità informativa" (*information visibility*) è il cuore dell'innovazione tecnico-giuridica di "BloodChain"[35]. Vale la pena sottolineare che gli autori non si sono limitati ad una proposta teorica, ma hanno fornito una validazione empirica della fattibilità e delle performance del sistema "BloodChain*"*, utilizzando *Hyperledger Caliper* per la valutazione, con risultati che dimostrerebbero la robustezza tecnica della soluzione. Tuttavia, rilevante risulta sicuramente l'attenzione riservata alla sicurezza e alla privacy: gli autori riconoscono che la gestione della privacy richiede ulteriori livelli di sofisticazione e propongono l'integrazione di un modello di controllo degli accessi basato sugli attributi ("Attribute-Based Access Control – ABAC") per una gestione dei permessi ancora più granulare.

6.- **Il trilemma della ricerca: "big data", "data harms" e risposte della "blockchain".**

La ricerca biomedica basata sui *big data* rappresenta, come già accennato, un altro ambito di possibile applicazione della tecnologia "blockchain", dove si dispiega in maniera paradigmatica la tensione dialettica tra il potenziale della innovazione tecnoscientifica e la necessità imprescindibile di salvaguardare il diritto fondamentale alla privacy, o più precisamente all'autodeterminazione informativa, dei soggetti coinvolti.

L'attuale paradigma scientifico, sottolinea il bioeticista Giovanni Rubeis[36] (2024), si sta spostando da studi su piccola scala a una "nuova normalità" caratterizzata da ricerche multicentriche su vasta scala, che mirano a integrare enormi volumi di dati multivariati per realizzare una medicina sempre più personalizzata e terapie centrate sul paziente. Tuttavia, rileva Rubeis, il trasferimento e l'archiviazione di dati sanitari così sensibili solleva un dilemma etico-giuridico fondamentale. I soggetti dei dati sono esposti a concreti 'danni da dati' (*"*data harms"), un concetto che include non solo la violazione della privacy, ma anche la perdita di controllo sul proprio dato ("disempowerment"), la preclusione da certi diritti ("disenfranchisement") e lo sfruttamento da parte di attori con scopo di lucro. Questa vulnerabilità è aggravata da un'intrinseca asimmetria di potere, un 'divario dei big data' ("big data divide") che separa i fornitori di dati (i cittadini) dai collettori e utilizzatori (istituzioni di ricerca, aziende), i quali controllano le infrastrutture tecnologiche e definiscono gli scopi dell'utilizzo. Proprio rispetto a queste criticità, la tecnologia "blockchain" emergerebbe come una potenziale soluzione tecnica: in primo luogo, la provenienza e tracciabilità dei dati, creando una catena cronologica, immutabile e verificabile, permette di ricostruire l'origine e gli spostamenti di ogni dato, rafforzando la fiducia nel processo di ricerca e facilitando la creazione di *audit trail* normativi. In secondo luogo, la decentralizzazione potrebbe mitigare le asimmetrie di potere e prevenire un uso commerciale monopolistico dei dati, allineandosi ai principi dell'*Open Science* e promuovendo un ecosistema di ricerca aperto alla collaborazione. In terzo luogo, argomenta

[35] Le et al., *BloodChain* cit. 23ss.
[36] Rubeis, *Ethical* cit. 495.

ancora Rubeis, l'immutabilità, ovvero la natura *append-only* dei blocchi, rende tecnicamente quasi impossibile alterare i dati, garantendone l'integrità e contribuendo ad affrontare la "crisi di riproducibilità" scientifica. Infine, il sistema di accesso e governance tramite "smart contracts" permette ai soggetti dei dati di definire in modo granulare le condizioni di accesso e utilizzo delle proprie informazioni. Questo meccanismo non solo protegge passivamente i dati, ma conferisce ai soggetti un controllo attivo, contrastando i fenomeni di "disempowerment" ed "exploitation" e facilitando procedure complesse come il ri-consenso.

Non manca, tuttavia, nella disamina di Rubeis, un focus sugli ostacoli nella implementazione pratica della tecnologia. Anzitutto la questione della scelta dell'architettura: le "blockchain" pubbliche (*permissionless*) sono vulnerabili ad abusi, mentre quelle private (*permissioned*), preferite in ambito sanitario, reintroducono un controllo centralizzato che rischia di minare i principi di apertura. Inoltre, la tecnologia non elimina ma, di fatto, complica la questione del consenso[37], presupponendo un'alfabetizzazione digitale che molti soggetti potrebbero non possedere, creando di fatto una barriera all'esercizio del controllo. L'integrazione nei flussi di lavoro si scontra con il "trilemma della "blockchain" tra sicurezza, decentralizzazione e scalabilità, e con la mancanza di standardizzazione che ostacola l'interoperabilità. Molteplici sono, inoltre, le incertezze circa la conformità con regolamenti esistenti come il GDPR o l'HIPAA degli "smart contracts" e i dubbi circa lo status giuridico di questi ultimi. Alla luce di questa ampia serie di chiaroscuri, Rubeis afferma con decisione che le soluzioni non sono da individuarsi a livello meramente tecnico ma che per realizzare il potenziale della "blockchain" sia indispensabile sviluppare e integrare delle misure di accompagnamento non tecniche, definite *enablers*. Tra queste l'autore propone modelli di consenso innovativi, come il meta-consenso, un approccio dinamico e a più livelli che si adatti alla logica degli "smart contracts". Al fondo rimane l'improrogabilità della definizione di un quadro giuridico chiaro circa la titolarità dei dati sanitari.

7.- **Proprietà e partecipazione: la condivisione dei dati genomici.**

Uno ulteriore scenario particolarmente discusso è quello della condivisione su larga scala di dati genomici: sul tema, Shabani[38] rileva che, nonostante, iniziative nazionali e internazionali come l'*All of Us Research Program* negli Stati Uniti e la *Global Alliance for Genomics and Health* abbiano sancito la condivisione responsabile dei dati come un principio cardine, permangono ostacoli concreti. Parte di queste difficoltà di governance deriva dall'adozione di approcci centralizzati e, pertanto, la ricerca di Shabani argomenta in favore delle potenzialità delle reti distribuite. In primo luogo, secondo l'autrice, la "blockchain" sovverte il concetto di "stewardship centralizzata" dei dati: mentre un modello centralizzato, come quello del database of *Genotypes and Phenotypes* (dbGaP) istituito dal NIH, affida a una terza parte il compito, intensivo in termini di risorse, di gestire il controllo degli accessi per un vasto numero di dataset[39], la "blockchain" prevederebbe un meccanismo di governance in cui l'autorità è ripartita tra molteplici attori fidati. Ciò consentirebbe ai

[37] U. Tatar, Y. Gokce, B. Nussbaum, Law versus technology: Blockchain, GDPR, and tough tradeoffs, in Computer Law & Security Review 38 (2020) 105454.

[38] M. Shabani, Blockchain-based platforms for genomic data sharing: A de-centralized approach in response to the governance problems?, in J. Am. Med. Inform. Assoc. 26.1 (2019) 76-80.

[39] Cfr. M. Shabani, B. Knoppers, P. Borry, From the principles of genomic data sharing to the practices of data access committees, in EMBO Molecular Medicine 7.5 (2015) 507-509.

nodi della rete di mantenere una *stewardship* locale sui database, esercitando una piena sovranità sulla concessione dei permessi di interrogazione e modifica relativi al proprio patrimonio informativo. Sebbene una *stewardship* locale possa essere offerta anche da reti distribuite tradizionali, la "blockchain" introduce un livello superiore di trasparenza ed efficienza. Un altro vantaggio fondamentale risiederebbe nelle capacità di *auditing* immutabile, fornendo un registro inalterabile delle informazioni critiche attraverso la rete e superando i limiti dei meccanismi di monitoraggio centralizzati la cui adeguatezza rimane discutibile. In secondo luogo, la tecnologia "blockchain" riconfigura il controllo degli accessi, in direzione di un modello partecipativo. Adottando una struttura "permissioned", in cui solo utenti pre-approvati possono accedere ai dati, il controllo può essere gestito in modo automatizzato. Un terzo ambito di trasformazione riguarda l'automazione degli accordi di accesso e del consenso: tramite uno *smart contract*, un individuo potrebbe autorizzare l'accesso ai propri dati solo a determinate condizioni o per scopi specifici, con la garanzia che tale autorizzazione sia «codificata ed eseguibile»[40]. Ad esempio, un paziente potrebbe creare uno *smart contract* che fornisce dati anonimizzati sulla sua biopsia tumorale a qualsiasi organizzazione di ricerca che li richieda, automaticamente, senza cioè rilasciare esplicitamente l'informazione. Questo meccanismo permetterebbe, inoltre, di tracciare esplicitamente i crediti accademici: l'accordo circa un contributo congiunto, ad esempio, potrebbe essere inserito in una "scatola" della "blockchain", rendendolo permanentemente visibile e impossibile da ripudiare unilateralmente per una delle parti. Un ulteriore aspetto riguarda invece l'analisi dei meccanismi di incentivazione, come l'"*Authorship Coin*", per premiare gli sforzi di condivisione e rispondere alle preoccupazioni dei ricercatori riguardo al giusto riconoscimento, una delle cause della ritenzione dei dati.

Il gruppo di ricercatori del Centro per l'Etica Biomedica dell'Università di Lovanio sostiene, da lungo periodo, invero, che, in un contesto caratterizzato da un vuoto normativo ma da un crescente supporto pubblico e accademico per il riconoscimento dei diritti di proprietà individuali sui dati genomici grezzi[41], la "blockchain" sia capace di fornire un ecosistema in cui gli individui possano mantenere la proprietà dei propri dati e decidere come condividerli. La vera svolta, quindi, è facilitata dalla tecnologia ma la trascende, risiedendo nella capacità di creare nuovi modelli di proprietà e di facilitare la partecipazione attiva degli individui. Se implementate con successo, queste soluzioni potrebbero trasformare la cultura della condivisione dei dati, rafforzando il ruolo di pazienti e cittadini e riducendo il monopolio dei fornitori di test, pubblici e privati, sulla gestione dei dati. In sintesi la "blockchain" aprirebbe alla possibilità di creare nuovi beni comuni ("commons") che si collocano in uno spazio intermedio tra il mercato e il bene pubblico.

Le ricerche di Shabani hanno il merito di analizzare la frontiera eticamente complessa dei "*DNA data marketplaces*". Questi mercati, mediati da "blockchain", in cui gli individui potrebbero tokenizzare e monetizzare i propri dati genetici, rappresentano il punto di massima tensione tra l'ideale dell'"empowerment" e il rischio della commodificazione totale della persona. Essi sollevano questioni etiche fondamentali riguardo alla giustizia e alla potenziale coercizione. Come evidenziato da J.J. Koplin[42], sebbene l'acquisto di dati genetici da parte di aziende private non sia intrinsecamente illecito, esso introduce seri rischi di sfruttamento ("exploitation"). La preoccupazione è che tali

[40] Shabani, *Blockchain-based* cit., 78.

[41] M. Shabani, D. Vears, P. Borry, Raw genomic data: storage, access, and sharing, in Trends in Genetics 34.1 (2018) 921ss.

[42] J. Koplin, The ethics of private companies purchasing DNA, in Bioethics 36.3 (2022) 267-274.

mercati possano esercitare una pressione indebita sui soggetti economicamente più vulnerabili, spingendoli a vendere i propri dati per necessità piuttosto che per una scelta pienamente autonoma, minando così i principi di giustizia distributiva[43].

8.- **Il fattore umano: limiti sociali e organizzativi all'innovazione tecnologica.**

Si propone, invece, di far emergere la complessità clinica, organizzativa, regolatoria ed etica il lavoro di Bautista e colleghi[44] che presenta l'applicazione MediLinker in vista di un passaggio da TRL4, validazione in un ambiente di laboratorio simulato a TRL5, validazione in un "ambiente rilevante" (una clinica di cure primarie, con pazienti reali che utilizzano i propri dati effettivi). L'articolo adotta una lente socio-tecnica[45], un approccio che considera la tecnologia non come un artefatto isolato, ma come un elemento interagente con *stakeholder*, processi organizzativi e quadri normativi. Attraverso il framework analitico "CORES" (*Clinical, Organizational and Regulatory, and Ethical and Social*), la ricerca si prefigge di identificare sistematicamente le problematiche associate all'implementazione clinica di *MediLinker* e di formulare raccomandazioni pratiche per affrontarle, basandosi sulle intuizioni di un gruppo di esperti del settore[46]. Le problematiche cliniche emerse dal focus group con gli esperti si articolano su quattro livelli interconnessi: il sistema clinico, l'amministrazione, gli operatori sanitari e i pazienti. Per quanto riguarda i pazienti, gli ambiti critici sono molteplici: la disparità nei livelli di alfabetizzazione sanitaria digitale che richiede meccanismi per prevenire la disinformazione derivante da un'errata interpretazione dei dati; l'usabilità dell'applicazione da validare su popolazioni diverse e vulnerabili, non solo, come nei primi tentativi, su studenti universitari giovani e in possesso di versatili competenze ; l'accessibilità da garantire anche su *smartphone* e sistemi operativi datati; e, infine, il meccanismo di verifica dell'identità basato su documenti ufficiali che rischia di escludere popolazioni vulnerabili come gli immigrati privi di documenti, contribuendo così a esacerbare le disuguaglianze sanitarie. Sul piano organizzativo-regolamentare, invece, emerge con forza il problema dell'*accountability*: in un sistema decentralizzato, non è chiaro chi sia legalmente responsabile in caso di violazione dei dati. Gli esperti sollevano la necessità di definire la "persona" giuridica delle organizzazioni e l'identità dei dispositivi all'interno della "blockchain" per poter attribuire le responsabilità in modo inequivocabile[47]. Una delle più gravi preoccupazioni etiche emerge dal *digital divide*.: richiedere uno *smartphone* connesso a Internet per accedere a servizi sanitari essenziali rischia di escludere le fasce più vulnerabili della popolazione, trasformando un potenziale strumento di equità in un ulteriore fattore di disuguaglianza sociale e sanitaria[48]. D'altronde come rilevano gli autori dell'*Eu Blockchain Observatory Forum*

[43] E. Ahmed, M. Shabani, DNA data marketplace: An analysis of the ethical concerns regarding the participation of individuals, in Frontiers in Genetics 10 (2019) 1107.
[44] J. Bautista, M. Usman, D. Harrell, E. Meyer, A. Khurshid, Clinical, organizational and regulatory, and ethical and social (CORES) issues and recommendations on blockchain deployment for healthcare: Evidence from experts, in "blockchain" in Healthcare Today 5 (2022) 1-14; e J. Bautista, U. Muhammad, D. Harrell, I. Desai, C. Holan, C. Cowley, A. Khurshid, Qualitative study of participant impressions as simulated patients of Medilinker a blockchain-based identity verification application, in ACI-Open 6 (2022) e1-e11.
[45] Cfr. R. Bostrom, J. Heinen, MIS problems and failures: A socio-technical perspective, Part II: The application of socio-technical theory, in MIS Quarterly 1.4 (1977) 11-28.
[46] Bautista et al., *Clinical* cit. 2.
[47] Bautista et al., *Clinical* cit. 6ss.
[48] C. Sieck, A. Sheon, J. Ancker, J. Castek, B. Callahan, A. Siefer, *Digital inclusion as a social determinant of health*, in *npj Digital Medicine* 4.1 (2021) 52.

(EUBOF) «uno dei paradossi del coinvolgimento del paziente è che i pazienti dichiarano interesse ad accedere alle loro informazioni sanitarie tramite un portale o un'app. Tuttavia, solo circa il 30% dei pazienti accede effettivamente alle proprie informazioni sanitarie»[49].
Infine, viene introdotto il concetto di *autonomia digitale legata alla salute* (*health-related digital autonomy*), Anche se un paziente utilizzasse MediLinker, argomentano infatti gli autori, per firmare digitalmente un consenso o una direttiva anticipata di trattamento (MPOA), non vi è alcuna garanzia che le istituzioni sanitarie, abituate a "firme autografe su moduli cartacei", riconoscano la validità legale di tale atto digitale, vanificando di fatto l'autonomia che la tecnologia intende conferire[50].

9.- **Progettare la responsabilità: principi per una "blockchain" etica in sanità.**
Come per le più ampiamente discusse applicazioni dell'intelligenza artificiale diversi autori hanno provato a delineare gli imperativi etici che devono guidare l'implementazione della tecnologia "blockchain" (ed in particolare nel delicato ecosistema sanitario). Pur riconoscendone il significativo potenziale trasformativo, e muovendo da un *background* ingegneristico-informativo, Ramachandran propone un'analisi che si allontana dalle visioni puramente tecno-ottimistiche e ha dedicato al tema ricerche[51] ed una monografia meritevole di attenzione [52]. Si argomenta la necessità di un approccio che, al fine di prevenire conseguenze non-intenzionali lesive della dignità dei soggetti, orienti teleologicamente l'innovazione. Ciò implica che la progettazione non sia un processo assiologicamente neutro, ma un'attività intrinsecamente normativa, chiamata a incorporare *a priori* i principi etici fondamentali come suo criterio direttivo secondo il modello "*Ethics by Design*"[53]. Ramachandran sottolinea un dilemma fondamentale e intrinseco alla natura stessa della "blockchain": la sua caratteristica più distintiva, l'immutabilità del registro, potrebbe collidere con la protezione dei diritti fondamentali della persona sanciti a livello internazionale, come il diritto di un paziente di modificare o richiedere la cancellazione dei propri dati sanitari. Questa tensione tra la permanenza del dato e l'autonomia individuale costituisce un nucleo problematico che necessita di soluzioni architetturali e giuridiche innovative; Ramachrandan scandaglia dunque la letteratura esistente e le proposte teoriche per far emergere un *framework* etico robusto, che risulti capace di guidare l'innovazione in modo responsabile, promuovendo fiducia pubblica, equità e benefici sociali a lungo termine[54]. Per affrontare questa complessità, l'autore individua cinque dimensioni etiche fondamentali che devono essere considerate in modo olistico e interconnesso: privacy, sicurezza, governance, sovranità dei dati e inclusività. La privacy e la sicurezza, di importanza capitale in ambito sanitario, richiedono l'impiego di solidi metodi crittografici e di meccanismi decentralizzati per il

[49] K. Votis, K. Livitckaia, T. Damvakeraki, N. Kostopoulos, N. Sarafidis, G. Giaglis, L. Dionysopoulos, M. Charalambous, *Blockchain Applications in the Healthcare Sector*, Bruxelles 2022, 5.
[50] Bautista et al., *Clinical* cit. 7.

[51] M. Ramachandran, Ethics of Blockchain by Design: Guiding a Responsible Future for Healthcare Innovation, in Blockchain in Healthcare Today 7 (2020) 10-30953.
[52] M. Ramachandran, Blockchain engineering: Secure, sustainable frameworks for healthcare applications, Singapore 2025, xx.
[53] Cfr. L. Floridi, *The ethics of technology: A developmental approach*, Oxford 2021; J. van den Hoven, P. E. Vermaas, I. van de Poel (curr.), *Designing in ethics*, Cambridge 2017.
[54] M. Ramachandran, Ethics of blockchain by design: Guiding a responsible future for healthcare innovation, in "blockchain" in Healthcare Today 7 (2024) 1.

controllo degli accessi, al fine di proteggere i dati da violazioni e abusi[55]. La decentralizzazione, se da un lato restituisce al paziente il controllo sui propri dati, dall'altro introduce complesse questioni di governance e di attribuzione della responsabilità in una rete di partecipanti distribuiti[56]. Per mitigare questi rischi, il *framework* etico deve incorporare controlli tecnici come chiavi crittografiche, pseudonimizzazione e *smart contracts* basati sul consenso.

Per superare l'apparente inconciliabilità tra il "diritto all'oblio" sancito dal GDPR e l'immutabilità della "blockchain", Ramachandran avanza una soluzione tecnica che risponde a precise esigenze etico-giuridiche di archiviazione *off-chain* dei dati sensibili. Secondo questo modello, solo i riferimenti crittografici (*hash*) dei dati verrebbero registrati in modo permanente sulla catena, mentre i dati reali risiederebbero in database sicuri e modificabili esterni ad essa. In questo modo, sarebbe possibile cancellare o aggiornare i dati rendendo obsoleto il relativo hash, senza alterare l'integrità della "blockchain". Per quanto riguarda invece l'enfasi dell'HIPAA, sulla protezione delle informazioni sanitarie (PHI) viene evidenziata una forte corrispondenza nelle capacità intrinseche della "blockchain" di supportare la crittografia e, soprattutto, nell'uso di reti *permissioned* (private), che consentono un controllo degli accessi basato sui ruoli, in piena aderenza allo standard del "minimo necessario". Come esempio paradigmatico di un'implementazione riuscita, viene citato il sistema *eHealth* dell'Estonia, che utilizza la "blockchain" per registrare gli accessi ai dati sanitari di oltre il 95% dei cittadini, combinando la trasparenza della catena con l'archiviazione off-chain dei dati sensibili in conformità con il GDPR.

Il cuore delle proposte di Ramachandran pulsa intorno a cinque principi guida (*best practice guidelines*), concepiti come un *framework* normativo per uno sviluppo etico della "blockchain" in sanità. La definizione di questi principi è finalizzata alla conciliazione tra la discussione di natura teorica e le direttive progettuali concrete. Il primo - *principio della proprietà dei dati e del consenso* - postula il diritto inalienabile del paziente di mantenere la proprietà e il controllo sull'uso e la condivisione dei propri dati, un diritto che, tramite le tecnologie in oggetto, potrebbe essere tecnicamente garantito tramite sistemi di gestione del consenso in tempo reale integrati negli *smart contracts*. Il secondo principio - *meccanismi di tutela della privacy* - impone l'integrazione di protocolli crittografici avanzati come elemento non negoziabile del *design*. Il terzo, che assume un decisivo rilievo sociale, è il principio di accesso equo e inclusività. Si postula che i sistemi "blockchain" siano progettati per essere accessibili a tutte le popolazioni, con l'obiettivo esplicito di mitigare, e non esacerbare, le disparità sanitarie esistenti. Il quarto principio affronta direttamente il vuoto di potere delle architetture decentralizzate: la *governance trasparente e responsabile*; esso richiederebbe l'implementazione di meccanismi di governance chiari e democratici, che favoriscano modelli inclusivi come le Organizzazioni Autonome Decentralizzate (DAO), in cui la responsabilità per le decisioni della rete è distribuita ma definita. Infine, il quinto ed ultimo principio - *interoperabilità e design sostenibile* - sottolinea la necessità pragmatica di integrare le nuove soluzioni con le infrastrutture sanitarie esistenti in modo fluido, sicuro e sostenibile nel tempo. È

[55] Cfr. G. Dagher, J. Mohler, M. Milojkovic, P. Marella, Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology, in Sustainable Cities and Society 39 (2018) 283-297; vedi anche A. Azaria, A. Ekblaw, T. Vieira, A. Lippman, MedRec: Using blockchain for Medical Data Access and Permission Management, in Proceedings of the 2nd International Conference on Open and Big Data (OBD), Wien 2016, 25-30.

[56] Cfr. K. Werbach, *The Blockchain and the New Architecture of Trust*, Cambridge (MA) 2018 e P. De Filippi, A. Wright, *Blockchain and the Law: The Rule of Code*, Cambridge (MA) 2018.

importante sottolineare che i principi guida, presentati come un *framework* interconnesso, non sono intesi come opzioni discrete, ma come un sistema organico di valori che deve informare l'intero ciclo di vita della tecnologia, dalla concezione alla sua governance continua[57][58].

L'intento è quello di una progettazione etica che non agisca come freno per l'innovazione ma, al contrario, quale catalizzatore per uno sviluppo tecnologico responsabile. Ramachandran, tra gli altri, afferma che l'inserimento di presidi di tutela per la persona sin dalle prime fasi della progettazione è la condizione imprescindibile per garantire che i sistemi "blockchain" siano centrati sulla dignità umana e sul principio del "primum non nocere", e che contribuiscano al miglioramento degli esiti sanitari globali. Tra le sfide future vi è lo sviluppo di framework etici scalabili, adattabili a contesti con risorse diverse. In secondo luogo, è necessario affrontare le complessità derivanti dall'integrazione della "blockchain" con IA e IoT, che introducono rischi specifici legati a bias algoritmici e privacy. Infine, risulta cruciale dare priorità a soluzioni concrete per l'equità e il divario digitale, attraverso una progettazione inclusiva che consideri accessibilità per reti a bassa larghezza di banda e utenti con limitata alfabetizzazione digitale. In definitiva, il lavoro di Ramachandran (2024) funge da bussola etico-giuridica, tracciando un percorso per l'evoluzione della "blockchain" in sanità guidato non solo dalla fattibilità tecnica, ma da un profondo impegno verso il benessere umano e la giustizia sociale.

10.- **Conclusioni. La "costituzionalizzazione" della "blockchain" come governo dell'innovazione.**

Nelle parti precedenti di questo lavoro sono stati ricostruiti alcuni dei temi centrali delle questioni etico-giuridiche relative all'implementazione della tecnologia "blockchain" in sanità. Le istituzioni europee sono attive sulle frontiere più avanzate di questo dibattito, ne è prova, tra le altre, il recente intervento del Comitato Europeo per la Protezione dei Dati (EDPB) che prova a definire una prima, provvisoria, sintesi. Le Linee Guida 02/2025, che analizzano nella loro versione preliminare aperta alla consultazione pubblica fino alla fine di giugno 2025, trascendono la dimensione di una semplice disamina tecnica per configurarsi, piuttosto, come un fondamentale atto di governo giuridico. Partendo dal presupposto che la « la scelta di una tecnologia incide direttamente sulle modalità del trattamento e sulla sua conformità al GDPR», l'EDPB l'EDPB aspira, peraltro con strumenti partecipativi, a avviare una complessa operazione di governo giuridico: ricondurre la logica dei registri distribuiti – che per sua natura tende a generare effetti immutabili e a non ammettere eccezioni – entro il perimetro di ragionevolezza, proporzionalità e tutela della dignità umana che costituiscono il fondamento del diritto europeo. Si tratta di una risposta diretta a quella che De Filippi e Wright definiscono una trasformazione epocale: «In definitiva, si assiste al passaggio da una società governata da leggi e istituzioni a una società governata da un nuovo tipo di legge, un nuovo tipo di istituzione, incorporati nell'infrastruttura tecnologica della rete. Questa è la nuova 'legge del codice' (rule of code)»[59]. Si tratterebbe, in sostanza, di un tentativo di riaffermare la supremazia dei principi che proteggono la persona rispetto ad un'architettura la cui logica interna, orientata all'immutabilità

[57] Y. Tang, J. Xiong, R. Becerril-Arreola, L. Iyer, Ethics of blockchain: A framework of technology, applications, impacts, and research directions, in Information Technology & People 33.2 (2020) 602 ss.
[58] C. Lapointe, L. Fishbane, The blockchain ethical design framework, in Innovations: Technology, Governance, Globalization 12.3-4 (2019) 50 ss.
[59] De Filippi, Wright, *Blockchain* cit. 18.

e alla disintermediazione, non contempla nativamente categorie giuridiche e umane come il diritto all'oblio, la fallibilità o il contesto, tentando così di risolvere le profonde tensioni emerse.

La prima tensione che le *Linee Guida* sembrano voler affrontare sarebbe quella tra l'utopia della sovranità individuale e la sua problematica attuazione. Le architetture ideali, come quelle proposte da Duong-Trung nei suoi lavori su *Smart Care* e *BloodChain,* prefigurano un paziente pienamente sovrano, controllore esclusivo del proprio "corpo elettronico". Questo ideale, tuttavia, come evidenziato dall'analisi socio-tecnica di Bautista, si scontra con la dura realtà del *digital divide* e della scarsa *eHealth literacy*. Di fronte a quella che potrebbe configurarsi come una "sovranità illusoria", la risposta dell'EDPB apparirebbe tanto pragmatica quanto garantista: riaffermare la centralità giuridica del titolare del trattamento. L'insistenza su questo ruolo non andrebbe letta come un semplice ritorno alla centralizzazione, quanto piuttosto come il tentativo di creare un presidio di responsabilità fiduciaria; una soluzione che, tuttavia, non è priva di ambiguità e che rischia di reintrodurre profili paternalistici. Poiché non sarebbe possibile garantire a ogni individuo la capacità tecnica di essere il sovrano di sé stesso, il diritto sembrerebbe direzionare un approccio pragmatico: l'immaturità delle condizioni per un *empowerment* tecnologico universale, imporrebbe a entità giuridicamente identificabili il dovere di agire per conto dell'interessato. La norma imporrebbe un dovere di protezione all'istituzione. Questo dovere, però, non andrebbe inteso come un atto meramente limitante, ma assumerebbe, in questa lettura, una precisa dimensione abilitante. Tale logica giuridica richiamerebbe da vicino il principio di eguaglianza sostanziale sancito dall'articolo 3 della Costituzione italiana, secondo il quale è compito della Repubblica «rimuovere gli ostacoli di ordine economico e sociale» che limitano di fatto la libertà e l'eguaglianza dei cittadini. In questo scenario, il divario digitale e la complessità tecnica rappresenterebbero esattamente quegli ostacoli che impediscono a molti di esercitare pienamente i propri diritti. Imponendo un dovere di tutela all'istituzione, la norma agirebbe attivamente per rimuovere queste barriere, cercando di garantire che l'autodeterminazione non sia un privilegio formale per i soli tecnicamente alfabetizzati, ma una possibilità sostanziale per tutti. Questa figura di garanzia agirebbe quindi in direzione del pieno sviluppo della autodeterminazione ma non dovrebbe rappresentare un punto di arrivo. Al contrario, una tale tutela giuridica andrebbe intesa come un supporto idealmente transitorio, la cui stessa necessità sottolineerebbe l'urgenza di investire in percorsi di formazione e alfabetizzazione digitale che possano, in futuro, rendere la sovranità individuale anche rispetto alla tecnologia "blockchain" un diritto effettivo e non solo proclamato.

La seconda tensione, di natura etico-economica, verrebbe affrontata opponendo ai rischi di commodificazione del dato la forza dei principi del GDPR. Le riflessioni di Shabani sui *DNA data marketplaces* e di Rubeis sui *data harms* svelano il rischio che il dato sanitario diventi una merce fluida, il cui valore economico prevale sulla sua natura personale. A questa deriva, che realizzerebbe i timori di tanti interpreti intorno alla reificazione della persona, le *Linee Guida* opporrebbero la limitazione della finalità e la minimizzazione dei dati. Questi principi agirebbero come un potente argine giuridico, poiché ogni trattamento dovrebbe essere ancorato a uno scopo esplicito e legittimo. Il diritto, in questo modo, cercherebbe di imporre un "freno etico", in linea con l'etica dei dati propugnata da Floridi, alla pura logica economica, riaffermando che il trattamento dei dati deve servire a un fine umano predeterminato.

La tensione più radicale, quella tra l'immutabilità della catena e il diritto alla cancellazione, troverebbe una soluzione che testimonia un acuto pragmatismo giuridico. Questo scontro tra una

caratteristica tecnica e un diritto fondamentale, la cui tutela è un imperativo etico come sottolineato da Ramachandran, appare irrisolvibile. La soluzione proposta dall'EDPB sarebbe il compromesso dell'archiviazione off-chain. Attraverso la raccomandazione «*as a general rule, storing personal data on a* "blockchain" *should be avoided*»[60], il Comitato non rigetterebbe la *tecnologia*, ma la "disarmerebbe" del suo potenziale lesivo. La "blockchain" verrebbe accettata per la sua funzione di 'notarizzazione', mentre i dati personali risiederebbero al di fuori. Questa visione è confermata dalla pratica industriale: come emerge dal report dell'EUBOF, attori come *Embleema* scelgono questa architettura perché «archiviare dati sanitari on-chain è pericoloso»[61], a dimostrazione di come questo approccio ibrido sia probabilmente l'unica via percorribile.

Infine, le Linee Guida affronterebbero la tensione tra innovazione e responsabilità, tentando di codificare in obbligo giuridico l'imperativo dell'"*Ethics by Design*" qui discusso a partire dai lavori di Ramachandran. Questo approccio sembrerebbe incarnare perfettamente la dinamica tra "*soft law*" e "*hard law*" che Luciano Floridi ha analizzato nel contesto delle tecnologie emergenti. Secondo questa lettura, di fronte a un'innovazione che avanza più rapidamente del processo legislativo, l'etica farebbe da ponte per la "soft law": un insieme di principi, raccomandazioni e buone pratiche (come appunto l'"*Ethics by Design*") che orientano lo sviluppo in modo responsabile, riempiendo il vuoto normativo. L'intervento del legislatore europeo con il GDPR, e di conseguenza l'enfasi dell'EDPB sul principio di "*Privacy by Design and by Default*" (Art. 25 GDPR), rappresenterebbe il momento in cui questa dinamica tra principi etici e "soft law" viene recepita e trasformata in "hard law" vincolante. La Valutazione d'Impatto sulla Protezione dei Dati (DPIA) non sarebbe più, quindi, solo un'astratta raccomandazione, ma un precetto legale operativo, lo strumento attraverso cui i progettisti sono costretti a porsi, *ex ante*, le domande fondamentali che ne determineranno la liceità: «1) I dati registrati sulla "blockchain" conterranno dati personali? 2) In caso affermativo, per quale motivo è necessario utilizzare una "blockchain" per questo trattamento? (Qual è la logica sottostante a tale scelta tecnologica? Quali alternative sono state prese in considerazione?) 3) Che tipo di "blockchain" si intende adottare? (È sufficiente una "blockchain" privata? È possibile utilizzare una "blockchain" *permissioned*? È ipotizzabile un'architettura basata su meccanismi di "zero-knowledge"?) 4) Quali misure tecniche e organizzative saranno adottate? (I dati personali verranno archiviati on-chain o off-chain? Saranno impiegate tecnologie volte a rafforzare la tutela della privacy – e in caso contrario, per quale motivo?)»[62].

Attraverso l'imposizione di un Titolare responsabile, la riaffermazione della finalità del trattamento, la soluzione pragmatica dell'off-chain e la codificazione della progettazione etica, le *Linee Guida* non sembrerebbero voler frenare la "blockchain", ma piuttosto incanalarla all'interno di un "recinto di costituzionalità". Si tratterebbe, in definitiva, del tentativo di potenziare un ecosistema di fiducia e garanzie legali che appare come il presupposto indispensabile per la legittimazione sociale e l'adozione a lungo termine di una tecnologia così potente.

[60] EDPB, Guidelines 02/2025 on processing of personal data through Blockchain technologies, Versione preliminare 1.1 del 8 aprile 2025, 2.

[61] Votis, Blockchain Applications cit. 41.

[62] EDPB, Guidelines 02/2025 on processing of personal data through blockchain technologies, Versione preliminare 1.1 del 8 aprile 2025, 11.

Abstract.- Il contributo analizza le complesse implicazioni etico-giuridiche derivanti dall'applicazione della tecnologia blockchain nel settore sanitario. Attraverso una rassegna critica della dottrina e l'esame di modelli applicativi, si portano ad evidenza le tensioni tra le caratteristiche tecniche della blockchain, come l'immutabilità e la decentralizzazione, e la tutela dei diritti fondamentali della persona, in particolare il principio di autodeterminazione informativa e i diritti sanciti dal GDPR. Dall'analisi della letteratura emerge come la blockchain possa abilitare modelli di sanità digitale paziente-centrici, rafforzando il controllo dell'individuo sui propri dati e migliorando la trasparenza e la sicurezza nella gestione delle informazioni cliniche e nella filiera farmaceutica. Tuttavia, emergono, al contempo, criticità significative, quali il rischio di conflitto tra l'immutabilità del registro e i diritti alla rettifica e cancellazione dei dati, le sfide poste dal divario digitale e la difficoltà di attribuire la responsabilità giuridica in sistemi distribuiti. Si conclude, pertanto, che la legittimità dell'innovazione dipende dalla capacità di integrare sin dalla progettazione presìdi di tutela della persona
La risposta regolatoria europea, come le linee guida dell'EDPB, viene presa in esame quale tentativo di "costituzionalizzazione" della tecnologia, che ne circoscrive l'applicazione in un perimetro di proporzionalità e garanzie legali.

The paper examines the complex ethical and legal implications arising from the application of blockchain technology in the healthcare sector.
Through a critical review of scholarly literature and an analysis of practical implementation models, it highlights the tensions between the technical features of blockchain—such as immutability and decentralization—and the protection of fundamental human rights, particularly the principle of informational self-determination and the rights enshrined in the GDPR.
The analysis of existing studies shows that blockchain can enable patient-centred digital healthcare models, strengthening individual control over personal data and improving transparency and security in the management of clinical information and in the pharmaceutical supply chain.
However, significant challenges also emerge, such as the potential conflict between the immutability of the ledger and the rights to rectification and erasure of data, the issues arising from the digital divide, and the difficulty of attributing legal responsibility within distributed systems.
It is therefore concluded that the legitimacy of innovation depends on the capacity to integrate safeguards for the individual from the very design stage.
The European regulatory response, such as the EDPB Guidelines, is examined as an attempt to achieve a form of *"constitutionalization"* of technology, which confines its application within a framework of proportionality and legal guarantees.