Dati sanitari e *NFT*: nuovi strumenti e sfide per il mercato digitale

di *Cristina Bosso* e *Valentina D'Adda*

SOMMARIO: 1. Dati sanitari: trattamento e circolazione in Europa. – 2. *NFT* e tutela dei dati sanitari. – 3. Potenziali benefici. – 4. Sfide e punti deboli. – 5. Conclusione.

1. Dati sanitari: trattamento e circolazione in Europa

Nel corso dell'ultimo decennio, in particolare dopo l'avvento della pandemia, si è assistito a una crescente digitalizzazione della sanità, anche alla luce dell'incremento della raccolta di *big data* e dello sviluppo dei processi di *machine learning* nell'ambito della ricerca medica transnazionale[1].

Tali fenomeni offrono spunti di riflessione in merito alle condizioni di trattamento e di circolazione dei dati sanitari, con particolare attenzione alla predisposizione di sistemi di sicurezza informatica da parte delle pubbliche amministrazioni, incaricate di detenere i dati dei pazienti in ragione dell'attività sanitaria svolta e spesso bersaglio di *cyber attack*[2]. Quanto alla circolazione dei dati, è interessante domandarsi quale sia il ruolo svolto dal paziente titolare degli stessi, sia al momento dell'iniziale trasferimento sia nel corso della loro successiva circolazione.

Gli aspetti riguardanti trattamento e circolazione si prestano ad essere analizzati da un punto di vista giuridico e tecnologico.

Da un punto di vista giuridico, occorre esaminare quanto previsto dal Regolamento generale sulla protezione dei dati (UE/2016/679) e nello specifico dagli artt. 4 par. 1 n. 15, 6 e 9 par. 1 e 2.

---

[1] Le indagini di mercato effettuate dalla società statunitense *Black Book Research* rivelano che tra agosto 2021 e gennaio 2022, l'integrazione della tecnologia sanitaria e della piattaforma dati dovrebbe raggiungere una dimensione di mercato globale di 21 miliardi di dollari entro il 2027. AP NEWS, *Innovaccer Data Activation Platform Rated Top End-to-End Hospital & Health System Population Health Solution, 2022 Black Book Survey* in apnews.com.

[2] Si veda, ad esempio, l'attacco subito dal sistema informatico sanitario della Regione Lazio nel luglio 2021. Per ulteriori approfondimenti: Il Sole 24 ore, *Attacco hacker alla Regione Lazio, indaga anche l'antiterrorismo*, 2 agosto 2021 in ilsole24ore.com; Regione Lazio, *Attacco hacker ai sistemi informatici della Regione Lazio,* 7 agosto 2021 in regione.lazio.it.

I dati relativi alla salute vengono definiti come "*attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute*". Il loro trattamento è in linea generale vietato, a meno che non si verifichi uno dei casi espressamente previsti, tra i quali rientra il conferimento del consenso da parte del titolare.

Viene prevista, inoltre, la possibilità di trattare tali dati, a prescindere dal consenso dell'interessato, quando vengano in rilievo ragioni di interesse pubblico, quali, ad esempio, la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria, dei medicinali e dei dispositivi medici[3].

Delineato il quadro normativo di riferimento, è possibile desumere che il titolare dei dati rivesta un ruolo marginale, in quanto solo eventualmente gli viene richiesto di prestare il consenso. Qualora questo non sia necessario, l'interessato rimane del tutto escluso dalla vicenda circolatoria che coinvolge i suoi dati sanitari e non esercita alcun tipo di controllo sui trasferimenti successivi.

Quanto alla prospettiva strettamente tecnologica, i dati sanitari sembrano essere conservati nella maggior parte delle ipotesi dalle pubbliche amministrazioni all'interno di *database* ad accesso protetto. Tuttavia, altri strumenti hanno acquisito importanza, fra cui i c.d. *API (application programming interfaces*), ossia delle applicazioni che, mediante modalità standard, espongono le funzionalità di altre applicazioni per agevolare la programmazione e l'integrazione tramite l'immediato accesso ai dati per mezzo di appositi algoritmi, così da facilitarne l'immediato uso e il trasferimento[4].

Tutto ciò premesso, occorre esaminare all'interno dell'emergente panorama tecnologico le soluzioni alternative che consentano maggior partecipazione e controllo da parte del titolare dei dati sanitari e maggior sicurezza nella conservazione e nella circolazione degli stessi.

---

[3] Si vedano anche le previsioni adottate dall'EDPB il 21 aprile 2020. European Data Protection Board, *Linee-guida 03/2020 sul trattamento dei dati relativi alla salute a fini di ricerca scientifica nel contesto dell'emergenza legata al COVID-19* in edpb.europa.eu.

[4] La compagnia Microsoft offre uno specifico pacchetto di *health data services* su *cloud* in azure.microsoft.com.

2. *NFT* e tutela dei dati sanitari

Nuove forme di proprietà digitale possono ispirare la creazione di un mercato digitale per i dati sanitari che consenta ai titolari di poter riguadagnare un adeguato controllo su di essi. La possibilità di utilizzare i *Non-Fungible Token* (*NFT* ossia *token* non fungibili) potrebbe rappresentare un incentivo alla creazione di un sistema maggiormente trasparente ed efficiente per la tutela di questi dati, caratterizzato da un maggior controllo esercitato dai pazienti stessi. Gli *NFT* sono stati inizialmente impiegati per prevenire la circolazione non autorizzata di opere d'arte digitali e si sono in seguito diffusi in altri ambiti, quali il *gaming*, la moda e l'assistenza sanitaria, portando alla creazione di un mercato multimiliardario[5].

Un *token* viene definito come un insieme di informazioni digitali che rappresenta digitalmente una posizione legale su un bene o un diritto su un oggetto specifico[6]. Per cercare di comprendere cosa si intenda con *token* non fungibile (*NFT*), è utile considerare la differenza tra il concetto di fungibilità e infungibilità: mentre una banconota viene definita come fungibile perché intercambiabile con altre banconote, un bene infungibile è dotato di una sua specifica individualità economica che non ne consente la sostituzione con un altro[7]. I *token* non fungibili sono di per sé unici, non intercambiabili e insostituibili e ogni *token* rappresenta la proprietà di un soggetto su uno specifico *asset* digitale[8].

Gli *NFT* sono creati "coniando" - dall'inglese "*minting*" - contenuti digitali su una *blockchain*.

Il *minting* comporta il caricamento, la verifica da parte di altri computer, la marcatura temporale dei contenuti, della posizione e dell'autore delle informazioni digitali. Tutte le transazioni successive vengono registrate su quello che può essere definito come "libro mastro digitale" (*digital ledger*) distribuito su una rete di computer. La ridondanza, insieme alla

---

[5] W. REHMAN, H.E ZAINAB, J. IMRAN, N. Z. BAWANY, *NFTs: Applications and Challenges*, 22nd International Arab Conference on Technology (ACIT), 2021.

[6] L. OLIVEIRA, L. ZAVOLOKINA, I. BAUER, G. SCHWABE, *To Token or not to Token: Tools for Understanding Blockchain Tokens*, International Conference of Information Systems, 2018. Esistono diversi tipi di *token* che possono essere usati come valuta (*bitcoin*) oppure come titoli, comprendendo non solo diritti di proprietà ma anche diritti di voto.

[7] E. PATCH, *Why everyone is talking about NFTs*, in Kiplinger's Personal Finance 5/2022, 69-72, 2022.

[8] D. DAS, P. BOSE, N. RUARO, C. KRUEGEL, G.VIGNA, *Understanding Security Issues in the NFT Ecosystem,* University of California, 2022.

difficoltà di calcolo e all'energia di elaborazione richiesta, rende particolarmente difficile la manomissione del registro delle transazioni[9].

I *token* non fungibili si sono diffusi grazie a contratti digitali composti da metadati che ne specificano i diritti di accesso e i termini di scambio. Gli *NFT* sono, infatti, costituiti da un codice unico di identificazione a 40 cifre (*hash*) e da un *URL* che si collega al contenuto online, formando uno *smart contract*[10]. Questi ultimi consistono in accordi digitali scritti in codice informatico, eseguito su una *blockchain* o altre *distributed ledger technologies* (*DLT*)[11] in maniera automatica e senza la necessità di alcun intervento umano[12].

Nell'assistenza sanitaria, proprio gli *smart contract* potrebbero essere utilizzati per designare una copia dei propri dati digitali controllata dal paziente stesso e i termini in base ai quali è possibile accedervi ed utilizzarli.

3. Potenziali benefici

Il sistema in esame, in quanto strumento di *data sharing*, presenta delle interessanti potenzialità poiché idoneo a supplire alle inefficienze e alla mancanza di trasparenza nel trasferimento di dati sanitari. Disciplinando in maniera puntuale i contratti che ne regolano lo scambio, potrebbe sorgere un *marketplace* innovativo in cui i pazienti sarebbero in grado di consultare i propri dati su apposite piattaforme e ne controllerebbero i relativi movimenti[13].

Peraltro, i soggetti interessati all'acquisizione dei dati potrebbero agevolmente verificarne la provenienza e l'autenticità grazie alle peculiari caratteristiche della *blockchain* e all'unicità dei

---

[9] K. KOSTICK-QUENET, K. D. MANDL, T. MINSSEN, I. GLENN COHEN, U. GASSER, I. KOHANE, A. L. MCGUIRE, *How NFTs could transform health information exchange* in *Science*, 375 (6580), 500 e ss., 2022.

[10] *Ibidem*.

[11] I *token* vengono registrati su una *blockchain* che rappresenta una tipologia particolare di *distributed ledger technology* (*DLT*). Con *ledger*, che letteralmente può essere tradotto come libro mastro o registro, si intende una tecnologia che applicando la crittografia permette di mantenere più copie di un libro mastro centrale attraverso una rete informatica. Ogni libro mastro conserva una copia del database digitale di tutte le transazioni mai avvenute ed è formato da tanti blocchi di documenti elettronici criptati, collegati tra loro e diffusi attraverso una fitta rete informatica *peer-to-peer*. R. DE CARIA, *The Legal Meaning of Smart Contracts*, in European Review of Private Law, 733, 2019.

[12] M. RASKIN, *The law and legality of smart contracts,* Georgetown Law Technology Review, 304, 2017.

[13] K. KOSTICK-QUENET, K. D. MANDL, T. MINSSEN, I. GLENN COHEN, U. GASSER, I. KOHANE, A. L. MCGUIRE, *op. cit*. Si veda anche il caso della piattaforma *Aimedis*, il primo *marketplace* in cui è possibile vendere *NFT* medici e scientifici a livello mondiale. Si distingue per la creazione di nuovi mercati, collegando ospedali, ricercatori e aziende di intelligenza artificiale, oltre che per l'offerta di *NFT* che standardizzano il mercato multimiliardario di dati medici e per la garanzia di sicurezza nelle operazioni di condivisione dati.

token. Sulla base degli *smart contract*, ogni paziente sarebbe in grado di individuare coloro che ricevono i dati, pur mantenendo la propria pseudonimizzazione.

Con il termine pseudonimizzazione si intende una forma di deidentificazione che utilizza un elemento sostitutivo, quale un numero o uno pseudonimo, per indicare il titolare dei dati personali[14]. Alcuni commentatori ritengono preferibile l'utilizzo di tale termine in luogo di anonimizzazione, in quanto quest'ultima sarebbe foriera di equivoci: dato l'elevato rischio di reidentificazione dei soggetti, l'anonimità non sarebbe un risultato effettivamente raggiungibile[15].

Infine, la tecnologia in esame potrebbe contribuire al superamento di alcune delle criticità del sistema di trasferimento dei dati personali tra l'Unione Europea e gli Stati Uniti. Come noto, la Corte di Giustizia dell'Unione Europea ha ritenuto illegittimo il c.d. *Privacy Shield*, ossia l'accordo che ne regolava il trasferimento[16], poiché tale meccanismo non consentiva, tra l'altro, ai titolari dei dati di ottenere un valido ristoro. Grazie agli *NFT*, vi sarebbero sostanzialmente due alternative: una di natura contrattuale, per cui il paziente potrebbe specificare nel corpo del contratto quali soggetti sono legittimati ad accedere ai dati; l'altra più strettamente tecnologica, per cui, tramite lo *smart contract*, verrebbe stabilito preventivamente e automaticamente che i dati siano resi indisponibili (*digitally locked*) a tutti coloro che non sono stati autorizzati.

4. Sfide e punti deboli

La tecnologia *NFT* viene considerata un esempio di *privacy by design*, un'espressione di recente conio che evidenzia il legame esistente fra tecnologia e privacy, per cui quest'ultima può essere più facilmente salvaguardata se la prima è plasmata in modo funzionale a tale obiettivo. Secondo alcuni autori, il legislatore dovrebbe farsi carico di disciplinare il *design*

[14] Il termine compare per la prima volta nel 2009 nel quadro di ISO/TS 25237:2008, relativo all'informatica nel settore sanitario. Si definisce in modo più tecnico come il "*processo per il quale i dati perdono il loro carattere nominativo*".

[15] I. RUBINSTEIN, W. HARTZOG, *Anonymization and Risk*, 91(2) Wash L. Rev. 703, 2016.

[16] Corte di Giustizia dell'Unione Europea, *Schrems II*, C-311/18, 16 luglio 2020, in curia.europa.eu.

delle nuove tecnologie, in quanto esso può svolgere un ruolo importante nella prevenzione delle violazioni della privacy[17].

Tramite l'utilizzo degli *NFT*, i dati sanitari potrebbero essere caricati su una *blockchain* pubblica come distinti e "originali" da parte degli istituti sanitari, tenuti a registrare ogni diagnosi o prescrizione relativa ai pazienti. In questo modo, il dato sanitario crittografato potrebbe essere accessibile esclusivamente ai soggetti esplicitamente autorizzati tramite uno *smart contract*.

In particolare, lo schema teorizzato prevede l'utilizzo della *blockchain* e degli *smart contract* da parte del paziente per acconsentire proattivamente (*prosent*) e in modo pseudonimo al trattamento dei dati per determinati usi. I pazienti potrebbero in questo modo specificare anticipatamente con quali soggetti accettano di condividere i propri dati, senza necessità di acconsentire ad ogni transazione: ciò garantirebbe un maggiore controllo sui dati stessi e la possibilità di effettuare scambi tempestivi ed efficaci[18].

Tuttavia, questa tecnologia non previene necessariamente ogni *data breach* perché le informazioni digitali contenute nella *blockchain* sono solamente i metadati di cui viene garantita l'integrità, la provenienza e i termini dei precedenti trasferimenti. Al contrario, i sottostanti dati sanitari non godono dello stesso livello di protezione, in quanto la loro tutela dipende dall'adozione di adeguati sistemi di *digital security* e in particolare di crittografia.

Inoltre, l'utilizzo della *blockchain* porta con sé una serie di questioni di carattere etico e giuridico legate alla possibilità di esercitare il diritto di cancellazione e quello di rettifica dei dati personali inesatti. Come noto, il regolamento in tema di protezione dei dati personali garantisce entrambi i diritti agli interessati (artt. 16 e 17 Regolamento UE/2016/679), ma questa previsione mal si concilia con la natura immutabile ed immodificabile della *blockchain*.

Come anticipato, l'uso degli *NFT* dovrebbe garantire la pseudonimizzazione dei pazienti, tuttavia solo pochi elementi basterebbero per la loro reidentificazione: infatti, i dati sanitari sono talvolta così particolari da poter essere paragonati a "impronte digitali" del soggetto.

---

[17] W. HARTZOG, *Privacy's Blueprint: The Battle to Control the Design of New Technologies (Introduction)*, Harvard University Press, 2018.

[18] *Ibidem.*

Per raggiungere l'obiettivo di pseudonimizzazione la crittografia svolge un ruolo essenziale, in particolare grazie alle funzioni *hash*.

5. Conclusioni

Alla luce delle considerazioni svolte, la tutela e il trasferimento dei dati personali sanitari si confermano essere due aspetti centrali e attuali, ampiamente ricompresi nella sfera d'azione delle istituzioni europee.

L'Unione europea ha messo in atto una precisa strategia digitale[19], da cui nel 2020 è scaturita una proposta di regolamento, il *Data governance act*[20], il cui presupposto è la constatazione che i dati sono una risorsa essenziale per la crescita economica, per lo sviluppo della società e per l'innovazione; infatti, le applicazioni *data driven* possono avere benefici per gli utenti in vari settori, fra cui quello sanitario.

Sulla scia di tale iniziativa legislativa, nel febbraio 2022 la Commissione europea ha presentato un'altra proposta di regolamento, il *Data act*[21], con l'intento di armonizzare la normativa in tema di accesso e utilizzo dei dati. In concreto, la riforma è volta alla creazione di infrastrutture comuni e di *data spaces* per ciascun settore di interesse, con l'obiettivo di agevolare la disponibilità e la circolazione dei dati, in sicurezza e nel rispetto della cornice normativa europea.

All'interno di questo contesto politico e normativo, la tecnologia *blockchain-NFT* potrebbe rappresentare una delle infrastrutture che il legislatore europeo mira a costruire per facilitare il trasferimento dei dati, così da permettere agli utenti di partecipare alle vicende circolatorie dei dati che li riguardano. Anche le amministrazioni pubbliche nazionali potrebbero beneficiare di tali strumenti innovativi e, di conseguenza, il sistema sanitario nel complesso ne gioverebbe.

---

[19] Commissione europea in digital-strategy.ec.europa.eu.

[20] Commissione europea, Regolamento del Parlamento e del Consiglio relativo alla *governance* europea dei dati, 25.11.2020, COM(2020) 767 final in eur-lex.europa.eu.

[21] Commissione europea, 23.2.2022, COM(2022) 68 final, Regolamento del Parlamento e del Consiglio sull'armonizzazione delle regole di accesso e utilizzo dei dati in digital-strategy.ec.europa.eu/en/policies/data-act.

A fronte delle riflessioni elaborate, si intravede all'orizzonte un ideale clima di rinnovamento che potrebbe rivoluzionare la gestione dei dati sanitari e il relativo *background* giuridico.