dirittoesalute
Rivista di sanità e responsabilità medica

La sanità del futuro tra tecnologie e privacy.

di Emilia Giusti*

Abstract IT: Il lavoro affronta il delicato tema del diritto sanitario, nell'ambito dei servizi pubblici essenziali e dell'intervento dello Stato in settori di mercato ad alto impatto valoriale, che in questi mesi sta guardando ad un cambiamento che introduce nuovi sistemi o applicazioni tecnologiche per controllare e gestire i dati del paziente salvaguardando comunque i limiti ed i doveri imposti dalla legge sulla privacy.
Si affronterà la possibilità di far ricorso a sistemi alternativi come la blockchain per guardare al futuro del sistema sanitario e per arrivare a conseguire l'interoperabilità tra i dati personali anche alla luce del dilemma tra importanza del dato per la crescita economica e tutela della persona.

Abstract EN: The paper deals with the delicate topic of health law, in the context of essential public services and the intervention of the state in market sectors with a high value impact, which in recent months is looking at a change that introduces new systems or technological applications to control and manage patient data while still safeguarding the limits and duties imposed by privacy law.
The possibility of using alternative systems such as blockchain to look to the future of the healthcare system and to achieve interoperability between personal data will be addressed, also in the light of the dilemma between the importance of data for economic growth and the protection of the individual.

Sommario: 1. Il diritto dei servizi pubblici e la privacy nella sanità di oggi. – 1.1. La responsabilità da utilizzo di nuove tecnologie e la gestione dei dati personali relativi alla salute. – 2. La gestione del dato personale relativo alla salute: dal fascicolo sanitario elettronico alle applicazioni tecnologiche per la salvaguardia

* Assegnista di ricerca, Scuola Superiore Sant'Anna.

della salute. – 3. La blockchain ed i suoi utilizzi. – 4. La Blockchain e la gestione dei dati personali relativi alla salute. – 5. Conclusioni.

1. Il diritto dei servizi pubblici e la privacy nella sanità di oggi.

I servizi pubblici essenziali, come servizi di interesse economico generale, che rappresentano una forma di partecipazione dello stato all'economia, stanno vedendo una accresciuta complessità nelle nuove tecnologie in linea con la digitalizzazione della pubblica amministrazione in un tentativo di semplificazione[1].

La digitalizzazione della pubblica amministrazione importa infatti una modifica sia negli aspetti riguardanti il regime giuridico di espletamento dell'attività sia nei profili giuridico-organizzativi legati alle attività medesime.

Il legislatore nel regolare anche in funzione propulsiva il processo di digitalizzazione dimostra un approccio economico al problema che valorizza le informazioni come risorsa essenziale per la crescita economica, la creazione di posti di lavoro e il progresso sociale.

Uno degli ambiti che hanno visto un accresciuto impatto della digitalizzazione nella erogazione del servizio è quello sanitario.

Si tratta allora di analizzare l'impatto delle nuove tecnologie sul servizio sanitario pubblico e le sfide che esso propone accentuando la dimensione di gestione del rischio nel sistema dei servizi pubblici essenziali che non devono perdere di vista i valori fondamentali cui sono improntati. È una prospettiva che, come anche dimostrato dagli strumenti attuativi del PNRR, fa perno sulla centralità della condivisione del patrimonio informativo pubblico come contributo essenziale per la trasformazione digitale dell'economia, dell'industria e della società europee.

Abbiamo vissuto e stiamo vivendo in questi anni il succedersi di leggi e decreti-legge che hanno cercato di riordinare la materia sanitaria.

Volendo fare un veloce excursus sulla materia medica potremmo sintetizzare così: siamo passati da un diritto alla cura che si concretizza in quell'intervento del medico, detentore dell'ars medica, a cui ci affidiamo e diamo fiducia per curarci nel migliore dei modi ad un diritto alla migliore cura in cui quell'affidamento, che è sempre stata alla base del rapporto tra medico e paziente, manca.

Dalla famosa sentenza della Cassazione, 22 gennaio 1999, n. 589[2] che introduceva la tesi per tanto tempo seguita, della responsabilità da "contatto

---

[1] Da ultimo L. TORCHIA, *Lo Stato digitale. Un'introduzione.* Bologna, 2023 in particolare capitolo 6.

[2] R. MATTEIS, *La responsabilità medica tra* scientia iuris *e regole di formazione giurisprudenziale – commento*, in *Danno e Resp.*, 1999, 7, 777, R. DE MATTEIS, *La responsabilità medica. Un sottosistema della responsabilità civile*, Padova, 1995, 1 e ss., V. ROPPO*, La responsabilità civile dell'impresa nel settore*

sociale" per cui anche in assenza di contratto si sarebbe applicata la responsabilità contrattuale tra il medico ed il paziente, siamo arrivati alla legge Gelli Bianco che ribaltando di nuovo gli schemi, ha reintrodotto la tanto sofferta responsabilità extracontrattuale tra il medico ed il paziente. Nel mezzo tra queste due visioni della responsabilità civile del medico, ricordiamo la legge Balduzzi[3] (legge 189/2012) che con il suo art.3, norma di difficile decifratura, più che risolvere i problemi delle contenzioni in materia medica ha aggiunto quesiti sul come dovesse essere giudicato l'agire del medico avanti ad un ricorso del paziente. Nel testo, infatti, è stato previsto che nel caso in cui l'esercente la professione sanitaria durante lo svolgimento della propria attività si fosse attenuto alle linee guida e buone pratiche accreditate dalla comunità scientifica non avrebbe risposto penalmente per colpa lieve. In tali casi restava fermo l'obbligo di cui all'art. 2043 del Codice civile. Il giudice anche nella determinazione del risarcimento del danno, avrebbe dovuto tenere debitamente conto della condotta di cui al primo periodo.
Questo articolo ha comportato il generarsi di una giurisprudenza assai contrastante tra chi riteneva che il richiamo fatto al 2043[4] del c.c. fosse solo legato al singolo caso di colpa lieve, nonostante il medico si fosse attenuto alle linee guida e buone pratiche, e chi invece considerava questo richiamo come il

dei servizi innovativi, in *Contratto e Impresa*, 1993, 89; C. CASTRONOVO *L'obbligazione senza prestazione ai confini tra contratto e torto*, in Scritti in onore di Luigi Mengoni, I, Le ragioni del diritto, Milano, 197 (dall'estratto) nel risalto conferito al vincolo, che si crea tra medico e paziente in virtù di quegli obblighi di cura al medico imposti dall'arte che professa, la cui violazione si configura *come culpa in non faciendo* dando origine a responsabilità contrattuale; E. GUERINONI, *Obbligazione da contatto sociale e responsabilità contrattuale nei confronti del terzo – il commento*, in Contratti, 1999, 11, 999; V. CARBONE, *La responsabilità del medico ospedaliero come responsabilità da contatto* in *Resp. civ. prev.*, 1999, 661 ss.

[3] A. QUERCI, *Le evoluzioni della responsabilità sanitaria, fra riforma Balduzzi, disegni di legge e novità giurisprudenziali*, in *Nuova Giur. Civ.*, 2014, 1, 20015; V. CARBONE, *La responsabilità del medico pubblico dopo la legge Balduzzi*, in *Danno e resp.*, 2013, IV, 392; L. CAJAZZO, M. MARZANO *La rilevanza delle linee guida nella valutazione della responsabilità professionale del medico e le novità della legge Balduzzi* – il commento in *Corriere Giur.*, 2013, 4, 479 (nota a sentenza); L. MATTINA, *Legge Balduzzi : diventa extracontrattuale la responsabilità del medico?* in *Danno e Resp.*, 2015, 1, 47; A. QUERCI, *Le evoluzioni della responsabilità sanitaria, fra Riforma Balduzzi e novità giurisprudenziali*, in *Nuova giur. civ. comm.*, 2014, II, 15; B. GRAZZINI, *Responsabilità dell'esercente le professioni sanitarie e rischio clinico nel c.d. «Decreto Balduzzi»,* cit., 1239-1240; S. ZAAMI, V. FINESCHI FRATI, M. GULINO, G. MONTANARI VERGALLO, *La riforma legislativa della responsabilità sanitaria e le prime applicazioni giurisprudenziali. Se vogliamo che tutto rimanga come è, bisogna che tutto cambi,* in *Resp. civ. prev.*, 2013, 1055.

[4] C. SCOGNAMIGLIO, *La natura della responsabilità del medico inserito in una struttura ospedaliera nel vigore della L. n. 189/2012,* in *Resp. civ. prev.*, 2013, F. GIARDINA, *Responsabilità contrattuale ed extracontrattuale: una distinzione attuale?* in *Riv. Crit. Dir. priv.*, 1987, 79 e ora, *Responsabilità contrattuale e responsabilità extracontrattuale (significato attuale di una distribuzione tradizionale)* Milano, 1993; D. MARCELLO, *Prestazione sanitaria e responsabilità civile, Il foro Napoletano*, Quaderni 35, Edizione Scientifiche italiane, 2019.

presupposto unico ed esclusivo di un cambiamento per cui, in assenza di un contratto, il paziente avrebbe potuto richiedere il risarcimento solo attraverso l'azione aquiliana. Questa legge è superata, del testo conserviamo il richiamo e l'introduzione alle linee guida ed alle buone pratiche ospedaliere che per la sempre più sensibile coscienza sociale sono divenuti un argomento costante nelle decisioni dei tribunali e nella dottrina di oggi.
In conclusione, possiamo affermare che nonostante gli sforzi del legislatore ancora non si è trovata un punto fermo nel sistema legislativo sanitario anche perché al quesito sulla natura della responsabilità del professionista e dell'ente ospedaliero si è aggiunto anche il quesito della natura della responsabilità da nuova tecnologia, da uso dei software, dei programmi e dei robot introdotti nell'ambito della cura ma soprattutto si è aggiunta la responsabilità nella gestione dei dati personali dei pazienti relativi alla salute, argomento nuovo e in larga diffusione.

1.1 La responsabilità da utilizzo di nuove tecnologie e la gestione dei dati personali relativi alla salute.

Sulla responsabilità derivante dall'uso delle nuove tecnologie la dottrina[5] ha scritto ipotizzando alternative come quella di pensare ad un criterio di valutazione facendo riferimento all'autonomia dell'intelligenza artificiale, della tecnologia, cercando di individuare il quantum di apporto dell'essere umano: quando è minimo e quindi l'agire dell'intelligenza artificiale è del tutto autonomo, anche nei suoi aggiornamenti, quando invece l'intervento dell'uomo è imprescindibile. Nell'analizzare la responsabilità da utilizzo di intelligenza artificiale, tecnologia, in campo medico, è stato fatto riferimento all'art. 2050 del c.c.[6], e quindi una responsabilità per l'esercizio di attività pericolose, anche se risulta imprescindibile capire se un caso come quello di un'intelligenza artificiale che si concretizza nell'utilizzo di un programma di calcolo come quelli prima esposti, possa essere considerato alla stregua di un'attività pericolosa[7] considerando anche che l'attività di questi programmi, il più delle volte, è quella

---

[5] E. GIUSTI, *Intelligenza artificiale e sistema sanitario, in Il ragionamento giuridico nell'era dell'intelligenza artificiale*, (a cura di) S. Dorigo, Pacini Giuridica, 2018, 309 e ss.
[6] G. MORANO, *Robotizzazione, intelligenza artificiale e P.A.* in www.neldiritto.it.
[7] M. TOPI, *Attività pericolose atipiche ex art. 2050 c.c.,* in *D&R*, 2016, 2, 155, nota a sentenza Cass., 29 luglio 2015, n. 16052. L'autore ha descritto l'iter laborioso che ha investito la definizione di "attività pericola. Elaborata inizialmente una tesi restrittiva tanto che inizialmente erano considerate pericolose solo le attività previste nel testo unico delle leggi di pubblica sicurezza, quelle aventi per scopo la prevenzione dei sinistri ed infortuni o per la tutela della pubblica incolumità, si è passati per mezzo dell'intervento della giurisprudenza a considerare pericolose anche quelle attività con una pericolosità intrinseca per loro natura o per i mezzi adoperati. Cfr. COMPORTI, *Esposizione al pericolo e responsabilità civile*, Napoli, 1965, 296; M. FRANZONI, *Il danno da attività pericolose nella giurisprudenza*, in *CI,* 1985, 180.

di far diagnosi, così come già fa il medico. Se l'errore fosse provocato da un cattivo funzionamento del programma si potrebbe anche ipotizzare di applicare le regole previste dal codice del consumo per responsabilità da prodotto difettoso e quindi rivalersi sul produttore o sul fornitore. Diversamente a quanto sopra, un'altra soluzione per individuare la responsabilità nell'uso dell'intelligenza artificiale, della tecnologia, potrebbe essere quella di considerare solo la diagnosi finale e quindi da chi quella diagnosi è stata firmata, un po' come succede in campo ingegneristico avanti alle grandi opere. Quando un ingegnere si serve, infatti, di un programma di calcolo strutturale questo stesso programma, con i dati a diposizione fornisce dei risultati attraverso i quali, il professionista prende una decisione e sottoscrive la decisione, addossandosene la colpa in caso di errore. Potrebbe quindi essere una responsabilità del professionista, a prescindere dalla macchina, dal suo proprietario o dal suo produttore.

Oltre al problema, quindi, su come inquadrare la natura di questa responsabilità, sussiste anche il quesito su come gestire i dati personali relativi alla salute delle persone in gran uso con le applicazioni tecnologiche.

Se, infatti, prima la privacy poteva essere considerata solo nella sua accezione statica e quindi nel non varcare la soglia dell'intimità familiare, personale, oggi di privacy vediamo una versione più dinamica che non si arresta al solo cercare di proteggere da accessi esterni ma anche di preservare le informazioni sensibili o meno della persona, nel decidere cosa è corretto che possa essere utilizzato e cose invece debba essere precluso agli estranei, in un costante desiderio di decidere noi e solo noi cosa mostrare di noi stessi. [8]

Con l'avvento del Codice della privacy del 2003 ma ancora di più con il regolamento UE 679 del 2016 ed il d.lgs. n. 101 del 2018 che armonizzerà le norme italiane alle novità europee, i dati personali, sono tornati ad essere oggetto di massima attenzione non solo nelle pronunce dei tribunali ma anche del Garante per la privacy che con i suoi richiami e le sue sanzioni ha, più volte statuito su numerose situazioni in cui, l'utilizzo del dato ancora di più quello sanitario risultava non essere poi così tanto lecito.

I dati sanitari sono parte di quella categoria che è stata definita dei c.d. "dati sensibili"[9], o "categorie particolari di dati" che godono di una speciale

[8] Si parla di "reinvenzione della privacy", S. RODOTÀ, *Il diritto di avere diritti*, 319; A.R. POPOLI, *Social Network e concreta protezione dei dati sensibili: luci ed ombre di una difficile convivenza*, in *Dir. Inf.,* 2014, p.981 e ss.; S. KOKOLAIS, *Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon*, in *Computer and Security,* 2017, p.122. Nella nostra letteratura questa dicotomia si chiama "paradosso della privacy per cui le preoccupazioni degli utenti non sembrano riguardare il loro comportamento on line, sul punto v. A. VIVARELLI, *Il consenso al trattamento dei dati personali nell'era digitale*, in *Il Foro Napoletano*, Quaderni 33, Edizioni Scientifiche Italiane, 2019, 125 e ss.

[9] F. CAGGIA, *Il trattamento dei dati personali sulla salute con particolare riferimento all'ambito sanitario*, in V. CUFFARO, R. D'ORAZIO, E V. RICCIUTO, *Il codice del trattamento dei dati personali*, Torino,

protezione da parte del Regolamento. Il reg. UE n. 679/2016, infatti, definisce i "dati relativi alla salute" come quei dati di una persona fisica in grado di rilevare "informazioni relative al suo stato di salute" (art. 4, n.15, GDPR).[10]
C'è una maggiore limitazione alla liceità di trattamento[11] di tali dati che sono ricompresi ed elencati nell'art. 9 come: «dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute, i dati relativi alla vita sessuale o all'orientamento sessuale della persona". Si tratta dunque di dati personali che meritano una specifica protezione perché, per loro natura, sono particolarmente sensibili sotto il profilo dei diritti e delle libertà fondamentali, «dal momento che il contesto del loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali».
La domanda, quindi, non potrà che essere quella di come riuscire a tutelare queste informazioni e come riuscire a gestirle, in quanto vi è chi ha contestato "l'idea che la persona eserciti un diritto di proprietà sui propri dati e ne possa disporre liberamente: la dimensione digitale è un prolungamento della dimensione umana, e come alla persona non si consente di alienare parti del proprio corpo che potrebbero comprometterne la funzionalità, allo stesso modo si dovrebbe proibire la cessione volontaria di dati personali che sono particolarmente sensibili. I diritti fondamentali sono indisponibili, sì che la cessione di dati che potrebbero essere utilizzati per procurare danno alla persona non dovrebbe essere consentita, neppure se vi fosse il consenso dell'interessato.".[12]
Alla regola generale, infatti, che vieta il trattamento dei dati c.d. sensibili, hanno fatto seguito, nel GDPR, tutta una serie di eccezioni molto ampie per cui tali categorie di dati possono essere trattati senza autorizzazione purché conformi

---

2007, p.407 e ss. Il Gruppo di lavoro Articolo 29, *Advice paper on special categories of data ("sensitive data"),* 20 aprile 2011, p.10 "*health-related …represents one of the most complex areas of sensitive data one where the member States display a great deal of legal uncertainty".* Il Gruppo di Lavoro Articolo 29, organismo europeo indipendente, si è occupato fino al maggio 2018 della privacy e dei dati personali. È stato oggi sostituito dal Comitato Europeo per la protezione die dati, ex art.68 e ss GDPR.

[10] Il considerando n.35 del GDPR integra tale nozione specificando che sono "dati personali relativi alla salute tutti quelli inerenti lo stato di salute dell'interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso".

[11] D. MESSINETTI, *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *Riv. crit. dir.priv.,* 1998, p.350., R. PANETTA, *Libera circolazione e protezione dei dati personali*, vol. I, Milano 2003, 504., V. CUFFARO, V. RICCIUTO, V. ZENO-ZENCOVICH, *Trattamento dei dati e tutela della persona,* Milano, 1998, 124 e ss., M.G. STANZIONE, *Il Regolamento europeo sulla privacy: origini e ambito di applicazione,* in *Eur. dir. priv.,* 2016,4, p.1249 e ss.

[12] G. CONTE, A. FUSARO, A. SOMA, V. ZENO-ZENCOVICH, *Dialoghi con Guido Alpa, un volume offerto in occasione del suo LXXI compleanno*, Collana l'unità del diritto, Roma Tre Press 2018, 353, 633.; N. IRTI, *La crisi della fattispecie in Un diritto incalcolabile*, Torino, Giappichelli, 2016, 19 e ss.

ai principi di proporzionalità e di necessità. Ciò accade: quando sussiste un interesse pubblico (art 9, par. 2, lett. g, GDP), per un fine terapeutico (par.2, lett. *h*), avanti ad un interesse generale alla salute collettiva (par.2, lett. *i*) per la ricerca scientifica (par.2, lett.j), esigenze di medicina preventiva o medicina del lavoro, di assistenza o terapia sanitaria, di gestione dei servizi sanitari, nonché motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati Membri.

Al di fuori di queste ipotesi la regola sarà quella del consenso[13] per governare il trattamento dei dati che dovrà essere chiaro, esplicito, libero, informato ed espresso attraverso una dichiarazione o un'azione positiva inequivocabile. All'interessato rimarrà comunque sempre possibile accedere ai propri dati (art.15) rettificarli (art.16), limitare il trattamento da parte del titolare (art.18), opporsi al trattamento (art.21) e proporre reclamo al garante o adire le sedi giudiziarie opportune (artt.77 e ss.) infine ed in via residuale potrà chiederne la cancellazione e la portabilità dei dati, nonostante l'applicabilità in ambito sanitario di queste ultime alternative sia discussa.

Il diritto alla cancellazione del dato[14], infatti, al pari della portabilità, in ambito sanitario, sembra trovare delle difficoltà in quanto non sarebbe evocabile avanti ad un interesse generale nel settore della sanità pubblica. Per cercare di ovviare è stato quindi proposto, a coloro che richiedono la cancellazione dei dati anche per evitare accessi ingiustificati, di far ricorso ad un diritto di opposizione, ad un diritto all'oscuramento così come previsto dall'art. 52 del d.lg.196 del 2003, che prevede la possibilità di oscuramento, su istanza di parte o d'ufficio, delle generalità o altri identificativi del medesimo interessato che siano stati riportati sulla sentenza o provvedimento, oppure di far ricorso all'utilizzo di tecniche di anonimizzazione o pseudonimizzazione del dato strettamente sanitario, così da

---

[13] È interessante l'analisi svolta da dottrina recente sul consenso in ambito di privacy. È stata infatti messa in luce la sua natura suppletiva rispetto al suo ruolo nella cura. Infatti, nel dato "il consenso sarà determinante per quelle finalità non prettamente mediche a quanto avviene nei social network o nei contratti digitali ove i dati personali sono oggetto di scambio fra utente e fornitore del servizio" v. M. CIANCIMINO, *Protezione e controllo dei dati in ambito sanitario e intelligenza artificiale*, in *Quaderni della Rassegna di diritto civile* diretta da P. PERLINGIERI, Edizioni Scientifiche Italiane, 40 e ss.; A.FICI E E. PELLECCHIA, *Il consenso al trattamento*, in R. PARDOLESI, *Diritto alla riservatezza e circolazione dei dati personali*, Vol. I, Milano, 2003, 504 e ss., G. OPPO, Sul consenso dell'interessato, in V. CUFFARO, V. RICCIUTO, V. ZENO-ZENCOVICH, *Trattamento dei dati e tutela della persona*, Milano, 1998, 124 e ss., S. NIGER, *Il mito del consenso alla luce del codice in materia di protezione dei dati personali,* in *Cyberspazio e diritto*, 2005,4, p.499 ss.

[14] G. FINOCCHIARIO, *Il diritto all'oblio nel quadro dei diritti della personalità*, in G. RESTA E V. ZENO ZENCOVICH, *Il diritto all'oblio su internet dopo la sentenza Google Spain, Roma,* 2015, 29, A. PALLADINO, "*Oblio 4.0" tra identità digitale e cancellazione dati: quale diritto?* in *De industria*, 2, 2019, p.85; G. CARAPEZZA FIGLIA, *Tutela dell'onore e libertà di espressione. Alla ricerca di un giusto equilibrio nel dialogo tra la Corte europea dei diritti dell'uomo e giurisprudenza nazionale*, *in dialogo tra Corte europea dei diritti dell'uomo e giurisprudenza nazionale,* in *Dir. fam. Pers., 2013, p.1028 e ss.*

far rimanere la memoria degli interventi effettuati ma con i dati del singolo inaccessibili. Si può fare ricorso a tecniche di criptografia così da rendere i dati accessibili esclusivamente dietro specifiche autorizzazioni in ossequio al principio di continenza e di minimizzazione dell'utilizzo di tali dati.

2. La gestione del dato personale relativo alla salute: dal fascicolo sanitario elettronico alle applicazioni per la salute.

Un aspetto importante del tema riguarda l'uso del fascicolo sanitario elettronico e dossier medico: il primo risale al d.l. 18 ottobre 2012 n. 179, art. 12[15] e nasce come strumento informatico che può essere attivato dal cittadino ed al cui interno possono confluire tutte le informazioni sanitarie che descrivono la salute della persona (dagli esami alle terapie.); il secondo invece (DSE) è una tipologia di documentazione in formato digitale che registra gli eventi clinici occorsi all'interessato ma in riferimento alla singola struttura sanitaria.

L'utilizzo che dovrebbe essere tratto, principalmente, dall'uso del fascicolo sanitario elettronico[16] risiede nella sua possibilità di concedere una interoperabilità dei dati contenuti tra le strutture ed i medici dell'intera nazione. Il Fascicolo Sanitario Elettronico è stato, infatti, tra le prime manifestazioni della cultura *e-Health*[17] in Italia con la quale si è progettata un'architettura al completo servizio dell'interazione tra i professionisti della salute – tra il medico o pediatra di famiglia e il medico specialista – e tra il cittadino e il medico.

---

[15] *V.* Regolamento in materia di fascicolo sanitario elettronico, D.P.C.M. 29 settembre 2015, n.178 ed il decreto del Ministero dell'Economia e delle Finanze, *Modalità tecniche e servizi telematici resi disponibili dall'infrastruttura nazionale per l'interoperabilità del Fascicolo Sanitario Elettronico*, del 4 agosto 2017, modificato con d.m. del 25 ottobre 2018. L'art.11 del d.l. 19 maggio 2020, n.34 ha da ultimo previso delle novità in tema di FSE per migliorare l'effettiva fruibilità e la tutela della riservatezza dei dati ivi previsti per poi raggiungere la realizzazione del Portale Nazionale FSE. V. a riguardo, G. COMANDÉ, L. NOCCO e V. PEIGNÉ, *Il fascicolo sanitario elettronico: uno studio multidisciplinare*, in *Riv. It. Med.leg.*, 2012, p.105 ss., P. GUARDA, *Fasciolo sanitario elettronico e protezione dei dati personali,* Trento, 2011.

[16] G. COMANDÉ, *Circolazione elettronica dei dati sanitari e regolazione settoriale: spunti ricostruttivi su "interferenze sistemtiche"* in AA. VV., *Studi in onore di Davide Messinetti,* Edizioni scientifiche Italiane, 2008, 279.; C.C. GIARDINA, *Il fascicolo sanitario elettronico tra norme e prassi*, in *Aziend'Italia,* 2021, 12, 2043.

[17] L. RUFO, *Il Dossier sanitario elettronico*, Il Mulino, 2018; G. EYSENBACH, *What is e-health*?, J Med Internet Res 2001 - vedi sito http://www.jmir.org/2001/2/e20/ (ultima consultazione giugno 2017) in cui si scrive che l'eHealth è un settore emergente interdisciplinare tra informatica medica, salute pubblica e affari, con riferimento ai servizi sanitari e le informazioni distribuite o elaborate attraverso Internet e le tecnologie correlate. In un senso più ampio, il termine caratterizza non solo lo sviluppo tecnologico, ma anche una scuola di pensiero, un modo di pensare, un atteggiamento, e un impegno al pensiero globale in rete, al fine di migliorare l'assistenza sanitaria a livello locale, regionale, e mondiale utilizzando le tecnologie dell'informazione e della comunicazione.

È un insieme di dati e documenti digitali di tipo sanitario e sociosanitario generati da eventi clinici, riguardanti l'assistito, riferiti a prestazioni erogate dal Servizio Sanitario Nazionale (SSN) e, a partire dal 19 maggio 2020, anche da strutture sanitarie private.
È lo strumento attraverso il quale il cittadino può tracciare, consultare e condividere la propria storia sanitaria. La norma stabilisce che l'infrastruttura del FSE gestisca l'insieme dei dati e dei documenti digitali di tipo sanitario e sociosanitario generati da eventi clinici presenti e trascorsi riguardanti l'assistito.
Le informazioni contenute nel Fascicolo sanitario elettronico sono disciplinate dal D.P.C.M. 29 settembre 2015, n. 178, Regolamento in materia di fascicolo sanitario elettronico, e vengono distinte tra: una parte essenziale delle informazioni e una parte correlata all'autonomia delle Regioni.
Il D.P.C.M. 29 settembre 2015, n. 178 stabilisce che ciascuna regione e provincia autonoma deve istituire il Fascicolo Sanitario Elettronico (FSE) attraverso una infrastruttura tecnologica capace di interoperare con le altre soluzioni regionali di FSE, esponendo opportuni servizi che consentono la realizzazione di una serie di processi interregionali. I servizi di interoperabilità permettono di effettuare le operazioni di ricerca, recupero, registrazione, cancellazione di documenti e trasferimento indice del FSE.
Con la conversione in Legge del Decreto Rilancio (D.L. n. 34/2020 convertito con modificazioni dalla Legge 17 luglio 2020, n. 77) sono state apportate diverse novità rilevanti per il Fascicolo Sanitario Elettronico. In particolare, sono state estese le "funzioni di sussidiarietà" dell'Infrastruttura Nazionale per l'Interoperabilità dei Fascicoli Sanitari Elettronici (INI) a tutte le regioni che non hanno ancora attivato il FSE o alcuni suoi servizi e il potenziamento di INI. Nel tempo il FSE potrà essere alimentato attraverso l'Infrastruttura Nazionale per l'Interoperabilità con i dati sanitari già disponibili in merito alla donazione degli organi, le vaccinazioni e le prenotazioni, contenuti nel Sistema Informativo Trapianti, nelle Anagrafi vaccinali regionali e nei CUP di ciascuna regione o provincia autonoma.
Rimane al centro sempre il controllo da parte del cittadino che può: scegliere a chi far consultare il suo fascicolo, aggiornare i propri dati identificativi, decidere quali informazioni mostrare o oscurare ai medici che debbano accedevi, verificare chi e quando lo abbiano esaminato.
Accanto a tale requisito il desiderio, soprattutto degli ultimi tempi ed anche a livello europeo di riuscire, attraverso il meccanismo della portabilità del dato, art. 20 GDPR, di far interagire non solo il fascicolo sanitario elettronico tra una regione e l'altra ma anche con dispositivi ed applicazioni con finalità latamente mediche o di monitoraggio della salute e viceversa. Si segnala a tal proposito un indirizzo della commissione europea per la realizzazione di un formato digitale

unico che possa far sì che i dati dei fascicoli sanitari arrivino a circolare tra gli stati membri[18].

Per questo e non solo dal fascicolo sanitario elettronico e dal dossier, sempre per trattare il fenomeno della gestione dei dati relativi alla salute, siamo arrivati alla creazione delle numerose applicazioni che in questi ultimi mesi avanti sempre all'insorgere del virus covid-19 hanno fatto ingresso nel nostro paese introducendo l'esigenza di riflettere sulla sicurezza nella gestione dei dati personali in uso nelle applicazioni tecnologiche.

Per la tracciabilità del virus, per esempio, è stata adottata dal nostro paese l'app Immuni[19], alla quale è stato affidato il monitoraggio dei contagi della penisola italiana. È una app liberamente scaricabile che deve monitorare i contatti avuti dal possessore dello smartphone e, se del caso, avvisare l'utente qualora entri in contatto con un soggetto poi risultato positivo al coronavirus. Da una prima analisi risultava essere un'applicazione in linea con il regolamento per la privacy comunitario in quanto non utilizzava la glocalizzazione ma la tecnologia Bluetooth low energy, i dati venivano eliminati terminata l'emergenza e comunque cifrati per garantire l'anonimato.

Nonostante ciò, non sono mancate le perplessità ed il Garante per la privacy è intervenuto sottolineandone i rischi per la privacy del cittadino e tra questi, il principale: la reidentificazione[20] .

Il rischio di reidentificazione è un rischio ricorrente nelle applicazioni tecnologiche che utilizzino tecniche di anonimizzazione o pseudoanonimizzazione del dato come il sistema appena ricordato. Interessante è un recente documento dell'aprile 2021 dell'Autorità di controllo spagnola (AEPD) e *dell'European Data Protection Supervisor* (EDPS) denominato "*10 misunderstanding related to anonymisation*"[21].

Un altro caso tra le pronunce del Garante per la protezione dei dati da cui continua emergere ancora la problematica della gestione del rischio dell'applicazione in riferimento all'utilizzo dei dati personali relativi alla salute è anche l'utilizzo del codice *QR-code*. Il *Qr-code* è un codice a barre bidimensionale, ossia a matrice, composto da moduli neri disposti all'interno di uno schema bianco di forma quadrata, impiegato in genere per memorizzare informazioni

---

[18] *European commission, Proposal for a Regulation of the european parliament and of the council, on the European Health Data Spac,* Strasbourg, 3.5.2022.

[19] Garante per la protezione dei dati personali, Provvedimento di autorizzazione al trattamento dei dati personali effettuato attraverso il Sistema di allerta Covid 19- App Immuni a seguito dell'aggiornamento della valutazione di impatto effettuata dal Ministero della salute su cui l'Autorità si era espressa con provvedimento del 1° giugno 2020-25 febbraio 2021.

[20] R.M. COLANGELO, *App mediche e protezione dei dati personali. Alcuni spunti giuridici tra Gdpr, codice privacy novellato e chiarimenti del Garante,* in *Autonomie locali e servizi sociali*, fasc.2, agosto 2019, Il Mulino.

[21] edps.europa.eu/data-protection/our-work/publications/papers/aepd-edps-joint-paper-10-misunderstandings-related_en

destinate a essere lette tramite un apposito lettore ottico o anche smartphone. Nell'ultimo periodo è stato forte il ricorso a tale strumento che ha creato nuovi processi comunicativi: dei collegamenti ipertestuali tra il mondo reale e quello online.
Attraverso l'utilizzo dell'applicazione Smart4You nell'Azienda sanitaria unica regionale Marche era possibile, infatti, leggere il Codice QR presente sul talloncino rilasciato a chiunque era stato sottoposto allo screening per il Covid-19 per poter consultare il proprio dossier medico con le cartelle cliniche, le varie prenotazioni ospedaliere e gli esiti.
L'applicazione è risultata, però, vulnerabile nella parte relativa alla gestione dello screening, limitatamente al servizio Screening Covid-19 San Benedetto e la app smart4you connessa con il medesimo screening. Il problema era relativo alla funzione di lettura rapida dell'esito del tampone consegnato ai soli partecipanti alle attività di screening Covid-19 nelle fasi iniziali di accettazione tramite QR-code, generato sequenzialmente e che associava direttamente partecipante-esito tampone. Il QR non era stato elaborato in modo casuale ma in modo progressivo per cui ad ogni numero corrispondeva un utente e cambiando una cifra era così possibile accedere al profilo di un altro. La violazione si era limitata ai soli dati anagrafici e, ove presente, al numero di cellulare del soggetto.
Il rischio per la privacy si sostanziava nella decodifica QR-code e quindi nell' acquisizione dei dati personali della singola persona ed anche in questo caso nell'associazione del dato. L'Azienda veniva richiamata dal Garante per la privacy che si pronunciava il 13 gennaio 2022 e per porre rimedio alle violazioni che stavano accadendo prevedeva che il fornitore NSB modificasse la generazione del QR-code con una codifica più complessa di tipo Hash, composta da una prima parte del codice fiscale unita a una sequenza casuale. Inoltre, sono state escluse la funzionalità di decodifica del codice fiscale con il nominativo degli assistiti regionali, la verifica della coerenza tra numero di cellulare con app smart4you e soggetto interrogato, includendo la possibilità di blocco o di *alert*.
È stata eliminata la funzionalità di sms con riportati il nominativo e gli esiti, *banning* degli indirizzi IP da cui provengono richieste reiterate, registrazioni multiple o richieste con codifiche o account errati.
Questi sono solo due esempi ma potremmo continuare oltre nell'analisi riscontrando quindi come sia davvero difficile gestire in sicurezza i dati personali della persona, ancora di più se legati alla salute.
Così però come non esiste un sistema che in assoluto possa dirsi sicuro ed attendibile, allo stesso modo è anche vero che ormai l'utilizzo del dato non si arresta al singolo esercizio ma va oltre per cui assistiamo anche al c.d. reimpiego[22] del dato, soprattutto in ambito sanitario, in cui è ricorrente e rimane

[22] Le nuove tecnologie dovrebbero essere chiamate tecnologie relazionali o R-technologies, e non più tecnologie informatiche, perché grazie ai nuovi programmi per elaborare è possibile

lecito anche in assenza di consenso ai sensi degli art.5, par.1, lett. b), e 6 par. 4, GDPR, fin tanto che è compatibile con l'uso per cui i dati sono stati ceduti, viceversa ha necessità di un'autorizzazione espressa quando, il reimpiego, sia in concreto incompatibile con l'uso per i quali i dati erano stati raccolti.
Forse l'idea, soprattutto per evitare la perdita, la distruzione dei dati personali o i rischi correlati alle applicazioni, potrebbe essere quella di abbandonare i sistemi utilizzati fino ad ora in ambito sanitario e guardare ad altri mezzi, studiandone le capacità: la blockchain.

3. La Blockchain ed i suoi utilizzi

Un'altra recente innovazione tecnologica che facilita e implementa l'uso del dato è Blockchain. A partire dagli Anni '90 sono stati molti i tentativi per risolvere il problema della "centralizzazione" di Internet, per lo più mediante lo studio di reti "peer-to-peer" (o "alla pari") e della crittografia, ma è solo con il *paper* pubblicato sotto lo pseudonimo Satoshi Nakamoto intitolato « *Bitcoin: A Peer-to-Peer Electronic Cash System* » che si arriva a trattare realmente di un sistema nuovo di pagamento virtuale: la blockchain[23].
Blockchain fa parte delle *distributed ledger Technologies (DLT)* e cioè di quelle tecnologie di registro distribuito e disintermediato peer-to-peer, diverse dalle architetture centralizzate *client-server*, che si basano sul controllo di un'autorità di gestione.
L'idea di uno strumento di pagamento virtuale sorgeva però già nel 1994 quando nacque il *DigiCash*, del servizio realizzato da David Chaum dove era ancora necessario prevedere la presenza di un ente centrale. L'idea di assicurare l'anonimato delle transazioni all'interno delle reti telematiche deriva dal movimento *cypherpunks*, ossia da un gruppo di soggetti (inizialmente costituito da Eric Hughes, Tim May e John Gilmore) che crearono una mailing list sulla quale venivano discussi i temi della privacy e della cifratura dei dati. Nel 1993 venne pubblicato il « *Cypherpunk Manifesto* » [24].
Successivamente, nel 1997, venne proposto *Hashcash* da Back, un modo per evitare il fenomeno dello spam nella posta elettronica, rendendo difficile e caro inviare messaggi non desiderati, mentre nel 1998 Wei Dai pubblicava la sua proposta di *B-money* attraverso cui si passava a descrivere un sistema

---

stabilire reticoli complessi di interconnessioni e di relazioni fra fornitori ed utenti, creando l'opportunità di quantificare e trasformare in merce, sotto forma di relazioni economiche a lungo termine, ogni aspetto dell'esperienza della vita di ciascuno, J. RIFKIN, *L'era dell'accesso,* trad. it., Oscar Mondadori, 2000.

[23] A.M. GAMBINO, C. BOMPREZZI, *Blockchain e protezione dei dati personali*, in *Diritto dell'informazione e dell'informatica, (II)* fasc. 3, 1° giugno 2019, p.619.

[24] M. NICOTRA, F. SARZANA DI S. IPPOLITO, *Diritto della blockchain, intelligenza artificiale e Iot,* Wolters Kluwer, 10, 307; https://www.activism.net/cypherpunk/manifesto.html, visitato il 5 agosto 2018.

decentralizzato di pagamento garantito dalla cifratura e dalla c.d. *"proof of stake* ", ossia dalla spinta dei partecipanti ad agire senza frodi nel network potendo altrimenti perdere i fondi depositati in caso di validazione di transazioni disoneste. Negli stessi anni Nick Szabo propose la definizione di *smart contract* , vale a dire contratti intelligenti capaci di eseguire automaticamente delle transazioni[25].

Nel 2004, Hal Finney teorizza la *proof of work* e nel 2005 Nick Szabo pubblica una proposta con oggetto il *Bitgold* senza porre un limite all'ammontare totale dei *Bitgold* prodotti, conferendo loro un valore diverso a seconda delle capacità computazionali investite per produrli.

Nel 2008 si arriva alla pubblicazione del *paper* di Satoshi Nakamoto in cui viene descritto il funzionamento di Bitcoin ed il 3 gennaio 2009, alla creazione del «*Genesis Block*» ossia del blocco iniziale della Blockchain Bitcoin.

La prima transazione in Bitcoin[26] venne effettuata il 12 gennaio 2009, ed il suo sviluppo è stato esponenziale. Oltre al Bitcoin, ad oggi si contano oltre 1600 *cripto-monete*, o *Alt-Coins (*che sta per "*Alternative Coins*", o "Monete Alternative"). Il vocabolo "*blockchain*" deriva quindi dal fatto che le transazioni vengono cronologicamente ordinate — attraverso dei server di marcatura temporale, o *timestamps* — mediante la divisione in "blocchi", univocamente identificati con una stringa alfanumerica ("*hash*") che risiede in un *header*, che prevede anche l'*hash* del blocco precedente, fino a realizzare una concatenazione di blocchi: da qui "blockchain", che equivale a "catena di blocchi". Ogni tentativo di frode è difficile, in quanto la modifica di ogni *hash* romperebbe la catena, causando il

---

[25] M. NICOTRA, F. SARZANA DI S. IPPOLITO, *Diritto della blockchain, intelligenza artificiale e Iot*, Ipsoa editore, 2018.

[26] Si diche che "il bitcoin, come unità di misura, non ha valore intrinseco, né diretto né indiretto, il suo valore non è legato alla ricchezza economica di una comunità, ma è dato dal volume di scambi con altre valute ed è condizionato dalla domanda e dall'offerta all'interno di un mercato virtuale. Il suo valore non è condizionato da nessun tipo di politica monetaria, non esistendo un ente sovraordinato o una banca centrale a cui sono attribuiti poteri di indirizzo o di intervento sull'emissione e circolazione della moneta; ciò costituisce, da un lato, una caratteristica essenziale ed un punto di forza del bitcoin, che nella sua genesi ha avuto come obiettivo principale la decentralizzazione della politica monetaria attraverso l'eliminazione di banche centrali ed intermediari e, da altro lato, rappresenta anche il suo maggior punto di debolezza essendo il valore del bitcoin rimesso alla volubilità del mercato senza possibilità di correzione e protezione del valore della valuta virtuale attraverso manovre di politica monetaria da parte di una banca centrale. Ciò determina un'elevatissima volatilità del valore (rectius: tasso) della moneta virtuale condizionato esclusivamente dal volume degli scambi, dalla domanda e dall'offerta e dalla fiducia nel sistema o più precisamente nelle piattaforme informatiche che gestiscono gli scambi. Il rischio concreto è che ad una regolamentazione legale da parte di una banca centrale o di altro intermediario finanziario si sostituisca una regolamentazione di fatto da parte di soggetti in grado di alterare le dinamiche della domanda e dell'offerta", così M. KROGH, *Transazioni in valute virtuali e rischi di riciclaggio. Il ruolo del notaio*, in Notariato, 2018, 2, 155 ss., Milano.

modificarsi degli *hash* susseguenti, e si renderebbe visibile per l'evidente contrasto con le altre copie presenti nei restanti nodi (cd "network").[27]
[28]Per descrivere questo sistema è stato fatto ricorso alla metafora di un registro immodificabile le cui copie sono distribuite sui vari nodi della rete. Il registro è organizzato in "blocchi" separati all'interno del quale sussistono degli insiemi di transazioni collegati per formare una "catena" sequenziale marcata temporalmente.
In ciascuno dei blocchi vengono registrate le transazioni - la cui provenienza e destinazione sono verificate tramite l'utilizzo delle chiavi pubbliche crittografiche - insieme ad altre informazioni.
Per proteggere, quindi, la sicurezza ed integrità del sistema Nakamoto, facendo ricorso al concetto di *proof of work*, è stato inserito un meccanismo per rendere difficoltosa la modifica o la cancellazione delle informazioni una volta salvate. La generazione degli *hash*, infatti, non avviene in modo automatico, bensì solo dopo una particolare procedura che richiede l'impiego di risorse computazionali per risolvere un determinato algoritmo matematico. I vari nodi, quindi, sono in competizione tra loro per la generazione di ogni *hash* di chiusura di ciascun blocco della catena, ed il primo che riesce a risolvere tale algoritmo, dando quindi prova di aver utilizzato risorse per giungere a tale scopo (e per tale motivo viene definita "*proof of work*"), comunicherà la soluzione nel network, che verrà verificata dagli altri nodi. [29]
Si distingue tra blockchain[30] di tipo "*permissionless*" e blockchain "*permissioned*". Le principali differenze sono in quattro aspetti: l'identificabilità dei soggetti che ne fanno uso; la modalità di selezione dei nodi e la grandezza del network; le particolarità relative al meccanismo del consenso condiviso; la trasparenza del contenuto dei blocchi.

---

[27] M. BENTIVOGLI - M. CHIRIATTI, *Blockchain: la tecnologia "umanizza" il lavoro,* in ilsole24ore.com, 12 agosto 2018
[28] Ancora M. NICOTRA, F. SARZANA DI S. IPPOLITO, op.cit. Per un'analisi più approfondita della tecnologia si rinvia a: R. GARAVAGLIA, *Tutto su blockchain* , 2018, Hoepli; M.ANDREAS ANTONOPOULOS, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies* , 2015, O 'Reilly; MELANIE SWAN, *Blockchain: blueprint for a new economy* , 2015, O'Reilly.
[29] Nota n. 8 "Tale processo di risoluzione dell'algoritmo matematico è ciò che viene definito "mining ". La risoluzione richiede un approccio per tentativi, nel senso che ciascun nodo tenta di fornire varie soluzioni, in breve lasso di tempo, fino a trovare quella giusta. Il protocollo Bitcoin, inoltre, calibra la difficoltà dell'algoritmo a seconda di quanti sono i partecipanti al network , rendendo più difficoltosa la soluzione in caso di aumento del numero dei partecipanti. Nella Blockchain Bitcoin il nodo che per primo risolve il problema matematico riceve inoltre un quantitativo di bitcoin in premio, quale incentivazione alla partecipazione attiva al network . tale premio è decrescente nel tempo ed allo stato attuale, con l'ampia diffusione che ha avuto Bitcoin, è quasi impossibile riuscire a "minare" un blocco con un hardware non specializzato." in F. SARZANA DI S. IPPOLITO E M. NICOTRA,op. cit.
[30] M. BELLINI, *Blockchain & Bitcoin* , 2018, *Milano Finanza*, 41 ss.

Altra distinzione è che nella blockchain *permissionless* (come ad esempio Bitcoin) in cui ciascuno può entrare a far parte del network, ed ogni computer può essere un nodo. In questo modo il network può crescere e rendere quindi il meccanismo del consenso di queste blokchain immutabili, essendo impossibile per la quantità di partecipanti ogni forma di modifica.
Nelle blockchain *permissioned,* viceversa, vi è una maggiore centralizzazione, perché un'entità centrale ha l'autorità di determinare chi può accedervi, dietro pre-identificazione. Il fatto che le identità che si celano dietro i nodi siano conosciute e che gli accessi siano controllati diminuisce il livello di immutabilità, posto che in astratto il raggiungimento della maggioranza necessaria per apportare cambiamenti è più semplice. Anche la trasparenza può essere diminuita, potendo escludere determinati nodi dalla visione integrale della blockchain. Vi sono poi le blockchain private e quelle pubbliche in cui quelle pubbliche non sono gestite da nessuno mentre quelle private si rifanno ad una singola persona tanto da essere descritte da Vitalik Buterin, colui che ha fondato Ethereum come "poco più di un sistema centralizzato tradizionale"[31].
Sintetizzando è possibile affermare che le caratteristiche delle tecnologie basate su registri distribuiti (*distributed ledger technologies o DLT*) e, in particolare, della blockchain[32] risiedono in: disintermediazione, decentralizzazione, distribuzione e vocazione transnazionale; immutabilità, inalterabilità e persistenza dei dati, meccanismo distribuito peer-to-peer di consenso, fiducia e incentivazione; trasparenza, tracciabilità e sicurezza; funzioni di hash (pseudonimizzazione), validazione temporale e crittografia asimmetrica.
Operare su un'infrastruttura del genere consente non solo di scambiare informazioni ma anche beni[33]. Della blockchain sono stati fatti innumerevoli usi, vale, da subito, la pena infatti ricordare la Risoluzione del Parlamento europeo del 3 ottobre 2018, riguardante le Tecnologie di registro distribuito e blockchain secondo cui è necessario creare fiducia attraverso la disintermediazione, nell'ambito di un'ampia definizione di tali tecnologie (ivi denominate DLT).

---

[31] V.L. PIATTI, *Blockchain, decentralizzazione e privacy: un nuovo approccio del diritto,* in *Ciberspazio e diritto*, vol.19, n.60 (1-2-2018), 179, 182-183.

[32] *European Union Blockchain Observatory and Forum* nel febbraio 2018 (*https://www.eublockchainforum.eu/about*) e la produzione da parte dello stesso dei Report su Blockchain and the future of digital assets; *Legal and regulatory framework of blockchains and smart contracts*, nonché su Blockchain for Government and Public Services, consultabili al link *https://www.eublockchainforum.eu/reports*. Per quanto riguarda l'Italia, la principale iniziativa è certamente quella condotta dal Ministero dello Sviluppo Economico, attraverso lo stabilimento di un gruppo di esperti per formulare proposte di policy per favorire lo sviluppo del settore della Blockchain (*https://www.mise.gov.it/index.php/it/blockchain*).

[33] G.B. MARTELLI, *L'importanza della blockchain nello sviluppo dei business futuri*, in www.studiomartelli.it.

A tal proposito ricordiamo *Everledger,*[34] una start-up che dal 2015 si è occupata di utilizzare blockchain per proteggere i diamanti. Per fare ciò si è occupata di catalogare con estrema precisione le caratteristiche di ogni diamante dando loro una identità digitale univoca attraverso l'accostamento ad un *hash crittografico* e quindi la registrazione in blockchain. Tutto ciò ha permesso di reperire i trasferimenti dei diamanti garantendo così la tracciabilità e l'autenticità. Altro esempio la *BCDiploma* che servendosi sempre della tecnologia blockchain ha digitalizzato e archiviato in blockchain i titoli universitari e simili o il progetto *DECODE* che vuole utilizzare la tecnologia blockchain a vantaggio della protezione dei dati personali.
Veniamo a considerare alcune applicazioni della blockchain che ne dimostrano le potenzialità applicative e i rischi legali.
Di Blockchain abbiamo trattato anche in riferimento all'arte[35]. È stato infatti chiarito dalla dottrina come nel nostro ordinamento giuridico non si possa predicare l'esistenza di un diritto o meglio di una facoltà di autentica esclusiva dell'opera d'arte e come invece tale ostacolo potrebbe essere superato attraverso il ricorso alle *distributed ledger Technologies*. Nel caso di contenuti creativi digitalizzati potrebbe essere così possibile tracciare e gestire la proprietà intellettuale facilitando la protezione dei diritti d'autore e dei brevetti mediante un registro pubblico che possa indicare in modo sicuro proprietà e diritti d'autore.
In questo registro virtuale tramite blockchain sarà quindi possibile annotarvi la paternità delle opere e la titolarità dei diritti di autore, le immagini ed il titolo dell'opera, l'anno di realizzazione, i materiali usati, le misure e la denominazione eventualmente di pezzo unico o di opera in serie, le informazioni sulla proprietà dell'opera e sui successivi trasferimenti tramite contratto così da verificarne la provenienza da una casa d'aste, da una galleria, da un collezionista, i certificati di autenticità.

---

[34] https://www.blockchain4innovation.it/mercati/legal/blockchain-24-carati-cosi-everledger-digitalizza-diamanti/.it

[35] G. MAGRI, *La Blockchain può rendere più sicuro il mercato dell'arte*? in *Aedon, Rivista di arte e diritto on line*, 2019, 1, ss e S. MORABITO*, L'applicabilità della blockchain nel diritto dell'arte,* in www.businnesjus.com, 6; G. LIBERATI BUCCIANTI, *L'opera d'arte nel mercato*, Torino, 2019.

In questo modo la catena farebbe da archivio ed un registro delle opere d'arte e delle sue caratteristiche ed i dati dell'opera potrebbero essere racchiusi in una tecnologia NFT[36] più indicata per tracciare le sue caratteristiche.[37]
Oltre a ciò, sarà possibile cristallizzare la c.d. arte immateriale e quindi quelle informazioni relative a quelle manifestazioni artistiche che esprimono un'idea, memorizzare le opere che si presentano come indicazioni dell'autore per la loro futura realizzazione o quelle che si identificano con certificati di tipo negoziale.[38]
Si potrà commercializzare le opere d'arte con più facilità, né un esempio le opere *CryptoPunk* o *Cryptokitties* che utilizzano la tecnologia blockchain per essere trasferite e per assicurare all'acquirente l'effettività dell'acquisto o l'opera *Forever Rose* creata dall'artista concettuale Kevin Abosch con la collaborazione della piattaforma *Gifto* che consente di scambiare e creare regali virtuali attraverso il meccanismo blockchain e *smarth contracts*.
Nonostante tutte queste buone intenzioni non sono mancate le criticità importanti.
Criticità che, come attenta dottrina[39] ha scritto, non si sviluppano nelle blockchain *permissioned* o private quanto nelle blockchain pubbliche in cui, per la vasta mole di partecipanti, la difficoltà principale sarà la possibilità di cancellare il dato o ancor di più modificarlo.
Gli aspetti sono molteplici perché può capitare che le attestazioni di autenticità indicate nei blocchi non siano state rese in modo veritiero per cui l'unica soluzione per non lasciare nella blockchain una informazione sbagliata non potrà essere se non quella di introdurre una nuova informazione come fosse una nota attraverso un ulteriore blocco; può accadere che il contratto di vendita possa perdere efficacia per recesso, annullamento, mancato adempimento dell'obbligo di consegna dei documenti di autenticità anche in questo caso la soluzione è quella di inserire ulteriori informazioni nei blocchi successivi; infine, può capitare che il contratto di vendita dell'opera d'arte possa in realtà celare

---

[36] Vedi https://www.kalwaltart.it/blog/2019luglio1930/realt%C3%A0-aumentata-con-tecnologia-nft/, secondo cui l'acronimo NFT (Natural Feature Tracking) esprime una tecnica relativamente recente: essa permette, "attraverso l'individuazione di punti e regioni con caratteristiche salienti, il riconoscimento di immagini. A differenza della tecnologia con i Marker, molto più restrittiva anche se robusta ed efficace, la tecnologia NFT permette più libertà nella scelta delle immagini da sottoporre al tracciamento".
[37] Sul punto è interessante l'articolo di A. DENZA (art advisor) NFT- *Non fungible Token* in contemporaryarttravellers.com in cui oltre a descrivere cosa sono gli NFT e cioè qualcosa di immateriale e non fungibile, si domanda se abbia senso farne una mostra perché non è chiaro che cosa si stia osservando. Per approfondimenti v. www.contemporaryarttravellers.com.
[38] A. DONATI, *Autenticità Authenticité, Authenticity dell'opera d'arte. Diritto, mercato, prassi virtuose*, in *Riv. dir. civ.,* 2015, 987 ss.
[39] G. FREZZA, *Blockchain, autenticazione e arte contemporanea* in *Diritto di Famiglia e delle Persone* (II), fasc. 2, 1° giugno 2020, p.489. L'autore mette in risalto le criticità che comunque sussistono nell'utilizzo della blockchain nel mondo artistico.

attività fraudolente per cui non si potrà fare altro che dichiarare la nullità della vendita e quindi spezzare la catena dei nodi.
Complicato è anche il rapporto con il regolamento UE 2016/679. Gli aspetti più dibattuti sono stati il problema dell'anonimato e dello pseudonimo, infatti l'art.25 del GDPR richiede misure tecniche ed organizzative adeguate per proteggere i dati, per cui si rende necessario capire se la piattaforma applica una forma di anonimato o meno. Così come si rende importante individuare il titolare del trattamento soprattutto nelle blockchain *permissionless*, quanto vengono conservati i dati che in realtà in questi casi sembrano rimanere nella piattaforma in modo perpetuo, il diritto alla cancellazione o come già visto la rettifica.
La blockchain comunque offre la pseudonimizzazione delle transazioni registrate e quindi permette di disaccoppiare i dati dell'operazione registrata rispetto ai dati di colui che l'ha posta in essere, minimizzando così i dati in circolazione. Gli strumenti, infatti, per anonimizzare le transazioni sono le chiavi pubblica e privata, *l'hash crittografico* del contenuto delle operazioni. L'anonimato così come offerto dalla blockchain è risultato un elemento d'interesse per i collezionisti ed i venditori che non vogliono figurare. [40]
Vediamo quindi come se da una parte sia una soluzione efficace per la protezione e l'autenticità dell'opera[41] dall'altra comunque porti con sé perplessità e qualche difficoltà che può essere superata solo accettando l'introduzione di un nuovo blocco o comunque della correzione se così la possiamo definire.
La Blockchain però non si è arrestata al solo mondo artistico ma si è estesa [42] anche a settori centrali per l'economia italiana ad esempio nel settore vitivinicolo. Le modalità di produzione vitivinicola e i suoi canali commerciali hanno già da tempo incalzato percorsi di adozione delle tecnologie di informazione e comunicazione per struttura un sistema di distribuzione su scala più ampia.
La dottrina[43] ha scritto come nel settore vitivinicolo la tecnologia blockchain possa essere risolutoria e foriera di grandi novità e facilitazioni. Assumendo infatti che la filiera inizi a partire dalla coltivazione del fondo rustico vitato, il

---

[40] M. MCCONAGHY, G. MCMULLEN, G. PARRY, T. MCCONAGHY, D. HOLTZMAN*, Visibility and digital art: Blockchain as an ownership layer on the Internet*, in *SC Special Issue: The Future of Money and Further Applications of the Blockchain*, vol. 26, n. 5, sett. 2017, pag. 461 ss; a G. MAGRI Op.cit. nonché G. FREZZA, op. cit.
[41] M. STERPI, *L'impatto delle nuove tecnologie sulla creazione, distribuzione e vendita delle opere d'arte*, in *L'opera d'arte nel mercato. Principî e regole,* (a cura di) G. LIBERATI BUCCIANTI, Torino, 2019, pag. 214 ss.
[42] *European union blockchain observatory and forum, Legal and regulatory framework of blockchains and smart contracts, Thermatic Report, Bruxelles, 2019.* A settembre 2019 ha prodotto il primo report di valutazione sulla blockchain e sul quadro giuridico applicabile.
[43] A. SABA, *Blockchain e vino: una nuova frontiera,* in *Diritto agroalimentare*, n.3, 2019, 491.

c.d. genesis block sarà costituito dall'impresa agricola che andrà a registrate i dati rilevanti sulla produzione. Questo succederà perché ciascun operatore della filiera sarà dotato di un numero d' identificazione univoco ed il registro così andrà ad archiviare e validare ciascun dato derivante dalle pratiche di campo e di cantina. Si costruiranno più blocchi che segneranno i vari passaggi del prodotto lungo la filiera per arrivare poi alla singola bottiglia a cui è possibile associare un codice.
Sempre attenta dottrina ricorda come attraverso i codici di riconoscimento degli operatori e i codici di controllo di hash la tecnologia blockchain permetterà di andare a ritroso partendo dalla bottiglia per arrivare alla vite.
Quindi vediamo come molteplici sono gli usi di questa tecnologia distribuita che non si arresta[44].
Il tribunale dell'Internet di Hangzhou[45] si è distinto, infatti, per aver inaugurato la prima piattaforma giudiziale in *blockchian* dedicata al controllo in materia di *digital copyright*. In sintesi, come ci riporta la dottrina recente, si tratta di un sistema distribuito, realizzato in partenariato con alcune imprese private specializzate, che offre agli autori che lamentino una lesione dei propri diritti in rete, la possibilità di acquisire, registrare e immediatamente condividere con gli uffici giudiziari la prova legale dell'illecito.
A livello europeo non vi è ancora univocità su questa tecnologia ma è stato istituito dalla Commission europea *l'EU Blockchain Observatory and Forum* che produce dal 2019 report di valutazione sul quadro giuridico applicabile alla tecnologia blockchain per poterne usufruire in più settori economici.

4. La Blockchain e la gestione dei dati personali relativi alla salute.

Una delle applicazioni di blockchain si ha in ambito sanitario consentendo di superare alcuni problemi di protezione del dato che troverebbero tutela non più secondo un approccio consensuale (la persona si tutela autorizzando l'uso dei propri dati) ma secondo un approccio gestionale e *risk based* (la corretta gestione del dato in chiave risk management riesce a tutelare la persona effettivamente consentendo l'uso del dato). Come abbiamo già detto una blockchain è un elenco decentralizzato e in continua crescita di record, chiamati "blocchi", che sono collegati tra loro in una catena attraverso un processo chiamato mining.

---

[44] G. SPOTO, *Gli utilizzi della blockchain e dell'Internet of Things nel settore degli alimenti,* in *Riv. Dir. alim.*, 2019, 13, n.1, 25-35.
[45] Sui casi cinesi v. WU E ZHENG *Electronic evidence in the blockchain era: New rules on authenticity and integrity*, in *Comp., L. & Sec. Rev.,* 2020, p.7 ss, CHAN E KOO, *Blockchain in Evidence in Internet Courts in China: The Fast Track for Evidence Collection for On line Disputes*, https://www.lexology.com/library/detail.aspx?g=1631e87b-155a-40b4-a6aa-5260a2e4b9bb; C. SANDEI, *Blockchain e sistema autoriale: analisi di una relazione complessa per una proposta metodologica*, in *Nuove Leggi Civ. Comm.*, 2021,1,194.

Questo processo trasforma le transazioni in sospeso in un puzzle matematico. I minatori (persone) risolvono il puzzle utilizzando sistemi informatici e producono il cosiddetto *hash*, una sequenza di lettere e numeri unica per il blocco.
Ogni blocco contiene un *hash crittografico* del blocco precedente, un t*imestamp* e i dati della transazione.
Una volta che la blockchain elabora le informazioni, ogni computer della rete si blocca nello stesso momento, creando un record digitale permanente e immutabile. Ogni sistema blockchain determina chi può aggiungere nuovi blocchi alla catena e come viene eseguita la procedura.
La Blockchain potrebbe aiutare a risolvere alcuni dei problemi dell'assistenza sanitaria, superando le sfide di interoperabilità[46]dei dati e potrebbe svolgere un ruolo cruciale nel mettere i pazienti al centro dell'ecosistema. In sintesi, la blockchain potrebbe essere applicata all'accesso e alla condivisione delle cartelle cliniche dei pazienti, alle applicazioni mobili e al monitoraggio remoto, nonché al sistema di gestione dei dati medici che consente ai pazienti di conservare le informazioni necessarie.
Nel 2019 Anthem, la seconda più grande assicurazione sanitaria, annunciò di voler utilizzare la tecnologia blockchain per archiviare i dati sanitari di quaranta milioni di pazienti.
Non esiste molta dottrina italiana che preveda l'adottabilità della blockchain in ambito sanitario sia perché fino ad ora non era mai stato associato l'utilizzo di questa tecnologia al mondo medico sia perché come abbiamo già visto nelle precedenti pagine, questa tecnologia anche se di grande valore porta con sé delle criticità legate soprattutto al suo rapporto con il regolamento del 2016 in tema di privacy della persona.
La ricerca[47] quindi mi ha portato ad affacciarmi ad altri sistemi come la lettura della Rivista Internazionale di Gestione sanitaria in cui ho trovato spunti sul tema della blockchain applicata al mondo sanitario.
Infatti, dopo aver appreso, come sussista una forte consapevolezza delle difficoltà legate all'interoperabilità ed allo scambio dei dati medici oltre che delle cartelle dei singoli cittadini, si passa ad analizzare il meccanismo della blockchain che, ritengono, semplificherebbe notevolmente il processo di condivisione dei dati sanitari e contribuirebbe a risolvere il problema della loro gestione e dell'interoperabilità nel settore sanitario.
Nella catena di blocchi sanitari autorizzati, infatti, i pazienti potrebbero essere identificati tramite il loro *hash* ID, che sarà il loro identificatore unico. L'*hashing* consentirebbe all'ID di essere unico e di garantire la privacy dell'utente. I

---

[46] ICHIKAWA D, KASHIYAMA M, UENO T. *Salute mobile resistente alle manomissioni grazie alla tecnologia blockchain*. JMIR Mhealth Uhealth. 2017;5(7):1-10.
[47] GORDON WJ, CATALINI C. *La tecnologia blockchain per l'assistenza sanitaria: facilitare la transizione verso l'interoperabilità guidata dal paziente*, *Comput Struct Biotechnol* J. 2018, 224-230.

pazienti dovranno condividere la chiave di decrittazione per i blocchi di dati a loro associati con gli operatori sanitari scelti. Questo sistema migliorerebbe la sicurezza, la privacy, l'interoperabilità e potrebbe mettere i pazienti al centro dell'ecosistema. Pazienti e fornitori trarrebbero grandi benefici da cartelle cliniche accurate, aggiornate e complete.

Si aggiunge, inoltre nel saggio che "[48]La blockchain potrebbe offrire diversi vantaggi per la sicurezza dei dati sanitari e la gestione delle identità. Può arginare le minacce e tenere i dati privati fuori dalle mani sbagliate. La blockchain cripta i dati quando vengono aggiunti alla catena e li rende immutabili e impossibili da decifrare. Autorizza le transazioni con una chiave di identificazione privata, nota solo all'individuo. In questo modo, a differenza dell'attuale tecnologia dei dati sanitari, un operatore sanitario sarebbe in grado di accedere ai dati medici di un paziente solo con un accesso esplicito al record della blockchain. Una migliore collaborazione dei dati tra i fornitori aumenterebbe la probabilità di una diagnosi accurata e la probabilità di successo dei trattamenti e consentirebbe alle strutture sanitarie di fornire un'assistenza efficace dal punto di vista dei costi. La blockchain può mantenere le informazioni dei pazienti sicure e protette, consentendo loro di condividerle con qualsiasi fornitore di servizi di loro scelta. Fornisce la prova della proprietà delle cartelle cliniche e garantisce l'autenticità per le tecniche anticontraffazione. Secondo un recente studio condotto da *BIS research*[49], entro il 2025 il settore sanitario potrebbe risparmiare fino a 100 miliardi di dollari all'anno incorporando la tecnologia della catena di blocco. Il risparmio si concretizzerebbe in una riduzione dei costi legati alla violazione dei dati, dei costi operativi, dei costi IT, delle frodi legate alla contraffazione e delle frodi assicurative. Il rapporto afferma, che si prevede che le applicazioni globali della blockchain nel mercato sanitario cresceranno a un tasso di crescita annuale composto di quasi il 64% dal 2018 al 2025. Entro il 2025 raggiungerà un valore di quasi sei miliardi."

Nella lettura straniera si troviamo contributi sull'analisi di alcuni sistemi già in uso di blockchain in ambito medico.

Ne è stato un esempio Patientory[50], un'azienda Software come un Service che offre un'applicazione distribuita basata su blockchain che consente a pazienti,

---

[48] M. ATTARAN, *La tecnologia blockchain nell'assistenza sanitaria: Sfide e opportunità,* in *Rivista Internazionale di gestione sanitaria* 2022, vol. 15, n.1, 78.

[49] Ricerca BIS. *Global Blockchain in Healthcare Market: FocusonIndustryAnalysisand Opportunity Matrix – Analysis and Forecast*, 2018- 2025. 2018 [citato 2020 Jan 15]. Disponibile da: https://bisresearch.com/industryreport/globalblockchain-in-healthcare-market-2024.html.

[50] R. ANGELES, *Assistenza sanitaria basata sulla blockchain:Tre progetti pilota Proof-of-Concept di successo da tenere in considerazione*, in *Rivista di tecnologia internazionale e gestione dell'informazione*, vol. 27, numero 3, 2018, Università di New Brunswick Fredericton, Canada; v. anche Rapporto Becker's Health IT & CIO (2017, 19 gennaio). Come *Patientory* utilizza la blockchain per mantenere i dati sicuri e aiutare a connettere i pazienti. Recuperato da

medici e organizzazioni sanitarie di accedere, archiviare e trasferire informazioni per soddisfare le esigenze dei pazienti e migliorare il coordinamento dell'assistenza sanitaria tra le varie istituzioni[51]. Patientory fornisce una piattaforma che consente a queste entità di interagire e comunicare facilmente, in quanto mette in correlazione sistemi di cartelle cliniche elettroniche (EMR) come Epic, Cerner, Allscripts e Meditech e altri sistemi di database relativi alla salute. L'azienda SaaS offre inoltre ai pazienti un'applicazione mobile che possono utilizzare per acquisire dati sulla salute da fonti tradizionali e non (ad esempio FitBit, ecc.) e creare i loro profili personali, archiviati in server sicuri conformi alla normativa HIPAA. Incoraggiando un maggiore impegno dei pazienti nei confronti della loro salute, l'app può anche essere utilizzata dai pazienti per contattare i loro fornitori di cure e altri pazienti con problemi di salute simili.

Patientory ricorre a *middleware criptato* per soddisfare gli scambi di transazioni ad alto volume nel settore sanitario; interfacce di programmazione delle applicazioni per facilitare lo scambio e il trasferimento rapido delle informazioni; e risorse di archiviazione delle informazioni sanitarie conformi allo standard HIPAA che rispettano le normative specifiche della geografia.

Patientory utilizza il token Patientory (PTOY) per sostenere le proprie operazioni[52].Una volta che i pazienti si iscrivono al servizio, ricevono gratuitamente una quantità di spazio per memorizzare le loro informazioni sanitarie personali.[53]

---

https://www.beckershospitalreview.com/healthcareinformation-technology/how-patientory-uses blockchain-to-keep-datasecure-and-help- connect-patients.html;

[51] A. GASKELL, (2017, 3 maggio). *Il movimento verso le blockchain in ambito sanitario*. Recuperato da https://www.huffingtonpost.com/entry/the-move-towardshealthcare-blockchains_us_59003a9be4b06feec8ac91e1

[52] MCFARLANE, C., BEER, M., BROWN, J. E PRENDERGAST, N. (2017). *Patientory: A Healthcare Peer-to-Peer* EMR Storage Network v1.1, Whitepaper. Maggio. Recuperato da *https://patientory.com/patientory_whitepaper.pdf.*

[53]1) Un'entità richiedente emette una richiesta di informazioni; questa richiesta è una transazione firmata crittograficamente che viene inviata al server RPC (Remote Procedure Call). Il server RPC verifica l'identità dell'entità richiedente utilizzando la firma della richiesta di accesso.

2) Il database delle chiavi pubbliche di accesso ai permessi riceve la firma dal server RPC e controlla se c'è una voce corrispondente nel database. Se c'è una corrispondenza, questo database invia un messaggio per accettare la richiesta.

3) Il server RPC invia anche una copia della richiesta in arrivo al server di aggregazione dei dati, che la inoltra ai minatori in base a un meccanismo di condivisione del carico.

4) I minatori inviano la richiesta al contratto di controllo della parte richiedente, che contiene informazioni sui permessi di accesso a specifici dati a cui la parte richiedente è autorizzata ad accedere. Se il contratto di controllo indica l'autorizzazione ad accedere alle informazioni richieste, allora la richiesta in arrivo è considerata valida.

È chiaro quindi come in paesi diversi dal nostro il ricorso alla blockchain in ambito sanitario in realtà sia già stato avviato. La preoccupazione per la privacy del paziente è arginata facendo riferimento al fatto che agenzie di regolamentazione, come *l'Office of the National Coordination for Health Information Technology* (ONC) degli Stati Uniti, richiedono che i partecipanti ai sistemi sanitari siano adeguatamente identificati e autenticati; che sia prevista un'infrastruttura informatica sicura e onnipresente per l'archiviazione e lo scambio di dati; controlli di accesso e procedure di autorizzazione per diverse fonti di dati esterni; gestione delle strutture di una varietà di fonti di dati. Fortunatamente, i principi di progettazione intrinseci della blockchain, che prevedono l'uso di una crittografia sicura e il supporto di solide *reti peer-to-peer*, dovrebbero soddisfare la maggior parte di questi requisiti. D'altra parte, un rischio importante nella rete blockchain è la possibilità di incidenti di malaffare che comportano la decrittazione imprevista e non autorizzata di informazioni private dei pazienti sulla blockchain[54].

5. Conclusioni

Alla base di queste soluzioni vi è il bisogno di superare il problema, soprattutto in ambito medico della interoperabilità dei dati. L'interoperabilità sanitaria, infatti, viene descritta come la capacità dei sistemi informatici ed applicazioni software eterogenei di comunicare, scambiare ed utilizzare i dati scambiati.
Consentire ai sistemi informativi di lavorare insieme è fondamentale per l'erogazione di cure efficaci per gli individui e le comunità. La condivisione dei dati è essenziale per raggiungere un trattamento ed una cura sicura.
Addirittura, questa interoperabilità viene catalogata come: fondamentale perché consente lo scambio tra i dati sanitari, strutturale perché definisce i formati per

5) Il contratto di controllo ha un sistema di puntatori *hash* che portano alle informazioni richieste. Il contratto di controllo invia un messaggio di evento al server di archiviazione HIPAA, che contiene i dati e risolve il
sistema di puntatori *hash*. Il contratto di controllo esegue una transazione di richiesta valida che, di fatto, attiva il sistema di messaggistica di eventi della blockchain, che contatta lo spedizioniere HIPAA.
6) Lo spedizioniere HIPAA riconosce la richiesta valida e crea una richiesta crittografata nei confronti del server di archiviazione HIPAA sulla base degli *hash* del messaggio dell'evento, che contiene la chiave pubblica del
richiedente.
7) Inoltre, il server di aggregazione dei dati invia la richiesta ai verificatori privati della blockchain, che confrontano la richiesta di informazioni con un "contratto target". Se la richiesta di informazioni è ritenuta valida, la transazione viene inserita nel blocco successivo della catena di blocchi attraverso il processo di mining. Viene inoltre generato un
messaggio di evento nella blockchain.

[54] ZHANG, P., SCHMIDT, D.C., & WHITE, J. (2018, 1 marzo) *Chapter One - Blockchain Technology Use Cases in Healthcare*, Advance in computers, Volume 111, 2018, 1-41.

i dati clinici scambiati ed infine semantica che richiede l'interpretabilità dei dati scambiati non solo in base alla sintassi ma anche in base al loro significato[55].
In Italia, viceversa, non vi sono ancora riferimenti a modelli sanitari che facciano ricorso alla blockchain ma solo idee nella speranza di un futuro prossimo utilizzo affinché i dati diventino sempre più ausilio per le strutture sanitarie e non un ostacolo nel loro utilizzo.
Quanto ripercorso ed affrontato ci porta a maturare la consapevolezza di come oramai, nonostante gli sforzi, sia sempre più complesso il ruolo del giurista e del diritto nel panorama tecnologico.
Si cercano nuove soluzioni e si affrontano nuove sfide. Inizialmente i problemi erano quasi ed esclusivamente legati alla cura ed ai profili di responsabilità oggi la cura ed il modus operandi rivestono sempre un grande spazio nel settore sanitario ma non si può ignorare il grande fenomeno della portabilità del dato e quindi della privacy della persona.
Sicuramente è una privacy più moderna rispetto a quella che abbiamo conosciuto vent'anni fa ma proprio perché d'avanguardia richiede maggior attenzione, più tutele e garanzie.
La blockchain oggi, offre quelle possibilità perché "può migliorare il controllo degli accessi, l'interoperabilità, la provenienza e l'integrità dei dati nel settore sanitario. La natura distribuita della blockchain, la struttura trasparente delle informazioni e l'immutabilità dei record conservati e archiviati da tutti gli utenti partecipanti possono contribuire a ridurre i costi di tutte queste operazioni garantendo allo stesso tempo la tutela della persona del paziente.

[55] ZHANG, P., SCHMIDT, D.C., & WHITE, J. op.cit.