Riflessioni sparse in tema di intelligenza artificiale e dati sanitari

Giuliano Mattace*

RANDOM THOUGHTS ON THE SUBJECT OF ARTIFICIAL INTELLIGENCE AND HEALTH DATA

ABSTRACT: The text examines the use of health data combined with modern artificial intelligence systems. The aim is to provide a brief and introductory treatment of the subject. In particular, it addresses several current issues with implications for constitutionally guaranteed rights. the legal bases for the processing of personal data in the context of clinical trials, consent as the legal basis for the primary and secondary use of personal data. The processing of digitised health data. Duties and obligations to provide information in healthcare.

KEYWORDS: Health data; artificial intelligence; fundamental rights; European Health Data Space

ABSTRACT: Il testo esamina l'uso dei dati sanitari combinato con i moderni sistemi di intelligenza artificiale. L'intento è quello di fornire una sintetica ed introduttiva trattazione della materia. In particolare, vengono affrontati diversi temi di attualità con implicazioni sui diritti costituzionalmente garantiti: le basi giuridiche per il trattamento dei dati personali nel contesto delle sperimentazioni cliniche, il consenso come base giuridica per l'uso primario e secondario dei dati personali. Il trattamento dei dati sanitari digitalizzati. I doveri e gli obblighi di informazione in ambito sanitario.

PAROLE CHIAVE: Dati sanitari; intelligenza artificiale; diritti fondamentali; European Health Data Space

SOMMARIO: 1. Premessa — 2. La pseudonimizzazione dei dati personali nella ricerca clinica — 3. Le basi giuridiche dei trattamenti dei dati personali nell'ambito delle sperimentazioni cliniche in Europa — 4. Le basi giuridiche dei trattamenti correlati a finalità di tutela della salute. L'uso primario e secondario dei dati — 5. Il consenso quale base giuridica per l'uso primario e secondario dei dati personali — 6. Il trattamento dei dati sanitari digitalizzati — 7. *European Health Data Space*: l'accessibilità ai dati sanitari — 8. Doveri e obblighi informativi in sanità.

Downloaded from www.biodiritto.org.
ISSN 2284-4503

* *Professore a contratto di Istituzioni di Diritto privato ed europeo, Università di Parma e Assegnista di ricerca, Università di Bologna. Mail: giuliano.mattace@unipr.it.* *Contributo sottoposto a doppio referaggio anonimo.*

Call

1. Premessa

L'utilizzo dei dati[1] rappresenta un elemento fondamentale per l'innovazione in ambito sanitario. Esemplificativo, in tal senso, è il ruolo centrale ricoperto dai cd. *big data*[2]. Questa tendenza si è rafforzata, negli ultimi anni, attraverso l'utilizzo preponderante dell'intelligenza artificiale, che consente di testare in modo economico e veloce la potenziale efficacia delle molecole più promettenti in differenti settori terapeutici nonché di svolgere esami diagnostici predittivi[3]. I dati in ambito sanitario rappresentano una risorsa importantissima sia per la medicina di precisione, sia per quella personalizzata, nonché per supportare studi su larga scala. La capacità di accedere, elaborare e condividere i dati sanitari rappresenta una risorsa strategica di primaria importanza per il progresso e l'innovazione del comparto sanitario, tanto in ambito europeo come in quello nazionale. La possibilità di sfruttare in pieno questo patrimonio prezioso risulta imprescindibile per garantire un'assistenza sanitaria maggiormente personalizzata e mirata, promuovere lo sviluppo di innovative soluzioni terapeutiche e tecnologiche, nonché per supportare la definizione di politiche sanitarie più efficaci.

Il GDPR definisce all'art. 4 come "dato relativo alla salute dell'individuo", ogni informazione attinente alla salute fisica o mentale di una persona nonché le informazioni derivanti da prestazione di servizi di assistenza sanitaria.

Il ruolo e il valore dei dati sono stati amplificati con l'introduzione di metodologie di analisi avanzate, come quelle basate su tecniche di *deep learning* e di *machine learning*: queste ultime sono in grado di processare grosse quantità di dati, sia in modo supervisionato che non supervisionato, alla ricerca di quelle caratteristiche utili alla risoluzione di problematiche caratterizzanti la salute del singolo individuo e alla stratificazione di gruppi di individui, per meglio organizzare le modalità di intervento.

Al fine di poter essere utilizzati in sintonia con i nuovi strumenti di intelligenza artificiale (nel prosieguo IA), i dati devono soddisfare precise caratteristiche volte a garantire la validità dei risultati ottenuti, riassunte in una serie di linee guida, principi FAIR[4], volti a garantire che i dati siano rintracciabili, accessibili, interoperabili e riutilizzabili (*Findable, Accessible, Interoperable e Reusable).*

---

[1] Sul presupposto che i dati sono elementi essenziali di ogni sistema di IA in quanto gli algoritmi si alimentano di dati, si allenano grazie a questi e li generano a livello di output, il GDPR, rappresenta un valido riferimento. Alcuni aspetti, quindi, sono stati da questo mutuati nel *Artificial Intelligence Act*, tra cui anche il principio di *accountability* o il principio di trasparenza o, ancora, l'approccio basato sul rischio, da cui discende la necessità di approntare tutto quanto è necessario per la tutela delle persone (tra cui le misure di sicurezza) non già in modo standard, bensì sulla base dei possibili rischi. Sul rapporto tra IA e privacy, si veda G. NATALE, *Artificial Intelligence and privacy rights*, in *Rassegna Avvocatura dello Stato*, 2023, 1, 40.

[2] V. A.C. NAZZARO, *L'utilizzo dei* Big data *e i problemi di tutela della persona,* in *Rassegna di diritto civile ,2018, 1239 ss.;* ID., *Privacy e Big data*, in *Corti fiorentine*, 2018, 13 ss.; A. MANTELERO, *Big data and data protection*, in G. GONZÁLEZ-FUSTER, P. DE HERT (a cura di), *Research Handbook on Privacy and Data Protection Law*, Cheltenham, 2022, 335.

[3] V. A. SPINA, *La medicina degli algoritmi: Intelligenza Artificiale, medicina digitale e regolazione dei dati personali*, in F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, 319.

[4] M.D. WILKINSON, M. DUMONTIER, I.J. AALBERSBERG, G. APPLETON, M. AXTON, A. BAAK, N. BLOOMBERG, J.W., BOITEN, *The FAIR Guiding Principles for scientific data management and stewardship,* in *Scientific data*, 2016, 3, 1-9.

Downloaded from www.biodiritto.org.
ISSN 2284-4503

Seguendo questi principi, i dati sono rintracciabili sia dall'essere umano, ma soprattutto dalla macchina, quando identificati in modo unico e persistente, corredati di informazioni descrittive e aggiuntive; sono accessibili se esiste la possibilità di consultare i dati (o almeno i loro metadati) attraverso sistemi di autenticazione e di autorizzazione che facciano uso di protocolli di sicurezza standard.
Al fine di garantire la riutizzabilità e l'interoperabilità, i dati devono essere documentati e descritti utilizzando formati e standard condivisi a livello internazionale.
La ricerca scientifica in ambito sanitario, che ha registrato un crescente impiego di soluzioni basate su strumenti di IA, è chiamata ad includere tra le fasi caratterizzanti la progettazione delle sperimentazioni cliniche proprio i principi FAIR sopra menzionati.
Questi ultimi vanno necessariamente connessi con altri due concetti fondamentali quando si parla di dati: il *data sovereignty* e il *data protection*.
Il primo concerne il diritto di un individuo di avere il pieno controllo sui dati; il secondo determina l'insieme dei protocolli dedicati alla protezione dei dati.
Data protection, *data sovereignty,* unitamente ai principi FAIR rappresentano elementi indispensabili nello sviluppo di una strategia europea per i dati.
Una corretta raccolta, codifica, standardizzazione e gestione dei dati sanitari può portare, tramite l'impiego di strumenti di IA, ad analisi e risultati attendibili, al fine di migliorare il percorso di gestione delle risorse e di cura. Sistemi non standardizzati ostacolano un tale approccio, mentre un'organizzazione funzionale di dati che utilizza standard e codifiche internazionali ne favorisce l'analisi, anche tramite strumenti avanzati, a supporto di una medicina avanzata, preventiva, predittiva e partecipativa nel rispetto della sicurezza e *privacy* dell'individuo.
Lo scritto si propone di analizzare in maniera sia pure sintetica e in un'ottica introduttiva diversi profili in tema di dati sanitari e intelligenza artificiale; materia quanto mai attuale, anche alla luce del recente *European Health Data Space*. I pur variegati temi trattati, apparentemente slegati tra di loro, si ricollegano sotto il *fil rouge* dell'innovatività nella tematica in commento.

2. La pseudonimizzazione dei dati personali nella ricerca clinica

I dati personali sono definiti dall'art. 4, n. 1 GDPR, definizione che ricomprende anche i dati relativi alla salute[5] ossia un insieme estremamente variegato composto da dati connessi «allo stato di salute fisica o mentale passata, presente o futura».
Ai fini dell'applicazione del GDPR, questi dati devono essere oggetto di trattamento[6].

[5] Si tratta, infatti, di: (*i*) informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria; (*ii*) numeri o simboli attribuiti all'interessato per identificarlo in modo univoco a fini sanitari; (*iii*) esiti di esami e controlli anatomici o relativi ad una sostanza organica, compresi i dati genetici e i campioni biologici; (*iv*) informazioni relative a degenza ospedaliera, malattie, disabilità, il rischio di contrarre malattie, indagini anamnestiche, trattamenti clinici o lo stato fisiologico o biomedico dell'interessato, indipendentemente che siano raccolti dagli operatori sanitari, oppure attraverso l'uso di *wearable device*, dispositivi medici o *test* diagnostici in vitro.
[6] Definito come quell'insieme di operazioni, anche automatizzate, quali «la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o

Downloaded from www.biodiritto.org.
ISSN 2284-4503

Quest'ultimo *ex* art. 4 n. 2 GDPR comprende qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali (o insiemi di dati personali), come ad esempio la raccolta, la registrazione, l'organizzazione, la diffusione o qualsiasi altra forma di messa a disposizione, la cancellazione o la distruzione.

E' escluso dall'ambito applicativo del GDPR, invece, il trattamento dei dati anonimi e dei dati che, sebbene inizialmente personali, sono stati successivamente sottoposti a processi di anonimizzazione che ne hanno cancellato definitivamente qualsiasi riferimento ad un determinato individuo, rendendolo così non più identificabile.

Il discrimine tra dati personali e anonimi risulta di difficile individuazione a causa delle tecniche di re-identificazione, in grado di estrarre informazioni di natura personale dall'analisi incrociata di *database* di dati anonimi. Allo scopo di stabilire se ci si trovi in presenza di dati personali o anonimizzati, il GDPR prevede di tenere in considerazione molteplici fattori quali «i costi e il tempo necessario per l'identificazione», le tecnologie attuali e in fase di sviluppo e i *set* di dati servibili dal soggetto che svolge il trattamento.

L'art. 4, par. 5 del GDPR disciplina le tecniche di pseudonimizzazione del dato, in altre parole la sostituzione di dati personali con gli pseudonimi (codici univoci) che, una volta decifrati tramite l'impiego di un'apposita chiave, permettono l'identificazione di una persona.

Le tecniche di pseudonimizzazione sono considerate misura di sicurezza del trattamento dei dati personali volte a garantire un livello adeguato di tutela degli interessati[7].

All'interno delle sperimentazioni cliniche, vige l'obbligo di pseudonimizzazione dei dati del paziente, ex art. 1.58 delle *Good Clinical Practice*[8]: questo riduce drasticamente il rischio che l'identità del paziente arruolato possa essere rilevata erroneamente o carpita fraudolentemente. La pseudonimizzazione consente, inoltre, al soggetto c.d. promotore di riportare il dato in chiaro in caso di specifiche esigenze attraverso la decodifica del codice univoco.

Non sono rare le ipotesi di impiego di dati anonimi, per irrobustire o verificare le evidenze scientifiche ottenute a conclusione dello studio.

Il perimetro dei dati clinici impiegati, quindi, oscilla tra i dati pseudonimizzati, con conseguente applicabilità del GDPR, e i dati anonimi che, esulando da tale normativa, comportano modalità di utilizzo più ampie e meno gravose. In tale contesto si inserisce il provvedimento n. 226 del giugno 2023[9], con cui il Garante per la protezione dei dati personali ha negato la natura anonima ai dati raccolti da una società nell'ambito di un progetto di raccolta e analisi di dati clinici fondato su un software gestionale in uso ai medici di base aderenti.

Questi ultimi, quali titolari del trattamento, raccoglievano e gestivano i dati dei pazienti, senza alcun intervento della azienda. A seguito dell'anonimizzazione dei dati, questi erano trasferiti alla società per lo svolgimento del proprio progetto.

---

l'interconnessione, la limitazione, la cancellazione o la distruzione"; la persona fisica o giuridica che svolge tali trattamenti è denominato titolare».

[7] Garante per la protezione dei dati personali, *Linee guida per i trattamenti di dati personali nell'ambito delle sperimentazioni cliniche di medicinali*, 24 luglio 2008, in G.U. n. 190 del 14 agosto 2008.

[8] Agenzia europea per i medicinali, *Guideline for good clinical practice E6(R2),* 1° dicembre 2016, EMA/CHMP/ICH/135/1995.

[9] Garante per la protezione dei dati personali, provvedimento n. 226 del 1° giugno 2023.

Downloaded from www.biodiritto.org.
ISSN 2284-4503

Il provvedimento evidenzia come la società avesse adottato diverse misure organizzative e tecniche volte a garantire l'anonimizzazione dei dati[10], quali ad esempio processi di randomizzazione dei dati, oltre al coinvolgimento di terze parti certificate, per ridurre il rischio di re-identificazione dei pazienti. Inoltre, le metodologie utilizzate risultavano assimilabili a quelle adottate in programmi afferenti alle principali istituzioni pubbliche sanitarie. Ciononostante, a giudizio del Garante, la società, in qualità di autonomo titolare del trattamento, avrebbe raccolto dati personali particolari violando il principio di correttezza del trattamento, nonché l'obbligo di informazione preventiva agli interessati;

Per tale ragione, l'Autorità ha ordinato alla società di pagare una sanzione pecuniaria e di conformare i trattamenti a quanto indicato nel provvedimento stesso. Secondo il Garante, la società sanzionata ha fondato il proprio progetto sull'erroneo presupposto della natura anonima dei dati trattati, posta l'insufficienza delle misure di anonimizzazione del dato dalla stessa adottate. Tuttavia, il provvedimento del Garante non sembra condivisibile, restringendo la categoria dei dati anonimi a quei casi in cui la re-identificazione sia impossibile in termini assoluti, in un'epoca storica dove la velocità dello sviluppo tecnologico e la disponibilità di *database* sempre più vasti, agendo sinergicamente, ampliano i margini di re-identificazione di un interessato;

Inoltre, sul piano normativo, il *test* di verifica sulla natura anonima o pseudonima dei dati oggetto di trattamento dovrebbe fondarsi, secondo il GDPR, sulla «ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica», nonché sulla verifica che i dati personali siano stati resi sufficientemente anonimi. Tali elementi sembrano essere stati considerati dal giudice in modo diverso in quanto ha disposto la sospensione parziale del provvedimento *de quo*, ove ha previsto la necessità di accertare se il *software* utilizzato renda impossibile la re-identificazione dell'interessato e, nel caso in cui tale impossibilità non sia totale, quale sia il concreto rischio di re-identificazione, nonché il suo costo quantomeno in termini di tempo[11].

Sotto il profilo dell'anonimizzazione dei dati personali si è di recente espresso il Tribunale dell'Unione europea. Il caso di specie prende avvio da una decisione del Garante europeo della protezione dei dati nei confronti del CRU (Comitato di Risoluzione Unico), relativamente al programma da questi adottato nei riguardi del *Banco Popular Español SA*, sulla base del regolamento n. 806/2014.

In tale contesto, CRU ha richiesto alla società Deloitte di valutare, ai sensi dell'art. 20 del suddetto Regolamento, se gli azionisti e i creditori avrebbero potuto ricevere un trattamento migliore nel caso in cui il *Banco Popular Español* fosse stato sottoposto a una procedura ordinaria di insolvenza.

A tal fine, CRU ha condiviso con la società Deloitte una serie di osservazioni generate dall'analisi di un questionario compilato, anche tramite l'inserimento dei propri dati personali, dagli azionisti e creditori coinvolti. Tali osservazioni erano state precedentemente oggetto di un processo di pseudonimizzazione mediante cui solo CRU avrebbe potuto risalire all'identità del soggetto compilante; ciò al solo fine di consentire la verifica, e la relativa prova, che ogni osservazione fosse stata trattata e debitamente presa in considerazione, mentre a Deloitte non era consentito l'accesso alla chiave di decifrazione di tali codici alfanumerici.

[10] Si veda in proposito E. PELLECCHIA, *Dati personali, anonimizzati. Pseudonimizzati, de-identificati: combinazioni possibili di livelli molteplici di identificabilità nel* GDPR, in *Nuove leggi civili commentate,* 2020, 360 ss.

[11] Tribunale di Milano, Ordinanza del 4 dicembre 2023, n. 2952, in *DeJure Online.*

Downloaded from www.biodiritto.org.
ISSN 2284-4503

A seguito dei reclami esperiti dagli azionisti che lamentavano la carenza, nella informativa sulla protezione dei dati personali loro fornita da CRU, della menzione di Deloitte quale potenziale destinatario dei propri dati personali, il GEPD ha aperto un'indagine formale conclusasi con l'accertamento della violazione dell'obbligo di informazione previsto del regolamento 2018/1725 [12], sulla base del fatto che le osservazioni trasmesse riportavano dati pseudonimizzati.

Il Tribunale è stato, quindi, chiamato da CRU ad esprimersi sulla vicenda al fine di annullare il provvedimento del GEPD, ai sensi dell'art. 263 TFUE. I Giudici del Lussemburgo hanno evidenziato l'importanza della valutazione degli elementi fattuali per lo svolgimento della verifica sulla natura anonima o meno dei dati: se da un lato, come sostenuto dal GEPD, l'indisponibilità in capo a Deloitte delle informazioni aggiuntive necessarie per identificare gli autori delle osservazioni non consente di escludere a priori il trattamento dei dati personali, dall'altro lato, una siffatta verifica deve svolgersi dal punto di vista di Deloitte stessa[13] . Pertanto, precisa il Tribunale, incombeva sul GEPD esaminare se le osservazioni inviate a Deloitte costituissero dati personali, tenendo in conto se Deloitte disponeva di mezzi legali e realizzabili in pratica che le consentissero di accedere alle informazioni aggiuntive necessarie per la re-identificazione degli autori delle osservazioni.

In conclusione, l'approccio adottato dal Tribunale pare discostarsi dall'interpretazione del Garante italiano sopra menzionato, in aderenza, invece, a quanto precisato nelle linee guida dell'EPBD[14] e delle Autorità garanti nazionali per la protezione dei dati, che hanno delineato alcuni approdi interpretativi in materia di anonimizzazione dei dati.

Sulla stessa scorta si pongono anche le c.d. Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica, all. 4 del d.lgs. 196/2003 (Codice Privacy), novellato dal d.lgs. 101/2018, le quali forniscono indicazioni tecniche utili a valutare quando ricorra l'identificabilità dell'interessato e quali siano i criteri da osservare per la valutazione del rischio di identificazione.

Si tratta, qui, di elementi di natura fattuale che dovrebbero essere oggetto di valutazione, anche sotto i profili della ragionevolezza, in sede di accertamento ispettivo, con il rischio, altrimenti, di restringere eccessivamente le possibilità di utilizzo dei dati e, pertanto, di conduzione degli studi clinici, come avvenuto nel citato caso italiano.

[12] Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati.

[13] V., Tribunale UE, sentenza 26 aprile 2023, causa T-557/20, Comitato di risoluzione unico (CRU), ECLI:EU:T:2023:219., paragrafo 97.

[14] Nello specifico, il parere 05/2014 dell'EPBD osserva che, sebbene nessuna tecnica di per sé consenta un'anonimizzazione efficace, l'applicazione congiunta di più misure può ridurre il rischio in termini di: (*i*) "*single out*"; (*ii*) "*linkability*"; (*iii*) "*inference*". Tale verifica sulla riduzione del rischio, deve svolgersi caso per caso.

Downloaded from www.biodiritto.org.
ISSN 2284-4503

3. Le basi giuridiche dei trattamenti dei dati personali nell'ambito delle sperimentazioni cliniche in Europa

La pseudonimizzazione e l'anonimizzazione dei dati non esauriscono i requisiti normativi per la liceità del trattamento dei dati personali [15]. A tal fine, infatti, il trattamento deve fondarsi su di una tra le sei "basi giuridiche" previste dall'art. 6 GDPR[16], la cui individuazione spetta al titolare.
A seconda che il titolare sia un ente pubblico o privato, e tenuto conto dell'attività di sperimentazione svolta, il trattamento dei dati personali correlati esclusivamente alle attività di ricerca può prevedere tre diverse basi giuridiche. Queste basi giuridiche, insieme alle disposizioni di cui all'art. 9 GDPR inerenti ai dati particolari, costituiscono le condizioni di liceità del trattamento.
A tal proposito, infatti, l'art. 9 dispone un divieto al trattamento dei dati particolari, a meno che non ricorra una delle esenzioni previste al seguente paragrafo 2. Pertanto, qualsiasi trattamento dei dati personali particolari, per superare il vaglio di legittimità previsto dal GDPR, deve fondarsi su una delle basi giuridiche di cui all'art. 6, e allo stesso tempo, prevedere il ricorrere di una delle esenzioni di cui al citato paragrafo 2 dell'art. 9. È doveroso osservare che la prima base giuridica adottabile per fondare un trattamento di dati personali ai fini di ricerca clinica è «l'esecuzione di un compito di interesse pubblico» di cui all'art. 6, par. 1, lett. *e*). Il GDPR chiarisce, infatti, che nella definizione di pubblico interesse sono ricompresi anche finalità inerenti alla salute, quali la sanità pubblica, la protezione sociale e la gestione dei servizi di assistenza sanitaria. L'utilizzo di questa base giuridica, però, è condizionato da un duplice requisito: la conduzione delle sperimentazioni cliniche deve, da un lato, rientrare direttamente nel mandato conferito al titolare e, dall'altro lato, derivare da una norma del diritto dell'Unione o di uno Stato membro. In questo ambito, un singolo atto giuridico può essere sufficiente come base per più trattamenti.
Tuttavia, tale atto dovrà stabilire la finalità del trattamento, le caratteristiche in base a cui designare il titolare, il tipo di dati personali in oggetto, gli interessati, i soggetti cui possono essere comunicati i dati personali, le limitazioni della finalità, il periodo di conservazione e altre misure per garantire un trattamento lecito e corretto[17].
Anche il legittimo interesse del titolare del trattamento, di cui all'art. 6, par. 1, lett. *f*), può fondare la liceità del trattamento, ma in tal caso sarà necessario svolgere un bilanciamento tra gli interessi del titolare e le "ragionevoli aspettative" dei diritti dei partecipanti alla sperimentazione.
Entrambe le suddette basi giuridiche devono accompagnarsi all'applicazione di una delle esenzioni elencate al citato art. 9, par. 2. Si tratta, innanzitutto, dell'ipotesi di cui alla lett. *i*), secondo cui il trattamento dei dati particolari è lecito se «necessario per motivi di interesse pubblico nel settore della sanità pubblica, sulla base del diritto dell'Unione o degli Stati membri». In tal caso, il concetto di sanità

[15] Sulla liceità del trattamento v. D. POLETTI, *Art. 6 - Liceità del trattamento*, in AA. VV, *Codice Della Privacy E Data Protection*, Milano, 191.
[16] Sull'impostazione normativa data dal GDPR in campo sanitario v., P. GUARDA, *I dati sanitari,* in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo,* Torino, 2019, 591 ss.
[17] Comitato europeo per la protezione dei dati, Parere 3/2019 relativo alle domande e risposte sull'interazione tra il regolamento sulla sperimentazione clinica e il regolamento generale sulla protezione dei dati (articolo 70, paragrafo 1, lettera b), 23 gennaio 2019.

Downloaded from www.biodiritto.org.
ISSN 2284-4503

pubblica è da interpretarsi estensivamente, in virtù del riferimento esplicito al regolamento n. 1338/2008.

Alla luce di ciò, rientrano in questa esenzione di cui all'art. 9, par. 2, lett. *i*) i trattamenti svolti per la «protezione da gravi minacce per la salute a carattere transfrontaliero» oppure per «la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici».

Il GDPR precisa che il concetto di ricerca scientifica è da intendersi in senso lato ricomprendendo, ad esempio, sviluppo tecnologico e dimostrazione, ricerca fondamentale, ricerca applicata e ricerca finanziata da privati, nonché gli studi svolti nell'interesse pubblico nel settore della sanità pubblica. Le previsioni di cui alle lettere *i*) e *j*) sono accomunate, quindi, dalla "necessarietà" del trattamento in base all'interesse pubblico sotteso, dal rispetto dei principi di proporzionalità e di finalità, nonché dalla previsione di «misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato».

Quale terza base giuridica disponibile al titolare per i trattamenti in esame figura il consenso *ex* art. 6, par. 1, lett. *a*).

Con specifico riferimento alle categorie di dati particolari, tenuto conto della loro natura sensibile sotto il profilo dei diritti e delle libertà fondamentali, tale consenso deve essere manifestato per iscritto[18]. Tuttavia, il consenso, quale base giuridica del trattamento nell'ambito delle sperimentazioni cliniche, comporta alcune criticità[19].

In buona sostanza, il consenso non è considerato libero se l'interessato non può rifiutarlo, senza che dal rifiuto espresso possa derivarne un qualche pregiudizio.

Infatti, il consenso non parrebbe la condizione di liceità più adatta ad un contesto dove, spesso, l'interessato non ha reali alternative alla sua prestazione, a costo altrimenti di rischiare di non vedersi arruolato in una sperimentazione clinica che può rappresentare l'unica soluzione ai propri bisogni terapeutici[20].

Peraltro, tale orientamento è conforme a quanto previsto dall'art. 28[21] del Regolamento 536/2014 con

[18] Attraverso la prestazione di un siffatto consenso esplicito, il paziente acconsente quindi che il titolare svolga un trattamento dei suoi dati personali, anche di natura particolare e tale trattamento può considerarsi lecito *ex* artt. 6 e 9 GDPR.

[19] Ai sensi del combinato disposto dagli artt. 5, 6, par. 1, lett. *a*) e 7 GDPR, il consenso deve essere prestato attraverso un atto positivo con cui l'interessato manifesta una volontà libera, specifica, informata e — novità introdotta dal GDPR — "inequivocabile", relativa al trattamento dei dati personali che lo riguardano, con ciò prevedendosi che l'interessato abbia una scelta effettiva e il controllo sui propri dati. Il GDPR stabilisce che, qualora l'interessato non disponga di una scelta effettiva, sentendosi invece obbligato ad acconsentire oppure rischi di subire conseguenze negative per il diniego al trattamento dei propri dati, il consenso non potrà considerarsi come validamente acquisito.

[20] V., Linee guida 5 del 2020 sul consenso ai sensi del regolamento (UE) 2016/679, 8 ss. In letteratura v., M. GUIDI, *L'interazione tra la normativa dell'ue in materia di protezione dei dati personali e il regolamento ue 536/2014 sulle sperimentazioni cliniche,* in *Diritto dell'Informazione e dell'Informatica*, 2, 2024, 157 ss.

[21] Tale norma specifica che: «ai fini della certificazione della libertà del consenso informato, lo sperimentatore dovrebbe tenere conto di tutte le pertinenti circostanze che possono influenzare la decisione di un potenziale soggetto di partecipare a una sperimentazione clinica, in particolare l'eventuale appartenenza del soggetto a un gruppo economicamente o socialmente svantaggiato o magari una sua situazione di dipendenza istituzionale o gerarchica potenzialmente in grado di influire in maniera non appropriata sulla decisione di partecipare».

Downloaded from www.biodiritto.org.
ISSN 2284-4503

riferimento al (differente) formato, requisito essenziale delle sperimentazioni cliniche che coinvolgono gli esseri umani[22]. Dunque, la prestazione di tali forme di consenso risponde a differenti necessità: da una parte, la tutela del diritto alla protezione dei dati di carattere personale, con riferimento al consenso previsto dal GDPR; dall'altra parte, la tutela del diritto alla dignità umana e all'integrità dell'individuo, per quanto attiene invece all'obbligo di raccolta del consenso informato dei partecipanti a una sperimentazione clinica.

Ciononostante, rispetto ad entrambi i suddetti consensi, soprattutto nell'ambito di sperimentazioni cliniche delicate quali, ad esempio, quelle relative ai farmaci salvavita, possono sorgere seri interrogativi sul pieno rispetto del principio della libertà della prestazione del consenso. Ne consegue la necessità di prevedere, in merito al consenso informato di carattere medico, una verifica rafforzata sulle intenzioni e condizioni del singolo che sottendono la sua decisione di sottoporsi alla sperimentazione clinica, adottando specifiche salvaguardie quali lo «scambio comunicativo continuo e interattivo» con i ricercatori e l'adeguamento agli «effettivi rischi e benefici di ciascun protocollo»; in merito al consenso sulla privacy, l'adozione di altre basi giuridiche, quali l'esecuzione di un compito di interesse pubblico o, in via residuale, il legittimo interesse.

4. Le basi giuridiche dei trattamenti correlati a finalità di tutela della salute. L'uso primario e secondario dei dati

Come detto, l'uso primario dei dati comprende i trattamenti correlati a finalità di tutela della salute, espressamente previsti dal Regolamento e correlati al monitoraggio delle condizioni di salute del paziente arruolato nello studio. Derivando da previsioni di legge, tali trattamenti possono considerarsi come necessari «per adempiere un obbligo legale al quale è soggetto il titolare del trattamento», ex art. 6, par. 1, lett. *c*) GDPR[23]. Tuttavia, anche questa base giuridica deve accompagnarsi alla già citata esenzione *ex* art. 9, par. 2, lett. *i)* GDPR, al fine di rendere lecito il trattamento dei dati sulla salute. Nell'ambito delle sperimentazioni cliniche, i dati personali possono essere utilizzati dal soggetto sperimentatore per fini scientifici diversi da quelli indicati nel protocollo di studio.

[22] F. Forni, *Consenso informato e sperimentazione clinica nella normativa dell'Unione europea*, in *Diritto comunitario e degli scambi internazionali*, 2012, 215.

[23] Si tratta dei trattamenti dei dati relativi agli obblighi imposti dal Regolamento in tema di: (*i*) reportistica della sintesi dei risultati della sperimentazione che, ai sensi dell'art. 37, para. 4 e 8, il promotore deve pubblicare sulla banca dati UE; (*ii*) comunicazione degli eventi avversi e di eventi avversi gravi, da parte dello sperimentatore al promotore, *ex* art. 41; (*iii*) comunicazione delle sospette reazioni avverse che, *ex* art. 42, devono essere riportate dal promotore all'Agenzia regolatoria nazionale, tramite la banca dati elettronica per le comunicazioni in materia di sicurezza di cui all'art. 40; (*iv*) monitoraggio obbligatorio, da parte del promotore, sull'affidabilità dei dati comunicati e sulla conduzione della sperimentazione, ai sensi dell'art. 48; (*v*) obblighi di registrazione, elaborazione, gestione e conservazione, in capo al promotore o allo sperimentatore, di tutte le informazioni sulla sperimentazione clinica, assicurando al contempo la riservatezza dei dati personali degli interessati, anche attraverso la previsione di misure tecniche e organizzative idonee a limitare il rischio di "*data breach*", ai sensi dell'art. 56; (*vi*) archiviazione del FSE permanente, inclusivo di tutti i documenti essenziali e i dati clinici generati durante la conduzione dello studio, per venticinque anni, come prescritto dall'art. 58; e, infine, (*vii*) sottoposizione ad attività ispettive condotte dall'autorità di uno Stato membro e relative anche ai dati clinici dei soggetti arruolati, *ex* art. 78.

Downloaded from www.biodiritto.org.
ISSN 2284-4503

Il c.d. uso secondario dei dati clinici, ricondotto al "trattamento ulteriore" di cui all'art. 5, par. 1, lett. *b*) GDPR[24], è particolarmente diffuso, a fronte della maggiore disponibilità dei dati dei pazienti che, conservati in archivi sanitari, offrono utili spunti di indagine su impieghi innovativi di farmaci, non prevedibili al tempo della loro raccolta.

Il trattamento dei dati personali per uso secondario gode di una presunzione di compatibilità con il trattamento per uso primario, con effetti in termini di riduzione degli oneri sostanziali e procedimentali in capo al titolare[25]. Tuttavia, l'art. 89 GDPR stabilisce l'obbligo di adottare la predisposizione di apposite misure tecniche e organizzative, per la tutela dei diritti e della libertà dell'interessato; inoltre, l'art. 6, par. 4 GDPR prevede obblighi aggiuntivi, ove il trattamento non sia fondato sul consenso dell'interessato o su un atto legislativo dell'Unione europea o degli Stati membri[26].

Il rispetto di tali disposizioni farebbe venire meno l'obbligo di richiesta di un ulteriore consenso agli interessati[27].

Tuttavia tale "agevolazione" potrebbe incontrare alcuni limiti pratici, dovuti alla libertà concessa agli Stati membri in merito alla possibilità di prevedere "disposizioni più specifiche" riguardo alle basi giuridiche del GDPR, nonché di apporre "ulteriori condizioni, comprese limitazioni" al trattamento dei dati sulla salute *ex* art. 9, par. 4.

Non deve pertanto stupire che nella legislazione degli Stati membri si riscontrino notevoli differenze.

5. Il consenso quale base giuridica per l'uso primario e secondario dei dati personali

L'art. 110 del Codice Privacy [28]prevede espressamente che i trattamenti dei dati sulla salute, per scopi primari e secondari, nell'ambito delle sperimentazioni cliniche sono ammissibili solo previa acquisizione del consenso dell'interessato.

Tale principio conosce due eccezioni: a) quando la ricerca viene svolta in base a disposizioni normative o regolamentari, il trattamento dovrà essere preceduto dalla redazione di una valutazione di impatto ai sensi degli artt. 35 e 36 GDPR; b) quando per ragioni particolari, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, o rischia di rendere impossibile (o di pregiudicare

[24] Secondo cui, qualora i dati siano soggetti ad un nuovo trattamento per finalità di ricerca scientifica, essa non è considerata a priori incompatibile con la finalità iniziale, salvo il rispetto dell'art. 89, par. 1 GDPR.

[25] Si veda a tal proposito A. Cabrio, *La seconda vita dei dati. Luci e ombre della normativa* privacy *in materia di* secondary data use, in F. Frattini (a cura di), *I dati. Il futuro della sanità: strumenti per una reale innovazione,* Milano, 2022, 25 ss.; G. Maglio, *L'uso dei dati nella Sanità: difficoltà procedurali e legislative, 2023,* in *agendadigitale.it*

[26] In tali casi, infatti, il titolare deve tenere conto: «*a*) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto; *b*) del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'interessato e il titolare del trattamento; *c*) della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali ai sensi dell'articolo 9; *d*) delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati».

[27] In tal senso può citarsi, ad esempio, l'art. 14, par. 5, lett. *b*) GDPR che esenta il titolare del trattamento dall'obbligo di fornire l'informativa privacy di cui ai par. da 1 a 4 dell'art. 14 GDPR, nella misura in cui ciò risulti impossibile o implichi uno sforzo sproporzionato.

[28] Codice in materia di protezione dei dati personali (D. lgs 30 giugno 2003, n.196).

Downloaded from www.biodiritto.org.
ISSN 2284-4503

gravemente) il conseguimento delle finalità della ricerca[29]. Inoltre, occorre tenere presente che gli ulteriori trattamenti e la conservazione dei dati personali per scopi di ricerca scientifica sono ammessi nei limiti posti dal quadro normativo di riferimento, sia nazionale che europeo, dalle Prescrizioni relative al trattamento dei dati personali effettuato per scopi di ricerca scientifica del 5 giugno 2019" e dalle regole di deontologia.

In particolare, queste ultime stabiliscono, per trattamenti a fini statistici o di ricerca scientifica, l'obbligo di implementare idonee forme di pubblicità. Una serie, quindi, di requisiti procedurali gravosi, che discendono dalla previsione del consenso quale unica base giuridica del trattamento dei dati personali per fini di ricerca scientifica, circostanza che rappresenta un *unicum* a livello europeo. Ancora più restrittiva è la norma applicabile ai trattamenti dei dati personali svolti da soggetti differenti rispetto a quello che ha redatto il protocollo di studio, per finalità ulteriori rispetto a quelle originariamente previste nel protocollo.

Dal punto di vista pratico, il trattamento dei dati per finalità ulteriori rispetto a quelle che ne avevano contraddistinto la raccolta svolta da un precedente titolare tende, rispetto alle ipotesi di cui all'art. 110, a riguardare interessati non più in grado, per via delle loro condizioni cliniche, di comprendere il contenuto del consenso, oppure decedute.

Da ciò consegue un'elevata complessità, per il nuovo promotore, di riuscire a contattare gli interessati al fine di richiedere loro di prestare nuovamente il proprio consenso[30]. Il tema dei trattamenti di dati personali nell'ambito della sperimentazione clinica può comportare l'emergere di istanze contrapposte: si rende necessario, pertanto, svolgere un processo di bilanciamento tra il diritto alla salute e il diritto alla protezione dei dati personali.

Da quest'ultima derivano, in favore dei partecipanti alle ricerche cliniche, le tutele in tema di trasparenza sull'utilizzo che si intenda fare dei loro dati personali[31], la necessità che il trattamento sia lecito nonché l'applicazione di misure di sicurezza volte a ridurre il rischio di utilizzi impropri dei dati. A livello dell'UE, tale bilanciamento deve essere effettuato secondo quanto previsto dall'art. 52, par. 1 della Carta dei diritti fondamentali dell'Unione europea[32].

Come ben stabilito dalla Corte di giustizia, l'esito di questo esame potrà comportare la compressione della tutela dei dati personali, intesa nella sua dimensione individuale, in virtù della valorizzazione della

[29] Il titolare deve, inoltre, dimostrare di aver adottato misure appropriate volte alla tutela dei diritti dell'interessato e aver sottoposto la sperimentazione al vaglio tanto del competente comitato etico a livello territoriale, quanto del Garante per la protezione dei dati personali, che sottoporrà al proprio controllo anche le ragioni che ostano al pieno espletamento degli obblighi informativi da parte del titolare.

[30] Dal punto di vista procedurale, invece, mentre le eccezioni all'utilizzo del consenso, quale base giuridica, ricalcano sostanzialmente quanto già previsto dall'art. 110, diverso risulta l'*iter* approvativo del trattamento dei dati ai fini di ricerca. Alla previa consultazione del Garante ai sensi dell'art. 36 GDPR, disposta dal citato art. 110, si contrappone l'autorizzazione preventiva di cui all'art. 110-*bis* per gli utilizzi ulteriori dei dati da parte dei terzi. Tale autorizzazione è ottenibile tramite decisione del Garante da adottarsi entro quarantacinque giorni dalla richiesta, decorsi i quali la mancata pronuncia equivale a rigetto.

[31] Sul piano del diritto italiano i dati personali formano una componente essenziale dell'identità dell'individuo e, per tale ragione, devono essere oggetto di una tutela rigorosa. Il diritto alla riservatezza dei dati personali costituisce, infatti, una manifestazione del diritto all'intangibilità della sfera privata.

[32] che stabilisce la legittimità delle restrizioni all'esercizio dei diritti fondamenti, a condizione che esse siano: (*i*) stabilite per legge; (*ii*) rispettose del nucleo essenziale del diritto compresso; (*iii*) proporzionate; e (*iv*) necessarie e dirette a finalità di interesse generale riconosciute dall'UE o alla protezione dei diritti e libertà altrui.

Downloaded from www.biodiritto.org.
ISSN 2284-4503

Call

sua funzione sociale, economica e di pubblica sicurezza [33]. Pertanto, le misure di pseudonimizzazione possono ben costituire uno strumento per garantire la privacy dei soggetti partecipanti alla sperimentazione e, contestualmente, non comprimere eccessivamente le possibilità di riutilizzo dei dati per ulteriori scopi clinici.

Si tratterebbe di un esempio di detto contemperamento. Di contro, sia l'interpretazione restrittiva del Garante per la protezione dei dati personali sulle tecniche di anonimizzazione dei dati adottata nel caso *Thin*, sia l'imposizione da parte del legislatore italiano del consenso quale base giuridica preferenziale, sembrano costituire un'eccessiva limitazione allo svolgimento della ricerca clinica.

Sotto il primo profilo, il *test* sulla anonimizzazione dei dati, soprattutto quando riferiti ai *big data*, dovrebbe basarsi su criteri di sufficienza e ragionevolezza in luogo dell'appiattimento verso indici di assolutezza che ben poco si attagliano ad un contesto, quello tecnologico, in continua evoluzione.

Sotto il secondo profilo, l'uso del consenso in via preferenziale non risulta trovare riscontro nel GDPR, dove le tre basi giuridiche spendibili per trattamenti in ambito di ricerca clinica sono disposte sul medesimo livello di rilevanza. Inoltre, il consenso non sembra garantire sufficientemente la libertà di scelta dell'interessato, date le conseguenze, in termini di salute, di un suo eventuale rifiuto e risulta squilibrato se osservato dal punto di vista dell'asimmetria informativa tra il paziente e il promotore della ricerca clinica.

Infine, gli artt. 110 e 110-*bis* devono leggersi all'interno della più ampia cornice del GDPR.

Sul punto si è recentemente espressa anchela Corte di Giustizia dell'Unione europea[34].

Nell'ambito del rinvio pregiudiziale avente ad oggetto l'interpretazione della normativa tedesca sul trattamento dei dati personali particolari, svolto da un organismo di controllo medico in qualità di servizio medico, nei confronti di un proprio dipendente, al fine di valutarne la capacità lavorativa, la Corte si è espressa sugli spazi di libertà concessi dall'art. 9, par. 4 GDPR agli Stati membri.

A tal proposito, i Giudici del Lussemburgo hanno precisato che: «uno Stato membro che intenda avvalersi della facoltà concessa all'articolo 9, paragrafo 4, di detto regolamento dovrebbe, conformemente al principio di proporzionalità, garantire che le conseguenze pratiche, segnatamente di ordine organizzativo, economico e sanitario, derivanti dagli ulteriori obblighi di cui tale Stato intende imporre il rispetto, non siano eccessive nei confronti dei titolari di un tale trattamento, i quali non dispongono necessariamente di dimensioni o di risorse tecniche e umane sufficienti per soddisfare tali obblighi».

Orbene, gli articoli 110 e 110-*bis* del Codice Privacy causano una restrizione eccessiva allo svolgimento di trattamenti di dati personali nell'ambito delle sperimentazioni cliniche, soprattutto da parte di operatori economici di piccole-medie dimensioni, non in grado di adempiere ai gravosi oneri procedurali imposti da tali norme. Un ulteriore contrasto potrebbe ravvisarsi, invece, tra gli obiettivi del GDPR: il contemperamento del diritto alla protezione dei dati personali e l'implementazione della libera circolazione di tali dati, nell'ambito delle sperimentazioni cliniche, pare distante dal trovare una composizione accurata, nonostante l'ambito della ricerca scientifica rientrasse fra quelli ritenuti maggiormente oggetto dell'intervento uniformatore operato proprio attraverso il GDPR. Mentre, quindi, la tutela rafforzata del trattamento dei dati sulla salute sembra costituire una misura ragionevole per la protezione

[33] Corte di giustizia dell'Unione europea, sentenza del 9 novembre 2010, Volker und Markus Schecke e Eifert, cause riunite C-92/09 e C-93/09, in *DeJure Online.*

[34] Corte di giustizia dell'Unione europea, sentenza del 21 dicembre 2023, ZQ, causa C-667/21, in *DeJure Online.*

Downloaded from www.biodiritto.org.
ISSN 2284-4503

del diritto alla vita privata, le menzionate discrepanze tra le discipline nazionali, sotto il profilo delle condizioni di liceità, rappresentano una limitazione alla libera circolazione e all'utilizzo di questi dati che non sembra affatto giustificabile in base allo spirito del GDPR. A tal proposito, l'art. 1 GDPR stabilisce un preciso divieto di limitare la libera circolazione dei dati personali nell'Ue «per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali».
Tali limitazioni possono fondarsi sui motivi di ordine pubblico, di pubblica sicurezza e di sanità pubblica, da applicarsi alla luce del principio di proporzionalità e della giurisprudenza della Corte di Giustizia dell'Unione europea. Motivi, questi, che non paiono ricorrere nell'ambito della restrizione alla circolazione dei dati sulla salute fine delle sperimentazioni cliniche. Inoltre, gli spazi di libertà, in capo agli Stati membri, sul mantenimento o introduzione di ulteriori condizioni, anche limitative, al trattamento dei dati relativi alla salute, non devono «ostacolare la libera circolazione dei dati personali all'interno dell'Unione quando tali condizioni si applicano al trattamento transfrontaliero degli stessi» .
Una lettura uniforme di tali fattispecie comporta difficoltà nello svolgimento di sperimentazioni che assumono un significato fondamentale per la piena applicazione del diritto alla salute sotto il profilo dell'accessibilità a farmaci innovativi. In conclusione, il pianificato intervento dell'EDPB sul tema delle sperimentazioni cliniche, sia il regolamento sull'intelligenza artificiale[35] e, soprattutto, sullo spazio europeo dei dati sanitari potranno costituire un utile strumento per dare adeguate risposte alle suddette criticità, considerando il carattere non assoluto del diritto alla protezione dei dati personali che deve essere contemperato con l'applicazione di altri diritti fondamentali, in ossequio ai principi delineati dalla Corte di Giustizia.

6. Il trattamento dei dati sanitari digitalizzati

La raccolta dei dati digitali pone il problema di ripensare il diritto alla tutela dei dati personali, che rappresenta un traguardo legislativo recentemente acquisito nella legislazione italiana ed europea[36].
Alcuni studiosi osservano come l'idea di *privacy*, originariamente intesa alla stregua di diritto della persona, rappresenta oggi un equivoco, a fronte di una nozione sempre più marcatamente patrimoniale dei dati personali, che sono diventati una nuova e importante ricchezza nel sistema dell'economia digitale[37].
La destinazione pubblica dei dati sanitari rappresenta un tema generalmente molto dibattuto in materia sanitaria.
La relazione tra i beni comuni e le informazioni si è rafforzata nelle teorie dei giuristi che avanzano proposte volte a costruire e proteggere i nuovi beni comuni della conoscenza[38].

[35] Sul punto, G. SMORTO, *Distribuzione del rischio e tutela dei diritti nel regolamento europeo sull'intelligenza artificiale. Una riflessione critica*, in *Foro italiano*, 5, IV, 2024, c. 208.
[36] A sostegno di una linea ermeneutica che valorizzi lo sforzo del legislatore europeo di rendere il sistema di protezione dei dati personali strumentale alla realizzazione dei diritti fondamentali v., su tutti, P. PERLINGIERI, Privacy *digitale e protezione dei dati personali tra persona e mercato,* in *Foro napoletano,* 2018*,* 481 ss.
[37] V. RICCIUTO, *L'equivoco della* privacy. *Persona* vs *dato personale*, Napoli, 2022.
[38] A. PRADI, *I beni comuni digitali*, Napoli, 2014.

Downloaded from www.biodiritto.org.
ISSN 2284-4503

Pertanto, le potenzialità di circolazione, fruizione e conservazione dei dati sanitari offerte dalla digitalizzazione[39] degli stessi hanno portato ad un dibattito sulla necessità di poterne condividere i benefici, ponendo l'esigenza di comprenderli nella nozione di beni comuni che, pur in assenza di una precisa definizione da parte del legislatore, raccoglie una crescente attenzione da parte di giuristi[40] ed economisti, oltre che dal formante giurisprudenziale[41].

Il riutilizzo e l'accessibilità dei dati aperti[42] devono essere contemperati con le esigenze della protezione dei dati personali degli interessati[43].

Volendo focalizzare l'attenzione sui dati sanitari digitalizzati, occorre garantire la possibilità di raccoglierli e di convertirli in formati interoperabili, condivisi e utilizzabili che funzionino con informazioni provenienti da diverse sorgenti.

Il Regolamento europeo 2022/8681 (c.d. *Data Governance Act)* introduce alcune disposizioni innovative volte ad ampliare il concetto di dato pubblico: da un lato, regolando la condivisione volontaria dei dati messi a disposizione dai cittadini stessi per finalità di interesse generale (ricerca scientifica, assistenza sanitaria), sollecitando la partecipazione attiva di questi per il miglioramento dei servizi pubblici, dall'altro, creando nuovi strumenti volti a fornire il riutilizzo dei dati oggetto dei diritti di terzi in possesso delle autorità pubbliche[44]; da una parte, la facoltà delle amministrazioni pubbliche di riutilizzare dei dati personali oggetto dei diritti di terzi in loro possesso impone alle medesime di garantire un riuso sicuro, predisponendo un ambiente adeguato e adoperando tecniche di condivisione attuali ed efficienti.

Ciò costituisce una funzione fondamentale dello Stato cui è attribuita la competenza legislativa esclusiva, *ex* art. 117, comma 2, Cost.

Pertanto, il settore sanitario rappresenta uno dei settori strategici nei quali la normativa europea mira ad istituire spazi di dati comuni che dovrebbero essere resi trovabili, interoperabili, accessibili e riutilizzabili garantendo un alto livello di sicurezza informatica.

---

[39] M.R. Nuccio, *Digitalizzazione e circolazione dei dati sanitari*, in *Tecnologia e Diritto*, 2, 2023, 357 ss.

[40] S. Rodotà, *Il terribile diritto: studi sulla proprietà privata e beni comuni,* Bologna, 1981, il quale ha anche elaborato una proposta legislativa nel 2007. Il tema è stato alimentato, tra gli altri, da U. Mattei, *Beni comuni. Un manifesto*. Bari, 2012.

[41] In Italia la giurisprudenza di legittimità ebbe ad occuparsene già con la sentenza (Cass. 9 marzo 1887), tornando a ribadire la nozione con la decisione delle Sezioni Unite 14 febbraio 2011, n. 3665.

[42] Art. 1, comma 1, lett. 1-*ter*, del CAD definisce i dati di tipo aperto come «i dati che presentano le seguenti caratteristiche: 1) sono disponibili secondo i termini di una licenza o di una previsione normativa che ne permetta l'utilizzo da parte di chiunque, anche per finalità commerciali, in formato disaggregato; 2) sono accessibili attraverso le tecnologie dell'informazione e della comunicazione, ivi comprese le reti telematiche pubbliche e private, in formati aperti ai sensi della lett. l-*bis*), sono adatti all'utilizzo automatico da parte di programmi per elaboratori e sono provvisti dei relativi metadati; 3) sono resi disponibili gratuitamente attraverso le tecnologie dell'informazione e della comunicazione, oppure sono resi disponibili ai costi marginali sostenuti per la loro riproduzione e divulgazione».

[43] Questo può essere facilitato applicando correttamente i Principi FAIR sin dalla progettazione del sistema di raccolta dei dati stessi. In tal modo la *privacy* non sarebbe un ostacolo, ove il trattamento venga attuato tramite algoritmi adeguati a garantire la sicurezza e l'esattezza dei dati sanitari digitali.

[44] Il regolamento crea lo *status* di fornitore di servizi di intermediazione dati, ossia quei soggetti che forniscono un ambiente sicuro in cui privati e aziende possono condividere i dati correttamente attraverso apposite piattaforme digitali.

Downloaded from www.biodiritto.org.
ISSN 2284-4503

Una soluzione utilizzata per rendere compatibile la circolazione dei dati sanitari digitalizzati con il trattamento dei medesimi, nel rispetto del diritto dell'interessato appare quella di renderli anonimi, garantendo la non identificabilità dell'interessato medesimo.
Il dato informativo reso anonimo non è più un dato personale e, pertanto, non rientra nell'ambito di applicazione del GDPR, essendo riutilizzabile per le suddette finalità.
In conclusione, la libera circolazione[45] del dato, senza applicare delle misure di tutela dell'interessato come prevista dal GDPR, può avvenire solo per i dati anonimi.
Tuttavia, anche per i dati pseudonimizzati[46] e de-identificati[47] è possibile un impiego, sebbene senza esclusione della reviviscenza della tutela dell'interessato ove venisse identificato e della responsabilità del titolare del trattamento.

7. *European Health Data Space*: l'accessibilità ai dati sanitari

L'accessibilità ai dati sanitari presenta un duplice aspetto: da un lato, offre al personale medico il trattamento dei dati sanitari, concedendo una visione d'insieme dello storico del paziente; dall'altro, apre possibili varchi all'utilizzo da parte di soggetti non legittimati ad agire in questi sistemi.
Sull'argomento è intervenuta l'Unione Europea con un accordo politico sullo Spazio Europeo dei Dati Sanitari con l'obiettivo di armonizzare le disposizioni riguardanti il fascicolo e il dossier sanitario in tutta l'Ue. Per comprendere la questione è opportuno premettere brevi cenni sulle linee guida del 16 luglio 2009 emanate dal Garante, il cui obiettivo è l'individuazione di un primo quadro di cautele concernenti l'accesso ai dati, le specifiche garanzie, responsabilità e i relativi diritti dei titolari. Nelle disposizione *de quibus* si rinviene per la prima volta una definizione di *dossier* e di fascicolo sanitario[48]: il primo è l'insieme dei dati personali, generati da eventi clinici, presenti e trascorsi, riguardanti l'interessato, i quali vengono condivisi tra i professionisti sanitari che lo assistono presso un'unica struttura sanitaria; il fascicolo sanitario è, invece, la cartella formata con riferimento a dati sanitari originati da diversi titolari del trattamento operanti in uno stesso ambito territoriale. Il titolare deve valutare, dunque, quali dati inserire nel fascicolo e nel dossier in relazione alla necessità di prevenzione, diagnosi, cura e riabilitazione e in virtù del consenso autonomo e specifico accordato dal paziente, rispettando il principio di minimizzazione (art 5. GDPR). In aggiunta a quanto sopra delineato, le linee guida nazionali del

[45] C. Perlingieri, *Transizione digitale nella sanità,* in *Tecnologia e Diritto*, 2, 2024, 485 ss.
[46] Il dato pseudonimizzato è reso solo transitoriamente anonimo tramite lo scorporo di alcune informazioni, che vengono conservate separatamente in modo da impedire l'identificazione del soggetto interessato (disciplinato dal GDPR). Per i dati pseudonimizzati la scelta del trattamento adeguato è rimessa al responsabile del trattamento, secondo il principio dell'*accountability*.
[47] I dati de-identificati sono una nuova categoria di dati che si inserisce tra i dati anonimi e pseudonimi e si distinguono da questi ultimi in quanto è proprio il soggetto interessato che può fornire quelle informazioni aggiuntive che provocano la re-identificazione; nei dati pseudonimi è il titolare del trattamento che custodisce adeguatamente le ulteriori informazioni che ne permettono l'identificazione. Il titolare del trattamento non potrà ritenersi esonerato dall'adozione delle opportune cautele per il trattamento del dato personale, laddove il dato ridivenisse tale per effetto della re-identificazione dell'interessato.
[48] C. Lolli, *FSE e Operatori sanitari* (E-Health): *Il Fascicolo Sanitario,* Milano, 2022*, passim.*

Downloaded from www.biodiritto.org.
ISSN 2284-4503

2010[49] e le successive linee guida comunitarie del 2015[50] si sono occupate principalmente dei requisiti che legittimano l'accesso al *dossier* o al fascicolo sanitario. In primo luogo, sono abilitati all'accesso solo coloro che assistono il paziente, fornendo cure e servizi. In secondo luogo, gli operatori sanitari sono legittimati ad accedere alle cartelle mediche dei soli pazienti che sono sottoposti a un trattamento, circoscrivendo tale accesso al limitato periodo della terapia. Successivamente, nel marzo 2022 è stato presentato dalla Commissione il progetto ideativo dello Spazio Europeo dei Dati Sanitari (EDHS)[51] e del fascicolo sanitario europeo, approvato nel mese di aprile 2024, il cui obiettivo è quello di «migliorare l'accesso delle persone fisiche ai loro dati sanitari elettronici personali e il loro controllo su tali dati […]. Il suo obiettivo è inoltre di migliorare il funzionamento del mercato interno istituendo un quadro giuridico uniforme in particolare per quanto riguarda lo sviluppo, la commercializzazione e l'uso di sistemi di cartelle cliniche elettroniche in conformità ai valori dell'Unione[52]».

In particolare, l'art.2 comma 2 lett. d) ed e) e l'art 5 della proposta definiscono l'uso primario dei dati sanitari elettronici come: il trattamento per la prestazione di servizi sanitari al fine di valutare, mantenere o ripristinare lo stato di salute della persona fisica.

Ai sensi dell'art. 34, l'uso secondario dei dati è ravvisabile, invece, nel trattamento funzionale ad attività di ricerca, istruzione, assistenza, sviluppo e innovazione, sicurezza e valutazione, attività di pubblico interesse nell'ambito della sanità pubblica e della medicina del lavoro.

La vera novità del Regolamento è rappresentata dall'apertura all'utilizzo dei dati sanitari per finalità che esulano dalla cura e dai trattamenti con la possibilità di instaurare una collaborazione tra privati, istituzioni e la collettività intera; così facendo si prevede un risparmio di 5 miliardi di euro nei prossimi 10 anni, grazie ad un ponderato uso dei dati sanitari per finalità di ricerca, innovazione e sviluppo di nuove *policy*.

La realizzazione dell'EHDS comporta una fondamentale interoperabilità dei sistemi informatici e delle conoscenze nonché una crescita addizionale del mercato sanitario digitale del 20-30%, cifre proporzionate all'efficientamento perseguito e al reale vantaggio per i pazienti. Il testo finale del Regolamento EHDS ha introdotto novità significative: l'interoperabilità e lo scambio di dati viene oggi esteso non solo tra i sistemi *EHR (Electronic Health Records*), ma anche ad altri servizi di accesso ai dati sanitari al fine di garantire uno scambio efficace di dati tra diversi sistemi e Paesi.

I sistemi di cartelle cliniche elettroniche devono dimostrare la conformità alle prescrizioni essenziali riguardo a interoperabilità e sicurezza definite dalla UE.

La Commissione dovrà fornire aggiornamenti regolari del formato europeo di scambio delle cartelle cliniche elettroniche, per integrare le revisioni dei sistemi di codifica e nomenclatura sanitari.

L'obiettivo è assicurare che i dati scambiati siano sempre pertinenti e utilizzabili, evitando futuri problemi di incompatibilità[53].

[49] Ministero della Salute, il Fascicolo Sanitario Elettronico. Linee guida Nazionali dell'11 novembre 2010.

[50] Garante per la Protezione dei Dati Personali, Linee guida in materia di dossier sanitario del 4 giugno 2015.

[51] Proposta di Regolamento del Parlamento Europeo e del Consiglio sullo spazio europeo dei dati sanitari, 2022/0140 (COD).

[52] Considerando 1 della proposta di Regolamento.

[53] Sono stati inoltre introdotti meccanismi efficaci per l'identificazione *online* e *offline* di persone fisiche e professionisti sanitari, basandosi sulla normativa dell'identità digitale europea.

Downloaded from www.biodiritto.org.
ISSN 2284-4503

Un'importante novità è rappresentata, poi, dall'introduzione di meccanismi di *opt-out* per l'uso secondario dei dati (il testo finale stabilisce i tipi di dati che possono essere utilizzati per finalità specifiche e le finalità vietate) il cui obiettivo è bilanciare le esigenze di ricerca e innovazione con il diritto alla *privacy*, consentendo alle persone fisiche un maggiore controllo sull'uso dei propri dati.

Tra le altre novità, occorre menzionare, l'istituzione di un'infrastruttura transfrontaliera obbligatoria per l'uso primario e secondario dei dati sanitari elettronici e l'introduzione un sistema di etichettatura volontaria per le applicazioni *wellness* che dichiarino interoperabilità con i sistemi EHR.

Tre sono i vantaggi evidenziati derivanti dall'implementazione dell'EHDS: una maggiore accuratezza diagnostica; l'efficienza dei costi; il sostegno all'invecchiamento della popolazione.

L'EHDS svolgerà un ruolo cruciale nell'affrontare le sfide poste dall'innovazione digitale della sanità, migliorando il coordinamento dell'assistenza sanitaria, ottimizzando i costi delle cure e sostenendo la ricerca. La disponibilità di dati sanitari con adeguati *standard*s qualitativi è il principale catalizzatore dello sviluppo di soluzioni digitali a supporto di decisioni cliniche affidabili e diagnosi sempre più accurate e precoci, costituendo l'EHDS un'opportunità unica per favorire la competitività europea in questo settore.

Lo spazio europeo dei dati sarà un pilastro dell'Unione europea della salute nonché il primo spazio Comune di dati dell'Ue in un settore specifico a emergere dalla strategia europea per i dati. L'EHDS permetterà ai pazienti di assumere il pieno controllo dei propri dati sanitari, facilitandone lo scambio per la fornitura di assistenza sanitaria in tutta l'Unione europea. Si promuove così anche un mercato unico per i sistemi di cartelle cliniche elettroniche e si attua un sistema affidabile ed efficiente per il riutilizzo dei dati sanitari ai fini di ricerca, sviluppo e innovazione, addestramento di algoritmi: ossia il c.d. uso secondario dei dati, per cui vi sarà una apposita piattaforma elettronica. Tuttavia, ciò non deve compromettere la tutela dei diritti fondamentali degli individui.

Gli organismi responsabili dell'accesso ai dati sono tenuti a condividere i dati nel rispetto del principio di minimizzazione e di limitazione della finalità, privilegiando la fornitura anonimizzata ove ciò ha risulti sufficiente rispetto alle finalità del trattamento del soggetto richiedente; laddove questo non sia sufficiente, l'accesso dovrà essere garantito previa pseudonimizzazione dei dati, i cui codici di decodifica sono detenuti esclusivamente all'organismo responsabile di riferimento, con divieto per l'utente di compiere operazioni di Reid identificazione (art 40 EHDS). In sintesi, il cosiddetto uso secondario dei dati ai fini di addestramento, prova e valutazione degli algoritmi, anche nell'ambito di dispositivi medici, sistemi di IA e applicazioni di sanità digitale. In tal modo, l'EHDS rappresenta una porta di accesso ai dati sanitari con lo scopo di favorire la creazione di dataset sintetici che vengano sfruttati per affinare applicazioni di IA nel campo sanitario. In ogni caso risulta essenziale garantire una maggiore armonizzazione con riferimento alla protezione dei dati personali in ambito sanitario[54]. A tal fine l'European Data Protection supervisor ha incoraggiato l'adozione di codici di condotta aventi ad oggetto specifiche linee guida per il trattamento dei dati sanitari al fine di fornire un quadro uniforme, auspicando misure che favoriscano la fiducia dei pazienti nel sistema di condivisione di dati che l'Ue vuole realizzare. L'

[54] Il GDPR, infatti, consente agli Stati membri di prevedere specifiche deroghe sia sotto il profilo dell'esercizio dei diritti da parte degli interessati sia con riferimento alle basi giuridiche per il trattamento di tali dati, con il rischio di favorire approcci differenziati tra gli Stati membri che potrebbero rappresentare un ostacolo alla raccolta dei dati all'interno dello spazio sanitario europeo.

Downloaded from www.biodiritto.org.
ISSN 2284-4503

EDPS evidenzia l'importanza di incorporare forme di garanzia per la protezione dei dati nello sviluppo e nella governance dello spazio europeo dei dati sanitari. L'Autorità europea ha incoraggiato il rispetto dei principi di cui all'art 5 GDPR da parte dei soggetti che rendono disponibili i dati; inoltre, il ricorso a misure organizzative e tecniche a protezione dei dati personali, tra cui le cui tecniche di anonimizzazione nonché di pseudonimizzazione

8. Doveri e obblighi informativi in sanità

La condivisione tra paziente e sanitario dell'esperienza decisionale che precede l'avvio di un atto diagnostico o di una cura rappresenta un momento centrale di garanzia di diritti di rilievo costituzionale, nonché presupposto di liceità dell'atto medico.
In tale settore l'asimmetria informativa tra le parti è destinata ad aumentare a fronte della diffusione dell'impiego di sistemi di intelligenza artificiale nell'erogazione di prestazioni terapeutiche o diagnostiche che condurrà a scenari ove i problemi di gestione del rischio e riparto delle responsabilità si affiancheranno a quelli di completa e corretta informazione al paziente circa possibilità, rischi e benefici connessi all'utilizzo di *device* medicali basati sull'intelligenza artificiale[55].
Un problema concerne la spiegabilità dell'IA, ossia la proprietà di un sistema di poter fornire una spiegazione a un individuo in modo soddisfacente, con riguardo alla catena di cause-effetto caratteristica di un determinato processo.
Un altro problema concerne la gestione della raccolta del consenso informato e del consenso al trattamento dei dati personali del paziente, in relazione a sé, quante e quali informazioni fornire al paziente con specifico riferimento al ruolo dell'IA nella prestazione sanitaria.
La limitata comprensibilità e, dunque, la possibilità di controllo delle tecnologie da parte del medico può sortire l'effetto di marginalizzare il ruolo del professionista nel contesto della prestazione.
La problematica concerne sia questioni di politica legislativa che di gestione del rischio da parte delle strutture sanitarie.
Inoltre, deficit informativi di strutture e professionisti sanitari possono trovare origine anche nelle mancanze imputabili al produttore del *device* medicale.
Quest'ultimo soggetto è tenuto a informare compiutamente la struttura sanitaria acquirente o committente o il singolo professionista sanitario delle caratteristiche dell'oggetto della fornitura.
La struttura sanitaria o il singolo medico devono, poi, debitamente rendere edotto il paziente nell'interesse del quale la prestazione *AI assisted* è fornita.
Il tema assume una dimensione organizzativa, con la struttura sanitaria chiamata a gestire in modo adeguato l'informazione ai pazienti e la raccolta del loro consenso, anche predisponendo protocolli e modelli aziendali idonei che tengano in considerazione lo sviluppo delle tecnologie della quale essa si avvale.

[55] C. PERLINGIERI, *Responsabilità civile e robotica medica*, in *Teconologia e Diritto*, 2020, 161 ss.; G. VOTANO, *Intelligenza artificiale in ambito sanitario: il problema della responsabilità civile,* in *Danno e Responsabilità,* 2022, 669 ss.; *M. GAMBINI, Nuovi paradigmi della responsabilità civile per l'Intelligenza artificiale,* in *Rassegna di diritto civile*, 2023, 1288 ss.

Downloaded from www.biodiritto.org.
ISSN 2284-4503

In materia di prestazioni sanitarie, l'obbligo informativo non è soggetto a valutazioni discrezionali da parte del medico e comprende tutti gli aspetti diagnostici e prognostici relativi al paziente, ivi incluso l'impiego di sistemi AI nella prestazione.

Occorre evidenziare che le norme in materia di consenso informato esigono che il professionista sanitario informi il paziente dell'utilizzo di IA, sia nel procedimento di elaborazione di diagnosi e proposta terapeutica, quanto nell'esecuzione di prestazioni.

Una volta riconosciuto il dovere del medico di garantire che il consenso informato del paziente alla prestazione sanitaria si formi anche con riguardo all'utilizzo dell'intelligenza artificiale nella sua esecuzione, ulteriore interrogativo concerne le possibili differenze di trattamento, quanto ai profili informativi, tra prestazioni eminentemente diagnostiche e prestazioni di natura terapeutica, domandandosi se l'utilizzo dell'IA nell'esecuzione delle prime possa essere sottaciuto nei confronti del paziente.

Il quesito in esame deve trovare risposta negativa, ritenendosi che non abbia ragione di sussistere alcuna distinzione fondata sulla natura diagnostica o terapeutica della prestazione, sotto il profilo della necessità di informare il paziente circa l'utilizzo dell'IA.

In assenza di ulteriori indicazioni normative, possono essere desunti i principi affermati nel formante giurisprudenziale, tra cui *in primis* la necessità di adottare un linguaggio che tenga conto del particolare stato soggettivo e del grado di conoscenze del paziente, della sua capacità di comprensione e sensibilità, in quell'ottica di personalizzazione delle cure alla quale le informazioni da veicolare devono, in particolar modo, comprendere «tutte le informazioni scientificamente possibili sulla prestazione che intende seguire, sulle conseguenze normalmente possibili, sia pure infrequenti, ivi inclusi i rischi prevedibili»[56].

Un ulteriore livello di indagine concerne il contenuto delle informazioni da fornire al soggetto interessato in quanto *data subject* di un trattamento di propri dati personali, in altri termini quelli destinati ad essere elaborati dall'IA nel contesto della prestazione sanitaria resa attraverso dispositivi *AI based* con riferimento alla normativa *data protection*.

Le norme di *data protection* riservano una peculiare tutela ai dati relativi alla salute, ricompresi nell'art. 9 del GDPR tra le categorie particolari di dati personali, il cui trattamento, anche automatizzato, è generalmente vietato, fatta eccezione per taluni casi, tra cui la sussistenza di interessi superindividuali, quali motivi di rilevante interesse pubblico nel settore della sanità.

Al tempo stesso, esenti dal suddetto divieto sono i trattamenti di dati necessari per finalità di medicina preventiva, diagnosi, assistenza o terapia sanitaria, qualora effettuati sotto la responsabilità di professionisti sanitari soggetti al segreto professionale.

Per contro, i trattamenti di dati svolti nel contesto di prestazioni di cura, ma non qualificabili come strettamente necessari, esigono differenti basi giuridiche, tra cui l'esplicito consenso dell'interessato fornito a fronte di un'idonea informativa.

Il consenso quindi mantiene, anche in ambito sanitario, una non trascurabile rilevanza come veicolo tramite il quale all'interessato è garantita la consapevolezza sia dell'utilizzo che sarà fatto dei dati a esso riferito, sia dei propri diritti di controllo sui relativi flussi informativi.

[56] Cass. Civ., 11 dicembre 2013, n. 27751, in *DeJure online*.

Downloaded from www.biodiritto.org.
ISSN 2284-4503

Inoltre, l'art. 22 GDPR limita la possibilità di ricorrere a processi decisionali basati sui trattamenti automatizzati di dati relativi alla salute, alla sola ipotesi in cui l'interessato vi abbia prestato il proprio consenso, esplicito e specifico, o alla sussistenza di motivi di rilevante interesse pubblico.

Tuttavia, la norma in questione è riferita ai casi nei quali le decisioni, ove incidenti in modo significativo sulla persona dell'interessato, siano basate unicamente sul trattamento automatizzato; la qual cosa potrebbe non sostenersi in relazione a decisioni come quelle assunte tramite *device* medicali con l'utilizzo dell'IA, per cui il controllo e la supervisione del medico *human in command* risultano imprescindibile garanzia della tutela della salute del paziente.

Quanto al contenuto dell'obbligo informativo, è lecito dubitare che l'art. 22 GDPR possa essere interpretato come direttamente istitutivo di un diritto alla spiegazione del funzionamento dei meccanismi alla base del trattamento automatizzato.

È unicamente per effetto di una lettura di tale normativa in combinato con il considerando 71 GDPR, che ricomprende la specifica informazione all'interessato nel novero delle garanzie adeguate da assicurare in caso di trattamento automatizzato, che parte della dottrina ravvisa nell'art 22 del GDPR la previsione di uno specifico diritto alla spiegazione[57].

Laddove sembra più pertinente il riferimento ad altre norme del Regolamento, tra cui l'art. 5 (istitutivo del principio di trasparenza), l'art. 12, nonché l'art. 13.

Con riferimento alla materia *de qua,* tale ultima previsione impone al titolare del trattamento di rendere noto all'interessato l'esistenza di un processo decisionale automatizzato e di fornire informazioni significative[58] sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato. Tali informazioni sono suscettibili di essere altresì oggetto del diritto di accesso di cui all'art 15 GDPR, ed in relazione alle quali deve essere garantita trasparenza, in funzione strumentale alla autodeterminazione informativa del paziente[59].

Quanto ai trattamenti di dati sanitari mediante AI, possiamo ipotizzare che, oltre all'informazione sulla natura dei dati trattati e all'esistenza di un trattamento automatizzato, al soggetto interessato debba essere reso noto anche il funzionamento del modello algoritmico utilizzato nel trattamento, il grado di autonomia della macchina e la logica con la quale opera l'algoritmo.

Una lettura combinata degli artt. 13 e 22 GDPR permette di declinare il contenuto dell'informazione relativa al trattamento automatizzato: quella della spiegazione *ex ante*, relativa al generale funzionamento del sistema, anche con riguardo ai meccanismi e alle logiche ad esso sottostanti, e quelle della

[57] M. PALMIRANI*, Interpretabilità, conoscibilità, abilità dei processi decisionali automatizzati*, in U. RUFFOLO (a cura di), *XXVI lezioni di diritto dell'intelligenza artificiale*, Torino, 2021, 72. Sul dibattito in letteratura tra coloro che rinvengono il fondamento dell'esistenza di un diritto alla spiegazione nel considerando 71 GDPR e coloro che ne escludono la sussistenza in quanto non contemplato nell'articolato del Regolamento, o quantomeno nell'art 22 GDPR, v. E. FALLETTI, *Decisioni automatizzate e diritto alla spiegazione*: alcune riflessioni comparatistiche, in *Diritto dell'informazione e dell'informatica,* 2019, 2, 169 ss.

[58] Quanto al contenuto di tali significative informazioni (in materia di *Data Protection),* il dovere informativo si traduce in un dovere di *disclosure* completa delle informazioni relative al trattamento, ma è ammesso un significativo ricorso alla sintesi purchè siano veicolate informazioni sufficienti a garantire l'autodeterminazione informativa e la possibilità di tutela dell'interessato.

[59] S. FRANCA, *Il trattamento dei dati nelle sperimentazioni di intelligenza artificiale riguardanti le pubbliche amministrazioni*, in A. PAJNO, F. DONATI, A. PERRUCCI (a cura di), *Intelligenza artificiale e diritto: una rivoluzione?,* vol. II, Bologna, 2022, 173 ss.

Downloaded from www.biodiritto.org.
ISSN 2284-4503

spiegazione *ex post*, afferente allo specifico *output* del trattamento nel caso specifico riguardante l'interessato.

Il quadro dei doveri informativi correlati all'impiego dei dispositivi medici dotati di IA va poi integrato con le prescrizioni di natura regolatoria, le quali impongono agli operatori del settore, sia nella fase *pre-market* che in quella *post-market*, specifici oneri di *disclosure* quanto a caratteristiche, funzionamento e rischi del *device*[60].

L'*AI Act* ha quale obiettivo quello di istituire un primo livello di un generale quadro normativo volto alla regolazione del settore dell'IA, con l'individuazione di requisiti produttivi, prescrizioni tecniche e doveri di *compliance* per lo sviluppo, la produzione, la commercializzazione e l'impiego di sistemi di IA, introducendo una sorta di standard di base uniformante nel territorio dell'Unione europea[61].

I sistemi di intelligenza artificiale destinati ad essere impiegati in sanità (anche come parte o componente di device medicali) sono categorizzati nell'*AI Act* come "ad alto rischio", risultando ricompresi tra quei sistemi il cui impiego è ritenuto suscettibile di presentare rischi significativi di danno per la salute e la sicurezza o di impatto negativo sui diritti fondamentali dell'individuo.

A tale qualificazione consegue l'applicazione di una serie di prescrizioni concernenti sia le caratteristiche, il cui rispetto deve essere garantito nella progettazione e nella realizzazione dei sistemi, sia specifici doveri di informazione, trasparenza e *disclosure* che si integrano talora sostituendosi, talora sovrapponendosi a quelli sopra citati. In primo luogo, il Regolamento prevede la necessità di garantire sufficienti livelli di trasparenza dei sistemi di IA, i quali devono essere sviluppati e impiegati in modo da permettere una idonea tracciabilità e spiegabilità dei meccanismi di funzionamento nonché la possibilità per gli utenti di interpretare e utilizzare adeguatamente l'*output* generato dal sistema. L'oggetto del dovere informativo si estende poi secondo il regolamento all'indicazione di quali funzioni nello specifico sono svolte dall'IA dalla presenza di *Human oversight* e del soggetto responsabile del processo decisionale della macchina. Questo dovere sussisterebbe in capo ai suoi produttori o fornitori in quanto riferito a caratteristiche che dovrebbero essere garantite sin dalla progettazione del sistema. Va bene tale previsione nel contesto dei dispositivi medici basati sugli a prevede in capo al produttore del device il dovere di trasmettere le informazioni in esame al professionista sanitario che di tale dispositivo si avvale. Tali previsioni possono leggersi come introduttive di un generale dovere di informazione quanto all'utilizzo di sistemi di IA nella prestazione; tenendo anche in considerazione come il professionista sanitario o la struttura sanitaria possono considerarsi anch'essi a loro volta fornitori del servizio basato sull'intelligenza artificiale. Nello stessa direzione depone anche un'altro articolo del Regolamento che attribuisce ad ogni persona soggetta a una decisione assunta dal *deployer* sulla base di un *output* reso dal sistema di IA ad alto rischio ove suscettibile di produrre effetti giuridici o comun-

[60] Non sarà oggetto di approfondimento l'analisi dei doveri informativi prescritti per ogni tipo di dispositivo medico (con o senza IA) dal Regolamento Ue 2017/745 (*Medical devices regulation*). Ci si limita ad affermare che tale Regolamento nel settore in esame ribadisce la centralità della trasparenza oltre che della tracciabilità dei dispositivi medici, con il fine di migliorare la sicurezza e la salute, tutelando la salute pubblica per rafforzare la consapevolezza dei pazienti e dei sanitari, consentendo loro di prendere decisioni informate, valorizzando l'importanza di garantire un accesso adeguato alle informazioni presentate per l'utilizzatore previsto.

[61] C. PERLINGIERI, *Intelligenza artificiale in ambito medico-sanitario:profili di ricostruzione normativa a seguito dell'AI ACT,* in *Rassegna di diritto civile,* 3, 2024, 907 ss.

Downloaded from www.biodiritto.org.
ISSN 2284-4503

Call

que un impatto su salute, sicurezza e diritti fondamentali, il diritto di richiedere al *deployer* una spiegazione chiara e significativa sul ruolo dell'IA nel processo decisionale, sui principali parametri usati per la decisione e sui dati di *input* che sono stati elaborati.

L'utilizzo di IA nelle prestazioni sanitarie (e nei *device* medicali) risulta sicuramente in grado di aumentare i livelli di sicurezza e qualità, con enormi benefici in termini di efficienza del complessivo sistema sanitario.

I sistemi di IA più avanzati restano tuttavia parzialmente opachi, presentando specifici profili di rischio, sui quali il paziente non può non essere adeguatamente informato.

La tematica non potrà che essere gestita tramite idonee politiche pubbliche, sia attraverso un adeguato sistema di controllo e certificazione preventiva dei dispositivi.

Tutto ciò risulta suscettibile di influenzare il livello di informazione che i medici saranno in grado di offrire ai pazienti.

Un ruolo centrale sarà ricoperto dalle strutture sanitarie, che saranno chiamate a formare opportunamente i propri professionisti, al fine di garantire che gli stessi siano in grado di informare compiutamente i pazienti.

Il diritto del paziente a essere informato circa le caratteristiche della prestazione e delle possibili connesse criticità è volto a garantire l'effettivo esercizio del diritto all'autodeterminazione quanto a decisioni afferenti alla salute.

Downloaded from www.biodiritto.org.
ISSN 2284-4503