UNIVERSITÀ DEGLI STUDI DI MESSINA
DIPARTIMENTO DI SCIENZE POLITICHE E GIURIDICHE

XXXVIII CICLO DEL DOTTORATO DI RICERCA IN SCIENZE DELLE PUBBLICHE AMMINISTRAZIONI.

Il trattamento giuridico dei dati sanitari:

INTEROPERABILITÀ E RISERVATEZZA NELL'ERA DELL'INTELLIGENZA ARTIFICIALE.

(Settore scientifico disciplinare: GIUR-01/A-Diritto Privato)

Dottoranda

Dott.ssa Vanessa Previti

Coordinatrice

Chiar.ma Prof.ssa Daniela Novarese

Tutor

Chiar.mo Prof. Roberto Amagliani

Anno Accademico 2024/2025

A mia madre,

Sole della mia vita e fiore della mia anima.

A mio padre,

Stella costante del mio cammino e instancabile ispirazione.

A Jessica,

che quotidianamente mi insegna la forza e la resilienza.

A Francesco,

che abita la parte più interna del mio cuore.

A Briciola,

che non ha mai parlato ma mi ha sempre detto tutto.

Indice

Secondo capitolo

Sezione I

Introduzione

Il lavoro in oggetto inizierà dall'analisi del dato sanitario in generale, attraverso lo studio della disciplina europea in materia e l'equivalente disposizione italiana e i relativi provvedimenti del Garante della Privacy, passando per dei *focus* specifici in tema di utilizzo delle informazioni sanitarie in relazione all'accertamento dell'infezione da HIV.

Successivamente, la ricerca si concentrerà sul trattamento dei dati sanitari durante la Pandemia da Covid-19 che ha avuto inizio nel

2020, i cui effetti – specie in merito all'utilizzo improprio degli stessi – si sono protratti fino alla stesura di questo lavoro; verrà dato un grande rilievo anche all'uso delle informazioni inerenti al contagio tramite l'applicazione Immuni e le equivalenti estere.

La terza parte del primo capitolo si occuperà, invece, dell'uso primario e secondario dei dati con un'attenzione peculiare alla ricerca scientifica, all'ambito farmaceutico e delle sperimentazioni cliniche, con un focus sull'impatto del Covid sulla ricerca scientifica, sui provvedimenti del Garante e sul ruolo dell'Agenzia Italiana del Farmaco in merito ai dati rivelatosi necessari per l'autorizzazione all'immissione in commercio e la conseguente diffusione dei vaccini che hanno contribuito al contenimento e alla cura del Covid-19.

Nel secondo capitolo, la prima sezione verrà dedicata alla digitalizzazione del dato sanitario con un approfondimento sia sulla telemedicina – con un *focus* sul rapporto con la ricerca scientifica, le *m-health app* e il cosiddetto "Patto con il cittadino" – sia sulla cartella clinica elettronica che sul Fascicolo Sanitario elettronico nella sua veste "tradizionale" e in quella "2.0".

La seconda sezione abbandonerà la dimensione nazionale per focalizzarsi su quella europea con l'analisi dello Spazio europeo dei dati sanitari e lo studio incrociato dell'uso primario e secondario delle informazioni inerenti alla salute in merito

all'EHDS con una prospettiva *de iure condendo* che affronterà il fallimento dell'anonimizzazione e la possibilità di utilizzare i dati sintetici.

La terza e ultima sezione del secondo capitolo tratterà la medicina degli algoritmi con l'analisi del rapporto tra intelligenza artificiale ed elaborazione dei dati sanitari con un inquadramento giurisprudenziale riconducibile al Consiglio di Stato in merito all'enucleazione dei principi fondamentali in materia e l'utilizzo dei medesimi da parte del Garante della Privacy.

Infine, si affronterà l'elaborazione di un dataset per lo sviluppo di macchine intelligenti e il disegno di legge italiano in materia di intelligenza artificiale specialmente in ambito sanitario.

L'ultimo capitolo di questo scritto si occuperà di analizzare il rapporto intercorrente tra intelligenza artificiale e responsabilità civile, attraverso il vaglio dell'invocabilità delle già esistenti categorie civilistiche di responsabilità, nel dettaglio circa l'applicabilità degli articoli 2050 e 2051 del Codice civile ai nuovi danni cagionati dall'utilizzo di strumentazioni intelligenti.

Nella seconda sezione vi sarà un *focus* sulla produzione e regolamentazione dei dispositivi medici intelligenti, sulla responsabilità del produttore per danno da prodotti difettosi, alla luce della nuova normativa unionale con il vaglio dell'eventuale

invocabilità dell'esimente da prodotto difettoso, al fine di escludere l'antigiuridicità della condotta.

L'ultima sezione del capitolo finale si addentrerà, dapprima nell'analisi del rapporto tra intelligenza artificiale e responsabilità sanitaria con peculiare riguardo alla natura della prestazione sanitaria e responsabilità del singolo operatore e della struttura ospedaliera che si serve di sistemi di IA; in ultima battuta questo lavoro si occuperà della figura del chatbot in ambito sanitario, provando a qualificare il tipo di responsabilità che si configura nell'eventualità in cui lo stesso dia delle informazioni scorrette che possano cagionare un danno.

Primo capitolo.

1.1. Il dato sanitario: inquadramento normativo e definizioni di carattere generale.

Nella società odierna, caratterizzata dal continuo tentativo di bilanciamento tra la trasparenza e il diritto alla riservatezza, nell'era della dematerializzazione e digitalizzazione di qualunque tipologia di informazione, analizzare l'argomento della tutela del

trattamento di quelle particolari categorie di dati che venivano anzitempo considerati sensibili(ssimi)[1], è un'attività particolarmente complessa.

Infatti, sebbene il c.d. «*right to be let alone*» fonda le sue radici negli Stati Uniti, tra la fine dell'Ottocento e l'inizio del Novecento, in Italia inizia ad assumere rilevanza giuridica tra gli anni Sessanta e Ottanta quale *ius excludendi alios* dalla propria vita privata, conferendo al diritto alla riservatezza un'accezione negativa finalizzata a non diffondere informazioni sul proprio conto.

Ad oggi tale definizione si rivela particolarmente anacronistica, tenuto conto del valore dei dati e della loro concorrenza al progresso culturale, economico e sociale.

Risulta infatti superata l'accezione del dato in senso negativo, essendo, invece, necessario definirlo, sussumerlo in categorie prestabilite, analizzando la disciplina del trattamento e le conseguenti responsabilità. Non è, inoltre, trascurabile il rilevante apporto dell'intelligenza artificiale nella gestione delle informazioni personali e, nel dettaglio, dei dati di carattere sanitario. Quindi questo lavoro intende, in prima battuta, analizzare, seppur brevemente, la definizione di "dato" in generale

---

[1] *Ex multis*, P. PICCOLO, *Accesso ai dati sensibili(ssimi) tra tutela della privacy e diritti "di pari rango" nelle cause di nullità matrimoniale* in *Dir. famiglia*, fasc.3, 2013, p. 1171.

e nel particolare di quello sanitario dal punto di vista normativo interno e europeo, per poi occuparsi del peculiare regime del trattamento delle suddette informazioni durante il periodo pandemico, attraverso un *focus* sulla differenza tra uso primario e secondario dei dati con una particolare attenzione all'utilizzo dei medesimi nelle attività di ricerca scientifica e nelle sperimentazioni cliniche effettuate dall'Agenzia Italiana del Farmaco, nel capitolo che segue, invece, si analizzerà pedissequamente l'*e-Health*, che è quel campo della medicina in cui si intersecano «informatica medica, sanità pubblica e attività economica, ricomprendente tutti quei servizi e quelle informazioni sanitarie forniti o condivisi attraverso l'uso di tecnologie informatiche e di telecomunicazione»[2], con particolare riguardo all'utilizzo degli algoritmi in materia e all'ausilio dell'intelligenza artificiale anche alla luce dell'IA Act[3].

Per comprendere l'ambito di applicazione oggettivo della disciplina del trattamento dei dati sanitari, si ritiene opportuno provvedere all'inquadramento normativo della nozione di "dato",

---

[2] C. IRTI, *L'uso delle "tecnologie mobili" applicate alla salute: riflessioni al confine tra la forza del progresso e la vulnerabilità del soggetto anziano*, in *Persona e Mercato*, 1/2023, p. 34.

[3] Regolamento europeo sull'Intelligenza artificiale, approvato il 14 maggio 2024, per la consultazione https://data.consilium.europa.eu/doc/document/PE-24-2024-INIT/it/pdf.

con specifico e peculiare riferimento alla nozione del medesimo inerente alla salute, così come individuato dal Regolamento 2016/679/UE.

Innanzitutto, in letteratura non vi è unanimità in merito alla definizione, una parte di dottrina[4], ritiene che il "dato" sia sinonimo di "informazione" e quindi «qualsiasi elemento di scrittura, suono e immagine dotato di contenuto informativo», altri[5] ritengono sussistente una differenza tra l'accezione di "dato" e quello di "informazione", affermando che «mentre il dato è sempre un elemento conoscitivo, l'informazione ha una connotazione in qualche maniera soggettiva, in quanto è quello che l'utente di volta in volta ricava dall'aggregazione dei dati che può ottenere consultando un database»[6].

Sebbene l'espressione "protezione dei dati personali" sembrasse riferita alla tutela del dato in sé, già la c.d. Direttiva Madre n. 46 del 1995 evidenziava che non era possibile scindere la protezione dei dati dalle persone fisiche e dal sentimento di fiducia e di affidamento che le stesse dovevano riporre nei confronti di coloro

---

[4] A. ZUCCHETTI, *Dati (trattamento dei)* in V. ITALIA (a cura di), *Enciclopedia degli enti locali, Atti, Procedimenti, Documentazione*, Giuffrè, Milano, 2007.
[5] D.U. GALLETTA, *Accesso civico e trasparenza della Pubblica amministrazione alla luce delle (previste) modifiche alle disposizioni del Decreto Legislativo n. 33/2013*, in *Federalismi.it*, 5, 2016.
[6] *Ibidem.*

ne effettuavano il trattamento, al fine di creare un'economia digitale in tutto il mercato interno.

Nell'ottica del raggiungimento dell'obiettivo di uniformità a livello comunitario, interviene, nel 2016, quale strumento strategico per il mercato unico digitale il Regolamento UE 679/2016 – *General Data Protection Regulation* – GDPR o RGPD "relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati", con lo scopo di prevedere una disciplina del diritto alla protezione dei dati personali in contemperamento con gli altri principi fondamentali, in ossequio al principio di proporzionalità.

Il legislatore europeo decide quindi di intervenire, abrogando la Direttiva Madre e scegliendo lo strumento del Regolamento[7] che «*ha portata generale. […] è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri*» in luogo della Direttiva che «*vincola lo Stato membro cui è rivolta per quanto riguarda il risultato da raggiungere, salva restando la competenza degli organi nazionali in merito alla forma e ai mezzi*»[8], lasciando, però, il potere, in capo agli Stati membri, di prevedere discipline in ambiti specifici, quali quello della salute,

[7] Art. 288 TFUE c. 1.
[8] Art. 288 TFUE c. 2.

tenuto conto delle molteplici diversità dei sistemi sanitari dei Paesi europei.

Preliminarmente, occupandosi di dati di carattere clinico, si ritiene impossibile scindere la nozione di dato da quella di informazione sanitaria, ancor più se inserita nel binomio informazione-attività medico sanitaria finalizzata alla tutela del paziente, «contraente debole»[9] per eccellenza, protagonista del principio di autodeterminazione terapeutica in un sempiterno tiro alla fune che vede da un capo la protezione della sfera personale del soggetto e della sua riservatezza e dall'altro il necessario trattamento dei dati sanitari, l'ostensione e l'interoperabilità.

Il dato sanitario, quindi, è una delle forme di manifestazione del «dato personale» in quanto ricompreso nella categoria dei «dati relativi alla salute», il che implica l'applicazione della relativa disciplina ogni qualvolta sia riferibile – in maniera diretta ovvero indiretta – ad una persona fisica puntualmente identificata o identificabile da parte del titolare del trattamento.

Infatti, sebbene il legislatore euro-unitario non preveda un'apposita disciplina del trattamento dei dati di carattere sanitario, già al considerando 35, chiarisce che «*nei dati personali*

[9] Tra gli altri, F. DI MARZIO, *Ancora sulla nozione di "consumatore" nei contratti*, in *Giust. Civ*. 2002, fasc. 1, 685 ss; F. RINALDI, *Incompatibilità tra la nozione di consumatore e quella di professionista debole*, in *Nuova giur. Civ. comm*., 2002, fasc. 1, p. 630 ss.

relativi alla salute dovrebbero rientrare tutti i dati riguardanti lo stato di salute dell'interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso»[10]. Gli stessi deriveranno «*dagli esami e controlli effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici*»[11].

Mentre l'art. 4, par. primo, n. 15, li qualifica come «*dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute*», by-passando la tradizionale tripartizione "dati personali", "dati sensibili" (o super-sensibili)" e "dati giudiziari"[12].

Il GDPR prevede un generale divieto di trattamento di talune categorie particolari di dati, all'art. 9, annoverando tra gli stessi «*dati genetici, dati biometrici intesi ad identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*», ma, confermando la precedente impostazione[13], ha previsto che in presenza di una serie di condizioni espressamente individuate dalla legge genericamente sussumibili in deroghe al precedente

[10] Considerando 35 del GDPR.
[11] *Ibidem.*
[12] Vedasi il c.d. Codice della Privacy, d. lgs. n. 196 del 2003.
[13] Art. 8, par. 2 della previgente Direttiva 95/46/CE.

divieto in due macro categorie – la prima riguarda la sfera privatistica, la seconda, invece afferisce alla sfera pubblicistica[14]– non opera la preclusione.

Con riferimento alla prima macrocategoria, il legislatore euro-unitario ha previsto – a titolo esemplificativo – che, trattandosi di contemperamento tra trattamento dei dati e rispetto dei diritti fondamentali dell'interessato e di altri soggetti, lo stesso sia previsto se necessario «*per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso»*[15].

Per quel che concerne, invece, la seconda macrocategoria e cioè la sfera pubblicistica, il GDPR autorizza il trattamento dei dati sanitari per *«motivi di interesse pubblico rilevante sulla base del diritto dell'Unione europea o del diritto dello Stato membro»,* di fatti, è consentito il «perseguimento di interesse pubblici da parte di soggetti deputati istituzionalmente al raggiungimento di finalità

[14] Tra gli altri, S. MELCHIONNA E F. CECAMORE, *Le nuove frontiere della sanità e della ricerca scientifica*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato, Commentario al Regolamento UE n. 679/2016 e al d. lgs. n. 101/2018*, Giuffrè, Milano, 2019, p. 585 ss.

[15] Art. 9, par. 2, lett. c) del Regolamento 2016/679/UE.

di programmazione, gestione, valutazione e controllo dell'assistenza sanitaria»[16].

Nel paragrafo che segue, si analizzerà nel dettaglio la disciplina del GDPR con riferimento al trattamento dei dati sanitari.

1.2. Il trattamento dei dati sanitari alla luce della disciplina prevista dal Regolamento 679/2016 – GDPR.

Nell'ottica di inquadramento generale della disciplina in materia di trattamento dei dati personali di carattere sanitario e prima di procedere all'analisi specifica della normativa italiana, si ritiene opportuno vagliare l'art. 9 del GDPR che al comma 1 prevede un divieto generale di trattamento di questa particolare tipologia di dati, disponendo che «[è] vietato trattare [...] dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona»[17] e che, in ogni caso, «[g]li Stati membri possono mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute»; precisando che detta

[16] S. MELCHIONNA e F. CECAMORE, *Le nuove frontiere della sanità e della ricerca scientifica*, op. cit.
[17] Art. 9, par. primo, GDPR.

previsione non trova applicazione quando si verifica uno dei seguenti casi:

- «a) l'interessato abbia prestato il proprio consenso esplicito al trattamento di tali dati per una o più finalità specifiche – fatta eccezione per l'eventualità in cui il diritto dell'Unione o degli Stati membri preveda che l'interessato non possa revocare il divieto di cui al paragrafo 1 dell'articolo in analisi»;
- «b) il trattamento sia necessario per assolvere gli obblighi ed esercitare i diritti specifici propri del titolare del trattamento (o dell'interessato) in determinate materie – quando il trattamento è stato autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo previsto dalle normative interne, tutelando, ad ogni modo, i diritti e gli interessi fondamentali - tra le quali rientrano il diritto del lavoro e della sicurezza sociale e la c.d. «protezione sociale»;
- «c) allorché ci si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso ed il trattamento risulti necessario per tutelare un interesse vitale dell'interessato (o di un'altra persona fisica)»;
- «d) quando ad agire per il trattamento dei dati sia una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali ed il trattamento

medesimo venga effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie»;

- «e) il trattamento riguardi dati personali resi manifestamente pubblici dall'interessato»;
- «f) il trattamento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria»;
- «g) il trattamento sia necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o di uno degli Stati membri;
- «h) il trattamento sia necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale, ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità o degli Stati membri o conformemente al contratto con un professionista della sanità»;
- «i) il trattamento sia necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, pur rispettando il diritto dell'Unione e degli Stati membri che possono prevedere misure

specifiche per tutelare il c.d. «segreto professionale» che impone che tali dati siano trattati sotto la responsabilità di un professionista soggetto all'obbligo di riservatezza»[18];

- «j) il trattamento sia necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici»[19].

L'intera disciplina del trattamento dei dati prevista dal GDPR è improntata al principio di trasparenza, per cui tutte le informazioni destinate al pubblico o all'interessato devono essere facilmente accessibili e di facile comprensione, utilizzando un linguaggio chiaro e semplice che permetta all'interessato di comprendere *se* vengono raccolti dati personali, da *chi* e per quale motivo.

L'art. 12, par. 1, nel dettaglio, sancisce che «*il titolare del trattamento debba adottare misure appropriate per fornire all'interessato tutte le informazioni necessarie»* attraverso le indicazioni previste dagli articoli 13 e 14 *e «le comunicazioni relative al trattamento dei dati personali in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori*»[20]. Le

[18] Art. 9, par. 3, GDPR.
[19] *Ibidem*.
[20] Art. 12, GDPR.

informazioni sono fornite per iscritto o con altri mezzi, se del caso in formato elettronico.

È prevista anche la possibilità, su richiesta dell'interessato, di fornire le informazioni oralmente, purché sia comprovata l'identità dell'interessato.

I successivi articoli 13 e 14 del GDPR prevedono nel dettaglio il contenuto dell'informativa, che mette in luce, specialmente per quel che concerne i dati sanitari, la centralità del principio dell'*accountability* dell'interessato.

Questo, però, non deve essere inteso come un atto di cancellazione del consenso informato, pilastro della disciplina del trattamento dei dati ante-GDPR, ma come la perdita della centralità e dell'indefettibilità del medesimo in forma scritta.

Di fatti, l'art. 7 del GDPR prevede che «qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato lo ha prestato»[21], per cui il titolare del trattamento non è più obbligato a documentare per iscritto il rilascio, da parte dell'interessato, del consenso al trattamento dei dati sanitari, né è obbligato all'uso della forma scritta, sebbene, secondo l'opinione del Garante[22] sia la modalità «più idonea a

[21] Art. 7, GDPR.

[22] "Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali", Garante della Privacy, Doc-Web 9892762, per la

configurare l'inequivocabilità del consenso ed il suo essere "esplicito"».

Il GDPR prevede che il consenso sia informato e specifico e che venga prestato liberamente dall'interessato. Se tale condizione legittimante è prestata nel contesto di una dichiarazione scritta che riguarda anche altre materie, la richiesta, ai sensi del sopra citato art. 7, par. 2, «è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro»[23]. L'interessato ha, comunque, il diritto di revocarlo in qualsiasi momento, non pregiudicando la liceità del trattamento effettuato prima della revoca.

Un'attenzione particolare viene rivolta dal legislatore europeo al trattamento automatizzato dei dati personali, infatti, l'art. 22 prevede, come principio generale, che «l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato che produca effetti giuridici che lo riguardano o che incida allo stesso modo significativamente sulla sua persona»[24], ma è lo stesso art. 22 che prevede che tale disposizione non si applica quando la decisione: «*a) sia necessaria*

---

consultazione del testo: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9892762.

[23] Art. 7, par. 2, GDPR.

[24] Art. 22, GDPR.

per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento»

oppure *«b) sia autorizzata dal diritto dell'Unione o degli Stati membri cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà e dei legittimi interessi dell'interessato»*

oppure *«c) si basi sul consenso esplicito dell'interessato»*[25].

L'art. 22 è stato considerato il cardine normativo che ha garantito il c.d. «principio della conservazione dell'elemento umano»[26] (*human in the loop*) in ogni circostanza in cui possano essere messi in discussione i diritti umani.

Inoltre, da questa previsione europea, ordinamenti nazionali – quali quello italiano – hanno sviluppato indirizzi della giurisprudenza amministrativa che ha tratto dal GDPR principi fondamentali[27] quali «la piena conoscibilità dei criteri applicati dai modelli automatizzati»[28] o «il diritto in capo all'organo titolare

[25] *Ibidem*.
[26] P. BENANTI, *Human in the loop, Decisioni umane e intelligenze artificiali*, Milano, 2022, p. 161.
[27] G. CERRINA FERONI, *IA nei processi decisionali della PA, il faro è la Costituzione*, in *Agenda Digitale UE*, pp. 1-28.
[28] Consiglio di Stato, sezione VI, 13 dicembre 2019, n. 8472.

della decisione di verificare la logicità e la legittimità degli esiti prodotti dagli algoritmi»[29].

La questione giuridica diventa di particolare interesse con riferimento al trattamento automatizzato dei dati sanitari, specie nell'eventualità in cui si inerisce l'ausilio dell'intelligenza artificiale, come si dirà nel capitolo che segue.

In generale, vige un divieto di trattamento di queste particolari categorie di dati tranne nell'ipotesi in cui «*a) esiste un consenso esplicito dell'interessato»;*

«b) deve essere perseguito un interesse pubblico rilevante nell'ambito della sanità pubblica»;

«c) il Titolare (o Responsabile) abbia adottato idonee ed adeguate misure di sicurezza per tutelare i diritti, le libertà e i legittimi interessi del paziente»[30].

Se invece, un Titolare o un Responsabile decide di usare i dati dei pazienti per attività di profilazione, allora questi deve concedere agli interessati il diritto di rinunciare all'attività (il cd. diritto di *opt-out*) e di revocare il consenso.

[29] Consiglio di Stato, sezione VI, 4 febbraio 2020, n. 881.

[30] Art. 22, par. 4, GDPR.

In ogni caso, «il Titolare (o Responsabile) dovrà adottare idonee misure di sicurezza che garantiscano all'interessato la tutela dei propri diritti e delle libertà fondamentali».

Sebbene la disciplina dettata dal legislatore euro-unitario sia molto specifica e nonostante sia stato scelto lo strumento del Regolamento in virtù della sua forza vincolante e della sua diretta applicabilità, viene lasciata, in capo agli Stati membri, la «libertà di mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute»[31], scelta non condivisa da parte di dottrina[32] che ritiene che tale norma impedisca una reale uniformità a livello europeo delle regole in materia di trattamento dei dati sensibili e, pertanto, anche dei dati sanitari.

Infatti, in letteratura si auspica che il considerando 53[33] finisca col persuadere i legislatori degli Stati membri in un'ottica di «una semplificazione delle barriere giuridiche che, ad oggi, ostacolano la circolazione all'interno dell'Unione non tanto e non solo dei dati

---

[31] Art. 9, par. 4, GDPR.

[32] F. CAGGIA, *Il trattamento dei dati sulla salute, con particolare riferimento all'ambito sanitario*, in V. CUFFARO- R. D'ORAZIO-V. RICCIUTO (a cura di), *Il codice del trattamento dei dati personali*, Torino, 2007, pp. 407-408.

[33] Secondo il considerando 53 le categorie particolari di dati personali che meritano una maggiore protezione dovrebbero essere trattate soltanto per finalità connesse alla salute, ove necessario per conseguire tali finalità a beneficio delle persone e dell'intera società.

sanitari, quanto anche di tutti quei servizi che caratterizzano il mondo della sanità elettronica»[34].

Nel paragrafo che segue, si procederà con l'inquadramento normativo della disciplina del trattamento dei dati personali di carattere sanitario dal punto di vista interno, analizzando nel dettaglio il d. lgs. n. 101 del 2018 con le modifiche apportate al Codice della Privacy.

1.3. Il D. lgs. n. 101 del 2018 e gli interventi del Garante della Privacy.

Al fine di comprendere nel dettaglio la disciplina in materia di trattamento dei dati personali di carattere sanitario, è d'uopo analizzare la genesi del decreto legislativo n. 101 del 2018[35], nato con l'intento di adeguare il quadro normativo nazionale alle disposizioni del GDPR.

Il provvedimento è stato adottato sulla base della legge di delegazione europea n. 163 del 25 ottobre 2017, che prevede, tra le altre cose, di «abrogare espressamente le disposizioni del

[34] F. CAGGIA, *Il trattamento dei dati sulla salute, con particolare riferimento all'ambito sanitario*, in V. CUFFARO - R. D'ORAZIO -V. RICCIUTO (a cura di), op. cit.

[35] In G.U. 4 settembre 2018, n. 205.

Codice in materia di trattamento dei dati personali incompatibili con le disposizioni contenute nel predetto RGPD»[36].

Per l'elaborazione del testo è stata istituita una Commissione di studio[37] che ha elaborato una bozza di decreto conformemente ai criteri indicati e ha constatato[38] che buona parte delle disposizioni del Codice fossero da abrogare espressamente per incompatibilità, nonostante ciò la scelta dello strumento del Regolamento rende le disposizioni in esso contenute direttamente applicabili[39] in ciascuno Stato membro, costituendo dunque la normativa primaria in merito alla tutela e al trattamento dei dati personali.

Le numerose clausole di flessibilità inserite nel GDPR hanno però reso l'intervento del legislatore interno ancora più determinante, ponendo al centro del suo lavoro il bilanciamento degli interessi giuridici coinvolti e provvedendo ad un'opera di novellazione del Codice vigente.

L'intervento di riassetto, perseguendo l'obiettivo della chiarezza e della semplificazione, ha evitato di duplicare talune disposizioni,

---

[36] Art. 13 della legge delega n. 163 del 25 ottobre 2017.
[37] Con decreto del Ministro della Giustizia del 14 dicembre 2017.
[38] Come si desume dalla relazione illustrativa allegata allo schema presentato alle competenti Commissioni parlamentari per il parere.
[39] Art. 288 del TFUE: «Il regolamento ha portata generale. Esso è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri».

simili ma non identiche, presenti sia nel Regolamento che nel Codice e ha abrogato le corrispondenti disposizioni interne ove la materia era già disciplinata a livello europeo, in virtù del principio di *accountability* in base al quale il legislatore europeo imputa le scelte relative alle principali caratteristiche del trattamento – quali le misure a tutela degli interessati - al titolare del trattamento chiamato a svolgere una valutazione, assumere una decisione e dimostrare che le misure scelte siano proporzionate ed efficaci.

Ad esempio, fra le scelte più importanti a livello interno, vi è quella di tutelare i provvedimenti e le autorizzazioni al trattamento dei dati sensibili adottati dall'Autorità garante della privacy, nonché i codici di deontologia e buona condotta vigenti che «restano fermi nell'attuale configurazione nelle materie oggetto di riserva normativa degli Stati membri, mentre possono essere, negli altri ambiti, riassunti e modificati su iniziativa delle categorie interessate quali codici di condotta, alla stregua del RGPD»[40].

Il decreto è suddiviso in sei Capi e si compone di 28 articoli, dedicati a specifici aspetti della materia: i Capi da I a IV (artt. da 1 a 16), con tecnica novellistica apportano al Codice le modifiche necessarie ad assicurarne la conformità al GDPR, abrogando le disposizioni incompatibili, modificandone altre e inserendo in

[40] Art. 40.

alcuni casi nuove disposizioni in esecuzione delle riserve normative previste dal GDPR; i Capi V e VI riguardano invece la parte extra-codicistica dell'intervento normativo. Il Capo V, sotto la rubrica "Disposizioni processuali", consta di un solo articolo, il 17, che, titolato "Modifiche all'articolo 10 del decreto legislativo 1° settembre 2011 n. 150", disciplina e chiarisce, sotto il profilo strettamente procedurale, l'*iter* per dirimere le controversie previste dall'art. 152 del Codice, riformulando l'art. 10, d.lgs. n. 150/2011 sulle suddette controversie in materia di protezione dei dati personali, in modo da avere in tale ambito una disciplina completa del ricorso giurisdizionale previsto dal GDPR. Il Capo VI, infine, è dedicato alle "Disposizioni transitorie, finali e finanziarie" (artt. 18-28).

Per quel che occupa il presente studio, con riferimento al trattamento di particolari categorie di dati, già definiti "sensibili" dal Codice previgente, viene, invece, stabilito l'obbligo di previsione normativa ed è individuato un elenco di trattamenti che si considerano effettuati per "motivi di interesse pubblico rilevante" (art. 2-*sexies* in relazione all'art. 9 del GDPR). Il regime normativo per tali trattamenti è sostanzialmente rimasto inalterato rispetto a quello previsto dal Codice per i trattamenti effettuati da soggetti pubblici (art. 20) e, in particolare, l'elenco predetto è tratto dalle diverse disposizioni del Codice riferite ai trattamenti

effettuati per finalità di rilevante interesse pubblico (ad es. artt. 64-73, che il decreto legislativo ha abrogato). Dal momento che è mutato il criterio per delimitare l'ambito applicativo di tale regime, le disposizioni in parola riguardano «i trattamenti effettuati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, indipendentemente dalla natura soggettiva del titolare».

Con riferimento ai «dati genetici, biometrici e relativi alla salute, oggetto di specifica "riserva" normativa nazionale (cfr. art. 9, par. 4, del GDPR) che lascia la possibilità in capo agli Stati membri di mantenere o introdurre ulteriori condizioni di liceità, comprese limitazioni, viene previsto che il relativo trattamento sia subordinato anche al rispetto di misure di garanzia disposte dal Garante (art. 2-*septies*)».

Nel dettaglio, l'articolo 75 del Codice sancisce che «l'adozione di tali misure di garanzia sia affidata all'emanazione di un provvedimento da parte del Garante per la protezione dei dati personali – sentito il Ministro della salute che, a tal fine, acquisisce il parere del Consiglio Superiore di Sanità – da adottare almeno ogni due anni tenendo in considerazione:

a) le linee guida, le raccomandazioni e le migliori prassi pubblicate dal Comitato europeo per la protezione dei dati e le migliori prassi in materia di trattamento dei dati personali;

b) l'evoluzione scientifica e tecnologica nel settore oggetto delle misure;

c)l'interesse alla libera circolazione dei dati personali nel territorio dell'Unione europea»[41].

E' intervenuto il Garante per la protezione dei dati personali con il provvedimento n. 55 del 7 marzo 2019[42], sollecitato a più riprese da parte degli operatori del settore, dei soggetti istituzionali competenti, dei responsabili della protezione dei dati e dei cittadini, a chiarire che le condizioni di liceità del paragrafo 2, art. 9 del GDPR, previste per il trattamento di particolari dati in ambito sanitario non possano sempre applicarsi, essendovi delle circostanze in cui si rinviene la necessità di ricorrere alla base giuridica per eccellenza e cioè il consenso dell'interessato.

Nel dettaglio, i trattamenti adottati per la cosiddetta finalità di cura[43] devono essere effettuati «da (o sotto la responsabilità di) un professionista sanitario soggetto al segreto professionale o da altra persona che sia anch'essa sottoposta all'obbligo di riservatezza, pertanto la circostanza che i titolari del trattamento dei dati siano

[41] Art. 75 del Codice della Privacy, novellato.

[42] Per la consultazione del medesimo, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9091942.

[43] Art. 9, par. 2, lett. h) e par. 3 del Regolamento.

privi di tale qualifica, non consente la sussumibilità dell'utilizzo in tale base giuridica, pur essendo prevista la finalità di cura»[44].

Inoltre, quanto alla delimitazione dell'oggetto dei trattamenti per i quali non è prevista la necessità del consenso dell'interessato, il provvedimento suddetto chiarisce che debbano essere solo quelli "necessari" ed essenziali per il perseguimento della finalità di cura della salute.

Pertanto, tutti gli ulteriori trattamenti di dati che siano attinenti ma non strettamente necessari alla cura della salute, richiedono, anche se dovessero essere effettuati da professionisti sanitari soggetti al segreto professionale, una differente base giuridica che lo stesso provvedimento in oggetto individua nel «consenso dell'interessato o in un altro presupposto di liceità ai sensi degli artt. 6 e 9, par. 2, del GDPR».

Ad esempio, richiedono il consenso del paziente le seguenti categorie: «trattamenti connessi all'utilizzo di App mediche, attraverso le quali autonomi titolari raccolgono dati, anche sanitari dell'interessato, per finalità diverse dalla telemedicina oppure quando, indipendentemente dalla finalità dell'applicazione, ai dati dell'interessato possano avere accesso soggetti diversi dai

[44] *Ibidem.*

professionisti sanitari o altri soggetti tenuti al segreto professionale»[45];

«trattamenti preordinati alla fidelizzazione della clientela, effettuati dalle farmacie attraverso programmi di accumulo punti, al fine di fruire di servizi o prestazioni accessorie, attinenti al settore farmaceutico-sanitario, aggiuntivi rispetto alle attività di assistenza farmaceutica tradizionalmente svolta dalle farmacie territoriali pubbliche e private nell'ambito del Servizio sanitario nazionale (SSN)»;

«trattamenti effettuati in campo sanitario da persone giuridiche private per finalità promozionali o commerciali (es. promozioni su programmi di screening, contratto di fornitura di servizi ammnistrativi, come quelli alberghieri di degenza)»;

«trattamenti effettuati da professionisti sanitari per finalità commerciali o elettorali[46]»;

«trattamenti effettuati attraverso il Fascicolo sanitario elettronico (d.l. 18 ottobre 2012, n. 179, art. 12, comma 5)».

In tali casi, «l'acquisizione del consenso, quale condizione di liceità del trattamento, è richiesta dalle disposizioni di settore,

[45] Cfr. FAQ CNIL del 17 agosto 2018 sulle applicazioni mobili in sanità.
[46] Cfr. provvedimento del Garante per la protezione dei dati personali del 6 marzo 2014, doc. web n. 3013267.

precedenti all'applicazione del Regolamento, il cui rispetto è ora espressamente previsto dall'art. 75 del Codice»[47].

Nei capitoli che seguono, si parlerà diffusamente del Fascicolo sanitario elettronico e dell'eliminazione del consenso all'alimentazione del medesimo avvenuto tramite il c.d. Decreto Rilancio[48], permanendo invece per la consultazione del Fascicolo da parte dei medici autorizzati.

Infine, quanto al caso della refertazione online, il consenso dell'interessato è richiesto dalle disposizioni di settore in relazione alla modalità di consegna del referto[49].

1.3.1. Focus sull'intervento del Garante in merito al trattamento dei dati personali in relazione all'accertamento dell'infezione da HIV.

Al fine di comprendere il ruolo del Garante della privacy con riferimento alla tutela della dignità della persona, si è ritenuto rilevante focalizzare l'attenzione sul rispetto della riservatezza dei malati di HIV in occasione dell'erogazione delle prestazioni sanitarie.

---

47 https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9091942 cit.

48 D. l. n. 34 del 19 maggio 2020.

49 Decreto del Presidente del Consiglio dei ministri dell'8 agosto 2013.

La prima questione analizzata dall'Autorità suddetta riguarda la possibilità da parte degli esercenti le professioni sanitarie di comunicare lo stato di sieropositività di una paziente alle persone a lei più vicine, con specifico riferimento al partner nell'eventualità in cui la stessa si fosse rifiutata di comunicare la propria condizione, esponendolo al rischio di contagio.

La questione è di particolare rilevanza e di estrema delicatezza, da un canto il decreto legislativo n. 196/2003 aveva previsto l'autorizzazione in capo «agli organismi sanitari e agli esercenti le professioni sanitarie a trattare i dati idonei a rivelare lo stato di salute, qualora i dati e le operazioni siano indispensabili per tutelare l'incolumità fisica e la salute di un terzo o della collettività, e l'interessato non abbia prestato il proprio consenso per iscritto o non possa prestarlo per effettiva irreperibilità, per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere»[50], d'altro canto, si evidenzia che il richiamato Codice della Privacy non prevedeva deroghe alle disposizioni di legge che stabiliscono "divieti o limiti più restrittivi" in materia di trattamento di alcuni dati.

In merito, di fatti, la legge n. 135 del 5 giugno 1990, in tema di Aids e HIV, prevede che «la comunicazione di risultati di

[50] Autorizzazione n. 2 del 1997 - Trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale (G. U. n. 279 del 29 novembre 1997)

accertamenti diagnostici diretti o indiretti per infezione da HIV può essere data esclusivamente alla persona cui tali esami sono riferiti»[51].

Pertanto, si è ritenuto che vada ricercato il consenso della persona interessata in qualsivoglia modo possibile, ai fini della comunicazione della positività ai familiari del paziente, sia attraverso un procedimento di sensibilizzazione del soggetto sieropositivo circa le gravi conseguenze di un comportamento omissivo sulla salute del partner spingendolo quindi alla comunicazione spontanea oppure a prestare il consenso all'informazione[52], sia attraverso la prospettazione della responsabilità penale del soggetto che, consapevole del proprio stato patologico abbia omesso di informare il partner[53].

---

[51] Art. 5, comma 4, legge n. 5 giugno 1990, n. 135.

[52] Cfr. al riguardo le Linee guida dell'Organizzazione Mondiale della Sanità del dicembre 2016 sul test di autodiagnosi Hiv e la notifica volontaria al partner, reperibili in http://www.who.int/hiv/pub/vct/hiv-self-testing-guidelines/en/, la Raccomandazione del Consiglio d'Europa No. R (89) 14 nel settore della sanità e nel contesto sociale, reperibile in https://rm.coe.int/09000016804caf46, le faq del Ministero della salute su Hiv e Aids.

[53] Vedasi Cass. Pen. sez. V, 25/10/2012, n.8351; Cass. pen., sez. un., 10 luglio 2002 n. 30328, Cass. pen., sez. IV, 6 marzo 2012 n. 17758, Cass. pen., sez. V, 18 dicembre 2008 n. 4941, Cass. pen., sez. IV, 2 ottobre 2008 n. 40924, Cass. pen., sez. IV, 21 giugno 2007 n. 39594.

La seconda questione riguarda l'eventualità in cui la comunicazione circa la positività del paziente avvenga tra due soggetti pubblici.

Il Garante si è occupato della circostanza in cui un Servizio di politiche del lavoro e formazione professionale provinciale, nel novero di una richiesta di visita sanitaria di controllo, aveva trasmesso copia della documentazione dalla quale emergeva la diagnosi di sieropositività anche alla società presso la quale il soggetto svolgeva attività lavorativa.

Orbene, sebbene sussistano degli obblighi normativi nei riguardi di un lavoratore per permettere al datore di lavoro di verificare le sue reali condizioni di salute nelle forme previste dalla legge, è necessario che nel fornire all'amministrazione di appartenenza quanto richiesto vi sia un'apposita documentazione per giustificare delle mancanze, consistente in un certificato medico che contenga la c.d. prognosi e cioè l'inizio e la durata della presunta malattia.

Si precisa, inoltre, che in mancanza di disposizioni normative che prevedano specifiche per particolari figure professionali, il datore di lavoro non è mai legittimato a chiedere ed ottenere certificazioni

mediche che contengano le diagnosi[54] pertanto qualsivoglia comunicazione di dati in materia sarà illegittima e nei confronti dell'amministrazione richiedente verrà avviato un procedimento sanzionatorio.

Sul punto, si ritiene opportuno fare riferimento anche alla giurisprudenza che prevede che «in materia di protezione dei dati personali, costituisce illecito trattamento di dati sensibili l'avvenuta comunicazione, benché effettuata in maniera riservata, da un soggetto pubblico ad un altro, della copia integrale del verbale relativo all'accertamento sanitario eseguito dalla Commissione medica di verifica, in relazione alla richiesta della parte interessata volta ad ottenere il riconoscimento della pensione di inabilità, recante, oltre alla necessaria valutazione medico legale circa l'idoneità all'impiego, altri suoi dati personali che, in quanto relativi alla diagnosi, agli esami obbiettivi ed agli accertamenti clinici e strumentali svolti, nonché ad informazioni anamnestiche, tra cui quelle relative all'infezione da HIV dalla stessa precedentemente contratta, debbono considerarsi irrilevanti ai fini del buon esito del procedimento e, pertanto, da omettere»[55].

---

[54] Cfr. "Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico", 14 giugno 2007, doc. web n. 1417809.

[55] Cass. Civ. sez. I, 29/05/2015, n.11223 in Giustizia Civile Massimario 2015

La terza questione affrontata dal Garante riguarda la possibilità per il soggetto interessato di ricevere i risultati diagnostici per l'accertamento dell'HIV sul proprio Fascicolo sanitario elettronico.

In una specifica FAQ sul sito dell'Autorità, è stato chiarito che la legge n. 135 del 90 prevede che «la comunicazione dei risultati di accertamenti diagnostici diretti o indiretti per l'infezione da HIV possa essere data esclusivamente alla persona a cui tali esami sono riferiti e che spetta alla struttura sanitaria individuare le modalità di intermediazione tra medico e paziente in merito al significato diagnostico dei referti»[56] e, nel momento in cui venga soddisfatta tale intermediazione, il referto HIV sarà disponibile al pari di ogni altro referto sul Fascicolo sanitario elettronico.

Pertanto, il personale sanitario che ha in carico il paziente potrà avere accesso a tale referto ma solo con il suo consenso.

1.4. Il trattamento dei dati sanitari durante il periodo di trasmissione del virus Sars-Covid-19.

1.4.1. Disposizioni correlate all'epidemia da Covid-19.

Diritto & Giustizia 2016, 4 maggio e Cass. civ., Sez. I, Ordinanza, 28/03/2022, n. 9919.

[56] Relazione annuale del 2022 dell'attività svolta dal Garante della Privacy.

La pandemia ha determinato l'attivazione del Garante della Privacy sotto plurimi aspetti, infatti, sin dal primo manifestarsi della diffusione del virus Sars-Covid-19 è stato chiamato a misurarsi – di concerto con l'attività del Comitato europeo per la protezione dei dati e dei gruppi di lavoro sovranazionali – con una difficilissima risposta istituzionale attivata per fronteggiare, tanto sul piano sanitario, quanto su quello economico e sociale gli effetti della diffusione del virus.

Inizialmente, si è ritenuto necessario provvedere a delle innovazioni sul piano pratico inimmaginabili e assolutamente imprevedibili per fronteggiare una pandemia senza precedenti.

La modifica più rilevante è stata la creazione di un sistema di allerta Covid-19 – di cui si parlerà approfonditamente nel prosieguo – che in Italia si è tradotto nella realizzazione dell'applicazione Immuni caratterizzata dalla volontarietà dell'adesione individuale, sempre nel tentativo di salvaguardare i diritti fondamentali delle persone, in particolare la dignità, la riservatezza e il diritto alla protezione dei dati personali.

Per quel che qui ci occupa, il decreto-legge n. 18 del 17 marzo 2020[57] ha trattato le disposizioni inerenti al trattamento dei dati

[57] Il Decreto-legge recante «misure di potenziamento del Servizio sanitario nazionale e di sostegno economico per famiglie, lavoratori e imprese connesse all'emergenza epidemiologica da Covid-19» (cd. Cura Italia), convertito con la legge 24 aprile 2020, n. 27.

personali nel contesto emergenziale all'art. 17-*bis*, al fine di «garantire l'efficacia delle misure di protezione dell'emergenza sanitaria ovvero ad assicurare la diagnosi e l'assistenza sanitaria delle persone contagiate e la gestione emergenziale del Servizio Sanitario Nazionale».

Come è stato detto in precedenza, l'art. 9, par. 2, lett. *g), h), e i)* del GDPR e l'art. 2-*sexies*, comma 2, lett. *t) e u)* del Codice della privacy[58] consentono a tutti i soggetti che, a vario titolo, siano incaricati nella gestione dell'emergenza, per motivi di sanità pubblica, di effettuare trattamenti di dati personali anche sensibili e giudiziari anche mediante scambio reciproco di informazioni che risultino necessarie per l'espletamento delle funzioni[59].

Inoltre, è stata consentita la comunicazione dei dati personali a soggetti pubblici e privati differenti[60] da quelli citati e con riferimento ai dati diversi da quelli di cui all'art. 9 di cui si è detto in precedenza e all'art. 10 riguardante i dati giudiziari del GDPR, nelle circostanze in cui ciò risulti indispensabile per la gestione dell'emergenza sanitaria in atto, sempre nel rispetto dei principi di

---

[58] Come novellato ai sensi del decreto legislativo n. 101 del 2018.

[59] In particolare, ci si riferisce, ai soggetti che lavorano presso il Servizio di protezione civile e ai soggetti attuatori di cui all'art. 1 dell'ordinanza del Capo del Dipartimento della protezione civile del 3 febbraio 2020, n. 630, agli uffici del Ministero della salute e dell'Istituto superiore di sanità e alle strutture pubbliche e private che operano nell'ambito del Ssn.

[60] Il riferimento viene fatto a coloro i quali hanno ricoperto un ruolo apicale.

cui all'art. 5 del GDPR e cioè adottando misure appropriate a tutela dei diritti e delle libertà degli interessati.

Inoltre, fino alla cessazione dello stato d'emergenza, nel bilanciamento tra salute pubblica, gestione della pandemia e salvaguardia della riservatezza dei soggetti interessati, le autorizzazioni per il trattamento delle proprie informazioni[61] possono essere date con modalità semplificate, anche in forma orale, e l'informativa di cui all'art. 13 e 14 GDPR può essere omessa o fornita in versione semplificata, previa comunicazione della limitazione effettuata.

Infine, una volta cessato lo stato d'emergenza, sono stati i medesimi soggetti a adottare delle misure che hanno ricondotto i trattamenti svolti nel contesto emergenziale nel novero delle competenze ordinarie e delle regole che disciplinano i trattamenti dei dati personali.

1.4.2. Attività di gestione dei dati inerenti alla salute dei pazienti affetti da Covid-19.

La pandemia da Covid-19, com'è noto, ha messo a dura prova gli equilibri già molto labili riguardo al rapporto tra riservatezza e

[61] Art. 2-*quaterdecies* del Codice della privacy.

ostensibilità dei dati di carattere sanitario, specie con riferimento a quelli riguardanti i pazienti affetti *da* o deceduti *per* Covid-19 da parte di strutture sanitarie.

Il Garante della Privacy è intervenuto sul tema più volte e in una circostanza ha sanzionato il titolare del trattamento nel caso in cui i parenti di un paziente deceduto avevano segnalato che l'ospedale che aveva avuto in cura il loro parente, aveva diffuso, senza alcuna forma di autorizzazione, numerose informazioni di dettaglio sulla storia clinica del defunto attraverso la diramazione di un comunicato stampa, successivamente riportato dalle testate giornalistiche.

Nel provvedimento[62] si è ritenuto che «l'esigenza di informare l'opinione pubblica sull'appropriatezza dell'assistenza sanitaria prestata ai pazienti ricoverati per covid-19» richiamata dalla struttura sanitaria in parola, non richiedeva la diffusione di informazioni cliniche di dettaglio sullo stato di salute del paziente. Infatti, con un comunicato stampa[63], sin dall'inizio del fenomeno pandemico, è stato previsto che con specifico riguardo alla diffusione dei dati personali inerenti le persone risultate positive al Covid sui *social media* e sugli organi di stampa – anche digitali – anche nella situazione di emergenza sanitaria, nella quale

[62] Provvedimento n. 35 del 27 gennaio 2021, doc. web n. 9549143.
[63] Comunicato stampa del 31 marzo 2020, doc. web n. 9303613.

l'informazione ha svolto un ruolo dirimente, non avrebbero potuto essere «disattese alcune garanzie a tutela della riservatezza e della dignità delle persone colpite dalla malattia contenute nella normativa vigente e nelle regole deontologiche relative all'attività giornalistica».

Attraverso le FAQ, inoltre, sono state fornite delle indicazioni in merito al divieto di diffondere i dati identificativi delle persone risultate positive al coronavirus o sottoposte ad isolamento domiciliare, chiarendo che le strutture sanitarie o qualsivoglia soggetto pubblico o privato non potessero diffondere, né tramite i propri siti web, né in altro modo, i nominativi dei soggetti risultati positivi o sottoposti ad isolamento per finalità di contenimento della diffusione della pandemia[64].

Dalla relazione dell'attività svolta dal Garante della privacy dell'anno 2020[65], emerge come siano pervenuti circa centocinquanta reclami e segnalazioni in merito al trattamento dei dati personali effettuati dalle strutture sanitarie nell'ambito della gestione della pandemia.

---

[64] Cfr FAQ sul trattamento dei dati nel contesto sanitario nell'ambito dell'emergenza sanitaria.

[65] Per una sintesi, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9676316, per il testo completo https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9676435.

In molti casi, il reclamo ha avuto ad oggetto la modalità attraverso la quale le strutture sanitarie hanno comunicato la positività ai pazienti e le regole inerenti il regime di isolamento, profilassi ecc,, essendo avvenuto attraverso l'invio di un'email in cui, erroneamente, tutti i destinatari erano stati inseriti in chiaro, circostanza che ha consentito, di fatto e senza giustificato motivo e senza alcuna base giuridica, a ciascuno di questi soggetti di venire a conoscenza dell'indirizzo di posta elettronica degli altri destinatari positivi e sottoposti ad isolamento.

Per ovviare a tale circostanza sarebbe stato sufficiente, per assecondare le esigenze di celerità delle strutture sanitarie in oggetto, inserire i destinatari nell'apposito spazio dedicato alla "copia conoscenza nascosta".

Altre istruttorie hanno riguardato, invece, l'eventualità in cui l'operatore sanitario, al fine di ricostruire la cosiddetta «filiera di contatti stretti del paziente risultato positivo al coronavirus abbia effettuato delle indagini per svelare l'identità dei medesimi»[66]; in questa circostanza, essendovi la necessità di bilanciare le esigenze di sanità pubblica e quelle relative alla tutela dei dati personali, conformemente a quanto indicato dal GDPR in merito all'eccezione al divieto di trattamento dei dati per motivi di

[66] Art. 3, comma 6, d.P.C.M. 8 marzo 2020, circolare del Ministero della salute 22 febbraio 2020, n. 5443 e successive modificazioni e integrazioni.

interesse pubblico nei settori della sanità pubblica, è stato ritenuto legittimo il comportamento dell'operatore sanitario inerente al disvelamento dell'identità del contatto stretto del soggetto positivo, così da ricostruire la catena dei contagi.

Un caso di rilevante importanza ha riguardato i chiarimenti forniti dalla Presidenza del Consiglio dei ministri circa la possibilità che i Dipartimenti dell'Amministrazione penitenziaria (DAP) potessero accedere direttamente alle banche dati relative alle persone positive al coronavirus e dunque sottoposte alla misura dell'isolamento domiciliare in vista della riattivazione dei colloqui con i propri congiunti.

Il Garante ha presunto che «stante la difficoltà di avere una lista aggiornata dei pazienti affetti da coronavirus e soprattutto l'eventualità in cui al tampone il soggetto risulti sì negativo ma magari con il virus in stato di incubazione, è stata prevista l'obbligatorietà del rispetto delle misure di distanziamento sociale e dell'adozione delle misure di protezione individuale da ambo i lati in occasione di tutte le visite».

In ogni caso, è stato previsto che la Direzione degli istituti penitenziari potesse avanzare «una richiesta alla competente prefettura – nella qualità di ente avente libero accesso alle banche dati relative ai soggetti positivi al coronavirus o sottoposti a isolamento domiciliare come contatti stretti – per avere

un'indicazione puntuale dei soggetti che possano essere ammessi ai colloqui con i congiunti detenuti, limitando la conoscenza dei dati realmente necessari per lo svolgimento delle funzioni»[67] senza per questo motivo avere un accesso generalizzato a tutte le informazioni che erano nella disponibilità delle varie Prefetture di Italia.

1.4.3. Utilizzo delle applicazioni per il controllo della diffusione del coronavirus.

Prima di focalizzare l'attenzione sull'applicazione per eccellenza che è nata con l'intento di tracciare e contenere la diffusione del virus e cioè Immuni – e le equivalenti previste in buona parte dei Paesi dell'Unione Europea – si è ritenuto opportuno analizzare le applicazioni promosse da regioni e da altri soggetti pubblici aventi una pluralità di finalità tra le quali: «tracciare una mappa del contagio tramite la compilazione di un questionario giornaliero da parte degli utenti, monitorare la diffusione del virus dei contagiati asintomatici previamente registrati su apposito portale, controllare i soggetti in isolamento domiciliare, tracciare i contatti, censire i soggetti che facevano ingresso nel territorio regionale nonché

[67] Art. 5, par. 1, lett. c) del GDPR.

raccogliere autodichiarazioni circa la sintomatologia da Covid-19 per facilitare i rapporti tra il paziente e l'operatore sanitario»[68].

Infatti, durante il periodo pandemico, proprio al fine di limitare le occasioni di contagio, le strutture sanitarie hanno ridotto all'essenziale le visite mediche dando invece grande spazio agli strumenti di telemedicina – applicazioni di telediagnosi, teleconsulto, teleassistenza e telemonitoraggio utilizzate dal personale medico – per fare diagnosi o monitorare le terapie. Essendovi comunque la finalità di cura ed essendo una differente modalità di svolgimento del rapporto medico/paziente, non è stato prevista la richiesta di un consenso specifico dell'interessato.

Nonostante ciò, è necessario che il titolare del trattamento effettui una valutazione di impatto[69], fornendo all'interessato un'informativa completa ed esaustiva, nel totale rispetto dei principi di integrità, riservatezza ed esattezza dei dati sanitari trattati.

È necessario sottolineare che, sebbene le applicazioni che forniscono una prestazione sanitaria siano state di dirimente importanza abbattendo totalmente le barriere fisiche, è sempre

---

[68] F. BRIZZI, *Dati sanitari, GDPR e Covid-19, Il caso della ricerca: tra scienza e diritto*, 2021, Key editore srl, p. 70.

[69] Art. 35 GDPR.

stata garantita la prestazione sanitaria in presenza, nel rispetto delle regole inerenti al distanziamento sociale.

Ma, se queste tipologie di applicazioni sono un valido alleato della relazione terapeutica, sussistono dei dubbi circa la legittimità delle singole applicazioni finalizzate al tracciamento dei contagi di stampo regionale.

Invero, il Garante, richiamando il quadro normativo legato ad un sistema di *contact tracing* digitale che aveva come obiettivo – poi timidamente raggiunto (*ndr*) – di uniformare a livello nazionale le garanzie poste a tutela degli interessati, nelle FAQ[70] ha chiarito che «con riguardo alle app regionali, l'installazione delle medesime non può essere obbligatoria, né condizionare l'accesso ad aree e territori in quanto ciò determinerebbe una lesione dei diritti fondamentali dell'individuo, quale ad esempio la libertà di circolazione e soggiorno prevista dall'art. 16 della Costituzione; esse devono trattare solamente i dati strettamente necessari a perseguire le finalità del trattamento, non raccogliendo dati ultronei – come ad esempio quelli relativi alla geolocalizzazione del dispositivo – e limitandosi a raccogliere solo i consensi per

[70] App nazionale di contact tracing e app regionali per COVID-19, pubblicate sul sito il 13 luglio 2020.

l'accesso a funzionalità o informazioni presenti nel dispositivo, se indispensabili»[71].

Di fatti, prima di addivenire alla realizzazione dell'app Immuni, vi è stata una lunga fase di "concertazione"[72] tra Autorità garante della privacy e Governo che di seguito verrà, brevemente, rappresentata.

Originariamente vi erano le dubbiose istanze, portate avanti dal Garante, dei costituzionalisti italiani in merito alla lesione dei diritti fondamentali con riferimento alle normative emergenziali.

In seguito, si è concordato che la soluzione paventata dall'Italia fosse in linea sia con la Costituzione sia con la normativa europea in conformità all'art. 23 del Regolamento generale sui dati personali e all'art. 15 della Direttiva e-Privacy che, sotto il paraurti previsto dall'art. 52, par. 1, della Carta dei diritti fondamentali dell'Unione europea, prevedono «limitazioni a mezzo di misure legislative di alcuni diritti nella misura in cui la limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata in una società democratica»[73] per

---

[71] Per la consultazione, https://www.garanteprivacy.it/temi/coronavirus/faq#app.

[72] Descritta pedissequamente nella Relazione 2020 del Garante della privacy.

[73] Articolo 23 del GDPR e sul punto vedasi F. BRIZZI, *Dati sanitari, GDPR e Covid-19, Il caso della ricerca: tra scienza e diritto*, 2021, Key editore srl, p. 76

tutelare una consistente serie di obiettivi tra i quali la sicurezza pubblica e la sanità pubblica[74].

In Italia, la base legale per lo sviluppo dell'App immuni è stata individuata nel decreto-legge n. 28/2020.

Infatti, le disposizioni in esso previste sono stata considerate «proporzionate con riferimento alla descrizione delle misure, all'indicazione di massima dei diritti limitati e alla finalità della scelta pianificata che fosse il meno impattante possibile»[75].

Inoltre, viene pienamente rispettato il criterio della gradualità, in quanto si è optato per una misura meno invasiva che lascia indietro lo spettro di una tecnologia tracciante *tout court* e di conseguenza pervasiva, facendo spazio ad una componente "solidaristica" e della volontarietà dell'uso dell'app.

In Australia[76], ad esempio, il cittadino che utilizza l'app di tracciamento viene considerato come "paziente" e il server governativo viene gestito da Amazon – un'azienda privata per l'appunto – che procede ad una mappatura dei casi, assicurandone però una rapida distruzione.

---

[74] M. PLUTINO, *"Immuni", Un'exposure notification app alla prova del bilanciamento tra tutela dei diritti e degli interessi pubblici*, in *Dirittifondamentali.it* - Fascicolo 2/2020, 28 maggio 2020.

[75] Rapporto annuale 2019 dell'European Data Protection Supervisor.

[76] M. PLUTINO, *"Immuni", Un'exposure notification app alla prova del bilanciamento tra tutela dei diritti e degli interessi pubblici*, op. cit.

In Norvegia[77], l'app viene prodotta da una no-profit governativa ma si serve dello strumento del *gps* e i dati vengono detenuti per trenta giorni in un server governativo.

Nei paragrafi che seguono, attraverso l'analisi pedissequa dell'applicazione di tracciamento e il confronto con le esperienze estere ci si interrogherà circa l'effettività di uno strumento che, tenuto conto del momento in cui è stato sviluppato, avrebbe dovuto essere forse (*ndr*) più pervasivo e impattante, in virtù dei suoi insuperabili rischi connessi alla tutela della privacy.

1.4.4. Il tracciamento dei contagi da Sars Covid-19 attraverso la tecnologia Bluetooth Low Energy: App immuni.

Con provvedimento n. 95 del 1° giugno 2020[78], il Garante ha autorizzato «il Ministero della salute ad avviare il trattamento dei dati relativi al Sistema di allerta Covid-19 (app Immuni) di cui all'art. 6 del d.l. n. 28 del 30 aprile 2020, con il parere reso ai sensi dell'art. 36, par. 5 e 58, par. 3, lett. c) del GDPR e dell'art. 2-*quinquiesdecies* del Codice della Privacy».

---

[77] M. PLUTINO, *"Immuni", Un'exposure notification app alla prova del bilanciamento tra tutela dei diritti e degli interessi pubblici*, op. cit.

[78]Per la consultazione, "Provvedimento di autorizzazione al trattamento dei dati personali effettuato attraverso il Sistema di allerta Covid 19- App Immuni - 1° giugno 2020 [9356568]".

Il trattamento dei dati personali è stato ritenuto «legittimo e proporzionato, dal momento che sono stati rispettati i diritti e le libertà degli interessati e sono state adottate confacenti misure di prevenzione e diagnosi finalizzate all'agevole presa in carico delle persone contagiate da parte del SSN e l'istantanea individuazione di nuovi focolai di infezione»[79].

Si è ritenuto fosse stata rispettata «la trasparenza, la correttezza e la sicurezza in ogni fase del trattamento».

In particolare, il Sistema implica il trattamento dei dati necessari e cioè, senza pretesa di esaustività, il «*Temporary Exposure key – TEK*»[80]*;* il «*Rolling Proximity Identifier – RPI*»[81]*,* «la data di inizio dei sintomi per le persone risultate positive al tampone naso faringeo per la rilevazione del Sars-CoV-2», «la notifica di avvenuta esposizione, al fine di allertare, per sanità pubblica, tutti

[79] *Ibidem.*

[80] Si tratta di una chiave di medio periodo della lunghezza di 128 bit, denominata TEK (Temporary Exposure Key), a sua volta generata al primo uso della app e, successivamente, rigenerata con frequenza giornaliera tramite un generatore pseudocasuale crittografico.
Da ogni chiave TEK possono essere ricavati con procedimento matematico fino a 144 RPI corrispondenti (la funzione utilizzata non è invertibile, per cui non è possibile calcolare la TEK da cui un certo RPI è stato ottenuto).

[81] Gli RPI (Rolling Proximity Identifiers) sono identificativi pseudonimizzati effimeri, tramite tecnologia BLE, che permettono contestualmente di ricevere gli analoghi identificativi trasmessi dai dispositivi utilizzanti la medesima app e rilevati in prossimità tramite l'uso della stessa tecnologia.

i soggetti che siano entrati in contatto con i soggetti risultati positivi al virus».

Nel paragrafo precedente si è accennato alla volontarietà dell'utilizzo dell'applicazione come espressione del concetto di altruismo dei dati[82] e come indicatore della mancanza di pervasività dello sviluppo di questa applicazione di tracciamento.

Il Comitato europeo per la protezione dei dati nelle sue linee guida[83] e l'Autorità garante della privacy hanno previsto che l'autodeterminazione dell'interessato si manifesti in tutte le fasi del suo funzionamento e cioè: il *download*, l'installazione, la configurazione, l'attivazione della tecnologia Bluetooth, il caricamento delle TEK sui sistemi di *back-end*[84] di Immuni in caso di risultato positivo del tampone, la raccolta delle differenti categorie di *analytic* nelle singole fasi in cui si espleta il trattamento, la consultazione del medico di famiglia a seguito del ricevimento del messaggio di *alert* e financo la possibile disinstallazione dell'applicazione.

---

[82] A. VIGORITO, *Sul crinale tra data altruism e social scoring: esperienze applicative della sequenza dati-algoritmi nel nuovo contesto regolatorio europeo*, in *medialaws*.

[83] Punti 24 e 31 delle linee guida 04/2020 sull'utilizzo dei dati di localizzazione e degli strumenti per il tracciamento dei contatti.

[84] Il back-end è costituito dai dati e dall'infrastruttura che fanno funzionare l'applicazione.

Con riguardo alla pseudonimizzazione, elemento fondamentale per tutelare i dati, da un lato si è provveduto alla distribuzione delle chiavi TEK ma non anche delle chiavi di decodifica, impedendo dunque di risalire all'identità dell'utente.

Infatti la predisposizione di adeguate tecniche di cifratura asimmetrica ha permesso di realizzare realmente la pseudonimizzazione per disaccoppiare le chiavi TEK con le chiavi di decodifica[85] per garantire il rispetto dell'art. 6, comma 2, lett. c) del d.l. n. 28/2020 e la pubblicazione delle TEK dei soli soggetti risultati positivi.

Dunque, il Garante, nel provvedimento di autorizzazione del trattamento ha previsto che «l'algoritmo, basato su criteri epidemiologici di rischio e modelli probabilistici (specificando i parametri di configurazione impiegati e le assunzioni effettuate), sia puntualmente indicato e costantemente aggiornato nella valutazione d'impatto, in osservanza del principio di responsabilizzazione» – come previsto dall'art. 6, comma 2, lett. b), del d.l. n. 28/2020 – ; «gli utenti siano adeguatamente informati in ordine alla possibilità che l'app generi notifiche di esposizione che non sempre riflettono un'effettiva condizione di rischio» (ad esempio, attraverso la probabilità che taluno entri in contatto con

[85] F. BRIZZI, op. cit.

un soggetto positivo al Covid in occasione del proprio lavoro ma con l'adozione dei DPI) e «fornisca agli utenti informazioni semplici e chiare sul funzionamento dell'algoritmo (anche attraverso una c.d. info-grafica)»; gli utenti dell'app potranno anche eliminare l'applicazione o disattivarla[86].

Con riferimento invece agli *analytic*[87], il Garante nel provvedimento su citato ha previsto che «gli stessi siano accuratamente protetti per impedire qualsivoglia forma di riassociazione dei dati a soggetti identificabili», «assicurando l'adozione di adeguate misure di sicurezza e tecniche di anonimizzazione da individuarsi in ragione delle specifiche finalità in concreto perseguite, nel rispetto dei principi di *privacy by design e by default* (art. 25 del Regolamento)»[88].

Con riguardo all'utilizzo dell'app da parte di minori che hanno compiuto quattordici anni, si è raccomandata una peculiare

---

[86] 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 - 1° giugno 2020 [doc. web n. 9356568] Registro dei provvedimenti n. 95 del 1° giugno 2020.

[87] Si fa riferimento alla circostanza in cui l'app trasmette, in maniera automatica e secondo un modello probabilistico, al backend di Immuni le c.d. Operational Info without Exposure e, se c'è stato un contatto a rischio le c.d. Operational Info with Exposure.

[88] 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 - 1° giugno 2020 [doc. web n. 9356568] Registro dei provvedimenti n. 95 del 1° giugno 2020.

attenzione in merito alle informazioni da fornire e alle notifiche da esposizione.

Per garantire un ulteriore miglioramento della sicurezza complessiva, il Garante ha previsto che siano ristretti i tempi di conservazione degli indirizzi IP sui dispositivi mobili in quanto tale dato potrebbe consentire la riconducibilità all'identificazione dell'utente risultato positivo; in ordine al tracciamento delle operazioni compiute dagli amministratori di sistema, queste devono essere trasparenti mentre, con riferimento all'eventualità in cui a seguito delle pubblicazioni delle TEK per svariate ragioni – omonimia, scambio di referti o meri errori materiali – si verifichi la necessità di un intervento di rettifica dei dati inseriti per ripristinarne l'accuratezza, deve essere prevista una celere modalità, al fine di non arrecare nocumento ad alcuno.

Prima di concludere l'analisi specifica del trattamento dei dati personali di carattere sanitario durante il periodo pandemico, si ritiene interessante procedere alla comparazione dell'utilizzo delle applicazioni di tracciamento negli altri paesi, europei e non.

1.4.4.1. Valutazione e comparazione delle esperienze estere in merito alle app di tracciamento del contagio.

Se nel paragrafo precedente è stata illustrata la normativa e la disciplina inerente all'app Immuni, ed è stato sottolineato come l'autorizzazione del Garante abbia fatto seguito ad un'intensa fase di concertazione con il Governo avente come nocciolo duro l'assoluto rispetto delle libertà costituzionalmente garantite, si è ritenuto, comunque, interessante vedere cosa è accaduto al di fuori del nostro Paese.

Ad esempio, in Cina[89] è stata sviluppata l'app *Trace Together* che sfrutta la funzionalità Bluetooth: un utente, infatti, scarica sul proprio *smartphone* l'applicazione e dal semplice *download* è possibile rilevare un altro dispositivo che abbia l'applicazione attiva e che si trovi nelle immediate vicinanze, generando dunque un'interazione che permetta la stima della vicinanza e della durata dell'incontro dei due utenti.

I dati suddetti venivano memorizzati nel telefono e nell'eventualità di una positività il Ministero della salute attraverso l'ID[90] del telefono avrebbe attivato il processo di ricerca degli utenti che fossero, potenzialmente, entrati in contatto con il contagiato per disporne la quarantena.

---

[89] F. LIALNG, *Covid-19 and Health Code: How Digital Platforms Tackle the Pandemic in China*, in *Soc. Med. + Soc*., v.6, 3/2020.

[90] l'ICC-ID acronimo di Integrated Circuit Card ID è un numero seriale stampato sulla scheda del cellulare.

La popolazione cinese però non ha colto in maniera entusiastica lo sviluppo di questa app di tracciamento, ravvisando un tentativo di intromissione del Governo nelle vite quotidiane dei cittadini, al contrario però, lo stesso potere centrale ha affermato a più riprese che il *download* dell'applicazione fosse un dovere morale[91] del cittadino cinese, in ossequio ai principi solidaristici di confuciana memoria.

L'esperienza australiana invece, rappresenta un fiore all'occhiello nella massimizzazione della sicurezza dei dati e nell'integrità del sistema con una legislazione mirata[92] con riguardo al trasferimento, l'archiviazione, l'uso e lo smaltimento dei dati, ciononostante, l'app *Covid Safe* non ha contribuito positivamente al tracciamento dei dati in virtù della scarsa diffusione[93] della stessa tra la popolazione a rischio e dello scarso valore predittivo. Inoltre, dal momento che neppure il personale sanitario ha potuto avere accesso ai dati derivanti dalle *app* scaricate dalla popolazione australiana, il lavoro effettuato dai medesimi e

---

[91] E. SETO, P. CHALLA, P. WARE, *Adoption of Covid-19 contact tracing apps: A balance between privacy and effectiveness*, in *Jou. of med. Inter. Res*., v.23, 3/2021.

[92] Emendamento Privacy, 4/2020.

[93] D.J. CURRIE, C.Q. PENG, D.M. LYLE, B.A. JAMESON, M.S. FROMMER, *Stemming the flow: how much can the Australian smartphone app help to control Covid-19*, in *Pub. Hea. Res. & Prac.*, v.30, 2/2020.

l'aggravio derivante dalla pandemia non ha condotto ai benefici desiderati[94].

In Svezia, invece, le autorità e la *Swedish Health*[95] hanno predisposto per gli operatori sanitari una piattaforma per inserire, in tempo reale, i dati inerenti ai pazienti affetti da infezione.

La *Swedish Health*, dunque, raccoglie i dati dell'applicazione denominata *Emergency Response App* e li mette a disposizione dei sanitari che monitorano lo stato delle strutture, indicando la gestione dei letti a disposizione, dei turni di lavoro del personale, delle dimissioni dei pazienti e dei ventilatori utilizzati.

Sebbene sulla carta si trattasse di uno strumento che nasceva con l'intento di velocizzare il lavoro del personale sanitario, dando una spinta all'efficienza del lavoro e di conseguenza alla qualità delle cure dei malati, le informazioni caricate a sistema risultavano spesso incomplete, complesse e talvolta erronee, tali da non garantire, soprattutto nei periodi di apice della pandemia, di disporre di un valido *data set*[96].

---

[94] F. VOGT, B. HAIRE, L. SELVEY, A.L. KATELARIS, & J. KALDOR, *Effectiveness evaluation of digital contact tracing for Covid-19 in New South Wales, Australia,* in *the Lanc. Pub. Hea*., v. 7, 3/2022, e250 ss.

[95] Il più grande fornitore di servizi sanitari senza scopo di lucro con sede a Seattle, in collaborazione con Microsoft.

[96] https://www.beckershospitalreview.com/healthcare-information-technology/swedish-health-services-taps-microsoft-to-build-app-that-tracks-covid-19-patients-hospital-capacity.html

Anche il Regno Unito e gli Stati Uniti si sono dotati di un app – *Covid Symptom Tracker* - che permette l'auto-segnalazione della sintomatologia da Covid-19, sia da parte di utenti sani sia da parte di pazienti affetti dal virus.

Invero, le risultanze dell'analisi a campione delle persone che hanno utilizzato l'app hanno rilevato che fattori di comorbità come l'anzianità, l'obesità, il diabete, le malattie polmonari, renali e cardiache pregresse comportavano una maggiore tendenza all'ospedalizzazione.

Nonostante le ottime premesse, l'utilizzo *on label*[97] dell'applicazione non è andato a buon fine, per una serie di motivazioni: innanzitutto l'utenza media del *download* era particolarmente giovane, secondariamente non venivano auto-segnalati tutti i sintomi e infine, si pregiudicavano tutti coloro i quali non possedevano uno *smartphone* o comunque non avevano grossa dimestichezza con la tecnologia e quindi, fra tutti, gli anziani che erano classificati come soggetti più a rischio[98].

---

[97] Definizione a contrario, rispetto a "off label" e cioè al di fuori dell'indicazione terapeutica.

[98] M.N. LOCHLAINN, K.A. LEE, C.H. SUDRE, T. VARSAVSKY, M.J. CARDOSO, C. MENNI, J.L. Du CADET, *Key predictors of attending hospital with COVID19: An association study from the Covid Symptom Tracker App in 2,618,948 individuals*, *medRxiv*, 2020.

Soltanto con l'aggiornamento dell'applicazione e il rilevamento da parte del marchio *Zoe Health Study*, è stato predisposto l'utilizzo *off label* della piattaforma.

Infatti, secondo le nuove indicazioni ciascun utente compila il proprio profilo, inserendo plurime sottospecie di informazioni sanitarie[99] che esulano dalla sintomatologia Covid e che forniscono «uno dei più grandi set di dati del mondo sulla funzione immunitaria attraverso sintomi correlati a COVID-19/influenza, risultati dei test, vaccinazioni e dati sugli effetti avversi delle vaccinazioni e altro»[100].

L'utilizzo di questa applicazione ha consentito la conduzione di uno studio su 63.002 partecipanti infetti che hanno segnalato i propri sintomi, permettendo di «quantificare le differenze di sintomi, rischio di ricovero ospedaliero e durata a seguito dell'infezione con le varianti *omicron* o *delta* tra le persone vaccinate (due o tre dosi) in un'ampia coorte comunitaria del Regno Unito tratta dall'app ZOE COVID Study»[101].

---

[99] Sintomi della menopausa, sintomi di pazienti oncologici.

[100] https://health-study.zoe.com/post/introducing-the-zoe-health-study

[101] C. MENNI, A.M. VALDES, L. POLIDORO, M. ANTONELLI, S. PENAMAKURI, A. NOGAL & T.D. SPECTOR, *Symptom prevalence, duration, and risk of hospital admission in individuals infected with SARS-CoV-2 during periods of omicron and delta variant dominance: a prospective observational study from the Zoe Covid Study*, in *the Lancet*, v.399, 10335/2022, p. 1618 ss.

Infine, questa carrellata comparatistica si conclude con l'esperienza della Germania che ha sviluppato un'applicazione per *smart-watch* che raccoglie dati su pulsazioni, temperatura e fasi del sonno quali indicatori per lo *screening* di malattie virali simil-influenzali[102], tali dati venivano trasmessi in tempo reale su una mappa interattiva online in cui le autorità avevano la facoltà di valutare le probabilità di incidenza Covid-19 in tutta la nazione.
Ma, la bassa mortalità *pro-capite* in Germania non è stata imputabile al tracciamento dei contagi tramite l'app – non tutte le persone esposte al virus erano in possesso di uno *smart-watch* o un *fitness tracker* e non vi era garanzia che i dati venissero trasmessi[103] - ma alle politiche sanitarie mirate, test diffusi e interventi sanitari mirati, pertanto anche in Germania il tracciamento digitale dei contagi da Covid-19 non ha fornito i risultati tanto auspicati.

1.5. Uso primario e secondario dei dati: la ricerca scientifica, definizioni e sguardo d'insieme.

[102] https://www.pressure.com/article/us-health-coronavirus-germany-tech/germany-launches-smartwatch-app-to-monitor-coronavirus-spread-idUSKBN21P1SS

[103] S. WHITELAW, M.A. MAMAS, E. TOPOL, & H.G. VAN SPALL, *Applications of digital technology in Covid-19 pandemic planning and response*, in *The Lan. Dig. Hea*, v. 2, 8/2022, e435 ss.

Uno degli ambiti in cui è maggiormente rilevabile la tensione tra dimensione individuale e collettiva dell'utilizzo dei dati sanitari è quello della ricerca scientifica.

In letteratura, risulta complicato trovare una definizione universalmente condivisa di ricerca in generale o scientifica nel particolare, infatti nel parere del 6 gennaio 2020[104], lo stesso *European Data Protection Supervisor*[105], ha raccomandato di intensificare maggiormente il dialogo tra le autorità di protezione dei dati e i comitati di revisione etica per una comprensione comune di quali attività possono essere annoverate nella nozione di "ricerca scientifica".

Non essendovi una definizione normativa, il GDPR inserisce all'interno del Considerando 159, una nozione particolarmente ampia includendo «sviluppo tecnologico e dimostrazione, ricerca fondamentale, ricerca applicata e ricerca finanziata da privati, oltre

---

[104] European Data Protection Supervisor, Un parere preliminare sulla protezione dei dati e la ricerca scientifica, 6 gennaio 2020.

[105] L'European Data Protection Supervisor è un'autorità europea indipendente, istituita dal Regolamento (CE) n. 45 del 2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati. L'EDPS lavora in stretto contatto con l'EDPB, che è l'unica istituzione che ha il compito di verificare la corretta applicazione del GDPR su tutto il territorio dell'UE.

a tenere conto dell'obiettivo dell'Unione di istituire uno spazio europeo della ricerca ai sensi dell'articolo 179, paragrafo 1, TFUE» ovvero «studi svolti nell'interesse pubblico nel settore della sanità pubblica»[106]. Dalla descrizione appena riportata emerge che il legislatore europeo richiede che la disciplina sulla protezione dei dati trovi uno spettro applicativo più ampio possibile, infatti, ad esempio, non è ravvisabile alcuna distinzione tra la ricerca scientifica finalizzata ad un interesse pubblico e la stessa finalizzata a fini privati e commerciali.

Sempre nel novero delle possibili definizioni inerenti alla ricerca scientifica, si può citare anche la Direttiva sul diritto d'autore del 2019[107], la quale, parlando degli enti e delle organizzazioni che svolgono attività di ricerca, stabilisce che «vista la varietà dei soggetti in causa è importante che vi sia un'interpretazione unanime del concetto di organismi di ricerca. Vi dovrebbero, ad esempio, rientrare, oltre alle università o agli altri istituti di istruzione superiore e alle loro biblioteche, anche entità come gli istituti di ricerca e gli ospedali che svolgono attività di ricerca. In

[106] Considerando 159, GDPR.

[107] Direttiva del Parlamento europeo e del Consiglio n. 790 del 2019sul diritto d'autore e sui diritti connessi nel mercato unico digitale e che modifica le direttive 96/9/CE e 2001/29/CE, per la consultazione integrale del testo, https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX%3A32019L0790.

genere, a prescindere dalle diverse forme e strutture giuridiche, in tutti gli Stati membri gli organismi di ricerca hanno in comune il fatto di agire senza scopi di lucro ovvero nell'ambito di una finalità di interesse pubblico riconosciuta dallo Stato. Tale finalità potrebbe tradursi, ad esempio, in un finanziamento pubblico oppure in disposizioni di leggi nazionali o in appalti pubblici. Viceversa, non si dovrebbero considerare organismi di ricerca ai fini della presente direttiva quelli su cui imprese commerciali abbiano, per ragioni strutturali quali la loro veste di azionisti o soci, un'influenza tanto determinante da consentire loro di esercitare un controllo da cui potrebbe derivare un accesso preferenziale ai risultati della ricerca».

Chiaramente, una ricerca scientifica si definisce tale se rispetta il rigore metodologico, la valutazione e la selezione delle fonti, l'analisi del contesto, l'individuazione e la scelta del campione, l'interpretazione critica e non pregiudiziale dei dati e, infine ma non per importanza, la responsabilità nella comunicazione dei risultati ai portatori di interesse[108].

Questi aspetti appena menzionati, oltre a qualificare la ricerca, costituiscono regole di *soft law* che sono norme prive di efficacia

[108] L. RUFO, *Le ricerche scientifiche durante l'emergenza sanitaria (il Covid-19). Quale base giuridica per l'arruolamento dei pazienti?* In *BioLaw Journal – Rivista di Biodiritto*, 21 marzo 2020.

vincolante ma tali da condizionare anche la normativa che è di indirizzo rispetto alle attività da svolgere.

Nel dettaglio, l'eticità di una ricerca scientifica in ambito sanitario è stabilita da un principio sancito dalla Dichiarazione di Helsinki nella quale si afferma che «la ricerca medica che coinvolge soggetti umani può essere condotta solo se l'importanza degli obiettivi supera i rischi e gli oneri a carico dei soggetti»[109].

Questi obiettivi non devono solamente tradursi in benefici personali per il soggetto della ricerca, ma anche in risultati utili per la collettività, quali il miglioramento delle *best practice* sanitarie di diagnosi e di cura.

Infatti, ad oggi, uno studio per essere considerato etico deve rispettare i principi e i requisiti fondamentali del Belmont Report[110] che sono: – in ordine non gerarchico ma cronologico – «il valore scientifico e sociale, la validità scientifica, la giustizia nella selezione dei soggetti, il rapporto favorevole tra rischi e benefici, la revisione indipendente, il consenso informato, il rispetto dei soggetti».

---

[109] V. World Medical Association, Dichiarazione di Helsinki – Principi etici per ricerche etiche riguardanti gli esseri umani, 64 th WMA General Assembly, Fortaleza, Brasil, October 2013.

[110] Gli "*Ethical Principles and Guidelines for the Protections of Human Subjects of Research"* sono noti come Belmont Report che è il primo documento sulla bioetica della sperimentazione umana edito negli Stati Uniti.

Tra quelli appena menzionati, il requisito più controverso è quello relativo all'ottenimento del consenso informato da parte dei soggetti arruolati – di cui ci si occuperà nel dettaglio nei paragrafi che seguono –, dal momento che un eventuale rifiuto può comportare il restringimento del campione.

Inoltre, visto che gli studi scientifici si fondano sui dati, rilevati *ad hoc* e su base volontaria ovvero ottenuti per altro scopo, è necessario acquisire il consenso alla partecipazione alla ricerca, per consentire ai soggetti interessati «di esprimere una libera e ponderata decisione prima di sottoporsi ad uno specifico trattamento sanitario e alla diretta gestione del completo set informativo sulla loro salute»[111].

1.5.1. Diritto e ricerca clinica: dal fondamento alla "digitalizzazione" delle funzioni biologiche umane.

Il ramo del diritto che si occupa della ricerca clinica nasce con l'intento di rispondere a pratiche sperimentali gravemente lesive degli elementari diritti fondamentali delle persone[112], di fatti

---

[111] F. BRIZZI, op. cit.

[112] C. CASONATO, M. TOMASI, *Diritti e ricerca biomedica: una proposta verso nuove consonanze*, in *BioLaw Journal – Rivista di BioDiritto*, n. 1/2019, evidenziano come l'impostazione originaria della regolamentazione è ancorata a ragioni storiche e segnata da un carattere reattivo. Il codice

originariamente le sperimentazioni compromettevano la dignità umana, pertanto, si è ritenuto necessario provvedere ad una regolamentazione giuridica che tutelasse i partecipanti agli studi, introducendo delle regole rigide per i ricercatori.

In tempi più recenti, la regolamentazione giuridica della ricerca ha affrontato nuove criticità, tenuto conto del verificarsi di vicende in cui interessi economico-finanziari sono prevalsi sul bene salute, come diritto individuale e interesse della collettività[113], svuotando di significato le basi giuridiche – quali ad esempio il consenso – che costituiscono, indiscutibilmente, i capisaldi delle sperimentazioni cliniche.

È d'uopo rammentare come la ricerca scientifica sia considerata dalla Costituzione come «un bene da promuovere»[114], al quale va assicurato «un regime di libertà»[115] e all'interno di questo quadro di principi, in quanto strumentale al raggiungimento di un

---

Norimberga è stato redatto come risposta alle sperimentazioni "disumane" condotte durante il periodo nazista e il Belmont Report come reazione agli studi sulla sifilide non controllata di Tuskegee.

[113] Cfr. *ex multis*, C. CASONATO, *I farmaci tra speculazioni e logiche costituzionali*, in *Rivista AIC*, 4/2017, con riferimento ai casi Gleevec, Sofosbuvir o al contenzioso Avastin-Lucentis.

[114] Art. 9 Cost.: «La Repubblica promuove lo sviluppo della cultura e la ricerca scientifica e tecnica».

[115] Art. 33 Cost.: «L'arte e la scienza sono libere e libero ne è l'insegnamento».

superiore livello di salute individuale e collettiva, gode di particolare favore.

Ad oggi la ricerca scientifica non è più solo appannaggio dei ricercatori, ma dei partecipanti allo studio e della società nella sua interezza, vi è anche un orientamento che riconosce l'esistenza di un vero proprio «diritto alla scienza»[116] da cui consegue la necessità di vedere il campo del diritto, della scienza e dell'etica come un gomitolo di lana a tre colorazioni che però fa parte del medesimo capo.

Pertanto, fermo restando il fondamento giuridico che non deve mai essere dimenticato e la *ratio* della genesi di tale branca del diritto, è necessario garantire un'apertura e un'evoluzione nel considerare la ricerca che utilizza campioni biologici, raccolti secondo plurime modalità, e i dati, genetici e biometrici che da essi possono derivare, attraverso un procedimento di "digitalizzazione delle funzioni umane" [117].

Tale evoluzione ha generato quattro nuove caratteristiche della ricerca clinica.

---

[116] J.M. WYNDHAM, M. W. VITULLO, *Define the human right to science*, in *Science*, 30 novembre 2018, p. 975.

[117] L. MARELLI, G. TESTA, *Scrutinizing the EU General Data Protection Regulation. How will new decentralized governance impact research,* in *Science, 360 (6388)*, 2018, pp. 496-498.

In prima battuta, gli oggetti delle sperimentazioni sono sempre più complessi: da un lato vi è il vantaggio di avere a disposizione dei dati oggettivi certamente più sicuri rispetto ai dati c.d. *self-reported* ai quali si faceva riferimento in precedenza, dall'altro però la dimensione degli stessi diventa sempre più crescente (c.d. *big data*), necessitando di utilizzare nuovi approcci come le metanalisi, le tecniche di intelligenza artificiale e il *data mining*[118].
In secondo luogo, è possibile effettuare le c.d. *secondary analyses* che permettono di avvalersi di campioni già individuati o dati già archiviati per altri scopi[119], grazie alle nuove tecnologie che possono conservarli per lunghi periodi di tempo e li rendono accessibili in diversi luoghi e tempi, essendo anche supportate da ingenti investimenti finanziari.
Inoltre, la ricerca oggi non è più confinata ad un luogo fisico e opera in *network* che conducono ampie collaborazioni – spesso di

[118]Si pensi, ad esempio, ai «sequenziamenti genetici di nuova generazione che consentono di processare completamente intere sequenze di DNA in tempi molto brevi, mettendo a disposizione dei ricercatori dati estremamente accurati, ma ancora di difficile interpretazione».
[119] La possibilità di procedere in questo modo implica che, in molti casi, i futuri utilizzi di campioni o dati non siano definiti e nemmeno immaginabili al momento dell'acquisizione – si parla infatti di raccolta open-ended – generando una sfida di atavica dimensione per la base giuridica per eccellenza e cioè il consenso informato.

carattere internazionale – che determinano la necessità di individuare *standard* interoperabili[120].

L'ultimo aspetto rilevante riguarda il mantenimento di un collegamento fra i dati e il soggetto generatore, soprattutto nei casi in cui il partecipante è effettivamente il paziente in cerca di diagnosi e di cura, in tale circostanza è controproducente l'anonimizzazione delle informazioni, caposaldo del GDPR.

Dall'analisi delle caratteristiche della ricerca contemporanea emerge un'importante incidenza sugli interessi dei partecipanti da cui deriva il dubbio circa l'attualità e l'effettività degli strumenti giuridici posti tradizionalmente a salvaguardia degli stessi.

Infatti, due sono le questioni più delicate e cioè la rivalutazione dello strumento del consenso informato come archetipo della legittimazione della sperimentazione clinica e le pratiche di anonimizzazione dei dati, quale baluardo di eticità.

Con riferimento alla prima questione, dall'analisi comparata e dalla letteratura scientifica consultata[121], specie con riferimento

---

[120]L. MARELLI, G. TESTA, op. cit.

[121] Ex multis, E. S. DOVE, *Biobanks, Data Sharing and the Drive for a Global Privacy Governance Framework*, in *Journal of law, Medicine and Ethics, 43(4)*, 2015, pp. 675-689 e D. MASCALZONI et al, *International Charter of Principles for Sharing Bio-specimens and Data*, in *European Journal of Human Genetics,* 23, 2015, pp. 721-728.

alle biobanche di ricerca[122] emerge un tendenziale allontanamento dall'impostazione tradizionale del consenso, inteso come attuale e specifico e richiesto per ogni singolo studio[123] nella direzione o di un consenso presunto con eventuale diritto di opzione o dell'obbligatoria partecipazione alla ricerca quale elemento imprescindibilmente collegato alla cittadinanza oppure come condizione per godere del diritto di accesso alle cure[124]. Al di là di queste due basi giuridiche estreme, sono state indicate in dottrina[125] e nelle fonti del diritto delle figure intermedie quali l'opzione di ampliare «la manifestazione di volontà (*blanket, open* o *broad consent*)»[126] o «la sua estensione nel tempo (*dynamic*

[122]I campioni umani vengono conservati nelle biobanche che svolgono il ruolo di custodi e sono responsabili della gestione dei campioni. Tre le principali biobanche di materiale biologico di origine umana: le biobanche di ricerca, sostanzialmente deputate a conservare e fornire risorse per studi finalizzati a tutelare la salute e migliorare la qualità della vita; le biobanche terapeutiche destinate alla gestione di materiale per uso terapeutico e quelle forensi.

[123]Si parla in questi casi di *Fresh consent*.

[124]S. Y. KIM, *Clinical Trials Without Consent?* in *Perspectives in Biology and Medicine*, 2016, 59 (1), pp. 132-146.

[125]M. TOMASI, *Genetica e Costituzione. Esercizi di eguaglianza, solidarietà e responsabilità*, Forthcoming.

[126]In relazione al modello più restrittivo si possono citare: il Protocollo addizionale alla Convenzione di Oviedo sulla ricerca biomedica, che richiede «un consenso informato, libero e espresso, specifico e documentato dalla persona» (art. 14), la Raccomandazione (2006) 4 del Consiglio d'Europa, il cui art. 10 co. 2 richiede che «informazione e consenso per l'ottenimento di materiali biologici per la ricerca siano il più possibile specifici in riferimento

consent)»[127] in modo tale da includere anche dei progetti di ricerca che non siano prevedibili al momento della dazione del consenso. Con riguardo alla seconda questione, è necessario effettuare una distinzione[128] tra anonimizzazione irreversibile, intermedia[129] e reversibile mediante l'accesso ad un codice. Il bilanciamento tra l'opzione più drastica e quella meno *tranchant* non è sempre agevole.

Da un lato, l'anonimizzazione tutela il paziente da qualsivoglia rischio di utilizzo abusivo e discriminatorio dei dati genetici, dall'altro renderla definitiva è quasi irrealizzabile, specie nei casi in cui sia coinvolta la sequenza di DNA della persona, che viene qualificata come «uno dei più affidabili e potenti identificatori personali»[130]. Inoltre, dal momento che i risultati degli studi

---

a ogni scopo di ricerca previsto»; la Carta dei diritti fondamentali dell'Unione Europea, che prevede che «i dati personali debbano essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata».

[127]I. BUDIN LJØSNE, H.J.A. TEARE, J. KAYE, *Dynamic Consent: a potential solution to some of the challanges of modern biomedical research*, in *BMC Medica Ethics*, 18 (4), 2017, pp. 1-10.

[128]B. S. ELGER, A.L. CAPLAN, *Consent and anonymization in research involving biobanks: Differing terms and norms present serious barriers to an international framework*, in EMBO Reports, 7 (7), 2006, pp. 661-666.

[129]Si fa riferimento «all'eventualità in cui le informazioni personali sono separate dal dato o dal campione ma il codice di collegamento non è nella disponibilità del ricercatore».

[130]*«The most accurate individual identifier is the DNA sequence itself […]. It is clear that these available genotypes, available in tens of hundreds of*

talvolta possono dipendere anche dalla possibilità di combinare diverse tipologie di dati o dal monitoraggio della malattia, l'impossibilità di ricontattare il partecipante rende, di fatto, inutile per lo stesso e per le sue speranze di guarigione, l'aver preso parte allo studio clinico.

1.5.2. La disciplina sul trattamento dei dati personali nella ricerca scientifica: il GDPR, l'European Data Protection Board e l'European Data protection supervisor.

1.5.2.1. Il regime "speciale" della ricerca scientifica.

Dopo aver studiato il fondamento del diritto nella ricerca e la concezione moderna della stessa, è opportuno focalizzarsi sul binomio ricerca scientifica in area sanitaria e trattamento dei dati personali, alla luce dell'entrata in vigore del GDPR.

Nonostante *l'«European Data Protection Board»*[131] (EDPB) e il connesso «*European Data Protection Supervisor»* (EDPS)

---

thousands of individuals in the repository, are more accurate identifiers than demographic variables alone – the combination is an accurate and unique identifier», The American Society of Human Gentics, ASHG Response to NIH on Genome-Wide Association Studies, 2006.

[131] L'*European Data Protection Board*, previsto dal Capo VII del GDPR, è un organismo europeo indipendente che contribuisce all'applicazione coerente delle norme sulla protezione dei dati in tutta l'Unione europea e

abbiano fatto chiarezza[132] sull'esistenza di un c.d. regime speciale che si applica alla ricerca scientifica, sussistono ancora dei dubbi circa la perimetrazione del medesimo.

Tale regime speciale si applica ai principi generali del GDPR quali «la legittimità del trattamento, la limitazione delle finalità e i diritti degli interessati e tenta di trovare il giusto equilibrio tra la protezione dei dati personali dell'individuo e la libertà delle scienze e delle arti, e, nel caso della ricerca sanitaria, la tutela della salute pubblica ex art. 32 Cost»[133].

Secondo l'EDPS, «la ricerca scientifica cui si applicano tali regole speciali deve essere condotta sulla base di standard metodologici ed etici settoriali pertinenti e deve perseguire l'obiettivo di far crescere la conoscenza e il benessere collettivo della società, invece di servire principalmente uno o più interessi privati»[134].

---

promuove la cooperazione tra le autorità di controllo. L'*European Data Protection Board* ha sostituito il *Working Party*, art. 29.

[132] In particolar modo si fa riferimento a *European Data protection Board*, 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)", adottato il 23 gennaio 2019. Il parere è stato adottato dall'EDPB a seguito di una richiesta di consulenza da parte della Commissione europea a norma dell'art. 70 del GDPR con riferimento al documento "Domande e risposte sull'interazione tra il regolamento sulla sperimentazione clinica e il regolamento generale sulla protezione dei dati".

[133] M. IASELLI, *La tutela dei dati personali in ambito sanitario*, Giuffrè, 2020.

[134] EDPS, Un parere preliminare sulla protezione dei dati e la ricerca scientifica, 6 gennaio 2020, 11.

Dall'analisi del GDPR, emerge che la prima disposizione ad occuparsi di ricerca scientifica è l'art. 5, relativo ai principi applicabili al trattamento dei dati personali, che alla lettera *b*), sancisce «il principio di limitazione delle finalità che impone al Titolare di raccogliere i dati per finalità determinati e specifici e dunque, ad esempio, se vengono trattati per finalità di cura o diagnosi sanitaria, gli stessi non potranno essere contemporaneamente o successivamente utilizzati per un obiettivo diverso che non sia stato esplicitato dall'interessato»[135]. La stessa lettera *b*), nel secondo capoverso, introduce «un'eccezione per alcuni trattamenti ulteriori, tra cui la ricerca scientifica, stabilendo che un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali»[136].

Dunque, l'art cinque introduce una sorta di "presunzione di compatibilità" «con la finalità primaria manifestata al momento della raccolta, resa necessaria dalla difficoltà di individuare pienamente la finalità di ricerca scientifica al momento dell'espressione del consenso»[137].

---

[135] Art. 5, lett. B), GDPR.
[136] *Ibidem*.
[137] Considerando 33 del GDPR.

Tale apertura, però, è stata interpretata in maniera restrittiva sia dall'EDPB nel parere su citato, sia dall'EDPS nel parere del 6 gennaio 2020.

Nel parere dell'EDPB viene effettuata un'importante distinzione tra utilizzo primario e secondario dei dati: «per uso primario si intende il trattamento di dati personali sanitari per la ricerca e per la fornitura di servizi sanitari al fine di valutare, mantenere o ripristinare lo stato di salute della persona fisica a cui si riferiscono tali dati, mentre per uso secondario si intende il trattamento di dati personali sanitari per scopi diversi da quelli per i quali i dati stessi sono stati inizialmente raccolti»[138]. Tale classificazione è stata accolta anche dalla Commissione europea, che ha stabilito che «il trattamento di dati legato esclusivamente a finalità di ricerca debba considerarsi ben distinto da quello relativo agli obiettivi di protezione della salute, come la valutazione degli standard di qualità e di sicurezza dei medicinali»[139].

---

[138] Criticità etiche e normative nel trattamento dei dati personali sanitari nella ricerca osservazionale, Documento del Centro di Coordinamento Nazionale dei Comitati Etici (CCNCE). 6 aprile 2023, per la consultazione integrale https://www.aifa.gov.it/documents/20142/1808580/Criticita_etiche_ricerca_osservazionale_06.04.2023.pdf

[139]European Commission, Directorate-General for health and food safety, Question and Answers on the interplay between the Clinical Trials Regulation and the General Data Protection Regulation in cui la Commissione sostiene che «*le operazioni di trattamento puramente connesse ad attività di ricerca devono essere distinte dalle operazioni di trattamento connesse a finalità di*

Pertanto, tale clausola di compatibilità non può rappresentare, secondo le autorità europee, «un'automatica autorizzazione generale ad elaborare ulteriormente i dati per scopi scientifici»[140]. Più precisamente, il Titolare, sulla base del principio di *accountability*, dovrà valutare caso per caso se lo scopo della ricerca scientifica sia effettivamente compatibile con l'uso primario dei dati, secondo le indicazioni contenute nel Considerando 50 del GDPR.

Un ulteriore strumento utile è il parere 03/2013[141] adottato dal Gruppo di Lavoro art. 29, secondo il quale i fattori che devono essere presi in considerazione al fine di valutare correttamente la sussistenza della compatibilità sono «la relazione tra finalità primaria e ulteriore, il contesto nel quale i dati sono stati raccolti e le ragionevoli aspettative degli interessati, la natura dei dati e il potenziale impatto sui diritti degli interessati generato dal riutilizzo dei dati, le misure di sicurezza implementate al fine di mitigare l'impatto»[142] e se, la finalità sia considerata compatibile,

---

tutela della salute, stabilendo al contempo standard di qualità e sicurezza per i medicinali mediante la generazione di dati affidabili e solidi (finalità legate all'affidabilità e alla sicurezza); queste due principali categorie di attività di trattamento rientrano in basi giuridiche diverse».

[140] Tale affermazione si desume dalle faq citate.

[141] Articolo 29 Data protection Working Party, Opinion 03/2013 on purpose limitatio, adottato il 21 aprile 2013.

[142] Per la consultazione integrale, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_it.pdf

alla luce del citato Considerando 50 non è necessario prevedere una base giuridica ultronea.

Infine, nell'eventualità in cui, la finalità di ricerca dovesse essere considerata compatibile, sarà necessario rispettare il principio di minimizzazione previsto dall'art. 89 del GDPR.

Pertanto, in mancanza di una differente base giuridica, stante l'esistenza di una compatibilità di finalità, sarà necessario minimizzare i dati, per poterli utilizzare in maniera ultronea rispetto all'esigenza primaria.

1.5.2.2. La base giuridica alla luce del GDPR.

Nel paragrafo precedente si è parlato di base giuridica necessaria per ammettere il trattamento dei dati sanitari e per comprenderne l'oggetto è necessario individuare preliminarmente le finalità prefigurata che si è resa trasparente tramite l'informativa.

Nello specifico, ai sensi dell'art. 6 GDPR le basi giuridiche del trattamento per la ricerca scientifica possono essere: «il

consenso»[143], «l'obbligo di legge»[144], «l'interesse pubblico»[145], nonché il «legittimo interesse del Titolare»[146] che non soltanto sarà tenuto a dimostrarlo ma anche a bilanciarlo con gli altri interessi e diritti coinvolti in potenza del soggetto interessato, secondo quanto previsto nel Parere WP29 6/2014 relativo al legittimo interesse[147].

Nell'eventualità in cui, nell'ambito della ricerca scientifica si trattino particolari categorie di dati – quali quelli sanitari – le basi giuridiche appena indicate dovranno allinearsi con quelle più specifiche indicate nell'art. 9, par. 2, GDPR.

Più precisamente, la lettera *a*) fa riferimento al consenso dell'interessato; la lettera *g*)[148] prevede che «il trattamento dei

---

[143] «Art. 6, par. 1, lett. a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità».

[144] «Art. 6, par. 1, lett. c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento».

[145] «Art. 6, par. 1, lett. e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento».

[146] «Art. 6, par. 1, lett. f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore».

[147] «Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE adottata il 9 aprile 2014».

[148] «Art. 9, par. 2, lett. g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che

dati personali sia giustificato dalla presenza di un interesse pubblico rilevante»[149]; la lettera *h*) [150], considera legittimo il trattamento di dati personali particolari laddove sia svolto nell'ambito della sanità pubblica in virtù di un interesse pubblico, che può essere, ad esempio, la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici e infine, la lettera *j*), prevede la legittimità del trattamento nell'eventualità in cui sia finalizzato ad effettuare attività di ricerca scientifica, in conformità a quanto previsto dall'art. 89 del GDPR, sulla base del diritto UE o nazionale.

1.5.3. La disciplina del Codice privacy – novellato ai sensi del d. lgs. n. 101/2018 – in materia di ricerca scientifica.

Dopo aver fatto riferimento alla disciplina prevista in materia dal GDPR, si ritiene necessario procedere all'analisi di alcune

---

deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato» (C55, C56).

[149]Per l'identificazione dell'interesse pubblico rilevante, si ritiene utile fare riferimento al Considerando 52 del GDPR, a cui si rinvia,

[150]«Art. 9, part. 2, lett. h), il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3».

previsioni specifiche introdotte dal legislatore italiano con il d. lgs. n. 101 del 2018 che ha rimodulato il Codice della Privacy, in materia di ricerca scientifica.

In prima battuta, si fa riferimento all'art. 2-*sexies*, rubricato "Trattamento di categorie particolari di dati personali necessario per motivi di interesse pubblico rilevante" che individua le ipotesi in cui al trattamento di dati particolari si applica l'art. 9, par. 2, lett. *g*) in tema di interesse pubblico rilevante, annoverando anche «trattamenti effettuati a fini di archiviazione nel pubblico interesse o di ricerca storica, concernenti la conservazione, l'ordinamento e la comunicazione dei documenti detenuti negli archivi di Stato negli archivi storici degli enti pubblici, o in archivi privati dichiarati di interesse storico particolarmente importante, per fini di ricerca scientifica, nonché per fini statistici da parte di soggetti che fanno parte del sistema statistico nazionale (Sistan)», da ciò deriva che la ricerca scientifica trova la sua condizione legittimante nell'interesse pubblico rilevante.

Secondariamente, è d'uopo citare l'art. 78, il quale prevede che «l'informativa privacy fornita dal medico di medicina generale (MMG) o dal pediatra di libera scelta (PLS) evidenzi, in maniera analitica, eventuali trattamenti di dati personali che presentano rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, con particolare riguardo ai trattamenti

effettuati per fini di ricerca scientifica anche nell'ambito delle sperimentazioni cliniche, sottolineando che il consenso, ove richiesto, sia manifestato liberamente»[151].

Infine, è d'interesse analizzare il Titolo VII, Capo III, con specifico riferimento agli artt. 99, 107, 110 e 110-*bis* del Codice.

L'articolo 99, in primo luogo, disciplina «la durata del trattamento ai fini di ricerca scientifica», prevedendo che «lo stesso possa essere effettuato anche oltre il periodo di tempo necessario per conseguire scopi diversi e ulteriori rispetto a quelli per i quali sono stati in precedenza raccolti o trattati»[152].

Per quel che concerne le basi giuridiche, l'art. 107 , rubricato «Trattamento di categorie particolari di dati personali», prevede che stante quanto previsto dall'articolo 2-*sexies* e al di là di particolari indagini a fini statistici o di ricerca scientifica previste dalla legge, «il consenso dell'interessato al trattamento di dati di cui all'articolo 9 del Regolamento, quando è richiesto, può essere prestato con modalità semplificate, individuate dalle regole deontologiche di cui all'articolo 106 o dalle misure di cui all'articolo 2-*septies*»[153].

---

[151] Art. 78 del novellato Codice della Privacy.
[152] Art. 99 del novellato Codice della privacy.
[153] Art. 107 del novellato Codice della privacy.

La norma, quindi, prevede che «nelle ipotesi in cui si sia valutato che la condizione legittimante della ricerca scientifica sia il consenso, questo potrà essere prestato attraverso delle misure semplificate individuate da regole deontologiche oppure misure di garanzia, entrambe individuate dal Garante tramite provvedimento»[154].

Se quanto previsto dall'art. 107 è abbastanza pacifico, i successivi artt. 110 e 110-*bis* sono di meno facile comprensione.

L'art. 110, rubricato «Ricerca medica, biomedica ed epidemiologia» prevede delle ipotesi in cui il consenso dell'interessato non sia necessario e cioè nell'eventualità in cui «la ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea in conformità all'articolo 9, paragrafo 2, lettera j), del Regolamento, ivi incluso il caso in cui la ricerca rientra in un programma di ricerca biomedica o sanitaria previsto ai sensi dell'articolo 12-*bis* del decreto legislativo 30 dicembre 1992, n. 502, ed è condotta e resa pubblica una valutazione d'impatto ai sensi degli articoli 35 e 36 del Regolamento». Ovvero quando per peculiari circostanze, «informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di

[154] Ivi.

pregiudicare gravemente il conseguimento delle finalità della ricerca». In tutte queste ipotesi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, e inoltre lo studio sarà «oggetto di motivato parere favorevole del competente comitato etico a livello territoriale e deve essere sottoposto a preventiva consultazione del Garante ai sensi dell'articolo 36 del Regolamento»[155].

Innanzitutto è rilevante delimitare l'ambito di applicazione, dal momento che all'interno del GDPR si è sempre fatto riferimento al concetto di ricerca scientifica e dunque ci si è domandati se quella contenuta nell'art. 110 fosse una sineddoche e quindi con "ricerca scientifica" si intendesse la più ampia area di scoperta e analisi, mentre con le locuzioni "ricerca medica" e "biomedica", ci si potrebbe riferire al sottoinsieme delle ricerche inerenti all'area più clinica (ad esempio farmacologica o di *medical device*), facendo riferimento al temine "ricerca epidemiologica" quando si guarda alla frequenza delle malattie[156].

L'interpretazione appena indicata è ulteriormente avvalorata dal «Provvedimento del 5 giugno 2019 del Garante della Privacy recante le prescrizioni relative al trattamento di categorie

[155] Art. 110 del novellato Codice della Privacy.
[156] M. IASELLI, op. cit.

particolari di dati, ai sensi dell'art. 21, comma 1, del d. lgs n. 101 del 10 agosto del 2018»[157].

Tale provvedimento pur riferendosi in generale alla ricerca scientifica, in verità sembra richiamare i casi previsti dall'art. 110 essendo stabilito che trova applicazione in tutte quelle ipotesi in cui a causa delle condizioni dei soggetti, non sia possibile fornire liberamente il consenso all'utilizzo dei dati per finalità di ricerca, complessivamente intesi[158].

Da un lato il Garante richiama "solo" la ricerca medica, biomedica ed epidemiologica e dall'altro il riferimento agli "studi" effettuati delimita l'ambito di applicazione alle sole ricerche che coinvolgono gli esseri umani.

Inoltre, con riferimento alla base giuridica richiesta per tale tipo di studi, il legislatore italiano ha ricollocato il consenso al vertice, individuando delle mere eccezioni a tale centralità.

Infatti, si fa riferimento sia al caso in cui il trattamento avvenga sulla base di disposizioni di leggi europee o nazionali – richiamando quanto previsto dall'art. 9, par. 2, lett. *j*) del GDPR – sia all'eventualità in cui informare gli interessati risulti

---

[157] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9124510

[158] «Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101», Garante della Privacy, [doc. web. n. 9124510].

impossibile o implichi uno sforzo sproporzionato tale da pregiudicare il risultato complessivo della ricerca – e in tale caso il trattamento può essere considerato lecito previa richiesta e ottenimento di un parere motivato da parte del Comitato Etico ovvero una valutazione d'impatto ex art. 35 GDPR ovvero un parere preventivo al Garante ex art. 36 GDPR.

Infine, l'art. 110 *bis* del Codice della Privacy introduce una disciplina *ad hoc* per il trattamento ulteriore dei dati da parte di un soggetto terzo.

Tale norma sembra abbracciare la nozione più ampia di ricerca scientifica e prevede che, nell'eventualità in cui risulti impossibile o implichi uno sforzo sproporzionato o rischi di pregiudicare la ricerca informare gli interessati, sia prevista l'obbligatorietà di un'autorizzazione da parte del Garante[159] per effettuare il trattamento.

Per completezza, è rilevante richiamare il comma 4 della suddetta previsione nella misura in cui specifica che «Non costituisce trattamento ulteriore da parte di terzi il trattamento dei dati personali raccolti per l'attività clinica, a fini di ricerca, da parte degli Istituti di ricovero e cura a carattere scientifico, pubblici e privati, in ragione del carattere strumentale dell'attività di

[159] Si tratta di una discrasia giuridica, dal momento che tale istituto non è più in vigore.

assistenza sanitaria svolta dai predetti istituti rispetto alla ricerca, nell'osservanza di quanto previsto dall'articolo 89 del Regolamento»[160].

1.5.4. La ricerca nell'ambito farmaceutico e delle sperimentazioni cliniche.

All'interno della ricerca scientifica effettuata in ambito sanitario, questo lavoro si occuperà degli istituti giuridici peculiari del settore farmaceutico.

In prima battuta si fa riferimento agli studi clinici, che, ai sensi del Regolamento 2014/536 (CTR), sono definiti come «qualsiasi indagine effettuata in relazione a soggetti umani volta a: a) scoprire o verificare gli effetti clinici, farmacologici o altri effetti farmacodinamici di uno o più medicinali; b) identificare eventuali reazioni avverse di uno o più medicinali; oppure c) studiare l'assorbimento, la distribuzione, il metabolismo e l'eliminazione di uno o più medicinali, al fine di accertare la sicurezza e/o l'efficacia di tali medicinali»[161], per cui si tratta di studi che si concretizzano in indagini sull'uomo in relazione ad un farmaco secondo l'AIC[162]

[160] Art. 110-bis del novellato Codice della Privacy, comma 4.
[161] Art. 2, paragrafo 2, punto 1) CTR.
[162] Autorizzazione all'immissione in commercio.

in cui la sottoposizione di un paziente ad una strategia terapeutica non è in alcun modo influenzata dall'inclusione del medesimo all'interno di uno studio[163].

In secondo luogo, vi è la sperimentazione clinica ed è una sottocategoria delle ricerche suddette ed è uno studio clinico che soddisfa una delle seguenti condizioni: «a) l'assegnazione del soggetto a una determinata strategia terapeutica è decisa anticipatamente e non rientra nella normale pratica clinica dello Stato membro interessato; b) la decisione di prescrivere i medicinali sperimentali e la decisione di includere il soggetto nello studio clinico sono prese nello stesso momento; o c) sono applicate ai soggetti procedure diagnostiche o di monitoraggio aggiuntive rispetto alla normale pratica clinica»[164]. In questo secondo caso si tratta di uno studio clinico svolto sull'uomo finalizzato a scoprire o verificare gli effetti clinici, farmacologici e farmacodinamici di uno o più medicinali sperimentali, o ad individuare reazioni avverse o a studiarne l'assorbimento, la distribuzione, il metabolismo e l'eliminazione, con l'obiettivo di accertarne la

[163] Art. 2, par. 1, lett. c) del d. lgs. n. 211 del 24 giugno 2003; art. 1, par. 1, lett. p) del d. lgs. n. 200 del 6 novembre 2007, Determinazione AIFA del 20 marzo 2008 – Linee guida per la classificazione e conduzione degli studi osservazionali sui farmaci; Circolare del Ministero della Salute n. 6 del 2 settembre 2008.

[164] Art. 2, par. 2, punto 2, CTR.

sicurezza e/o l'efficacia[165], in tale ipotesi sarà lo sperimentatore a individuare il fattore da studiare.

Infine, la farmacovigilanza è definita come lo «studio sulla sicurezza dei medicinali dopo l'autorizzazione: lo studio farmaco-epidemiologico o la sperimentazione clinica effettuati conformemente alle condizioni stabilite all'atto dell'autorizzazione all'immissione in commercio allo scopo di identificare o quantificare un rischio per la sicurezza, correlato ad un medicinale per il quale è già stata rilasciata un'autorizzazione»[166].

1.5.4.1. La base giuridica ai sensi del GDPR.

Nel paragrafo precedente si è fatto riferimento alle definizioni contenute nel CTR – *Clinical Trials Regulation* che aveva avuto come obiettivo quello di uniformare tutte le procedure connesse alle sperimentazioni cliniche di medicinali ad uso umano nell'Unione Europea, cercando di ridurre al minimo la burocrazia secondo un approccio basato sul rischio.

---

[165] Art. 2, par. 1, lett. a) del d.lgs. n. 211 del 24 giugno 2003 3 art. 1, par. 1, lett. o del d. lgs. n. 200 del 6 novembre 2007.

[166] Art. 1, comma 1, lett. p) del d.lgs. n. 219 del 24 aprile 2006 così come modificato dal d.lgs. n. 42 del 4 marzo 2014.

Sebbene il CTR sia datato 2014, è stato necessario attendere il 31 gennaio 2022 per la sua generale applicazione in quanto solo nel luglio del 2021 è stato rimosso l'ultimo ostacolo alla sua applicazione e cioè la piena funzionalità del *Clinical Trial Information System*, il nuovo portale che, insieme alla banca dati UE, diventerà «l'unico punto di accesso per la presentazione dei dati e delle informazioni concernenti le sperimentazioni cliniche»[167].

Secondo il ventesimo Rapporto Nazionale – Anno 2023, pubblicato dall'AIFA – Agenzia Italiana del Farmaco, «il triennio 2020-2022, può essere considerato un periodo straordinario per le sperimentazioni cliniche, in quanto caratterizzato da due eventi eccezionali, emersi quasi contemporaneamente: uno di portata mondiale, la pandemia da COVID-19, e l'altro di portata solo europea, l'applicazione del Regolamento (UE) 536/2014. La parziale coincidenza temporale dei due eventi ha amplificato l'impatto di entrambi, integrandone gli effetti e le conseguenti influenze sulle sperimentazioni cliniche, accelerando e condizionando forse anche il cambio di paradigma».

Si ritiene necessario approfondire, in questa sede, il rapporto intercorrente tra il CTR e il GDPR, essendo il primo entrato in

[167] Artt. 80-82 CTR.

vigore soltanto nel 2022, sebbene sia stato predisposto nel 2014. Infatti, il Considerando n. 1 del CTR enuncia che «in una sperimentazione clinica si dovrebbero tutelare i diritti, la sicurezza, la dignità e il benessere dei soggetti nonché produrre dati affidabili e robusti. Gli interessi dei soggetti dovrebbero sempre essere prioritari rispetto a tutti gli altri interessi», mentre il Considerando n. 76 rafforza ulteriormente la tutela dei diritti fondamentali all'interno degli studi.

L'art. 28, par. 1, lett. *d*) del CTR, prevede che «La conduzione di una sperimentazione clinica è consentita esclusivamente se tutte le seguenti condizioni sono soddisfatte: […] sono rispettati il diritto all'integrità fisica e mentale dei soggetti, il diritto alla vita privata e alla protezione dei dati che li riguardano in conformità della direttiva 95/46/CE»[168].

Dunque, il rapporto intercorrente tra CTR e GDPR non è stato sottovalutato, in quanto in più occasioni si fa, vicendevolmente, riferimento al rispetto della normativa a tutela dei dati personali durante le sperimentazioni cliniche.

È fondamentale valutare però su quali basi giuridiche si verificherà il trattamento dei dati personali raccolti durante la conduzione

[168] Leggasi GDPR: il CTR è nato nel 2014, quando era ancora in vigore la Direttiva Privacy, abrogata nel 2016 dal GDPR.

dello studio e quali siano le finalità per le quali tali dati vengono raccolti e trattati.

In prima battuta si fa riferimento all'esecuzione di tutti quegli adempimenti necessari a svolgere una valutazione della sicurezza e dell'affidabilità dei dati raccolti nell'ambito della sperimentazione clinica[169] e cioè si fa riferimento a quei dati che documentano eventi avversi o anomali, come comunicati dallo sperimentatore al promotore e, successivamente, oggetto della relazione cui quest'ultimo è tenuto annualmente nei confronti dell'EMA[170].

In tale circostanza la base giuridica di riferimento è quella prevista dall'art. 6 comma 1, lett. *c*) GDPR, dal momento che «il trattamento dei dati è necessario a adempiere un obbligo legale al quale è soggetto il titolare del trattamento»[171].

Con riferimento specifico ai dati particolari, la condizione di liceità è ravvisabile nell'art. 9, comma 2, lett. *i*) del GDPR in base al quale «il trattamento è necessario per fornire la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali ovvero nell'art. 9, comma 2, lett. *j*) del GDPR

[169] Combinato disposto degli articoli 41 e 43 del CTR.
[170] Agenzia europea per i medicinali.
[171] Art. 6 comma 1, lett. c) del GDPR.

secondo cui il trattamento è autorizzato per fini di archiviazione di pubblico interesse e di ricerca scientifica»[172].

In seconda battuta si fa riferimento all'utilizzo di dati per generici scopi di ricerca.

La questione è particolarmente complessa e ha investito più volte il Comitato Europeo per la protezione dei dati che con l'Opinion 3/2019[173] ha chiarito che per la finalità di ricerca scientifica è possibile utilizzare in alternativa: «il consenso esplicito dell'interessato»[174], «l'esecuzione di un compito di interesse pubblico»[175] ovvero «l'interesse legittimo del Titolare del trattamento»[176].

Il Comitato effettua un'importante distinzione in merito ai due tipi di consensi presenti in materia di trial clinici: il consenso informato alla sperimentazione clinica del CTR e il consenso (esplicito) al trattamento dei dati personali in ambito GDPR.

---

[172] Art. 9, comma 2, lett. I) del GDPR.

[173] Per la consultazione integrale vedasi https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-32019-concerning-questions-and-answers_it

[174] «Art. 6, comma 1, lett. a) GDPR congiuntamente all'art. 9, comma 2, lett. a) GDPR».

[175] «Art. 6, comma 1, lett. e) GDPR».

[176] «Art. 6, comma 1, lett. f) GDPR congiuntamente all'art. 9, comma 2, lett. i) o j) GDPR».

Il Capo V del CTR specifica i requisiti previsti per il consenso informato alla sperimentazione clinica, richiamando quanto previsto dalla Dichiarazione di Helsinki, affermando che «la base giuridica assicura la protezione del diritto alla dignità e all'integrità della persona e non riguarda la disciplina della protezione dei dati personali dell'individuo»[177].

Il consenso al trattamento dei dati personali deve, invece, essere libero, specifico, informato e inequivocabile nonché esplicito, per il trattamento dei dati particolari.

Il nodo cruciale, particolarmente discusso in dottrina, è quello relativo all'aggettivo "libero", in quanto è necessario garantire che l'interessato abbia una reale libertà di scelta, nonché una reale capacità di controllo sulle sue scelte[178].

La difficoltà si rinviene, innanzitutto, nella asimmetria tra promotore e interessato che si traduce in situazioni in cui il soggetto si trovi in condizioni economiche/sociali svantaggiate ovvero non sia nella pienezza delle sue capacità.

Per tale motivo, il Comitato nell'*Opinion* citata ha previsto due alternative alla c.d. centralità del consenso e cioè con riferimento all'art. 6, comma 1, lett. *e*) del GDPR, il trattamento dei dati personali nel novero delle sperimentazioni cliniche può essere

---

[177] https://www.evidence.it/articoli/pdf/e1000059.pdf

[178] F. BRIZZI, op. cit.

considerato necessario per l'esecuzione di un compito di interesse pubblico quando l'esecuzione delle sperimentazioni cliniche rientri direttamente nel mandato, nelle *mission* e nei compiti che il diritto nazionale conferisce ad un organismo pubblico o privato ovvero con riferimento all'art. 6, comma1, lett. *f*) del GDPR[179].

Tuttavia, con specifico riguardo all'utilizzo secondario di cui all'articolo 28 comma 2 del CTR, il Comitato sottolinea che per quel che concerne l'utilizzo di dati personali "al di fuori del campo di applicazione del protocollo", è necessario che il promotore richieda il consenso specifico all'interessato.

In ogni caso, per un utilizzo ulteriore dei dati è necessaria una differente base giuridica ma questo approccio esclude l'applicabilità della cosiddetta "presunzione di compatibilità" di cui all'articolo 5.1. lett. *b*) del GDPR secondo cui i dati ulteriormente trattati per la ricerca scientifica non sono considerati a priori incompatibili con la finalità iniziale, a condizione che ciò avvenga conformemente alle disposizioni dell'articolo 89 del GDPR che prevede che, in determinate condizioni, il Titolare del trattamento possa maneggiare ulteriormente i dati senza avere un'ulteriore base giuridica.

---

[179] Secondo l'art. 6, comma 1, lett. f del GDPR: «Il trattamento dei dati può essere considerato necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato».

1.5.4.2. L'impatto del Covid 19 sulla ricerca scientifica.

1.5.4.2.1. Linee guida 03/2020 dell'EDPB.

Il 21 aprile 2020 *l'European Data Protection Board* (EDPB) ha adottato un documento avente ad oggetto «le linee guida sul trattamento dei dati relativi alla salute a fini ricerca nel contesto dell'epidemia da COVID-19» per far luce su talune questioni giuridiche particolarmente urgenti, riguardanti l'uso dei dati relativi alla salute per finalità di ricerca scientifica quali «la base giuridica del trattamento, la possibilità di ulteriore trattamento, l'attuazione di adeguate misure di salvaguardia e l'esercizio dei diritti degli interessati».[180]

In prima battuta è necessario sottolineare la centralità del GDPR, sia come faro della corretta gestione del trattamento dei dati personali anche per le finalità di ricerca scientifica connesse alla pandemia e alle conseguenti necessarie tutele dei diritti fondamentali degli individui, sia come strumento che incentiva la ricerca scientifica prevedendo un'esplicita eccezione al divieto di trattamento di categorie particolari di dati, come detto in precedenza, per sostenere l'elaborazione giuridica dei dati che

[180] F. BRIZZI, op. cit.

hanno consentito la realizzazione dei vaccini o l'utilizzo degli anticorpi monoclonali per la cura dell'infezione da COVID-19.

L'EDPB individua, quali basi giuridiche per il trattamento dei dati relativi alla salute nel contesto pandemico, il consenso e l'interesse pubblico.

Con riferimento alla prima condizione di legittimità, il Comitato richiama il citato parere 3/2019, sottolineando «che il consenso deve essere libero, specifico, informato, non ambiguo e manifestato attraverso una dichiarazione o azione positiva inequivocabile del soggetto interessato, raccolto ai sensi del combinato disposto degli artt. 6, comma 1, lett. *a*) e 9, comma 2, lett. *a*) del GDPR»[181].

L'EDPB sottolinea che nel caso di un consenso prestato all'interno di uno studio non interventistico che sia finalizzato alla ricerca di sintomi e a studiare l'evoluzione di una malattia di cui non si hanno evidenze scientifiche – come nel caso del Covid – non si realizza il paventato "evidente squilibrio di potere" tra promotore e interessato tale da indurre un vizio nel consenso, ma deve essere garantito, in ogni caso, ai soggetti il diritto di revocare in qualsiasi momento tale manifestazione di volontà.

[181] Parere 3/2019 dell'EPDB.

Nell'eventualità in cui sia esercitata la revoca, tutte le precedenti operazioni di trattamento rimangono legittime ma il Titolare dovrà interrompere le nuove attività e, in assenza di ulteriori basi giuridiche per la conservazione di un ulteriore trattamento, i dati dovranno essere cancellati.

Con riguardo invece, alla seconda condizione di legittimità, «i dati personali relativi alla salute possono alternativamente essere utilizzati per finalità di ricerca scientifica, pur in assenza del consenso dei soggetti interessati, nell'eventualità in cui ci siano specifiche leggi emanate dal legislatore europeo o di uno Stato membro, nel caso in cui il trattamento sia necessario per motivi di interesse pubblico nel settore della sanità pubblica – quali la protezione da gravi minacce per la salute a carattere transfrontaliero – con la previsione di misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, nel dettaglio con riguardo al segreto professionale[182] ovvero ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità all'art. 89, paragrafo 1, GDPR»[183].

In ogni caso l'Opinion dell'EDPB sottolinea che deve essere rispettato «il principio di proporzionalità rispetto alla finalità perseguita, l'essenza del diritto alla protezione dei dati con

[182] Ai sensi dell'art. 9, paragrafo 2, lett. i) del GDPR.
[183] Parere 3/2019 dell'EPDB, cit.

previsione di misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato. Tali basi giuridiche possono, dunque, essere utilizzate per trattare dati relativi alla salute nell'ambito di studi basati su una vasta popolazione, condotti sulle cartelle cliniche dei pazienti COVID-19»[184].

Visto che l'attività di ricerca scientifica comporta il processare una notevole quantità di dati sanitari, l'EDPB ha ritenuto assolutamente necessario sottolineare il rispetto dei principi fondamentali in materia di trattamento e nel dettaglio sono stati previsti: obblighi di trasparenza e informativa nei confronti dei soggetti interessati[185]; limitazione di finalità e presunzione di compatibilità[186]; minimizzazione dei dati e limitazione della

[184]«Linee-guida 03/2020 sul trattamento dei dati relativi alla salute a fini di ricerca scientifica nel contesto dell'emergenza legata al COVID-19», disponibili al https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032020-processing-data-concerning-health-purpose_it

[185] L'EDPB ha sottolineato nelle linee guida citate «la centralità dell'art. 14 del GDPR rispetto ai trattamenti con finalità di ricerca scientifica, dal momento che i dati vengono spesso raccolti non direttamente presso il soggetto interessato ma tramite canali diversi come le cartelle cliniche, chiarendo che il requisito di cui all'art. 89, comma 1, del GDPR può essere soddisfatto fornendo all'interessato l'informativa entro un periodo di tempo ragionevole prima dell'avvio del nuovo progetto di ricerca».

[186] L'EDPB, nel ricordare che «l'ulteriore trattamento dei dati personali a fini di ricerca scientifica non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali, evidenzia che, data la complessità della questione, essa sarà esaminata nel dettaglio nelle apposite

conservazione nella ricerca scientifica[187]; integrità e riservatezza[188]; esercizio dei diritti degli interessati[189]; trasferimenti internazionali di dati a fini di ricerca scientifica[190].

1.5.4.2.2. I provvedimenti dell'Autorità Garante della Privacy.

Sulla scia delle linee guida elaborate dall'EDPB durante la pandemia, in Italia il Garante per la protezione dei dati personali ha chiarito che «i centri di sperimentazione possono trattare dati personali, anche relativi alla salute dei pazienti affetti da COVID-19, per sperimentazioni cliniche dei medicinali – come gli studi

---

linee guida che saranno adottate dallo stesso Ente in materia di trattamento dei dati relativi alla salute ai fini della ricerca scientifica».

[187] Secondo l'EDPB «i dati devono essere resi anonimi ogni volta in cui la ricerca scientifica possa essere condotta con tali modalità e devono essere previsti termini di conservazione che siano proporzionati».

[188] Tenuto conto del periodo pandemico e dalla circolazione massiva dei dati, l'EDPB suggerisce l'adozione di ulteriori forme di sicurezza consistenti nella pseudonimizzazione, cifratura, non disclosure agreements, restrizioni e distribuzione dei ruoli di accesso. Particolare importanza viene assegnata ai DPO che dovrebbero essere consultati dai titolari in merito al trattamento dei dati relativi alla salute per finalità di ricerca scientifica nel contesto dell'epidemia COVID-19.

[189] In linea di principio la pandemia non ha comportato una restrizione o limitazione di questo tipo di diritti e qualora lo abbia fatto, essa è avvenuta nella misura strettamente necessaria.

[190] Nell'ambito della pandemia è sorta l'esigenza di instaurare una solida cooperazione internazionale con conseguente circolazione dei dati relativi alla salute ai fini di ricerca scientifica al di là dello Spazio Economico Europeo.

clinici sperimentati sui medicinali di fase I, II, III, e IV, gli studi osservazionali sui farmaci e i programmi di uso terapeutico compassionevole – in maniera strettamente necessaria per il contrasto della pandemia, sulla base delle condizioni legittimanti previste dal GDPR»[191].

Viene inoltre chiarito che, nell'eventualità in cui non sia possibile rilevare la base giuridica legittimante in capo all'interessato, «i titolari saranno tenuti a raccogliere la condizione legittimante, previa esibizione di idonea informativa, presso chi esercita legalmente la potestà di questi ultimi, da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato»[192].

Se, invece, non sia possibile acquisire la base giuridica neppure nelle modalità precedentemente previste e questo possa comportare un nocumento nella ricerca, «i titolari che intendano svolgere trattamenti di dati che riguardano studi sperimentali[193] e

[191] FAQ - Trattamento dati nel contesto delle sperimentazioni cliniche e delle ricerche mediche nell'ambito dell'emergenza sanitaria da covid-19.

[192] Cfr. punto 4.11.2 delle «Prescrizioni relative al trattamento dei dati genetici, allegato 4 al provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati», [doc. web n. 9124510].

[193] Gli studi sperimentali, in particolar modo gli studi randomizzati controllati (RCT), rappresentano il gold standard nella valutazione di efficacia di un intervento sanitario preventivo, terapeutico o riabilitativo. Si tratta di sperimentazioni pianificate, disegnate e condotte su un gruppo specifico di

usi compassionevoli dei medicinali per uso umano[194], per la cura e la prevenzione del virus, non sono obbligati, nella fase emergenziale, alla preventiva sottoposizione del progetto di ricerca, alla valutazione di impatto e alla consultazione preventiva del Garante di cui all'art. 110 del Codice in materia di protezione dei dati personali»[195].

Con specifico riferimento alle «ricerche mediche relative al Covid-19 finanziate dal Ministero della salute sulla base del bando adottato il 1 aprile 2020 per invitare gli Istituti di ricovero e cura a carattere scientifico (IRCSS) a presentare progetti di ricerca medica finalizzati a migliorare la comprensione dell'epidemia da COVID»[196], il Garante ha chiarito che «i trattamenti di dati personali anche relativi alla salute svolti dagli IRCCS beneficiari dei predetti fondi, nell'ambito delle ricerche finalizzate al contrasto della pandemia, possono essere svolti senza il consenso

---

pazienti, allo scopo di definire il miglior trattamento possibile per gli individui affetti da una specifica patologia o condizione.

[194] L'uso compassionevole, noto anche come accesso ampliato, è l'uso terapeutico di farmaci sperimentali al di fuori degli studi clinici. Secondo la definizione dell'Agenzia Europea per i Medicinali (EMA), è "un'opzione di trattamento che consente l'uso di un medicinale non autorizzato in fase di sviluppo"

[195] V. LEMMA, *COVID-19: il trattamento dei dati sanitari tra privacy e interesse pubblico*, in www.osservatoriomalattierare.it.

[196] XVIII LEGISLATURA— DISEGNI DI LEGGE E RELAZIONI— DOCUMENTI— DOC. CXXXVI N. 3.

degli interessati, in quanto ineriscono alle funzioni di rilevante interesse pubblico attribuite, tra gli altri, anche ai soggetti del Servizio sanitario nazionale. I già menzionati IRCSS che trattano dati personali nell'ambito delle ricerche mediche finanziate dal Ministero non devono, pertanto, effettuare gli adempimenti previsti dall'art. 110 del Codice»[197].

Per quel che riguarda gli studi osservazionali[198], da un'interpretazione letterale delle FAQ del Garante della privacy emerge che nell'oggettiva impossibilità di ottenere idonea base giuridica, i promotori di uno studio dovranno «sottoporre il proprio progetto e la valutazione d'impatto ad una consultazione preventiva del Garante», se si trattasse di studio interventistico, ne sarebbero esentati[199].

Una tale diversificazione di regime giuridico non sarebbe molto ragionevole[200], dal momento che gli studi che sono meno invasivi

---

[197]Vedasi altresì art. 14 d.l. 9 marzo 2020, n. 14 e art. 17 d.l. n. 18 del 17 marzo 2020 e le Prescrizioni relative al trattamento dei dati genetici, allegato 4 al provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati-Faq Garante della Privacy.

[198] Lo studio osservazionale è un esempio di studio scientifico descrittivo o analitico in cui il team di ricercatori si limita a osservare i fenomeni, senza intervenire in maniera diretta su di essi.

[199] Faq del Garante della Privacy cit.

[200]https://www.iss.it/documents/20126/0/Rapporto+ISS+COVID-19+42_2020+%281%29.pdf/7fbd7a22-ba86-e323-1ff8-ebe2d4ae5da9?t=1608041817126

della sfera personale – e cioè gli studi osservazionali – subirebbero un trattamento deteriore rispetto agli studi che presentano rischi diretti per la persona umana; pertanto, si dovrebbe abbracciare una definizione più ampia della nozione di "studio sperimentale".

Inoltre, tra le ipotesi di impossibilità di acquisizione del consenso informato rientra, secondo le indicazioni del Garante, l'eventualità in cui la ricerca coinvolga il trattamento di "dati relativi a pazienti defunti", pertanto è chiaro che si faccia riferimento ad un'accezione estesa del sintagma "studi sperimentali", non essendo possibile condurre uno studio interventistico su un defunto.

1.5.4.2.3. Il ruolo dell'Agenzia Italiana del Farmaco (AIFA).

Innanzitutto, l'articolo 40 del decreto-legge n. 23 dell'8 aprile 2020 ha previsto che, limitatamente al periodo dello stato di emergenza, «al fine di migliorare la capacità di coordinamento e di analisi delle evidenze scientifiche disponibili sui medicinali, l'AIFA (Agenzia Italiana del Farmaco) può accedere a tutti i dati degli studi clinici sperimentali, osservazionali e dei programmi di

uso terapeutico compassionevole, per pazienti con COVID-19»[201].

I protocolli degli studi osservazionali sui medicinali sono preliminarmente valutati dalla Commissione tecnico scientifica (CTS) dell'AIFA e successivamente gli esiti verranno comunicati al Comitato tecnico scientifico dell'Unità di crisi.

Inoltre, sia nell'autorizzazione all'immissione in commercio dei quattro vaccini che hanno costituito oggetto della profilassi di massa durante il periodo pandemico, sia nell'utilizzo compassionevole dei medicinali e nell'utilizzo *off-label* degli anticorpi monoclonali, l'Agenzia ha avuto un ruolo predominante anche e soprattutto con riferimento alla gestione dei dati in possesso.

Infatti, con riferimento al primo ambito, l'AIFA, in uno studio pubblicato sul proprio sito ha chiarito che «gli studi che hanno portato alla messa a punto dei vaccini COVID-19 non hanno saltato nessuna delle fasi di verifica dell'efficacia e della sicurezza previste per lo sviluppo di un medicinale, anzi, questi studi hanno visto la partecipazione di un numero assai elevato di volontari, circa dieci volte superiore a quello di studi analoghi a quello di studi analoghi per lo sviluppo di altri vaccini».

---

[201] «Ordinanza del Ministero della salute del 21 febbraio 2020 – Ulteriori misure profilattiche contro la diffusione della malattia infettiva COVID-19».

Con riferimento alla gestione farmaco sperimentale (IMP), laddove il Promotore abbia individuato o disponga di un deposito ove il farmaco è stoccato, eccezionalmente e a causa delle limitazioni alla circolazione, è stata prevista la consegna diretta da parte del deposito al soggetto in sperimentazione. Per questa modalità, è stato necessario individuare le procedure per il mantenimento di tutte le garanzie di controllo e tracciabilità di consegna, comprese le condizioni di trasporto e l'individuazione di un corriere dedicato che operi secondo procedure per la consegna diretta dei farmaci sperimentali ai soggetti partecipanti, adottando tutte le misure necessarie a garantire la confidenzialità delle informazioni riconducibili al soggetto, quali le istruzioni di cui all'art. 29 del GDPR, che il titolare del trattamento dei dati personali è tenuto a fornire a chiunque agisca sotto la sua autorità o la designazione a responsabile del trattamento dei dati ai sensi dell'art. 28 GDPR.

Con riguardo, infine, alle analisi cliniche e/o indagini strumentali, tenuto conto della circostanza secondo cui tali esami possano essere effettuate in strutture vicine al domicilio del soggetto, dovranno essere preferite strutture pubbliche o private che siano state riconosciute idonee a condurre studi clinici secondo il DM 19 marzo 1998 o laboratori privati che abbiano le condizioni di cui alla determina AIFA 809/2015.

Anche in questa circostanza, il titolare del trattamento dei dati sarà tenuto ad attenersi a quanto previsto dall'art. 28[202] del GDPR o, in alternativa, a quanto indicato nell'art. 24[203] del GDPR.

Fatta queste necessarie premesse di inquadramento normativo e di carattere generale al fine di introdurre la tematica del lavoro in oggetto, nei paragrafi che seguono si procederà all'analisi dettagliata dei fenomeni di digitalizzazione del dato sanitario, anche con riguardo all'utilizzo degli strumenti di intelligenza artificiale.

---

[202] Art. 28 del GDPR: «Responsabile del trattamento. 1. Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato».

[203] Art. 24 del GDPR: «Responsabilità del titolare del trattamento 1. Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario. 2. Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento. 3. L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento».

Secondo capitolo

Sezione I

2. La digitalizzazione del dato sanitario.

2.1. La sanità digitale.

Sebbene la declinazione del diritto alla salute rispetto all'evoluzione della ricerca scientifica e tecnologica non sia questione recente e rappresenti un punto focale degli studi giuridici – non soltanto civilistici ma anche costituzionalistici – dedicati al settore sanitario, la pandemia da Covid-19 ha, drammaticamente, evidenziato il valore e la necessità di provvedere all'elaborazione strutturale di una sanità digitale, proprio a seguito dell'adozione delle regole di distanziamento sociale, del ricorso alla telemedicina[204], delle difficoltà oggettive riscontrate nel prenotare esami strumentali da remoto o nel ricevere i referti in formato *online*.

[204] Vedi *infra*.

Ancor prima della pandemia, però, l'Italia con il d.l. n. 179/2012 aveva previsto un'intera sezione dedicata alla sanità digitale, la n. 4, che rubricava l'art. 12 «Fascicolo sanitario elettronico, sistemi di sorveglianza nel settore sanitario e governo della sanità digitale», ma che, nonostante le buone intenzioni era rimasta lettera morta.

Di fatti, sebbene vi fossero degli aspetti indubbiamente positivi, la digitalizzazione della sanità ha sottolineato enormemente il *digital divide*[205], in quanto ha escluso coloro i quali non hanno accesso ad internet o che non sono in grado di utilizzare la tecnologia informatica in maniera efficiente[206], con il rischio di un'evidente discriminazione «per l'eguaglianza dei diritti esercitabili online» in virtù dell'avvento della società digitale[207], in forza di quella c.d. «libertà informatica»[208] che è divenuta una pretesa di libertà

[205] C. CAPORALI, *Invecchiamento e divari di genere nell'uso degli strumenti di eHealth* in *Culture e Studi del Sociale*, n. 9/2024, pp. 92-106.

[206] L. FERRARO, *Il Regolamento UE 2016/679 tra Fascicolo Sanitario Elettronico e Cartella Clinica Elettronica: il trattamento dei dati di salute e l'autodeterminazione informativa della persona in BioLaw Journal – Rivista di BioDiritto*, n. 4/2021, pp. 91-114.

[207] G. PELLICANÒ, *Sanità digitale, stato dell'arte e prospettive future* in *Smart eLab*, n. 14/2019; D. GRECO, *Sanità digitale dopo la pandemia: lo scenario*, 25 maggio 2021, in https://www.agendadigitale.eu/sanita/sanita-digitale-dopo-la-pandemia-lo-scenario/

[208] T. E. FROSINI, *Il costituzionalismo nella società tecnologica* in *Il diritto dell'informazione e dell'informatica*, n. 4/2020, p. 467.

positiva di servirsi degli strumenti informatici per fornire e ottenere informazioni di ogni genere.

Se da una parte l'integrazione di strumenti di *e-Health* nel sistema sanitario è auspicabile in quanto in grado, ad alcune condizioni, di migliorare l'efficacia e l'efficienza delle prestazioni offerte (anche abbattendo le distanze fisiche e i tempi di attesa) e di incentivare l'*empowerment* del paziente, mettendolo al centro e promuovendone le *capabilities*; dall'altra, l'utilizzo di queste tecnologie ha messo in luce la presenza di molteplici criticità e punti di debolezza che, se non adeguatamente affrontati, possono avere – al contrario – effetti negativi sul funzionamento stesso del sistema sanitario nonché sulla salute del paziente, oltre ad aumentare le disuguaglianze proprio delle persone che hanno maggiormente bisogno di cura ma dispongono di minori risorse.

A ciò è necessario aggiungere la resistenza degli «operatori sanitari maggiormente abituati all'uso dell'analogico, in luogo del digitale, che servendosi degli strumenti informatici potrebbero rendere i servizi sanitari più rapidi e senz'altro più efficienti»[209].

La digitalizzazione del dato sanitario ha consentito la lettura di rapporti c.d. tradizionali – quello tra medico e paziente e quello tra

[209] S. CORONATO, *Gli strumenti necessari al processo di digitalizzazione del S.S.N.* in *Diritto sanitario moderno*, n. 3/2019, p. 169.

struttura sanitaria e utente del servizio sanitario – sotto una lente differente e sicuramente nuova.

Infatti, l'impatto dell'*e-Health* e delle applicazioni dell'intelligenza artificiale nella relazione terapeutica e diagnostica si riverbera sull'effettività del diritto alla salute, costringendo l'interprete a verificare se le "vecchie" garanzie costituzionali per tutelare il diritto individuale alla salute siano in grado di gestire e soddisfare le "nuove" domande di protezione del bene salute che emergono quotidianamente dall'evoluzione scientifica e tecnologica[210].

Infatti, le nuove tecnologie impattano sul diritto alla salute nella sua dimensione complessiva, sia per quel che riguarda i profili riguardanti la libertà di cura e cioè di autodeterminazione terapeutica, che per quel che concerne il diritto a ricevere trattamenti sanitari e quindi l'accesso alle cure in maniera eguale con specifico riguardo all'intelligenza artificiale, sia con riferimento alle nuove formulazioni del consenso informato per ricevere delle diagnosi supportate dall'intelligenza artificiale[211]

---

[210] D. MORANA, T. BALDUZZI, F. MORGANTI, *La salute "intelligente": eHealth, consenso informato e principio di non discriminazione*, in *Federalismi.it*, n. 34/2022, pp. 127-151.

[211] *Ibidem* che richiama: G. SARTOR, *Intelligenza artificiale e diritto. Un'introduzione*, Giuffrè, 1996; A. D'ALOIA, *Il diritto verso "il mondo nuovo". Le sfide dell'intelligenza artificiale*, *in BioLaw Journal-Rivista di BioDiritto*, n. 1/2019, pp. 3 ss; S. DORIGO (a cura di), *Il ragionamento*

che per quel che attiene al principio di non discriminazione in ambito terapeutico[212].

Prima di analizzare nel dettaglio gli strumenti di sanità digitale sia in Italia, sia in Europa, è d'interesse studiare la macroarea *dell'e-Health* che ricomprende «ogni forma di applicazione al settore sanitario delle tecnologie dell'informazione e della comunicazione (o ICT, *information and comunication technologies*)»[213] e consta sia delle applicazioni medico-sanitarie dell'intelligenza artificiale[214], sia dell'*e-Health* in senso stretto[215], cui sono

---

giuridico nell'era dell'intelligenza artificiale, Pacini giuridica, 2020; E.A. FERIOLI, *Digitalizzazione, intelligenza artificiale e robot nella tutela della salute*, in A. D'ALOIA, (a cura di), *Intelligenza artificiale e diritto. Come regolare un mondo nuovo*, Franco Angeli, 2020, p. 423 ss.

[212] *Ibidem* che richiama: P. ZUDDAS, *Intelligenza artificiale e discriminazioni*, in A.a. V.v., *Liber amicorum per Pasquale Costanzo – Diritto costituzionale in trasformazione, I, Costituzionalismo, Reti e intelligenza artificiale*, *Consulta OnLine*, 2020, p. 461.

[213] Cfr. Le linee guida dell'OMS, *Recommendations on digital interventions for health system strengthening*, pubblicate nel 2019 e citate da D. MORANA, T. BALDUZZI, F. MORGANTI, *La salute "intelligente": eHealth, consenso informato e principio di non discriminazione*.

[214] G. FARES, *Artificial intelligence in social and health services: A new challenge for public authorities in ensuring constitutional rights*, in M. BELOV (a cura di), *The IT revolution and its impact on State, constitutionalism and public law*, Hart Publishing, Oxford, 2021, p. 269 ss.

[215] Nella risoluzione WHA58.28 del 2005, adottata dall'Assemblea mondiale della sanità, organo legislativo dell'OMS, l'eHealth è definita come «*the cost-effective and secure use of information and communication technologies in support of health and health-related fields, including health-care services, health surveillance, health literature, and health education, knowledge and research*».

riconducibili, tra l'altro e senza pretesa di esaustività, la telemedicina intesa quale «modalità di erogazione della prestazione sanitaria attraverso tecnologie innovative che consentono di sviluppare la relazione medico-paziente senza la necessità di una compresenza fisica dei soggetti coinvolti»[216] e il fascicolo sanitario elettronico[217] «quale modalità di

[216] Così, D. MORANA, T. BALDUZZI, F. MORGANTI, *La salute "intelligente": eHealth, consenso informato e principio di non discriminazione* che cita le *Linee di indirizzo nazionali* in tema di telemedicina adottate dal Ministero della salute nel 2012, le quali precisano anche, a p. 10, che la telemedicina «comporta la trasmissione sicura di informazioni e dati di carattere medico nella forma di testi, suoni, immagini o altre forme necessarie per la prevenzione, la diagnosi, il trattamento e il successivo controllo dei pazienti». Alla nozione di telemedicina sono riconducibili, come ulteriormente precisato nelle *Indicazioni nazionali per l'erogazione di prestazioni in telemedicina* del 2020, la televisita, il telemonitoraggio di parametri vitali, la telerefertazione, la teleassistenza da parte di professionisti sanitari non medici (come infermieri o fisioterapisti) *etc*.

[217] D. MORANA, T. BALDUZZI, F. MORGANTI, *La salute "intelligente": eHealth, consenso informato e principio di non discriminazione* op. cit. che prevede che «Il fascicolo sanitario elettronico è stato introdotto con il d.l. 18 ottobre 2012, n. 179 («Ulteriori misure urgenti per la crescita del Paese»), convertito con modificazioni in l. 17 dicembre 2012, n. 221, sul quale si è innestato, di lì a qualche anno, il d.P.C.M. 29 settembre 2015, n. 178, recante «Regolamento in materia di fascicolo sanitario elettronico»; più di recente, nel pieno dell'emergenza pandemica, sull'art. 12 del d.l. n. 179 del 2012, che contiene la disciplina del fascicolo sanitario elettronico e che già aveva subito modifiche negli anni precedenti, è intervenuto massicciamente il d.l. 19 maggio 2020, n. 34 («Misure urgenti in materia di salute, sostegno al lavoro e all'economia, nonché di politiche sociali connesse all'emergenza epidemiologica da COVID-19»), convertito con modificazioni in l. 17 luglio 2020, n. 77, con l'intento di semplificare, «accelerare e potenziare gli indiscutibili vantaggi derivanti da un più celere scambio d'informazioni» in ambito sanitario, soprattutto in periodo d'emergenza (E. SORRENTINO e A.F.

conservazione, accessibilità e circolazione dei dati che attengono alla salute individuale»[218], di cui si parlerà diffusamente nei paragrafi che seguono.

Lo studio in oggetto si interrogherà sull'effettività della tutela del diritto alla salute, del rapporto medico-paziente, della protezione dei dati sanitari[219] attraverso questa nuova erogazione delle prestazioni, proprio per evitare che il ricorso alla telemedicina e alle risorse dell'*E-health* sia un mezzo attraverso il quale venga incrinata o svuotata di contenuto «quella alleanza terapeutica che è un corollario della libertà di cura»[220] o venga messo in dubbio in alcun modo il limite costituzionale del rispetto della dignità umana.

Conclusa, fortunatamente (n.d.r..), la parentesi pandemica, si è provveduto a valorizzare tali strumenti anche nella "normalità", in

---

SPAGNUOLO, *La sanità digitale in emergenza Covid-19. Uno sguardo al fascicolo sanitario elettronico*, in *federalismi.it - Osservatorio di diritto sanitario*, n. 30, 2020, p. 243).

[218] D. MORANA, T. BALDUZZI, F. MORGANTI, *La salute "intelligente": eHealth, consenso informato e principio di non discriminazione op. cit* che cita *Ex multis*, G. CRISAFI, *Fascicolo sanitario elettronico: "profilazione" programmazione sanitaria*, in *federalismi.it*, n. 5/2021, p. 96 ss.

[219] D. MORANA, T. BALDUZZI, F. MORGANTI, *La salute "intelligente": eHealth, consenso informato e principio di non discriminazione* che cita A. MARTANI, *Le incertezze del diritto nel contesto della sanità moderna: sfide presenti e future*, in C. PICIOCCHI, M. FASAN e C.M. REALE (a cura di), *Le (in)certezze del diritto*, Editoriale Scientifica, 2021, p. 197 ss.

[220] D. MORANA, T. BALDUZZI, F. MORGANTI, *La salute "intelligente": eHealth, consenso informato e principio di non discriminazione, op.cit.*

funzione ancillare e integrativa rispetto agli approcci tradizionali della medicina di prossimità.

Infatti il decreto ministeriale n. 77 del 23 maggio 2022 – in attuazione della Missione 6[221], Componente 1, del Piano nazionale di ripresa e resilienza – nel sostenere che il Servizio sanitario nazionale «si basa su tre principi fondamentali: universalità, uguaglianza ed equità» e che «[i]l perseguimento di questi principi richiede un rafforzamento della sua capacità di operare come un sistema vicino alla comunità, progettato per le persone e con le persone»[222], sottolinea sia l'importanza del potenziamento della capillarità dell'assistenza socio-sanitaria di prossimità, sia l'innovazione e la digitalizzazione dei servizi, tenuto conto che «lo sviluppo della telemedicina va considerato un elemento abilitante per l'attuazione della riorganizzazione dell'assistenza territoriale»[223].

---

[221] Cfr. Piano Nazionale di Ripresa e Resilienza (PNRR), in https://www.governo.it/sites/governo.it/files/PNRR.pdf, 222 ss., che è stato definitivamente approvato in sede europea il 13 luglio 2021, con Decisione di esecuzione del Consiglio a seguito della proposta della Commissione. Più dettagliatamente, la Missione 6 relativa alla salute si articola in due Componenti: la prima (M6C1) che riguarda le Reti di prossimità, le strutture intermedie e la telemedicina per l'assistenza sanitaria territoriale, la seconda (M6C2) finalizzata allo sviluppo dell'Innovazione, della ricerca e della digitalizzazione del Servizio Sanitario Nazionale.

[222] Cfr. d.m. Salute 23 maggio 2022, n. 77, Allegato 1, par. 2.

[223] D. MORANA, T. BALDUZZI, F. MORGANTI, *La salute "intelligente": eHealth, consenso informato e principio di non discriminazione* che cita l'Allegato 1, par. 15 del decreto n. 77 del 23 maggio 2022.

Oltre al PNRR quale diretta conseguenza del *Next Generation EU*, nel Programma *EU4Health*, istituito dal Regolamento UE 2021/522, è previsto un programma d'azione dell'Unione in materia di salute per il periodo 2021-2027 che ha, tra gli altri obiettivi, quello di «rafforzare l'uso e il riutilizzo dei dati sanitari per la prestazione di assistenza sanitaria e per la ricerca e l'innovazione, promuovere la diffusione di strumenti e servizi digitali, nonché la trasformazione digitale dei sistemi sanitari, anche sostenendo la creazione di uno spazio europeo dei dati sanitari»[224], di cui si parlerà nei paragrafi che seguono.

2.1.1. Strumenti di carattere nazionale di attuazione della sanità digitale: la telemedicina.

Nel novero dell'analisi degli strumenti di carattere nazionale di attuazione della sanità digitale, si è ritenuto opportuno trattare dapprima la telemedicina in generale, per poi focalizzare l'attenzione sul fascicolo sanitario elettronico e la cartella clinica elettronica.

---

[224] Art. 4, par. 1, lett. F, vedasi sul tema D. MORANA, T. BALDUZZI, F. MORGANTI, *La salute "intelligente": eHealth, consenso informato e principio di non discriminazione* che cita M. FERRARA, *Dalla mobilità dei pazienti alla interoperabilità dei sistemi sanitari. Spunti sull'adozione di un formato europeo di scambio delle cartelle sanitarie elettroniche (Raccomandazione UE 2019/243)*, in *federalismi.it*, n. 5/2021, p. 24 ss.

La Telemedicina è stata definita dall'Organizzazione Mondiale della Sanità (OMS) nel 1997 come «l'erogazione di servizi sanitari, quando la distanza è un fattore critico, per cui è necessario usare, da parte degli operatori, le tecnologie dell'informazione e delle telecomunicazioni al fine di scambiare informazioni utili alla diagnosi, al trattamento ed alla prevenzione delle malattie e per garantire un'informazione continua agli erogatori di prestazioni sanitarie»[225].

Storicamente il primo riferimento alla telemedicina nella letteratura medica è apparso nel 1950, descrivendo una trasmissione telefonica di immagini radiologiche tra West Chester, Philadelphia e la Pennsylvania, coprendo così una distanza di 24 miglia. Sulla base di questo primo lavoro, i radiologi canadesi hanno creato un sistema di teleradiologia nel 1950. Il primo uso medico della videocomunicazione negli Stati Uniti risale al 1959 quando medici dell'Università del Nebraska hanno utilizzato una televisione bidirezionale interattiva per trasmettere esami neurologici e altre informazioni per gli studenti di medicina. Successivamente è stato applicato lo stesso metodo nella terapia di gruppo e nel 1964 è stato stabilito un legame di telemedicina con

[225] WHO-REPORT: *A health telematics policy in support of WHO's Health-For-All strategy for global health development: report of the WHO group consultation on health telematics*, 11-16 December, Geneva, 1997 (doc. web)

l'ospedale di Stato di Norfolk (112 miglia di distanza) per fornire supporto in logopedia, esami neurologici, diagnosi di casi psichiatrici difficili, consultazioni di casi, seminari di ricerca e formazione. Nel 1959, un radiologo canadese ha riferito consultazioni diagnostiche basate sulle immagini fluoroscopiche trasmesse da un cavo coassiale. Nel 1961, una rivista di anestesiologia ha riferito radiotelemetria per il monitoraggio dei pazienti.

La trasmissione s2s (*ship to shore*) di elettrocardiogrammi (ECG) e raggi X è stata segnalata nel 1965 e, poco dopo, nel 1967, si è avuta la prima trasmissione transoceanica. Ancora nel 1967, i medici dell'Università di Miami ed i vigili del fuoco della medesima città hanno riferito l'uso pionieristico di canali radio esistenti per trasmettere i ritmi elettrocardiografici dalle unità di soccorso al Jackson Memorial Hospital. Oggi è uso comune per i paramedici trasmettere ritmi cardiaci ed ECG a 12 derivazioni per servizi ospedalieri di emergenza. Tra gli anni 1960-1970, sono state avviate varie altre applicazioni di telemedicina, molte delle quali a beneficio di agenzie federali, tra cui il Dipartimento di Salute, Istruzione, i servizi sociali e la *National Aeronautics and Space Administration* (NASA). Un insieme di partner tra cui il servizio della Sanità, la NASA e la azienda *Lockheed* si sono uniti a sponsorizzare STARPAHC (*Space Technology Applied to Rural*

Papago Advanced Health Care), che ha testato le possibilità di utilizzare comunicazioni satellitari per fornire servizi ai residenti di posti isolati. Questo progetto STARPAHC è durato circa 20 anni. Successivamente, negli anni 1970-1980, il servizio sanitario degli Stati Uniti e il Dipartimento della difesa americana hanno finanziato una serie di progetti di «teleradiologia». Questi progetti hanno portato alla realizzazione di un *network* per il trasferimento di immagini digitali finalizzato a promuovere lo sviluppo e l'attuazione della «tele-cardiologia» civile e militare[226].

Queste e altre tipologie di sperimentazioni servono dal nostro punto di vista ad evidenziare come sia fondamentale reperire una quantità di dati biomedici o bio-medicosanitari verificati al fine di dar vita a *database* da utilizzare per l'aggiornamento costante dei *device* in uso per il monitoraggio di queste patologie.

«La prestazione in Telemedicina viene integrata nel tradizionale rapporto personale medico-paziente per migliorarlo in termini di efficacia, efficienza e appropriatezza. La Telemedicina deve altresì ottemperare a tutti i diritti e obblighi propri di qualsiasi atto sanitario. Il suo utilizzo consente quindi, sia di trovare nuove risposte ai tradizionali problemi della medicina, sia di creare nuove opportunità per il miglioramento del servizio sanitario tramite una

---

[226] R. GOLDSHTEIN, *Medicina e chirurgia a distanza: inquadramento, stato dell'arte ed applicazioni cliniche*, Tor Vergata University Press, 2005, p. 4.

maggiore collaborazione tra medici (anche di diverse specialità), istituti e laboratori. Nell'ambito della diagnostica clinica, questa disciplina permette al medico di effettuare diagnosi su un paziente a distanza, attraverso la trasmissione di dati prodotti da strumenti diagnostici. Inoltre, permette di effettuare il teleconsulto che è uno dei più comuni e forse il più importante vantaggio della telemedicina che consiste nel fornire un'opinione clinica a distanza supportata da dati acquisiti inviati ad un medico remoto che li analizza producendo di fatto una seconda valutazione clinica su un paziente»[227].

Si pensi, al riguardo, al successo dell'app denominata «FlagMii» – sperimentata a partire dal 2019 in alcune regioni Italiane (tra le quali l'Emilia Romagna ed il Piemonte) –, il cui utilizzo consente di ridurre i tempi d'intervento nelle operazioni di soccorso e garantisce un supporto «da remoto» per gestire, nell'immediato, situazioni critiche quali, ad esempio, un arresto cardiaco o un parto; si tratta di un *software* per centrali operative di emergenza interamente dedicato alla gestione delle chiamate provenienti da smartphone il cui scopo è quello di creare un vero e proprio *link* tra la persona che chiede supporto e il cd. *call-taker* ossia

[227] *Ibidem.*

l'operatore medico-sanitario che, dalla centrale operativa, detta le istruzioni per l'intervento in tempo reale (cd. *real time operating*). Le tecniche telemediche, inoltre, contribuiscono alla fruizione della cd. «formazione a distanza» attraverso applicazioni informatiche che hanno quale finalità principale la formazione/specializzazione di medici attraverso l'uso delle tecnologie di *e-learning*[228].

Le "indicazioni nazionali per l'erogazione dei servizi di telemedicina" approvate dalla Conferenza Permanente per i rapporti tra lo Stato, le Regioni e le Province autonome di Trento e Bolzano il 17 dicembre 2020 definiscono la telemedicina come «un approccio innovativo alla pratica sanitaria che consente l'erogazione di servizi a distanza attraverso l'uso di dispositivi digitali, Internet, software e reti di comunicazione»[229].

---

[228] A. MARCHESE, *Profili civilistici dell'information technology in ambito sanitario* in *Quaderni della Rassegna di diritto civile diretta da Pietro Perlingieri,* Edizioni Scientifiche Italiane, p. 192.

[229] A. MARCHESE, *Profili civilistici dell'information technology in ambito sanitario* che cita «Le prime Linee di Indirizzo Nazionali sono state definite nel 2012 dal Consiglio Superiore della Sanità e approvate con intesa tra il Governo, le Regioni e le Province autonome di Trento e Bolzano nel 2014. Sono state poi aggiornate a seguito dell'emergenza sanitaria da Covid-19 nel 2020. Nel 2021 sono state pubblicare le "Indicazioni nazionali per l'erogazione di prestazioni e servizi di teleriabilitazione da parte delle professioni sanitarie". Tutte le indicazioni sono disponibili su https://www.salute.gov.it/portale/ehealth/dettaglioContenutiEHealth.jsp?area=eHealth&id=5525&lingua=italiano&menu=telemedicina

Tra i servizi di telemedicina sono compresi «la televisita, il teleconsulto medico, la teleconsulenza medico-sanitaria, la teleassistenza, la tele-refertazione e il telemonitoraggio»[230].

La telemedicina è un supporto fondamentale nell'attuale modello organizzativo del servizio sanitario pubblico. L'Agenzia Nazionale per i Servizi Sanitari (AGENAS) ha difatti precisato che «la telemedicina svolge una funzione di raccordo tra il sistema di cura, di emergenza e urgenza e l'assistenza domiciliare e capillare di pazienti, nella maggior parte dei casi affetti da una o più cronicità»[231].

Con il decreto 21 settembre 2022 del Ministero della Salute sono stati definiti i requisiti funzionali e i livelli di servizio della telemedicina[232].

Il «Piano Nazionale di Ripresa e Resilienza (PNRR) ha poi previsto ingenti investimenti sia per la costruzione di una

---

[230] *Ex multis*, V. SICA, S. SELVAGGI, *Telemedicina. Approccio multidisciplinare alla gestione dei dati sanitari*, Milano, 2010; C. BOTRUGNO, *The spread of telemedicine in routine medical practice: towards an ad hoc ethics*, in *Ragion pratica*, 1, 2016, pp. 185-206; C. FARALLI, R. BRIGHI, M. MARTONI, *Strumenti, diritti, regole e nuove relazioni di cura: il Paziente europeo protagonista nell'e-Health*, Torino, 2015; G. DE VERGOTTINI, C. BOTTARI, *La sanità elettronica*, Bologna, 2018.

[231] Agenzia nazionale per i servizi sanitari, *Le Centrali Operative. Standard di servizio, modelli organizzativi, tipologie di attività ed esperienze regionali*, supplemento alla rivista semestrale *Monitor*, 2022.

[232] Ministero della Salute, Decreto 21 settembre 2022 "Approvazione delle linee guida per i servizi di telemedicina - Requisiti funzionali e livelli di servizio" in G.U. Serie Generale n. 256 del 2 novembre 2022.

Piattaforma Nazionale di Telemedicina (PNT) che per l'aumento dei servizi di telemonitoraggio e telecontrollo per i pazienti con patologie cardiologiche, respiratorie, neurologiche, diabetologiche e oncologiche, oltre che per soluzioni di teleconsulto, televisita e teleassistenza, più in generale»[233]. AGENAS è il soggetto responsabile dell'attuazione delle dei progetti sotto la vigilanza del Ministro della Salute e del Ministro per l'innovazione tecnologica e la transizione digitale. In questo contesto la telemedicina è considerata una chiave di volta per tre principali obiettivi: «colmare i divari geografici del sistema sanitario italiano, migliorare l'assistenza e il percorso dei singoli pazienti, aumentare l'efficienza generale con la promozione dell'assistenza domiciliare, delle cure di prossimità e del monitoraggio da remoto delle patologie»[234]. La casa del paziente diventerà sempre più «il primo luogo di cura»[235].

---

[233] il PNRR, piano M6C1, investimento 1.2.3 "Telemedicina per un migliore supporto ai pazienti cronici" in *https://www.agenas.gov.it/view-article-id-2329-la-telemedicina-catid-85*

[234] G. BINCOLETTO, *L'uso secondario di dati sanitari per fini di ricerca nella telemedicina: la tutela dei dati personali tra regole e prassi in ricerca* in *Sanità e protezione dei dati personali: scenari applicativi e prospettive future*, in E. CHIZZOLA, P. GUARDA, V. MARONI, L. RUFO (a cura di), Atti del convegno Trento, 29 settembre 2023.

[235] D. MANTOAN, A. BORGHINI, *Potenziamento dell'assistenza sanitaria e della rete sanitaria territoriale*, in *Monitor 45*, 2021, 10-13 e A. URBANI, *Innovazione, ricerca e digitalizzazione del SSN*, in *Monitor 45*, 2021, pp. 46-47.

Un profilo interessante riguarda la ricerca di un punto di contatto tra lo sviluppo della telemedicina e la ricerca scientifica attraverso l'uso dei dati sanitari raccolti nel corso dei servizi a distanza per finalità di ricerca, il cosiddetto utilizzo secondario dei dati, già trattato nel primo capitolo di questo lavoro.

2.1.1.2. Il connubio tra telemedicina e ricerca scientifica.

L'importanza dell'utilizzo secondario dei dati è stata, a più riprese, analizzata in questo lavoro ma si è ritenuto interessante verificare come la digitalizzazione del dato sanitario possa avere un impatto positivo sulla ricerca scientifica.

Da un lato le piattaforme e gli applicativi possono essere fondamentali per reclutare i partecipanti agli studi – velocizzando gli oneri richiesti per raccogliere le adesioni alla ricerca, aumentando la mole di dati e includendone altri che sono esterni alle piattaforme tradizionali – dall'altro, combinando le informazioni con quelle tratte dai dispositivi medici o generate direttamente dai pazienti, sarà possibile raggiungere più individui, avere maggiori risultati e ridurre i costi della ricerca[236].

---

[236] M. BOCCHINO, *Significato dei Real World Data nell'era della medicina digitale: realtà e prospettive* in *Ricerca in sanità e protezione dei dati personali: scenari applicativi e prospettive future*, in E. CHIZZOLA, P.

Ad esempio, un possibile ambito che necessita di processare una rilevante quantità di dati è quello dell'addestramento di algoritmi di intelligenza artificiale – di cui si parlerà diffusamente in seguito – per l'elaborazione di modelli predittivi o assistenti personali virtuali che vengono integrati nelle *m-health app* che sono «delle applicazioni che vengono messe a disposizione dall'azienda sanitaria o dalla struttura medica ai pazienti per un loro utilizzo quotidiano attraverso uno smartphone o altro dispositivo equiparabile»[237].

Alcuni progetti di questa tipologia sono promossi dalle aziende sanitarie e dalle Regioni e Province autonome.

Nell'ambito della Provincia autonoma di Trento, è stata prevista «con delibera n. 2475 del 22 dicembre 2022 l'approvazione e il finanziamento del Progetto "Sanità digitale e intelligenza artificiale – Strumenti per avvicinare il Servizio sanitario ai cittadini e per lo sviluppo del "sistema provinciale", promosso dal Centro di competenza sulla sanità digitale TrentinoSalute 4.0"»[238].

GUARDA, V. MARONI, L. RUFO (a cura di), Atti del convegno Trento, 29 settembre 2023.

[237] G. BINCOLETTO, *mHealth app per la televisita e il telemonitoraggio. Le nuove frontiere della telemedicina tra disciplina sui dispositivi medici e protezione dei dati personali*, in *BioLaw Journal – Rivista di BioDiritto*, n. 4/2021, pp. 381-407.

[238] M. BOCCHINO, *Significato dei Real World Data nell'era della medicina digitale: realtà e prospettive*, op. cit. che prevede che «sono previsti studi di ricerca nell'ambito dell'intelligenza artificiale e della telemedicina per gli

È opportuno sottolineare però che l'utilizzo secondario dei dati attraverso la telemedicina dovrà essere sempre bilanciato con il «diritto individuale e fondamentale alla protezione dei dati personali in capo all'interessato-paziente, specialmente nell'ambito sanitario in cui la confidenzialità è essenziale»[239].

2.1.1.2.1. Un esempio di proattività nell'ambito della telemedicina: le m-health app.

ambiti di cardiologia (predizione rischio di complicanze), oculistica (predizione rischio di retinopatia diabetica ed *early detection* su lattanti) e benessere e stili di vita della gravidanza fisiologica. I progetti prevedono la raccolta di dati clinici e immagini e il riuso di altri dati già a disposizione dell'Azienda Provinciale per i Servizi Sanitari. TrentinoSalute4.0 è il Centro di Competenza sulla Sanità Digitale governato congiuntamente da Provincia autonoma di Trento, Azienda Provinciale per i Servizi Sanitari e Fondazione Bruno Kessler quale "spazio condiviso" e "Laboratorio congiunto" per supportare lo sviluppo della sanità digitale nella Provincia autonoma di Trento attraverso un approccio di sistema. Tale Centro è stato istituito con la delibera della Giunta Provinciale n. 2412 del 20 dicembre 2016».

[239] P. AURUCCI, *Il trattamento dei dati personali nella ricerca biomedica. Problematiche etico-giuridiche*, Napoli, 2022 e M.G. HANSSON, *Striking a Balance Between Personalised Genetics and Privacy Protection from the Perspective of GDPR*, in S. SLOKENBERGA et al. (a cura di), *GDPR and Biobanking*, Cham, 2021, 31-42; J. MADIR (a cura di), *Healthtech. Law and Regulation*, Cheltenham, 2020. Sulla confidenzialità è necessario riferirsi innanzitutto al par. 24 della *Declaration of Helsinki on Ethical Principles for Medical Research Involving Human Subjects*, disponibile in rete https://www.wma.net/policies-post/wma-declaration-of-helsinki-ethical-principles-for-medical-research-involving-human-subjects.

Nel capitolo precedente si è parlato dell'utilizzo secondario dei dati e dell'importanza e della centralità della base giuridica del consenso con riferimento all'uso dei medesimi, nel documento "Criticità etiche e normative nel trattamento dei dati personali sanitari nella ricerca osservazionale"[240], il Centro di Coordinamento nazionale dei Comitati etici, però, propone di superare la logica del consenso per i dati pseudonomizzati, sostituendo il meccanismo con un "*opt-out*"[241] – ossia permettendo al singolo di esercitare un suo dissenso in relazione al trattamento di un suo dato sanitario, con ciò distinguendo tale facoltà dal diritto alla cancellazione ed evitando di circoscriverla nei limiti connaturati all'esercizio di quel diritto – o procedendo verso un consenso generale.

Si tende dunque ad optare per una soluzione che non escluda del tutto la base giuridica del consenso ma allo stesso tempo incentivi l'utilizzo secondario dei dati raccolti nell'ambito della telemedicina servendosi anche delle *m-health app*.

---

[240] Criticità etiche e normative nel trattamento dei dati personali sanitari nella ricerca osservazionale, Documento del Centro di Coordinamento Nazionale dei Comitati Etici (CCNCE). 6 aprile 2023, per la consultazione integrale https://www.aifa.gov.it/documents/20142/1808580/Criticita_etiche_ricerca_osservazionale_06.04.2023.pdf

[241] S. CORSO, *Trattamento di dati sanitari e tutela della persona. Dal consenso alla volontà* in *Il comitato di ricerca si confronta - atti del II ciclo di Seminari (2022-2023)*, di F.A. BELLA, N. POSTERARO, M.A. SANDULLI (a cura di), p. 64.

Ad esempio, nella Provincia di Trento è stata elaborata TreC+ dell'Azienda Provinciale per i Servizi Sanitari (APSS), che si basa sul concetto di *personal health record*[242] ma che offrirà dei servizi di telemedicina come, ad esempio, la funzione di televisita per tutti gli utenti e la previsione di un telemonitoraggio per coloro i quali siano affetti da malattia croniche[243].

---

[242] Su questi sistemi si v. ex multis G. BINCOLETTO, *Data Protection Issues in Cross-Border Interoperability of Electronic Health Record Systems within the European Union*, in *Data & Policy*, 2, 3, 2020, pp. 1-11; G. BINCOLETTO, *A Data Protection by Design Model for Privacy Management in Electronic Health Records,* in Privacy Technologies and Policy, 7th Annual Privacy Forum, Lecture Notes in Computer Science, 2019, pp. 161-181; G. VERGOTTINI, C. BOTTARI, *La sanità elettronica*, Bologna, 2018; P. GUARDA, R. DUCATO, *From Electronic Health Records to Personal Health Records: emerging Legal Issues in the Italian Regulation of eHealth*, in *International Review of Law, Computers & Technology*, 2016, pp. 271-285; C. FARALLI, R. BRIGHI, M. MARTONI et al., *Strumenti, diritti, regole e nuove relazioni di cura: Il Paziente europeo protagonista nell'e-Health,* Torino, 2015; G. COMANDÉ, L. NOCCO, e V. PEIGNÉ, *An empirical study of healthcare providers and patients' perceptions of electronic health records*, in *Computers in Biology and Medicine*, 2015, pp. 194-201; C. GEORGE, D. WHITEHOUSE, P. DUQUENOY, eHealth: legal, ethical and governance challenges, Berlin Heidelberg, 2012; P. GUARDA, *Fascicolo sanitario elettronico e protezione dei dati personali*, p. 94, Trento, 2011.

[243] G. BINCOLETTO, P. GUARDA, *A proactive GDPR-compliant solution for fostering medical scientific research as a secondary use of personal health data*, in *Opinio Iuris in Comparatione* n. 1/2021, pp. 43-76; C. ECCHER et al., *TreC Platform. An integrated and evolving care model for patients' empowerment and data repository, in Journal of Biomedical informatics*, 102, 2020, 103359; S. TESTA, O. MAYORA-IBARRA, E.M. PIRAS et al., *Implementation of televisit healthcare services triggered by the COVID-19 emergency: the Trentino Province experience*, in *Z Gesundh Wiss*., 2021, 1-16; L. GIOS et al., *Use of eHealth Platforms and Apps to Support Monitoring and Management of Home-Quarantined Patients With COVID-19 in the*

Nel caso di specie, il paziente iscritto all'anagrafe di Trento potrà scaricare l'applicazione fornita dal servizio sanitario dallo *store*, autenticarsi con delle specifiche credenziali[244], fare l'*upload* di informazioni e accedere ai dati relativi alla propria salute fisica o mentale e selezionare uno più servizi assistenziali.

Dall'altro lato, il personale sanitario – complessivamente inteso – attraverso un cruscotto *web* può interagire con il soggetto in varie forme – sia con il caricamento dei referti o altri dati del paziente sia fissando un appuntamento di televisita da effettuare tramite videochiamata con l'inserimento di una chat all'interno dell'applicazione che permetterà anche lo scambio di fotografie e dati.

Se invece il paziente fosse affetto da una malattia cronica, il medico curante dovrà attivare il servizio di telemonitoraggio che si tradurrà nel controllo della terapia e della cura somministrata tramite la raccolta attiva dei parametri effettuata dal soggetto

---

Province of Trento, in JMIR formative research, 5.5, 2021, e25713. Si v. inoltre i siti ufficiali dell'applicazione, in Rete: https://trec.trentinosalute.net/fast-trec; https://www.apss.tn.it/Servizi-e-Prestazioni/Cartella-clinica-del-cittadinoTreC

[244] Le credenziali sono generalmente associate al numero di tessera sanitaria del paziente iscritto all'anagrafe del servizio sanitario regionale e prevedono un doppio livello di identificazione che garantisca la sicurezza nell'utilizzo dell'applicativo da parte dell'interessato. Questa modalità di autenticazione c.d. "forte" è raccomandata dall'autorità garante francese in *Commission nationale de l'informatique et des libertés*, The CNIL's Guide on Security of personal data, 2018, pp. 7-9.

oppure attraverso la connessione dell'*app* con un dispositivo indossabile (*smartwatch* o bracciali in generale) o sottocutaneo (contraccettivo impiantabile o *pacemaker*) che misura alcuni parametri vitali con specifici sensori[245].

Nonostante tali applicazioni siano state considerate all'unanimità innovative, sono stati sollevati, però, plurimi problemi in merito alla conformità con le regole e i principi dell'ordinamento giuridico[246].

La Commissione Europea nel 2018 ha analizzato con un approccio multidisciplinare il mercato dei servizi di telemedicina a livello internazionale[247] evidenziando l'esistenza di alcune criticità economiche, sociali e tecniche che sono «l'assenza di una strategia coordinata per l'impiego dei sistemi di telemedicina a livello

---

[245] G. BINCOLETTO, *mHealth app per la televisita e il telemonitoraggio. Le nuove frontiere della telemedicina tra disciplina sui dispositivi medici e protezione dei dati personali, op.cit.*

[246] T. MULDER, *Health apps, their privacy policies and the GDPR*, in *European Journal of Law and Technology*, 10.1, 2019, disponibile in Rete su SSRN: https://ssrn.com/abstract=3506805; Comitato nazionale per la bioetica, Mobile-Health e applicazioni per la salute: aspetti bioetici, 2015; P. QUINN, et al., *The data protection and medical device frameworks - obstacles to the deployment of mHealth across Europe?*, in *European Journal of Health Law*, 20.2,2013, pp. 185–204; D. LUPTON, *M-health and health promotion: The digital cyborg and surveillance society*, in *SocTheory Health* 10, 2012, pp. 229–244.

[247] European Commission Consumers, Health, Agriculture And Food Executive Agency, Provision of a market study on telemedicine, in Retehttps://www.digitalhealthnews.eu/images/stories/pdf/2018_provision_marketstudy_tel-emedicine_en.pdf.

europeo, ma anche a livello nazionale; la mancanza di specifiche regole giuridiche per questo settore; la mancanza di standard uniformi e linee guida internazionali per l'interoperabilità di tali sistemi; la necessità di proteggere la sicurezza dei sistemi e l'applicazione delle regole in materia di protezione dei dati personali; l'opportunità di definire questioni relative alla responsabilità medica in caso di utilizzo di tali sistemi; la regolamentazione della professione del medico o del personale sanitario in relazione a questi servizi»[248].

In assenza di una disciplina specifica per tali applicazioni, la conformità a legge risulta particolarmente complessa.

In particolare, durante «la progettazione di applicativi *software* per la televisita e per il telemonitoraggio si dovrà tenere conto delle tutele e degli obblighi previsti nelle diverse discipline quali ad esempio il GDPR in merito alla tutela dei dati personali e il Regolamento UE 2017/745[249] in quanto il *software* di queste app è utilizzato in contesto medico e può assumere una destinazione

[248] G. BINCOLETTO, *mHealth app per la televisita e il telemonitoraggio. Le nuove frontiere della telemedicina tra disciplina sui dispositivi medici e protezione dei dati personali, op.cit*

[249] Regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medici, che modifica la direttiva 2001/83/CE, il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE del Consiglio, GU L 117 del 5.5.2017.

d'uso considerata tale dalla disciplina prevista da tale fonte sovranazionale per il *software as a medical device* (SaMD)»[250].

Inoltre, è necessario che queste applicazioni siano conformi a svariati requisiti previsti dagli obblighi di certificazione e che siano rispettate le disposizioni previste in ambito di sicurezza dei sistemi informativi.

Infine, è opportuno accennare – nel capitolo seguente se ne parlerà diffusamente – al cambiamento della disciplina relativa alla responsabilità medica, la regolamentazione della professione con riferimento ai servizi di tele-visita e telemonitoraggio e i cambiamenti relativi alla relazione medicale con il paziente.

2.1.1.2.2. ...e il Patto con il cittadino.

Il Centro *Digital Health & Wellbeing* della Fondazione Bruno Kessler di Trento e il Centro di Competenza "TrentinoSalute 4.0"[251] ha elaborato quello che viene definito il "Patto con il cittadino" che prevede «l'utilizzo di a) una piattaforma di servizi

[250] G. BINCOLETTO, *mHealth app per la televisita e il telemonitoraggio. Le nuove frontiere della telemedicina tra disciplina sui dispositivi medici e protezione dei dati personali, op.cit*

[251] Ci si riferisce al lavoro effettuato nell'ambito del progetto "*Telemedicina, ricerca scientifica e Big Data: le nuove frontiere della sanità digitale e la protezione dei dati personali*" da parte di P. GUARDA, P. TRAVERSO, D. CONFORTI, S. FORTI et al.

sanitari digitali; b) un applicativo di telemedicina connesso alla piattaforma; c) un agente conversazionale o *chatbot* sviluppato e inserito all'interno dell'applicativo che possa fornire informazioni sulle iniziative di ricerca, mostrare l'informativa per il trattamento dei dati personali e raccogliere il consenso informato sia a partecipare alla ricerca che al trattamento dei dati; d) un portale *web* che raccoglie tutte le ricerche e iniziative in atto per pubblicità e trasparenza»[252].

Per quel che concerne la piattaforma, sarà dirimente per il ricercatore e l'operatore dell'azienda sanitaria predisporre un progetto di ricerca che tratti i dati sanitari dei pazienti servendosi di un protocollo che individui i criteri per essere inclusi in uno studio e la documentazione necessaria che dovrà essere sottoposto all'approvazione del Centro etico competente.

Nella fase antecedente e cioè in quella di pianificazione, si dovrà programmare il trattamento dei dati personali seguendo l'approccio *data protection by design*[253] determinando *ab origine* i requisiti, le misure tecniche e organizzative, i rischi, i ruoli dei

---

[252] G. BINCOLETTO, *L'uso secondario di dati sanitari per fini di ricerca nella telemedicina: la tutela dei dati personali tra regole e prassi in ricerca, op. cit.*

[253] E. KOULIERAKIS, Certification as guidance for data protection by design in *International Review of Law, Computers & Technology*, *38*(2), pp. 245–263.

soggetti coinvolti, i flussi di dati, i documenti e tutto ciò che sia conforme al quadro normativo.

Nel dettaglio, il paziente iscritto all'anagrafe sanitaria già si serve dei servizi di telemedicina offerti da tale applicativo ma nel momento in cui effettua il *download* verrà informato del fatto che potrà essere contattato per partecipare ad un'attività di ricerca[254].

Nell'eventualità in cui l'utente dovesse acconsentire, riceverà una comunicazione in cui si chiarirà che per ogni attività di ricerca dovrà essere richiesto un esplicito consenso, così come da normativa sulla protezione dei dati personali ma, la mancata prestazione della manifestazione di volontà all'uso secondario dei dati non potrà mai interferire con l'accesso alle cure e ai servizi forniti tramite il sistema di telemedicina.

Se il paziente avrà acconsentito a ricevere gli inviti per partecipare alle attività di ricerca, sarà contattato dal *chatbot*[255] quando il ricercatore o l'operatore sanitario in generale inserisce il protocollo di ricerca nella piattaforma.

---

[254] Si fa riferimento sia ad iniziative volte al miglioramento continuo della piattaforma, all'accettabilità e all'usabilità dell'applicazione, studi epidemiologici e progetti specifici in ambito socio-sanitario-assistenziale.

[255] Il chatbot nel contesto dell'analisi in oggetto può essere equiparato alla figura del mandatario e pertanto il ricercatore alla stregua del mandante (articoli 1703-1730 codice civile) avrebbe un generale potere di controllo e indirizzo sull'attività del mandatario ovvero potrebbe applicarsi la disciplina della rappresentanza. Per tutte le considerazioni in oggetto, vedasi approfonditamente la terza sezione del terzo capitolo.

Il *chatbot* sarà programmato in modo da elaborare i messaggi per «verificare i requisiti di eleggibilità allo studio, presentare la ricerca, la sua informativa e quella relativa al trattamento dei dati personali e sottoporre il modulo dei consensi. L'informativa potrà prevedere fin da subito una procedura di anonimizzazione dei dati personali raccolti per future finalità di ricerca scientifica»[256], è garantita, in ogni caso, la possibilità di chiedere informazioni direttamente al personale sanitario che si occupa della sperimentazione.

L'archiviazione dei consensi specifici in modalità digitale ne rende agevole sia la conservazione sia la reperibilità[257], sia eventualmente il suo ritiro.

L'identificazione del paziente partecipante avviene attraverso l'accesso tramite credenziali con doppio fattore di autenticazione[258].

---

[256] G. BINCOLETTO, *L'uso secondario di dati sanitari per fini di ricerca nella telemedicina: la tutela dei dati personali tra regole e prassi in ricerca, op. cit.,* p. 123.

[257] Sul tema del consenso elettronico e la decentralizzazione della ricerca vedasi F. GABRIELLI, M. ZIBELLINI, R. TRIOLA, M. BOCCHINO (a cura di), Rapporto ISTISAN n. 4 del 2022, Decentralized Clinical Trial: nuovo approccio alla sperimentazione clinica per facilitare il paziente e velocizzare la ricerca.

[258] Spid o Carta d'identità elettronica – CIE, mentre nel caso di minori o altri soggetti con figure responsabili a prestare il consenso in loro vece, si valuterà se rimanere nella modalità tradizionale di contatto o far gestire ai medesimi gli applicativi.

Se la ricerca richiede l'uso di dati generati dal paziente, lo stesso potrà inserirli in autonomia negli applicativi o potrà rispondere ai questionari mentre sarà compito del chatbot informare il partecipante degli sviluppi della ricerca, indicando anche articoli scientifici sul tema e risultati.

È d'uopo sottolineare che il trattamento dei dati personali avverrà sempre nel rispetto delle normative e potrà essere anticipato da una DPIA (Valutazione d'impatto della protezione dei dati)[259] e sarà necessaria sempre la presenza di un DPO[260] a vigilare sulle attività.

L'esempio di questo progetto evidenzia come sia possibile responsabilizzare maggiormente il paziente in ossequio al principio di accountability senza però perdere di vista l'importanza dell'uso secondario dei dati al fine di ottenere dei risultati che consentano di avere nuove attività di cura.

2.1.2. Strumenti di carattere nazionale di attuazione della sanità digitale: la cartella clinica elettronica.

La Cartella Clinica Elettronica (CCE) è «un documento digitale, ossia la trasposizione digitale dei moduli cartacei che si

[259] Sul tema, https://www.garanteprivacy.it/valutazione-d-impatto-della-protezione-dei-dati-dpia-

[260] Per completezza, https://www.garanteprivacy.it/responsabile-della-protezione-dei-dati-rpd-

adoperavano e, in molti casi ancora si utilizzano, per documentare le attività svolte nei reparti o negli ambulatori»[261].

È necessario, sin dal principio, sottolineare che la cartella clinica elettronica non deve essere confusa con la «gestione elettronica» della cartella clinica cartacea. Quest'ultima, infatti, – più correttamente definibile quale cartella informatica – non è altro che l'esito di una procedura di memorizzazione della cartella clinica tradizionale in un formato digitale (ad esempio mediante scansione dei singoli documenti, conversione degli stessi in formato PDF e successiva loro archiviazione su un supporto di memorizzazione *on-line* o *off-line*).

Strutturalmente, invece, la cartella clinica elettronica è un documento informatico nativo digitale[262] che contiene i dati clinici-diagnostici di un soggetto creato *ad hoc* al fine di essere detenuto dalla struttura sanitaria che lo ha in cura e che sarà nelle

---

[261] Cfr. Agenda Digitale, in https://www.agendadigitale.eu/sanita/cartella-clinica-elettronica-serve-una-riprogettazione/ Per C. INGENITO, *La rete di assistenza sanitaria on-line: la cartella clinica elettronica*, in *federalismi.it*, 5, 2021, 76, «la cartella clinica è, secondo il Ministero della Sanità, "il chi, cosa, quando e come dell'assistenza al paziente nel corso dell'ospedalizzazione, strumento informativo individuale, finalizzato a rilevare tutte le informazioni anagrafiche e cliniche significative, relative ad un paziente e ad un singolo episodio di ricovero"». Ancora sulla cartella clinica, v. F. FRÈ, *La cartella clinica nel sistema sanitario italiano*, in *Ragiusan*, 291-292, 2008, p. 352 ss.

[262] A. MARCHESE, *Profili civilistici dell'information technology in ambito sanitario, op. cit.,* p. 195.

condizioni – tramite un rapido accesso alle informazioni ivi contenute – gestire tutti dati relativi alla storia clinica del paziente. Questo strumento consente di raccogliere ogni informazione relativa alle indagini e alle procedure mediche effettuate su un paziente da parte della struttura sanitaria e, di converso, consente al personale di avere accesso a tutta la documentazione[263].

---

[263] Il *drafting approach* consigliato – oggi in buona parte tenuto presente anche nell'elaborazione della cartella clinica elettronica – è il risultato di un'organizzazione dei dati orientata per problemi; da qui il nome tecnico, usualmente utilizzato, di «cartella clinica orientata per problemi» (CCOP ovvero anche POMR – *problem oriented medical record*) frutto di una lenta ma costante evoluzione concettuale finalizzata alla creazione di uno strumento che consenta – con una certa rapidità – una valutazione qualitativa e globale dell'attività medico-assistenziale e, al contempo, una visione completa di tutti i dati necessari ad una corretta pianificazione dei problemi diagnostici relativi al singolo paziente.
La logica sottesa è quella di evidenziare, quanto più chiaramente possibile, tutti gli eventi clinici ritenuti qualificanti per l'adozione del regime di ricovero e dell'eventuale (successivo) intervento. Attraverso la CCOP si valorizza altresì un approccio assistenziale di tipo globale e pluridisciplinare che interessa non solo la comunicazione tra medici con differenti competenze specialistiche ma anche tra questi ed il personale paramedico ed infermieristico. Le informazioni devono pertanto essere organizzate attraverso una collocazione scalare che prevede: -a) inizialmente una premessa dedicata ad una sintetica descrizione di tutte le informazioni fornite al paziente nel corso delle prime visite e dell'esito delle terapie iniziali (eventualmente includendo, in questa prima fase, il resoconto delle domande rivolte dal medico e delle risposte date dal paziente); -b) e, successivamente, quattro parti metodico-cliniche così suddivise: -1) lista delle problematiche su base attiva e su base inattiva (vale a dire una lista aggiornata di tutte le problematiche riscontrate durante il periodo nel quale il paziente è stato in cura come diagnosi pregresse, stati sintomatici e fisiopatologici, segnali di sofferenza obiettivabili, esami di laboratorio ed altre informazioni rilevanti

Il primo riferimento normativo è rinvenibile nell'art. 47-*bis*, 1 comma, del d.l. n. 5/2012, laddove si evince che «nei limiti delle risorse umane, strumentali e finanziarie disponibili a legislazione vigente, nei piani di sanità nazionali e regionali si privilegia la gestione elettronica delle pratiche cliniche, attraverso l'utilizzo della cartella clinica elettronica, così come i sistemi di prenotazione elettronica per l'accesso alle strutture da parte dei cittadini con la finalità di ottenere vantaggi in termini di accessibilità e contenimento dei costi»[264].

---

quali quelle direttamente collegate a problemi di ordine psichico o di ordine sociale o ad altri fattori di rischio); -2) dati clinici definitivi e di base (si tratta di tutti quei dati connessi alla sintomatologia che ha condotto al ricovero, delle pregresse condizione psico-fisiche del paziente, della morbilità attuale, degli altri dati anamnestici emersi o riferiti, dal c.d. esame obiettivo e dall'esito delle indagini strumentali e di laboratorio già in possesso del paziente); -3) piano terapeutico iniziale e finale; -4) diario clinico (strutturato secondo il modello SOVP, vale a dire: -S) tutte le informazioni soggettive riferibili alla sintomatologia evidenziata; -O) le informazioni oggettive che descrivono un significativo cambiamento del quadro clinico del paziente; -V) la valutazione e la scelta di un determinato piano terapeutico; -P) il piano terapeutico. L'utilizzo della CCOP consente, poi, la possibilità di un controllo sulla qualità e funzionalità della cartella clinica specialmente dopo l'introduzione anche nel nostro sistema di sanità pubblica e privata del DRG system (*diagnosis related groups*) e delle connesse modalità attuative del correlato sistema di finanziamento. In estrema sintesi, il sistema DRG consiste nella aggregazione funzionale di gruppi di pazienti omogenei (vale a dire «omologabili» in quanto presentano un analogo consumo di risorse sanitarie in funzione delle patologie accertate o denunciate: ad es., tutti i cardiopatici o i diabetici residenti sul territorio di competenza di una determinata ASP).

[264] Articolo 47-bis - Semplificazione in materia di sanità digitale, 1 comma del d.l. n. 5/2012.

Con l'art. 13, 5 comma, d.l. n. 179/2012, è stato poi aggiunto il comma 1-*bis* al suddetto art. 47-bis, per cui «a decorrere dal 1° gennaio 2013, la conservazione delle cartelle cliniche può essere effettuata, senza nuovi o maggiori oneri a carico della finanza pubblica, anche solo in forma digitale»[265].

Dunque, con questi atti aventi forza di legge si è avuto il passaggio definitivo «dall'ordinaria cartella clinica cartacea alla corrispondente documentazione in formato digitale, evidenziandone subito i vantaggi in termini di accessibilità e contenimento dei costi, ai sensi dell'art. 47-*bis*, 1 comma»[266].

Quanto al contenuto della cartella è necessario riferirsi al d.m. della Sanità 5 agosto del 1977 rubricato «Determinazione dei requisiti sulle case di cura private» che all'art. 24 prevede che per «ogni ricoverato si deve procedere alla compilazione della cartella clinica da cui risultino le generalità complete, la diagnosi di entrata, l'anamnesi familiare e personale, l'esame obiettivo, gli esami di laboratorio e specialistici, la terapia, gli esiti e i postumi»[267]; al d.p.c.m. 27 giugno 1986 denominato «Atto di indirizzo e coordinamento dell'attività amministrativa delle

---

[265] Articolo 47-bis - Semplificazione in materia di sanità digitale, 1 comma bis del d.l. n. 5/2012.

[266] L. FERRARO, *Il Regolamento UE 2016/679 tra Fascicolo Sanitario Elettronico e Cartella Clinica Elettronica: il trattamento dei dati di salute e l'autodeterminazione informativa della persona, op.cit.*

[267] Decreto Ministeriale 5 agosto del 1977.

regioni in materia di requisiti delle case di cura private»[268] e alla Circolare del Ministero della Sanità, 14 marzo 1996, n. 900.2/2.7/1990.

Anche l'art. 26 del Codice di Deontologia Medica interviene sul punto affermando che «il medico redige la cartella clinica quale documento essenziale dell'evento ricovero, con completezza, chiarezza e diligenza e ne tutela la riservatezza; le eventuali correzioni vanno motivate e sottoscritte. Il medico riporta nella cartella clinica i dati anamnestici e quelli obiettivi relativi alla condizione clinica e alle attività diagnostico-terapeutiche a tal fine praticate; registra il decorso clinico assistenziale nel suo contestuale manifestarsi o nell'eventuale pianificazione anticipata delle cure nel caso di paziente con malattia progressiva, garantendo la tracciabilità della sua redazione»[269].

---

[268] D.p.c.m. 27 giugno 1986.

[269] Art. 26 del Codice deontologico 2018, per tali riferimenti in letteratura cfr. P. GUARDA, *Fascicolo Sanitario Elettronico e protezione dei dati personali,* Trento, 2011, p. 150 ss., e C. SARTORETTI, *La cartella clinica tra diritto all'informazione e diritto alla privacy,* in R. FERRARA (a cura di), *Trattato di biodiritto*, diretto da S. RODOTÀ, P. ZATTI, Milano, 2010, pp. 583 ss., la quale precisa altresì che «la compresenza all'interno della cartella clinica di informazioni anagrafiche (c.d. "dati comuni") e di dati riguardanti le condizioni di salute (c.d. "dati sensibili") di un individuo fa di questo atto il documento sanitario contenente il maggior numero di informazioni personali» (in particolare p. 579), da cui poi si ricava, il profilo problematico della gestione dei dati.

Sussiste un'atavica diatriba sulla natura giuridica della cartella clinica.

Infatti secondo autorevole dottrina[270] la cartella clinica può essere considerata «come un *tertium genus*, collocandosi in una posizione intermedia tra scrittura privata e atto pubblico ed essendo ragionevolmente assimilabile ad una "certificazione amministrativa", infatti, essendo […] la cartella formata in momenti assistenziali diversi e per di più da operatori con ruoli professionali, cultura e competenze assai differenti, né essendovi alcun obbligo normativo di un'individuale sottoscrizione delle annotazioni apportate da costoro, non può che scaturirne un atto dai requisiti formali e sostanziali molto lontani da quelli che l'atto pubblico deve possedere ai sensi degli artt. 2699 e 2700 cod. civ.»[271].

La giurisprudenza[272], invece, è da tempo unanime nel qualificare la cartella clinica, sia su supporto cartaceo che informatico, come atto pubblico «facente piena prova fino a querela di falso del decorso clinico della malattia del paziente e dei vari fatti clinici che lo interessano». Ne deriva che per le attestazioni contenute

---

[270] F. BUZZI, C. SCLAVI, *La cartella clinica: atto pubblico, scrittura privata o "tertium genus"?* in *Rivista Italiana di Medicina legale*, 1997, p. 1182 ss.

[271] P. GUARDA, *Fascicolo Sanitario Elettronico e protezione dei dati personali, op. cit*.

[272] Cass. S.U. n. 7958 del 11.07.1992.

nella cartella clinica, redatta da un'azienda ospedaliera pubblica o da ente convenzionato con il servizio sanitario pubblico, è applicabile lo speciale regime di cui agli articoli 2699 e ss cod. civ. per quanto attiene «alle sole trascrizioni delle attività espletate nel corso di una terapia o di un intervento, restando, invece, non coperte da fede privilegiata le valutazioni, le diagnosi o, comunque, le manifestazioni di scienza o di opinione in essa espresse»[273].

Anche una parte di dottrina[274] aderisce a questa giurisprudenza appena citata, sottolineando che si tratta di «un'esplicazione del potere certificativo e partecipe della natura pubblica dell'attività sanitaria cui si riferisce».

Ad aggiungersi al contenuto tipico della cartella clinica c.d. tradizionale vi sono le caratteristiche della medesima in formato dematerializzato e cioè che il contenuto sia «organizzato come base per ogni successiva elaborazione e per garantire un adeguato livello di qualità», per cui sono utili un minimo di dati concordato, un dizionario di dati comune predefinito, i sistemi di codifica

[273] Cass. Civ. n. 37314 del 29.05.2013.

[274] C. SARTORETTI, *La cartella clinica tra diritto all'informazione e diritto alla privacy,* op.cit., p. 586.

condivisi e il loro formato standard, nonché «riportare le informazioni sull'esito delle terapie e sullo stato del paziente»[275]. Inoltre, il sistema di gestione delle cartelle cliniche elettroniche deve garantire la connessione con altri sistemi, per favorire l'interoperabilità dei dati sanitari[276], il collegamento con i registri istituzionali e, ove opportuno, anche con le cartelle cliniche dei familiari, nel rispetto delle regole relative alla privacy[277].

---

[275] G. CIPRIANO, *La cartella clinica digitale*, in *Il Diritto sanitario moderno*, 1, 2008, p. 19 s., secondo cui è necessario prestare attenzione anche alle «prestazioni del sistema», nel senso di garantire un'agevole immissione di dati, un loro rapido recupero e una disponibilità della cartella clinica in ogni momento della giornata. Come evidenzia P. GUARDA, *Fascicolo Sanitario Elettronico e protezione dei dati personali,* cit., p. 153 ss., diversa, rispetto a quanto si sta trattando, è la cartella infermieristica (art. 69, d.P.R. n. 384/1990), poiché si tratta di uno strumento «volto a contenere la registrazione dei dati e l'insieme dei documenti di pertinenza infermieristica sul caso oggetto di cura. Essa svolge anche funzioni di certificazione ed organizzazione di tutto il patrimonio informativo e delle attività assistenziali della persona, raccolte e/o eseguite dall'infermiere […]. Il nucleo centrale è caratterizzato dal piano di assistenza personalizzato».

[276] D. TUZZOLINO, *La portabilità dei dati sanitari* in A. THIENE e S. CORSO (a cura di), *La protezione dei dati sanitari, privacy e innovazione tecnologica tra salute pubblica e diritto alla riservatezza* – Atti del convegno, Rovigo 4 novembre 2022.

[277] G. CIPRIANO, *La cartella clinica digitale*, op. cit., Come evidenziato da A. Marchese in op. cit., per creare una cartella clinica elettronica è necessario disporre di un software apposito con il quale provvedere alla sua compilazione ed alla sua validazione (mediante strumenti di firma elettronica avanzata) e, successivamente, alla sua conservazione all'interno di un *digital archive* (non fisico ma virtuale) che gli consenta di raggiungere la medesima (se non addirittura più elevata) efficacia probatoria già riconosciuta alla cartella in formato cartaceo. L'opzione per la cartella clinica elettronica anziché per quella informatica è, poi, strettamente legata al tema della

Dal punto di vista della sicurezza, la cartella clinica elettronica si serve del protocollo e-PR (*elecronic Patient Record*)[278] che

sicurezza dei dati contenuti, atteso che gli strumenti digitali offrono al riguardo una peculiare innovatività in termini di efficienza ed efficacia.

[278] I protocolli i-PR (*internet Patient Records*), dei quali il citato *electronic Patient Record* (e-PR) è quello più noto, rappresentano – al momento – l'ultima frontiera in tema di protezione informatica dei dati clinici; basati su una tecnologia di interscambio dati e di criptazione digitale, consentono una perfetta operabilità su tutti i forms (le parti da compilare) della cartella elettronica garantendo al contempo la simultanea registrazione degli accessi dei singoli operatori e la loro precisa identificazione mediante una procedura di riconoscimento che prevede l'utilizzo di credenziali elettroniche avanzate. Sulla validità di tale metodologia, comunque in costante evoluzione ed aggiornamento, cfr. C. CAPE, *Electronic Patient Record (EPR) Benefits realisation case study*, in *Oxford University Hospitals NHS Trust, Health and Social Care Information Centre*, Oxford, 2015, pp. 1-92, spec. p. 8 secondo cui «[i]t is well recognised that healthcare information technology (IT) is a critical enabler of improved care and efficiency across health and social care, 'Better use of data and technology has the power to improve health, transforming the quality and reducing the cost of health and care services. It can […] reduce the administrative burden for care professionals and support the development of new medicines and treatments. In recent years there has been an increasing focus on the need to account for the benefits enabled by major investments in IT systems. These IT systems have been in use for a number of years in many trusts and it is widely thought the systems and related change efforts have yet to deliver significant benefits that were expected» ed ancóra «[t]his system comprises a series of software applications which bring together key clinical and administrative data in one place. The system is going live in phases. There are a number of benefits from implementing EPR, not least the ability for clinicians to view a patient's medical record when and where they need it, without having to wait for the paper record to be brought or found. Further benefits include greater legibility of key clinical information and increased accuracy of data. For example, the Trust's award-winning Positive Patient Identification (PPIP) technology enables clinicians to identify patients at the bedside by barcode scanning of their wrists. This means that by using the scanner, a small handheld device, an instant test request can be generated and printed at the bedside. Replacing

permette sia di monitorare le patologie di più pazienti simultaneamente, contribuendo a ridurre i tempi necessari per la diagnosi, sia di tenere aggiornati i dati del singolo paziente, evitando il rischio di duplicare esami già eseguiti ovvero "superati" da altri accertamenti.

Sebbene si parlerà diffusamente nei paragrafi che seguono del Fascicolo sanitario elettronico, si ritiene opportuno individuare già in questa sede la differenza intercorrente tra lo stesso e la cartella clinica elettronica.

Infatti, se il primo è funzionale a rappresentare la storia clinica di un paziente e raccoglie ogni forma di informazione sanitaria proveniente da ospedali, ambulatori, studi medici nell'arco della sua intera vita, la seconda è un documento digitale predisposto dalla singola struttura sanitaria presso la quale è in cura un paziente in un determinato momento della vita[279], per cui si può affermare che la CCE sia una parte del FSE.

Tra i vantaggi della CCE vi è senza dubbio la dematerializzazione del documento cartaceo, in ossequio a quanto disposto dall'art. 47-*bis*, 1 comma del d.l. n. 5/2012, che migliora la qualità dei servizi

---

paper forms with the new electronic requesting and labelling system is both quicker and reduces the risk of samples being mislabelled».

[279] N. POSTERARO, *La digitalizzazione della sanità in Italia: uno sguardo al Fascicolo Sanitario Elettronico (anche alla luce del Piano Nazionale di Ripresa e Resilienza)*, in *federalismi.it*, 26/2021, p. 197 ss.

di cui necessita il paziente e ne riduce enormemente i costi[280], anche se è necessario ricordare quanto detto dal Gruppo di Articolo 29 in occasione del Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche del 15 febbraio 2007 e cioè che «i sistemi di CCE possono assicurare maggiore qualità e sicurezza dell'informazione medica di quanto consentano le forme tradizionali di documentazione. Tuttavia, parlando di tutela dei dati, va sottolineato che i sistemi di CCE danno la possibilità non solo di trattare una quantità maggiore di informazioni di natura personale (ad esempio in nuovi contesti o per aggregazione), ma anche di rendere i dati del paziente più facilmente disponibili ad una cerchia di destinatari più ampia di prima»[281].

---

[280] S. CORONATO, *Gli strumenti necessari al processo di digitalizzazione del S.S.N., op. cit.,* vedasi tra gli altri, A. Marchese in op. cit. secondo cui «La digitalizzazione delle procedure comporta infatti: - a) un risparmio diretto in termini di azzeramento dei costi di stampa e archiviazione; stimati rispettivamente circa 10 Euro-cent e 20 Euro-cent per singolo foglio (il più delle volte utilizzato sul solo fronte e non anche sul retro); - b) un risparmio indiretto in termini di (tempo e) spese di trasmissione, apprezzabile ogni qualvolta le informazioni mediche contenute nella cartella clinica necessitino di essere portate a conoscenza di altri soggetti (ad es. altri specialisti) con il beneficio aggiuntivo di un potenziamento dell'efficienza complessiva del sistema secondo i canoni della c.d. «diagnosi aggregata».

[281] Gruppo di Articolo 29 in occasione del Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche del 15 febbraio 2007.

Inoltre, in letteratura è stato evidenziato un ulteriore vantaggio e cioè l'eliminazione del problema relativo alla sicurezza degli archivi per custodire le informazioni sanitarie[282] in quanto la digitalizzazione della cartella clinica impedisce il suo materiale deposito e quindi esclude il danneggiamento o la distruzione imputabili ad eventi umani o naturali.

Parimenti, con la dematerializzazione è possibile condividere la CCE con i medici specialisti o con il MMG con evidenti vantaggi sia per il paziente[283] – che verrà curato in maniera specifica avendo il sanitario un quadro chiaro e puntuale della condizione – sia sul piano del risparmio delle spese.

Da ultimo, è stata prevista la possibilità della cd. interconnessione tra i sistemi, infatti la Raccomandazione UE 2019/243 del 6 febbraio 2019 prevede «lo sviluppo di un formato europeo di scambio delle cartelle cliniche elettroniche al fine di consentire che, nell'Unione, i dati sanitari elettronici siano accessibili e

---

[282] L. FERRARO, op. cit.

[283] Secondo G. CIPRIANO, op. cit., «gli ultimi 30 anni hanno evidenziato, con dati quantitativi, che spesso la cartella clinica cartacea non è disponibile durante la visita (fino al 30 % delle visite), e che per esempio gli esami di laboratorio vengono molte volte ripetuti perché i risultati non vengono resi disponibili al medico in modo tempestivo. Quando le cartelle sono disponibili, spesso alcuni dati essenziali non sono presenti. Ad esempio, in uno studio sui medici di medicina generale è stato riscontrato che l'età del paziente mancava nel 10% dei casi, che i farmaci non erano trascritti nel 30%, che la diagnosi mancava nel 40%».

scambiabili in maniera sicura, interoperabile e transfrontaliera» visto che «ogni anno si registrano oltre due milioni di casi in cui un cittadino residente in uno Stato membro richiede assistenza sanitaria in un altro»[284].

In questa sede si ritiene opportuno richiamare il progetto del settembre 2020 denominato "*X-eHealth-eXchanging electronic Health records in a common framework"* che mira a sviluppare «una intelaiatura per un formato di scambio di cartelle cliniche elettroniche, interoperabile, sicuro e transfrontaliero, al fine di gettare le basi per il progresso del settore dell'*e-Health*»[285]. Focalizzato sui servizi transfrontalieri, il consorzio europeo, guidato dal Portogallo, promuove uno spazio comune europeo interoperabile per i dati sanitari comuni per i cittadini e gli operatori sanitari, in conformità con le normative sulla privacy e sulla sicurezza informatica[286].

Si tratta di un progetto antesignano dello Spazio europeo dei dati sanitari – EHDS di cui si parlerà dettagliatamente nei paragrafi che seguono.

---

[284] Considerando n. 3 della Raccomandazione UE 2019/243 del 6 febbraio 2019.

[285] https://cordis.europa.eu/project/id/951938/reporting

[286] https://www.fascicolosanitario.gov.it/progetto-x-ehealth

2.1.3. Strumenti di carattere nazionale di attuazione della sanità digitale: il Fascicolo sanitario elettronico.

Accanto alla Cartella Clinica Elettronica nel d.l. n. 179 del 2012, all'art. 12[287], viene istituito il Fascicolo sanitario elettronico e i

[287] Fascicolo sanitario elettronico, sistemi di sorveglianza nel settore sanitario e governo della sanità digitale 1. Il fascicolo sanitario elettronico (FSE) è l'insieme dei dati e documenti digitali di tipo sanitario e sociosanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito, riferiti anche alle prestazioni erogate al di fuori del Servizio sanitario nazionale. Ai fini del presente comma, ogni prestazione sanitaria erogata da operatori pubblici, privati accreditati e privati autorizzati è inserita, entro cinque giorni dalla prestazione medesima, nel FSE in conformità alle disposizioni del presente articolo. 2. Il FSE è istituito dalle regioni e province autonome, conformemente a quanto disposto dai decreti di cui al comma 7, entro il 30 giugno 2015, nel rispetto della normativa vigente in materia di protezione dei dati personali, a fini di: a) diagnosi, cura e riabilitazione; a-bis) prevenzione; a-ter) profilassi internazionale; b) studio e ricerca scientifica in campo medico, biomedico ed epidemiologico; c) programmazione sanitaria, verifica delle qualità delle cure e valutazione dell'assistenza sanitaria. *((c-bis) valutazioni e accertamenti sanitari per il riconoscimento di prestazioni assistenziali e previdenziali.))* 2-bis. Per favorire la qualità, il monitoraggio, l'appropriatezza nella dispensazione dei medicinali e l'aderenza alla terapia ai fini della sicurezza del paziente, è istituito il dossier farmaceutico quale parte specifica del FSE, aggiornato a cura della farmacia che effettua la dispensazione. 3. Il FSE è alimentato con i dati degli eventi clinici presenti e trascorsi di cui al comma 1 in maniera continuativa e tempestiva, senza ulteriori oneri per la finanza pubblica, dai soggetti e dagli esercenti le professioni sanitarie che prendono in cura l'assistito sia nell'ambito del Servizio sanitario nazionale e dei servizi sociosanitari regionali sia al di fuori degli stessi, nonché, su iniziativa dell'assistito, con i dati medici in possesso dello stesso. Il sistema del FSE aggiorna contestualmente anche l'indice di cui al comma 15-ter e alimenta l'ecosistema dati sanitari (EDS) di cui al comma 15-quater.

sistemi di sorveglianza nel settore sanitario, definito in dottrina come «un supporto informatico contenente dati personali di natura amministrativa, sociale e sanitaria che riflettono un'immagine passata, presente e futura dello stato di salute di una persona al fine di facilitarne l'accesso e l'utilizzo da parte dei terzi autorizzati»[288], sin dalla sua istituzione è stata sottolineata l'innovatività e il suo ruolo di "semplificatore" del trattamento sanitario, essendo «una nuova forma di comunicazione e gestione dei dati del paziente che permette di far confluire in unico documento informatizzato tutti i dati sanitari di quest'ultimo, in modo da facilitare l'accesso e l'utilizzo degli stessi da parte dei terzi autorizzati al momento del bisogno»[289].

Nelle "Linee guida in tema di Fascicolo sanitario elettronico (FSE) e di dossier sanitario" del 16 luglio 2009, il Garante per la protezione dei dati personali lo qualificò come «condivisione informatica, da parte di distinti organismi o professionisti, di dati e documenti sanitari che vengono formati, integrati e aggiornati nel tempo da più soggetti, al fine di documentare in modo unitario e in termini il più possibile completi un'intera gamma di diversi

---

[288] S. CORSO, *La protezione dei dati sanitari, op. cit.* e V. PEIGNÈ, *Il fascicolo sanitario elettronico, verso una «trasparenza sanitaria» della persona* in Riv. It. Med. Leg., 2012, p. 105.

[289] S. CORSO, *La protezione dei dati sanitari*, *op. cit.,* e G. COMANDÈ, L. NOCCO, V. PEIGNÈ, *Il Fascicolo sanitario elettronico: uno studio multidisciplinare*, in Riv. It. Med. Leg. 2012, p. 105.

eventi sanitari riguardanti un medesimo individuo e, in prospettiva, l'intera sua storia clinica», riferendosi «all'insieme dei diversi eventi clinici occorsi ad un individuo, messo in condivisione logica dai professionisti o organismi sanitari che assistono l'interessato, al fine di offrirgli un migliore processo di cura»[290].

Sul sito istituzionale dell'Agenzia per l'Italia Digitale (AgID) dedicato al FSE, esso viene definito come «lo strumento attraverso il quale il cittadino può tracciare e consultare tutta la storia della propria vita sanitaria, condividendola con i professionisti sanitari per garantire un servizio più efficace ed efficiente»[291].

La definizione dell'art. 12, comma 1, del d.l. n. 179 del 2012 è stata modificata dal d.l. n. 34 del 2020 che prevede si tratti di «un insieme di dati e documenti digitali di tipo sanitario e sociosanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito, riferiti anche alle prestazioni erogate al di fuori del Servizio Sanitario Nazionale».

2.1.3.1. La genesi del FSE.

---

[290] "Linee guida in tema di Fascicolo sanitario elettronico (FSE) e di dossier sanitario" del Garante per la protezione dei dati personali del 16 luglio 2009 n. 25, consultabili in https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1634116

[291] Definizione presente su www.fascicolosanitario.gov.it

La genesi del FSE nasce dall'esigenza – maturata da lungo tempo non soltanto a livello nazionale, italiano e straniero ma anche sovranazionale[292] – avvertita sia dai pazienti sia dal personale sanitario di una «più agevole accessibilità ai dati relativi alla salute del paziente, per il miglior perseguimento dello scopo di cura»[293]. Sin da subito viene sottolineata la centralità della persona e la tutela dei suoi dati personali[294].

Il modello di FSE sviluppato in Italia si caratterizza per l'infrastruttura, basata su una rete nazionale di architetture regionali, i cui nodi sono costituiti dalle Regioni stesse[295].

---

[292] Si veda P. GUARDA, I dati sanitari, in V. CUFFARO – R. D'ORAZIO – V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, p. 613 e ss. Cfr. le Comunicazioni della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale e al Comitato delle Regioni, COM/2004/0356, Sanità elettronica – migliorare l'assistenza sanitaria dei cittadini europei: piano d'azione per uno spazio europeo della sanità elettronica, 30 aprile 2004, e COM/2005/0229, i2010 – Una società dell'informazione per la crescita e l'impiego, 1° giugno 2005, entrambe consultabili in www.eur-lex.europa.eu.
Vedasi anche G. VICARELLI – M. BRONZINI, *La sanità digitale: dimensioni di analisi e prospettive di ricerca* in *Politiche sociali*, 2018, fasc. 2, p. 147 ss. Spec. 150.

[293] P. GUARDA, *Fascicolo Sanitario Elettronico e protezione dei dati personali*, op.cit., p. 26.

[294] S. CORSO, *Sanità digitale e riservatezza. Interpretazioni sul Fascicolo sanitario elettronico* in A. THIENE e S. CORSO (a cura di), *La protezione dei dati sanitari, privacy e innovazione tecnologica tra salute pubblica e diritto alla riservatezza*, in Atti di Convegno – Rovigo 4 novembre 2022, p. 96.

[295] *Ibidem* e vedasi anche Ministero della salute, *Il fascicolo sanitario elettronico, Linee guida nazionali*; V. PEIGNÈ, *Il fascicolo sanitario*

Sin dalla sua istituzione è emersa la potenzialità di tale strumento, dal momento che al fine primario di cura si è affiancato quello di analisi e di gestione[296].

Inoltre, è possibile soddisfare un'esigenza di natura economica, dal momento che l'efficienza perseguita con l'utilizzo di tale strumento consentirebbe una riduzione degli errori medici e la conseguente diminuzione dei costi[297] e la conservazione degli esiti e la loro non dispersione permetterebbe di evitare la reiterazione di esami diagnostici già effettuati con minori spese per le strutture sanitarie e una conseguente efficiente allocazione delle risorse disponibili[298].

---

elettronico verso una «trasparenza sanitaria» della persona, op. cit., che riporta come modelli differenti quello francese e quello inglese che si caratterizzano rispettivamente per un'architettura centralizzata a livello nazione e per una mista; sul punto si veda anche V. PEIGNÈ, *Verso il fascicolo Sanitario Elettronico: presentazione della riforma francese* in *Dir. Internet*, 2007, p. 626 e P. COLETTI, *L'innovazione digitale nell'amministrazione pubblica: le azioni delle Regioni*, in *Amministrare*, 2013, fasc. 3, p. 463 ss.

[296] S. CORSO, *Sanità digitale e riservatezza. Interpretazioni sul Fascicolo sanitario elettronico*, op. cit.

[297] G. COMANDÈ, *Ricerca in sanità e data protection: un puzzle…risolvibile*, in *Riv. It. Med. Leg*. 2019, p. 187 ss; N. BUSCA, *Il trattamento dei dati sanitari nell'ambito della ricerca e della sperimentazione clinica* in www.rivistaresponsabilitamedica.it, 26 settembre 2020.

[298] V. PEIGNÈ, *Il fascicolo sanitario elettronico, verso una «trasparenza sanitaria» della persona, op. cit.*

Quanto alla regolamentazione, è opportuno richiamare il D.P.C.M. 29 settembre 2015, n. 178[299] , recante "Regolamento in materia di fascicolo sanitario elettronico"[300].

Invece, con riferimento alla progettazione – prevista dall'art. 12 comma 15 ter del d.l. n. 179 del 2012 da parte dell'Agenzia per l'Italia Digitale (AgID) di concerto con il Ministero della salute, il Ministero dell'economia e delle finanze e le Regioni – di un'infrastruttura nazionale per garantire l'interoperabilità dei FSE attraverso l'utilizzo del Sistema della Tessera sanitaria, l'AgID ha emanato una circolare, la n. 4 del 1 agosto 2017 rubricata "Documento di progetto dell'Infrastruttura Nazionale per l'Interoperabilità dei Fascicoli Sanitari Elettronici (art. 12 – comma 15-*ter* – d.l. 179/2012)".

Secondo le ulteriori modifiche apportate nel 2022 all'art. 12, la progettazione di tale infrastruttura è stata affidata all'AGENAS, invece che all'Agenzia per l'Italia digitale, ma, sia nella fase di attuazione del Piano nazionale di ripresa e resilienza e fino al 31 dicembre 2026, verrà curata dalla struttura della Presidenza del Consiglio dei ministri competente per l'innovazione tecnologica e

[299] Gazzetta Ufficiale n. 263 del 11 novembre 2015"

[300] Per un approfondimento si richiama A. THIENE, *Salute, riserbo e rimedio risarcitorio* in *Rivista italiana di medicina legale e del diritto in campo sanitario*, 4/2015.

la transizione digitale di concerto con il Ministero della salute e il Ministro dell'economia e delle finanze (comma 15-*ter.1*).

Questa infrastruttura dovrà inoltre garantire l'identificazione dell'assistito tramite l'allineamento con l'Anagrafe Nazionale degli Assistiti (ANA).

2.1.3.2. La disciplina del FSE "tradizionale".

Sebbene la disciplina del Fascicolo sanitario elettronico sia stata oggetto di plurime modifiche normative, si è ritenuto opportuno focalizzare l'attenzione dello studio sulla questione dell'alimentazione con i dati e della base giuridica prevista dalla normativa, la cui centralità si è affievolita e cioè il consenso.

Ai sensi dei commi 1 e 3 del citato e rinovellato art. 12, si legge che «il FSE viene alimentato con i dati degli eventi clinici presenti e trascorsi riguardanti l'assistito, inerenti anche alle prestazioni erogate al di fuori del Servizio sanitario nazionale, in maniera continuativa e tempestiva dai soggetti e dagli esercenti le professioni sanitarie che hanno in cura l'assistito stesso, nonché, su iniziativa di quest'ultimo, con i dati medici in suo possesso», inoltre, costituisce parte essenziale ed integrante il dossier

farmaceutico[301] per favorire «qualità, monitoraggio e appropriatezza nella dispensazione dei medicinali e aderenza alla terapia per la sicurezza del paziente e aggiornamento a cura della farmacia che effettua la dispensazione»[302].

Quanto al contenuto del FSE, si può distinguere un "nucleo minimo" di dati e documenti e quelli integrativi che si compone di: dati identificativi e amministrativi dell'assistito[303], referti, verbali di pronto soccorso, lettere di dimissioni, profilo sanitario sintetico[304], dossier farmaceutico, consenso o diniego alla donazione degli organi e tessuti.

---

[301] Art. 12, comma 2-bis, d.l. n. 179/2012.

[302] Art. 5, D.L. 69 del 2013.

[303] Art. 21 del d. P.C.m. n. 178/2015 secondo cui «1. Il FSE deve garantire l'allineamento dei dati identificativi degli assistiti con i dati contenuti nell'Anagrafe nazionale degli Assistiti (ANA) e, nelle more dell'istituzione dell'ANA, nelle anagrafi sanitarie regionali, allineate con l'anagrafe nazionale della popolazione residente di cui all'articolo 62 del CAD. I dati necessari per la corretta identificazione dell'assistito in fase di alimentazione del FSE sono elencati nel disciplinare tecnico. 2. I dati amministrativi dell'assistito sono costituiti dalle informazioni relative alla posizione dell'assistito nei confronti del SSN, sia con riferimento alla rete d'offerta del SSN che ad altre informazioni, correlate all'organizzazione della regione o provincia autonoma di assistenza. I dati amministrativi necessari per la corretta individuazione della posizione amministrativa dell'assistito nei confronti del SSN sono elencati nel disciplinare tecnico.

[304] Art. 3, del d. P.C.m. n. 178/2015 secondo cui «1. Il profilo sanitario sintetico, o "patient summary", è il documento sociosanitario informatico redatto e aggiornato dal MMG/PLS, che riassume la storia clinica dell'assistito e la sua situazione corrente conosciuta. 2. La finalità del profilo sanitario sintetico è di favorire la continuità di cura, permettendo un rapido inquadramento dell'assistito al momento di un contatto con il SSN. 3. I dati

I dati e i documenti integrativi comprendono invece: «prescrizioni, prenotazioni, cartelle cliniche, bilanci di salute, assistenza domiciliare, piani diagnostico-terapeutici, assistenza residenziale e semiresidenziale, erogazione farmaci, vaccinazioni, prestazioni di assistenza specialistica, prestazioni di emergenza/urgenza, prestazioni di assistenza ospedaliera in regime di ricovero, certificati medici, taccuino personale dell'assistito»[305], «relazioni relative alle prestazioni erogate dal servizio di continuità assistenziale, autocertificazioni, partecipazioni a sperimentazioni cliniche, esenzioni, prestazioni di assistenza protesica, dati a supporto delle attività di telemonitoraggio, dati a supporto delle attività di gestione integrata dei percorsi diagnostico-terapeutici»[306].

---

essenziali che compongono il profilo sanitario sintetico sono quelli individuati nel disciplinare tecnico allegato che costituisce parte integrante del presente decreto, di seguito denominato disciplinare tecnico. 4. In caso di variazione del MMG/PLS, sarà facoltà del nuovo MMG/PLS di mantenere il documento precedentemente redatto oppure di redigerne uno nuovo. Ogni modifica o aggiornamento al profilo sanitario sintetico implica, comunque, la creazione di una nuova versione, separata da quella originaria.

[305] Articolo 2 - Contenuti del Fascicolo Sanitario Elettronico.

[306] 1. Il taccuino personale dell'assistito è una sezione riservata del FSE all'interno della quale è permesso all'assistito di inserire dati e documenti personali relativi ai propri percorsi di cura, anche effettuati presso strutture al di fuori del SSN. 2. I dati e i documenti inseriti nel taccuino personale dell'assistito sono informazioni non certificate dal SSN e devono essere distinguibili da quelli inseriti dai soggetti di cui all'articolo 12.

I dati e i documenti appena menzionati possono essere consultati, per le medesime finalità di cura, secondo le indicazioni della normativa relativa al FSE cd. tradizionale, solo con il consenso dell'assistito[307] e sempre nel rispetto del segreto professionale, salvo i casi di accesso in emergenza[308].

È opportuno sottolineare che il mancato consenso non può pregiudicare in alcun caso il diritto alla prestazione sanitaria.

Come dispone l'art. 13 del d.P.C.M. citato «l'accesso alle informazioni del fascicolo da parte dei menzionati soggetti che prendono in cura l'assistito è ammesso se, oltre all'esplicito consenso da parte sua, le informazioni da trattare sono esclusivamente quelle pertinenti al processo di cura in atto e i soggetti che accedono alle informazioni rientrano nelle categorie di soggetti abilitati alla consultazione indicate dall'assistito e sono effettivamente coinvolti nel processo di cura. In una sezione

---

[307] L'assistito, negando il consenso all'accesso da parte del professionista pur per finalità di cura, può selezionare il personale medico che accede alle informazioni del suo fascicolo.

[308] 1. Nei casi di cui all'articolo 82 del Codice in materia di protezione dei dati personali, gli operatori del SSN e dei servizi sociosanitari regionali possono accedere al FSE a seguito di esplicita dichiarazione da loro sottoscritta, consultando le sole informazioni rese visibili dall'assistito, ai sensi delle disposizioni degli articoli 5 e 8. Tali dichiarazioni e gli accessi
ai dati sono memorizzati in maniera tale che l'assistito possa verificarli, consultando il proprio FSE.

apposita viene registrato ogni accesso alle informazioni del fascicolo»[309].

Un approfondimento a parte merita l'affievolimento della centralità della base giuridica del consenso all'alimentazione del FSE.

L'infografica del Garante della Privacy del 19 giugno 2020 prevede che «con i recenti interventi di semplificazione, il FSE viene automaticamente alimentato, in modo che lo stesso assistito possa facilmente consultare i propri documenti socio-sanitari, anche se generati da strutture sanitarie situate al di fuori della Regione di appartenenza, grazie all'interoperabilità assicurata dal Sistema Tessera sanitaria»[310].

Le modifiche normative apportate alla disciplina del FSE "tradizionale" sembrano aver «sancito il passaggio ermeneutico di questa figura cioè del FSE, da strumento principalmente per la persona e la tutela dei suoi diritti fondamentali, primo fra tutti quello alla sua salute, a strumento primariamente per la pubblica amministrazione e la garanzia di maggiore efficienza, nel contesto del funzionamento del Servizio Sanitario nazionale»[311].

---

[309] Art. 13 del D.P.C.M. 178/2015.
[310] Infografica del Garante della Privacy del 19 giugno 2020.
[311] S. CORSO, *Modifiche alla disciplina sul trattamento dei dati relativi alla salute*, in www.rivistaresponsabilitamedica.it, 29 gennaio 2022.

Infatti, l'esistenza e la prevalenza dell'interesse pubblico nel settore della sanità pubblica – tenuto conto dell'ampiezza delle materie in cui l'interesse pubblico può qualificarsi rilevante ai sensi dell'art. 2-*sexies* del 2 comma – rende – di fatto – una clausola genere l'esistenza di un interesse pubblico che fa eccezione al divieto di trattamento.

Per cui si può affermare, aderendo alla tesi sostenuta da autorevole dottrina[312] che il consenso – inteso quale base giuridica legittimante il trattamento dei dati personali – sia rimasto solo un "mito".

2.1.4. ... il Fascicolo sanitario elettronico 2.0

Il 24 ottobre 2023 è stato pubblicato in Gazzetta Ufficiale il decreto del Ministero della salute del 7 settembre 2023 rubricato "Fascicolo sanitario elettronico 2.0", una sorta di aggiornamento

---

[312] S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, Bologna, 1973, pp. 45 ss.; Secondo G. ALPA, in D'ORAZIO, FINOCCHIARO, POLLICINO, RESTA (a cura di), *Codice della Privacy e Data protection*, Milano, 2021, sub art. 1, d. lgs. 30 giugno 2023, n. 196, «è dunque fallace rimettere il controllo al semplice consenso dell'individuo alla raccolta dei dati che lo riguardano. Questa è un'altra regola che Rodotà enuncia nel suo programma di intervento legislativo, ma è ben consapevole del fatto che il consenso non basta: perché una volta catalogate, organizzate, manipolate, conservate e messe in circolazione, al consenso occorre affiancare il controllo, di qui, per l'appunto il titolo del libro che parla di elaboratori e controllo sociale».

tecnologico e giuridico della "precedente" figura dinnanzi analizzata.

Il bisogno di procedere alla regolamentazione e di adeguare il diritto alla tecnologia è testimoniato dall'attenzione dedicata dagli studi giuridici agli sviluppi scientifici sintomo di «una maturata consapevolezza del legame che avvince sempre più la tecnica e il diritto, facendosi talvolta persino compenetrazione»[313], passando «dagli elaboratori elettronici»[314] «all'intelligenza artificiale»[315].

---

[313] N. IRTI, *Il diritto nell'età della tecnica*, Napoli, 207, Tra gli altri, G. ZACCARIA, *Normatività giuridica e normatività algoritmica* in Aa. Vv. *Liber Amicorum per Paolo Zatti*, Napoli 2023, p. 159 ss; P. PERLINGIERI, *Note sul «potenziamento cognitivo»* in *Tecnologie e diritto*, 2021, p. 209 ss.

[314] S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, Bologna, 1973.

[315] Gli studi giuridici sul tema ormai non si contano. Ci si limita qui a ricordare E. FAZIO, *Intelligenza artificiale e diritti della persona*, Napoli, 2023; AA.VV., in C. CAMARDI (a cura di), *La via europea per l'intelligenza artificiale.* Atti del convegno del progetto dottorale di alta formazione in scienze giuridiche, Ca' Foscari Venezia, 25-26 novembre 2021, Padova, 2022; AA.VV., in C. CASONATO, M. FASAN e S. PENASA (a cura di), *Diritto e intelligenza artificiale*, sezione monografica in DPCE online, 2022, p. 155 ss.; D. DI SABATO, *I sistemi di IA tra esigenze di tutela della persona e efficienza del mercato*, in *Teoria e prassi del diritto*, 2022, p. 201 ss.; E. FROSINI, *L'orizzonte giuridico dell'intelligenza artificiale*, in Dir. inf., 2022, p. 5 ss.; AA.VV., in G. M. RICCIO, G. ZICCARDI e G. SCORZA (a cura di), *Intelligenza artificiale. Profili giuridici*, Padova, 2022; AA.VV., in A. D'ALOIA (a cura di), *Intelligenza artificiale e diritto. Come regolare un mondo nuovo*, Milano, 2021; AA.VV., in G. ALPA (a cura di), *Diritto e intelligenza artificiale,* Pisa, 2020; AA.VV., in U. RUFFOLO (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020; AA.VV., *AI: profili giuridici. Intelligenza Artificiale: criticità emergenti e sfide per il giurista* in *BioLaw Journal – Rivista di BioDiritto*, 2019, p. 205 ss.

Tra le novità di maggior rilievo introdotte dal d.l. 27 gennaio 2022 n. 4 (decreto sostegni *ter*), convertito con modificazioni con l. 28 marzo 2022, n. 25, incidendo ancora sul testo dell'art. 12 del d.l. n. 179 del 2012 (plurime volte citato ndr.), vi è la previsione dell'inserimento nel FSE di «ogni prestazione sanitaria – erogata tanto da operatori pubblici, quanto da privati accreditati o privati autorizzati – entro cinque giorni dalla prestazione medesima»[316]; «la realizzazione da parte del Ministero della salute dell'Ecosistema dei Dati Sanitari (EDS), alimentato dai dati trasmessi dalle strutture sanitarie e socio-sanitarie, dagli enti del Servizio sanitario nazionale e da quelli resi disponibili tramite il sistema Tessera Sanitaria, oltreché dal FSE stesso[317]; l'assunzione, da parte di AGENAS, del ruolo di Agenzia nazionale per la sanità digitale e l'acquisto di specifiche funzioni elencate tra cui quella di «promozione e realizzazione di servizi sanitari e sociosanitari basati sui dati, destinati rispettivamente agli assistiti e agli operatori sanitari, al fine di assicurare strumenti di consultazione dei dati dell'EDS omogenei sul territorio nazionale» e di «gestione della piattaforma nazionale di telemedicina»[318].

[316] Art. 12, comma 1, d.l. n. 179/2012.
[317] Art. 12, comma 15-*quater*, d.l. n. 179/2012.
[318] Art. 12, comma 15-*undecies*, d.l. n. 179 del 2012.

A seguito di tali modifiche, infatti, la rubrica dell'istituto in oggetto è stata modificata in «Fascicolo sanitario elettronico, sistemi di sorveglianza nel settore sanitario e governo della sanità digitale».

Infatti, il "nuovo" FSE è regolato da una molteplicità di fonti di diversa provenienza eterogenee per intenti e per contenuti che sono lo specchio di una tutela multilivello[319] del diritto tipica di svariate materie, prima fra tutte la protezione dei dati personali[320].

I contenuti del FSE vengono riorganizzati.

Infatti, se l'art. 2 del d.p.c.m. n. 178/2015 distingueva con due elenchi il nucleo minimo – uguale per tutti i fascicoli – dai dati e documenti integrativi – che invece erano imputabili alle politiche sanitarie delle singole regioni – per un totale di ventinove categorie di contenuti, l'art. 3 del decreto FSE 2.0 fa riferimento ad un elenco di tredici categorie di contenuti[321].

---

[319] G. CERRINA FERONI, *Sanità digitale e assetti istituzionali*, G. CERRINA FERONI (a cura di) in *Le nuove frontiere della medicina, assetti istituzionali e gestione dei dati*, pp.15-32, 2024.

[320] C. COLAPIETRO, *Il diritto alla protezione dei dati personali in un sistema delle fonti multilivello. Il Regolamento UE 2016/679 parametro di legittimità della complessiva normativa italiana sulla privacy*, Napoli, 2018. Cfr. R. D'ORAZIO, La tutela multilivello del diritto alla protezione dei dati personali e la dimensione globale, in V. CUFFARO, R. D'ORAZIO e V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, p. 61 ss.

[321] Il dettaglio dei singoli contenuti è riportato nell'allegato A del decreto.

Permangono il profilo sanitario sintetico e il taccuino personale dell'assistito, di cui agli artt. 4 e 5 del decreto FSE 2.0, ma in una veste diversa, più favorevole per i diritti dell'assistito[322] e con maggiore aderenza alle nuove tecnologie[323].

Il dossier farmaceutico è stato eliminato e sarà regolato dal decreto attuativo delle disposizioni di cui al comma 15-quater dell'art. 12 d.l. n. 179/2012, come servizio reso disponibile dall'EDS.

Inoltre, è stato previsto uno speciale regime per taluni dati relativi alla salute, considerati di spiccata sensibilità.

L'art. 6 del decreto FSE 2.0, rubricato come l'art. 5 del D.P.C.M. n. 178/2015 "Dati soggetti a maggiore tutela dell'anonimato" sancisce che siano ostensibili solo all'assistito «i dati e i documenti sanitari e socio-sanitari disciplinati dalle disposizioni normative a tutela delle persone sieropositive, delle donne che si sottopongono

---

[322] Il *patient summary* rispetta esplicitamente il diritto all'oscuramento e l'assistito può consultare i vari profili redatti nel tempo. Ai sensi dall'art. 4, comma 6°, del decreto FSE 2.0, in caso di variazione del medico di medicina generale o del pediatra di libera scelta, il nuovo MMG/PLS redige un nuovo *patient summary.*

[323] Nel taccuino personale potranno confluire i dati generati da dispositivi medici e wearable. Il FSE si apre quindi alla c.d. *m-Health* e al connesso uso di App, per smartphone, smartwatch e tablet. V. la ricostruzione critica di C. IRTI, *L'uso delle "tecnologie mobili" applicate alla salute: riflessioni al confine tra la forza del progresso e la vulnerabilità del soggetto anziano*, op.cit. p. 32 ss. Cfr. I. RAPISARDA, *La privacy sanitaria alla prova del mobile ecosystem. Il caso delle app mediche*, in *Le nuove leggi civili commentate*, 2023, p. 184 ss.

.

a un'interruzione volontaria di gravidanza, delle vittime di atti di violenza sessuale o di pedofilia, delle persone che fanno uso di sostanze stupefacenti, di sostanze psicotrope e di alcool, delle donne che decidono di partorire in anonimato, nonché i dati e i documenti riferiti ai servizi offerti dai consultori familiari»[324].

Sarà l'assistito a poter decidere se rendere tali referti visibili a soggetti terzi, nell'esercizio dei diritti di cui all'art. 9[325].

Ad ogni modo, non è possibile rimuovere il documento oscurato dal FSE, dal momento che non è prevista la possibilità di cancellare e rimuovere dati o documenti che sono stati caricati sul Fascicolo sanitario elettronico, indipendentemente dal loro contenuto effettivo o dalla sensibilità della relativa informazione.

Un altro elemento di rilievo è il riconoscimento – previsto dall'art. 12, comma 3 – di una responsabilità per coloro i quali sono tenuti all'alimentazione del FSE per «la mancata, intempestiva o inesatta alimentazione stessa», in ottemperanza alle indicazioni espresse dal Garante della Privacy nel provvedimento n. 294 del 2022[326]

---

[324] Art. 6 del decreto FSE 2.0.

[325] Nell'art. 9 viene riconfermato il diritto all'oscuramento, il cui esercizio comporta che i documenti individuati dall'assistito e quelli logicamente connessi non siano più visibili nel FSE, compreso lo stesso oscuramento (c.d. oscuramento dell'oscuramento). L'oscuramento non è irreversibile e può essere revocato.

[326] Per la consultazione, https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9802729

circa l'assenza di «una vera e propria obbligatorietà di caricare dati e documenti nel FSE, a fronte della mancanza di una regola che contemplasse espressamente una responsabilità per soggetti determinati».

Ai sensi dell'art. 21, le operazioni svolte sul FSE sono registrate e l'assistito può prendere visione delle registrazioni effettuate[327].

In ogni caso, è prevista una notifica per l'assistito per ogni operazione effettuata sul FSE.

Con riferimento alla consultazione dei dati e dei documenti del FSE per finalità di diagnosi, cura e riabilitazione, prevenzione e profilassi internazionale – non per finalità di studio o di ricerca

[327] Tra le operazioni che vengono registrate, vi è anche la consultazione del FSE. La possibilità di verificare gli accessi per la consultazione di una banca dati è una garanzia notevole, specialmente in ambito sanitario. Questo fu anche uno degli aspetti alla base della pronuncia della Corte europea dei diritti dell'uomo del 2008, nel caso I. c. Finlandia. La sentenza, peraltro, ha il pregio di affermare la peculiare rilevanza della protezione del dato circa la sieropositività all'HIV. Le considerazioni sull'importanza della protezione dei dati relativi alla salute sono reputate «especially valid as regards protection of the confidentiality of information about a person's HIV infection, given the sensitive issues surrounding this disease. The domestic law must afford appropriate safeguards to prevent any such communication or disclosure of personal health data as may be inconsistent with the guarantees in Article 8 of the Convention». Corte EDU 17 luglio 2008, n. 20511/03, I. c. Finlandia, in www.hudoc.echr.coe.int, punto 38. Cfr, sub art. 8, S. BARTOLE, P. DE SENA e V. ZAGREBELSKY (a cura di), Commentario breve alla Convenzione europea dei diritti dell'uomo, Padova, 2012, p. 316, nonchè C. ANGIOLINI, *Health and Data Protection* in P. IAMICELI, F. CAFAGGI e C. ANGIOLINI (a cura di), Casebook Judicial Protection of Health as a Fundamental Right, Roma, 2022, p. 126 ss.

scientifica o di governo della sanità – è ancora previsto il consenso come base giuridica che deve essere «libero, specifico, informato e inequivocabile nonché granulare cioè espresso per ciascuna finalità di trattamento e – per i dati sensibili – esplicito[328].

Per quel che concerne l'accesso in emergenza, l'art 20 prevede che «nell'eventualità in cui un soggetto che non abbia espresso il consenso alla consultazione del FSE versi in condizioni di impossibilità fisica, incapacità di agire o incapacità naturale e al contempo di rischio grave, imminente e irreparabile per la sua salute o incolumità fisica», gli operatori e gli esercenti le professioni sanitarie possono accedere dapprima al suo profilo sanitario sintetico e, solo ove necessario «verificata l'incapacità di esprimere il consenso, anche agli altri dati e documenti del FSE, limitatamente al tempo indispensabile per assicurare le cure e comunque fatta eccezione per quelli che egli ha deciso di oscurare».

2.1.5. Considerazioni sul tema.

[328] V. le Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679, Versione 1.1, adottate dal Comitato europeo per la protezione dei dati il 4 maggio 2020, consultabili in www.edpb.europa.eu

Dall'analisi della disciplina sia della cartella clinica elettronica che del Fascicolo sanitario elettronico nella sua veste originaria e nella sua versione 2.0., è emersa quella che dalla letteratura[329] è stata definita «l'amministrativizzazione della protezione dei dati personali»[330] e cioè «il superamento della regola di diritto privato da parte della regola di diritto pubblico, o meglio amministrativo»[331].

Infatti, negli ultimi tempi si è assistito al superamento del modello volontaristico e "consensocentrico" a favore di un paradigma di circolazione dei dati di carattere personale che sia ispirato al principio di solidarietà[332] attraverso la realizzazione della funzione sociale del diritto alla protezione dei dati personali che, come

---

[329] S. CORSO, *Il fascicolo sanitario elettronico 2.0.: spunti per una lettura critica* in *Le nuove leggi civili commentate* n. 2/2024, p. 359.

[330] S. CORSO, Sanità digitale e riservatezza. Interpretazioni sul fascicolo sanitario elettronico in *La protezione dei dati sanitari. Privacy e innovazione tecnologica tra salute pubblica e diritto alla riservatezza, 2023.*

[331] P. PERLINGIERI, *La pubblica amministrazione e la tutela della privacy. Gestione e riservatezza dell'informazione nell'attività amministrativa*, in *Annali della Facoltà di Economia dell'Università degli Studi del Sannio*, 2003, n. 8, p. 211 ss., ora in P. PERLINGIERI, *La persona e i suoi diritti. Problemi del diritto civile,* Napoli, 2005, p. 255 ss.

[332] M. CIANCIMINO, *Circolazione "secondaria" di dati sanitari e biobanche. Nuovi paradigmi contrattuali e istanze personalistiche- Nota a Cass. 7 ottobre 2021 n. 27325,* in *Dir. fam. pers*., 2022, p. 68. Cfr. I. RAPISARDA, *Ricerca scientifica e circolazione dei dati personali. Verso il definitivo superamento del paradigma privatistico?* in *Eur. dir. priv*., 2021, p. 335 ss. Sul principio di solidarietà, *ex plurimis*, G. ALPA, *Solidarietà. Un principio normativo*, Bologna, 2022.

espresso al 4 considerando, va contemperato con gli altri diritti fondamentali[333].

Ciò non determina il superamento del principio personalista[334] ma una sua lettura in chiave di maggiore responsabilizzazione del soggetto di diritto i cui dati circolano, non già attraverso lo strumento del consenso che non ha più i connotati e la forza giuridica dell'origine ma tramite un riadeguamento delle categorie del diritto privato al nuovo ambiente sanitario[335], permeato dalle nuove tecnologie.

Sezione II

3. La sanità digitale europea: lo Spazio europeo dei dati sanitari.

Nonostante dalla sezione precedente sia emerso come in Italia si stia procedendo verso la dematerializzazione e la digitalizzazione

---

[333] A. RICCI, *Sulla «funzione sociale» del diritto alla protezione dei dati personali*, in *Contr. Impr*., 2017, p. 586.

[334] E. BATTELLI, *Necessità di un umanesimo tecnologico: sistemi di intelligenza artificiale e diritti della persona*, in *Dir. Fam. Pers.* 2022, p. 109 e F. MATTEI, *Il punto di equilibrio tra sanità digitale e diritto alla protezione dei dati personali: la persona al centro delle nuove tecnologie,* G. CERRINA FERONI (a cura di) in *Le nuove frontiere della medicina, assetti istituzionali e gestione dei dati*, 2024.

[335] P. ZATTI, *Il diritto all'identità e «l'applicazione diretta» dell'articolo 2 della Costituzione* in G. ALPA, M. BESSONE e L. BONESCHI (a cura di), *Il diritto all'identità personale,* Padova, 1981.

dei dati sanitari, è evidente come le politiche si siano sempre più concentrate sullo sviluppo di sistemi informativi aventi ad oggetto la gestione dei singoli episodi clinici relativi allo stato di malattia che hanno condotto alla realizzazione di *data warehouse*[336], definiti in letteratura[337] quale «strumento cardine della conoscenza delle aziende sanitarie».

Nell'era del digitale si assiste, però, al superamento della staticità dei dati, dei costi di manutenzione e alla necessità di predisporre delle infrastrutture che consentano di incamerare grandi volumi di dati.

Proprio sulla base di tale spinta, nasce la volontà euro-unitaria[338] di creare uno Spazio europeo dei dati sanitari per rendere i dati sanitari più facilmente accessibili per i professionisti e per i pazienti (sia nel proprio Paese sia all'estero) e, allo stesso tempo, creare le condizioni operative di interoperabilità «al fine di

---

[336] Un data warehouse è un tipo di sistema di data management progettato per abilitare e supportare le attività di business intelligence (BI), in particolare gli analytics. I data warehouse servono esclusivamente ad eseguire query e analisi e spesso contengono grandi quantità di dati storici. I dati all'interno di un data warehouse sono generalmente derivati da una vasta gamma di origini come i file di registro dell'applicazione e le applicazioni di transazione. Per maggiori informazioni, https://www.oracle.com/it/database/what-is-a-data-warehouse/

[337] L. RUFO, *Digitalizzazione e condivisione dei dati sanitari: uno spazio comune europeo dei dati*, in V. SALVATORE (a cura di) Digitalizzazione, intelligenza artificiale e tutela della salute nell'Unione europea.

[338] Commissione Europea, Proposta di regolamento per istituire lo spazio europeo dei dati sanitari, 3 maggio 2022, COM (2022) 197/2.

riutilizzare queste informazioni per promuovere ricerca e innovazione, nel rispetto della riservatezza e della sicurezza informatica»[339].

La Commissione europea, nel febbraio 2020, ha elaborato una strategia europea dei dati[340] che è stata un elemento centrale della trasformazione tecnologica prevista dal programma europeo *NextGenerationEU*[341].

Tale strategia ha previsto, tra gli altri settori, anche quello sanitario ritenuto «essenziale per compiere progressi nella prevenzione, nell'individuazione e nella cura delle malattie, nonché per compiere decisioni consapevoli e basate sulle evidenze al fine di

---

[339] L. RUFO, *Digitalizzazione e condivisione dei dati sanitari: uno spazio comune europeo dei dati, op.cit.*

[340] Commissione Europea, Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni. Una strategia europea per i dati, 19 febbraio 2020, COM (2020)66 final.

[341] Si tratta di uno strumento temporaneo pensato per stimolare la ripresa dopo il drammatico periodo della Pandemia da Covid-19. Costituisce il più ingente pacchetto di misure di stimolo mai finanziato in Europa. In particolar modo, per ricostruire l'Europea dopo la pandemia di Covid-19 è stato stanziato un totale di 2.018 miliardi di euro a prezzi correnti. L'obiettivo finale è di arrivare ad avere un'Europa più ecologica, digitale e resiliente. Cfr. Regolamento (UE) 2021/241 del Parlamento europeo e del Consiglio del 12 febbraio 2021 che istituisce il dispositivo per la ripresa e la resilienza, pubblicato nella GUUE n. 57 del 18 febbraio 2021.

migliorare l'accessibilità, l'efficacia e la sostenibilità dei sistemi di assistenza sanitaria»[342].

Sulla base di questa strategia, nel maggio del 2022, la Commissione europea ha presentato una proposta di Regolamento per istituire uno Spazio europeo dei dati sanitari (*European Health Data Space – EHDS*)[343] che ha come obiettivo il miglioramento dell'accesso e del controllo dei dati sanitari delle persone fisiche (cosiddetto uso primario dei dati), la possibilità di procedere al riutilizzo dei dati per finalità di studio e di ricerca (cosiddetto uso secondario dei dati) nonché la garanzia di un più efficiente funzionamento del mercato interno al fine di ottenere una riduzione dei costi inerenti alla salute e una migliore allocazione delle risorse per garantire ulteriori livelli essenziali di assistenza.

La proposta appena menzionata è stata accompagnata da un parere congiunto EDPB-GEPD[344] che ha previsto che si potrà «mirare ad agevolare la condivisione dei dati sanitari, anche rafforzando la fiducia in quegli intermediari di condivisione dei dati che si prevede saranno utilizzati nei diversi spazi di dati. Non mira

---

[342] Commissione Europea, Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, cit., p. 26.

[343] Commissione Europea, Proposta di regolamento per istituire lo spazio europeo dei dati sanitari, cit.

[344] Il comitato europeo per la protezione dei dati (EDPB) e il Garante europeo della protezione dei dati (GEPD).

invece a riconoscere, modificare o sopprimere diritti sostanziali in materia di accesso ai dati e loro utilizzo»[345].

Secondo autorevole dottrina, la Proposta potrà «aiutare le persone ad assumere il controllo dei propri dati sanitari, sostenerne l'uso per migliorare l'erogazione dell'assistenza sanitaria, la ricerca, l'innovazione e l'elaborazione delle politiche, consentire all'UE di sfruttare appieno le potenzialità offerte da uno scambio, utilizzo e riutilizzo sicuro dei dati sanitari»[346].

È necessario sottolineare, però, che trattandosi di un «ecosistema specifico»[347] che tiene conto di «strutture, regole, norme e pratiche comuni e una struttura di governo che punta a sostenere la loro libera circolazione, nonché favorire un autentico mercato unico dei dati clinici prodotti dai sistemi di cartelle cliniche elettroniche, dai dispositivi medici e dai sistemi di intelligenza artificiale puntando, altresì, verso il loro riutilizzo per la ricerca e l'innovazione (c.d. uso secondario dei dati)», un ruolo centrale viene assunto dalla fiducia dei soggetti coinvolti e dalla sicurezza delle infrastrutture attraverso la compatibilità con l'art. 9 par. 2 del GDPR[348] –

---

[345] EDPB-EDPS, Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health.

[346] L. RUFO, *Digitalizzazione e condivisione dei dati sanitari: uno spazio comune europeo dei dati, op. cit.*

[347] *Ibidem.*

[348] Per uno sguardo d'insieme vedasi A. THIENE, *Art. 9 Trattamento di categorie particolari di dati*, in R. D'ORAZIO, G. FINOCCHIARO, O.

ampiamente analizzato nel capitolo precedente – e con le finalità individuate nell'art. 34 par. 1, lett. f) e g) della proposta[349].

Dopo la fase di trilogo tra i rappresentanti del Parlamento europeo, del Consiglio dell'Unione europea e della Commissione europea, a seguito di procedura legislativa ordinaria è stato definitivamente approvato dal Parlamento europeo nel mese di aprile del 2024, con pubblicazione del testo sulla Gazzetta Ufficiale dell'Unione europea nell'autunno 2024, il Regolamento europeo per l'istituzione dello Spazio europeo dei dati sanitari (anche indicato come European Health Data Space o EHDS o Regolamento EHDS).

3.1. L'uso primario dei dati e lo Spazio europeo dei dati sanitari.

POLLICINO, G. RESTA (a cura di), *Codice della privacy e data protection*, Giuffrè, Milano, 2021, p. 240 ss.

[349] Gli organismi responsabili dell'accesso ai dati sanitari forniscono l'accesso ai dati sanitari elettronici di cui all'articolo 33 solo se la finalità prevista del trattamento perseguito dal richiedente è conforme: f) ad attività di sviluppo e innovazione per prodotti o servizi che contribuiscono alla sanità pubblica o alla sicurezza sociale, oppure che garantiscono elevati livelli di qualità e sicurezza dell'assistenza sanitaria, dei medicinali o dei dispositivi medici;
g) ad attività di addestramento, prova e valutazione degli algoritmi, anche nell'ambito di dispositivi medici, sistemi di IA e applicazioni di sanità digitale, che contribuiscono alla sanità pubblica o alla sicurezza sociale, oppure che garantiscono elevati livelli di qualità e sicurezza dell'assistenza sanitaria, dei medicinali o dei dispositivi medici.

Per procedere all'elaborazione di un'Unione europea della salute[350] con lo scopo di «dare alle persone la possibilità di controllare i propri dati sanitari; promuovere un mercato unico dei servizi e dei prodotti di sanitò digitale; garantire l'interoperabilità e la sicurezza dei dati sanitari nonché la parità di condizioni per i fabbricanti del *device*; mettere a frutto il potenziale dell'economia dei dati sanitari e garantire un quadro coerente ed efficiente per il riutilizzo dei dati sanitari per la ricerca, l'innovazione, l'elaborazione delle politiche e le attività normative»[351] e garantire il rispetto dei principi FAIR di reperibilità, accessibilità, interoperabilità e riutilizzabilità[352], è necessario uniformarsi ad alcune normative di settore vigenti[353] oltre che al GDPR.

---

[350] V. DI FELICE, *Lo spazio europeo dei dati sanitari* in *Nota su atti dell'Unione europea*, Servizio studi del Senato, n. 102, luglio 2022.

[351] L. RUFO, *Digitalizzazione e condivisione dei dati sanitari: uno spazio comune europeo dei dati, op. cit.*

[352] Per un maggiore approfondimento sui principi FAIR si veda: https://www.go-fair.org/fair-principles/

[353] La proposta sullo spazio europeo dei dati sanitari è connessa ad altre normative vigenti o che sono in fase di discussione da parte delle istituzioni europee quali: il Regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio, del 30 maggio 2022 ('Data Governance Act'); il Regolamento (UE) 2023/2854 del Parlamento europeo e del Consiglio del 13 dicembre 2023 riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo e che modifica il Regolamento (UE) 2017/2394 e la Direttiva (UE) 2020/1828 ('Data Act'); il Regolamento (UE) 2024/1183 del Parlamento europeo e del Consiglio, dell'11 aprile 2024, che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale.

Quanto all'uso primario dei dati – di cui si è diffusamente parlato nel capitolo precedente – non sussiste alcuna criticità rispetto al quadro normativo già esistente.

Infatti, non è stato messo in discussione né il diritto di accedere immediatamente, gratuitamente e in forma facilmente leggibile, consolidata e accessibile ai propri dati sanitari da parte degli interessati – previsto dall'art. 15 del GDPR[354] – né il diritto alla portabilità dei dati[355] che invece acquisisce un valore aggiunto in considerazione della Proposta di cui in oggetto dal momento che spesso il limite della portabilità dei dati sanitari è rinvenibile nella mancanza di interoperabilità e di armonizzazione delle norme tecniche tra Stati membri o nella possibilità di "portare" i dati che si basano sulla base giuridica del consenso o del contratto.

Di fatti, con riferimento a quest'ultimo diritto, nell'eventualità in cui i fornitori di assistenza sanitaria si trovino in Stati membri diversi, tali dati verranno trasmessi nel novero dello scambio di cartelle cliniche europee tramite l'infrastruttura prevista dal Regolamento EHDS.

---

[354] Per un commento all'art. 15 GDPR si veda A.M. GAMBINO, M. SIRAGUSA, *Art. 15 Diritto di accesso dell'interessato*, in *Diritto, mercato, tecnologia*, 10 maggio 2023.

[355] Per un approfondimento, D. TUZZOLINO, *La portabilità dei dati sanitari*, op. cit.

Un elemento chiarito a più riprese dal Regolamento è la mancanza della dazione di un corrispettivo a fronte della concessione di tali dati elettronici.

Dal momento che si tratta di diritti che devono essere garantiti gratuitamente, è previsto che «il fornitore ricevente non sarà tenuto a compensare il fornitore di assistenza sanitaria per la messa a disposizione dei dati sanitari elettronici e che non si potrà addebitare direttamente o indirettamente agli interessati un compenso, un indennizzo o dei costi per la condivisione dei dati o per l'accesso agli stessi».

Secondo autorevole dottrina[356], non è sufficiente «l'attuazione di una mera interoperabilità tecnologica (cioè la capacità dei sistemi di connettersi tra loro e scambiarsi informazioni e dati), ma servirebbe garantire anche, mediante standardizzazione, un'interoperabilità sintattica, semantica e contestuale».

Il regolamento individua determinate categorie prioritarie di dati sanitari[357] e prevede che l'accesso debba essere garantito almeno per le informazioni che vengono qualificate come prioritarie che

---

[356] L. BOLOGNINI, S. ZIPPONI, *Prospettive future in sanità: Spazio europeo dei dati sanitari e regolazione dei dati sintetici* in *Privacy e diritto dei dati sanitari*, pp. 265-266.

[357] Quali tra gli altri le prescrizioni elettroniche; le dispensazioni elettroniche; gli studi di imaging medico e relativi rapporti di imaging; i risultati dei test medici, compresi i risultati di laboratorio e di altre diagnosi e i relativi rapporti.

siano rilevanti per l'esecuzione della prestazione sanitaria tramite sistemi disciplinati dal Regolamento in oggetto.

Gli Stati membri saranno chiamati ad istituire uno o più servizi di accesso ai dati sanitari elettronici a livello nazionale, regionale o locale e uno più servizi di delega che consentano ad una persona fisica di autorizzare altre persone fisiche a sua scelta ad accedere ai propri dati sanitari elettronici per suo conto e consentendo ai rappresentanti legali dei pazienti di accedere ai dati sanitari elettronici delle persone fisiche di cui curano gli affari, conformemente al diritto nazionale.

Un altro diritto previsto dal Regolamento in oggetto, in ossequio al bilanciamento tra diritto alla salute e alla protezione dei dati personali di carattere sanitario, è quello di limitare l'accesso degli operatori sanitari e dei fornitori di assistenza sanitaria alla totalità o a parte dei loro dati sanitari elettronici, specificando che questa limitazione potrebbe compromettere la prestazione dell'assistenza sanitaria loro fornita e gli Stati membri dovranno stabilire le regole e le salvaguardie specifiche relative a tali meccanismi di restrizione.

Nell'eventualità in cui venga esercitato tale diritto[358], i professionisti sanitari non avranno accesso ai dati del paziente, salva l'esistenza di uno stato di necessità per la salvaguardia degli interessi vitali dell'interessato.

Inoltre, il Regolamento, per ovviare alla circostanza in cui i dati sanitari del soggetto siano consultati per finalità improprie ha previsto l'invio di notifiche automatiche aventi ad oggetto l'accesso da parte dei professionisti effettuati nell'ambito del contesto dell'assistenza sanitaria, specificando: «a) l'operatore sanitario o le altre persone che hanno avuto accesso ai dati sanitari elettronici personali; b) la data e l'ora dell'accesso; c) i dati sanitari elettronici personali a cui si ha avuto accesso».

In aggiunta, gli Stati membri potranno prevedere restrizioni a questo diritto in circostanze eccezionali: ad esempio nell'eventualità in cui la divulgazione metterebbe in pericolo gli interessi vitali o i diritti dell'operatore sanitario o la cura della persona fisica.

Il secondo capitolo del Regolamento prevede, tra le altre cose, anche la facoltà in capo agli stati membri di predisporre delle

[358] Corrispondente al c.d. "diritto di oscuramento" o "diritto di oscuramento dell'oscuramento" previsto dalla legislazione italiana per il Fascicolo sanitario elettronico.

normative interne che garantiscono il diritto di "*opt-out*", ovvero la rinuncia all'utilizzo primario dei dati.

In tale ipotesi, le persone saranno messe nelle condizioni di rinunciare all'accesso ai dati sanitari elettronici personali registrati in un sistema EHR[359], ma tale diritto deve essere sempre reversibile e "bypassato" nel caso in cui l'accesso ai dati da parte del fornitore di assistenza sanitaria sia necessario per proteggere gli interessi vitali dell'interessato o di altra persona fisica.

È stato previsto che le persone fisiche possano presentare un reclamo a un'autorità per la salute digitale, designata da ogni Stato membro e, se il reclamo dovesse avere ad oggetto i diritti appena esaminati, tale autorità la trasmetterà alle autorità di vigilanza competenti secondo il GDPR.

Sul punto, nella versione definitiva del Regolamento si evidenzia come in Italia la competenza esclusiva sia in capo all'Autorità Garante per la protezione dei dati personali al fine di evitare una duplicazione di capacità sanzionatoria.

Per ovviare a uno degli obiettivi per cui è stato predisposto il Regolamento in oggetto – cioè l'abbattimento delle barriere linguistiche, materiali e fisiche e il raggiungimento di una migliore

[359] l'EHR è la versione digitale della cartella clinica di un paziente. L'EHR registra in tempo reale informazioni centrate sul paziente che sono disponibili istantaneamente e in modo sicuro agli utenti autorizzati.

esperienza di cura per il malato – è stato previsto un formato europeo di scambio delle cartelle cliniche elettroniche, indipendentemente dallo Stato membro di appartenenza con meccanismi di identificazione.

Ciascun Stato membro dovrà provvedere affinché «i fornitori di assistenza sanitaria registrino, in formato elettronico all'interno di un sistema di cartelle cliniche elettroniche, i pertinenti dati sanitari che rientrano almeno nelle categorie prioritarie riguardo ai servizi sanitari da essi prestati alle persone fisiche. Nel caso di elaborazione di dati in formato elettronico, i fornitori di assistenza sanitaria dovranno garantire che i dati sanitari elettronici personali delle persone fisiche da loro tratte siano aggiornati con le informazioni relative all'assistenza sanitaria fornita. Nel caso di aggiornamento ovvero registrazione dei già menzionati dati sanitari, le cartelle cliniche elettroniche devono identificare il professionista sanitario, l'ora e il fornitore di assistenza sanitaria che ha effettuato la registrazione o l'aggiornamento»[360].

Nell'ambito delle plurime variazioni normative che hanno condotto alla versione definitiva entrata in vigore è stato fortemente modificato il diritto di opposizione.

---

[360] Articolo 13 - Registrazione dei dati sanitari elettronici personali del Regolamento del Parlamento Europeo e del Consiglio sullo Spazio europeo dei dati sanitari e che modifica la direttiva 2011/24/UE e il regolamento (UE) 2024/2847.

Infatti, in origine gli Stati membri avrebbero potuto consentire che le persone fisiche avessero il diritto di opporsi alla registrazione dei loro dati sanitari in un sistema di cartelle cliniche elettroniche (stabilendo le norme e le garanzie specifiche relative a tali meccanismi di opposizione).

Nella versione entrata in vigore, invece, è stato previsto un meccanismo più attenuato di *opt-out* che si traduce in un diritto di rinunciare all'accesso ai dati sanitari elettronici registrati in un sistema EHR ferma restando permanenza dei medesimi nei sistemi di cartelle cliniche elettroniche, per cui, secondo la dottrina[361] «più che un vero "*opt-out*" all'utilizzo primario dei dati, si tratta, quindi, di una rinuncia ad un proprio diritto di consultazione».

Inoltre, con riferimento all'infrastruttura *MyHealth@EU*[362], prevista dall'art. 12 del Regolamento, è garantita la possibilità di assicurare alle persone fisiche interessate una piena disponibilità

---

[361] L. BOLOGNINI, S. ZIPPONI, *Prospettive future in sanità: Spazio europeo dei dati sanitari e regolazione dei dati sintetici, op. cit.*

[362] È l'infrastruttura di servizi digitali per l'assistenza sanitaria online (eHealth) che facilita lo scambio transfrontaliero di dati sanitari, inclusi i profili sanitari sintetici e le ricette elettroniche. Attraverso i "servizi essenziali", la Commissione europea mette a disposizione dei paesi dell'UE un'infrastruttura comune di tecnologie dell'informazione e della comunicazione e servizi trasversali (terminologia, interoperabilità). I paesi possono quindi creare dei "servizi generici" per collegare i sistemi nazionali di assistenza sanitaria online attraverso gli sportelli nazionali per l'eHealth, con il sostegno finanziario del programma per le telecomunicazioni del meccanismo per collegare l'Europa (2015-2020) e del programma "UE per la salute" (2021-2027).

dei dati sanitari in formato elettronico garantendo, in ossequio a quanto previsto dal GDPR, il diritto di opposizione ai dati sanitari – nel caso di informazioni che possano avere un impatto significativo sulla salute della persona fino a quando un professionista della salute non sia nelle condizioni di spiegare alla persona medesima il significato degli stessi – e la limitazione dell'accesso da parte dei professionisti sanitari alla totalità o a parte dei dati sanitari. Anche in questo caso, però, è prevista la clausola generale che, *mutatis mutandis*, potrebbe ricondursi alla causa di giustificazione dello stato di necessità nel diritto penale in base alla quale «qualora il trattamento dei dati sia necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica, il prestatore di assistenza sanitaria o il professionista sanitario può in ogni caso avere accesso ai dati sanitari elettronici oggetto della limitazione».

Gli Stati membri dovranno designare, oltre all'autorità nazionale per la salute digitale, un punto di contatto nazionale per l'uso primario dei dati sanitari che si inserirà in un *network* di comunicazione con le altre autorità degli Stati membri e nel novero della piattaforma centrale di interoperabilità per la salute digitale nell'ambito dell'infrastruttura transfrontaliera *MyHealth@EU*.

I singoli Stati dovranno garantire che tutti gli operatori sanitari complessivamente intesi siano collegati ai punti di contatto

nazionali e in grado di effettuare scambi di dati in maniera bilaterale.

Infine, anche con riguardo alla legittimazione dell'uso dei dati si applica il combinato disposto dell'art. 6, par. 1, lett. *c*) del GDPR riguardante la necessità per il titolare del trattamento di adempiere agli obblighi previsti dalla legge con l'art. 9, par. 2, lett. *i*) del GDPR che fa, invece, riferimento «alla necessità di trattamento per motivi di interesse pubblico nel settore della sanità pubblica come quello di assicurare standard elevati di qualità e sicurezza dei servizi sanitari, dei medicinali e dei dispositivi medici».

3.2. Norme sui sistemi di cartelle cliniche elettroniche e applicazioni per il benessere.

Nell'ambito dell'analisi del Regolamento sullo spazio europeo dei dati sanitari, il capitolo III è dedicato alle norme e i requisiti previsti per i sistemi di cartelle cliniche elettroniche e le applicazioni per il benessere.

L'analisi dell'interoperabilità delle cartelle cliniche elettroniche deve essere letta in armonia con quanto detto in precedenza sul tema con riferimento alla disciplina nazionale.

Nella versione originaria si precisava che le norme riguardavano i sistemi di cartelle cliniche elettroniche «destinati dal fabbricante

all'uso primario delle categorie prioritarie dei dati sanitari», nella versione definitiva si chiarisce, invece, che «i requisiti si applicano solo alle "componenti armonizzate" dei sistemi EHR, ovvero la componente europea di interoperabilità e quella di registrazione per i sistemi EHR».

Il Regolamento prevede una serie di requisiti tecnici e prescrizioni quali condizioni essenziali e attivazione delle cartelle cliniche e classifica gli obblighi a seconda che si tratti del produttore, dell'importatore o del distributore.

Quanto all'attestazione di conformità, vi sono visioni non conformi nelle varie proposte delle Istituzioni europee.

Secondo la Commissione, infatti, spetterebbe agli stessi fabbricanti delle cartelle cliniche elettroniche garantire la conformità dei sistemi e redigere un'autocertificazione che però non riuscirebbe a garantire l'integrità, mancando un soggetto terzo e imparziale.

Il Parlamento europeo aveva, invece, predisposto una procedura di valutazione di conformità con emissione del relativo certificato da parte di un organismo terzo e indipendente.

È prevalsa l'idea della Commissione e quindi che «siano i produttori a garantire che i componenti armonizzati dei loro sistemi EHR e i sistemi EHR in quanto tali siano conformi ai requisiti essenziali stabiliti e alle specifiche comuni stabiliti dal

Regolamento e a redigere la documentazione tecnica dei loro sistemi EHR».

Un sistema peculiare è previsto per le applicazioni per il benessere per cui è stata istituita una forma di etichettatura volontaria, consistente nell'indicazione della conformità ai requisiti e alle specifiche comuni dell'EHDS, qualora il fabbricante ne dichiari l'interoperabilità con un sistema di cartelle cliniche elettroniche in relazione ai componenti armonizzati dei sistemi EHR.

È d'uopo sottolineare che la possibilità di scambio dei dati tra applicazioni per il benessere e le cartelle cliniche elettroniche non implica la totale e generale trasmissione di tutti i dati sanitari ma l'utente sarà sempre nelle condizioni di individuare quali categorie di dati sanitari desidera inserire nel sistema di interoperabilità delle CCE.

3.3. L'uso secondario dei dati sanitari elettronici.

Il fulcro e l'aspetto più rivoluzionario del Regolamento sullo spazio europeo dei dati sanitari riguarda l'uso secondario dei dati. Nella proposta originaria, il capitolo IV prevedeva delle categorie minime di dati elettronici sanitari che i titolari dei dati avrebbero dovuto mettere a disposizione per uso secondario e, al comma 5 dell'art. 33, prevedeva che «qualora il diritto nazionale avesse

prescritto il consenso della persona fisica, gli organismi responsabili dell'accesso ai dati sanitari si sarebbero comunque basati sugli obblighi di cui al presente capo per fornire l'accesso ai dati sanitari elettronici».

Tale disposizione, in combinato disposto con quanto specificato nel Considerando 37 EHDS, sembrava individuare nel Regolamento sullo Spazio europeo dei dati sanitari la base giuridica necessaria per l'uso secondario dei dati personali, anche particolari, per finalità di ricerca scientifica, medica e biomedica.

Nel testo definitivo del Regolamento prevale la corrente più conservatrice e viene fissato «il diritto delle persone fisiche di rinunciare, in qualsiasi momento e senza indicarne i motivi, al trattamento dei dati sanitari elettronici personali che le riguardano per uso secondario (opzione sempre reversibile)» e viene previsto che «gli Stati membri debbano prevedere un meccanismo di non partecipazione accessibile e facilmente comprensibile, in base al quale le persone fisiche dovranno avere la possibilità di esprimere esplicitamente la loro volontà di non far trattare i loro dati sanitari elettronici personali per uso secondario», non pregiudicando in ogni caso la liceità del trattamento che ha avuto luogo prima che la persona abbia scelto di non consentirlo.

Resta sempre salva la possibilità per le legislazioni degli Stati membri di superare tale meccanismo di *opt-out*, qualora ricorrano

delle condizioni e «ove la richiesta di accesso sia presentata da un ente del settore pubblico o da un'istituzione, un organo, un ufficio o un'agenzia dell'Unione con il mandato di svolgere compiti nell'ambito della salute pubblica, fatte salve le misure specifiche e adeguate per proteggere i diritti fondamentali e i dati personali delle persone fisiche previste dalla legge nazionale, pur nel rispetto dei requisiti del capitolo III».

Secondo una corrente di dottrina[363] tale scelta è da considerarsi favorevole, in quanto viene tutelato l'obiettivo di prevedere delle normative che tutelino l'armonizzazione degli Stati membri.

Qualora, invece, fosse stata rimessa la discrezionalità agli Stati membri sarebbe stato vanificato lo scopo dell'uso secondario dei dati, non rendendo accessibile una quantità sufficiente di dati, creando una disparità tra i pazienti europei, a seconda dello Stato membro di appartenenza.

Il legislatore europeo ha, invece, lasciato una maggiore discrezionalità in capo agli Stati con riferimento ad alcune categorie di dati quali «i dati genetici, epigenomici e genomici umani; altri dati molecolari umani come la trascrittomica proteomica, la metabolomica, la lipidomica e altri dati omici; i dati sanitari delle biobanche e i database associati; dati delle

[363] L. BOLOGNINI, S. ZIPPONI, *Prospettive future in sanità: Spazio europeo dei dati sanitari e regolazione dei dati sintetici, op.cit.*

applicazioni *wellness*», in quanto spetterà agli Stati membri la possibilità di introdurre misure più severe e garanzie aggiuntive a livello nazionale per salvaguardare il valore e la sensibilità dei dati medesimi.

3.3.1. Le finalità per cui è consentito l'uso secondario dei dati.

Il Regolamento ha individuato le finalità per cui è consentito l'uso secondario dei dati che sono state considerate particolarmente rilevanti e di portata innovativa:

«interesse pubblico nell'ambito della salute pubblica e professionale, come le attività di protezione contro le gravi minacce transfrontaliere alla salute e la sorveglianza della salute pubblica o le attività che garantiscono alti livelli di qualità e sicurezza dell'assistenza sanitaria, compresa la sicurezza dei pazienti e dei prodotti medicinali o dispositivi medici»;

«attività di definizione delle politiche e di regolamentazione per supportare gli enti del settore pubblico o le istituzioni, le agenzie e gli organismi dell'Unione comprese le autorità di regolamentazione, nel settore della salute o dell'assistenza a svolgere i compiti definiti nei loro mandati»;

«statistiche, come le statistiche ufficiali a livello nazionale, multinazionale e dell'Unione definite nel Regolamento (UE) n. 223/2009 relative ai settori della salute o dell'assistenza»;

«attività di istruzione o insegnamento nei settori della salute o dell'assistenza a livello di formazione professionale o superiore»;

«ricerca scientifica relativa ai settori della salute o dell'assistenza, contribuendo alla salute pubblica o alla valutazione della tecnologia sanitaria, o garantendo alti livelli di qualità e sicurezza dell'assistenza sanitaria, dei medicinali o dei dispositivi medici, con l'obiettivo di beneficiare gli utenti finali, come i pazienti, gli operatori sanitari e gli amministratori della sanità incluso: attività di sviluppo e innovazione di prodotti e servizi; formazione, test e valutazione degli algoritmi, anche nei dispositivi medici, nei dispositivi medici diagnostici in vitro, nei sistemi AI e nelle applicazioni di salute digitale»;

«migliorare l'erogazione delle cure, l'ottimizzazione dei trattamenti e la fornitura di assistenza sanitaria, sulla base dei dati sanitari elettronici di altre persone fisiche»[364].

Nel Regolamento è previsto dunque lo sviluppo di prodotti e servizi che si servono dei sistemi di Intelligenza artificiale e di

[364] Articolo 53- Finalità per le quali è possibile trattare i dati sanitari elettronici per l'uso secondario del Regolamento sullo Spazio europeo dei dati sanitari.

algoritmi ma si vieta perentoriamente l'eventuale distorsione delle risultanze.

Inoltre, è vietato l'accesso ai dati sanitari elettronici e il trattamento dei medesimi con finalità pregiudizievoli che si traducono nell'adozione di decisioni basate sui medesimi.

E' d'uopo chiarire che l'uso secondario dei dati sarà gestito a livello centralizzato da appositi organismi responsabili dell'accesso ai dati che saranno designati dagli Stati membri e avranno il compito di valutare le richieste e concedere le autorizzazioni: in particolare, l'utente dovrà presentare una richiesta circostanziata e corredata da una serie di informazioni quali le finalità perseguite e le misure di sicurezza e l'organo responsabile per l'accesso ai dati dovrà decidere entro tre mesi dalla richiesta e, a seguito della verifica della sussistenza delle condizioni, concedere l'autorizzazione.

A seguito di concessione dell'autorizzazione, sarà richiesto al titolare dei dati di metterli a disposizione e dovrà farlo in un termine ragionevole e cioè non oltre i tre mesi dalla richiesta.

L'accesso a tali dati dovrà avvenire in forma anonimizzata o pseudonomizzata.

Anche per l'uso secondario dei dati è prevista una specifica infrastruttura (*HealthData@EU*) e dunque ciascuno Stato membro dovrà individuare un punto di contatto nazionale che sarà un

gateway organizzativo e tecnico che consentirà e sarà responsabile dell'utilizzo dei dati sanitari elettronici e si collegherà all'infrastruttura transfrontaliera per l'uso secondario dei dati sanitari elettronici per facilitare l'accesso e l'utilizzo alle informazioni per uso secondario per i diversi partecipanti all'infrastruttura suddetta.

In conclusione, dunque si può ritenere che l'EHDS sarà uno strumento prezioso per i cittadini e pazienti dell'UE e per i ricercatori, i medici e l'industria dal momento che si creerà un'infrastruttura di scambio di dati sicura e allineata che risponderà all'obiettivo primario di migliorare la cura dei pazienti e di predisporre una regolamentazione dell'uso secondario dei dati.

Se non sussistono perplessità per quel che concerne l'uso primario dei dati e l'interoperabilità dei medesimi, è necessario spendere qualche parola in più con riferimento all'uso secondario dei dati.

Infatti, sebbene il riconoscimento del *training* di sistemi di intelligenza artificiale e di algoritmi e della possibilità di prevedere un meccanismo di *opting out* invece del semplice consenso siano da considerare avanguardisti, residuano delle perplessità in merito al coordinamento con le altre normative in materia di dati e all'effettiva armonizzazione tra i diversi Stati membri.

Una soluzione plausibile potrebbe tradursi nell'implementazione dell'utilizzo dei dati sintetici all'interno dello Spazio europeo dei dati sanitari di cui si parlerà nell'ultimo paragrafo che segue.

3.3.2. L'utilizzo dei dati sintetici e il fallimento delle tecniche di anonimizzazione.

Nel paragrafo precedente si è a lungo analizzata l'importanza del riutilizzo del dato sanitario, sottolineando che la concreta utilità dell'informazione è massima quanto più alta è la sicurezza della non riconducibilità del dato alla persona titolare del medesimo.

Proprio perché è stato ipotizzato in letteratura il fallimento dell'anonimizzazione[365], negli ultimi tempi si è parlato di produrre dei dati sintetici, a partire dall'elaborazione di informazioni anche personali, reali e veramente esistenti[366], attraverso processi artificiali che consentano di elaborare dei *fac-simile data*.

Infatti, sebbene l'anonimizzazione o, *rectius* la pseudonomizzazione, dovesse, in linea teorica, «massimizzare la protezione dei dati personali e, allo stesso tempo, minimizzarne la

[365] C.A. TROVATO, C. RAUCCIO, *L'anonimizzazione è morta? Un'analisi dei dati sintetici come proposta per superare la dicotomia dato personale-dato non personale*, in *Ciberspazio e Diritto*, n. 2/2022.
[366] I cd. *Real world data* o *real life data*.

perdita»[367], le tecniche ad oggi utilizzate forniscono un'utilità inversamente proporzione alla tutela[368], pertanto, se il fine è quello di proteggere le informazioni e comunque trarne giovamento, una soluzione potrebbe essere l'utilizzo dei dati c.d. sintetici, creati tramite una specifica tecnica di anonimizzazione basata su modelli di *machine learning* di tipo generativo[369], con lo scopo di mantenere le caratteristiche originali dei dati ma rimuovendo ogni corrispondenza tra quelli reali e quelli artificiali[370].

Sebbene non ci sia ancora una normativa in materia, l'*European Data Protection Supervisor*, ne ha sottolineato[371] l'importanza, individuandone vantaggi e svantaggi. Se infatti, l'EDPS individua l'equità come conseguenza positiva dell'utilizzo – in quanto un *data set* equo impedisce il verificarsi di discriminazioni – in dottrina[372], invece, ciò viene considerato come un rischio, poiché si teme che i dati generati artificialmente possano riflettere gli stessi pregiudizi esistenti in società, perpetrando comportamenti

---

[367] *Ibidem*.

[368] F. LIU, *A statistical overview on data privacy*, in *Notre dame journal of law, ethics e public policy*, vol. 34, 2010, p. 477.

[369] K. EL EMAM, L. MOSQUERA, R. HOPTROFF, *Practical Synthetic Data Generation*, 2020.

[370] C. A. TROVATO, C. RAUCCIO, *op. cit.*

[371] https://www.edps.europa.eu/press-publications/publications/techsonar/synthetic-data_en?etrans=it

[372] C. A. TROVATO, C. RAUCCIO, *op. cit.*; A. GUPTA, D.L. BHATT, A. PANDEY, *Transitioning from Real to Synthetic data: Quantifying the bias in model*, in *Synthetic Data Generation Workshop at ICLR*, 2021.

discriminatori.

Infatti, se dal punto di vista dell'*output* di sintetizzazione è possibile addivenire ad un dato che non consente la riconducibilità all'interessato e in quanto tale ormai ineluttabilmente anonimo e dunque non oggetto delle tutele e degli adempimenti in materia di protezione di dati personali, il punto di diritto più critico si colloca nella fase iniziale e cioè quando «il dato personale vero e reale deve essere elaborato per costruire il modello che, poi, consentirà al sistema di intelligenza artificiale di generare i dati sintetici non personali o per addestrarne il sistema»[373].

Infatti, secondo la dottrina maggioritaria[374], l'elaborazione di dati

---

[373] L. BOLOGNINI, S. ZIPPONI, *Prospettive future in sanità: Spazio europeo dei dati sanitari e regolazione dei dati sintetici, op.cit.*

[374] Tra gli altri, cfr. N. PATKI, R. WEDGE, K. VEERAMACHANENI, *The Synthetic Data Vault* in *2016 IEEE International Conference on Data Science and Advanced Analytics (DSAA)*, 2016, pp. 399-410; E. CHOI, S. BISWAL, B. MALIN, J. DUKE, W.F. STEWART, J. SUN, *Generating Multi-Label Discrete Patient Records Using Generative Adversarial Networks*, in *Proceeding of Machine Learning for Healthcare*, vol. 68, 2017, pp. 286-296; L. XU, K. VEERAMACHANENI, *Synthesizing Tabular Data using Generative Adversarial Networks,* arxiv:1811.11264, 2018; S.M. BELLOVIN, P.K. DUTTA, N. REITINGER, *Privacy and Synthetic Datasets*, «STAN. TECH. L. REV.», vol. 22, n. 1, 2019; A.B. REINER, R. ALMOG, Y. GORELIK, I. HOCHBERG, L. NASSAR, T. MASHIACH, M. KHAMAISI, Y. LURIE, Z.S. AZZAM, J. KHOURY, D. KURNIK, R. BEYAR, *Analyzing Medical Research Results Based on Synthetic Data and Their Relation to Real Data Results: Systematic Comparison from Five Observational Studies*, in *JMIR medical informatics*, vol. 8, n. 2: e16492, febbraio 2020. Il National Cancer Registration and Analysis Service (NCRAS) istituito nell'ambito del Public Health England (PHE) ha realizzato nel 2018 un dataset (the Simulacrum) che contiene dati artificiali di pazienti

personali, anche sensibili, per lo sviluppo di modelli e/o di addestramento di sistemi intelligenti generativi di dati sintetici sarebbe riconducibile ad almeno tre distinte macro-fattispecie di finalità ultronee rispetto ad occasioni di cura che potrebbero sussumersi: a) nel trattamento di dati per fini statistici o di ricerca scientifica, nei casi in cui il trattamento dei dati personali reali sia necessario per la progettazione e la validazione scientifica o statistica di modelli di generazione di dati sintetici, nel rispetto dell'art. 89 GDPR analizzato ampiamente nel primo capitolo e della legislazione nazionale in materia; b) nel trattamento di dati per finalità didattiche o di pubblicazione scientifica, in ottemperanza al Considerando 159 del GDPR secondo cui «per rispondere alla specificità del trattamento dei dati personali per finalità di ricerca scientifica dovrebbero applicarsi condizioni specifiche, in particolare per quanto riguarda la pubblicazione o la diffusione in altra forma di dati personali nel contesto delle finalità di ricerca scientifica»; c) nel trattamento dei dati per fini giornalistici o di manifestazione del pensiero, ad esempio per la pubblicazione di articoli, saggi e anche nella libera espressione artistica, come individuato dall'art. 136, comma 1, lett. *c*) del

affetti da un tumore per favorire l'attività di ricerca del centro, disponibile al link https://simulacrum.healthdatainsight.org.uk/

Codice della Privacy.

Le questioni giuridiche di particolare rilievo sono riconducibili all'esistenza e la necessità della copertura normativa in materia di protezione dei dati e la sussistenza di una base giuridica legittimante il trattamento dei dati *ancora* personali nella fase propedeutica allo sviluppo di un modello di «sintetizzazione e/o di addestramento e/o di monitoraggio e/o di validazione di sistemi di IA per la generazione dei dati sintetici»[375].

Quanto alla prima questione, ammettendo l'esistenza di una corretta procedura di anonimizzazione, il dato cesserebbe di ricevere copertura normativa in materia di protezione dei dati personali in quanto «valutare se si è ancora in presenza di dati considerabili come personali richiede un'analisi del rischio basata su identificabilità e impatto diretto o indiretto sugli individui»[376].

Per quel che concerne il secondo quesito di diritto, la soluzione è più complessa.

Infatti, se il trattamento dei dati personali si esaurisce nella loro anonimizzazione con una mera "spremitura"[377] contestuale delle caratteristiche necessarie alla sintetizzazione, esso si potrebbe

---

[375] L. BOLOGNINI, S. ZIPPONI, *Prospettive future in sanità: Spazio europeo dei dati sanitari e regolazione dei dati sintetici, op.cit.*

[376] F. E. BROZZETTI, *I dati sintetici: panacea della privacy?* in *top legale*, 23 gennaio 2024.

[377] L. BOLOGNINI, S. ZIPPONI, *Prospettive future in sanità: Spazio europeo dei dati sanitari e regolazione dei dati sintetici, op.cit.*

inquadrare giuridicamente nell'adempimento dell'obbligo di rispetto dell'art. 89 del GDPR e della normativa nazionale in materia di trattamenti per fini statistici, di ricerca scientifica, didattici, di pubblicazione scientifica o di manifestazione del pensiero, nonché dei principi di limitazione della conservazione e di *data protection by-default* e a sostegno di questa tesi si richiama il Codice di condotta della Regione Veneto, approvato dal Garante, di cui si parlerà brevemente, che esclude la necessarietà di una base giuridica per l'anonimizzazione preventiva dei dati.

Inoltre, non è condivisibile l'orientamento che invoca il legittimo interesse o l'esecuzione di compiti di interesse pubblico in quanto difficilmente darebbe copertura giuridica alle categorie particolari di dati di cui all'art. 9 del GDPR e la richiesta del consenso al solo fine di procedere all'anonimizzazione dei dati potrebbe risultare sproporzionata e «incoerente con il bilanciamento tra diritti, libertà e interessi cui richiama il Considerando 4 del GDPR»[378].

Qualora invece non fosse percorribile la via dell'immediata anonimizzazione e invece si dovesse prendere in considerazione una perdurante elaborazione dei dati in forma personale – per consentire validazioni, verifiche e monitoraggio con i dati reali o anche di sviluppare modelli e sistemi in grado di generare dati

[378] *Ibidem*.

sintetici non sufficientemente anonimi – dovranno essere applicati gli articoli 6, 7, 9, 10 e il Capo IX del GDPR nonché le norme nazionali rilevanti in materia di condizioni di liceità e basi giuridiche dei trattamenti di dati personali, con conseguente aggravio degli oneri per i generatori dei dati sintetici.

Una soluzione potrebbe essere riscontrabile nel Regolamento europeo sull'Intelligenza artificiale in cui sono previste delle basi di legittimazione del trattamento dei dati personali anche sensibili per la prevenzione e la correzione di *bias* dei sistemi di IA che potrebbero applicarsi anche a sistemi generativi di dati sintetici.

In precedenza, si è fatto riferimento al Codice di condotta per l'utilizzo di dati sulla salute a fini didattici e di pubblicazione scientifica promosso da Azienda sanitaria ULSS 9 Scaligera e Regione Veneto[379] che, a parere di alcuni autori, potrebbe essere considerato un primo passo di positivizzazione regolatoria in materia di dati sintetici e *privacy*, sebbene ancora parziale per soggetti e settori trattando l'inserimento della sintetizzazione tra le tecniche di anonimizzazione dei dati personali con finalità di generazione e condivisione di dati sintetici in campo sanitario.

Si auspica, inoltre, un intervento del Garante della Privacy per

[379] Approvato il 14 gennaio 2021 dal Garante per la protezione dei dati personali, in seguito attuato con Deliberazione della Giunta regionale n. 1633 del 19 dicembre 2022, pubblicata sul Bur Veneto n. 10 del 24 gennaio 2023.

individuare le basi giuridiche necessarie per la lavorazione e trasformazione in dati sintetici di dati personali relativi alla salute e sensibili per finalità di ricerca scientifica e per garantire che queste informazioni, totalmente prive di capacità re-identificativa, possano costituire il cardine del futuro della medicina.

Sezione III

4. La medicina degli algoritmi.

Se l'*e-Health* si traduce nella digitalizzazione e nella dematerializzazione delle prestazioni sanitarie, l'introduzione dell'Intelligenza artificiale in medicina ha fatto emergere non soltanto un necessario ammodernamento degli strumenti ma «una vera e propria epistemologia e metodologia del sapere medico che, facendo leva sui dati digitali, crea nuovi paradigmi terapeutici e diagnostici»[380].

Infatti, l'IA aiuta, completa, modifica e – in astratto – sostituisce il giudizio umano in ordine ai trattamenti adeguati o ai parametri e alle prognosi mediche attraverso la scoperta di *patterns* dai dati, la

[380] 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,* Giappichelli.

costante sperimentazione e la generazione di ipotesi tramite complessi sistemi di analisi di dati.

Se i benefici dell'innovazione digitale nel campo della salute pubblica sono inestimabili (si pensi alla possibilità di diagnosticare malattie in tempi più rapidi e in modo accurato attraverso la medicina personalizzata o di precisione o alla capacità della macchina di carpire in maniera accurata il comportamento dei pazienti ed evitare errori nella gestione del caso), la questione giuridica di rilevante importanza riguarda l'applicazione delle norme relative alla protezione dei dati personali nell'uso e nello sviluppo dei sistemi di IA[381], essendo fondamentale sottolineare che non è dirimente analizzare le norme sulla tutela dei dati solo con riferimento all'impatto sulla persona ma anche in virtù del fatto che il dato diventa l'*alfa* e l'*omega* degli strumenti di Intelligenza artificiale.

Senza pretesa di esaustività, si ritiene necessario, in questa fase introduttiva del tema, procedere alla definizione di Intelligenza artificiale.

Il Consiglio di Stato, nell'ambito di una controversia riguardante la vittoria di una gara d'appalto per la fornitura di dispositivi medici, ha affermato che un algoritmo tradizionale può operare

---

[381] U. PAGALLO, *Intelligenza Artificiale e diritto: Linee guida per un oculato intervento normativo* in *Sistemi Intelligenti*, 3/2017, pp. 615-636.

con differente autonomia, a seconda della sua complessità. Pertanto, ciò che lo distingue dall'intelligenza artificiale non è l'automazione del procedimento, ma il fatto che l'AI utilizza tecniche (es. il *machine learning*) che non applicano regole preimpostate, ma «elaborano costantemente nuovi criteri di inferenza tra dati e assumono decisioni efficienti sulla base di tali elaborazioni, secondo un processo di apprendimento automatico»[382].

La *machine learning* si può distinguere in *supervised* e *unsupervised,* nel primo caso gli algoritmi sono stati programmati in modo tale da raggiungere determinati risultati predittivi; nel secondo caso, invece, gli algoritmi dovranno trovare delle regolarità nell'insieme dei dati, in assenza di indicazione sui risultati che dovranno essere ottenuti[383].

Attraverso la nuova lente dell'intelligenza artificiale, l'identità biologica viene scomposta in una sequela di informazioni funzionali alla gestione efficiente ed automatizzata della malattia senza però perdere di vista il riferimento alla persona umana e alla sua dignità; attraverso la gestione intelligente dei dati, ad esempio, si può condurre alla divisione in gruppi della popolazione affetta

---

[382] Consiglio di Stato, sentenza n. 7891/2021.

[383] Z. OBERMEYER, E.J. EMANUEL, *Predicting the future – Big data, Machine Learning and Clinical Medicine*, in *New England Journal of Medicine*, 375/2016.

da una determinata patologia sia dal punto di vista della diagnosi che della terapia: un paziente affetto da tumore della mammella che è portatore del gene BRCA1 o BRCA2[384] sarà sottoposto ad una cura farmacologica diversa rispetto a chi ha la stessa patologia ma non risulta portatore del medesimo gene e attraverso la sotto categorizzazione e l'acquisizione di altri dati – quali le condizioni ambientali della persona – sarà possibile addivenire a modelli di cura sempre più accurati.

I dati e i micro-dati del paziente sono non soltanto necessari per fornire al singolo un trattamento personalizzato ma una fonte preziosa per approfondire le conoscenze umane in materia di salute e medicina, trasformando la relazione medicale[385].

La rivoluzione copernicana attuata dall'IA ha messo in discussione l'applicazione di categorie giuridiche tradizionali ai nuovi fenomeni, ad esempio non è più rilevante la distinzione tra informazioni considerate sensibili perché chiaramente riconducibili alla salute e non sensibili perché collegati ad altri aspetti della quotidianità dell'essere umano in quanto le inferenze

---

[384] B. CHEN, A. J. BUTTE, *Leveraging Big Data to Transform Target Selection and Drug Discovery* in *Clinical Pharmacology and Therapeutics*, vol. 99 del 2016.

[385] S. A. WALDMAN, A. TERZIC, *Big Data Transforms Discovery-Utilization Therapeutics Continuum* in *Clinical Pharmacology and Therapeutics*, vol. 99 del 2016, pp. 250-254.

possibili – derivanti dall'incrocio di dati – conducono a conclusioni riguardanti l'individuo nel suo complesso[386].

Un risultato corroborato anche da un recente riconoscimento giurisprudenziale in merito all'interpretazione della normativa riguardante la *data retention* delle informazioni riguardanti le telecomunicazioni da parte della Corte di Giustizia che afferma che «l'insieme dei metadata derivanti dall'uso degli strumenti di telecomunicazione […] presi nel loro complesso, possono permettere di trarre conclusioni molto precise riguardo alla vita privata delle persone i cui dati sono stati conservati, come le abitudini quotidiane, i luoghi di soggiorno permanente o temporaneo, gli spostamenti giornalieri e non, le attività svolte, le relazioni sociali di queste persone e gli ambienti sociali da esse frequentati»[387].

Inoltre, sussiste un problema riguardante la disciplina dei dati trattati per fini dell'assistenza sanitaria e di cura e di ricerca scientifica e cioè l'applicazione del fenomeno della *Real-World*

---

[386] M. KOSINSKI, D. STILLWELL, T. GRAEPEL, *Private traits and attributes are predictable from digital records of human behavior* in *Proceedings of the National Academy of Sciences*, 110/2013, pp. 5802-5805.

[387] Sentenza della Corte di Giustizia dell'Unione europea, casi riuniti C-293/12 e C- 594/12 Digital Rights Ireland, paragrafo 27.

Evidence (RWE)[388] al campo medico per consentire che le informazioni inerenti ad un paziente generate dalla somministrazione di terapie o i dati derivanti dalle cartelle sanitarie elettroniche possano essere utilizzate sia allo scopo di fornire risposte o nuovi risultati su una certa terapia o medicinale[389] che al fine di ricerca e sviluppo.

Un'altra questione giuridica interessante, di cui si parlerà diffusamente in seguito, riguarda il controllo dei rischi e delle responsabilità derivanti dai prodotti "intelligenti" nel campo della medicina susseguente ad una quasi "naturale" asimmetria informativa tra produttori e consumatori di medicinali che giustifica un necessario intervento pubblico finalizzato a proteggere la collettività da prodotti nocivi o comunque rischiosi diffusi a seguito di autorizzazione all'immissione in commercio e i cui effetti sono controllati nell'ambito della farmacovigilanza.

---

[388] S. PRILLA, S. GROENENVELD, *Real-World Evidence to Support EU Regulatory Decision Making—Results from a Pilot of Regulatory Use Cases*, in *Clinical Pharmacology & Therapeutics, Vol. 116, Issue 5, Novembre 2024.*

[389] La Food and Drug Administration (FDA) ha pubblicato una linea guida per l'utilizzo di Real World Data al fine di prendere decisioni regolatorie sui dispositivi medici: cfr. Use of Real World evidence to support Regulatory Decision- Making for Medical Devices, 31 agosto 2017, disponibile al https://www.fda.gov/regulatory-information/search-fda-guidancdocuments/use-real-world-evidence-support-regulatory-decision-making-medical-devices.

Infatti, se si pensa ad esempio alle pillole "intelligenti"[390], si sovrapporranno i rischi derivanti dall'assunzione dei medicinali e quelli relativi al trattamento dei dati.

Le applicazioni di intelligenza artificiale e robotica in medicina determineranno l'aumento di scenari di bilanciamento di rischi in cui sarà sempre più complesso, in assenza di una disciplina giuridica *ad hoc*, fornire delle risposte regolatorie ottimali[391].

Questo avviene già frequentemente nelle soluzioni cd. classiche in cui il sistema regolatorio deve raggiungere delle soluzioni idonee a trovare un bilanciamento tra la protezione della *privacy* e la sicurezza dei pazienti e della salute pubblica in generale – ad esempio quando sistemi di raccolta dei dati tramite dispositivi o applicazioni vengono utilizzati per coadiuvare il paziente nella corretta assunzione e utilizzo del medicinale – ma, sarà ancora più complesso trovare un equilibrio nei casi più innovativi in cui gli algoritmi diventano parte integrante dei prodotti medicinali e decidono, alla luce dei dati dei pazienti, una quantità sicura ed efficace di principio attivo.

---

[390] Si fa riferimento a prodotti medicinali di ultima generazione che vengono assunti dai pazienti ma che rilasciano le sostanze attive nel corpo attraverso dispositivi digitali che monitorano le funzioni vitali dell'organismo e incrociano i dati sanitari dei pazienti secondo un modello prestabilito.

[391] Per un inquadramento della questione, A. SPINA, *A regulatory Mariage de Figaro: Risk Regulation, Data Protection and Data Ethics* in *European Journal of Risk Regulation*, vol.8/2017, pp. 88-94.

4.1. Intelligenza artificiale e il trattamento dei dati relativi alla salute.

Sebbene l'utilizzo dell'intelligenza artificiale e degli algoritmi in ottica di programmazione della sanità o della medicina predittiva[392], a fini diagnostici, nel percorso di cura o a scopi terapeutici[393] sia di rilevante importanza, è indubbio che «la rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali»[394]. Infatti, è chiarito in letteratura che «la protezione dei diritti personali è un'estrinsecazione del diritto alla salute come diritto della personalità mentre nell'orizzonte giuridico è una parte rilevante della persona umana»[395].

---

[392] N. GHIBELLINI, *La medicina di iniziativa. L'impiego dell'algoritmo nel trattamento dei dati relativi alla salute* in A. THIENE, S. CORSO (a cura di), *La protezione dei dati sanitari, privacy e innovazione tecnologica tra salute pubblica e diritto alla riservatezza* in Atti del convegno, Rovigo 4 novembre 2022, p. 159.

[393] Si veda sul punto, F. PASQUALE, *New laws of Robotics, Defending Human expertise i*n the *Age of AI*, Cambridge-Londra, 2020, pp. 30 ss.

[394] Considerando n. 6 del Regolamento sull'AI e nella prospettiva del diritto costituzionale, M. BASSINI, *Il diritto costituzionale alla privacy nel prisma dell'evoluzione tecnologica*, in *Dir. Cost*. 2023, pp. 83 ss.

[395] «La persona umana si prospetta nella sua unitarietà psico-fisica come un mondo soggettivo condizionato dalle circostanze ambientali, sociali, economiche, sì che diventa impossibile separare il bene salute dal valore complessivo della persona; questa assume una concreta realizzazione nel rispetto della storicità del momento. La libertà della persona ed i suoi effettivi contenuti, il particolare atteggiarsi del rapporto della persona con l'autorità

La digitalizzazione della sanità che è stata ampiamente trattata nei paragrafi precedenti ha costituito il necessario predecessore dell'utilizzo dell'intelligenza artificiale nel diritto, abbracciando trasversalmente plurimi settori[396], assumendo una valenza

dell'apparato della comunità in cui vive, il grado di socialità ed eticità dell'ambiente, sono elementi che incidono sulla qualità dello sviluppo della persona e pertanto sulla sua salute, intesa come equilibrio psichico, mentale e quindi fisico». P. PERLINGIERI, *Il diritto alla salute quale diritto della personalità*, in *La persona e i suoi diritti. Problemi del diritto civile*, a cura di P. PERLINGIERI, Napoli, 2005, p. 106.

[396] Si pensi, ad esempio, al rilievo assunto dall'intelligenza artificiale nel settore pubblico e agli interrogativi che pone al diritto amministrativo. Cfr. M. MACCHIA, A. MASCOLO, *Intelligenza artificiale e sfera pubblica: lo stato dell'arte*, in Giorn. dir. amm., 2022, p. 556 ss.; L. PAGANELLI, *Il settore pubblico alla sfida dell'intelligenza artificiale*, in C. CAMARDI, (a cura di), La via europea per l'Intelligenza artificiale. Atti del Convegno del Progetto Dottorale di Alta Formazione in Scienze Giuridiche - Ca' Foscari Venezia, 25-26 novembre 2021, p. 157 ss.; F. FAINI, *Intelligenza artificiale, diritto e pubblica amministrazione*, in *Intelligenza artificiale e diritto. Come regolare un mondo nuovo,* a cura di D'ALOIA, Milano, 2021, p. 385 ss.; M. TRESCA, *Lo «Stato digitale». Big data, open data e algoritmi: i dati al servizio della pubblica amministrazione*, in Riv. trim. dir. pubbl., 2021, p. 545 ss.; A. DI MARTINO, *Intelligenza artificiale e decisione amministrativa automatizzata*, in Tecnologie e diritto, 2020, p. 83 ss. Peraltro, deve osservarsi come, a livello nazionale, proprio la giurisprudenza amministrativa abbia enucleato chiaramente tre principi dell'operare algoritmico: conoscibilità del processo decisionale, non esclusività della decisione e non discriminazione algoritmica. R. MATTERA, *Processo – Decisioni algoritmiche. Il Consiglio di Stato fissa i limiti*, in *Nuova Giur.* Civ., 2020, 4, 809 (nota a sentenza); A. MASCOLO, *Gli algoritmi amministrativi: la sfida della comprensibilità*, in *Giornale Dir. Amm*., 2020, 3, 366 (nota a sentenza); M. TIMO, *Algoritmo – il procedimento di assunzione del personale al vaglio del Consiglio di Stato*, in *Giur. It*., 2020, 5, 1190 (nota a sentenza).

Allo stesso modo, si può pensare al rilievo che assume nel mercato e al punto di vista del diritto della concorrenza e dell'economia. V. GAMBINO, IA e pratiche commerciali scorrette, in CAMARDI (a cura di), op. cit., p. 383 ss.; S.

istituzionale e confrontandosi con il sistema giuridico e i valori dell'assetto costituzionale[397].

Prima di affrontare nel dettaglio dei casi di studio nell'ambito dei quali la dottrina si è interrogata sulla disciplina da applicare, si è ritenuto necessario richiamare l'art. 22, par. 1 del GDPR già analizzato in precedenza e qui per comodità solo richiamato relativo al diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, includendo espressamente una delle procedure più utilizzate nel settore e cioè

ORLANDO, *Regole di immissione sul mercato e pratiche di intelligenza artificiale vietate*, in: Persona e Mercato. 3/2022, p. 267 ss. In materia contrattuale, distingue il 'contratto algoritmico', dal 'contratto telematico' e dal 'contratto cibernetico' A. GENTILI, *La volontà nel contesto digitale: interessi del mercato e diritti delle persone* in *Riv. trim. dir. e proc. civ.*, 2022, p. 701 ss.

[397] V. CASONATO, M. FASAN e S. PENASA (a cura di), *Diritto e intelligenza artificiale, sezione monografica* in *DPCE online*, 2022, fasc. 1, pp. 155 ss.; A. D'ALOIA (a cura di), Intelligenza artificiale e diritto. Come regolare un mondo nuovo, op. cit. I A. D'ALOIA, *l diritto verso "il mondo nuovo". Le sfide dell'Intelligenza Artificiale*, 7 ss.; A. D'ALOIA, *Il diritto e l'incerto mestiere del vivere*, in *Ricerche di biodiritto*, Padova, 2021, p. 203 ss.; A. D'ALOIA, *Il diritto verso "il mondo nuovo". Le sfide dell'Intelligenza Artificiale*, in *BioLaw Journal - Rivista di BioDiritto*, 2019, p. 3 ss.; U. RUFFOLO (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020. Cfr. T.E. FROSINI, *L'orizzonte giuridico dell'intelligenza artificiale*, in Dir. inf., 2022, p. 5 ss.; T.E. FROSINI, *L'orizzonte giuridico dell'intelligenza artificiale*, in C. CAMARDI (a cura di), *op. cit.,* p. 7 ss. V. anche F. FAINI, *Intelligenza artificiale e regolazione giuridica: il ruolo del diritto nel rapporto tra uomo e macchina*, in *Federalismi,* n. 2/2023, p. 1 ss., consultabile all'indirizzo: www.federalismi.it, 25 gennaio 2023, nonché i contributi in E. GABRIELLI e U. RUFFOLO (a cura di), *Intelligenza Artificiale e diritto*, in *Giur.it*., 2019, p. 1657 ss.

la profilazione[398] e i principi fondamentali elaborati dal Consiglio di Stato in materia di utilizzo dell'algoritmo nel trattamento dei dati personali.

Richiamando quanto detto nel capitolo precedente in merito alla profilazione, si è ritenuto, invece, necessario analizzare la pronuncia in materia amministrativa e la compatibilità della medesima con la disciplina sulla protezione dei dati personali.

---

[398] V. LAGIOIA, G. SARTOR e A. SIMONCINI, nel Codice della privacy e data protection, in R. D'ORAZIO – G. FINOCCHIARO – O. POLLICINO – G. RESTA (a cura di) Milano, 2021, sub art. 22, reg. U.E. n. 679/2016, p. 378 ss.; L. A. BYGRAVE, nel *The EU General Data Protection Regulation (GDPR). A Commentary*, a cura di C. KUNER, L. A. BYGRAVE e C. DOCKSEY, Oxford University Press, 2020, sub art. 22, p. 522 ss. Una previsione simile, ma in una forma più sintetica e, per così dire, "embrionale", era contenuta al corrispondente art. 15 della Direttiva n. 46 del 1995. Previsioni di tenore analogo sono contenute in altri atti di diritto derivato dell'Unione, come all'art. 11 della Direttiva n. 680 del 2016 o agli artt. 24 e 77 del Regolamento n. 1725 del 2018. Sul piano del diritto internazionale, la disposizione trova corrispondenze nell'art. 9 della c.d. Convenzione 108 – nella versione modernizzata del 2018 – e nella Raccomandazione del Consiglio d'Europa, adottata dal Comitato dei Ministri il 21 novembre 2020, *Protection of individuals with regard to automatic processing of personal data in the context of profiling - Recommendation CM/Rec (2021)8 (2021*), che prende il posto della precedente Raccomandazione del 2010. Tra gli altri, C. Di FRANCESCO MAESA, *La profilazione nel contesto del diritto internazionale*, in A. ADINOLFI e A. SIMONCINI (a cura di), in *Protezione dei dati personali e nuove tecnologie. Ricerca interdisciplinare sulle tecniche di profilazione e sulleloro conseguenze giuridiche*, p. 75 ss., spec. Pp. 91 ss.; L. A. BYGRAVE, nel *The EU General Data Protection Regulation (GDPR). A Commentary op. ult. cit*., p. 529, osserva che le radici normative dell'art. 22 del Regolamento risalgono alla legge francese del 1978, c.d. Informatique et Libertés.

4.1.1. L'utilizzo dell'algoritmo nel trattamento dei dati personali nell'ambito della sentenza n. 8742 del 2019 del Consiglio di Stato.

Nell'ambito della gestione dei dati, l'utilizzo di un algoritmo costituisce senza dubbio un importante alleato.

In prima battuta poiché utilizzare un algoritmo consente di individuare con certezza la percentuale di probabilità che si verifichi un evento o un disturbo o una patologia, secondariamente perché si considera l'eventualità in cui si elabori un algoritmo che elabori dati in chiave preventiva.

Chiaramente è necessario sottolineare che la predisposizione di un elaboratore elettronico che possa generare dati così come l'utilizzo delle informazioni di carattere sanitario ai fini dell'addestramento degli strumenti di intelligenza artificiale di cui si parlerà nel prosieguo devono tenere conto della normativa in tema di tutela dei dati personali.

In linea generale, si devono vagliare le condizioni di liceità e le basi giuridiche che legittimano il trattamento secondo quanto indicato dagli artt. 5 e 6 del GDPR.

Nel particolare, è d'uopo richiamare la disciplina già analizzata relativa al trattamento dei dati sanitari e dunque l'art. 9 del GDPR che prevede in astratto un generale divieto di trattamento dei dati

particolari al paragrafo 1 a cui fa seguito l'elencazione di una serie di eccezioni già vagliate in precedenza.

Ulteriore norma da menzionare è l'art. 22 GDPR, appena richiamato, relativo ai processi decisionali automatizzati.

In via preliminare, si sottolinea la mancanza all'interno del Regolamento GDPR della definizione di processo decisionale automatizzato, la quale però è rinvenibile nelle Linee Guida sul processo decisionale automatizzato relativo alle persone fisiche e sulla profilazione ai sensi del regolamento 2016/679 del WP9, ove è specificato che «il processo decisionale esclusivamente automatizzato consiste nella capacità di prendere decisioni impiegando mezzi tecnologici senza coinvolgimento umano»[399].

Anche tale disposizione ha la stessa struttura dell'art. 9 del GDPR, prevedendo una regola generale al paragrafo 1 e una serie di eccezioni al paragrafo 2: il primo stabilisce che l'interessato ha il diritto di non essere sottoposto ad una decisione basata unicamente sul trattamento automatizzato, il successivo introduce le condizioni alla presenza delle quali il paragrafo 1 non trova applicazione.

Per cui, dal momento che l'algoritmo ha ad oggetto dati di carattere sanitario che potrebbero essere sottoposti a procedure

[399] Il documento, adottato il 3 ottobre 2017, nella versione emendata e adottata in data 6 febbraio 2018, è consultabile in ec.europa.eu.

decisionali automatizzate, i trattamenti dei medesimi dovranno superare il vaglio di legittimità.

Si è ritenuto opportuno, in questa sede, procedere all'analisi della sentenza n. 8472 del Consiglio di Stato che, anche se non ha trattato nello specifico i dati sanitari, ha fissato alcuni principi fondamentali e gli elementi di garanzia per l'utilizzo di algoritmi in sede decisoria pubblica.

Con riferimento a questi ultimi, si fa riferimento a: «a) la piena conoscibilità a monte del modulo utilizzato e dei criteri applicati e b) l'imputabilità della decisione all'organo titolare del potere, il quale deve poter svolgere la necessaria verifica di logicità e legittimità della scelta e degli esiti affidati all'algoritmo»[400].

Con riguardo alla piena conoscibilità il Consiglio di Stato sottolinea che «sia un elemento di garanzia richiesto anche dal GDPR e ciò al fine di arginare il rischio di trattamenti connessi all'utilizzo degli algoritmi, richiamando gli artt. 13 e 22 del GDPR».

Per quel che concerne i tre principi fondamentali, i giudici amministrativi enucleano: a) il principio di conoscibilità «secondo cui ognuno ha diritto a conoscere l'esistenza di processi decisionali automatizzati che lo riguardino ed in questo caso a

[400] Utilizzo degli algoritmi nel procedimento amministrativo –Cons. St., sez. VI, 13 dicembre 2019, n. 8472 - Pres. Montedoro, Est. Ponte.

ricevere informazioni significative sulla logica utilizzata»; b) il principio di non esclusività della decisione algoritmica, in virtù del quale «nel caso in cui una decisione automatizzata produca effetti giuridici che riguardano o che incidano significativamente su una persona, questo ha diritto a che tale decisione non sia basata unicamente su tale processo automatizzato»; c) il principio della non discriminazione algoritmica secondo cui «è opportuno che il titolare del trattamento utilizzi procedure matematiche o statistiche appropriate per la profilazione, mettendo in atto misure tecniche e organizzative adeguate al fine di garantire, in particolare, che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori»[401].

4.1.2. L'utilizzo dei principi elaborati dal Consiglio di Stato nei provvedimenti del Garante italiano per la protezione dei dati personali in tema di dati sanitari.

Per completezza, si procederà all'analisi dei provvedimenti recenti del Garante per la protezione dei dati personali in tema di medicina d'iniziativa, in materia di stratificazione dei pazienti durante il Covid, di diffusione illecita di dati personali e immagini

[401] Utilizzo degli algoritmi nel procedimento amministrativo –Cons. St., sez. VI, 13 dicembre 2019, n. 8472 - Pres. Montedoro, Est. Ponte.

riguardanti la salute e la vita privata di un individuo sui social media e di trattamento dei dati sanitari per finalità di ricerca senza il consenso esplicito degli interessati.

In primo luogo, si menziona il parere reso dal Garante della Privacy al Consiglio di Stato n. 43 del 5 marzo 2020[402].

L'intervento era stato sollecitato ai sensi dell'art. 58, par. 3, lett.*b*) del Regolamento e riguardava la creazione di un *data base* di livello individuale per procedere alla stratificazione degli utenti del SSN.

In questa occasione, il Garante rilevava come «la predetta attività rappresentasse una profilazione dell'utente del servizio sanitario nazionale, in quanto consisteva in un trattamento automatizzato di dati personali volto a valutare determinati aspetti privati, relativi ad una persona fisica, in particolare per analizzarne e prevederne la situazione economica e sanitaria e l'eventuale correlazione di tali elementi (riconducibile, quindi alla previsione di cui all'art. 4, par. 1 n. 4 del Regolamento)».

Sulla base di tali premesse, il Garante concludeva che «il quadro normativo non soddisfaceva i requisiti previsti dalla disciplina in materia di protezione dei dati personali (artt. 5, 6, 9 e 89 GDPR e

[402] Parere al Consiglio di Stato sulle nuove modalità di ripartizione del fondo sanitario tra le regioni preposte dal Ministero della salute e basate sulla stratificazione della popolazione, provvedimento n. 43 del 5 marzo 2020 [doc. web n. 9304455], in www.garanteprivacy.it.

artt. 2-*ter* e 2-*sexies* del Codice) e pertanto non era rinvenibile una base giuridica anche per la cd. attività di stratificazione di tutti gli utenti del SSN, volta a definire un profilo sanitario individuale legato alla presenza di patologie croniche e connesso ad un profilo reddituale individuale (*status* sociale)».

In data 25 maggio 2020, il Garante teneva un'audizione presso la Commissione parlamentare per la semplificazione avente ad oggetto la tematica del rapporto tra diritto alla salute, protezione dei dati e utilizzo della tecnologia[403].

Il Garante aveva rilevato che «la medicina d'iniziativa e la profilazione del rischio sanitario, sebbene fosse volta alla personalizzazione della medicina e al miglioramento dell'offerta terapeutica, coinvolgeva aspetti molto delicati dell'esistenza umana» e dunque concludeva sulla necessità di «garantire un'adeguata supervisione della profilazione, che, se fondata su dati o inferenze inesatti, rischia di determinare pregiudizi all'interessato e errori sul piano complessivo del governo clinico».

È interessante analizzare anche i tre provvedimenti correttivi e sanzionatori che il Garante ha adottato nei riguardi di tre Aziende

[403] Audizione del Presidente del Garante per la protezione dei dati personali nell'ambito dell'indagine conoscitiva in materia di semplificazione dell'accesso ai cittadini ai servizi erogati dal Servizio Sanitario Nazionale del 25 maggio 2020, doc. web n. 9351203.

sanitarie del Friuli-Venezia Giulia[404] censurandole in quanto, attraverso l'utilizzo di algoritmi, si era proceduto alla classificazione degli assistiti in relazione al rischio di avere o meno complicanze in caso di infezione da Covid-19 e ciò – ad avviso dell'Autorità – in assenza di un'idonea base giuridica.

Di fatti, il Garante ha ritenuto non idonea la legge regionale del Friuli-Venezia Giulia n. 22 del 2019 e le relative delibere attuative, né l'art. 1 della legge n. 34 del 2020 e dunque non è stato rispettato il disposto dell'art. 2 *sexies* del Codice della Privacy.

Da ultimo, è parso utile analizzare due provvedimenti dell'Autorità Garante emessi l'11 aprile del 2024 e il 9 maggio del 2024 in materia di violazione della privacy in contesti sanitari e di ricerca.

Il primo caso riguardava un caso emblematico di diffusione illecita di dati personali e immagini aventi ad oggetto la salute e la vita privata di un individuo minorenne sui social media, sussistendo la violazione dell'art. 5 del GDPR e degli artt. 137 e 139 del Codice della Privacy che limitano la diffusione dei dati personali per fini

[404] I tre provvedimenti [doc. web nn. 9844989, 9845156 e 9845312] sono tutti consultabili in www.garanteprivacy.it, tra gli altri F. ZANOVELLO, *Misure di garanzia e rischio di data breach in ambito sanitario* in A. THIENE, S. CORSO (a cura di), *La protezione dei dati sanitari, privacy e innovazione tecnologica tra salute pubblica e diritto alla riservatezza* – Atti del convegno, Rovigo 4 novembre 2022.

giornalistici, imponendo il rispetto della riservatezza e della dignità dei soggetti coinvolti.

Il Garante ha previsto il divieto di ulteriore trattamento delle immagini illecitamente diffuse, un ammonimento per la violazione delle disposizioni di trattamento dei dati e l'annotazione nel registro interno dell'Autorità; infatti, se da un lato è riconosciuto il diritto alla libertà di espressione, dall'altro questo non può ledere ed entrare in conflitto con la tutela della dignità e della privacy.

Il secondo provvedimento riguarda il trattamento dei dati sanitari per finalità di ricerca senza consenso esplicito degli interessati con la giustificazione della difficoltà organizzativa nell'ottenerlo in ottemperanza al nuovo, difficile, bilanciamento tra il diritto alla protezione dei dati personali cd. particolari e il necessario progresso della medicina e del miglioramento delle condizioni di vita.

Sebbene questi ultimi provvedimenti non riguardassero l'utilizzo di metodologie predittive, gli stessi rientrano in un discorso più ampio riguardante la necessità di trasparenza in merito al flusso dei dati sanitari e degli attori coinvolti nella nuova relazione medicale cd. intelligente, avallando l'interpretazione che il Garante offre dell'art. 7 commi 1, 2, 2-bis della legge n. 34 del 2020 nel provvedimento citato n. 70/2022 secondo cui non è possibile «rinvenire la base giuridica dei trattamenti svolti

dall'Azienda nell'art. 1 del d.l. n. 34 del 2020, atteso che il legislatore, proprio in tale atto normativo, quando ha voluto attribuire ad un soggetto pubblico funzioni istituzionali legate allo sviluppo di metodologie predittive in ambito sanitario, lo ha fatto espressamente, individuando un percorso normativo conforme a quanto previsto dalla disciplina in materia di protezione dei dati personali».

4.1.3. L'utilizzo dei dati sanitari per creare un dataset per lo sviluppo di macchine intelligenti.

Secondo una parte di dottrina, «i dati sono beni pubblici in senso economico e, essendo informazioni codificate e digitalizzate, sono caratterizzati da non rivalità e non escludibilità»[405] e infatti possono essere fruibili contemporaneamente da più soggetti e la loro circolazione e duplicazione è generalmente gratuita ed illimitata[406]. Nei capitoli e paragrafi che precedono si è parlato a più riprese dei dati sanitari, della definizione dei medesimi e di ciò che può sussumersi in questa macrocategoria.

---

[405] B. BUZZELLI, *Dati sanitari e implementazione dell'Intelligenza artificiale*, 50.

[406] G. COLANGELO, *Accesso ai Data e condizioni di licenza F/RAND*, in V. FALCE, G. GHIDINI, G. OLIVIERI (a cura di), Informazione e Big Data tra Innovazione e Concorrenza, Milano, 2018, pp. 135-147.

Il GDPR, però, non fa riferimento ad una disciplina specifica nel caso di utilizzo dei dati sanitari per la creazione di un *dataset* per istruire un sistema di intelligenza artificiale e quindi nel prosieguo, attraverso riferimenti alla dottrina maggioritaria, si analizzerà sia cosa si intende per *dataset* sia la possibilità di inserire tale attività in una categoria di trattamento di dati già esistente e disciplinata dal Regolamento.

In prima battuta, quando il GDPR definisce il trattamento, si riferisce a «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»[407] e pur essendovi un elenco nel testo europeo, lo stesso non è tassativo[408].

L'analisi incrociata delle norme e la definizione di *dataset* – creato dal programmatore a seguito della raccolta e organizzazione di una grande quantità di dati eterogenei[409]– consentono la sussumibilità

[407] Articolo 4 del GDPR.

[408] L'art. 4, par. 2 del GDPR elenca come trattamento dei dati le seguenti attività: «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, raffronto o interconnessione, limitazione, cancellazione o distruzione»

[409] Quali le ecografie, i raggi, il profilo sintetico del paziente, la prescrizione e la dispensazione elettroniche, i risultati e i rapporti di laboratorio, le lettere di dimissione ospedaliera e le immagini medicali e i referti di immagini.

dello stesso all'interno dei trattamenti dei dati in generale e nel particolare di quelli sanitari.

La disciplina dal Regolamento prevede, come detto in più circostanze lungo questo scritto, il divieto generale di trattamento delle categorie particolari di dati previsto dal paragrafo 1 dell'art. 9 e una sequela di eccezioni a tale divieto, già analizzate.

Nel caso di specie, al fine di comprendere in quale categoria si può ascrivere l'eccezione del trattamento dei dati per addestrare una macchina intelligente sarebbe necessario individuare il fine ultimo del loro utilizzo che è quasi una *probatio* diabolica.

Innanzitutto, è d'uopo individuare le fonti da cui questi dati vengono reperiti per la creazione del *dataset* che sono eterogenee. Infatti, le informazioni si possono trovare nelle cartelle cliniche elettroniche, nelle prescrizioni di farmaci, nei rapporti di laboratorio, nelle richieste di risarcimento e rimborsi, negli esiti segnalati dai pazienti e in altri strumenti di gestione dei dati utilizzati all'interno dei sistemi sanitari, da intermediari dei dati ovvero raccolti dagli enti che sviluppano device capaci di rilevare

in tempo reale i parametri di chi li indossa[410] nell'ambito sanitario ma anche al di fuori di tale settore[411].

Fatta questa necessaria premessa di metodo, è d'uopo richiamare i principi applicabili al caso di specie.

L'art. 5, lett. b) del GDPR stabilisce che «i dati possono essere raccolti per finalità determinate e successivamente trattati in modo compatibile con quelle finalità, la raccolta per una finalità ulteriore non è incompatibile con le finalità iniziali».

Nel dettaglio bisogna valutare se individuata la finalità per la prima raccolta dei dati, sia necessario determinare se il riutilizzo dei medesimi all'interno della macchina intelligente, tenuto conto dell'obiettivo individuato dal programmatore, sia compatibile o meno con questo ovvero se la nuova funzione sia di pubblico

---

[410] Tra gli altri, O. DIGGELMANN, M. N. CLEIS, L. SCAFFARDI affermano che «questi device non sono solo quelli che si possono trovare all'interno di una struttura ospedaliera, ma sono anche i dispositivi mobili come gli orologi intelligenti o le applicazioni per gli smartphone che consentono di controllare l'uso delle medicine prescritte ovvero per dare diagnosi attorno ai sintomi dei pazienti evidenziano l'utilità di questi dispositivi che consentono di provvedere a valutazioni personalizzate per l'utente del device, ridurre la domanda di personale medico, consentire forme di assistenza efficace ma a costi contenuti».

[411] I device possono essere anche sensori che controllano oggetti fisici, gestione dei flussi di attività amministrative, dispositivi di sorveglianza, ovvero dagli smartphone che accedono ad internet come motore di ricerca, ai social, alle transazioni commerciali salvando i dati relativi alle operazioni svolte dall'utente. I trattamenti dei dati ottenuti mediante l'utilizzo di IoT sono regolati inoltre anche dal Regolamento sui dati.

interesse o di ricerca scientifica e dunque considerabile compatibile già in astratto.

Dunque, emerge la compatibilità della normativa in materia di utilizzo dei dati per finalità di ricerca scientifica con il trattamento dei dati sanitari al fine di addestrare la macchina intelligente ma sussistono dei dubbi invece circa la disciplina applicabile nel caso in cui la macchina così implementata debba svolgere funzioni direttamente connesse alla cura del paziente.

Da ultimo, all'interno del Regolamento sullo Spazio europeo dei dati sanitari già precedentemente analizzato e che si richiama, è stato inserito nell'art. 53 rubricato "Finalità per le quali è possibile trattare i dati sanitari elettronici per l'uso secondario" il comma 1, lett. *e*) che prevede che « Gli organismi responsabili dell'accesso ai dati sanitari concedono l'accesso ai dati sanitari elettronici di cui all'articolo 51 per l'uso secondario a un utente dei dati sanitari solo se il trattamento dei dati da parte dell'utente è necessario per una delle finalità seguenti: e) ricerca scientifica nel settore sanitario o dell'assistenza che contribuisce alla sanità pubblica o alla valutazione delle tecnologie sanitarie o che garantisce elevati livelli di qualità e sicurezza dell'assistenza sanitaria, dei medicinali o dei dispositivi medici, con l'obiettivo di favorire gli utenti finali, quali i pazienti, i professionisti sanitari e gli amministratori sanitari, tra cui: i) attività di sviluppo e innovazione per prodotti o

servizi; ii) attività di addestramento, prova e valutazione degli algoritmi, anche nell'ambito di dispositivi medici, dispositivi medico-diagnostici in vitro, sistemi di IA e applicazioni di sanità digitale»[412].

Prevedendo una disciplina specifica sull'argomento in materia e stante la diretta applicabilità del Regolamento, si può ritenere colmata la lacuna normativa circa la base giuridica legittimante l'addestramento dei sistemi di intelligenza artificiale generativa in ambito sanitario.

4.2. Disegno di legge italiano in materia di intelligenza artificiale: specifiche in ambito sanitario.

In concomitanza con l'adozione dell'AI Act il 13 marzo 2024 – con l'obiettivo di supportare la diffusione delle tecniche di intelligenza artificiale in diversi settori sociali ed economici e di garantire un livello uniforme di tutela degli interessi pubblici in materia di salute, sicurezza e diritti fondamentali tra tutti gli Stati membri dell'Unione – da parte del Parlamento europeo, il Consiglio dei ministri n. 78 del 23 aprile 2024 ha deliberato un disegno di legge che disciplina l'uso dell'Intelligenza artificiale

[412]Articolo 53 del Regolamento sullo Spazio europeo dei dati sanitari.

nei settori demandati dal Regolamento all'autonomia normativa degli Stati Membri. L'iter di approvazione ha preso l'avvio con la presentazione del disegno di legge al Senato il 20 maggio 2024.

L'obiettivo del D.D.L. è la promozione di «un utilizzo corretto, trasparente e responsabile, in una dimensione antropocentrica, dell'intelligenza artificiale, volto a coglierne le opportunità» (art. 1 D.D.L.) e a migliorare le condizioni di vita dei cittadini e la coesione sociale.

Il comma 2 dell'art. 1 prevede espressamente che tutte le norme devono essere interpretate e applicate in conformità al diritto dell'Unione europea.

Nei paragrafi che seguono si analizzeranno nel dettaglio gli artt. 7-8-9 del d.d.l. in materia di intelligenza artificiale, tenuto conto dei rilievi effettuati in materia da parte del Garante per la protezione dei dati personali.

4.2.1. Articolo 7 del d.d.l. n. 1146 – «Uso dell'intelligenza artificiale in ambito sanitario e di disabilità».

Per quel che qui ci occupa, l'art. 7 del disegno di legge in parola individua «gli scopi, i diritti (in particolare d'informazione), le condizioni e i limiti connessi all'impiego, nel settore sanitario, dei sistemi di intelligenza artificiale, con particolare riguardo al

divieto di selezione e condizionamento dell'accesso alle prestazioni sanitarie con criteri discriminatori, alla riserva alla professione medica del momento decisionale del processo diagnostico e terapeutico, nel cui ambito l'intelligenza artificiale svolge una funzione meramente ausiliaria, nonché ai requisiti di affidabilità, verificabilità e aggiornamento dei dati e dei sistemi a tal fine utilizzati»[413].

L'art. 7 del disegno di legge quindi, nell'evidenziare l'importante contributo fornito dall'utilizzo di sistemi di intelligenza artificiale al potenziamento del sistema sanitario e alla prevenzione e alla cura delle malattie, individua degli importanti limiti e principi in materia.

Innanzitutto, il comma 1 sancisce il necessario rispetto dei diritti, delle libertà e degli interessi della persona nonché la tutela della protezione dei dati personali.

Il comma 2 pone un divieto esplicito circa il condizionamento dell'accesso alle prestazioni sanitarie a criteri discriminatori con l'ausilio di strumenti di intelligenza artificiale proprio per evitare che si verifichino situazioni distorsive che incidono sui diritti fondamentali degli individui.

---

[413] Parere del Garante per la protezione dei dati personali su uno schema di disegno di legge recante disposizioni e deleghe in materia di intelligenza artificiale – 2 agosto 2024, disponibile su www.garantedellaprivacy.it [doc. web. 10043532].

Il comma 3 garantisce all'interessato il diritto di informazione circa l'utilizzo di tecniche di intelligenza artificiale, i vantaggi diagnostici e terapeutici provenienti dalle nuove tecnologie nonché la logica decisionale utilizzata anche in un'ottica di eventuale responsabilità per i danni cagionati ai soggetti terzi[414].

Nel comma 4, invece, si fa riferimento all'individuazione di sistemi di intelligenza artificiale per contribuire all'accessibilità, all'autonomia, alla sicurezza e ai processi di inclusione sociale

---

[414] A tal proposito si rammenta che il regolamento del Parlamento europeo e del Consiglio UE del 2024, c.d. "AI act", approvato dal Consiglio UE in via definitiva il 21 maggio 2024, qualifica i sistemi di intelligenza artificiale nell'ambito dell'assistenza sanitaria come "ad alto rischio", ponendo in capo ai soggetti fornitori maggior obblighi di informazione al fine di garantire la trasparenza nell'impiego di tali strumenti.
Il Dipartimento per la trasformazione digitale prevede che «In specie il regolamento europeo considera ad alto rischio un numero limitato di sistemi di intelligenza artificiale che possono potenzialmente avere ripercussioni negative sulla sicurezza delle persone o sui loro diritti fondamentali, tutelati dalla Carta dei diritti fondamentali dell'Unione europea. Prima di immettere un sistema di intelligenza artificiale ad alto rischio sul mercato dell'Unione europea o di farlo entrare in servizio, i fornitori dovranno sottoporlo ad una valutazione della conformità, dovranno quindi dimostrare che il loro sistema è conforme ai requisiti obbligatori per un'IA affidabile (ad esempio: qualità dei dati, documentazione e tracciabilità, trasparenza, sorveglianza umana, accuratezza, cibersicurezza e robustezza).
Dovranno essere addestrasti e testati con set di dati sufficientemente rappresentativi per ridurre al minimo il rischio di integrare distorsioni inique nel modello e garantire che, se presenti, queste possano essere risolte mediante opportune misure di rilevazione, correzione e attenuazione. Dovranno essere tracciabili e verificabili, garantendo la conservazione dell'opportuna documentazione, compresi i dati utilizzati per addestrare l'algoritmo, fondamentali per le indagini ex post», https://repubblicadigitale.gov.it/portale/-/l-intelligenza-artificiale.

delle persone con disabilità che tengano anche conto del progetto di vita individuale, personalizzato e partecipato.

Il comma 5 prevede che i sistemi di intelligenza artificiale possano fungere da supporto e mai da fondamento esclusivo nei processi di prevenzione, diagnosi, cura e scelta terapeutica, lasciando sempre impregiudicata la decisione in capo al personale sanitario.

Infine, il comma 6 stabilisce, nell'ottica di minimizzare la possibilità di incorrere in errori, che i sistemi di intelligenza artificiale in ambito sanitario debbano essere affidabili e periodicamente verificati ed aggiornati.

Nel citato parere del Garante della Privacy, quanto all'articolo in oggetto è stato ritenuto di «integrare l'articolo 7, richiamando nell'ambito del settore sanitario, i requisiti previsti dall'articolo 10 dell'AI act per i sistemi di intelligenza artificiale considerati ad alto rischio, con specifico riferimento al trattamento dei dati particolari di cui all'articolo 9 del Regolamento, in particolare prevedendo che sia preferito l'uso di dati sintetici o anonimi e siano indicate particolari limitazioni per l'utilizzo di dati sanitari (divieto di trasmissione, trasferimento o comunicazione), nonché la limitazione della conservazione».

4.2.2. Art.8 del d.d.l. n. 1146 – «Ricerca e sperimentazione scientifica nella realizzazione di sistemi di intelligenza artificiale in ambito sanitario».

L'art. 8 del d.d.l. in argomento disciplina «dichiarandone il rilevante interesse pubblico, i trattamenti di dati, anche personali, effettuati per la ricerca e la sperimentazione scientifica nella realizzazione di sistemi di intelligenza artificiale in ambito sanitario, con legittimazione *ex lege* dell'uso secondario dei dati personali, anche appartenenti alle categorie particolari di dati di cui all'articolo 9 del Regolamento, privi di elementi identificativi diretti, previa informativa agli interessati, nonché comunicazione al Garante cui non segua, nei trenta giorni successivi, il blocco»[415]. Con riferimento al comma 1, «i trattamenti dei dati anche personali eseguiti da soggetti pubblici e privati senza scopo di lucro per la ricerca e la sperimentazione scientifica nella realizzazione di sistemi di intelligenza artificiale per finalità terapeutica e farmacologica, in quanto necessari ai fini della realizzazione e

[415] Parere del Garante per la protezione dei dati personali su uno schema di disegno di legge recante disposizioni e deleghe in materia di intelligenza artificiale – 2 agosto 2024, disponibile su www.garantedellaprivacy.it [doc. web. 10043532]

dell'utilizzazione di banche dati e modelli di base, sono dichiarati di rilevante interesse pubblico»[416].

Più nel dettaglio si fa riferimento a tali finalità: «prevenzione, diagnosi e cura di malattie, sviluppo di farmaci, terapie e tecnologie riabilitative, realizzazione di apparati medicali, incluse protesi e interfacce fra il corpo e strumenti di sostegno alle condizioni del paziente, salute pubblica, incolumità della persona, salute e sicurezza sanitaria»[417].

Per quel che riguarda la dichiarazione di interesse pubblico a cui fa riferimento il comma 1 del disegno di legge in disamina, essa è disposta in attuazione dell'articolo 32 della Costituzione e in ossequio a quanto previsto dall'articolo 9, paragrafo 2, lettera g) del Regolamento UE 2016/679[418].

---

[416] Comunicato stampa Consiglio dei Ministri, N. 78.

[417] Atti parlamentari, disegno di legge n. 1146 del 2024, Senato della Repubblica.

[418] È d'uopo rammentare che l'articolo 32 della Costituzione, tra le altre cose, stabilisce che la Repubblica tutela la salute come diritto fondamentale dell'individuo e interesse della collettività. La richiamata disposizione del regolamento UE 2016/679 (art. 9, par. 2, lett. G)) consente il trattamento di determinate categorie di dati "sensibili", tra cui quelli relativi alla salute, se il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri. La disposizione richiamata precisa che il trattamento deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi del soggetto.

Con riguardo al comma 2 dell'art. 8 del disegno di legge in esame, si disciplina «l'uso secondario dei dati personali che siano privi degli elementi identificativi diretti da parte di soggetti pubblici e privati senza scopo di lucro e per le finalità descritte dal comma precedente, restando fermo l'obbligo di informativa dell'interessato – che può essere ottemperato anche mediante la messa a disposizione di un'informativa generale sul sito internet del titolare del trattamento e inoltre non è richiesto ulteriore consenso dell'interessato anche nell'eventualità in cui sia richiesto originariamente per legge»[419].

Il comma 3 dell'articolo in esame stabilisce che «i trattamenti dei dati analizzati dai commi 1 e 2 devono essere oggetto di approvazione da parte dei comitati etici interessati, devono essere comunicati al Garante per la protezione dei dati personali insieme con informazioni sulle misure per assicurare la sicurezza del trattamento e sulla valutazione dell'impatto del trattamento medesimo (artt. 24,25,32 e 35 GDPR), nonché con l'indicazione espressa dei soggetti individuati quali responsabili del trattamento. Infine, il comma in oggetto prevede un termine dilatatorio per l'inizio dei trattamenti in questione che possono essere iniziati decorsi trenta giorni dalla già menzionata comunicazione»[420].

[419] Art. 8, comma 2, d.d.l. intelligenza artificiale.
[420] Art. 8, comma 3, d.d.l. intelligenza artificiale.

Il 4 e ultimo comma precisa che «restano fermi i poteri ispettivi, interdittivi e sanzionatori del Garante per la protezione dei dati personali»[421].

A tal proposito il Garante, nell'ambito del parere sul disegno di legge già in precedenza esaminato, rilevato che «il comma 1 andrebbe conformato ai requisiti di determinatezza previsti dagli articoli 6, par. 3, lett. B) e 9, par. 2, lett. G) del Regolamento, nonché 2-*sexies* del Codice»; che «l'uso secondario dei dati (sempre nei limiti della presunzione di non incompatibilità del fine di cui all'articolo 5, par. 1, lett. B) del Regolamento) esige la previsione delle garanzie sancite dall'articolo 89 del Regolamento medesimo per il trattamento funzionale, tra gli altri, a scopi di ricerca.

Esse non sono, infatti, assorbite dal solo riferimento, al comma 2, al ricorso a dati privi di elementi identificativi diretti (che, peraltro, è opportuno sostituire con riferimento al concetto di "dati pseudonomizzati", in analogia con il comma 1-bis dell'articolo 2-sexies del Codice, come modificato dal decreto legge 2 marzo 2024, n. 19, convertito con modificazioni dalla legge 29 aprile 2024, n. 56)»; che «al comma 2 è peraltro necessario sopprimere il riferimento alla possibilità di assolvere l'obbligo di informativa

[421] Art. 8, comma 4, d.d.l. intelligenza artificiale.

in forma generale, con pubblicazione sul sito web del titolare, non compatibile con tale ipotesi di uso secondario di dati»; che «al comma 3, è opportuno chiarire che il decorso del termine non consuma i poteri tipici dell'Autorità, volti all'accertamento di eventuali illeciti», dispone l'integrazione e la modifica dell'articolo 8 alla luce di quanto appena indicato.

4.2.3. Art. 9 del d.d.l. 1146 – «Disposizioni in materia di fascicolo sanitario elettronico, sistemi di sorveglianza nel settore sanitario e governo della sanità digitale».

L'articolo 9 del disegno di legge in esame ha apportato delle rilevanti modifiche al d.l. n. 179 del 2012 – analizzato approfonditamente nella prima sezione del presente capitolo – in materia di Fascicolo sanitario elettronico aggiungendo il nuovo articolo 12-*bis* in tema di intelligenza artificiale nel settore sanitario per assicurare che gli strumenti tecnologici avanzati siano applicabili anche al campo sanitario.

Nell'articolo in oggetto viene previsto al comma 1 che «le soluzioni di intelligenza artificiale aventi funzione di supporto alle finalità di cui all'articolo 12, comma 2 del citato D.L. devono essere disciplinate con uno o più decreti del Ministro della salute, di concerto con l'Autorità politica delegata in materia di

innovazione tecnologica e transizione digitale e con l'Autorità delegata per la sicurezza della Repubblica e *cybersicurezza*, sentita la Conferenza permanente Stato-Regioni». La finalità perseguita è quella di garantire strumenti e tecnologie avanzate nel campo medico.

Attraverso i decreti approvati con la procedura appena indicata, si dispone che «devono essere individuati i soggetti che, nell'esercizio delle proprie funzioni, accedono alle soluzioni di intelligenza artificiale tramite le modalità definite dai medesimi decreti».

Si dispone[422], inoltre, che «per il supporto alle finalità di cura e, in particolare per l'assistenza territoriale, deve essere istituita una piattaforma di intelligenza artificiale la cui progettazione, realizzazione, messa in servizio e titolarità vengono attribuite all'Agenzia nazionale per i servizi sanitari regionali (AGENAS)[423], in qualità di Agenzia nazionale per la sanità digitale.

---

[422] Art. 12-bis, comma 2, del d.l. 179 del 2012.

[423] Tra le altre cose, l'articolo 42 del D.L. 19/2024 PNRR ha poi previsto alcune norme per il potenziamento delle competenze dell'Agenzia nazionale per i servizi sanitari regionali – Agenas, in materia di Fascicolo sanitario elettronico (FSE) e senza nuovi o maggiori oneri per la finanza pubblica, prevedendo che l'Agenas estenda l'esercizio delle proprie competenze attualmente previste per i soli livelli centrali (Ministero del lavoro e politiche sociali e Ministero della salute) e regionali di governo, anche con riferimento allo studio e alla ricerca scientifica in campo medico, biomedico ed

Più nel dettaglio, tale piattaforma dovrà erogare i seguenti servizi di supporto: «1) ai professionisti sanitari per la presa in carico della popolazione assistita; 2) ai medici nella pratica clinica quotidiana con suggerimenti non vincolanti; 3) agli utenti per l'accesso ai servizi sanitari delle Case di Comunità»[424].

Inoltre, è previsto che «tale piattaforma deve essere alimentata con i dati strettamente necessari per l'erogazione dei servizi di cui al medesimo comma 2 che saranno trasmessi dai relativi titolari del trattamento»[425]. Si precisa che Agenas è il soggetto titolare del trattamento dei dati raccolti e generati all'interno di tale piattaforma.

Oltretutto «l'Agenzia, con proprio provvedimento, dopo aver acquisito i previ pareri del Ministero della salute e del Garante per

---

epidemiologico e relativamente alla programmazione sanitaria, alla verifica delle qualità delle cure ed alla valutazione dell'assistenza sanitaria che rientrano nel FSE. Tra i compiti dell'AGENAS vi rientra quello della gestione dell'Intelligenza Artificiale e della valutazione delle tecnologie sanitarie (Health Technology Assessment – HTA) relative ai dispositivi medici, nell'ambito della gestione della piattaforma nazionale di telemedicina. All'Agenzia si attribuiscono inoltre le attività relative alla raccolta e alla gestione dei dati utili anche pseudonimizzati, garantendo che gli interessati non siano direttamente identificabili, nell'ambito dell'attività di monitoraggio dell'erogazione dei servizi di telemedicina necessario per il raggiungimento degli obiettivi riconducibili al sub-intervento di investimento M6C1 1.2.3.2 "Servizi di telemedicina", tra cui il target comunitario M6C1-9, nonché per garantire la tempestiva attuazione del sub intervento M6C1 1.2.2.4 "COT-Progetto pilota di intelligenza artificiale".

[424] Art. 9 d.d.l. intelligenza artificiale.

[425] Art. 12-bis, comma 3, del d.l. 179 del 2012.

la protezione dei dati personali, oltre che dell'Agenzia per la Cybersicurezza nazionale, e valutato l'impatto del trattamento, specifica i tipi di dati trattati e le operazioni eseguite all'interno della piattaforma, nonché le misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio e per tutelare i diritti fondamentali e gli interessi dell'interessato, in coerenza con le disposizioni del Regolamento UE 2016/679, vale a dire il Regolamento generale sulla protezione dei dati».[426]

Il comma 2 dell'articolo 9 in esame si conclude con la previsione della clausola di invarianza degli oneri finanziari.

A tal proposito il Garante, nell'ambito del parere sul disegno di legge già in precedenza esaminato, ha osservato che l'articolo 9 deve integrare i requisiti già indicati nell'articolo 7 e nell'articolo 10 dell'AI Act; deve prevedere il parere del Garante medesimo sui decreti attuativi di cui al comma 1, primo periodo dell'articolo 12-*bis* del decreto-legge n. 179 del 18 ottobre 2012 in ragione dell'incidenza di tali atti sulla protezione dei dati; inoltre, deve essere modificato il comma 4 nella parte in cui non prevede che la fonte abilitata all'integrazione della norma sia di rango regolamentare; infine l'Autorità ha suggerito di rivalutare

[426] Disposizioni e delega al Governo in materia di intelligenza artificiale – A.S. n. 1146-B.

l'attribuzione della titolarità dei trattamenti effettuati attraverso la piattaforma, tenendo conto dei poteri decisori attribuiti al dicastero.

4.3. Conclusioni in materia di intelligenza artificiale.

A seguito dell'entrata in vigore del Regolamento europeo sull'intelligenza artificiale, l'adozione di un disegno di legge in materia analoga è stata una scelta obbligata e necessaria, tenendo conto della celerità con cui viaggia l'innovazione tecnologica e dell'affanno del diritto nel raggiungerla.

Sebbene la dimensione antropocentrica dell'intelligenza artificiale sia il punto focale della normativa, in più circostanze si ravvisa l'esistenza di un'attività promozionale circa i vantaggi – indiscussi – dell'applicazione delle nuove tecnologie all'ambito sanitario ma si tiene poco conto dei rischi o, per lo meno, di quelli imprevedibili.

L'attività consultiva del Garante della privacy ha evidenziato la necessità di apporre dei correttivi al disegno di legge, sia con riferimento al pericolo di utilizzi distorsivi degli strumenti di intelligenza artificiale che possano alterare i criteri di accesso alle prestazioni sanitarie e dunque violare il carattere di universalità del servizio sanitario nazionale che è un caposaldo della legge

istitutiva del medesimo e dell'erogazione delle cure; sia con riguardo alla necessaria pseudonomizzazione dei dati sanitari utilizzati per finalità di ricerca e di studio, con un'attenzione peculiare ai dati sintetici che possono essere considerati il futuro nel settore, superando il fallimento delle tecniche di anonimizzazione; sia, infine, con riguardo alla piattaforma di intelligenza artificiale e al ruolo attribuito all'Agenas, sottolineando il pericolo dell'affidamento del trattamento di dati particolari a queste nuove tecnologie.

Si evince un cauto ottimismo in merito all'utilizzo dell'intelligenza artificiale in ambito sanitario, ma non possono invece trascurarsi i rischi connessi all'utilizzo e soprattutto le responsabilità derivanti dalla medesima nell'eventualità in cui vengano arrecati danni a soggetti terzi, sia nell'ambito dell'utilizzo improprio dei dati sanitari o nella fuga degli stessi, sia a seguito di utilizzo di strumenti cd. artificiali in ausilio alle attività diagnostiche o chirurgiche, che, dei danni provocati dai dispositivi medici cd. AI-*based* o dai medicinali intelligenti, di cui si parlerà nel capitolo che segue.

Terzo capitolo

Sezione I

5.4. Intelligenza artificiale e applicazioni in ambito sanitario: cenni introduttivi.

Dopo aver trattato nei capitoli che precedono sia il dato sanitario che la sua interoperabilità, sia gli strumenti di sanità digitale previsti a livello unionale ed interno e aver analizzato, per quanto possibile e allo stato attuale delle conoscenze scientifiche e giuridiche, l'avvento dell'intelligenza artificiale e il suo utilizzo con riferimento al dato sanitario e alla salute in generale, nello scritto in oggetto si è ritenuto di vagliare i profili di responsabilità civile derivanti dall'utilizzo di dispositivi dotati di intelligenza artificiale[427], in specie medici, analizzandone lo stato dell'arte e le eventuali prospettive *de iure condendo*.

Infatti, l'intelligenza artificiale ha assunto e – continuerà a farlo – un ruolo sempre più rilevante nel settore sanitario, in quanto sia il *machine learning*, sia i dispositivi c.d. intelligenti e la robotica

[427] Tra gli altri, M. RATTI, *Riflessioni in materia di responsabilità civile e danno cagionato da dispositivo intelligente alla luce dell'attuale scenario normativo*, in *Contratto e impresa*, 3/2020.

«concorrono ad accrescere i livelli di qualità ed efficienza delle prestazioni assistenziali, e offrono straordinarie prospettive di sviluppo della scienza medica»[428].

Sebbene «non esista una definizione unanimemente condivisa di intelligenza artificiale»[429], ai fini della dissertazione che segue, si ritiene di accogliere l'accezione contenuta all'interno della «Carta etica europea sull'utilizzo dell'Intelligenza Artificiale nei sistemi giudiziari e negli ambiti connessi», adottata dalla Commissione Europea per l'efficienza della Giustizia, istituita dal Comitato dei Ministri del Consiglio d'Europa nel 2002[430], secondo la quale essa è «un'insieme di metodi scientifici, teorie e tecniche finalizzate a riprodurre, mediante le macchine, le capacità cognitive degli esseri umani i cui attuali sviluppi mirano a far svolgere alle macchine compiti complessi precedentemente svolti da esseri umani»[431].

---

[428] M. SAVINI NICCI, G. VETRUGNO, *Machine learning, dispositivi "intelligenti" e robotica: la responsabilità civile di strutture e professionisti sanitari* di U. RUFFOLO e M. GABBRIELLI (a cura di), in *Intelligenza Artificiale, dispostivi medici e diritto: Un dialogo fra saperi: giuristi, medici e informatici a confronto.*

[429] M. IENCA, *Intelligenza2: per un'unione di intelligenza naturale e artificiale*, Torino, 2019, 13 e V. G. ROMANO, *Diritto, robotica e teoria dei giochi: riflessioni su una sinergia*, in G. ALPA (a cura di), *Diritto e intelligenza artificiale*, Pisa, 2020, p. 107 ss.

[430] In questi termini, G. UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, in AA. VV., *Giurisdizione Penale, intelligenza artificiale ed etica del giudizio*, Milano, 2021, p. 9 ss.

[431] *Ibidem*.

Dunque, se vi è accordo sull'accezione dell'intelligenza artificiale che comprende *software* e programmi capaci di attuare con successo e con un più o meno elevato grado di autonomia operazioni generalmente attribuibili all'attività umana quali l'assunzione di decisioni per raggiungere determinati obiettivi, vi è altresì unanimità di vedute per quel che riguarda il *machine learning* e cioè quando si parla di «tecniche basate su algoritmi che migliorano automaticamente attraverso l'esperienza, il feedback e l'uso di dati, utilizzate, ad esempio, per classificare nuovi dati o prevedere dati futuri»[432] e il *deep learning* che è «quella tecnica che sfrutta gli algoritmi come reti di decisioni (reti neurali o reti neurali profonde) per imparare dai dati»[433].

La questione giuridica diventa più complessa quando l'intelligenza artificiale viene applicata alla medicina; infatti, se da un lato essa limita l'imprevedibilità connaturata nel pensiero e nell'agire umano, dall'altro viene utilizzato dalla macchina un differente tipo di "sapere".

Nel dettaglio, la medicina c.d. tradizionale trae il suo fondamento da metodi analitici e si basa sul confronto tra un numero esiguo di dati per verificare, ad esempio, se un determinato trattamento è

---

[432] F. CASCINI, *Digitalizzazione della Sanità e sicurezza delle cure*, in F. GELLI, M. HAZAN, D. ZORZIT, F. CASCINI (a cura di), *Responsabilità, rischio e danno in sanità*, Milano, 2022, p. 1063 e ss.

[433] *Ibidem*.

efficace per una malattia attraverso l'accertamento del nesso di causalità tra applicazione farmaceutica ed eradicazione della patologia mentre l'apprendimento automatico opera su un grande volume di dati e ha un limitato potere esplicativo dal momento che l'algoritmo può identificare correlazioni tra migliaia di variabili ma non può stabilire se quelle correlazioni corrispondano, in concreto, a nessi di causalità accertati[434].

Sebbene siano plurime le criticità relative all'applicazione dell'intelligenza artificiale in sanità, è indubbio che vi siano dei nuovi studi che sottolineano la capacità della macchina di «diagnosticare alcune tipologie di tumori cutanei con un livello di accuratezza sovrapponibile o persino superiore a quello di dermatologi affermati, di identificare specifiche anomalie della conduzione atrio-ventricolare così come farebbe uno specialista cardiologo esperto, di interpretare reperti radiologici o istopatologici al pari di specialisti radiologi e anatomo-patologi qualificati»[435] o attraverso l'acquisizione dei rilievi biometrici di fungere da assistente agli psichiatri per cercare di addivenire ai

---

[434] M. SAVINI NICCI, G. VETRUGNO, *Machine learning, dispositivi "intelligenti" e robotica: la responsabilità civile di strutture e professionisti sanitari*, op. cit.

[435] E. TOPOL, *Deep Medicine: how artificial intelligence can make healthcare human again*, New York, 2019, p. 17 ss.

pensieri che si celano dietro le espressioni facciali[436] o di supporto al campo operatorio attraverso la possibilità di selezionare i dati che possono essere mostrati attraverso un visore in sovraimpressione durante la procedura.

È necessario sottolineare, però, che la maggior parte – se non la totalità – dei sistemi che poggiano su modelli di intelligenza artificiale sono addestrati per trovare le correlazioni tra i dati immessi: pertanto, se il *cluster* di dati non è all'origine sufficientemente rappresentativo o vi sono dei *bias* iniziali, gli stessi si riverbereranno sui risultati finali.

Ad esempio, una revisione sistematica dei contributi di letteratura in materia di ricorso a modelli di Intelligenza Artificiale correlato al *risk assesment* relativo all'interpretazione dei dati di *imaging* diagnostico ha condotto alla seguente conclusione «esistono pochi studi prospettici di *deep learning* e studi randomizzati nell'*imaging* medico. La maggior parte delle sperimentazioni non randomizzate non sono prospettiche, sono ad alto rischio di distorsioni e si discostano dagli standard di segnalazione esistenti. Nella maggior parte degli studi mancano dati e codici, e i gruppi di comparatori umani sono spesso piccoli. Gli studi futuri dovrebbero ridurre il rischio di *bias*, migliorare la rilevanza clinica

[436] M. KAPLAN, *When the robots feel your pain*, in *The economist*, 27 novembre 2016.

del mondo reale, la rendicontazione e la trasparenza e temperare adeguatamente le conclusioni»[437].

Ancora, lo stesso confronto tra le metodiche applicate risulta inficiato dalla scarsa riproducibilità in quanto «lo sviluppo dell'intelligenza artificiale in ambito clinico attraverso l'applicazione di *machine learning* è un'area fertile di ricerca, ma il rapido ritmo del cambiamento, la diversità delle differenti tecniche e la molteplicità dei parametri di messa a punto rendono difficile ottenere un quadro chiaro di quanto accurati questi sistemi potrebbero essere nella pratica clinica o di come essi siano riproducibili in diversi contesti clinici»[438].

Nonostante queste rilevanti criticità, non manca chi ha aderito alla tesi avanzata dal Parlamento europeo con la risoluzione del 12 febbraio 2019 secondo cui affidando all'AI il compito di analizzare i dati raccolti e confrontarli con le conoscenze mediche, il medico recupererebbe il tempo necessario per stabilire una comunicazione «più efficace e profonda e per esaltare l'attitudine simpatetica e di condivisione della sofferenza»[439].

---

[437] M. NAGENDRAN et al., *Artificial intelligence versus clinicians: systematic review of design, reporting standards and claims of deep learning studies*, in *BMJ*, 2020, p. 368, m689.

[438] R. CHALLEN, J. DENNY, M. PITT et al., *Artificial intelligence, bias and clinical safety*, in *BMJ Quality & Safety*, 2019, 28, pp. 231-237.

[439] Nel paragrafo 71 della risoluzione in oggetto si sottolinea che «l'intelligenza artificiale e la robotica presentano potenziali vantaggi per

Sebbene non ci sia ancora unanimità di vedute in merito al vantaggio o al nocumento che l'intelligenza artificiale possa apportare all'ambito medico, nella dissertazione in oggetto si è voluto focalizzare l'attenzione sul profilo inerente alla responsabilità civile derivante dall'uso dell'AI, sia in generale sia con specifico riguardo ai danni cagionati dai dispositivi medici intelligenti, di cui si tratterà ampiamente nei paragrafi che seguono.

5.5. Intelligenza artificiale e responsabilità civile: lo stato dell'arte unionale.

In prima battuta, nelle risoluzioni del 16 febbraio 2017[440] e del 12 febbraio 2019[441] il Parlamento europeo ha illustrato «i rilevanti benefici che l'Intelligenza artificiale e la robotica possono procurare in ambito assistenziale»[442]; ha sottolineato che, in ogni

---

l'assistenza, ad esempio aiutando medici e infermieri a dedicare più tempo ad attività di valore elevato, come l'interazione con i pazienti».

[440] Risoluzione del Parlamento europeo del 16 febbraio 2017 "recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica – 2015/2103 (INL)".

[441] Risoluzione del Parlamento europeo del 12 febbraio 2019 "su una politica industriale europea globale in materia di robotica e Intelligenza artificiale – 2018/2088 (INI)"

[442] Robot e dispositivi intelligenti – osserva il Parlamento europeo – offrono un "contributo" assai significato "nel settore della salute", migliorando le pratiche e le tecniche di prevenzione, diagnosi e cura delle malattie,

caso, è «fondamentale rispettare il principio dell'autonomia supervisionata dei beni *self learning*, assicurando all'operatore sanitario adeguati poteri di controllo e di intervento su tali beni»[443]; ha affermato che «il progresso tecnologico rende necessaria l'introduzione di norme specifiche, volte a regolare la responsabilità civile per i danni derivanti dall'uso di robot e dispositivi intelligenti»[444], invitando la Commissione europea a presentare una proposta di atto legislativo in materia.

La successiva risoluzione del 20 ottobre 2020[445] ribadisce l'esigenza di definire, con apposito regolamento, un regime di "responsabilità civile per l'Intelligenza artificiale". A tal proposito,

---

aumentando efficienza e qualità delle prestazioni riabilitative, promuovendo lo sviluppo della medicina "personalizzata" e dell'assistenza a distanza, consentendo una più efficace gestione del personale e delle risorse finanziarie, e favorendo, in ultima analisi, la definizione di un ecosistema sanitario più sostenibile, efficiente e orientato ai risultati".

[443] Si fa riferimento al principio dell'*human in command* previsto dal paragrafo 33 della risoluzione del 16 febbraio 2017 e il paragrafo AK della risoluzione del 12 febbraio 2019.

[444] Si legge, nel paragrafo AI della risoluzione del 16 febbraio 2017 che «l'attuale quadro giuridico non sarebbe sufficiente a coprire i danni causati dalla nuova generazione di robot [e più in generale dai sistemi di intelligenza artificiale], in quanto questi possono essere dotati di capacità di autoapprendimento che implicano un certo grado di imprevedibilità nel loro comportamento, dato che imparerebbero in modo autonomo, in base alle esperienze diversificate di ciascuno, e interagirebbero con l'ambiente in modo unico e imprevedibile».

[445] Risoluzione del Parlamento europeo del 20 ottobre 2020 "recante raccomandazioni alla Commissione su un regime di responsabilità civile per l'Intelligenza artificiale – 2020/2014".

il Parlamento europeo ha proposto di distinguere le nuove tecnologie con riferimento al rischio correlato al loro utilizzo, prevedendo per i sistemi c.d. ad alto rischio[446] un regime di responsabilità oggettiva – accompagnato dalla previsione di un obbligo di copertura assicurativa – e conservando invece, per tutti gli altri sistemi, un regime di responsabilità fondato sulla colpa[447].
È necessario richiamare la risoluzione del 3 maggio 2022 che dedica ampio spazio ai rapporti tra "Intelligenza artificiale e salute" e che si pone in continuità con le precedenti risoluzioni appena citate[448].
Il 28 settembre 2022, la Commissione europea ha pubblicato una Proposta di direttiva sulla "responsabilità da Intelligenza

[446] Il Parlamento europeo al paragrafo 15 della risoluzione del 20 ottobre 2020 «è convinto che un sistema di IA presenti un alto rischio quando il suo funzionamento autonomo ha un alto potenziale di causare danni a una o più persone, in un modo che è casuale e che va ben oltre quanto ci si può ragionevolmente attendere; è del parere che, al momento di stabilire se un sistema di IA sia ad alto rischio, si debba anche tenere conto del settore in cui è possibile prevedere l'insorgere di rischi significativi e della natura delle attività svolte: ritiene che l'importanza del potenziale dipenda dall'interazione tra la gravità dei possibili danni, la probabilità che il rischio causi un danno o un pregiudizio e la modalità di utilizzo del sistema di IA».
[447] La scelta di un "approccio proporzionato al rischio" e la conseguente distinzione tra sistemi di IA ad alto rischio e non ad alto rischio è stata mutata dal Regolamento IA già citato in questo scritto.
[448] Risoluzione del Parlamento europeo del 3 maggio 2022 "sull'Intelligenza artificiale in un'era digitale – 2020/2266 (INI)"

artificiale"[449] che muove dalla considerazione che «le norme nazionali vigenti in materia di responsabilità, in particolare per colpa, non sono adatte a gestire le azioni di responsabilità per danni causati da prodotti e servizi basati sull'IA»[450] poiché «le caratteristiche specifiche, tra cui la complessità, l'autonomia e l'opacità possono rendere difficile, o eccessivamente costoso, per quanti subiscono un danno, identificare la persona responsabile e dimostrare che sussistono i presupposti ai fini dell'esito positivo di un'azione». L'iniziativa si inserisce in un "pacchetto di misure" riguardante le nuove tecnologie, formato altresì dalla proposta di revisione delle norme in materia di sicurezza dei prodotti e, soprattutto, dal regolamento sull'Intelligenza artificiale.

La proposta in tema di responsabilità civile «si prefigge l'obiettivo di promuovere la diffusione di un'IA affidabile affinché sia possibile sfruttarne i vantaggi, garantendo a coloro che hanno subito danni causati dall'IA una protezione equivalente a quella di cui beneficiano quanti subiscono danni causati da prodotti di altro

[449] Proposta di direttiva del Parlamento europeo e del Consiglio "relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale – 2022/0303 (COD)":

[450] Proposta di Direttiva della Commissione europea del 28 settembre 2022. Nel paragrafo che segue si analizzeranno le tesi della dottrina che hanno tentato di applicare le discipline già previste dal codice civile a queste nuove forme di danni.

tipo»[451]. In questo modo, come prevede la relazione di accompagnamento, «si riduce, inoltre, l'incertezza giuridica per le imprese che sviluppano o utilizzano l'IA in relazione alla possibile esposizione alla responsabilità e si previene la frammentazione derivante da adeguamenti specifici all'IA delle norme nazionali in materia di responsabilità civile»[452].

La Commissione, pur richiamando espressamente le risoluzioni del Parlamento europeo, se ne discosta sia nella scelta dello strumento legislativo (viene scelta la direttiva in luogo del regolamento), che nel contenuto delle soluzioni proposte.

Di fatti, non viene prevista una forma di responsabilità oggettiva – come individuato e auspicato dalla citata risoluzione del 20 ottobre 2020 – ma vengono introdotte «misure volte "ad alleggerire l'onere della prova" posto a carico dei soggetti danneggiati che esercitino – o intendano farlo – l'azione di responsabilità»[453].

---

[451] Proposta di Direttiva della Commissione europea del 28 settembre 2022.

[452] Proposta di Direttiva della Commissione europea del 28 settembre 2022.

[453] La Commissione segue, in realtà, un "approccio a più fasi". La prima fase si esaurisce nell'introduzione delle misure – relative, appunto, all'onere probatorio disciplinate dagli articoli 3 e 4 – disciplinate dagli articoli 3 e 4 della proposta di direttiva. Quest'ultima prevede poi, nell'articolo 5, che – decorso un certo lasso di tempo dal recepimento della "nuova" disciplina da parte degli Stati membri – la Commissione sia chiamata a "esaminare gli effetti" di tali misure e, "se del caso" a formulare una proposta legislativa, valutando in particolare l'opportunità di introdurre "norme in materia di responsabilità oggettiva" (da associare, in ipotesi, ad un regime di assicurazione obbligatoria). La soluzione prospettata dal Parlamento europeo nella risoluzione del 20 ottobre 2020 (responsabilità oggettiva e assicurazione

L'art 3 della proposta di direttiva stabilisce che gli Stati membri debbano provvedere affinché, su richiesta del danneggiato, l'autorità giurisdizionale «possa ordinare [al fornitore o ad un utente] la divulgazione di elementi di prova rilevanti in relazione a specifici sistemi di IA ad alto rischio – definiti tali dall*'AI act* – che si sospetta abbiano cagionato danni».

La divulgazione di tali elementi è disposta se «il destinatario dell'ordine si sia rifiutato di esibirli spontaneamente, e sempre che, l'attore abbia presentato fatti e prove sufficienti a sostenere la plausibilità della domanda di risarcimento del danno».

L'ordine del Giudice deve rispondere a criteri di "necessità" e "proporzionalità" rispetto alla specifica pretesa risarcitoria fatta valere dal danneggiato: in particolare «occorre tener conto dei legittimi interessi di tutte le parti, compresi i terzi interessati, specialmente in relazione alla protezione dei segreti commerciali e delle informazioni riservate»[454].

Nell'eventualità in cui il convenuto non adempia all'ordine di divulgazione, opererà, ai sensi dell'articolo 3, paragrafo 5 della proposta, una «presunzione relativa di non conformità e dunque, si presume, salvo prova contraria, la non conformità a un

obbligatoria) si colloca così – seguendo la logica della Commissione – in una fase successiva e meramente eventuale dell'iter legislativo.

[454] Articolo 3, paragrafo 4 della proposta di Direttiva.

pertinente obbligo di diligenza da parte del convenuto, che gli elementi di prova richiesti [e non divulgati] erano intesi a dimostrare».

L'articolo 4 stabilisce, invece, una presunzione *iuris tantum* di «esistenza del nesso di causalità tra la colpa del convenuto e l'*output* prodotto da un sistema di IA o la mancata produzione di un output da parte di tale sistema.

La presunzione postula il concorso di tre condizioni:

a) l'attore deve aver dimostrato – o l'organo giurisdizionale deve aver presunto, ai sensi del citato articolo 3, paragrafo 5 – la colpa del convenuto o di una persona della cui condotta il convenuto sia responsabile, "consistente nella inosservanza di un obbligo di diligenza previsto dal diritto dell'Unione o nazionale e direttamente inteso a proteggere dal danno verificatosi";
b) deve essere "ragionevolmente probabile", alla luce delle concrete "circostanze del caso", che il comportamento colposo abbia influito sull'*output* o sul mancato *output* del sistema intelligente;
c) l'attore deve aver dimostrato che il danno è stato causato dall'*output* (o dal mancato *output*) di tale sistema»[455].

Con specifico riguardo alla posizione dell'«utente di un sistema di IA» quale può essere l'operatore sanitario, l'articolo 4, paragrafo

[455] Articolo 4 della Proposta di direttiva sulla responsabilità civile.

3, della proposta precisa che la condizione di cui al punto a) «è soddisfatta se l'attore dimostra che l'utente: *(i)* non ha rispettato l'obbligo di utilizzare il sistema di IA o di monitorarne il funzionamento conformemente alle istruzioni per l'uso che accompagnano tale sistema o, se del caso, non ha rispettato l'obbligo di sospenderne o interromperne l'uso secondo quanto previsto dalla legge sull'IA; oppure *(ii)* ha esposto il sistema di IA a dati di input sotto il suo controllo che non sono pertinenti alla luce della finalità prevista dal sistema»[456].

La proposta di direttiva precisa, infine:

– «che, nel caso di azioni di responsabilità per danni cagionati da sistemi di IA ad alto rischio, la presunzione di nesso causale non si applica se il convenuto dimostra che l'attore può ragionevolmente accedere ad elementi di prova e competenze sufficienti per dimostrare l'esistenza del nesso»;
– «che, ove l'azione riguardi sistemi "non ad alto rischio", tale presunzione si applica solo se l'organo giurisdizionale nazionale ritiene eccessivamente difficile per l'attore dimostrare l'esistenza del nesso di causalità».

[456]Vedasi Relazione illustrativa della Proposta di direttiva sulla responsabilità da IA. Si rinvia, in entrambi i casi, al Regolamento sull'intelligenza artificiale.

– «che, in ogni caso, il convenuto ha il diritto di confutare la presunzione, fornendo i necessari elementi di prova».

La proposta di direttiva – come hanno segnalato i primi commentatori in letteratura[457] – lascia, sia per la natura dello strumento individuato, sia per la delicatezza della tematica, ampi margini di intervento al legislatore nazionale, fermandosi sul tema dell'onere probatorio.

Gli Stati membri regolano «gli aspetti generali della responsabilità civile» e «possono adottare o mantenere in vigore norme nazionali più favorevoli all'attore», rispetto a quelle individuate dalla Commissione.

Nell'attesa che l'iter unionale proceda e che la dottrina si pronunci sul tema, nel paragrafo che segue si analizzeranno i vari schieramenti dottrinali in merito alla sussumibilità all'interno di istituti già previsti nel Codice civile delle nuove forme di responsabilità per danni cagionati da dispositivi intelligenti, con un *focus* specifico sui dispositivi medici.

5.6. Le "nuove" voci di danno da sistemi di intelligenza artificiale: riconducibilità alle categorie già esistenti in diritto o necessità di intervento normativo?

[457] Tra gli altri, G. PROIETTI, *Responsabilità civile, inadempimento e sistemi di intelligenza artificiale*, in www.giustiziacivile.com, 7 febbraio 2023.

Negli ultimi anni la dottrina si è posta più volte il quesito della sussumibilità delle ipotesi di responsabilità civile per danni cagionati da sistemi di intelligenza artificiale nelle categorie c.d. "tradizionali di responsabilità civile extracontrattuale" previste dal nostro ordinamento, con specifica attenzione alle forme "speciali" disciplinate dal Codice civile, tra le quali, e senza pretesa di esaustività, la responsabilità da cosa in custodia[458].

[458] Il «sistema di intelligenza artificiale» è definito «un sistema basato su software o integrato in dispositivi hardware che mostra un comportamento che simula l'intelligenza, tra l'altro raccogliendo e trattando dati, analizzando e interpretando il proprio ambiente e intraprendendo azioni, con un certo grado di autonomia, per raggiungere obiettivi specifici» dall'art. 3, lett. a) della Proposta di Regolamento del Parlamento europeo e del Consiglio sulla responsabilità per il funzionamento dei sistemi di intelligenza artificiale, formulata nella Risoluzione del 20 ottobre 2020, recante raccomandazioni alla Commissione europea su un regime di responsabilità civile per l'intelligenza artificiale (2020/2014(INL). Tra i numerosi contributi sulle rilevanti questioni giuridiche sollevate dall'impiego dell'intelligenza artificiale, nei più svariati settori, cfr. P. PERLINGIERI, S. GIOVA, I. PRISCO (a cura di), *Rapporti civilistici e intelligenze artificiali: attività e responsabilità*, Napoli, 2020, *passim*; ID. (a cura di), *Il trattamento algoritmico dei dati tra etica, diritto e economia*, Napoli, 2020, *passim*; G. ALPA (a cura di), *Diritto e intelligenza artificiale. Profili generali, soggetti, contratti, responsabilità civile, diritto bancario e finanziario, processo civile*, Pisa, 2020, *passim*; U. RUFFOLO (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Torino, 2020, *passim*; A. SANTOSUOSSO, *Intelligenza e diritto. Perché le nuove tecnologie sono una grande opportunità per il diritto*, Milano, 2020, *passim*; S. FARO, T.E. FROSINI, G. PERUGINELLI (a cura di), *Dati e algoritmi. Diritto e diritti nella società digitale*, Bologna, 2020, *passim*; D. BUZZELLI, M. PALAZZO (a cura di), *Intelligenza artificiale e diritti della persona*, Pisa, 2022, *passim*; M. TAMPIERI, *L'intelligenza artificiale e le sue evoluzioni. Prospettive civilistiche*, Padova, 2022, *passim*.

Prima di entrare nel vivo dell'analisi, è opportuno premettere che le nuove forme di tecnologia, specialmente in forma automatizzata, possono dar luogo a nuovi scenari, profondamente diverse da quelli già affrontati a livello giurisprudenziale[459] .

Questo accade non soltanto quando i danni vengono cagionati da robot che sostituiscono gli esseri umani nel compimento delle proprie attività, ma anche quando sono cagionati da «intelligenze artificiali, dotate di capacità di autoapprendimento, le cui scelte siano assunte in base all'elaborazione di un algoritmo»[460].

Di fatti, queste ultime assumono decisioni autonome che conseguono ad un processo di adattamento definito di *self learning*: «il sistema intelligente si confronta con la realtà e si trasforma coerentemente con i dati esperienziali acquisiti nel tempo»[461], elaborando decisioni e comportamenti che potrebbero non essere previsti in fase di progettazione e rappresentare il

---

[459] A. AMIDEI, *Robotica intelligente e responsabilità: profili e prospettive evolutive del quadro normativo europeo*, in *Giur. It.*, 2021, p. 100.

[460] C. DEL FEDERICO, *Intelligenza artificiale e responsabilità civile. Alcune osservazioni sulle attuali proposte europee* in *Jus Civile*, 5/2023 e L. COPPINI, *Robotica e intelligenza artificiale: questioni di responsabilità civile*, in *Politica del diritto*, 2018, p. 722. È imprescindibile la puntualizzazione che non si può parlare di un'unica intelligenza artificiale, ma deve diversamente parlarsi di intelligenze artificiali al plurale, giacché le stesse possono differenziarsi, a seconda dei tipi di machine learning o di agenti software, più o meno autonomi.

[461] U. SALANITRO, *Intelligenza artificiale e responsabilità: la strategia della Commissione Europea*, in *Riv.dir.civ.*, 2020, p. 1247.

«risultato di interazioni inaspettate tra i componenti del sistema o con il contesto nel quale operino»[462].

Tali decisioni sono molto spesso opache, incontrollabili e non facilmente accertabili, determinando anche l'erroneità degli *output* e potenziali discriminazioni (tra gli altri fenomeni, si pensi al *credit scoring* che incide in Italia sulla decisione delle banche di erogare prestiti e mutui e in Cina viola la sfera privata dell'individuo[463]) e la compromissione delle «libertà e dei diritti fondamentali della personali, quali la sicurezza, la salute, la vita privata, la protezione dei dati personali, l'integrità, la dignità, l'autodeterminazione»[464].

---

[462] L. COPPINI, op.cit., p. 721. Più precisamente, l'art. 3, lett. b) della Proposta di Regolamento del Parlamento europeo e del Consiglio sulla responsabilità per il funzionamento dei sistemi di intelligenza artificiale, cit., definisce «autonomo» il «sistema basato sull'intelligenza artificiale che opera interpretando determinati dati forniti e utilizzando una serie di istruzioni predeterminate, senza essere limitato a tali istruzioni, nonostante il comportamento del sistema sia legato e volto al conseguimento dell'obiettivo impartito e ad altre scelte operate dallo sviluppatore in sede di progettazione».

[463] V. PREVITI, *Siamo davvero i nostri dati? I meccanismi distorsivi premianti di social scoring in Cina, Olanda e Italia*, in *DPCE online*, 2/2024.

[464] Sul punto cfr. M. GAMBINI, *Responsabilità civile e controlli del trattamento algoritmico*, in. P. PERLINGIERI, S. GIOVA, I. PRISCO (a cura di), *Il trattamento algoritmico dei dati tra etica, diritto e economia*, op.cit., p. 314; sull'erroneità degli output, D. DI SABATO, *Strumenti riparatori e risarcitori*, ivi, p. 338. Autorevolmente P. PERLINGIERI, *Relazione conclusiva*, ivi, p. 383, puntualizza come l'esigenza di ovviare all'opacità del procedimento algoritmico si avverta in ogni settore e che il rischio digitale si pone tanto come collettivo, quanto individuale. Avendo specifico riguardo alla protezione dei dati personali «nell'era dell'intelligenza artificiale», arguta dottrina (T.E. FROSINI, *La privacy nell'era dell'intelligenza artificiale*, in

Posto che allo stato attuale non esiste una normativa *ad hoc*, è necessario chiedersi chi sia il soggetto giuridicamente responsabile delle condotte autonome dei sistemi intelligenti[465].
Individuarlo è di estrema rilevanza, in quanto è certamente probabile che la responsabilità sia imputabile a più soggetti che intervengono nel "ciclo di vita" dei sistemi di intelligenza artificiale, creandolo, procedendo alla manutenzione e al controllo dei rischi associati[466].
Innanzitutto, è necessario rappresentare i due approcci seguiti dalla letteratura giuridica ai fini dell'identificazione del centro di imputazione della responsabilità, nei cui confronti il danneggiato possa esercitare la pretesa risarcitoria.

DPCE online, 1/2022, p. 282 ss.), dopo aver posto in evidenza che quest'ultima pone nuove questioni giuridiche riferite alla privacy, rimarca che il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, c.d. Regolamento generale sulla protezione dei dati personali, non è compatibile con i modelli attuali di gestione algoritmica dei flussi di dati personali che determinano decisioni in vari ambiti.

[465] Sul punto si v. la "Relazione della Commissione al Parlamento europeo, al Consiglio e al Comitato economico e sociale europeo sulle implicazioni dell'intelligenza artificiale, dell'Internet delle cose e della robotica in materia di sicurezza e responsabilità", 19 febbraio 2020, (COM (2020), 64 final), p. 19; cfr. le argute riflessioni di G. COMANDÈ, *Multilayered (Accountable) Liability for Artificial Intelligence*, in S. LOHSS, R. SCHULZE, D. STAUDENMAYER (a cura di), *Liability for Artificial Intelligence and the Internet of Things*, Baden, 2019, p. 169.

[466] G. CAPILLI, *I criteri di interpretazione della responsabilità*, in G. ALPA (a cura di), *Diritto e intelligenza artificiale*, op. cit, p. 477.

Parte della dottrina ha riconosciuto l'esistenza di una soggettività giuridica, quantomeno parziale, ai sistemi di intelligenza artificiale[467].

Il vantaggio sarebbe quello di limitare la responsabilità dei programmatori e degli utilizzatori dei servizi, senza però determinare un arresto del progresso tecnologico; inoltre, «la soggettività sarebbe connessa alla formazione di un patrimonio ovvero alla costituzione di un fondo assicurativo dedicato, obbligando gli operatori, che si ritenga debbano sopportare il rischio, ad effettuare conferimenti»[468]. Tale ricostruzione è stata avallata dalla letteratura giuridica che evidenzia che «non sarebbe impossibile, sotto il profilo giuridico-concettuale, potendosi ricavare il riconoscimento della soggettività giuridica dal modello delle persone giuridiche o da quello dei patrimoni separati»[469].

---

[467] *Ex multis*, G. SARTOR, *Gli agenti software: nuovi soggetti del ciberdiritto*?, in *Contr. e impr.*, 2002, 2, p. 483 ss.; G. TEUBNER, *I soggetti giuridici digitali? Sullo status privatistico degli agenti software autonomi*, Napoli, 2019, *passim* e la prefazione al volume di P. FEMIA, *Soggetti responsabili. Algoritmi e diritto civile*, ivi, p. 5 ss. Sul tema cfr. anche D. DI SABATO, *Gli smart contracts: robot che gestiscono il rischio contrattuale*, in Contr.impr., 2017, p. 389; M.L. LACRUZ MANTECÓN, *Robots y personas. Una aproximación jurídica a la subjetividad cibernética*, Reus, Madrid, 2020.

[468] G. D'ALFONSO, *Il regime di responsabilità da cose in custodia tra questioni tradizionali e "responsabilità da algoritmo"*, *EJPLT*, 2022.

[469] P. SERRAO D'AQUINO, *La responsabilità civile per l'uso di sistemi di intelligenza artificiale nella Risoluzione del Parlamento Europeo del 20 ottobre 2020 "Raccomandazioni alla Commissione sul regime della*

Inizialmente, anche le Istituzioni europee hanno aderito a tale tesi a seguito di un notevole dibattito che ha riguardato il riconoscimento della soggettività giuridica alle macchine e che ha occupato sia gli studiosi di diritto che quelli di filosofia morale[470]. Nonostante ciò, molteplici voci in letteratura hanno espresso opinioni di senso contrario, sostenendo che «debba respingersi l'idea del riconoscimento della "personalità elettronica" ai sistemi di intelligenza artificiale, dal momento che finisce con l'esaltare, in maniera esorbitante, le prerogative delle macchine che, seppure intelligenti, sono, in ogni caso, creazione dell'uomo, rispondono integralmente alla programmazione da costui prevista di fatto e sono incapaci di autodeterminazione e di libertà di scelta»[471].

---

responsabilità civile e intelligenza artificiale", § 1, in www.giustiziainsieme.it/it/news/127main/dirittoeinnovazione/ § 2.

[470] L'opportunità di attribuire una "personalità elettronica" ai robot, capaci di autoapprendimento (self-learning), è stata vagliata dalla Risoluzione del Parlamento europeo del 16 febbraio 2017, recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica (2018/C 252/25), Considerando 59, lett. F).

[471] Tra i numerosi autori, cfr. A. BERTOLINI, *Robots as Products: the case for a realistic analysis of robotics applications and liability rules*, in *Law Innov. Technol.*, 2013, 1, p. 214 ss.; L. COPPINI, op.cit., p. 722 ss.; M. COSTANZA, *L'intelligenza artificiale e gli stilemi della responsabilità civile*, in *Giur it.*, 2019, p. 1686 ss.; M. INFANTINO, *La responsabilità per danni algoritmici: prospettive europeo continentali*, in *Resp.civ.prev.*, 2019, p. 1762 ss.; U. RUFFOLO, *La responsabilità da artificial intelligence, algoritmo e smart product: per i fondamenti di un diritto dell'intelligenza artificiale self learning*, in ID. (a cura di), *Intelligenza artificiale. Il diritto, i diritti e l'etica*, op.cit., p. 93 ss.; G. FINOCCHIARO, *Intelligenza artificiale e responsabilità*, in *Contr.impr.*, 2020, p. 713 ss.; F. NADDEO, *Intelligenza artificiale: profili di*

Da qui il corollario di diritto secondo cui possono essere considerati "oggetti" e non "soggetti" di diritto, con la conseguente assenza di un *tertium genus* di responsabilità.

E' necessario dire che, dopo un'iniziale apertura a livello europeo da parte del Parlamento, nella Risoluzione del 16 febbraio 2017 già citata, tale tesi è stata progressivamente abbandonata sia dal Comitato economico e sociale europeo che ha esposto plurime perplessità di carattere giuridico ed etico[472] e successivamente dal Parlamento europeo medesimo che ha affermato che tali sistemi non possiedono «né una personalità giuridica, né una coscienza umana e che il loro compito consiste nel servire l'umanità»[473].

---

responsabilità, in *Comparazione e diritto civile*, 2020, p. 1161; L. ULISSI, *I profili di responsabilità della macchina dell'apprendimento nell'interazione con l'utente*, in G. ALPA (a cura di), *Diritto e intelligenza artificiale*, op.cit., p. 436; G. COMANDÉ, *Intelligenza artificiale e responsabilità tra liability e accountability: il carattere trasformativo dell'IA e il problema della responsabilità*, in *Analisi Giuridica dell'Economia*, 2019, p. 175.

[472] Parere del Comitato economico e sociale europeo su "L'intelligenza artificiale. Le ricadute dell'intelligenza artificiale sul mercato unico (digitale), sulla produzione, sul consumo, sull'occupazione e sulla società", 2017/C 288/01", punto 3.33.

[473] Si fa riferimento alla Proposta di Regolamento del Parlamento europeo e del Consiglio del 20 ottobre 2020 sulla responsabilità per il funzionamento dei sistemi di intelligenza artificiale (considerando 6), cit. Lo sviluppo di tecnologie emergenti solleva importanti questioni di carattere etico che sono state oggetto di esame da parte del Parlamento europeo che, lo stesso giorno, ha emanato la Risoluzione recante raccomandazioni alla Commissione, concernenti il quadro relativo agli aspetti etici dell'intelligenza artificiale, della robotica e delle tecnologie correlate (2 020/2012(INL)), sulla quale cfr. le notazioni di M. CASTILLA BAREA, *La universidad ante los desafíos éticos de la inteligencia artificial. Reflexiones a propósito del nuevo «marco*

Seguendo questo filone dottrinale, le tecnologie emergenti dovrebbero essere trattate come "beni" e la responsabilità ricadrebbe su un soggetto specifico, in relazione alle circostanze del caso concreto, tra i molteplici soggetti che sono coinvolti nella produzione, operatività o impiego dei sistemi intelligenti.

Nel dettaglio, bisogna chiedere se e sulla base di quali presupposti la responsabilità possa gravare sull'ideatore-autore-progettista dell'algoritmo che abbia veicolato l'apprendimento e l'addestramento ovvero «su colui che lo utilizzi o lo produca o lo incorpori in un prodotto oppure in un componente dello stesso; oppure, sull'utilizzatore o sul titolare ovvero sul custode del dispositivo digitale»[474].

In prima battuta, è rilevante sottolineare che «l'algoritmo, quale creazione intellettuale, pur non essendo un componente avulso dal prodotto finale, attribuisce l'anima al *software* di un'intelligenza artificiale al quale conferisce l'attitudine ad apprendere»[475].

Dunque, nell'attribuzione della c.d. responsabilità da algoritmo, la prima considerazione da fare è che "autore" e "produttore" di

---

europeo de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas», in *Edunovatic 2020, Conference Proceedings: 5th Virtual International Conference on Education, Innovation and ICT*, December 10 - 11, 2020, p. 630 ss.

[474] U. RUFFOLO, *Intelligenza artificiale, machine learning e responsabilità da algoritmo*, p. 1691.

[475] Per tutte le considerazioni che seguono, vedasi U. RUFFOLO, op. cit.

un'entità intelligente che lo inserisca in un prodotto intelligente potrebbero non essere la stessa persona, in quanto se l'algoritmo può essere qualificato come un progetto, un'idea, l'ideatore del medesimo sarebbe quindi un mero fornitore di idee e pertanto sarebbe giuridicamente complesso determinare una sua responsabilità autonoma.

Parimenti, se l'algoritmo fosse, invece, una "componente immateriale", potrebbe essere qualificato come produttore non soltanto il produttore del *software* ma anche l'inventore dell'algoritmo, nella sua qualità di fabbricante del prodotto intelligente, «in modo tale da determinare non soltanto la responsabilità contrattuale verso il proprio committente ma anche la responsabilità extracontrattuale verso i terzi danneggiati dal prodotto difettoso intelligente»[476].

Un altro elemento da valutare è l'eventualità in cui i danni provenienti dai sistemi di intelligenza artificiale derivino da *bias* che siano imputabili in forma diretta o indiretta dall'addestratore[477].

In questa circostanza, si potrebbe porre la questione della sua responsabilità da considerarsi concorrente con quella del

---

[476] G. D'ALFONSO, *Il regime di responsabilità da cose in custodia tra questioni tradizionali e "responsabilità da algoritmo"*, op. cit.

[477] Figura identificabile in colui che "addestri" un'entità artificiale intelligente e/o con quella dell'ideatore dell'algoritmo, se distinto da quest'ultimo.

produttore e/o dell'ideatore dell'entità artificiale, se distinto da quest'ultimo.

Da ultimo, si può prevedere «l'imputabilità della responsabilità per i danni cagionati da dispositivi intelligenti in capo all'utilizzatore, titolare o custode in ossequio alla relazione di custodia con il bene che costituisce il fondamento della responsabilità da cosa in custodia ex art. 2051 cod. civ»[478].

Se l'identificazione dei soggetti in astratto responsabili può essere considerata più o meno pacifica, più complesso è individuare sia il regime di imputazione che la natura della responsabilità che può essere loro attribuita[479].

La dottrina ha individuato due orientamenti. Da un lato, ci si è chiesti[480] se «le categorie giuridiche esistenti possano essere considerate congrue a rispondere alle sfide dell'intelligenza artificiale attraverso un'interpretazione ermeneutica delle norme civilistiche sulla responsabilità civile e della disciplina della

---

[478] G. D'ALFONSO, *Il regime di responsabilità da cose in custodia tra questioni tradizionali e "responsabilità da algoritmo"*, op. cit.

[479] I. GIUFFRIDA, *Liability for AI Decision-Making: Some Legal and Ethical Considerations*, in *Fordham Law Review*, 2019, 88, 2, p. 443.

[480] E. SEVERINO, N. IRTI, *Dialogo su diritto e tecnica*, Roma-Bari, 2001, pp. 28 ss.; G. ALPA, Prefazione, in ID. (a cura di), *Diritto e intelligenza artificiale*, op.cit., p. 14.

responsabilità da prodotto difettoso»[481] ovvero se, in assenza di soluzioni appropriate risulti essenziale la previsione di nuovi paradigmi di tutela che devono essere introdotti con riforme legislative di rilievo che dettino nuove regole o prevedano delle modifiche a quelle esistenti[482].

A seguito dell'importante mutamento di opinione del Parlamento europeo e della posizione assunta dal Governo italiano attraverso le proposte degli esperti del MISE[483], si ravvisa che, in assenza di

---

[481] Di tale avviso, ex multis, G. FINOCCHIARO, op. cit., pp. 713 ss; U. RUFFOLO, *La responsabilità da artificial intelligence, algoritmo e smart product*, op. cit., pp. 96 e ss; L. Coppini, op. cit., p. 739.

[482] G. TEUBNER, op.cit., pp. 26 ss.; A. SANTOSUOSSO, C. BOSCARATO, F. CAROLEO, *Robot e diritto: una prima ricognizione*, in *Nuova giur.civ.comm*., 2021, p. 494 ss.; R.M. AGOSTINO, *Intelligenza artificiale e processi decisionali*, in *Mercato Concorrenza Regole*, 2020, p. 373; G. COMANDÉ, *Intelligenza artificiale e responsabilità tra liability e accountability*, op.cit., p. 170; C. LAENZA, *Intelligenza artificiale e diritto: ipotesi di responsabilità civile nel terzo millennio*, in *Resp.civ. prev.*, 2021, p. 118.

[483] Se inizialmente il Parlamento europeo, con la Risoluzione del 16 febbraio 2017, recante raccomandazioni alla Commissione concernenti norme di diritto civile sulla robotica, cit., esortava la Commissione all'adozione di un intervento legislativo innovativo sulle questioni giuridiche attinenti allo sviluppo e all'impiego della robotica e dell'intelligenza artificiale; in un secondo momento, con la Risoluzione del 12 febbraio 2019, relativa a una politica industriale europea globale in materia di robotica e intelligenza artificiale (2018/2088(INI)), il Parlamento europeo ha diversamente chiesto alla Commissione di riesaminare i regimi esistenti di responsabilità correttamente funzionanti, allo scopo verificarne la congruità; inoltre, nell'allegato A della Risoluzione del 20 ottobre 2020, recante raccomandazioni alla Commissione europea su un regime di responsabilità civile per l'intelligenza artificiale, cit., nel formulare gli obiettivi della suddetta proposta di regolamento sulla responsabilità per il funzionamento dei sistemi di intelligenza artificiale, ha dichiarato che, invece di sostituire i

una normativa specifica *ad hoc* e prima che si preveda la necessità della stessa, sia dirimente effettuare una valutazione ermeneutica della sussumibilità delle nuove forme di danno nelle categorie già esistenti.

In quest'ottica bisogna individuare le potenziali situazioni di conflitto che possano essere causate dai nuovi sistemi intelligenti con specifico riferimento a circostanze che richiedono una differente gradazione di responsabilità – come accade per i danni cagionati in ambito sanitario e come verrà analizzato nella sezione che segue – e a soluzioni concernenti il caso concreto.

Dunque, è necessario effettuare un'interpretazione sistematica ed assiologica evolutiva[484] della disciplina attualmente vigente senza perdere di vista né la prospettiva *de iure condendo* in ambito europeo né il granitico sistema assiologico vigente nell'ordinamento italiano, effettuando un bilanciamento degli

---

regimi esistenti di responsabilità correttamente funzionanti, è opportuno operare gli adeguamenti necessari per l'intelligenza artificiale. Tale approccio è stato condiviso, in assenza di una normativa ad hoc, dal Governo italiano, con le "Proposte per una strategia nazionale per l'Intelligenza Artificiale", elaborate, a luglio 2020, dal Gruppo di esperti dell'innovazione tecnologica, istituito presso il Ministero dello Sviluppo Economico, punto 5.1.2. Al riguardo, cfr. C. PERLINGIERI, *Responsabilità civile e robotica medica*, in *Tecnologie e diritto*, 2020, p. 162 s.

[484] È necessario seguire l'influente insegnamento di P. PERLINGIERI nel suo scritto *L'interpretazione della legge come sistematica ed assiologica: il brocardo in claris non fit interpretatio, il ruolo dell'art. 12 disp. Prel. Codice civile e la nuova scuola dell'esegesi*, in *Rass. Dir. Civ.* 1985.

interessi contrapposti con assoluta centralità e primazia della persona umana sulle ragioni del mercato.

5.6.1. Lo stato dell'arte dell'invocabilità delle già esistenti categorie civilistiche di responsabilità.

Innanzitutto, nella riconducibilità delle nuove forme di danno nelle categorie civilistiche di responsabilità già esistenti è necessario analizzare due aspetti[485].

Il primo attiene alla responsabilità in capo al produttore in quanto le nuove forme di tecnologia che sono parte di beni e servizi possono determinare nuovi rischi per la sicurezza degli acquirenti e degli utenti; il secondo riguarda la diversità delle normative in materia di responsabilità degli Stati dell'Unione.

Dunque, prima di analizzare le discipline italiane in materia, è opportuno richiamare la normativa europea riguardante la responsabilità da prodotto difettoso che «concerne il risarcimento dei danni cagionati da difetti di fabbricazione di un prodotto, introducendo un regime di responsabilità oggettiva che prescinde dall'accertamento della colpa»[486].

---

[485] U. SALANITRO, *Intelligenza artificiale e responsabilità: la strategia della Commissione europea* in *Rivista di diritto civile*, p. 1253, 6/2020.

[486] La disciplina è attualmente dettata dalla direttiva comunitaria 85/374/CE del Consiglio del 25 luglio 1985 sulla responsabilità per danni da prodotti

Tale disciplina potrebbe in astratto essere applicata ricomprendendo i sistemi di intelligenza artificiale nella nozione di "prodotto"[487] e prevedendo la sussistenza del difetto[488] all'interno di un errore di progettazione, programmazione – e dunque l'algoritmo – o di costruzione[489].

Tenuto conto dei sistema di intelligenza artificiale *self-learning*, della qualificazione dell'algoritmo quale componente immateriale del dispositivo intelligente potrebbe scaturire la responsabilità dell'ideatore dell'algoritmo, se diverso dal produttore dell'entità intelligente che lo incorpori in ossequio alla norma che stabilisce che «la responsabilità è da configurarsi sia in capo al produttore

---

difettosi, ormai confluita in Italia nel Codice del Consumo, negli artt. 114 ss. La direttiva si inserisce nell'ambito di un quadro normativo europeo di riferimento, nel quale rientrano provvedimenti che sono espressione dell'attuazione del principio di precauzione, quale strumento per gestire l'incertezza, facendo sì che la responsabilità da danno da prodotto difettoso sia traslata ai soggetti produttori (U. IZZO, *La precauzione nella responsabilità civile*, Padova, 2004, p. 1).

[487] Ai sensi dell'articolo 2 della direttiva e dell'articolo 115, comma 1, Cod. Cons. che lo definiscono come «ogni bene mobile, anche se forma parte di un altro bene mobile o immobile».

[488] Ai sensi degli articoli 6 della direttiva e 117 cod. cons. che qualificano un prodotto "difettoso" «quando non offre la sicurezza che ci si può legittimamente attendere tenuto conto delle circostanze».

[489] Sul punto e per le riflessioni che seguono, cfr. L. COPPINI, op.cit., pp. 727-729; U. RUFFOLO, *Intelligenza artificiale, machine learning e responsabilità da algoritmo*, op.cit., p. 1693 ss., specialmente p. 1698. Sul ruolo che la responsabilità da prodotto difettoso è adeguata a svolgere nel governo dei nuovi rischi attinenti allo sviluppo delle tecnologie digitali, si v. anche R. MONTINARO, *Responsabilità da prodotto difettoso e tecnologie digitali tra soft law e hard law*, in *Persona e mercato*, 2020/4, p. 365 ss.

che realizza il prodotto finito, sia del produttore della materia prima o di un componente dello stesso»[490].

La criticità evidenziata da plurima dottrina quanto all'applicabilità di tale forma di responsabilità è che il paradigma della responsabilità da prodotto difettoso non copre la totalità dei nuovi danni derivanti dall'intelligenza artificiale, «in quanto applicabile alle ipotesi in cui i pregiudizi siano cagionati da un errore di progettazione, programmazione o costruzione»[491].

---

[490] Art. 3 della direttiva e art. 115, comma 2 bis del Codice del Consumo.

[491] Si rimarchi, vieppiù, che la disciplina della responsabilità del produttore solleva una serie di perplessità sull'idoneità a far fronte a tutte le sfide poste dall'intelligenza artificiale. Le perplessità sollevate dalla dottrina attengono a più profili. Si dubita precipuamente che i moderni prodotti di intelligenza artificiale, quantomeno i più avanzati, possano rientrare nella tradizionale definizione di «prodotto», dal momento che i sistemi di *deep learning* (apprendimento automatico) e di *full automation* (automazione completa) agiscono in piena autonomia, secondo processi non sempre controllabili da parte dei produttori. Per un attento esame della questione cfr. *ex multis*, I. ZURITA MARTÍN, *La responsabilidad civil por los daños causados por los robots inteligentes como productos defectuosos*, Reus, Madrid, 2020, *passim*; recensito da F. J. JIMÉNEZ MUÑOZ, in *Actualidad Jurídica Iberoamericana* Nº 14, febrero 2021, p. 1141 ss.; C. LAENZA, op.cit., p. 1018; A. BERTOLINI, *Artificial Intelligence and Civil Liability*, in *Study Requested by the JURI committee, Policy Department for Citizens' Rights and Constitutional Affairs Directorate General for Internal Policies*, Bruxelles, 2020, p. 56; U. RUFFOLO, *Responsabilità da produzione e gestione dell'a.i. self-learning*, in P. PERLINGIERI, S. GIOVA, I. PRISCO (a cura di), *Rapporti civilistici e intelligenze artificiali: attività e responsabilità*, op.cit., p. 233 ss. Assume pertanto pregnante rilievo l'iniziativa della Commissione europea che, il 28 settembre 2022, ha presentato la proposta per una direttiva del Parlamento europeo e del Consiglio sulla responsabilità per prodotti difettosi (Brussels, 28.9.2022 COM(2022) 495 final 2022/0302 (COD)), nell'ambito di un pacchetto di due proposte di direttive che dovranno essere approvate dal

Dunque, dopo aver effettuato la necessaria premessa di carattere unionale, è opportuno analizzare le categorie civilistiche di responsabilità.

Se, infatti, l'articolo 2043 del codice civile assume rilievo in quanto previsione di carattere generale che è per sua natura atipica e dunque applicabile a qualsiasi tipologia di illecito, la struttura della norma sarebbe di per sé insufficiente in quanto «il danneggiato si troverebbe di fronte a difficoltà probatorie nel dimostrare la sussistenza dei presupposti della responsabilità, in riferimento non soltanto all'evento oggettivo del nesso di causalità tra l'attività del sistema intelligente e l'evento dannoso, ma

---

Parlamento europeo e dal Consiglio, finalizzato ad adeguare le norme sulla responsabilità civile all'economia circolare, all'era digitale ed all'impatto delle catene globali del valore, garantendo l'allineamento necessario tra questi due strumenti giuridici necessari. La prima propone la revisione della disciplina dettata dalla direttiva sulla responsabilità per danno da prodotti difettosi, ponendosi gli obiettivi di dare alle imprese la certezza giuridica e la parità di condizioni di cui necessitano per investire in prodotti nuovi ed innovativi e di garantire ai soggetti danneggiati da prodotti difettosi un elevato livello di tutela di cui abbiano bisogno, al fine di incentivare l'impiego di prodotti digitali. La Commissione europea ritiene che la modernizzazione della direttiva europea che, per quasi quarant'anni, ha assicurato la sicurezza legale ai cittadini, fornendo loro gli strumenti per la richiesta di un risarcimento di danni causati da prodotti difettosi, sia necessaria per aggiornare le regole al nuovo contesto di trasformazione verde e digitale, in particolar modo per adattarle alle nuove tecnologie, come l'intelligenza artificiale.

soprattutto con riguardo all'elemento soggettivo della colpevolezza del danneggiante»[492].

Parte della dottrina[493] ha ripreso le disposizioni disciplinanti le tradizionali ipotesi di responsabilità vicaria, relative al danno cagionato da soggetti diversi dal chiamato a risarcire, facendo riferimento all'art. 2048 cod. civ.

Secondo tali autori, «la responsabilità del programmatore o dell'addestratore dei sistemi di intelligenza artificiale sarebbe da equiparare alla posizione del precettore, nella sua accezione di figura preposta ad istruire gli allievi, assimilando il sistema intelligente ad un apprendista; dunque, gli stessi dovrebbero rispondere dei danni causati dal sistema, a meno che non dimostrino di non aver potuto impedire il fatto»[494].

La tesi, però, è agevolmente confutabile dal momento che bisogna escludere sia il ricorso all'art. 2048 che all'art. 2047 del codice in

---

[492] G. D'ALFONSO, *Il regime di responsabilità da cose in custodia tra questioni tradizionali e "responsabilità da algoritmo"*, op. cit. e Tra gli altri, U. SALANITRO, op. cit., p. 1247; A. AMIDEI, op. cit. p. 96; F. NADDEO, op. cit. p. 1151.

[493] M. COSTANZA, *Robot e impresa*, in U. RUFFOLO (a cura di), *Intelligenza artificiale e responsabilità*, Milano, 2017, p. 112 s; A. SANTOSUOSSO, M. TOMASI, *Diritto, scienza, nuove tecnologie*, Padova, 2021, p. 333 e ss.; U. PAGALLO, *The law of robots. Crimes, contracts and torts*, New York, 2013, p. 128 s. ritiene che tale regime sia preferibile ad altri di responsabilità extracontrattuale, unitamente all'art. 2050 c.c.

[494] G. D'ALFONSO, *Il regime di responsabilità da cose in custodia tra questioni tradizionali e "responsabilità da algoritmo"*, op. cit.

quanto tali norme sono «dirette a regolamentare le responsabilità discendenti dal controllo o dall'educazione di particolari "tipi" di esseri umani, statuendo così una disciplina molto settoriale»[495].

Inoltre, l'applicazione analogica dell'art. 2049 del Codice civile, nel delineare la responsabilità dell'imprenditore per i danni cagionati da un sistema intelligente preposto allo svolgimento di mansioni connesse alla propria attività finisce con l'individuare gli elementi costitutivi della fattispecie nel rapporto di preposizione e nel nesso di causalità tra lo svolgimento delle mansioni e il danno provocato al soggetto terzo, determinandone l'impossibilità di applicazione.

Infatti, «la *ratio* della norma consiste nella responsabilizzazione del committente, per una determinata ipotesi di errore dell'intelligenza umana del suo commesso e sarebbe complicato interpretare esclusivamente la norma in riferimento ai danni causati dal loro comportamento o dalle decisioni di sistemi non umani, a causa di un difetto della loro intelligenza artificiale»[496].

Dunque, è necessario richiamare e analizzare la disciplina della responsabilità da cose in custodia, attraverso l'interpretazione

---

[495] U. RUFFOLO, *Intelligenza artificiale, machine learning e responsabilità da algoritmo*, op.cit., p. 1698. In posizione critica si v. anche L. COPPINI, op.cit., p. 726; G. FINOCCHIARO, *Intelligenza artificiale e diritto. Intelligenza artificiale e protezione dei dati personali*, in *Giur. It.*, 2019, p. 1657.

[496] G. G. CRUDELI, *Sistemi di intelligenza artificiale autonomi e responsabilità datoriale*, in *Diritto della sicurezza sul lavoro*, 2/2024.

evolutiva dell'art. 2051 in via sistematica, tenendo conto sia dell'ambito di applicazione delle "responsabilità speciali" sia del perimetro della "responsabilità da prodotto difettoso".

Innanzitutto, l'art. 2050 tratta la responsabilità per l'esercizio di attività pericolose e una parte di letteratura giuridica ha richiamato tale norma assumendo che «l'impiego dell'intelligenza artificiale rappresenti un'attività pericolosa, per il semplice utilizzo di sistemi intelligenti»[497].

Si reputa che «qualora si consenta ad un automa dotato di capacità adattive e di apprendimento di interagire con un uomo, non esista alcuna sicurezza che lo stesso non possa tenere comportamenti lesivi dei diritti dei terzi»[498].

Il ricorso all'art. 2050 «avrebbe inoltre il pregio di attribuire al soggetto danneggiato una possibile strada alternativa rispetto alla

---

[497] L. COPPINI, op.cit., p. 735 afferma che si potrebbe reputare che sia divenuta pericolosa l'attività di produzione di macchine ad elevata automazione «in funzione dei nuovi pericoli di fallibilità del prodotto» ed applicare l'art. 2050 c.c., imputando la responsabilità allo sviluppatore dell'intelligenza artificiale. Cfr. anche M. SCIALDONE, *Il diritto dei robot: la regolamentazione giuridica dei comportamenti non umani*, in E. PIETRAFESA, F. MARZANO, T. MEDICI (a cura di), *La rete e il fattore C: Cultura, Complessità, Collaborazione*, Volume II, Roma, Stati Generali dell'Innovazione, 2016, p. 76; A. SANTOSUOSSO, M. TOMASI, op.cit., p. 329 ss.

[498] Tra gli altri, Cfr. C. LAENZA, op. cit. 1018.

responsabilità per prodotto difettoso, al fine di ottenere il ristoro dei danni subiti»[499].

Tale soluzione non è condivisa in letteratura[500], visto che «l'intelligenza artificiale non è intrinsecamente pericolosa e non le si addice tale attributo, dal momento che essendo il simbolo della tecnica è, per ciò stesso, più affidabile dell'uomo rappresentando, dall'altra parte, un mezzo correttivo o integrativo delle imprecisioni umane»[501].

Al contrario, «potrebbe accadere che la pericolosità non concerna l'attività svolta dai sistemi intelligenti in sé, quanto piuttosto le interazioni del sistema con il mondo esterno. Pertanto, potrebbe succedere che un'attività produttiva, ritenuta fino ad oggi non pericolosa, lo divenga con l'ingresso dell'intelligenza artificiale nel processo di produzione o direttamente nel prodotto: si pensi ad esempio alla circolazione dei veicoli che, potendo assumere connotati di pericolosità, potrebbe essere attratta dalla disciplina dell'art. 2050 Codice civile»[502].

---

499 A. AMIDEI, *Intelligenza artificiale e product liability: sviluppi del diritto dell'Unione Europea*, in *Giur. It*., 2019, p. 1725 ss.

500 G. D'ALFONSO, *Il regime di responsabilità da cose in custodia tra questioni tradizionali e "responsabilità da algoritmo"*, *EJPLT*, op. cit.

501 M. COSTANZA, *L'intelligenza artificiale e gli stilemi della responsabilità civile*, op. cit., p. 1688.

502 G. D'ALFONSO, *Il regime di responsabilità da cose in custodia tra questioni tradizionali e "responsabilità da algoritmo"*.

Dunque, la disciplina della responsabilità da attività pericolosa può essere invocata, in via interpretativa, in concorrenza con quella della responsabilità da prodotto difettoso, al fine di «imputare la responsabilità per i danni causati da sistemi intelligenti al produttore di un bene che incorpori l'intelligenza artificiale e, qualora non coincida con quest'ultimo, all'autore dell'algoritmo che conferisca al dispositivo la capacità di apprendere»[503].

Si perviene a tale tesi, partendo dalla giurisprudenza[504] che accorda come concorrente la tutela offerta dal regime di cui all'art. 2050 Codice civile, anche nelle ipotesi di danno da prodotto difettoso, qualora la sua fabbricazione o la sua distribuzione si riveli qualificabile come attività pericolosa[505].

---

[503] *Ibidem*.

[504] Si ricordi che, sia la normativa europea sia quella nazionale prevedono che alla responsabilità del produttore si cumulano quelle previste da tutte le altre norme.

[505] Il cumulo delle due discipline assumerebbe peculiare connotazione, in relazione all'alta incidenza nel settore dell'intelligenza artificiale del c.d. rischio da sviluppo che, come noto, rappresenta una causa di esclusione della responsabilità per danno da prodotto difettoso. Il rischio da sviluppo, quando sia molto elevato, potrebbe costituire una situazione specifica di attività qualificabile come pericolosa, proprio in quanto diretta a produrlo. Tale circostanza legittimerebbe l'applicazione dell'art. 2050 c.c., soprattutto in settori innovativi e a rapida evoluzione, quale quello dell'intelligenza artificiale, in cui sovente le conoscenze tecniche, relative alla potenziale difettosità di un dispositivo intelligente, sono assenti al momento della sua

Con riferimento alla responsabilità da cosa in custodia, l'art. 2051 andrebbe letto congiuntamente all'art. 2052, relativo alla responsabilità per i danni cagionati da animali[506], in quanto in entrambe le norme il criterio di imputazione consiste nella custodia con il solo limite del caso fortuito.

Secondo altra parte di dottrina[507], l'interprete potrebbe imputare la responsabilità da intelligenza artificiale all'utilizzatore o al titolare oppure al custode, richiamando o l'art. 2052 o l'art. 2051 in relazione al fatto che «si configuri il dispositivo intelligente quale un'entità dinamica ed evolutiva come un animale, oppure in una logica naturalistica che sottolinei che lo stesso non è né un

commercializzazione e sopravvengono successivamente, quando il prodotto è già sul mercato e sono tali da classificarlo come difettoso. Si condividono le argomentazioni di U. RUFFOLO, op.ult.cit., pp. 1684-1697.

[506] G. D'ALFONSO, *Il regime di responsabilità da cose in custodia tra questioni tradizionali e "responsabilità da algoritmo"* op. cit.; U. RUFFOLO, op.ult.cit., pp. 1699, parla dell'art. 2052 come norma fotocopia dell'art. 2051.

[507] Per le osservazioni sull'applicabilità degli artt. 2051 e 2052 c.c. in tale contesto, G. D'ALFONSO, *Il regime di responsabilità da cose in custodia tra questioni tradizionali e "responsabilità da algoritmo"*, cfr. L. COPPINI, op.cit., p. 734; A. SANTOSUOSSO, C. BOSCARATO, F. CAROLEO, op.cit., p. 495; U. RUFFOLO, op.ult.cit., p. 1699; M. SCIALDONE, op.cit., p. 78; Gruppo Di Esperti Mise, *Proposte per una strategia italiana per l'intelligenza artificiale*, p. 50; M. RATTI, *Riflessioni in materia di responsabilità civile e danno cagionato da dispositivo intelligente alla luce dell'attuale scenario normativo*, in *Contr.impr.*, 2020, p. 1174 ss.

animale, né un essere umano ma rientra viceversa nella categoria delle cose in senso proprio»[508].

In realtà, anche l'adesione all'art. 2052 va respinta[509] in quanto sebbene il comportamento degli animali sia imprevedibile come quello dei dispositivi intelligenti[510], il proprietario dell'animale, tramite l'addomesticamento, effettua un controllo sulla capacità di reazione dell'animale mentre il titolare/utilizzatore/custode dei dispositivi intelligenti non soltanto non conosce, di base i meccanismi di funzionamento e di reazione al mondo esterno ma ha anche una limitata, o nulla, possibilità di incidere sui loro comportamenti e sulle loro decisioni[511].

Anche il richiamo alla responsabilità da cose in custodia ha sollevato numerose critiche in letteratura.

Da un lato, si è affermato che «l'art. 2051 fa riferimento ad una *res* inanimata e che perciò rappresenterebbe un'entità lontana dai

---

[508] L. FORT, V. IEVA, *Intelligenza artificiale, responsabilità civile e interpretazione analogica*, in www.biodiritto.org, 8/2020, p.2.

[509] F. NADDEO, op.cit., p. 1158; M. SCIALDONE, op.cit., p. 79. Contra A. BERTOLINI, *Robots as Products*, op. cit., p. 227 fa leva sulla differenza tra animale e dispositivo intelligente.

[510] M. BASSINI, L. LIGUORI, O. POLLICINO, *Sistemi di intelligenza artificiale, responsabilità e accountability. Verso nuovi paradigmi*, in F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018, p. 333 ss.

[511] A. LIOR, *AI Entities as AI Agents: Artificial Intelligence Liability and the AI Respondeat Superior Analogy*, in *Mitchell Hamline Law Review*, 2020, 46, 5, 2, pp. 1060-1062.

dispositivi intelligenti che sono capaci di comportamenti e decisioni, senza la supervisione umana»[512].

Si è anche sostenuto che «il parametro della custodia potrebbe risultare inidoneo, in considerazione della circostanza che la custodia di un dispositivo intelligente, soprattutto se autonomo, sarebbe eccessivamente complessa e squilibrata per il custode che potrebbe non essere in grado di controllarlo. Ancora, qualora il titolare/utilizzatore/custode fosse citato in giudizio, la prova dell'esimente del caso fortuito, concernente l'imprevedibilità della decisione o del comportamento del dispositivo, potrebbe divenire insormontabile»[513].

Secondo altra dottrina[514], l'applicazione dell'art. 2051 del Codice civile quale forma di responsabilità oggettiva, è applicabile quando il dispositivo intelligente non costituisce «un mezzo di causazione del pregiudizio, per mezzo di un'autonoma azione del titolare/utilizzatore/custode, quanto, viceversa, fonte stessa del danno». In tale ipotesi la sussumibilità della responsabilità in tale

---

[512] M. COSTANZA, *L'intelligenza artificiale e gli stilemi della responsabilità*, op.cit., p. 1687; G. SARTOR, *Gli agenti software e la disciplina giuridica degli strumenti cognitivi*, in *Dir.Inf. Informatica*, 2003, p. 55 ss.

[513] L. FORT, V. IEVA, *Intelligenza artificiale, responsabilità civile e interpretazione analogica*, op. cit., p. 15 che rimarcano che quanto detto inciderebbe sulle scelte economiche dei consumatori che, in qualità di utilizzatori finali, sarebbero disincentivati ad acquistare i prodotti suddetti.

[514] M. RATTI, op. cit., p. 1174 ss.

categoria giuridica sarebbe ragionevole, in quanto «il dispositivo intelligente ha una natura evolutiva ed autonoma, caratteristica che lo distingue dagli esseri inanimati ed il danno sarebbe, in realtà, insito nel dinamismo intrinseco della "cosa intelligente"»[515].

È necessario sottolineare che l'imputabilità della responsabilità in capo all'utilizzatore, al titolare o al custode del dispositivo digitale deriverà dalla qualificabilità della relazione tra questi e lo stesso in termini di rapporto di custodia[516] e dalla sussistenza o dalla perdita di possibilità di controllarne le condizioni di rischio[517].

La disciplina in questione non potrà essere applicata se il dispositivo rappresenta un sistema chiuso, in tale ipotesi il produttore dell'*hardware* non consentirà l'utilizzo di *software* di aziende che non siano espressamente autorizzate e quindi il titolare/utilizzatore/custode non potrà avere alcuna ingerenza sulle condizioni di rischio del dispositivo in oggetto, mentre nel caso di sistema aperto, gli stessi soggetti avranno un certo livello di

---

[515] G. D'ALFONSO, *Il regime di responsabilità da cose in custodia tra questioni tradizionali e "responsabilità da algoritmo"op.cit.*

[516] Ossia la sussistenza o meno del "potere di governo" che tali soggetti esercitano sulla "cosa".

[517] Per le argomentazioni che seguono, relative all'imputazione della responsabilità ex art. 2051 c.c., cfr. U. SALANITRO, op.cit., p. 1257 ss. che richiama G. WAGNER, *Robot liability*, in S. LOHSSE, R. SCHULZE, D. STAUDENMAYER (a cura di), *Liability for Artificial Intelligence and the Internet of Things*, Baden-Baden, 2019, p. 49 ss

controllo sui *software* utilizzati e dunque potranno essere ad essi imputati i danni cagionati dai dispositivi intelligenti c.d. open.

Tale forma di responsabilità è stata riconosciuta in letteratura[518] anche in capo a chi "addestri" un'entità artificiale intelligente o la esponga ad "esperienze" idonee ad istruirla in concomitanza con la responsabilità del produttore del dispositivo e/o con l'ideatore dell'algoritmo, se distinto da questo.

Nel dettaglio, tale responsabilità deriva dalla circostanza che «tale soggetto utilizza o gestisce la "cosa" munita di intelligenza artificiale *self-learning*, indirizzandola verso una *mentalitè* capace di sconfinare in comportamenti malevoli o devianti, senza, tuttavia, prevedere meccanismi inibitori. L'addestratore sarebbe, quindi, responsabile per i danni provocati dalla cosa intelligente giacché i comportamenti della stessa, seppure non indirizzati da tale soggetto, sarebbero sicuramente il frutto e la conseguenza del suo insegnamento o dell'apertura del dispositivo ad esperienze da questi condotte»[519].

In conclusione, e prima di affrontare nella prossima sezione la questione inerente ai dispositivi medici intelligenti e la responsabilità per danni derivanti dal robot in ambito sanitario,

---

[518] Tra gli altri, U. RUFFOLO, nei suoi scritti pluricitati.

[519] G. D'ALFONSO, *Il regime di responsabilità da cose in custodia tra questioni tradizionali e "responsabilità da algoritmo" op. cit.*

l'applicazione della disciplina della responsabilità aquiliana alle nuove forme di danno solleva rilevanti difficoltà in ordine all'onere probatorio gravante sul soggetto danneggiato.
Infatti, si aderisce alla tesi portata avanti da autorevole dottrina con riferimento all'invocabilità di regimi di responsabilità oggettiva quali la responsabilità da attività pericolose o da cose in custodia ma si attende l'intervento delle istituzioni euro unitarie per provvedere all'adeguamento del diritto ai mutamenti tecnologici della società civile, così come accaduto con il Regolamento 1689/2024 (AI act).

Sezione II

6.4. Dispositivi medici AI-based: produzione e regolamentazione.

Se nella sezione precedente si è a lungo parlato della problematica legata alla disciplina della responsabilità civile applicabile per i danni cagionati dall'impiego dell'intelligenza artificiale, nel paragrafo in oggetto e in quelli che seguiranno si intende trattare dapprima la produzione e la regolamentazione dei dispositivi medici intelligenti e secondariamente la questione inerente alla responsabilità del medico che se ne serve.

Sebbene le evidenze scientifiche mostrino in maniera univoca che l'utilizzo di *medical device AI based* fornisca dei risultati virtuosi sia in termini di efficienza del sistema sanitario sia di miglioramento dello *standard* di cura nel paziente, lo stesso elemento fondante dell'intelligenza artificiale che risiede nella capacità di apprendimento e di evoluzione autonoma costituisce il fattore di rischio più grande quando lo stesso impatta sul bene primario per eccellenza che è la salute.

Infatti, stante la natura non statica dei dispositivi medici intelligenti, è ravvisabile la possibilità di avere degli esiti imprevedibili e inesplicabili e dunque la regolazione dell'intelligenza artificiale, la sua produzione e l'impiego per scopi sanitari è divenuta di primaria importanza per il moderno giurista, sia «sugli eventuali limiti da apporre per l'impiego dell'AI in sanità, sia per la stessa autonomia dell'AI, anche in relazione ai poteri e ai doveri di controllo e sorveglianza in capo all'essere umano "in command"»[520], che facendo riferimento ad una corretta allocazione della responsabilità.

[520] A. AMIDEI, *La produzione di dispositivi medici AI-based: regolazione e responsabilità*, in U. RUFFOLO, M. GABBRIELLI (a cura di), *Intelligenza artificiale, dispositivi medici e diritto. Un dialogo tra saperi: giuristi, medici e informatici a confronto*, p. 122.

Innanzitutto, con riferimento alla regolazione *ex ante*, il principale riferimento in materia è il Regolamento UE 2017/745[521] che riscrivendo la disciplina di cui all'abrogata Direttiva 93/42/CEE non ne ha modificato radicalmente l'assetto sia con riguardo alla struttura dei controlli preventivi finalizzati all'apposizione della marcatura CE o alla cosiddetta dichiarazione di conformità UE; alla suddivisione dei *device* in classi di rischio e ai controlli di follow-up a seguito dell'immissione in commercio dei medesimi.
Il Regolamento individua una pluralità di doveri e di responsabilità incombenti sia sul produttore del dispositivo, sia sull'importatore – colui che immette sul mercato dell'Unione un dispositivo proveniente da un Paese terzo – sia sul distributore che sul cosiddetto mandatario del fabbricante – il soggetto che deve essere nominato come rappresentante dal produttore nell'eventualità in cui questo sia stabilito in uno Stato al di fuori dell'UE[522].

---

[521] Regolamento UE 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medici, entrato in vigore il 25 maggio 2017. L'abrogazione delle previgenti direttive in materia e l'applicazione di talune disposizioni del Regolamento, inizialmente prevista per il 26 maggio 2020, è stata rinviata, per il Covid, al 26 maggio 2021. Sul regolamento vedasi il commento di A. PISANI TEDESCO, *Il nuovo quadro normativo europeo dei dispositivi medici*, in *Dir. Comm. Int.* 2022, 3, p. 675 ss. Alla predetta norma si affianca, poi, il Regolamento UE 2017/746 del Parlamento europeo e del Consiglio del 5 aprile 2017, relativo ai dispositivi medico-diagnostici in vitro, applicabile a partire dal 26 maggio 2022.
[522] Tra gli altri, M. CENINI, *La responsabilità solidale del "mandatario" nell'ambito della disciplina europea sui dispositivi medici*, in *Resp. Civ. e prev.*, 2020, 5, p. 1401 e ss.

Tali previsioni dovranno essere lette sia in combinato con le normative di "*product safety*"[523] sia con il Regolamento sull'Intelligenza Artificiale.

Dal punto di vista meramente definitorio, l'art. 2 del Regolamento qualifica come "dispositivo medico" «*qualunque strumento, apparecchio, apparecchiatura, software, impianto, reagente, materiale o altro articolo destinato dal fabbricante ad essere impiegato sull'uomo, da solo o in combinazione»* per finalità mediche, ossia per porre in essere, mediante mezzi non farmaceutici, attività di «*diagnosi, prevenzione, monitoraggio, previsione, prognosi, trattamento o attenuazione* di malattie o disabilità, di *studio, sostituzione o modifica dell'anatomia oppure di un processo o uno stato fisiologico o patologico»* oppure di esame di campioni provenienti dal corpo umano al fine di fornire informazioni.

---

[523] Il Regolamento afferisce, infatti, al corpus definito di "normativa verticale" inerente alla sicurezza dei prodotti, come norme settoriali che si innestano su una "normativa orizzontale" che sancisce il generale obbligo di immettere sul mercato prodotti sicuri che è rappresentata dalla Direttiva 2011/95/CE.
Con riferimento a quest'ultima è stata approvata del legislatore UE una Direttiva volta alla sua abrogazione e sostituzione, al fine di adeguare la normativa all'espansione del commercio elettronico e al progresso delle tecnologie emergenti. Per una visione d'insieme sul punto, tra gli altri, E. Al MUREDEN, *La responsabilità del fabbricante nella prospettiva della standardizzazione delle regole sulla sicurezza dei prodotti* in E. Al MUREDEN, *La sicurezza dei prodotti e la responsabilità del produttore. Casi e materiali*, Torino, 2017, p. 1 ss.

Dunque, "dispositivo medico" è ogni *device* al quale il produttore abbia attribuito uno scopo di natura "medico sanitaria" intendendosi per tale il fine di «monitorare, ristorare, correggere e modificare in modo apprezzabile e dunque non per via meramente farmacologica funzioni fisiologiche degli esseri umani»[524].

Ai fini del lavoro in oggetto, il Regolamento ha definitivamente chiarito la questione dell'estensione delle normative in tema di sicurezza dei prodotti in ordine ai dispositivi medici anche al *software* – e dunque ai sistemi *AI-based* – anche nell'eventualità in cui il dispositivo medico sia un *software*, assumendo un rilievo importante che sia «specificamente destinato dal fabbricante ad essere impiegato per una o più destinazioni d'uso mediche indicate nella definizione di dispositivo medico»[525], anche ai fini del riparto delle responsabilità, come si dirà a breve.

Resta, invece, escluso dalla nozione di dispositivo medico «il *software* destinato a finalità generali, anche se utilizzato in un

[524] In tali termini si era espressa anche la giurisprudenza della Corte di Giustizia UE, in particolare, Corte Gust. UE, 15 gennaio 2009, C-140/07, Hecht-Pharma in Rass. Dir. Farm., 2009, 2, 427 e ss.; Corte Giust. UE, 30 aprile 2009, C-27/08 Bios Naturproductke in Ragiusan, 2009, 305; Corte Giust. UE, 22 novembre 2012, C-219/11, Brain Products in Rass. Dir. Farm. 2013,4, 939 ss.

[525] Considerando n. 19 del Regolamento in oggetto.

contesto sanitario, o il *software* per fini associati allo stile di vita e al benessere»[526].

Il Regolamento in oggetto individua quattro classi di rischio – classe I, IIA, IIb e III – parametrate alla destinazione d'uso e all'interazione con il paziente considerando grado e tipologia di invasività e durata del contatto con il corpo umano[527].

Se per la prima categoria di dispositivi è sufficiente un'autocertificazione, per le altre è necessaria l'approvazione della marcatura di conformità da parte di un organismo verificato. Inoltre, l'utilizzo del criterio del contatto umano e dell'invasività del medesimo ai fini della classificazione del dispositivo incontra notevoli criticità quando si tratta dei *device* in oggetto.

Si pensi che quando si parla di «*software* avanzati, anche *AI-based*, utilizzati per l'esame dei dati clinici a fini di elaborazione di diagnosi o ancora a sistemi di personalizzazione terapeutica, per i quali l'effettivo contatto fisico con il corpo umano risulterebbe quantomeno limitato, potendo tuttavia il funzionamento del dispositivo rivelarsi particolarmente incidente sulla salute del paziente»[528].

---

[526] *Ibidem*.

[527] Per un'analisi sul punto, F. LAGIOIA, *L'intelligenza artificiale in sanità, un'analisi giuridica*, Torino, 2020, p. 85 ss.

[528] A. AMIDEI, op. cit.

In aggiunta, non può non evidenziarsi la necessità di una disciplina specifica per superare l'intrinseca opacità dei dispositivi intelligenti che potrebbe condurre alla necessità di una valutazione da parte di organismi notificati *ex ante,* se si considera, ad esempio, l'eventualità in cui venga immesso nel commercio un farmaco c.d. intelligente[529].

È inoltre evidente che le prescrizioni dei doveri di monitoraggio *ex post* ed eventuale adozione di correttivi sono più pregnanti laddove si parli di dispositivi medici *AI-based*, in considerazione del fatto che gli stessi possono evolversi anche successivamente alla propria immissione in commercio in maniera non prevedibile *ex ante*.

6.5. Dispositivi medici intelligenti e AI act.

Come detto in precedenza, le norme relative ai dispositivi medici devono essere lette in combinato disposto con la disciplina prevista dall'*Artificial Intelligence Act* che si applica ai «sistemi di AI destinati ad essere impiegati come o quali componenti di

[529] Ad esempio, è stato sviluppato il DPS-1181 da parte di Exscentia, un'azienda di Oxford, e la giapponese Sumitomo Dainippon Pharma: il farmaco servirà per la fase iniziale del trattamento di diversi disturbi ossessivo compulsivi. Il DPS-1181 è stato formulato da Centaur Chemist, un sistema di AI sviluppato da Exscentia appositamente per la ricerca farmacologica.

dispositivi medici […] qualificati come "ad alto rischio", ossia comportanti un elevato pericolo di danno per la salute e la sicurezza e comunque un rischio di impatto negativo sui diritti fondamentali delle persone fisiche»[530].

Il Regolamento considera come ad alto rischio «i sistemi di AI destinati ad essere utilizzati come componenti di prodotti, o costituenti essi stessi prodotti, ricompresi nell'ambito applicativo di altre norme unionali che, in base a una valutazione di rischio già compiuta a monte dal legislatore, ne subordinino la circolazione al positivo esito di una preventiva valutazione di conformità e dunque le citate norme UE in materia di dispositivi medici»[531].

La qualificazione dei dispositivi come altamente impattanti sui diritti fondamentali determina l'assoggettamento a «doveri di compliance, sin dalla loro progettazione (*by design*), a requisiti di trasparenza, supervisione umana, qualità dei dati, robustezza (anche in termini di *cybersecurity*), accuratezza e tracciabilità»[532].

La complessità dei sistemi e la loro intrinseca opacità però non consente di «garantire la prevedibilità e la tracciabilità del generale sviluppo evolutivo del sistema nel corso del suo processo di

---

[530] Tra gli altri, F. DONATI, *Diritti fondamentali e algoritmi nella Proposta di Regolamento sull'intelligenza artificiale*, in A. PAJNO, F. DONATI, A. PERRUCCI (a cura di), *Intelligenza artificiale e diritto: una rivoluzione? Vol. 1*, Bologna, 2022, p. 111 e ss.

[531] A. AMIDEI, op.cit.

[532] *Ibidem*.

autoapprendimento»[533] ma, eventualmente, spiegare l'*iter* decisionale che ha seguito l'intelligenza artificiale nel caso specifico.

È evidente, dunque, che nel settore in oggetto si necessiti di una disciplina che coinvolga le autorità di settore sia nella fase antecedente all'immissione in commercio che in quella della farmacovigilanza.

In particolare, secondo autorevole dottrina[534] «in materia di *device sanitari AI-powered*, un sistema di regole che subordini la possibilità di utilizzo di sistemi di AI nella diagnostica così come nella terapia e nella chirurgia alla presenza di un'autorevole "certificazione", ove essa verifichi anche l'idoneità, la correttezza e la rappresentatività dei *training data* sui quali l'AI è stata addestrata e la presenza di eventuali "blocchi" che impediscono taluni esiti indesiderati del percorso di evoluzione della macchina, potrebbe offrire tutele ulteriori al paziente che all'impiego di tali tecnologie sia sottoposto. […] Senza giungere all'estremo di una eccessiva deresponsabilizzazione del singolo professionista sanitario "*in command*" e/o della struttura sanitaria della cui dotazione il sistema in questione faccia parte, i quali dovrebbero,

---

[533] M. PALMIRANI, *Interpretabilità, conoscibilità, spiegabilità dei processi decisionali automatizzati*, in U. RUFFOLO (a cura di), *XXVI Lezioni di Diritto dell'intelligenza artificiale*, p. 69 ss.

[534] Tra tutti, A. AMIDEI, op. cit.

infatti, restare sempre onerati dell'obbligo di controllare l'operato dell'AI e di discostarsene, quando necessario».

La questione diventa ancora più complessa laddove si pensi all'evoluzione patologica dell'AI certificata in ambito sanitario e cioè in caso di danni derivanti dall'utilizzo della medesima – di cui si parlerà nei paragrafi che seguono diffusamente sia dal punto di vista del produttore e dell'ente certificatore che del medico e della struttura sanitaria che si servirà di tale strumentazione – in materia di istruttoria e di oneri probatori in capo alle parti.

Infatti, da un canto è irrealistico pretendere che il danneggiato possa dimostrare tecnicamente la mancanza di conformità del sistema ovvero chiedere al produttore di svelare in giudizio il meccanismo di funzionamento del sistema impiegato ovvero effettuare complesse operazioni ingegneristiche, ma, d'altro canto è altresì impossibile negare tutela al soggetto danneggiato e il ristoro del danno ingiusto dallo stesso patito.

6.6. La responsabilità del produttore dei dispositivi medici AI-based*: criticità, stato dell'arte ed esimenti.*

Prima di trattare la questione relativa alla responsabilità del professionista sanitario e della struttura presso cui opera, è opportuno focalizzare l'attenzione sulla responsabilità del

produttore di dispositivi medici *AI-Based* che è il risultato di un ginepraio di norme codicistiche e di derivazione unionale alcune delle quali oggetto di modifica allo stato attuale dello scritto, al fine di adattarne l'impostazione allo sviluppo tecnologico[535].

Infatti, in aggiunta alle responsabilità, contrattuali ed extracontrattuali, del produttore nei riguardi della struttura sanitaria e/o del medico a cui sia fornito il device, si ravvisa l'esistenza di una responsabilità da prodotto (oggettiva o comunque *strict* e non basata sulla colpa) [536] nell'eventualità in cui

---

[535] Tra gli altri, C. PERLINGIERI, *Responsabilità civile e robotica medica*, in *Tecnologie e diritto*, 2020, 1, p. 161 ss.; U. RUFFOLO, *Tecnologie emergenti ed intelligenza artificiale in sanità: rischi e responsabilità*, in U. RUFFOLO, M. SAVINI NICCI (a cura di), *Le nuove frontiere della responsabilità medica*, Milano, 2022, p. 249 ss; M. SAVINI NICCI, G. VETRUGNO, *Intelligenza artificiale e responsabilità nel settore sanitario* in U. RUFFOLO (a cura di), *Intelligenza artificiale – Il diritto, i diritti, l'etica*, p. 601 ss.; N. RIZZO, *Strutture della responsabilità civile e intelligenza artificiale: i problemi in medicina*, in M. FACCIOLI (a cura di), *Profili giuridici dell'utilizzo della robotica e dell'intelligenza artificiale in medicina*, Napoli, 2022.

[536] Si aderisce a quell'orientamento giurisprudenziale che ha qualificato, in opposizione a quanto previsto dagli orientamenti dottrinari maggioritari, la responsabilità da prodotto non come oggettiva ma "presunta", basandosi sul fatto che l'art. 120 del Codice del Consumo impone al danneggiato non la prova del mero nesso causale, ma quella della difettosità del prodotto, non essendo sufficiente la dimostrazione della sussistenza del nesso eziologico a trasferire sul produttore l'onere di dimostrare che il prodotto non era difettoso o la sussistenza di altre cause di esclusione della responsabilità. Cfr. da ultimo, Cass. Civ., 7 aprile 2022, n. 11317 in Danno e resp., 2023, 3, 363, con nota di G. DI MARTINO, *Sulla natura della responsabilità per danno da prodotto difettoso* o Cass. Civ. 15 marzo 2007, n. 6007, in Foro it. 2007, 2414, con nota di A. PALMIERI, *Difetto e condizioni di impiego del prodotto: ritorno alla responsabilità per colpa?*; Cass. Civ. 2013, n. 13458 e Cass.Civ. 6 agosto

sia riconosciuto un difetto del prodotto che abbia causato il danno all'utilizzatore finale.

Vi è uniformità di vedute in dottrina circa la riconducibilità del dispositivo medicale all'alveo del "prodotto" da cui discende la responsabilità del suo fabbricante e il fatto che l'eventuale utilizzo del medesimo da parte del professionista sanitario non comporti di per sé l'esclusione della diretta responsabilità del produttore nei confronti del paziente leso nei suoi diritti[537].

La questione diventa giuridicamente più complessa quando si tenta di definire il concetto di "prodotto difettoso".

La c.d. difettosità è intesa «non come presenza di un qualsivoglia margine di insicurezza – e dunque come pretesa di assoluta innocuità del bene – ma come carenza delle caratteristiche di sicurezza che il pubblico dei consumatori può legittimamente attendersi (il c.d. *consumer expectation test*)»[538].

2013, n. 18654 entrambe in Danno e resp., 2014, 5, 502 ss, con nota di C. BALDASSARRE, *Responsabilità del produttore: danno risarcibile, onere della prova e logica giuridica.*

[537] In senso opposto, A. FIORENTINI, *Machine learning e dispositivi medici: riflessioni in materia di responsabilità civile*, in *Corr. Giur.*, 2021, 10, p. 1264 che ritiene "assai improbabile che il paziente intenti causa direttamente nei confronti del produttore, posta la ritenuta carenza in capo a quest'ultimo di un duty of care verso il paziente stesso".

[538] Art. 6 della Direttiva 85/374/CEE e in Italia art 117 del Codice del Consumo.

Da ciò deriva la natura di clausola generale della nozione di difettosità e dunque la difficoltà di elaborare un elenco tassativo di casi in cui il dispositivo medico possa considerarsi difettoso, ma, ciononostante deve analizzarsi il rapporto intercorrente tra il difetto del *device* e il rispetto dei requisiti produttivi di cui alla disciplina prevista e analizzata e la conclusione se possa considerarsi difettoso un prodotto che viene fabbricato rispettando i principi della medesima.

Da un lato, la verifica della conformità del prodotto deve essere effettuata sulla base dello stesso alle caratteristiche richieste dalla normativa di settore[539], al *consumer expectation test* già citato che dovrebbe essere esteso anche ai requisiti di sicurezza del prodotto e alla "presunzione di difettosità" che si avrebbe in tutte le circostanze in cui il prodotto "non rispetta i requisiti obbligatori di sicurezza stabiliti dal diritto dell'Unione o nazionale intesi a proteggere dal rischio del danno verificatosi".

Dall'altro lato però, non si può giungere al paradosso giuridico secondo cui tutti i prodotti la cui immissione in commercio sia avvenuta a seguito di certificazione di conformità, siano per ciò stesso sicuri e "non difettosi" per addivenire «all'esonero dalla

[539] Regolamento UE 2017/745 e Regolamento sull'Intelligenza artificiale fra tutti.

responsabilità da prodotto difettoso»[540], stante la mancata coincidenza in generale tra la nozione di "prodotto non difettoso" e quella di "prodotto sicuro"[541].

In definitiva quindi, l'osservanza dei parametri di sicurezza non può automaticamente tradursi in una causa di esonero della responsabilità *tout court* ma tenuto conto della peculiarità del settore, «si potrebbe legittimare non una totale coincidenza bensì una maggiore integrazione tra rispetto dei requisiti fissati dalle rilevanti previsioni regolatore e non esclusione della difettosità del *device* ma esenzione della responsabilità per il produttore […] in forza dell'esimente da rischio di sviluppo»[542].

---

[540] In questo senso e pertanto in senso opposto alla tesi cui si aderisce nello scritto, P. TRIMARCHI, *La responsabilità civile: atto illecito, rischio, danno*, Milano, 2019, p. 419, il quale sostiene che «la generale formula secondo la quale il prodotto è difettoso se non offre la sicurezza che ci si può legittimamente attendere dovrebbe trovare applicazione soltanto ove non esistano, con riguardo alla specifica categoria di prodotto, requisiti di sicurezza prescritti o anche solo raccomandati dalla normativa unionale o nazionale o presi in considerazione da codici di buona condotta in materia di sicurezza».

[541] In questi termini, C. CASTRONOVO, *Responsabilità civile*, Milano 2019 che alla pagina 802 osserva che «gli standard di sicurezza indicati dall'autorità certo non vincolano il produttore se non verso il basso e che ritenere sufficiente il rispetto di tali standard al fine di esentare il produttore da responsabilità da prodotto difettoso condurrebbe a concludere che "norme dettate per una protezione basilare dei consumatori e dei fruitori del prodotto si convertirebbero in facili espedienti di irresponsabilità, con una conseguente rimozione del rischio connesso con l'attività produttiva»

[542] A. AMIDEI, op. cit.

6.6.1. La c.d. product liability *alla luce della Direttiva 2022/0302(COD) sulla responsabilità per danno da prodotti difettosi.*

La questione dell'applicabilità dell'esimente del rischio di sviluppo ai prodotti a più elevata complessità tecnologica e dunque ai dispositivi medici in oggetto è giuridicamente molto complessa. Il riferimento è alla norma che prevede «l'esclusione della responsabilità del produttore in relazione a difetti che quest'ultimo non fosse oggettivamente nella posizione di poter considerare, gestire e prevenire in quanto originati da cause che, all'epoca della commercializzazione del prodotto, erano ignote, tenuto conto dello stato della scienza e della tecnica al momento dell'immissione in commercio»[543].

Dal punto di vista normativo, è necessario richiamare la Direttiva del Parlamento Europeo e del Consiglio sulla responsabilità per danno da prodotti difettosi, che abroga la direttiva 85/374/CEE del Consiglio che prevede che «i fabbricanti dovrebbero pertanto

[543] Sul tema, M. BIN, *L'esclusione della responsabilità*, in G. ALPA, M. BIN, P. CENDON (a cura di), *La responsabilità del produttore*, cit., p. 136 e ss; P. TRIMARCHI, *La responsabilità del fabbricante nella direttiva comunitaria*, in Riv. soc, 1986, 3, p. 593 ss; G. GHIDINI, *Art. 5 – Prodotto difettoso* e C.M. VERARDI, *Art. 6 – Esclusione della responsabilità*, entrambi in G. ALPA, U. CARNEVALI, F. DI GIOVANNI, G. GHIDINI, U. RUFFOLO, C.M. VERARDI, *La responsabilità per danno da prodotti difettosi* alle pagine 53 e ss e 84 e ss.

essere esentati dalla responsabilità se dimostrano che con ogni probabilità il difetto che ha causato il danno non esisteva nel momento cui hanno immesso il prodotto sul mercato o l'hanno messo in servizio, oppure che il difetto è sopravvenuto dopo tale momento»[544].

Il Regolamento sull'intelligenza artificiale disciplina all'articolo 8 che «i sistemi di IA ad alto rischio rispettano i requisiti stabiliti nella presente sezione, tenendo conto delle loro previste finalità nonché dello stato dell'arte generalmente riconosciuto in materia di IA e di tecnologie correlate all'IA. Nel garantire conformità a tali requisiti si tiene conto del sistema di gestione dei rischi di cui all'articolo 9».

Se un prodotto contiene un sistema di IA cui si applicano i requisiti del presente regolamento e i requisiti della normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A, i fornitori sono responsabili di garantire che il loro prodotto sia pienamente conforme a tutti i requisiti applicabili previsti dalla normativa di armonizzazione dell'Unione applicabile.

«Nel garantire la conformità dei sistemi di IA ad alto rischio di cui al paragrafo 1 ai requisiti di cui alla presente sezione e al fine di garantire la coerenza, evitare duplicazioni e ridurre al minimo gli

[544] Considerando n. 50.

oneri aggiuntivi, i fornitori possono scegliere di integrare, se del caso, i necessari processi di prova e di comunicazione nonché le informazioni e la documentazione che forniscono relativamente al loro prodotto nella documentazione e nelle procedure esistenti e richieste in conformità della normativa di armonizzazione dell'Unione elencata nell'allegato I, sezione A».

Nel dettaglio, la Direttiva suddetta ha previsto che «Un operatore economico di cui all'articolo 8 non è responsabile del danno causato da un prodotto difettoso se prova una delle situazioni seguenti:

a) nel caso del fabbricante o dell'importatore, che non ha immesso il prodotto sul mercato né lo ha messo in servizio;

b) nel caso di un distributore, che non ha messo il prodotto a disposizione sul mercato;

c) che è probabile che il difetto che ha causato il danno non esistesse al momento in cui il prodotto è stato immesso sul mercato, messo in servizio o, nel caso di un distributore, messo a disposizione sul mercato, o che tale difetto è sopravvenuto dopo tale momento;

d) che il carattere difettoso che ha causato il danno è dovuto alla conformità del prodotto a requisiti giuridici;

e) che lo stato oggettivo delle conoscenze scientifiche e tecniche al momento dell'immissione del prodotto sul mercato o della sua

messa in servizio oppure durante il periodo in cui il prodotto è stato sotto il controllo del fabbricante non permetteva di scoprire l'esistenza del difetto;

f) nel caso del fabbricante di un componente difettoso come indicato all'articolo 8, paragrafo 1, primo comma, lettera b), che il carattere difettoso del prodotto in cui è stato integrato il componente è dovuto alla concezione del prodotto o alle istruzioni date dal fabbricante del prodotto al fabbricante del componente;

g) nel caso di una persona che modifichi il prodotto come indicato all'articolo 8, paragrafo 2, che il difetto che ha causato il danno riguarda una parte del prodotto non interessata dalla modifica.

2. In deroga al paragrafo 1, lettera c), un operatore economico non è esentato dalla responsabilità se il carattere difettoso di un prodotto è dovuto a uno dei seguenti elementi, a condizione che il prodotto sia sotto il controllo del fabbricante:

a) un servizio correlato;

b) software, compresi aggiornamenti o migliorie;

c) la mancanza degli aggiornamenti o delle migliorie del software necessari per mantenere la sicurezza;

d) una modifica sostanziale del prodotto»[545].

[545] Articolo 11 - Esenzione dalla responsabilità della Direttiva 2022/0302.

Dall'analisi della disciplina si evince sia la cristallizzazione giuridica della cosiddetta esimente da sviluppo del prodotto sia il dovere, gravante sul produttore, di monitorare e di aggiornare il sistema con l'obbligo di dimostrare che lo stato delle conoscenze scientifiche e tecniche impediva di scoprire la difettosità del prodotto non soltanto fin tanto che il medesimo sia stato immesso in commercio ma anche successivamente e cioè finché il prodotto è rimasto sotto il suo controllo, prevedendo un onore aggiuntivo non esclusivamente in merito al funzionamento del prodotto medesimo ma anche con riguardo allo stato delle conoscenze tecniche e scientifiche rilevanti per garantire la sicurezza con conseguente obbligo di adottare ogni misura necessaria alla luce del progredire di tali conoscenze.

Si può dunque concludere sul punto che la dottrina[546] ha previsto una prospettiva diacronica che riguardi sia la fase antecedente all'immissione in commercio sia quella successiva della responsabilità derivante dai danni cagionati dai dispositivi medici intelligenti discendente dal combinato disposto della normativa di stampo unionale riguardanti i prodotti difettosi e di quella in materia di responsabilità civile.

[546] Tra tutti, A. AMIDEI, op. cit.

6.6.2. La concorrente invocabilità del regime di responsabilità da attività pericolosa.

Nella sezione precedente, in cui si è parlato diffusamente della responsabilità civile derivante dagli strumenti di intelligenza artificiale, si era convenuti che, stante la necessità di prevedere forme di responsabilità *ad hoc*, la categoria civilistica più calzante con tali strumenti caratterizzati dall'autoapprendimento, fosse quella prevista dal combinato disposto dell'art. 2050 e 2051 del Codice civile.

Nel paragrafo in oggetto, si analizzerà la possibile applicazione del regime della responsabilità da attività pericolosa anche ai danni cagionati dai dispositivi medici intelligenti[547].

La questione è risalente nel tempo e aveva già previsto l'applicabilità del regime ex art. 2050 cod. civ. all'attività di produzione dei farmaci, inoltre, l'evoluzione delle pratiche mediche aveva indotto la giurisprudenza a considerare come

[547] Pioneristico in materia fu U. RUFFOLO nel suo scritto *Le responsabilità da artificial intelligence, algoritmo e smart product: per i fondamenti di un diritto dell'intelligenza artificiale self-learning* mentre dubitano della possibilità di estendere al settore dell'AI il regime di responsabilità da attività pericolosa U. SALANITRO, *Intelligenza artificiale e responsabilità: la strategia della Commissione Europea*, in *Riv. Dir. Civ.* 2020, 6, p. 1246 ss; A. LEPORE, *I.A. e responsabilità civile. Robot, autoveicoli e obblighi di protezione, in Tecnologie e diritto*, 2021, 1, p.193 ss.

pericolose talune ipotesi di attività precedentemente non considerate come tali[548]; alla luce del crescere del ricorso all'automazione intelligente – ad esempio nel campo della diagnostica – e all'impiego di sistemi in sanità già definiti dall'*AI act* come ad alto rischio non soltanto nell'ambito della produzione di dispositivi medici intelligenti ma anche sul versante dell'attività clinica, diagnostica, terapeutica e chirurgica che si serve di tali strumenti, ci si interroga circa l'estensione dell'applicazione dell'art. 2050 cod. civ.

È rilevante sottolineare che le due forme di responsabilità – quella da prodotto difettoso e quella da attività pericolosa – possono essere concorrenti, nonostante il tema sia fortemente dibattuto sia in dottrina[549] che in giurisprudenza[550].

---

[548] Tra cui, in particolare, quelle legate alle trasfusioni e all'impiego di emoderivati.

[549] U. RUFFOLO, *Art. 15 – Responsabilità secondo altre disposizioni di legge*, in G. ALPA, U. CARNEVALI, F. DI GIOVANNI, G. GHIDINI, U. RUFFOLO, C.M. VERARDI, *La responsabilità per danno da prodotti difettosi*; U. RUFFOLO, E. AL MUREDEN, *Autonomous vehicles e responsabilità nel nostro sistema e in quello statunitense*, in *Giur. It*, 2019, 7, p. 1704 e ss; A. L. BITETTO, *Responsabilità da prodotto difettoso: strict liability o neglicence rule?* in *Danno e resp.*, 2006, 3, p. 259 ss.

[550] Il riferimento è alle note Corte Giust. UE, 25 aprile 2002, C-154/00, Commissione c. Repubblica ellenica; Corte Giust. UE, 2002, C-52/00, Commissione c. Repubblica francese; Corte Giust. UE, 2002, C-183/00, Medicina Asturiana, tutte in Resp. Civ. e prev., 2002, 4-5, p. 997 ss., con nota di S. BASTIANON, *Responsabilità del produttore per prodotti difettosi: quale tutela per il consumatore?* in senso contrario Tribunale di Sassari, 12 luglio 2012, in *Rass. Dir. farm.*, 2012, p. 1185 ss, che aveva escluso la possibilità di

Si tratta, infatti, di *ratio* differenti in quanto non sono neppure coincidenti i presupposti di "pericolosità" e di "difettosità" e, inoltre, la disciplina di cui all'art. 2050 è riconducibile ai più generali criteri di attribuzione della responsabilità, indipendentemente dal fatto che il danno derivi dal prodotto difettoso mentre la c.d. "*product liability*" è una normativa speciale rinvenibile nel Codice del Consumo.

In conclusione, è dibattuto se per gli sviluppatori e/o gli utilizzatori di sistemi di AI ad alto rischio in ambito sanitario, le "misure idonee" richieste dall'art. 2050 del Codice civile si identifichino nel rispetto degli *standard* e delle procedure previste nelle normative specifiche di dettaglio in precedenza analizzate.

Sezione III

concorso tra le due azioni extracontrattuali affermando che "la responsabilità da produttore per farmaco difettoso rientra nell'alveo della responsabilità extracontrattuale del produttore disciplinata dal D.P.R. n. 224/1988 e per l'effetto del D. lgs. 206/2005, quale disciplina speciale rispetto all'art. 2050 cod.civ., non essendo consentito il cumulo di due azioni extracontrattuali ai fini risarcitori».

7.4. Intelligenza artificiale e responsabilità sanitaria: natura della prestazione sanitaria e responsabilità del singolo operatore.

L'adozione di infrastrutture tecnologiche ad oggi potrebbe mettere in crisi il modello classico di responsabilità professionale sanitaria se si considera che, in caso di danno, tale responsabilità non può essere imputata semplicemente al medico, estraneo ai processi di formazione e di addestramento della macchina, per il sol fatto che nell'espletamento della propria attività si sia servito di strumentazioni intelligenti.

Il primo interrogativo giuridicamente rilevante derivante dall'impiego dell'IA riguarda la qualificazione dell'attività *strictu sensu* medica svolta dal professionista sanitario quale obbligazione di mezzi o obbligazione di risultato, con le diverse conseguenze in termini di responsabilità.

Infatti, sebbene l'attività sanitaria sia stata da sempre considerata «in virtù della nota di aleatorietà impressale dalle ineliminabili imperfezioni della scienza medica e dell'imprevedibilità delle reazioni dell'organismo umano»[551], l'esempio principe delle obbligazioni di mezzi[552]; vi sono diverse ipotesi nelle quali la

---

[551] M. FACCIOLI, *Intelligenza artificiale e responsabilità sanitaria* in *La nuova Giurisprudenza civile commentata*, n. 3, 1 maggio 2023, p. 732.

[552] G. D'AMICO, *Responsabilità per inadempimento e distinzione tra obbligazioni di mezzi e di risultato*, in *Il diritto delle obbligazioni e dei*

giurisprudenza ritiene che possano sussistere gli estremi per prevedere un'obbligazione di risultato in capo al medico[553].

Come è stato evidenziato da una parte di dottrina[554], l'idea che sta a fondamento di questi indirizzi giurisprudenziali appena citati è che «l'esecuzione di determinati trattamenti sanitari è presieduta da regole tecniche molto specifiche e altamente vincolanti, al punto da potersi istituire anche con il conforto del dato statistico, uno stretto collegamento tra il rispetto di quelle regole e il raggiungimento di un certo esito clinico e, di conseguenza, tra il fallimento delle cure da un lato e la sussistenza di un errore nell'esecuzione del trattamento dall'altro».

Per quanto l'intelligenza artificiale in campo medico possa ridurre al minimo la possibilità di errore, non è possibile aderire alle teorie

---

contratti: verso una riforma? Atti del Convegno per il cinquantenario della Rivista di diritto civile, Cedam, 2006, 154; A. DI MAJO, *Il giudizio di responsabilità civile del medico dopo la legge Gelli e cioè la perizia "guidata"* in *Giur. It.*, 2018, p. 844.

[553] Si tratta di trattamenti di natura estetica, delle cure odontoiatriche, dei c.d. interventi di routine nonché delle fattispecie in cui si afferma che «il risultato positivo è una conseguenza statisticamente fisiologica della prestazione professionale diligente e che, pertanto, si configura un inadempimento del sanitario non solo allorquando alla prestazione medica consegua l'aggravamento dello stato morboso o l'insorgenza di nuova patologia, ma anche quando l'esito risulti […] caratterizzato da inalterazione rispetto alla situazione che l'intervento medico-chirurgico ha reso necessario» (Cass. Civ. 13.4.2007, n. 8826, in Giur. It. 2008, 63 ripresa e richiamata da Cass. Civ. 8.10.2008, n. 24791).

[554] G. D'AMICO, *Responsabilità per inadempimento e distinzione tra obbligazioni di mezzi e di risultato,* op. cit.

che assimilano gli interventi effettuati con l'ausilio dell'intelligenza artificiale alle obbligazioni di risultato; infatti, l'impiego dell'AI può qualificarsi quale prestazione neutrale rispetto alla qualificazione giuridica della prestazione sanitaria che in assenza di ulteriori elementi idonei dovrebbe essere qualificata come obbligazione di mezzi «la responsabilità per l'inadempimento delle quali è dominata dal criterio della colpa parametrata sul canone della diligenza professionale ex art. 1176, comma 2, cod. civ. e sul rispetto delle linee guida e delle buone pratiche clinico-assistenziali di cui all'art. 5 della legge Gelli Bianco»[555].

Sotto altro profilo, non è condivisibile la previsione di «un'automatica correlazione tra la sofisticatezza e l'innovatività dei sistemi di IA impiegati in medicina e l'applicazione della limitazione della responsabilità ai soli casi di dolo e colpa grave prevista dall'art. 2236 cod. civ. per il caso di prestazioni implicanti problemi tecnici di speciale difficoltà»[556], infatti la sussistenza di tale presupposto deve essere valutata caso per caso, non essendo

---

[555] A. COLARUOTOLO, *Intelligenza artificiale e responsabilità medica: novità, continuità e criticità*, in *Resp. Med*. 2022, p. 306.

[556] Sul tema, M. GAZZARA, *In difesa dell'art. 2236 cod. civ.*, in *Nuovo dir. Civ.*, 2020, p. 53 e ss; M. TESCARO, *L'art. 2236 cod. civ. e l'auspicabile contenimento della responsabilità civile del prestatore d'opera*, in *Studium iuris*, 2021, p. 32 e ss.

sufficiente «la potenziale prospettabilità di problemi di speciale difficoltà desunta da categorie astratte e predefinite»[557].

Si ritiene[558] che guardando alla responsabilità colposa, possa escludersi che il medico venga chiamato a rispondere del malfunzionamento di un sistema di intelligenza artificiale che fuoriesce dall'ambito del suo controllo in forza dell'elevato grado di autonomia e opacità, rimanendo invece la sua responsabilità circoscritta alle sole ipotesi in cui il danno sia derivato da uno scorretto utilizzo della macchina imputabile alla propria negligenza[559].

---

[557] A. COLARUOTOLO, *Intelligenza artificiale e responsabilità medica: novità, continuità e criticità,* op. cit.

[558] G. VOTANO, *Intelligenza artificiale in ambito sanitario: il problema della responsabilità civile*, in *Danno e resp.*, 2022; A. D'ADDA, *Danni «da robot» (specie in ambito sanitario) e pluralità di responsabili tra sistema delle responsabilità civili ed iniziative di diritto europeo*, in *Riv. Dir. Civ.*, 2022, p. 807 ss., il quale ritiene tale conclusione riferibile alla sola figura del medico ausiliario della struttura sanitaria, mentre il medico libero professionista dovrebbe invece rispondere, al pari della struttura stessa, anche del difettoso funzionamento dell'IA impiegata nell'adempimento del contratto stipulato con il paziente, trattandosi di una scelta esecutiva del debitore comportante rischi riconducibili all'ambito del rischio professionale assunto con l'accettazione dell'incarico.

[559] Come affermano sia G. VOTANO, op.cit., sia A. COLARUOTOLO, op, cit., il personale sanitario può essere ritenuto responsabile per essersi avvalso dell'IA senza avere le competenze necessarie, per aver utilizzato un sistema intelligente nella consapevolezza o nella colpevole ignoranza della sua difettosità, per non aver rilevato la scorrettezza delle indicazioni fornite dalla macchina nei limiti in cui questa fosse rilevabile con una verifica diligente, o ancora per avere impiegato tali tecnologie per affrontare un caso clinico le cui specificità imponevano l'impiego di metodi di cura tradizionali.

In senso contrario[560] sono state prospettate soluzioni basate sul rischiamo alla disciplina codicistica delle forme speciali di responsabilità extracontrattuale.

Taluni sostengono, come detto nella sezione precedente del lavoro in oggetto, che «chi si avvale di un sistema di IA risponderebbe dei danni cagionati dallo stesso in quanto l'uno e l'altro sarebbero assimilabili, in via di interpretazione analogica a precettore ed allievo ai sensi dell'art. 2048, comma 2°, a preponente e preposto ai sensi dell'art. 2049 cod. civ. o a proprietario e animale ai sensi dell'art. 2052 cod. civ. »[561], ma questa corrente di pensiero, già inapplicabile all'utilizzo di intelligenza artificiale in generale, non trova spazio neppure nel settore speciale di cui si tratta.

---

[560] Tale prospettiva si applica con particolare evidenza alle responsabilità del medico ospedaliero che assume natura ex lege extracontrattuale in assenza di un contratto stipulato con il paziente ai sensi dell'art. 7, comma 3° della Legge Gelli-Bianco. Anche nei confronti del medico che invece è contrattualmente responsabile nei confronti del paziente possono trovare applicazione le norme in questione essendo pacifico che nelle ipotesi in cui coesistono la fattispecie dell'inadempimento e dell'illecito civile, come tipicamente avviene nell'ambito sanitario, il danneggiato ha la facoltà di agire a sua scelta in via contrattuale o in via aquiliana (sul punto, tra tutti, BIANCA, *Diritto civile*, 5, *La responsabilità*, 2021 p. 536 e ss). Al fine di responsabilizzare il medico per il malfunzionamento dell'IA non appare, invece, già *prima facie* possibile richiamare la soluzione praticata in campo ingegneristico, che addossa all'ingegnere gli errori del programma di calcolo utilizzato facendo leva sulla sottoscrizione del progetto da parte del professionista, tra gli altri sul punto E. GIUSTI, *Intelligenza artificiale e sistema sanitario*, in S. DORIGO (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*.

[561] A. SANTOSUOSSO, C. BOSCARATO, F. CAROLEO, *Robot e diritto: una prima ricognizione* nella *Nuova giurisprudenza commentata*, 2012, II, p. 513.

Non appare altresì convincente ricondurre tale responsabilità nell'alveo del regime di cui all'art. 2050 cod. civ., per le ragioni citate nella sezione precedente e perché l'attività medica non può essere qualificata come pericolosa, con eccezione dei pochi casi già citati.

La tesi maggiormente condivisa in dottrina e anche in giurisprudenza[562] riguarda l'applicazione della responsabilità, sostanzialmente oggettiva, da cose in custodia ai sensi dell'art. 2051 cod. civ.

Più in particolare, si ravvisa una responsabilizzazione piuttosto rigorosa dell'utilizzatore del robot o del dispositivo *AI-Based*, anche nell'eventualità in cui il sinistro derivi da scelte autonome, imprevedibile e opache della macchina.

---

[562] A. ALBANESE, *La responsabilità civile per i danni da circolazione dei veicoli ad elevata automazione*, in *Europa e d. priv.*, 2019, p. 1007, che opportunamente rileva come il requisito del «naturale dinamismo della cosa» postulato dall'art. 2051 c.c. troverebbe speciale conferma proprio nel caso di macchina di intelligenza artificiale. V. anche M. RATTI, *Riflessioni in materia di responsabilità civile e danno cagionato da dispositivo intelligente alla luce dell'attuale scenario normativo*, in *Contratto e impr.*, 2020, p. 1182; contra M. COSTANZA, *L'intelligenza artificiale e gli stilemi della responsabilità civile*, in *G. it.*, 2019, p. 1688. In generale, sull'imputazione all'utilizzatore ovvero al produttore dei danni da veicoli autonomi – e sugli effetti in termini di (divergenti) interessi da tutelare – cfr. anche E. Al MUREDEN, *Autonomous cars e responsabilità civile tra disciplina vigente e prospettive de iure condendo*, in *Contratto e impr.,* 2019, p. 895 ss.; F.P. PATTI, *The European Road to Autonomous Vehicle*, in *43 Fordham International L. J.*, 2019, 1, p. 136 ss.

Dunque, si giungerebbe a imputare una responsabilità al medico che si sia servito dell'intelligenza artificiale nell'espletamento della propria attività anche quando non sia accertata un'imperizia nell'esecuzione della prestazione, nella logica secondo cui il debitore è responsabile per il fatto dell'ausiliario[563].

Seguendo questo ragionamento logico giuridico, essendo prevista la complementarità della responsabilità del produttore del dispositivo e dell'operatore che se ne serve, il danneggiato potrà agire nei confronti del medico che potrà agire in rivalsa nei confronti del fabbricante che sarà maggiormente in grado di internalizzare i costi del risarcimento nel novero del proprio rischio di impresa[564].

7.5. *La responsabilità della struttura ospedaliera nell'uso dei sistemi di IA.*

La questione circa la configurabilità della responsabilità del medico dipendente di una struttura ospedaliera chiamato dal proprio ospedale ad effettuare una prestazione sanitaria servendosi di una macchina messa a disposizione dalla struttura è giuridicamente rilevante.

---

[563] Per questa tesi, vedasi A. D'ADDA citato.
[564] *Ibidem*.

Infatti, l'attuale normativa vigente in tema di responsabilità civile in ambito sanitario è rappresentata dalla c.d. Legge Gelli-Bianco (n. 24 dell'8 marzo 2017) [565] che prevede un doppio binario di responsabilità: contrattuale della struttura sanitaria per i danni provocati dai propri ausiliari ex artt. 1218 e 1228 cod. civ. ed extracontrattuale ex art. 2043 cod. civ. per quanto attiene all'operatore sanitario.

Nel paragrafo precedente si è trattata l'ipotesi di utilizzo di dispositivi medici intelligenti da parte del professionista sanitario al di fuori dell'ambito ospedaliero, ma se il *device* medesimo costituisce uno strumento di lavoro di cui si avvale il medico per l'espletamento della sua attività all'interno della struttura ospedaliera, sarà necessario distinguere se il danno sia stato causato da imperizia o negligenza dall'ipotesi in cui la condotta del medico non ha avuto alcun ruolo nella causazione del danno ingiusto.

---

[565] Per una ricostruzione accurata del tema vedasi: E. A. EMILIOZZI, *La responsabilità medica*, Milano, 2023; R. DE MATTEIS, *Le responsabilità in ambito sanitario. Il regime binario: dal modello teorico ai risvolti applicativi*, Milano, 2017; N. TODESCHINI (a cura di), *La responsabilità in medicina. Dalla discussione del caso pratico alla regola. Una guida operativa completa alla riforma Gelli Bianco; la colpa civile e penale, il consenso informato, i procedimenti e i profili assicurativi*, Milano, 2023.

Nel primo caso, il medico sarà responsabile a titolo aquiliano, ai sensi dell'art. 7 della legge Gelli Bianco[566], essendo «la regia dell'intervento ancora tutta umana»[567] e l'azione colposa del medico condurrà alla responsabilità dell'ente nosocomiale per responsabilità da inadempimento contrattuale[568], alla luce del profilo "a doppio binario" della responsabilità medica.

Nel secondo caso, invece, se il danno cagionato al paziente non è ascrivibile alla condotta dell'operatore sanitario ma sia conseguenza di un errore imprevedibile e non prevenibile derivante esclusivamente dal dispositivo intelligente, si configurerebbe la responsabilità dell'ospedale «poiché quest'ultimo è tenuto all'obbligazione di fornire assistenza sanitaria al paziente, cui accedono prestazioni accessorie di protezione tra cui potrebbe essere inclusa anche quella relativa all'utilizzo di sistemi di IA»[569].

---

[566] N. TODESCHINI, *L'art. 7 della legge Gelli Bianco, il doppio binario che non c'è*, in P. CENDON (diretto da), *La responsabilità medica: guida operativa alla riforma Gelli Bianco. Inquadramento, profili civili e penali, assicurazione, procedimento stragiudiziale e giudiziale, casistica.* Milano, 2019, p. 1056.

[567] C. PERLINGIERI, *Responsabilità civile e robotica medica*, in *Tecn. Dir.*, 2020, p. 171 ss.

[568] G. ALPA, *Ars interpretandi e responsabilità sanitaria nella nuova legge Gelli Bianco*, in Contr. Impr., 2017, pp. 728 ss. In giurisprudenza vedasi Cass. 27 agosto 2014 n. 18304 e Cass. 15 giugno 2021, n. 16936.

[569] R. SCOTTI, *La responsabilità civile dei danni cagionati da sistemi di intelligenza artificiale in ambito sanitario* in *Giustizia civile*, 1/2024.

Si tratta di una obbligazione che ha un contenuto complesso, constando di una molteplicità di prestazioni eterogenee poste a carico della struttura sanitaria nei confronti del paziente non esauribili nelle cure mediche e chirurgiche ma in una serie di obblighi accessori che non consentono di ricondurre la prestazione al contratto d'opera professionale, configurandosi invece «un contratto atipico a prestazioni corrispettive (c.d. contratto di spedalità)»[570] che affonda le radici nella giurisprudenza di legittimità[571].

---

[570] Cass. 8 giugno 2023, n. 16272 secondo cui «in tema di responsabilità medica, la presa in carico di un paziente da parte di una struttura inserita nella rete del SSN, per la sottoposizione ad un trattamento medico chirurgico, determina l'instaurazione di un rapporto contrattuale atipico a prestazioni corrispettive – il c.d. contratto di spedalità – idoneo a fondare, in caso di esito infausto dell'intervento, la legittimazione passiva dell'ente in relazione all'azione di responsabilità proposta dal paziente o dai suoi eredi, essendo a tal fine irrilevante che, nella organizzazione interna del Servizio sanitario nazionale, la struttura stessa e il suo personale siano stati posti sotto la direzione amministrativa e medica di un'altra istituzione pubblica, la cui responsabilità può eventualmente aggiungersi a quella della struttura sanitaria adita, senza però eliderne la titolarità del rapporto dal lato passivo».

[571] Cass. Sez. Un. N. 577 dell'11 gennaio 2008, in Foro it., 2008, I, p. 455, con nota di A. PALMIERI, in *Giur. It.*, 2008, 1653 con nota di A. CIATTI, in *Nuova. Giur. Civ. comm.*, 2008, I, p. 612, con nota di R. DE MATTEIS, in *Resp. Civ. e prev.*, 2008, p. 856, con nota di M. GORGONI, in *Danno e resp.*, 2008, p. 871, con nota di A. NICOLUSSI. Secondo le Sezioni Unite: «La struttura privata sanitaria conclude necessariamente col paziente che ad essa si rivolga un contratto atipico (c.d. contratto di spedalità o di assistenza sanitaria), in virtù del quale la prima si obbliga a fornire al secondo un'adeguata prestazione di contenuto sanitario. Ne consegue che per effetto di tale contratto la clinica è direttamente responsabile nei confronti del paziente che abbia patito un danno in conseguenza di un deficit organizzativo della

Dunque, in letteratura si riconosce che il sinistro cagionato al paziente dalla macchina artificiale determinerebbe di per sé una responsabilità contrattuale in capo alla struttura sanitaria «in base al mero inadempimento della stessa, nei limiti dell'impossibilità non imputabile»[572].

Inoltre, in dottrina si è sostenuto che la struttura ospedaliera risponde anche a concorrente titolo extracontrattuale.

Sul punto, si è ritenuto[573] che si possa applicare la disciplina sulla responsabilità per l'esercizio delle attività pericolose ai sensi dell'art. 2050 cod. civ., in quanto «la riconduzione del danno derivante da dispositivo intelligente è dovuta ai caratteri che connotano tali strumenti, i quali sono autonomi e, quindi, incontrollabili e imprevedibili e, dunque, possiedono in sé un'intrinseca potenzialità lesiva, idonea a fondarne una responsabilità da entità irrazionale reagente e dotata di intrinseco dinamismo»[574]. Infatti, secondo questo filone di letteratura e di

---

struttura sanitaria, come pure in conseguenza di un errore del personale medico o paramedico a nulla rilevando in quest'ultimo caso né che l'errore materiale del danno sia o meno dipendente della clinica né che la prestazione sia stata resa o meno in regime di convenzionamento con il S.S.N.».

[572] R. SCOTTI, op. cit.

[573] D. DE MARTINI, *I fatti produttivi di danno risarcibile*, Padova, 1983, 241; U. RUFFOLO, *Le responsabilità da artificial intelligence, algoritmo e smartproduct: per i fondamenti di un diritto dell'intelligenza artificiale self-learning*, in U. RUFFOLO-G.ALPA-A.BARBERA (a cura di), *Intelligenza artificiale. Il diritto, i Diritti e l'etica, Milano*, 2020, p. 110.

[574] D. DE MARTINI, *I fatti produttivi di danno risarcibile*, op. cit.

giurisprudenza[575] il criterio della pericolosità sarà dato dalla valutazione dell'idoneità dello strumento di IA a provocare danni e l'attività si ritiene pericolosa perché il danno è correlato alla natura ovvero al mezzo adoperato, avendo una potenzialità lesiva superiore al normale.

Di segno opposto è chi[576] invece ritiene che «l'uso di sistemi intelligenti dovrebbe prevenire i rischi ed incrementare il miglioramento della salute, in quanto strumenti correttivi e più efficienti rispetto all'attività umana, sicché sarebbe una contraddizione qualificarli come mezzi potenzialmente pericolosi».

---

[575] Cass. 15 ottobre 2004, n 20334; Cass. 10 febbraio 2003, n. 1954, in Foro it. Rep., 2003, voce Responsabilità civile n. 252; Cass. 30 ottobre 2002, n. 8148, in Gius. 2002, n. 19; Cass. 28 febbraio 2000, n. 2220, in Foro it., 2000, I, 1828 e in Danno e resp. 2000, p. 614, con nota di F. DI CIOMMO; Cass. 29 luglio 2015, n. 16052 con nota di M. TOPI. Secondo l'esperienza giurisprudenziale più recente, sono considerate attività pericolose non solo quelle qualificate come tali dalla legge di pubblica sicurezza e da altre leggi speciali, ma anche quelle che, per la loro stessa natura o per le caratteristiche dei mezzi adoperati, comportino, in ragione della loro spiccata potenzialità offensiva, una rilevante possibilità del verificarsi del danno. Vedasi inoltre la sentenza della Cassazione n. 19180 del 19 luglio 2018 che prevede che «dovendosi, di conseguenza accertare in concreto il requisito della pericolosità con valutazione svolta caso per caso, tenendo presente che anche un'attività per natura non pericolosa può diventarlo in ragione delle modalità con cui viene esercitata o de mezzi impiegati per espletarla. L'indagine fattuale deve essere svolta seguendo il criterio della prognosi postuma, in base alle circostanze esistenti al momento dell'esercizio dell'attività».

[576] M. COSTANZA, *L'intelligenza artificiale e gli stilemi della responsabilità civile*, in *Giur. It.*, 2019, p. 1686; E. PALMERINI, *La responsabilità medica e la prova dell'inesatto adempimento*, p. 783.

Altri autori[577] hanno ipotizzato l'applicabilità dell'art. 2051 cod. civ., con riferimento alle responsabilità del danno cagionato dalle cose in custodia con l'ente ospedaliero che si qualifica come custode e la macchina intelligente quale *res*[578], essendosi osservato che «tra le cose in custodia si annovererebbero anche le cose utilizzate quali strumenti di lavoro: anzi, il requisito del naturale dinamismo della cosa, quale presupposto della regola speciale di tale responsabilità, potrebbe ben adattarsi proprio all'ipotesi della macchina di intelligenza artificiale autonoma. E non a caso è stata suggerita anche per i casi di sinistro cagionato da una *driverless car*»[579].

Ai fini dell'individuazione del soggetto "custode" la giurisprudenza di legittimità nell'individuare gli elementi del rapporto di custodia, mette in risalto il potere di governo sulla *res*[580], attribuendo la responsabilità per il danno provocato da IA a

---

[577] Autorevolmente, U. RUFFOLO, *Intelligenza artificiale, machine learning e responsabilità da algoritmo*, in *Giur. It.*, 2019, p. 1699.

[578] Cass. 28 novembre 1995 n. 12300 e Cass. 18 febbraio 2000, n. 1859 prevedono che nel concetto di res non riguardi solo le come mobili e immobili inerti, ma anche le cose in movimento, volendo inserire in tali categorie le cose che possiedono un intrinseco dinamismo.

[579] A. D'ADDA, *Responsabilità "da robot": i soggetti responsabili e i loro rapporti interni (con speciale riferimento all'ambito sanitario)*, in U. SALANITRO (a cura di), *SMART la persona e l'infosfera*, p. 161.

[580] Custode, ai sensi dell'art. 2051 cod. civ., è colui che ha «il potere di governo» sulla cosa da intendersi come potere di controllarla, di eliminare le situazioni di pericolo che siano insorte e di escludere i terzi dal contatto. Sul punto, in giurisprudenza Cass. 12 luglio 2006, n. 15779; Cass. 29 luglio 2016,

colui che ha il controllo del sistema e che non ha evitato il danno, salvo il caso fortuito[581].

Secondo altra opinione[582] l'inapplicabilità della disposizione codicistica è riconducibile al fatto che la *res* intelligente non è inanimata ma dotata di una intrinseca funzione attiva che le consente l'elaborazione di un risultato in modo del tutto autonomo. Infatti, tenuto conto dell'assoluta imprevedibilità delle macchine, dovute alla loro connaturata opacità, si ritiene che la stessa possa essere sussunta nell'alveo del caso fortuito che interrompe il nesso di causalità tra le cose in custodia e l'evento dannoso.

Infine, la responsabilità nosocomiale è del tutto esclusa se si ravvisa il fondamento del danno in un difetto riconducibile alla fase di realizzazione del dispositivo che non sia suscettibile di essere rilevato con l'ordinaria diligenza richiesta all'ospedale, venendo in rilievo in tale circostanza l'esclusiva responsabilità del produttore e dell'addestratore della macchina intelligente.

---

n. 15761; Cass. 1 febbraio 2018, n. 2478; Cass. 23 maggio 2019, n. 13966; Cass, 27 maggio 2022, n. 17252. In dottrina, sul punto G. D'ALFONSO, *Il regime di responsabilità da cose in custodia tra questioni tradizionali e "responsabilità da algoritmo"*, op. cit.

[581] L. COPPINI, *Robotica e intelligenza artificiale: questioni di responsabilità civile.*

[582] G. SARTOR, *Gli agenti software e la disciplina giuridica degli strumenti cognitivi* in *Dir. Inf.*, 2003, p. 55 ss.

7.6. *Conclusioni in materia di responsabilità civile e intelligenza artificiale in ambito sanitario.*

Allo stato della scrittura di questo lavoro non vi sono elementi per estendere con certezza la normativa dettata in tema di responsabilità sanitaria all'eventualità in cui il danno sia cagionato da sistemi di IA.

Mettendo a confronto l'uomo e la macchina, è evidente come le regole tradizionali appaiono del tutto inadeguate e come «le caratteristiche dei dispositivi di apprendimento automatico, sembrano porsi in evidente contrasto con il criterio di imputabilità della colpa, della causalità e del nesso eziologico della medesima»[583].

È, inoltre, complesso individuare l'origine del danno essendo plurime le tipologie di rischio che possono svilupparsi dai dispositivi intelligenti, incidendo anche su beni giuridici fondamentali quali la vita e la salute.

Il profilo giuridico più complesso è quello relativo all'individuazione del percorso che ha condotto ad una determinata diagnosi, ad una determinata cura, essendo un sistema per sua natura opaco e anche dell'onere della prova del

[583] R. SCOTTI, *op. cit*.

danneggiato che si troverebbe nella *probatio diabolica* della dimostrazione degli elementi che hanno condotto al danno.
Si auspica, quindi, di legare «l'esistenza del nesso di causalità a meccanismi di presunzioni in grado di agevolare la posizione processuale del paziente in tema di onere probatorio»[584].

8.1. Il chatbot: definizioni e disciplina.

Il chatbot viene definito come un «programma informatico che elabora e produce conversazioni scritte o orali con una persona umana, in genere un utente della rete che visita un sito web che offre al pubblico beni e servizi»[585], il *software* "fingerà" di essere umano per aiutare le persone che si interfacciano nei diversi compiti, ricevendo come *input* delle informazioni o domande espresse in linguaggio naturale, sarà nelle condizioni di rispondere ed eseguire uno o più comandi forniti dall'utente[586].
Storicamente i primi chatbot erano basati sul c.d. *pattern matching* che consisteva nell'accoppiare le occorrenze di una stringa di

[584] *Ibidem*.
[585] P. SAMMARCO, *Osservazioni sulla responsabilità da informazioni inesatte fornite da un chatbot*, in *Il diritto dell'informazione e dell'informatica*, 1/2024.
[586] L. ALIMENTI, E. SCIARRETTA, *I chatbot nel campo medico* in S. CAPOGNA, A. DEL CIMMUTO, C. FONZO (a cura di), *L'istruzione, il lavoro e la società ai tempi dell'emergenza pandemica globale*, 1/2021.

linguaggio di programmazione informatica all'interno di un'altra ed erano dei semplici programmi informatici che rispondevano in maniera elementare alle richieste degli utenti, oggi gli stessi si basano sull'intelligenza artificiale e sull'apprendimento automatico, attraverso l'utilizzo del linguaggio naturale o delle reti neurali per adattarsi ad una mole di informazioni sempre più grande, per garantire livelli crescenti di personalizzazione del servizio.

Prima di analizzare nel dettaglio taluni casi pratici di *chatbot* in ambito sanitario e le relative responsabilità, si analizzerà la questione giuridica circa la soggettività dello stesso, sottoposta all'attenzione del giudice del Tribunale Civile dello Stato canadese del British Columbia che si è occupato del caso di un *chatbot* del sito web di una compagnia aerea che ha fornito informazioni rivelatesi errate riguardanti le modalità per usufruire di una tariffa scontata per l'acquisto di biglietti aerei a causa di un lutto di un familiare[587].

Nella parte argomentativa della sentenza appena citata si rileva che la difesa del soggetto che ha elaborato il sito *web* dotato del *chatbot* ha addotto l'autonomia soggettiva e giuridica del software rispetto all'impresa, ma come affermato in letteratura «è sempre

[587] *Civil Resolution Tribunal of British Columbia*, 14 febbraio 2024.

un programma informatico che, seppur complesso e dotato di un grado variabile di indipendenza, rimane pur sempre tale»[588] e interagisce con «l'utente attraverso uno scambio di informazioni secondo precise istruzioni già prefissate (algoritmi)»[589].

Sebbene sia indubbio che il *software* debba avere un certo grado di intelligenza, di autonomia, di capacità di elaborare e memorizzare i risultati informativi condivisi e appresi, per la sua natura di bene informatico, seppure autonomo nell'operatività, non si può qualificare come soggetto di diritto e non si ritiene possibile aderire a quella tesi avanzata in dottrina che considera il

---

[588] G. SARTOR, *Gli agenti software: nuovi soggetti del ciberdiritto?*, in *Contratto e impresa*, 2002, p. 465 qualifica questi programmi come «una tipologia di software capace di azione autonoma in contesti complessi», mentre lo stesso autore in *Cognitive automata and the law: electronic contracting and the intentionality of software agents*, in Artif. Intell. Law, 17/2009, 253 che attribuisce «all'agente intelligente una capacità cognitiva».

[589] Negli Stati Uniti d'America, secondo l'Uniform Electronic Transaction Act (UCITA), «l'electronic agent is a computer program or an electronic or other automated means used independently to initiate an action, or to respond to electronic messages or performances, on the person's behalf without review of action by an individual at the time of the action or response to the message or performance». L'uso di tali risorse informatiche si indirizza su più versanti: per l'attività contrattuale attraverso la funzione di perfezionare accordi nell'ambito dello spazio telematico, ma esistono forme diverse di tali programmi per elaboratore che possono essere dedicati alla ricerca di mere informazioni sulla rete telematica (c.d. news bot), o a compiti di censori all'interno di un gruppo di discussione che, autonomamente, cancellano i messaggi a contenuto promozionale o che contengono espressioni sconvenienti o lesive dei diritti altrui (c.d. cancel bot), o che assumono il ruolo di avversari virtuali per giochi in rete (c.d. game bot).

chatbot quale rappresentante del suo creatore con applicazione della disciplina prevista per la rappresentanza dal codice civile[590].

8.2. Il chatbot *in ambito sanitario: definizioni e casi pratici.*

Il *chatbot* in ambito sanitario è uno strumento dotato di intelligenza artificiale che fornisce assistenza ai pazienti e ai fornitori attraverso l'automazione di attività quali il controllo dei sintomi, la programmazione degli appuntamenti e l'educazione sanitaria.

Nonostante l'utilizzo di tale *software* costituisca un ausilio nella gestione del malato sul versante sanitario e un'assistenza ventiquattrore su ventiquattro, sette giorni su sette, dal lato del paziente e del suo *caregiver*, i rischi connessi sono particolarmente rilevanti, sia con riferimento alla gestione dei dati sanitari sia con riguardo al contenuto delle informazioni mediche fornite dai *chatbot*.

---

[590] G. SARTOR, *L'intenzionalità dei sistemi informatici e il diritto*, in *Riv. Trim. dir. e proc. civ.*, 23/2003, invece ricorre all'istituto della rappresentanza – computer *alter ego* del *dominus* – per imputare gli atti del computer direttamente al dominus che lo ha programmato o fatto programmare. Tuttavia, considerando il chatbot come un rappresentante, seppur elettronico, si attribuisce ad esso, inevitabilmente, una soggettività giuridica che non può esistere per un'entità diversa dalla persona.

In prima battuta, si intende analizzare uno studio condotto in Italia presso l'Università "La Sapienza" di Roma[591], secondo il quale i ricercatori hanno selezionato 30 pazienti sottoposti a tre procedure comuni: filler dermici, iniezioni di botulino e blefaroplastica estetica; le domande più frequenti poste da tali pazienti sono state registrate e inviate a ChatGpt 3.5 e Google Bard v. 1.53 (ribattezzato Gemini); le risposte fornite sono state valutate da 13 chirurghi plastici estetici esperti su una scala *Likert* per accessibilità, accuratezza e utilità complessiva.

Dallo studio in oggetto è emerso che «le valutazioni generali delle risposte dei *chatbot* sono state positive; i chirurghi generalmente le hanno trovate accurate e chiare, ma i primi e più rilevanti dubbi sono emersi nel momento in cui i sistemi venivano interrogati riguardo alle fonti delle informazioni fornite».

Inoltre, «non è emersa una netta differenziazione nell'affidabilità dei due strumenti utilizzati, Bard e ChatGpt, ma è emerso un differente approccio nell'utente che interroga un *chatbot* di intelligenza artificiale generativa rispetto al tradizionale motore di ricerca di Google, ormai foriero di fake news».

---

[591] F.R. GRIPPAUDO, M. JERI, M. PEZZELLA, M. ORLANDO, D. RIBUFFO *Assessing the Informational Value of Large Language Models Responses in Aesthetic Surgery: A Comparative Analysis with Expert Opinions*. Aesthetic Plast Surg. 2025 Feb 18.

Le conclusioni a cui sono addivenuti i medici sono infatti le seguenti «sebbene i *chatbot* abbiano il potenziale per fornire ai pazienti un accesso veloce e immediato alle informazioni sulla chirurgia plastica estetica, i loro attuali limiti in termini di trasparenza e completezza richiedono cautela nell'utilizzarli come fonte primaria di informazioni. Sono necessarie ulteriori ricerche per sviluppare *chatbot* più affidabili per applicazioni sanitarie».

Prima di analizzare la disciplina riguardante l'imputazione della responsabilità per i danni cagionati da tali assistenti virtuali in ambito sanitario, saranno brevemente analizzati alcuni *software* già esistenti e utilizzati in tale settore.

"Unaremissione"[592] è un'applicazione oncologica che si rivolge ai sopravvissuti e a coloro i quali stanno affrontare la malattia e si occupa di medicina integrativa, curando l'esercizio fisico, la nutrizione, il sonno e le pratiche di gestione dello stress dovuto alla diagnosi. L'utente avrà la possibilità di chiedere se un determinato alimento possa reagire con i suoi farmaci e per le domande urgenti, potrà consultare un oncologo di guardia ventiquattrore su ventiquattro, sette giorni su sette.

L'applicazione *Buoy*[593] è stata sviluppata da un gruppo di medici e *data science* presso gli Harvard Innovation Labs per effettuare

[592] https://businesspump.com/oneremission-chatbot-ai-success/.
[593] https://www.buoyhealth.com

l'attività di triage tramite un chatbot; infatti, gli utenti scriveranno a *Buoy* i loro sintomi e riceveranno un riscontro, comprese le potenziali cause e la gravità e sulla base di una valutazione algoritmica, il chatbot, a seguito di tale comparazione, raccomanderà i passi successivi e offrirà un servizio di *follow up* via sms.

"Florence"[594] è un'assistente sanitario personale progettato per impostare promemoria per i farmaci, fornire informazioni dettagliate sui medicinali, tenere traccia di parametri come il peso corporeo, l'umore e i cicli mestruali, individuare medicinali o farmacie più vicine che possiedono un determinato prodotto.

"Youper"[595] è un chatbot progettato per supportare gli utenti che stanno affrontando una patologia mentale.

L'obiettivo, tramite i principi della terapia cognitivo-comportamentale (CBT), è quello di coinvolgere gli utenti in brevi conversazioni interattive per riorganizzare i pensieri o gestire le emozioni, tenendo traccia dell'umore, attraverso il c.d. diario dei pensieri.

"Molly" di "Sensely"[596] è un assistente medico virtuale, in grado di valutare i sintomi di un paziente utilizzando sia il testo che la

[594] https://www.florence.chat
[595] https://www.youper.ai
[596] https://sensely.com

comunicazione vocale. Il chatbot di Sensely è un agente vocale AI che interagisce con gli utenti. Infatti, quando i pazienti segnalano i loro sintomi, il *software* analizza i dati e le informazioni raccolte tramite il suo algoritmo per vagliare le condizioni dei pazienti e "raccomandare" una diagnosi. I pazienti potranno anche inviare immagini e video per ottenere una diagnosi più precisa e un sistema di *triage* a colori che gli consentirà di comprendere la gravità dell'emergenza.

"Babylon Health"[597] è un servizio di abbonamento britannico che consente ai pazienti di avere consultazioni in telemedicina con medici e operatori sanitari tramite messaggio di testo e videomessaggi.

Lo stesso dispone di un chatbot per il controllo dei sintomi che vengono analizzati sulla base di un *database* di malattie per fornire una diagnosi pertinente e un trattamento adeguato; il paziente potrà avviare una chat video con un medico reale che può prescrivere farmaci, indirizzare ad un altro specialista o prenotare un esame strumentale.

8.3. La responsabilità per i danni cagionati dal chatbot in ambito sanitario: una prospettiva de iure condendo.

[597] https://www.mobihealthnews.com/news/babylons-ai-enabled-symptom-checker-added-recently-acquired-higis-app

Nei paragrafi precedenti si è proceduto alla definizione del *chatbot* in generale e nel particolare con riguardo ai dati sanitari, è stato analizzato sia uno studio condotto in Italia circa l'affidabilità e l'attendibilità dello stesso nell'ambito della chirurgia plastica estetica, sia una pluralità di assistenti virtuali sanitari operanti in vari ambiti e in svariati Paesi.

Sebbene si aderisca alla tesi sostenuta dalla dottrina e in precedenza citata che nega una soggettività giuridica in capo al chatbot, in questo paragrafo conclusivo si tenterà di analizzare che tipo di responsabilità potrebbe essere in astratto imputabile al sistema automatizzato.

Da un lato, qualora si considerasse il *software* utilizzato dalla struttura sanitaria come un mediatore, che dunque ai sensi dell'art. 1754 del codice civile è «colui che mette in relazione due o più parti, per la conclusione di un affare, senza essere legato ad alcuna di esse da rapporti di collaborazione, di dipendenza o di rappresentanza», potrebbe incorrere in responsabilità qualora, ai sensi dell'art. 1759 del codice civile, omettesse di «comunicare alle parti le circostanze a lui note relative alla valutazione e alla sicurezza dell'affare, che possono influire sulla conclusione di esso» e dunque, *mutatis mutandis*, il chatbot potrebbe incorrere in responsabilità nell'eventualità in cui, in ambito sanitario,

omettesse di riferire circostanze utili e fondamentali per la conclusione del contratto di spedalità.

Ma, attribuire una tale responsabilità all'agente elettronico significherebbe conferirgli non soltanto una soggettività e dunque una capacità giuridica ma anche una capacità di agire che una macchina non ha e non può avere.

Qualora, invece, si aderisse alla teoria citata in precedenza di assimilazione del computer al soggetto che se ne serve, utilizzando l'istituto della rappresentanza si finirebbe con l'attribuire gli effetti giuridici degli atti dell'assistente c.d. intelligente alla persona che lo ha programmato o che lo ha fatto programmare, prevedendo anche in questa circostanza la responsabilità del produttore del dispositivo ovvero una corresponsabilità con la struttura sanitaria che si sia servita del *chatbot*, ma questa teoria incontra gli stessi limiti della precedente e cioè significherebbe configurare l'assistente virtuale quale centro di imputazione giuridica che aprirebbe scenari imprevedibili e lontani dalla visione antropocentrica dell'intelligenza artificiale a cui aderisce l'Italia.

L'ultimo aspetto da prendere in considerazione in questo scritto è relativo alla responsabilità per l'erogazione di informazioni inesatte fornite da un sistema automatizzato addestrato da un soggetto professionista che nell'ambito della propria attività eroga risposte su sollecitazione di un utente.

L'informazione fornita da un *chatbot* non va considerata solo da un punto di vista contenutistico ma anche in senso funzionalistico «come oggetto di comunicazione al pubblico che assume anche un fine specialistico, inteso come regola di condotta posto a carico di alcuni soggetti che entrano in relazione con altri»[598].

Nello scenario eventuale di un chatbot in ambito sanitario che fornisca un consiglio medico o una diagnosi errata, arrecando un danno ad un soggetto, seguendo quest'ultima teoria potrebbero concorrere sia la disciplina della responsabilità extracontrattuale della *culpa in contrahendo* – in quanto l'aver fornito un'informazione errata può aver condotto a concludere un contratto, quale quello di spedalità, che altrimenti non sarebbe stato contratto – che quella della responsabilità contrattuale derivante dal contatto sociale che ingenera l'affidamento dei soggetti coinvolti in virtù di «una serie di doveri di collaborazione e protezione volti alla salvaguardia di determinati beni

[598] Come previsto da V. ZENO-ZENCOVICH, *Informazione (profili civilistici)*, in *Dig. Civ.*, IX, Torino, 1993, 420, il termine informazione ha assunto nell'era contemporanea un significato polisenso o polisemantico: in un primo senso, di tempo contenutistico, per informazione si intende qualsiasi dato rappresentativo della realtà che viene conservato da un soggetto oppure comunicato da un soggetto ad un altro; nel senso funzionalistico, sotto il termine informazione si ricomprendono quelle attività di comunicazione al pubblico svolte da taluni mezzi, quali la stampa, la radio e la televisione; in una terza accezione di tipo specialistico, l'informazione integra un obbligo posto a carico di taluni soggetti quando entrano in rapporto con altri, come avviene nelle trattative contrattuali.

giuridici»[599], di obbligazioni in ossequio alla relazione che si instaura indipendentemente dall'esistenza di un contratto[600], di rapporti giuridici che prevedono regole di condotta quali la buona fede, la protezione dei diritti altrui e l'obbligo di informazione, ai sensi degli artt. 1175 e 1375 del codice civile[601].

L'inadempimento delle prestazioni determina la responsabilità da contatto sociale che potrebbe in astratto applicarsi al caso di specie, ingenerando «un'inosservanza all'obbligo di comportamento rappresentato dall'erogazione di informazioni corrette, esaustive e veritiere nei confronti di chi ha fatto affidamento sull'assistente vocale entrando in contatto con lui»[602].

---

[599] F. VENOSTA, *"Contatto sociale" e affidamento*, Milano, 2021.

[600] Tra gli altri, G. STELLA RICHTER, *Contributo allo studio dei rapporti di fatto nel diritto privato*, in *Riv. Trim. dir. proc. civ.*, 1977, p. 151.

[601] Tra le altre, Cass. Civ. 27 ottobre 2017, n. 25644; Cass. Civ. 12 luglio 2016, n. 14188.

[602] C. CASTRONOVO, *L'obbligazione senza prestazione. Ai confini tra contratto e torto*, in *Le ragioni del diritto. Scritti in onore di Luigi Mengoni*, I, Milano, 1995, p. 147 che riconduce al contatto sociale le ipotesi delle informazioni erronee fornite da un professionista al di fuori dell'adempimento di un'obbligazione avente tale oggetto, delle informazioni contenute in un prospetto finanziario relativo ad una società o ad una operazione di investimento, dell'informazione erronea formulata da un professionista su incarico di un cliente e comunicata a un terzo che su di essa fonda un affidamento e resta deluso. In campo sanitario, vedasi, D. PITTELLA, *Dall'obbligazione senza prestazione alla responsabilità extracontrattuale del medico: rigetto locale o totale del contratto "qualificato"?* in *Contr. e impr.*, 2020, p. 418.

La situazione è ancora più complessa in quanto trattandosi di dati sanitari, è necessario che questi *chatbot* siano sviluppati nel rispetto delle normative stringenti in materia di informazioni mediche previste dal GDPR e dall'HIPAA statunitense.

Inoltre, non è astrattamente possibile pensare che un assistente vocale per quanto correttamente istruito e addestrato, possa fornire in autonomia delle diagnosi che non siano supportate da un medico "umano" o delle prescrizioni medicali, in quanto, sebbene l'intelligenza artificiale debba essere considerata un ausilio del contratto di spedalità, non potrà mai sostituirsi all'uomo.

Allo stato attuale dello scritto, non è configurabile l'esistenza di una responsabilità giuridicamente rilevante in capo al chatbot, in quanto non è qualificabile come soggetto di diritto, bisognerà attendere, in una prospettiva *de iure condendo*, che venga adottata la Direttiva relativa all'adeguamento delle norme in materia di responsabilità civile extracontrattuale all'intelligenza artificiale per comprenderne la collocazione, la qualificazione e la giustiziabilità delle pretese risarcitorie.

Conclusioni

Quando questo lavoro ha iniziato a prendere forma, lo scenario giuridico e mondiale era notevolmente diverso rispetto a quando si è concluso: sebbene la pandemia fosse finita, gli effetti della medesima erano ancora notevolmente evidenti e per poterli trattare è stato necessario analizzare generalmente e genericamente il dato sanitario nella sua disciplina interna e sovranazionale per poter comprendere come il Covid – che aveva comportato notevoli restrizioni a libertà fondamentali – aveva, invece, consentito la circolazione di dati cosiddetti sensibilissimi anche in assenza di un'idonea base giuridica originariamente prevista dal GDPR.

La circolazione di tali informazioni sanitarie, la cui fluidità è stata imputabile alla congiuntura pandemica, ha messo in luce talune criticità e ha messo in discussione il reale concetto di riservatezza del dato alla luce di episodi che hanno esposto gli utenti a fughe di informazioni o di applicazioni che, sebbene fossero nate con l'intento di contingentare la diffusione e la circolazione del virus, non erano predisposte per tutelare effettivamente la privacy dei pazienti.

La pandemia ha determinato anche l'esigenza di discutere circa la base giuridica legittimante l'utilizzo dei dati per finalità di ricerca, essendo necessario partire dal dato per addivenire ai risultati in

materia sanitaria che si sono rivelati cruciali per la sperimentazione e l'immissione in commercio dei vaccini che hanno garantito il superamento della pandemia.

In maniera collaterale e anche grazie all'adozione del PNRR, è emerso in modo ormai evidente il bisogno di abbattere le barriere fisiche sia con riguardo alla formazione, alla circolazione e alla diffusione della cartella clinica e del Fascicolo sanitario elettronico del paziente, determinando una storia clinica virtuale che bypassa la materialità e si sottrae ad errori imputabili al paziente che producono effetti anche sull'efficacia e sull'efficienza della prestazione sanitaria; sia con riguardo all'abbattimento della necessaria compresenza di entrambe le parti contraenti di un contratto di spedalità, essendosi ampiamente diffuse svariate forme di dematerializzazione di prestazioni sanitarie attraverso il ricorso alla telemedicina.

Nel lavoro in oggetto si è analizzato ampiamente anche lo Spazio europeo dei dati sanitari che aveva come obiettivo principale l'abbattimento delle barriere dei singoli Stati dell'Unione, attraverso la realizzazione di un'unione di dati sanitari che avrebbe dovuto consentire ai cittadini europei, tramite un profilo sanitario sintetico, di fruire dei servizi inerenti alla salute in assenza di ostacoli linguistici o materiali, ma allo stato attuale dello scritto gli

obiettivi prefissati in materia non sono stati raggiunti, sussistendo notevoli ritrosie da parte di taluni Stati membri.

La ricerca ha trasversalmente e a più riprese trattato l'intelligenza artificiale e come la stessa abbia inciso sia sul dato sanitario, sull'addestramento di algoritmi in materia, rivoluzionando anche le modalità di esecuzione di una prestazione sanitaria, accelerando l'utilizzo di dispositivi medici intelligenti e ne ha trattato – o ha provato a farlo – le forme di responsabilità sussistenti, oscillando tra la necessità di individuare nuove categorie giuridiche e l'applicazione analogica di quelle già esistenti, evidenziandone ogni criticità.

Da ultimo si è trattato della figura del chatbot, la cui soggettività giuridica e la conseguente esistenza di una responsabilità civile è al centro del dibattito giuridico attuale.

Nel momento in cui questo scritto si conclude, non si dispone degli strumenti per affermare nero su bianco quali saranno gli effetti dell'intelligenza artificiale e del macrocosmo prestazioni sanitarie/dispositivi medici/medicinali intelligenti e determinare con assoluta certezza quale sia la forma di responsabilità civile più consona ai danni cagionati dai medesimi, essendo necessario attendere l'intervento del legislatore europeo che affermi con chiarezza chi sono i soggetti di diritto a cui imputare il danno – e se tra questi possa esservi il chatbot –, che tipo di responsabilità si

configura, la modalità di esercizio delle azioni risarcitorie e i tempi dei medesimi.

Bibliografia

AA.VV., *AI: profili giuridici. Intelligenza Artificiale: criticità emergenti e sfide per il giurista* in *BioLaw Journal – Rivista di BioDiritto*, 2019.

AA.VV., in A. D'ALOIA (a cura di), *Intelligenza artificiale e diritto. Come regolare un mondo nuovo*, Milano, 2021.

AA.VV., in C. CAMARDI (a cura di), *La via europea per l'intelligenza artificiale.* Atti del convegno del progetto dottorale di alta formazione in scienze giuridiche, Ca' Foscari Venezia, 25-26 novembre 2021, Padova, 2022;

AA.VV., in C. CASONATO, M. FASAN e S. PENASA (a cura di), *Diritto e intelligenza artificiale*, sezione monografica in DPCE online, 2022.

AA.VV., in G. ALPA (a cura di), *Diritto e intelligenza artificiale,* Pisa, 2020.

AA.VV., in G. M. RICCIO, G. ZICCARDI e G. SCORZA (a cura di), *Intelligenza artificiale. Profili giuridici*, Padova, 2022.

AA.VV., in U. RUFFOLO (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020.

R.M. AGOSTINO, *Intelligenza artificiale e processi decisionali*, in *Mercato Concorrenza Regole*, 2020.

E. Al MUREDEN, *Autonomous cars e responsabilità civile tra disciplina vigente e prospettive de iure condendo*, in *Contratto e impr.,* 2019.

E. Al MUREDEN, *La responsabilità del fabbricante nella prospettiva della standardizzazione delle regole sulla sicurezza dei prodotti* in E. Al MUREDEN, *La sicurezza dei prodotti e la responsabilità del produttore. Casi e materiali*, Torino, 2017.

A. ALBANESE, *La responsabilità civile per i danni da circolazione dei veicoli ad elevata automazione*, in *Europa e d. priv.*, 2019

L. ALIMENTI, E. SCIARRETTA, *I chatbot nel campo medico* in S. CAPOGNA, A. DEL CIMMUTO, C. FONZO (a cura di), *L'istruzione, il lavoro e la società ai tempi dell'emergenza pandemica globale*, 1/2021.

G. ALPA (a cura di), *Diritto e intelligenza artificiale. Profili generali, soggetti, contratti, responsabilità civile, diritto bancario e finanziario, processo civile*, Pisa, 2020.

G. ALPA, *Ars interpretandi e responsabilità sanitaria nella nuova legge Gelli Bianco*, in Contr. Impr., 2017.

G. ALPA, in D'ORAZIO, FINOCCHIARO, POLLICINO, RESTA (a cura di), *Codice della Privacy e Data protection*, Milano, 2021.

G. ALPA, *Solidarietà. Un principio normativo*, Bologna, 2022.

A. AMIDEI, *Intelligenza artificiale e product liability: sviluppi del diritto dell'Unione Europea*, in *Giur. It*., 2019.

A. AMIDEI, *La produzione di dispositivi medici AI-based: regolazione e responsabilità*, in U. RUFFOLO, M. GABBRIELLI (a cura di), *Intelligenza artificiale, dispositivi medici e diritto. Un dialogo tra saperi: giuristi, medici e informatici a confronto.*

A. AMIDEI, *Robotica intelligente e responsabilità: profili e prospettive evolutive del quadro normativo europeo*, in *Giur. It.*, 2021.

C. ANGIOLINI, *Health and Data Protection* in P. IAMICELI, F. CAFAGGI e C. ANGIOLINI (a cura di), Casebook Judicial Protection of Health as a Fundamental Right, Roma, 2022.

P. AURUCCI, *Il trattamento dei dati personali nella ricerca biomedica. Problematiche etico-giuridiche*, Napoli, 2022.

C. BALDASSARRE, *Responsabilità del produttore: danno risarcibile, onere della prova e logica giuridica* in Danno e resp. 2014.

S. BARTOLE, P. DE SENA e V. ZAGREBELSKY (a cura di), Commentario breve alla Convenzione europea dei diritti dell'uomo, Padova, 2012.

M. BASSINI, *Il diritto costituzionale alla privacy nel prisma dell'evoluzione tecnologica*, in *Dir. Cost*. 2023.

M. BASSINI, L. LIGUORI, O. POLLICINO, *Sistemi di intelligenza artificiale, responsabilità e accountability. Verso nuovi paradigmi*, in F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Torino, 2018.

S. BASTIANON, *Responsabilità del produttore per prodotti difettosi: quale tutela per il consumatore?* in Resp. Civ. e prev., 4-5/2002.

E. BATTELLI, *Necessità di un umanesimo tecnologico: sistemi di intelligenza artificiale e diritti della persona*, in *Dir. Fam. Pers.* 2022.

S.M. BELLOVIN, P.K. DUTTA, N. REITINGER, *Privacy and Synthetic Datasets*, «STAN. TECH. L. REV.», vol. 22, n. 1/2019.

P. BENANTI, *Human in the loop, Decisioni umane e intelligenze artificiali*, Milano, 2022.

A. BERTOLINI, *Artificial Intelligence and Civil Liability*, in *Study Requested by the JURI committee, Policy Department for Citizens' Rights and Constitutional Affairs Directorate General for Internal Policies*, Bruxelles, 2020

A. BERTOLINI, *Robots as Products: the case for a realistic analysis of robotics applications and liability rules*, in *Law Innov. Technol.*, 1/2013.

C. M. BIANCA, *Diritto civile*, 5, *La responsabilità*, 2021.

G. BINCOLETTO, *A Data Protection by Design Model for Privacy Management in Electronic Health Records,* in Privacy Technologies and Policy, 7th Annual Privacy Forum, Lecture Notes in Computer Science, 2019.

G. BINCOLETTO, *Data Protection Issues in Cross-Border Interoperability of Electronic Health Record Systems within the European Union*, in *Data & Policy*, 2-3/2020.

G. BINCOLETTO, *L'uso secondario di dati sanitari per fini di ricerca nella telemedicina: la tutela dei dati personali tra regole e prassi in ricerca* in *Sanità e protezione dei dati personali: scenari applicativi e prospettive future*, in E. CHIZZOLA, P. GUARDA, V. MARONI, L. RUFO (a cura di), Atti del convegno Trento, 29 settembre 2023.

G. BINCOLETTO, *mHealth app per la televisita e il telemonitoraggio. Le nuove frontiere della telemedicina tra disciplina sui dispositivi medici e protezione dei dati personali*, in *BioLaw Journal – Rivista di BioDiritto*, n. 4/2021.
G. BINCOLETTO, P. GUARDA, *A proactive GDPR-compliant solution for fostering medical scientific research as a secondary use of personal health data*, in *Opinio Iuris in Comparatione* n. 1/2021.

A. L. BITETTO, *Responsabilità da prodotto difettoso: strict liability o neglicence rule?*, in *Danno e resp.*, 3/2006.
M. BOCCHINO, *Significato dei Real World Data nell'era della medicina digitale: realtà e prospettive* in *Ricerca in sanità e protezione dei dati personali: scenari applicativi e prospettive future*, in E. CHIZZOLA, P. GUARDA, V. MARONI, L. RUFO (a cura di), Atti del convegno Trento, 29 settembre 2023.

L. BOLOGNINI, S. ZIPPONI, *Prospettive future in sanità: Spazio europeo dei dati sanitari e regolazione dei dati sintetici* in *Privacy e diritto dei dati sanitari*.
C. BOTRUGNO, *The spread of telemedicine in routine medical practice: towards an ad hoc ethics*, in *Ragion pratica*, 1/2016.

F. BRIZZI, *Dati sanitari, GDPR e Covid-19, Il caso della ricerca: tra scienza e diritto*, 2021, Key editore srl.
F. E. BROZZETTI, *I dati sintetici: panacea della privacy?* in *top legale*, 23 gennaio 2024.
I. BUDIN LJØSNE, H.J.A. TEARE, J. KAYE, *Dynamic Consent: a potential solution to some of the challanges of modern biomedical research*, in *BMC Medica Ethics*, 18 (4), 2017.

N. BUSCA, *Il trattamento dei dati sanitari nell'ambito della ricerca e della sperimentazione clinica* in www.rivistaresponsabilitamedica.it, 26 settembre 2020.

B. BUZZELLI, *Dati sanitari e implementazione dell'Intelligenza artificiale*.

D. BUZZELLI, M. PALAZZO (a cura di), *Intelligenza artificiale e diritti della persona*, Pisa, 2022.

F. BUZZI, C. SCLAVI, *La cartella clinica: atto pubblico, scrittura privata o "tertium genus"?* in *Rivista Italiana di Medicina legale*, 1997.

L. A. BYGRAVE, *The EU General Data Protection Regulation (GDPR). A Commentary*, a cura di C. KUNER, L. A. BYGRAVE e C. DOCKSEY, Oxford University Press, 2020, sub art. 22.

F. CAGGIA, *Il trattamento dei dati sulla salute, con particolare riferimento all'ambito sanitario*, in V. CUFFARO- R. D'ORAZIO-V. RICCIUTO (a cura di), *Il codice del trattamento dei dati personali*, Torino, 2007.

C. CAPE, *Electronic Patient Record (EPR) Benefits realisation case study*, in *Oxford University Hospitals NHS Trust, Health and Social Care Information Centre*, Oxford, 2015.

C. CAPORALI, *Invecchiamento e divari di genere nell'uso degli strumenti di eHealth* in *Culture e Studi del Sociale*, n. 9/2024.

F. CASCINI, *Digitalizzazione della Sanità e sicurezza delle cure*, in F. GELLI, M. HAZAN, D. ZORZIT, F. CASCINI (a cura di), *Responsabilità, rischio e danno in sanità*, Milano, 2022.

C. CASONATO, *I farmaci tra speculazioni e logiche costituzionali*, in *Rivista AIC*, 4/2017.

C. CASONATO, M. TOMASI, *Diritti e ricerca biomedica: una proposta verso nuove consonanze*, in *BioLaw Journal – Rivista di BioDiritto*, n. 1/2019.

V. CASONATO, M. FASAN e S. PENASA (a cura di), *Diritto e intelligenza artificiale, sezione monografica* in *DPCE online*, 2022, fasc. 1.

M. CASTILLA BAREA, *La universidad ante los desafíos éticos de la inteligencia artificial. Reflexiones a propósito del nuevo «marco europeo de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas»*, in *Edunovatic 2020, Conference Proceedings: 5th Virtual International Conference on Education, Innovation and ICT*, December 10 - 11, 2020.

C. CASTRONOVO, *L'obbligazione senza prestazione. Ai confini tra contratto e torto*, in *Le ragioni del diritto. Scritti in onore di Luigi Mengoni*, I, Milano, 1995.

C. CASTRONOVO, *Responsabilità civile*, Milano, 2019.

M. CENINI, *La responsabilità solidale del "mandatario" nell'ambito della disciplina europea sui dispositivi medici*, in *Resp. Civ. e prev.*, 5/2020.

G. CERRINA FERONI, *IA nei processi decisionali della PA, il faro è la Costituzione*, in *Agenda Digitale UE*, 1-28.

G. CERRINA FERONI, *Sanità digitale e assetti istituzionali*, G. CERRINA FERONI (a cura di) in *Le nuove frontiere della medicina, assetti istituzionali e gestione dei dati.*

R. CHALLEN, J. DENNY, M. PITT et al., *Artificial intelligence, bias and clinical safety*, in *BMJ Quality & Safety*, 28/2019.

B. CHEN, A. J. BUTTE, *Leveraging Big Data to Transform Target Selection and Drug Discovery* in *Clinical Pharmacology and Therapeutics*, vol. 99 del 2016.

E. CHOI, S. BISWAL, B. MALIN, J. DUKE, W.F. STEWART, J. SUN, *Generating Multi-Label Discrete Patient Records Using Generative Adversarial Networks*, in *Proceeding of Machine Learning for Healthcare*, vol. 68/2017.

M. CIANCIMINO, *Circolazione "secondaria" di dati sanitari e biobanche. Nuovi paradigmi contrattuali e istanze personalistiche- Nota a Cass. 7 ottobre 2021 n. 27325,* in *Dir. fam. pers*., 2022.

G. CIPRIANO, *La cartella clinica digitale*, in *Il Diritto sanitario moderno*, 1/2008.

G. COLANGELO, *Accesso ai Data e condizioni di licenza F/RAND*, in V. FALCE, G. GHIDINI, G. OLIVIERI (a cura di), *Informazione e Big Data tra Innovazione e Concorrenza*, Milano, 2018.

C. COLAPIETRO, *Il diritto alla protezione dei dati personali in un sistema delle fonti multilivello. Il Regolamento UE 2016/679 parametro di legittimità della complessiva normativa italiana sulla privacy*, Napoli, 2018.

A. COLARUOTOLO, *Intelligenza artificiale e responsabilità medica: novità, continuità e criticità*, in *Resp. Med*. 2022.

P. COLETTI, *L'innovazione digitale nell'amministrazione pubblica: le azioni delle Regioni*, in *Amministrare*, 3/2013.

G. COMANDÉ, *Intelligenza artificiale e responsabilità tra liability e accountability: il carattere trasformativo dell'IA e il problema della responsabilità*, in *Analisi Giuridica dell'Economia*, 2019.

G. COMANDÉ, L. NOCCO, e V. PEIGNÉ, *An empirical study of healthcare providers and patients' perceptions of electronic health records*, in *Computers in Biology and Medicine*, 2015.

G. COMANDÈ, L. NOCCO, V. PEIGNÈ, *Il Fascicolo sanitario elettronico: uno studio multidisciplinare*, in Riv. It. Med. Leg. 2012.

G. COMANDÈ, *Multilayered (Accountable) Liability for Artificial Intelligence*, in S. LOHSS, R. SCHULZE, D. STAUDENMAYER (a cura di), *Liability for Artificial Intelligence and the Internet of Things*, Baden, 2019.

G. COMANDÈ, *Ricerca in sanità e data protection: un puzzle…risolvibile*, in *Riv. It. Med. Leg*. 2019.

L. COPPINI, *Robotica e intelligenza artificiale: questioni di responsabilità civile*, in *Politica del diritto*, 2018.

L. COPPINI, *Robotica e intelligenza artificiale: questioni di responsabilità civile.*

S. CORONATO, *Gli strumenti necessari al processo di digitalizzazione del S.S.N.* in *Diritto sanitario moderno*, n. 3/2019, p. 169.

S. CORSO, *Il fascicolo sanitario elettronico 2.0.: spunti per una lettura critica* in *Le nuove leggi civili commentate* n. 2/2024.

S. CORSO, *Modifiche alla disciplina sul trattamento dei dati relativi alla salute*, in www.rivistaresponsabilitamedica.it, 29 gennaio 2022.

S. CORSO, *Sanità digitale e riservatezza. Interpretazioni sul Fascicolo sanitario elettronico* in A. THIENE e S. CORSO (a cura di), *La protezione dei dati sanitari, privacy e innovazione tecnologica tra salute pubblica e diritto alla riservatezza*, in Atti di Convegno – Rovigo 4 novembre 2022.

S. CORSO, Sanità digitale e riservatezza. Interpretazioni sul fascicolo sanitario elettronico in *La protezione dei dati sanitari. Privacy e innovazione tecnologica tra salute pubblica e diritto alla riservatezza, 2023.*

S. CORSO, *Trattamento di dati sanitari e tutela della persona. Dal consenso alla volontà*, F.A. BELLA, N. POSTERARO, M.A. SANDULLI (a cura di) in *Il comitato di ricerca si confronta - atti del II ciclo di Seminari (2022-2023).*

M. COSTANZA, *L'intelligenza artificiale e gli stilemi della responsabilità civile*, in *Giur. It.*, 2019.

M. COSTANZA, *Robot e impresa*, in U. RUFFOLO (a cura di), *Intelligenza artificiale e responsabilità*, Milano.

G. CRISAFI, *Fascicolo sanitario elettronico: "profilazione" programmazione sanitaria*, in *federalismi.it*, n. 5/2021.

G. G. CRUDELI, *Sistemi di intelligenza artificiale autonomi e responsabilità datoriale*, in *Diritto della sicurezza sul lavoro*, 2/2024.

D.J. CURRIE, C.Q. PENG, D.M. LYLE, B.A. JAMESON, M.S. FROMMER, *Stemming the flow: how much can the Australian smartphone app help to control Covid-19*, in *Pub. Hea. Res. & Prac.*, v.30, 2/2020.

A. D'ADDA, *Danni «da robot» (specie in ambito sanitario) e pluralità di responsabili tra sistema delle responsabilità civili ed iniziative di diritto europeo*, in *Riv. Dir. Civ.*, 2022

A. D'ADDA, *Responsabilità "da robot": i soggetti responsabili e i loro rapporti interni (con speciale riferimento all'ambito sanitario)*, in U. SALANITRO (a cura di), *SMART la persona e l'infosfera.*

G. D'ALFONSO, *Il regime di responsabilità da cose in custodia tra questioni tradizionali e "responsabilità da algoritmo"*, *EJPLT*, 2022.

A. D'ALOIA (a cura di), Intelligenza artificiale e diritto. Come regolare un mondo nuovo, Franco Angeli.

A. D'ALOIA, *Il diritto e l'incerto mestiere del vivere*, in *Ricerche di biodiritto*, Padova, 2021.

A. D'ALOIA, *Il diritto verso "il mondo nuovo". Le sfide dell'intelligenza artificiale*, *in BioLaw Journal-Rivista di BioDiritto*, n. 1/2019.

G. D'AMICO, *Responsabilità per inadempimento e distinzione tra obbligazioni di mezzi e di risultato*, in *Il diritto delle obbligazioni e dei contratti: verso una riforma? Atti del Convegno per il cinquantenario della Rivista di diritto civile*, Cedam, 2006.

R. D'ORAZIO, La tutela multilivello del diritto alla protezione dei dati personali e la dimensione globale, in V. CUFFARO, R. D'ORAZIO e V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019.

C. DEL FEDERICO, *Intelligenza artificiale e responsabilità civile. Alcune osservazioni sulle attuali proposte europee* in *Jus Civile*, 5/2023.

D. DE MARTINI, *I fatti produttivi di danno risarcibile*, Padova, 1983.

R. DE MATTEIS, *Le responsabilità in ambito sanitario. Il regime binario: dal modello teorico ai risvolti applicativi*, Milano, 2017.

G. DE VERGOTTINI, C. BOTTARI, *La sanità elettronica*, Bologna, 2018.

V. DI FELICE, *Lo spazio europeo dei dati sanitari* in *Nota su atti dell'Unione europea*, Servizio studi del Senato, n. 102, luglio 2022.

C. Di FRANCESCO MAESA, *La profilazione nel contesto del diritto internazionale*, in A. ADINOLFI e A. SIMONCINI (a cura di), in *Protezione dei dati personali e nuove tecnologie. Ricerca interdisciplinare sulle tecniche di profilazione e sulleloro conseguenze giuridiche*.

A. DI MAJO, *Il giudizio di responsabilità civile del medico dopo la legge Gelli e cioè la perizia "guidata"* in *Giur. It.*, 2018.

A. DI MARTINO, *Intelligenza artificiale e decisione amministrativa automatizzata*, in Tecnologie e diritto, 2020.

G. DI MARTINO, *Sulla natura della responsabilità per danno da prodotto difettoso* in Foro it. 2007.

F. DI MARZIO, *Ancora sulla nozione di "consumatore" nei contratti*, in *Giust. Civ*. 1/2002.

D. DI SABATO, *Gli smart contracts: robot che gestiscono il rischio contrattuale*, in Contr.impr., 2017.

D. DI SABATO, *I sistemi di IA tra esigenze di tutela della persona e efficienza del mercato*, in *Teoria e prassi del diritto*, 2022.

D. DI SABATO, *Strumenti riparatori e risarcitori* in. P. PERLINGIERI, S. GIOVA, I. PRISCO (a cura di), *Il trattamento algoritmico dei dati tra etica, diritto e economia.*

F. DONATI, *Diritti fondamentali e algoritmi nella Proposta di Regolamento sull'intelligenza artificiale*, in A. PAJNO, F. DONATI, A. PERRUCCI (a cura di), *Intelligenza artificiale e diritto: una rivoluzione? Vol. 1*, Bologna, 2022.

S. DORIGO (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*, Pacini giuridica, 2020

E. S. DOVE, *Biobanks, Data Sharing and the Drive for a Global Privacy Governance Framework*, in *Journal of law, Medicine and Ethics, 43(4)*, 2015.

C. ECCHER et al., *TreC Platform. An integrated and evolving care model for patients' empowerment and data repository, in Journal of Biomedical informatics*, 102/2020.

K. EL EMAM, L. MOSQUERA, R. HOPTROFF, *Practical Synthetic Data Generation*, 2020.

B. S. ELGER, A.L. CAPLAN, *Consent and anonymization in research involving biobanks: Differing terms and norms present serious barriers to an international framework*, in EMBO Reports, 7 (7), 2006.

E. A. EMILIOZZI, *La responsabilità medica*, Milano, 2023.

M. FACCIOLI, *Intelligenza artificiale e responsabilità sanitaria* in *La nuova Giurisprudenza civile commentata*, n. 3, 1 maggio 2023

F. FAINI, *Intelligenza artificiale e regolazione giuridica: il ruolo del diritto nel rapporto tra uomo e macchina*, in *Federalismi,* n. 2/2023.

F. FAINI, *Intelligenza artificiale, diritto e pubblica amministrazione*, in *Intelligenza artificiale e diritto. Come regolare un mondo nuovo,* a cura di D'ALOIA, Milano, 2021.

C. FARALLI, R. BRIGHI, M. MARTONI et al., *Strumenti, diritti, regole e nuove relazioni di cura: Il Paziente europeo protagonista nell'e-Health,* Torino, 2015.

G. FARES, *Artificial intelligence in social and health services: A new challenge for public authorities in ensuring constitutional rights*, in M. BELOV (a cura di), *The IT revolution and its impact on State, constitutionalism and public law*, Hart Publishing, Oxford, 2021.

S. FARO, T.E. FROSINI, G. PERUGINELLI (a cura di), *Dati e algoritmi. Diritto e diritti nella società digitale*, Bologna, 2020.

E. FAZIO, *Intelligenza artificiale e diritti della persona*, Napoli, 2023

P. FEMIA, *Soggetti responsabili. Algoritmi e diritto civile*, in G. TEUBNER, *Soggetti giuridici digitali? Sullo status privatistico degli agenti software autonomi*.

E.A. FERIOLI, *Digitalizzazione, intelligenza artificiale e robot nella tutela della salute*, in A. D'ALOIA, (a cura di), *Intelligenza artificiale e diritto. Come regolare un mondo nuovo*, Franco Angeli, 2020.

M. FERRARA, *Dalla mobilità dei pazienti alla interoperabilità dei sistemi sanitari. Spunti sull'adozione di un formato europeo di scambio delle cartelle sanitarie elettroniche (Raccomandazione UE 2019/243)*, in *federalismi.it*, n. 5/2021.

L. FERRARO, *Il Regolamento UE 2016/679 tra Fascicolo Sanitario Elettronico e Cartella Clinica Elettronica: il trattamento dei dati di salute e*

l'autodeterminazione informativa della persona in BioLaw Journal – Rivista di BioDiritto, n. 4/2021.

G. FINOCCHIARO, *Intelligenza artificiale e diritto. Intelligenza artificiale e protezione dei dati personali*, in *Giur. It.*, 2019.

G. FINOCCHIARO, *Intelligenza artificiale e responsabilità*, in *Contr.impr.*, 2020.

A. FIORENTINI, *Machine learning e dispositivi medici: riflessioni in materia di responsabilità civile*, in *Corr. Giur.*, 2021.

L. FORT, V. IEVA, *Intelligenza artificiale, responsabilità civile e interpretazione analogica*, in www.biodiritto.org, 8/2020.

F. FRÈ, *La cartella clinica nel sistema sanitario italiano*, in *Ragiusan*, 291-292, 2008.

T. E. FROSINI, *Il costituzionalismo nella società tecnologica* in *Il diritto dell'informazione e dell'informatica*, n. 4/2020.

T. E. FROSINI, *L'orizzonte giuridico dell'intelligenza artificiale*, in Dir. inf., 2022.

T.E. FROSINI, *La privacy nell'era dell'intelligenza artificiale*, in *DPCE online*, 1/2022.

E. GABRIELLI e U. RUFFOLO (a cura di), *Intelligenza Artificiale e diritto*, in *Giur.it*., 2019.

F. GABRIELLI, M. ZIBELLINI, R. TRIOLA, M. BOCCHINO (a cura di), *Decentralized Clinical Trial: nuovo approccio alla sperimentazione clinica per facilitare il paziente e velocizzare la ricerca*, Rapporto ISTISAN n. 4 del 2022.

D.U. GALLETTA, *Accesso civico e trasparenza della Pubblica amministrazione alla luce delle (previste) modifiche alle disposizioni del Decreto Legislativo n. 33/2013*, in *Federalismi.it*, 5/2016.

A.M. GAMBINO, M. SIRAGUSA, *Art. 15 Diritto di accesso dell'interessato*, in *Diritto, mercato, tecnologia*, 10 maggio 2023.
M. GAZZARA, *In difesa dell'art. 2236 cod. civ.*, in *Nuovo dir. Civ.*, 2020.
A. GENTILI, *La volontà nel contesto digitale: interessi del mercato e diritti delle persone* in *Riv. trim. dir. e proc. civ.*, 2022.
C. GEORGE, D. WHITEHOUSE, P. DUQUENOY, eHealth: legal, ethical and governance challenges, Berlin Heidelberg, 2012.

N. GHIBELLINI, *La medicina di iniziativa. L'impiego dell'algoritmo nel trattamento dei dati relativi alla salute* in A. THIENE, S. CORSO (a cura di), *La protezione dei dati sanitari, privacy e innovazione tecnologica tra salute pubblica e diritto alla riservatezza* in Atti del convegno, Rovigo 4 novembre 2022.
G. GHIDINI, *Art. 5 – Prodotto difettoso* e C.M. VERARDI, *Art. 6 – Esclusione della responsabilità*, entrambi in G. ALPA, U. CARNEVALI, F. DI GIOVANNI, G. GHIDINI, U. RUFFOLO, C.M. VERARDI, *La responsabilità per danno da prodotti difettosi.*
L. GIOS et al., *Use of eHealth Platforms and Apps to Support Monitoring and Management of Home-Quarantined Patients With COVID-19 in the Province of Trento*, in JMIR formative research, 5.5/2021.

I. GIUFFRIDA, *Liability for AI Decision-Making: Some Legal and Ethical Considerations*, in *Fordham Law Review*, 2019, 88, 2.
E. GIUSTI, *Intelligenza artificiale e sistema sanitario*, in S. DORIGO (a cura di), *Il ragionamento giuridico nell'era dell'intelligenza artificiale*.
R. GOLDSHTEIN, *Medicina e chirurgia a distanza: inquadramento, stato dell'arte ed applicazioni cliniche*, Tor Vergata University Press, 2005.

F.R. GRIPPAUDO, M. JERI, M. PEZZELLA, M. ORLANDO, D. RIBUFFO *Assessing the Informational Value of Large Language Models Responses in Aesthetic Surgery: A Comparative Analysis with Expert Opinions*. Aesthetic Plast Surg. 2025 Feb 18.

P. GUARDA, *Fascicolo sanitario elettronico e protezione dei dati personali*, Trento, 2011.

P. GUARDA, I dati sanitari, in V. CUFFARO – R. D'ORAZIO – V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019.

P. GUARDA, P. TRAVERSO, D. CONFORTI, S. FORTI et al., *Telemedicina, ricerca scientifica e Big Data: le nuove frontiere della sanità digitale e la protezione dei dati personali.*

P. GUARDA, R. DUCATO, *From Electronic Health Records to Personal Health Records: emerging Legal Issues in the Italian Regulation of eHealth*, in *International Review of Law, Computers & Technology*, 2016.

A. GUPTA, D.L. BHATT, A. PANDEY, *Transitioning from Real to Synthetic data: Quantifying the bias in model*, in *Synthetic Data Generation Workshop at ICLR*, 2021.

M.G. HANSSON, *Striking a Balance Between Personalised Genetics and Privacy Protection from the Perspective of GDPR*, in S. SLOKENBERGA et al. (a cura di), *GDPR and Biobanking*, Cham, 2021.

M. IASELLI, *La tutela dei dati personali in ambito sanitario*, Giuffrè, 2020.

M. IENCA, *Intelligenza2: per un'unione di intelligenza naturale e artificiale*, Torino, 2019.

M. INFANTINO, *La responsabilità per danni algoritmici: prospettive europeo continentali*, in *Resp.civ.prev.*, 2019.

C. INGENITO, *La rete di assistenza sanitaria on-line: la cartella clinica elettronica*, in *federalismi.it*, 5/2021.

C. IRTI, *L'uso delle "tecnologie mobili" applicate alla salute: riflessioni al confine tra la forza del progresso e la vulnerabilità del soggetto anziano*, in *Persona e Mercato*, 1/2023.

N. IRTI, *Il diritto nell'età della tecnica*, Napoli, 2017.

U. IZZO, *La precauzione nella responsabilità civile*, Padova, 2004.

F. J. JIMÉNEZ MUÑOZ, in *Actualidad Jurídica Iberoamericana* Nº 14, febrero 2021.

M. KAPLAN, *When the robots feel your pain*, in *The economist*, 27 novembre 2016.

S. Y. KIM, *Clinical Trials Without Consent?* in *Perspectives in Biology and Medicine*, 59/2016

M. KOSINSKI, D. STILLWELL, T. GRAEPEL, *Private traits and attributes are predictable from digital records of human behavior* in *Proceedings of the National Academy of Sciences*, 110/2013.

E. KOULIERAKIS, Certification as guidance for data protection by design in *International Review of Law, Computers & Technology*, *38*(2).

M.L. LACRUZ MANTECÓN, *Robots y personas. Una aproximación jurídica a la subjetividad cibernética*, Reus, Madrid, 2020.

C. LAENZA, *Intelligenza artificiale e diritto: ipotesi di responsabilità civile nel terzo millennio*, in *Resp.civ. prev.*, 2021.

F. LAGIOIA, *L'intelligenza artificiale in sanità, un'analisi giuridica*, Torino, 2020.

V. LAGIOIA, G. SARTOR e A. SIMONCINI, nel Codice della privacy e data protection, in R. D'ORAZIO – G. FINOCCHIARO – O. POLLICINO – G. RESTA (a cura di) Milano, 2021, sub art. 22, reg. U.E. n. 679/2016.

V. LEMMA, *COVID-19: il trattamento dei dati sanitari tra privacy e interesse pubblico*, in www.osservatoriomalattierare.it.

A. LEPORE, *I.A. e responsabilità civile. Robot, autoveicoli e obblighi di protezione, in Tecnologie e diritto*, 2021.

F. LIALNG, *Covid-19 and Health Code: How Digital Platforms Tackle the Pandemic in China*, in *Soc. Med. + Soc*., v.6, 3/2020.

A. LIOR, *AI Entities as AI Agents: Artificial Intelligence Liability and the AI Respondeat Superior Analogy*, in *Mitchell Hamline Law Review*, 2020.

F. LIU, *A statistical overview on data privacy*, in *Notre dame journal of law, ethics e public policy*, vol. 34/2010.

M.N. LOCHLAINN, K.A. LEE, C.H. SUDRE, T. VARSAVSKY, M.J. CARDOSO, C. MENNI, J.L. Du CaDET, *Key predictors of attending hospital with COVID19: An association study from the Covid Symptom Tracker App in 2,618,948 individuals*, *medRxiv*, 2020.

D. LUPTON, *M-health and health promotion: The digital cyborg and surveillance society*, in *SocTheory Health* 10, 2012.

M. MACCHIA, A. MASCOLO, *Intelligenza artificiale e sfera pubblica: lo stato dell'arte*, in Giorn. dir. amm., 2022.

J. MADIR (a cura di), *Healthtech. Law and Regulation*, Cheltenham, 2020.

D. MANTOAN, A. BORGHINI, *Potenziamento dell'assistenza sanitaria e della rete sanitaria territoriale*, in *Monitor 45*/2021.

A. MARCHESE, *Profili civilistici dell'information technology in ambito sanitario* in *Quaderni della Rassegna di diritto civile diretta da Pietro Perlingieri,* Edizioni Scientifiche Italiane

L. MARELLI, G. TESTA, *Scrutinizing the EU General Data Protection Regulation. How will new decentralized governance impact research,* in *Science, 360 (6388)*, 2018.

A. MARTANI, *Le incertezze del diritto nel contesto della sanità moderna: sfide presenti e future*, in C. PICIOCCHI, M. FASAN e C.M. REALE (a cura di), *Le (in)certezze del diritto*, Editoriale Scientifica, 2021.

D. MASCALZONI et al, *International Charter of Principles for Sharing Bio-specimens and Data*, in *European Journal of Human Genetics,* 23, 2015.

A. MASCOLO, *Gli algoritmi amministrativi: la sfida della comprensibilità*, in *Giornale Dir. Amm*., 3/2020,(nota a sentenza).

F. MATTEI, *Il punto di equilibrio tra sanità digitale e diritto alla protezione dei dati personali: la persona al centro delle nuove tecnologie* in G. CERRINA FERONI (a cura di), *Le nuove frontiere della medicina, assetti istituzionali e gestione dei dati*, 2024.

R. MATTERA, *Processo – Decisioni algoritmiche. Il Consiglio di Stato fissa i limiti*, in *Nuova Giur.* Civ., 4/2020, (nota a sentenza).

S. MELCHIONNA, F. CECAMORE, *Le nuove frontiere della sanità e della ricerca scientifica*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato, Commentario al Regolamento UE n. 679/2016 e al d. lgs. n. 101/2018*, Giuffrè, Milano, 2019.

C. MENNI, A.M. VALDES, L. POLIDORO, M. ANTONELLI, S. PENAMAKURI, A. NOGAL & T.D. SPECTOR, *Symptom prevalence, duration, and risk of hospital admission in individuals infected with SARS-CoV-2 during periods of omicron and delta variant dominance: a prospective observational study from the Zoe Covid Study*, in *the Lancet*, v.399, 10335/2022.

R. MONTINARO, *Responsabilità da prodotto difettoso e tecnologie digitali tra soft law e hard law*, in *Persona e mercato*, 2020/4.

D. MORANA, T. BALDUZZI, F. MORGANTI, *La salute "intelligente": eHealth, consenso informato e principio di non discriminazione*, in *Federalismi.it*, n. 34/2022.

T. MULDER, *Health apps, their privacy policies and the GDPR*, in *European Journal of Law and Technology*, 10.1.2019.

F. NADDEO, *Intelligenza artificiale: profili di responsabilità*, in *Comparazione e diritto civile*, 2020.

NAGENDRAN M. et al., *Artificial intelligence versus clinicians: systematic review of design, reporting standards and claims of deep learning studies*, in *BMJ*, 2020.

Z. OBERMEYER, E.J. EMANUEL, *Predicting the future – Big data, Machine Learning and Clinical Medicine*, in *New England Journal of Medicine*, 375/2016.

S. ORLANDO, *Regole di immissione sul mercato e pratiche di intelligenza artificiale vietate*, in Persona e Mercato. 3/2022.

U. PAGALLO, *Intelligenza Artificiale e diritto: Linee guida per un oculato intervento normativo* in *Sistemi Intelligenti*, 3/2017.

U. PAGALLO, *The law of robots. Crimes, contracts and torts*, New York, 2013.

L. PAGANELLI, *Il settore pubblico alla sfida dell'intelligenza artificiale*, in C. CAMARDI, (a cura di), La via europea per l'Intelligenza artificiale. Atti del Convegno del Progetto Dottorale di Alta Formazione in Scienze Giuridiche - Ca' Foscari Venezia, 25-26 novembre 2021.

E. PALMERINI, *La responsabilità medica e la prova dell'inesatto adempimento*.

A. PALMIERI, *Difetto e condizioni di impiego del prodotto: ritorno alla responsabilità per colpa?* In *Resp. civ. prev.,* 2007.

M. PALMIRANI, *Interpretabilità, conoscibilità, spiegabilità dei processi decisionali automatizzati*, in U. RUFFOLO (a cura di), *XXVI Lezioni di Diritto dell'intelligenza artificiale.*

F. PASQUALE, *New laws of Robotics, Defending Human expertise i*n the *Age of AI*, Cambridge-Londra, 2020.

N. PATKI, R. WEDGE, K. VEERAMACHANENI, *The Synthetic Data Vault* in *2016 IEEE International Conference on Data Science and Advanced Analytics (DSAA)*, 2016.

F.P. PATTI, *The European Road to Autonomous Vehicle*, in *43 Fordham International L. J.*, 2019,

V. PEIGNÈ, *Il fascicolo sanitario elettronico, verso una «trasparenza sanitaria» della persona* in Riv. It. Med. Leg., 2012.

V. PEIGNÈ, *Verso il fascicolo Sanitario Elettronico: presentazione della riforma francese* in *Dir. Internet*, 2007.

G. PELLICANÒ, *Sanità digitale, stato dell'arte e prospettive future* in *Smart eLab*, n. 14/2019; D. GRECO, *Sanità digitale dopo la pandemia: lo scenario*, 25 maggio 2021, in https://www.agendadigitale.eu/sanita/sanita-digitale-dopo-la-pandemia-lo-scenario/.

C. PERLINGIERI, *Responsabilità civile e robotica medica*, in *Tecnologie e diritto*, 2020.

P. PERLINGIERI, *Il diritto alla salute quale diritto della personalità*, in *La persona e i suoi diritti. Problemi del diritto civile*, a cura di P. PERLINGIERI, Napoli, 2005.

P. PERLINGIERI, *L'interpretazione della legge come sistematica ed assiologica: il brocardo in claris non fit interpretatio, il ruolo dell'art. 12 disp. Prel. Codice civile e la nuova scuola dell'esegesi*, in *Rass. Dir. Civ.* 1985.

P. PERLINGIERI, *La persona e i suoi diritti. Problemi del diritto civile,* Napoli, 2005.

P. PERLINGIERI, *La pubblica amministrazione e la tutela della privacy. Gestione e riservatezza dell'informazione nell'attività amministrativa*, in *Annali della Facoltà di Economia dell'Università degli Studi del Sannio*, 8/2003.

P. PERLINGIERI, *Note sul «potenziamento cognitivo»* in *Tecnologie e diritto*, 2021.

P. PERLINGIERI, *Relazione conclusiva, in* P. PERLINGIERI, S. GIOVA, I. PRISCO (a cura di), *Il trattamento algoritmico dei dati tra etica, diritto e economia.*

P. PERLINGIERI, S. GIOVA, I. PRISCO (a cura di), *Il trattamento algoritmico dei dati tra etica, diritto e economia*, Napoli, 2020,

P. PERLINGIERI, S. GIOVA, I. PRISCO (a cura di), *Rapporti civilistici e intelligenze artificiali: attività e responsabilità*, Napoli, 2020.

P. PICCOLO, *Accesso ai dati sensibili(ssimi) tra tutela della privacy e diritti "di pari rango" nelle cause di nullità matrimoniale* in *Dir. famiglia*, 3/2013.

A. PISANI TEDESCO, *Il nuovo quadro normativo europeo dei dispositivi medici*, in *Dir. Comm. Int.* 3/2022.

D. PITTELLA, *Dall'obbligazione senza prestazione alla responsabilità extracontrattuale del medico: rigetto locale o totale del contratto "qualificato"?* in *Contr. e impr.*, 2020.

M. PLUTINO, *"Immuni", Un'exposure notification app alla prova del bilanciamento tra tutela dei diritti e degli interessi pubblici*, in *Dirittifondamentali.it* - 2/2020, 28 maggio 2020.

N. POSTERARO, *La digitalizzazione della sanità in Italia: uno sguardo al Fascicolo Sanitario Elettronico (anche alla luce del Piano Nazionale di Ripresa e Resilienza)*, in *federalismi.it*, 26/2021.

V. PREVITI, *Siamo davvero i nostri dati? I meccanismi distorsivi premianti di social scoring in Cina, Olanda e Italia*, in *DPCE online*, 2/2024.

S. PRILLA, S. GROENENVELD, *Real-World Evidence to Support EU Regulatory Decision Making—Results from a Pilot of Regulatory Use Cases*, in *Clinical Pharmacology & Therapeutics, Vol. 116, Issue 5, Novembre 2024.*

G. PROIETTI, *Responsabilità civile, inadempimento e sistemi di intelligenza artificiale*, in www.giustiziacivile.com, 7 febbraio 2023.

P. QUINN, et al., *The data protection and medical device frameworks - obstacles to the deployment of mHealth across Europe?*, in *European Journal of Health Law*, 20.2.2013.

I. RAPISARDA, *La privacy sanitaria alla prova del mobile ecosystem. Il caso delle app mediche*, in *Le nuove leggi civili commentate*, 2023.

I. RAPISARDA, *Ricerca scientifica e circolazione dei dati personali. Verso il definitivo superamento del paradigma privatistico?* in *Eur. dir. priv*., 2021.

M. RATTI, *Riflessioni in materia di responsabilità civile e danno cagionato da dispositivo intelligente alla luce dell'attuale scenario normativo*, in *Contratto e impr.*, 2020.

A.B. REINER, R. ALMOG, Y. GORELIK, I. HOCHBERG, L. NASSAR, T. MASHIACH, M. KHAMAISI, Y. LURIE, Z.S. AZZAM, J. KHOURY, D. KURNIK, R. BEYAR, *Analyzing Medical Research Results Based on Synthetic Data and*

Their Relation to Real Data Results: Systematic Comparison from Five Observational Studies, in *JMIR medical informatics*, febbraio 2020.

A. RICCI, *Sulla «funzione sociale» del diritto alla protezione dei dati personali*, in *Contr. Impr*., 2017.

F. RINALDI, *Incompatibilità tra la nozione di consumatore e quella di professionista debole*, in *Nuova giur. Civ. comm*., 1/2002.

N. RIZZO, *Strutture della responsabilità civile e intelligenza artificiale: i problemi in medicina*, in M. FACCIOLI (a cura di), *Profili giuridici dell'utilizzo della robotica e dell'intelligenza artificiale in medicina*, Napoli, 2022.

S. RODOTÀ, *Elaboratori elettronici e controllo sociale*, Bologna, 1973.

V. G. ROMANO, *Diritto, robotica e teoria dei giochi: riflessioni su una sinergia*, in G. ALPA (a cura di), *Diritto e intelligenza artificiale*, Pisa, 2020.

U. RUFFOLO (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Torino, 2020.

U. RUFFOLO, *Art. 15 – Responsabilità secondo altre disposizioni di legge*, in G. ALPA, U. CARNEVALI, F. DI GIOVANNI, G. GHIDINI, U. RUFFOLO, C.M. VERARDI, *La responsabilità per danno da prodotti difettosi.*

U. RUFFOLO, E. AL MUREDEN, *Autonomous vehicles e responsabilità nel nostro sistema e in quello statunitense*, in *Giur. It*, 7/2019.

U. RUFFOLO, *Intelligenza artificiale, machine learning e responsabilità da algoritmo*, in *Giur. It.*, 2019.

U. RUFFOLO, *Le responsabilità da artificial intelligence, algoritmo e smartproduct: per i fondamenti di un diritto dell'intelligenza artificiale self-learning*, in U. RUFFOLO-G.ALPA-A.BARBERA (a cura di), *Intelligenza artificiale. Il diritto, i Diritti e l'etica, Milano*, 2020.

U. RUFFOLO, *Tecnologie emergenti ed intelligenza artificiale in sanità: rischi e responsabilità*, in U. RUFFOLO, M. SAVINI NICCI (a cura di), *Le nuove frontiere della responsabilità medica*, Milano, 2022.

L. RUFO, *Digitalizzazione e condivisione dei dati sanitari: uno spazio comune europeo dei dati*, in V. SALVATORE (a cura di) Digitalizzazione, intelligenza artificiale e tutela della salute nell'Unione europea.

L. RUFO, *Le ricerche scientifiche durante l'emergenza sanitaria (il Covid-19). Quale base giuridica per l'arruolamento dei pazienti?* In *BioLaw Journal – Rivista di Biodiritto*, 21 marzo 2020.

U. SALANITRO, *Intelligenza artificiale e responsabilità: la strategia della Commissione europea* in *Rivista di diritto civile*, 6/2020.

P. SAMMARCO, *Osservazioni sulla responsabilità da informazioni inesatte fornite da un chatbot*, in *Il diritto dell'informazione e dell'informatica*, 1/2024.

A. SANTOSUOSSO, C. BOSCARATO, F. CAROLEO, *Robot e diritto: una prima ricognizione* nella *Nuova giurisprudenza commentata*, 2/2012.

A. SANTOSUOSSO, *Intelligenza e diritto. Perché le nuove tecnologie sono una grande opportunità per il diritto*, Milano, 2020,

G. SARTOR*, Cognitive automata and the law: electronic contracting and the intentionality of software agents*, in Artif. Intell. Law, 17/2009,

G. SARTOR, *Gli agenti software e la disciplina giuridica degli strumenti cognitivi*, in *Dir.Inf. Informatica*, 2003.

G. SARTOR, *Gli agenti software: nuovi soggetti del ciberdiritto?*, in *Contratto e impresa*, 2002.

G. SARTOR, *Intelligenza artificiale e diritto. Un'introduzione*, Giuffrè, 1996.

G. SARTOR, *L'intenzionalità dei sistemi informatici e il diritto*, in *Riv. Trim. dir. e proc. civ.*, 23/2003.

C. SARTORETTI, *La cartella clinica tra diritto all'informazione e diritto alla privacy,* in R. FERRARA (a cura di), *Trattato di biodiritto*, diretto da S. RODOTÀ, P. ZATTI, Milano, 2010.

M. SAVINI NICCI, G. VETRUGNO, *Intelligenza artificiale e responsabilità nel settore sanitario* in U. RUFFOLO (a cura di), *Intelligenza artificiale – Il diritto, i diritti, l'etica*.

M. SAVINI NICCI, G. VETRUGNO, *Machine learning, dispositivi "intelligenti" e robotica: la responsabilità civile di strutture e professionisti sanitari* di U. RUFFOLO e M. GABBRIELLI (a cura di), in *Intelligenza Artificiale, dispostivi medici e diritto: Un dialogo fra saperi: giuristi, medici e informatici a confronto.*

M. SCIALDONE, *Il diritto dei robot: la regolamentazione giuridica dei comportamenti non umani*, in E. PIETRAFESA, F. MARZANO, T. MEDICI (a cura di), *La rete e il fattore C: Cultura, Complessità, Collaborazione*, Volume II, Roma, Stati Generali dell'Innovazione, 2016.

R. SCOTTI, *La responsabilità civile dei danni cagionati da sistemi di intelligenza artificiale in ambito sanitario* in *Giustizia civile*, 1/2024.

P. SERRAO D'AQUINO, *La responsabilità civile per l'uso di sistemi di intelligenza artificiale nella Risoluzione del Parlamento Europeo del 20 ottobre 2020 "Raccomandazioni alla Commissione sul regime della responsabilità civile e intelligenza artificiale".*

E. SETO, P. CHALLA, P. WARE, *Adoption of Covid-19 contact tracing apps: A balance between privacy and effectiveness*, in *Jou. of med. Inter. Res*., v.23, 3/2021.

E. SEVERINO, N. IRTI, *Dialogo su diritto e tecnica*, Roma-Bari, 2001.

V. SICA, S. SELVAGGI, *Telemedicina. Approccio multidisciplinare alla gestione dei dati sanitari*, Milano, 2010.

E. SORRENTINO e A.F. SPAGNUOLO, *La sanità digitale in emergenza Covid-19. Uno sguardo al fascicolo sanitario elettronico*, in *federalismi.it - Osservatorio di diritto sanitario*, n. 30/2020.

A. SPINA, *A regulatory Mariage de Figaro: Risk Regulation, Data Protection and Data Ethics* in *European Journal of Risk Regulation*, vol.8/2017.

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,* Giappichelli.

G. STELLA RICHTER, *Contributo allo studio dei rapporti di fatto nel diritto privato*, in *Riv. Trim. dir. proc. civ.*, 151/1977.

M. TAMPIERI, *L'intelligenza artificiale e le sue evoluzioni. Prospettive civilistiche*, Padova, 2022.

M. TESCARO, *L'art. 2236 cod. civ. e l'auspicabile contenimento della responsabilità civile del prestatore d'opera*, in *Studium iuris*, 2021.

S. TESTA, O. MAYORA-IBARRA, E.M. PIRAS et al., *Implementation of televisit healthcare services triggered by the COVID-19 emergency: the Trentino Province experience*, in *Z Gesundh Wiss*., 2021.

G. TEUBNER, *I soggetti giuridici digitali? Sullo status privatistico degli agenti software autonomi*, Napoli, 2019.

A. THIENE, *Art. 9 Trattamento di categorie particolari di dati*, in R. D'ORAZIO, G. FINOCCHIARO, O. POLLICINO, G. RESTA (a cura di), *Codice della privacy e data protection*, Giuffrè, Milano, 2021.

A. THIENE, *Salute, riserbo e rimedio risarcitorio* in *Rivista italiana di medicina legale e del diritto in campo sanitario*, 4/2015.

M. TIMO, *Algoritmo – il procedimento di assunzione del personale al vaglio del Consiglio di Stato*, in *Giur. It*., 5/2020, 1190 (nota a sentenza).
N. TODESCHINI (a cura di), *La responsabilità in medicina. Dalla discussione del caso pratico alla regola. Una guida operativa completa alla riforma Gelli Bianco; la colpa civile e penale, il consenso informato, i procedimenti e i profili assicurativi*, Milano, 2023.
N. TODESCHINI, *L'art. 7 della legge Gelli Bianco, il doppio binario che non c'è*, in P. CENDON (diretto da), *La responsabilità medica: guida operativa alla riforma Gelli Bianco. Inquadramento, profili civili e penali, assicurazione, procedimento stragiudiziale e giudiziale, casistica.* Milano, 2019.
M. TOMASI, *Diritto, scienza, nuove tecnologie*, Padova, 2021.
M. TOMASI, *Genetica e Costituzione. Esercizi di eguaglianza, solidarietà e responsabilità*, Forthcoming.
E. TOPOL, *Deep Medicine: how artificial intelligence can make healthcare human again*, New York, 2019.
M. TRESCA, *Lo «Stato digitale». Big data, open data e algoritmi: i dati al servizio della pubblica amministrazione*, in Riv. trim. dir. pubbl., 2021.
P. TRIMARCHI, *La responsabilità civile: atto illecito, rischio, danno*, Milano, 2019.
P. TRIMARCHI, *La responsabilità del fabbricante nella direttiva comunitaria*, in Riv. soc, 1986.
C.A. TROVATO, C. RAUCCIO, *L'anonimizzazione è morta? Un'analisi dei dati sintetici come proposta per superare la dicotomia dato personale-dato non personale*, in *Ciberspazio e Diritto*, n. 2/2022.
D. TUZZOLINO, *La portabilità dei dati sanitari* in A. THIENE e S. CORSO (a cura di), *La protezione dei dati sanitari, privacy e innovazione tecnologica*

tra salute pubblica e diritto alla riservatezza – Atti del convegno, Rovigo 4 novembre 2022.

G. UBERTIS, *Intelligenza artificiale, giustizia penale, controllo umano significativo*, in AA. VV., *Giurisdizione Penale, intelligenza artificiale ed etica del giudizio*, Milano, 2021.

L. ULISSI, *I profili di responsabilità della macchina dell'apprendimento nell'interazione con l'utente*, in G. ALPA (a cura di), *Diritto e intelligenza artificiale*.

A. URBANI, *Innovazione, ricerca e digitalizzazione del SSN*, in *Monitor 45*, 2021.

F. VENOSTA, *"Contatto sociale" e affidamento*, Milano, 2021.

G. VERGOTTINI, C. BOTTARI, *La sanità elettronica*, Bologna, 2018.

G. VICARELLI – M. BRONZINI, *La sanità digitale: dimensioni di analisi e prospettive di ricerca* in *Politiche sociali*, 2/2018.

A. VIGORITO, *Sul crinale tra data altruism e social scoring: esperienze applicative della sequenza dati-algoritmi nel nuovo contesto regolatorio europeo*, in *medialaws*.

F. VOGT, B. HAIRE, L. SELVEY, A.L. KATELARIS, & J. KALDOR, *Effectiveness evaluation of digital contact tracing for Covid-19 in New South Wales, Australia,* in *the Lanc. Pub. Hea*., v. 7, 3/2022.

G. VOTANO, *Intelligenza artificiale in ambito sanitario: il problema della responsabilità civile*, in *Danno e resp.*, 2022

G. WAGNER, *Robot liability*, in S. LOHSSE, R. SCHULZE, D. STAUDENMAYER (a cura di), *Liability for Artificial Intelligence and the Internet of Things*, Baden-Baden, 2019.

S. A. WALDMAN, A. TERZIC, *Big Data Transforms Discovery-Utilization Therapeutics Continuum* in *Clinical Pharmacology and Therapeutics*, vol. 99 del 2016.

S. WHITELAW, M.A. MAMAS, E. TOPOL, & H.G. VAN SPALL, *Applications of digital technology in Covid-19 pandemic planning and response*, in *The Lan. Dig. Hea*, v. 2, 8/2022.

J.M. WYNDHAM, M. W. VITULLO, *Define the human right to science*, in *Science*, 30 novembre 2018.

L. XU, K. VEERAMACHANENI, *Synthesizing Tabular Data using Generative Adversarial Networks*, 2018.

G. ZACCARIA, *Normatività giuridica e normatività algoritmica* in Aa. Vv. *Liber Amicorum per Paolo Zatti*, Napoli 2023.

F. ZANOVELLO, *Misure di garanzia e rischio di data breach in ambito sanitario* in A. THIENE, S. CORSO (a cura di), *La protezione dei dati sanitari, privacy e innovazione tecnologica tra salute pubblica e diritto alla riservatezza* – Atti del convegno, Rovigo 4 novembre 2022.

P. ZATTI, *Il diritto all'identità e «l'applicazione diretta» dell'articolo 2 della Costituzione* in G. ALPA, M. BESSONE e L. BONESCHI (a cura di), *Il diritto all'identità personale,* Padova, 1981.

V. ZENO-ZENCOVICH, *Informazione (profili civilistici)*, in *Dig. Civ.*, IX, Torino, 1993.

A. ZUCCHETTI, *Dati (trattamento dei)* in V. ITALIA (a cura di), *Enciclopedia degli enti locali, Atti, Procedimenti, Documentazione*, Giuffrè, Milano, 2007.

P. ZUDDAS, *Intelligenza artificiale e discriminazioni*, in A.a. V.v., *Liber amicorum per Pasquale Costanzo – Diritto costituzionale in trasformazione, I, Costituzionalismo, Reti e intelligenza artificiale*, *Consulta OnLine*, 2020.

I. ZURITA MARTÍN, *La responsabilidad civil por los daños causados por los robots inteligentes como productos defectuosos*, Reus, Madrid, 2020.

Giurisprudenza citata

Cass. pen. sez. V, 25/10/2012, n.8351.

Cass. pen., sez. Un., 10 luglio 2002 n. 30328.

Cass. pen., sez. IV, 6 marzo 2012 n. 17758.

Cass. pen., sez. V, 18 dicembre 2008 n. 4941.

Cass. pen., sez. IV, 2 ottobre 2008 n. 40924.

Cass. pen., sez. IV, 21 giugno 2007 n. 39594.

Cass. civ. sez. I, 29/05/2015, n.11223.

Cass. civ., sez. I, Ordinanza, 28/03/2022, n. 9919.

Cass. S.U. n. 7958 del 11.07.1992.

Cass. pen. sez. V, n. 37314 del 29.05.2013.

Corte EDU 17 luglio 2008, n. 20511/03, I. c. Finlandia, in www.hudoc.echr.coe.int.

Consiglio di Stato, sentenza n. 7891/2021.

Sentenza della Corte di Giustizia dell'Unione europea, casi riuniti C-293/12 e C- 594/12 Digital Rights Ireland, paragrafo 27.
Corte Gust. UE, 15 gennaio 2009, C-140/07 Hecht-Pharma.
Corte Giust. UE, 30 aprile 2009, C-27/08 Bios Naturproductke.
Corte Giust. UE, 22 novembre 2012, C-219/11, Brain Products.
Cass. civ., sez. III, 7 aprile 2022, n. 11317.
Cass. civ., sez. III, 15 marzo 2007, n. 6007.
Cass. civ., sez. III, 29 maggio 2013, n. 13458.
Cass.civ., sez. III, 6 agosto 2013, n. 18654.
Corte Giust. UE, 25 aprile 2002, C-154/00, Commissione c. Repubblica ellenica.
Corte Giust. UE, 2002, C-52/00, Commissione c. Repubblica francese.
Corte Giust. UE, 2002, C-183/00, Medicina Asturiana.
Tribunale di Sassari, 12 luglio 2012.
Cass. civ., sez. III, 13 aprile 2007, n. 8826.
Cass. civ., sez. III, 8 ottobre 2008, n. 2479.
Cass. civ., sez. III, 27 agosto 2014 n. 18304.
Cass. civ., sez. IV, 15 giugno 2021, n. 16936.
Cass. civ., sez. III, 8 giugno 2023, n. 16272.
Cass. sez. un. n. 577 dell'11 gennaio 2008.
Cass. civ., sez. III, 15 ottobre 2004, n 20334.
Cass. civ, sez. III, 10 febbraio 2003, n. 1954.
Cass. civ., sez. III, 30 ottobre 2002, n. 8148.
Cass. civ., sez. III, 28 febbraio 2000, n. 2220.
Cass. civ., sez. III, 29 luglio 2015, n. 16052.
Cass. civ., sez. III, n. 19180 del 19 luglio 2018.

Cass. sez. un., 28 novembre 1995 n. 12300.

Cass. civ., sez. III, 18 febbraio 2000, n. 1859.

Cass. civ. sez. III, 12 luglio 2006, n. 15779.

Cass. civ., sez. III, 29 luglio 2016, n. 15761.

Cass. civ., sez. III, 1 febbraio 2018, n. 2478.

Cass. civ., sez. III, 23 maggio 2019, n. 13966.

Cass, civ., sez. V, 27 maggio 2022, n. 17252.

Civil Resolution Tribunal of British Columbia, 14 febbraio 2024.

Cass. Civ. sez. I, 27 ottobre 2017, n. 25644.

Cass. Civ. sez. I, 12 luglio 2016, n. 14188.