Diritto moderno
e interpretazione classica

Claudio Sarra, Anna Zilio,
Giulia De Bona

Diritto alla salute, protezione dei dati personali e intelligenza artificiale

Filosofia del Diritto

FrancoAngeli
OPEN ACCESS

Diritto moderno
e interpretazione classica

 Isbn: 9788835178699

Diritto moderno e interpretazione classica

Direttore: Francesco Cavalla

Condirettori: Stefano Fuselli, Paolo Moro

Il progetto editoriale, significativamente denominato "Diritto moderno e interpretazione classica", muove dalla convinzione fondamentale secondo la quale ancor oggi – quando l'esperienza giuridica presenta una moltiplicazione, spesso confusa, di norme, dottrine, posizioni – non sia possibile svolgere una critica autentica all'attività del legislatore e dell'interprete senza ricorrere a quei principi risalenti che hanno costituito la formazione del diritto in Occidente. Sono i principi che concernono la coerenza o la contraddittorietà tra i detti, la ragione deduttiva e dialettica, i limiti della conoscenza e del potere; sono i principi che diciamo classici non già, e non tanto, perché prodotti in una determinata epoca, quanto perché capaci di rivelare la loro attuale efficacia in ogni momento storico e segnatamente in quello presente. Continuando dunque un sapere antico, i testi del "progetto" tenteranno di distinguere "il troppo e il vano" di fronte a nuove tesi e nuovi problemi.
In particolare, in alcuni saggi appartenenti alla serie *Principî di filosofia forense*, si cercherà di dare una versione organica, corredata di opportuni riferimenti culturali, della filosofia che gli attori del processo producono implicitamente nello sforzo di addivenire, attraverso il contraddittorio, a una conclusione vera per tutti.

Claudio Sarra, Anna Zilio,
Giulia De Bona

DIRITTO ALLA SALUTE, PROTEZIONE DEI DATI PERSONALI E INTELLIGENZA ARTIFICIALE

FrancoAngeli
OPEN ACCESS

 Isbn: 9788835178699

La pubblicazione di questo volume è stata possibile grazie al contributo dell'Università degli Studi di Padova – Dipartimento di Diritto Privato e Critica del Diritto, con Progetto finanziato dall'Unione Europea - Next Generation EU – Piano Nazionale Resistenza e Resilienza (PNRR) - Missione 4 Componente 2 Investimento 1.3 – Avviso N. 341 del 15/03/2022 del Ministero dell'Università e della Ricerca - Award number: PE0000013, decreto di concessione del finanziamento n. 0092328 del 28/03/2024, CUP J33C22002830006, "Beyond compliance: AI Act made usable in healthcare" (acronimo: UseAI).

Isbn e-book Open Access: 9788835178699

Copyright © 2025 by FrancoAngeli s.r.l., Milano, Italy. Isbn: 9788835178699

Indice

Premessa

di *Claudio Sarra*

Questo lavoro si inserisce in un più ampio progetto di ricerca finanziato sui fondi del c.d. PNRR e che ha avuto come titolo "UseAI. Beyond compliance: AI Act made usable in healthcare".

Tale progetto ha visto la partecipazione di tre nuclei di ricerca principali, uno giuridico, ad opera degli Autori di questo lavoro, uno tecnico e uno psicologico – rispettivamente a cura del prof. Nicolò Navarin e della prof.ssa Anna Spagnolli dell'Università di Padova – con lo scopo di elaborare delle modalità informazione degli "stakeholders" principali, impegnati a vario titolo in ambito sanitario, per un utilizzo consapevole e socialmente adeguato dell'intelligenza artificiale in un settore così delicato.

La collaborazione tra studiosi di discipline molto diverse tra loro è apparsa necessaria data l'inevitabile interdisciplinarietà che caratterizza oramai qualsiasi problematica dovuta all'intervento di innovazioni tecnologiche potenzialmente rivoluzionarie. In effetti, appare oggi ineludibile stabilizzare tavoli di confronto tra i diversi saperi in ogni luogo ove la tecnologia si ponga come strategica per il miglioramento dell'organizzazione ma che preveda anche un impatto potenzialmente significativo sui diritti e le libertà delle persone. Tali relazioni sono spesso rese problematiche dalla settorializzazione dei saperi, che, se, da un lato, costituisce l'inevitabile conseguenza della specializzazione, dall'altro, rischia di compromettere sia le condizioni per un dialogo costruttivo che, in prospettiva, la formazione delle giovani generazioni. Queste ultime, invece, devono essere preparate a sfide che non sono più affrontabili partendo da chiusure concettuali aprioristiche.

Sul punto si registrano negli ultimi anni numerose iniziative a livello universitario di "ibridazione dei saperi" con l'istituzione di veri e propri curricula universitari nei quali i giovani vengono esposti programmaticamente a discipline un tempo ritenute distanti e non comunicanti. Un esempio si può

trovare nell'avvio del Corso di Laurea triennale in "Diritto e Tecnologia" presso la Scuola di Giurisprudenza dell'Università di Padova nell'a.a. 2020-2021. Si è trattato di un progetto didattico innovativo e pionieristico giacché costruito con la partecipazione di docenti provenienti dai dipartimenti giuridici ma anche scientifici ed economici, quali i dipartimenti di matematica, di ingegneria e di economia.

Lo studente che si presti a seguire un tale corso di studi viene così a contatto con i diversi linguaggi, le diverse metodologie didattiche, le diverse ricostruzioni delle varie problematiche nonché le diverse forme conseguenti di verifica. Si tratta di una sfida per la formazione alla quale tutti, studenti e docenti, sono chiamati a partecipare per offrire quelle competenze realmente trasversali che sempre più sono richieste nel mondo contemporaneo.

Tornando al progetto, il presente lavoro vuole offrire un'esposizione delle principali – non certo tutte – questioni giuridiche che devono essere tenute presenti quando si voglia elaborare una strategia di informazione degli stakeholders nel settore sanitario allorché si introduca il tema di un utilizzo sistematico dell'intelligenza artificiale, concentrandosi, in particolare su quelli che sono al momento i due atti normativi più importanti, per ampiezza di impatto e centralità di contenuto, vale a dire il Regolamento Europeo sulla protezione dei dati personali e il recente Regolamento sull'intelligenza artificiale.

La ricostruzione delle tematiche correlate alla sanità presenti in tali fondamentali atti, viene collocata, di necessità, in un contesto più ampio ove sono richiamati ulteriori atti regolativi rilevanti ed in particolare – nella prima parte – il Regolamento sullo spazio europeo dei dati sanitari, approvato in via definitiva lo scorso 21 gennaio e, a sua volta, destinato ad interagire nella prassi con gli altri atti e regolamenti che costituiscono il "diritto europeo dei dati" in un modo che, al momento, non è del tutto prevedibile. Va ricordato che – come è stato per il GDPR – anche i due regolamenti appena citati prevedono un differimento della loro applicabilità che sarà scaglionata nel tempo e caratterizzata dall'istituzione di una complessa governance multilivello, sicché il quadro completo di molte questioni cruciali per la pratica lo si avrà soltanto in futuro.

Va qui segnalato – quale *vox clamantis in deserto* – che, nonostante le apparenze e le presupposizioni di molti, specialmente tra i non giuristi, l'affluvio normativo, quando risulta alluvionale, se può essere sbandierato come un risultato politico da portare al proprio elettorato di riferimento, non costituisce mai una garanzia di maggior certezza del diritto, ma, al contrario, spesso ne aggrava l'incertezza. Ed invero, in un settore in grande trasfor-

mazione, l'obsolescenza di alcuni atti anche molto recenti, unitamente alla complessità dei (molti) nuovi che dovrebbero coordinarvisi fanno presagire l'avvento di un contenzioso che non sarà facile per nessuno sciogliere. A tale ovvia considerazione deve aggiungersi che la crescita della formazione dei professionisti più giovani nel settore IT, grazie anche ai nuovi progetti formativi cui si è accennato, determinerà una maggiore consapevolezza delle questioni critiche che, dunque, si accompagnerà ad un "coraggio" maggiore nel far valere i diritti relativi anche nelle sedi giudiziali.

E, a questo proposito, mi permetto di invitare gli amici avvocati che lavorano giudizialmente a non esitare nel portare a giudizio le molte questioni che derivano dall'utilizzo ormai diuturno ed ubiquo della tecnologia, giacché, in tempi tanto rivoluzionari, quanto più essa viene messa in discussione, tanto più saremo sicuri che i nostri diritti e le nostre libertà sono prese in carico seriamente e con radicalità.

Come insegna la prospettiva processuale del diritto – autorevole Scuola filosofica di specifica tradizione patavina – è nel processo che si gioca il senso della libertà che il diritto deve presidiare.

Quanto al testo, esso è suddiviso in tre parti principali ad opera dello scrivente, dell'avv. Anna Zilio e della dott.ssa Giulia De Bona che hanno collaborato al progetto: nella prima parte è offerto uno sguardo di insieme sul tema del diritto alla salute nel contesto di una trasformazione tecnologica che, si vedrà, si annuncia coinvolgere financo il *design* delle stesse infrastrutture di comunicazione. Qui si presenteranno inoltre, le linee essenziali del Regolamento sullo spazio europeo dei dati sanitari e una panoramica sulle questioni etiche presenti nella letteratura in quanto rilevanti per il settore sanitario. Le altre parti sono dedicate al GDPR e all'*AI Act* con un focus specifico sulla applicazione sanitaria e con riferimento ad alcuni stakeholders giudicati rilevanti per il prosieguo del progetto.

Nella speranza che il lavoro qui presentato sia di ausilio a quanti lavorino o pensino di lavorare nel settore sanitario, in qualsiasi posizione, per affrontare le sfide del futuro prossimo, esprimo qui il mio più sentito ringraziamento alle due coautrici e ai Colleghi impegnati con me in questo progetto.

Febbraio 2025

I. Il diritto alla salute nell'era della datificazione

di *Claudio Sarra*

1. Introduzione

Il 22 luglio 1946, al termine della Conferenza Internazionale sulla Salute tenutasi a New York, veniva adottato il documento istitutivo dell'Organizzazione Mondiale della Sanità, cui l'Italia ha aderito ufficialmente l'11 aprile 1947.

Con l'ottenimento del numero di adesioni previsto dall'art. 80 di tale documento, e con la sua conseguente entrata in vigore il 7 aprile 1948, l'Organizzazione – il cui scopo è "il raggiungimento da parte di tutti i popoli del più alto livello possibile di salute" (art. 1) – era ufficialmente costituita.

Si crea così la base istituzionale per una convergenza operativa interculturale in uno degli ambiti più complessi e sensibili della vita umana, nel quale fattori naturali, culturali, economici e sociali si intersecano così profondamente da incidere sulla qualità della vita e financo sulla stessa esistenza degli individui e dei popoli. In quel documento fondativo, la salute viene definita come uno "stato di completo benessere fisico, mentale e sociale non limitato alla mera assenza di malattia o di infermità"[1], e il godimento del più

1. Cfr. Preambolo alla *Costituzione dell'Organizzazione mondiale della sanità.*

alto livello possibile di tale condizione è dichiarato un diritto fondamentale dell'essere umano in quanto tale. Lo sviluppo della salute di tutti i popoli è ritenuto un fattore decisivo per garantire la pace e la sicurezza; esso richiede la collaborazione tra individui e tra gli Stati, la condivisione delle conoscenze mediche e psicologiche allo stato disponibili, la partecipazione pubblica in condizione di corretta informazione e impone che i Governi siano responsabili per la salute dei loro popoli[2].

L'apertura del diritto alla salute, così definito, oltre i limiti dell'assenza di malattia e fino al raggiungimento del più alto stato di benessere possibile, se spiega la complessità degli apparati dedicati alla sua resa effettiva, comporta anche la possibilità di giustificare, in nome della richiesta collettiva di salute, sempre nuovi interventi nonché di ampliare i settori di riferimento e le strutture necessarie. Tutto ciò, naturalmente, porta inevitabilmente all'aumento della richiesta economica e, potenzialmente, di adempimenti rivolti ai singoli in nome dell'interesse generale a veder garantito un certo standard di salute pubblica e di efficienza del sistema sanitario, rendendo così delicatissime le dinamiche tra la libertà individuale e l'interesse collettivo.

Entrambi aspetti, questi, presenti nella configurazione giuridica del fenomeno nel quadro ordinamentale interno fin dal livello costituzionale, dove l'art. 32 Cost., come è noto, dichiara la salute al contempo "fondamentale diritto dell'individuo e interesse della collettività", con ciò introducendo la novità rispetto al passato di un impegno diretto del potere pubblico alla tutela e alla promozione del diritto individuale alla salute e non solo a farsi carico degli aspetti relativi alla igiene e sanità collettiva[3].

La formula costituzionale è ripetuta, poi, all'art. 1 della legge 23 dicembre 1978, n. 833, istitutiva del Servizio Sanitario Nazionale mediante il quale, secondo il comma primo, la Repubblica persegue concretamente la tutela della salute. Esso è costituito "dal complesso delle funzioni, delle strutture, dei servizi e delle attività destinati alla promozione, al mantenimento ed al recupero della salute fisica e psichica di tutta la popolazione senza distinzione di condizioni individuali o sociali e secondo modalità che assicurino l'eguaglianza dei cittadini nei confronti del servizio" (art. 1, comma 3, L. 833/1978).

---

2. *Ibidem.*

3. Sull'attenzione esclusiva agli aspetti collettivi nell'impostazione liberale ottocentesca, cfr. Giglioni F., *Manuale di diritto sanitario,* Neldiritto Editore, Ba, 2024, Cap. 1; per una storia approfondita della salute in Italia dal 1943 ad oggi, cfr. Luzzi S., *Salute e sanità nell'Italia repubblicana,* Donzelli, Roma, 2004.

Il diritto alla salute, dichiarato "fondamentale", si correla intimamente con il principio personalistico che informa l'ordinamento costituzionale italiano e la sua tutela effettiva costituisce una condizione essenziale per il riconoscimento in atto della stessa dignità della persona.

La salute, infatti, condiziona essenzialmente l'effettiva libertà personale del soggetto e la possibilità di sviluppare pienamente la propria personalità, esigenze, queste, che implicano il dovere della Repubblica di intervenire per rimuovere gli ostacoli che ne impediscano la realizzazione (art. 3 Cost., II comma).

D'altro lato, proprio il rispetto della persona umana esige di limitare la pretesa pubblica sul soggetto, anche di fronte alla necessità eccezionale di imposizione, per legge, di trattamenti sanitari obbligatori (art. 32, II. comma)[4].

Naturalmente, data la ricordata potenziale estensione del concetto di salute, non tutte le possibili richieste di prestazioni sanitarie rientrano nel c.d. "nucleo irriducibile del diritto alla salute protetto dalla Costituzione come ambito inviolabile della dignità umana" (Corte cost., 509/2000), sicché, fuori da questo ristretto ambito, l'effettiva esigibilità di prestazioni sanitarie nei confronti della Repubblica dipende dal bilanciamento con ulteriori valori, ivi incluso quello della sostenibilità economica per le finanze pubbliche. In un contesto caratterizzato da queste direttrici fondamentali, l'evoluzione tecnologica gioca un ruolo essenziale in tutte le direzioni.

Essa, da un lato, si è mostrata cruciale per garantire l'effettiva offerta delle migliori prestazioni allo stato delle conoscenze, sia nel senso della più accurata scelta ed applicazione terapeutica, sia in quello di un'adeguata organizzazione delle strutture e di un accesso alle prestazioni che sia efficiente ed effettivamente, il più possibile, equo.

Dall'altro, richiede anche costanti e ingenti investimenti nell'aggiornamento delle disponibilità materiali e delle competenze del personale chiamato ad utilizzarle, venendo così a dipendere dalle più generali politiche economiche messe in atto dallo Stato e dagli altri enti pubblici coinvolti (relativamente alla sanità pubblica). Impegni finanziari, questi, che si aggiungono a quelli relativi all'organizzazione delle strutture e del personale per la fornitura concreta delle prestazioni sanitarie.

Inoltre, posta la correlazione diretta ed ineliminabile tra massimazione dell'efficienza tecnica ed invasività nella sfera dei diritti e delle libertà

4. Cfr, Morana D., *La salute come diritto costituzionale,* Giappichelli, Torino, 2022. Per una rassegna sulla giurisprudenza costituzionale in tema di diritto alla salute sebbene ormai un po' datato, cfr. Minni F., Morrone A., *Il diritto alla salute nella giurisprudenza della Corte costituzionale italiana,* in *AIC,* 2013, 3, pp. 1-12.

dell'individuo[5], unita all'aumento della complessa interazione dei sistemi tecnologici contemporanei, in un settore, quello sanitario, che già di per sé coinvolge le persone nelle loro sfere più intime, ne consegue che il rispetto della libertà, dell'autonomia e dei diritti fondamentali dei soggetti interessati, in particolare quanto alla loro c.d. *privacy informazionale*[6]*,* diventano di giorno in giorno sempre più problematici.

Infine, come ha mostrato l'esperienza storica e socio-culturale che ha portato alla nascita della *bioetica,* non va sottovalutato l'impatto che l'evoluzione tecnologica ha sulla autocoscienza dell'uomo contemporaneo, sulla comprensione ed accettazione dei limiti della propria natura e sugli stessi concetti essenziali ("vita", "morte") su cui costruisce la comprensione di sé e del mondo che lo riguarda. Queste trasformazioni socio-culturali sono idonee a modificare la soglia di accettabilità sociale delle pratiche applicate a tutela della salute, determinando, ad esempio, un aumento della richiesta di accesso alle prestazioni e di un rapporto continuativo, in particolare con l'avanzare dell'età, con le strutture sanitarie.

All'interno di questo quadro in evoluzione, i recenti sviluppi delle applicazioni basate sui dati che si riconducono al concetto generale di "intelligenza artificiale" sono destinate ad incidere profondamente, promettendo delle rivoluzioni nel modo di pensare e vivere la tutela della salute.

Sul piano giuridico, le sfide si annunciano di grande complessità.

Innanzi tutto, ogni innovazione tecnologica di rilievo pone problematiche regolatorie sin dal suo stesso proporsi: come mostrato dal c.d. "dilemma di Collingridge"[7], la stessa scelta di intervenire o no nella regolazione di un processo di sviluppo in corso può avere effetti indesiderati su di esso, limitandolo fino a farvi perdere incisività (e, di conseguenza, determinando una perdita di competitività nel settore rispetto ad aree dove sono state prese scelte differenti). Oppure, può rafforzarlo venendo ad offrire chiarezza normativa circa le possibili conseguenze dei comportamenti che lo realizzano. Tuttavia, la scelta tra queste due opzioni generalissime avviene senza la possibilità di sapere *ex ante* quale delle due sia preferibile nel contesto di riferimento.

Da questo punto di vista, il momento attuale, quanto allo spazio giuridico europeo, è caratterizzato da uno sviluppo normativo importante ma ancora

5. Ciò che non è né contingente né eliminabile, cfr. Sarra C., *Il mondo-dato,* CLEUP, II ed., Padova, 2022; Sarra C., *La dignità della persona nell'era della datificazione e dell'intelligenza artificiale,* KRONT, Roma, 2025.

6. Per *privacy informazionale* si intende l'effettiva facoltà del soggetto di controllare il patrimonio di dati-informazioni che lo riguardano.

7. Collingridge D., *The Social Control of Technology,* Frances Printer, London, 1980, Ch. 1.

non del tutto compiuto, e dall'incertezza tipica che ogni sistema normativo nuovo e complesso porta con sé nel momento in cui è chiamato ad interagire con settori innovativi con riferimento ai quali non sono consolidate linee interpretative idonee a garantire alla pratica sviluppi ordinati e senza sorprese.

Alcuni di questi atti, quali il Regolamento Europeo per la protezione dei dati personali, il nuovo Regolamento sull'intelligenza artificiale e quello, di recentissima approvazione, sulla creazione dello spazio europeo per i dati sanitari, saranno qui esaminati con *focus* sull'utilizzo dell'IA nel settore sanitario e in un'ottica di ausilio alle esigenze informative della prassi.

2. La sanità come settore iper-complesso

In un ordinamento nel quale la tutela della salute è intesa come un compito fondamentale delle istituzioni pubbliche, i cittadini fanno esperienza della complessità del sistema deputato a realizzarla molto presto nella loro esistenza. Dalla nascita, alle prime cure da parte del pediatra di famiglia, alle vaccinazioni, ai primi malanni e così via sino alla fine della vita, l'esistenza di ciascuno è costellata di interventi da parte di questo insieme di apparati, strutture e soggetti di varia qualifica ai quali ci si affida per le proprie esigenze di salute, offrendo al contempo l'accesso agli aspetti più intimi di sé.

L'evoluzione tecnologica contemporanea traduce e gestisce l'universo di queste relazioni nella forma dei "dati", e "data-driven" si dice, oggi, la società che, disponendo di immense e sempre crescenti quantità di dati, da esse trae elementi di conoscenza (nella forma di rappresentazioni di correlazioni statistiche e di previsioni basate su di esse) idonee a supportare i processi decisori che si rendano necessari.

La miniaturizzazione, la riduzione dei costi, la diffusione capillare di dispositivi capaci di "captare" aspetti della persona, elaborarne i dati e trasferirli assieme a quelli prodotti da altri, indossati (*smart watch*, cellulari, occhiali a realtà aumentata ecc.) o presenti nel contesto (videocamere di sorveglianza, sensori e rilevatori di elementi ambientali, *smart objects* ecc.), determinano la società "datificata" su cui molto si è discusso e si discute, in particolare, negli ultimi vent'anni.

Ora, se da un lato la disponibilità di grandi quantità di dati costituisce un bene preziosissimo per potervi estrarre informazioni e forme di conoscenza fondamentali per prendere decisioni, una tale diffusione di dispositivi comporta la continua produzione di quantità tali da generare non banali problemi relativi alle infrastrutture di supporto di tutte queste operazioni. Si tratta di

quella parte *hard,* fatta di cavi, tralicci, *servers*, *data center*, e molto altro che spesso non è immediatamente presente alla coscienza dell'utente medio, il quale, anzi, vive l'esperienza di un continuo alleggerimento delle sue dotazioni tecnologiche particolari accompagnato dalla diffusione di "metafore" (ad es. *cloud*) che ne nascondono ancor di più la presenza e la rilevanza.

Eppure, l'efficienza promessa dalla specifica temperie tecnologica del nostro tempo, dipende totalmente da quella di queste infrastrutture fondamentali, i cui problemi si traducono immediatamente in impossibilità di compiere adempimenti anche cruciali, tanto dipendiamo da esse.

Così, l'ammasso continuo di produzione da miliardi di puntiformi centrali di dati, se deve essere usato per prendere decisioni vitali, richiede immediatezza nelle trasmissioni e una crescente potenza di elaborazione a tutti i livelli, giacché la debolezza di un anello della catena (una trasmissione inefficiente – *bottleneck* – in un luogo geografico, ad esempio), si può tradurre in un'inefficienza dell'intero sistema, generando conseguenze gravi o addirittura catastrofiche a seconda dell'essenzialità del settore dove le decisioni devono essere prese.

Si capisce, quindi, la necessità di studiare modelli di interconnessione tra i dispositivi che distribuiscano la produzione e l'elaborazione dei dati tra di essi e su diversi livelli a seconda delle necessità e al fine di garantire efficienza e tempestività dell'accesso alle informazioni e alle eleborazione essenziali al processo decisorio.

Quanto detto trova immediata concretizzazione proprio con riferimento all'evoluzione delle tecnologie applicate alla salute.

Ed invero, la datificazione della persona consente la rilevazione di informazioni utili alla presa in carico e cura della stessa in modalità molto più ampie rispetto al passato.

Così, l'avvento di dispositivi indossabili, applicabili senza eccessiva invasività sul paziente, o addirittura ingeribili[8], in grado di rilevare con continuità aspetti della sua situazione sanitaria (come la frequenza cardiaca, la pressione arteriosa, il livello glicemico, ecc.), se da un lato, rende possibile una sorta di medicina ubiquitaria, presente e partecipe ovunque si trovi il paziente, dall'altro implica potenzialmente la connessione di miliardi di dispositivi e, naturalmente, la produzione, l'elaborazione e la trasmissione di quantità di dati sempre maggiori.

In questo scenario, le possibilità di azione sul paziente si diversificano, aprendo spazi nuovi per la cura ma anche generando nuove aspettative di

8. Per esempio, per una rassegna, si veda, Mandsberg N.K., *et al*, *Orally ingestible medical devices for gut engineering,* in *Advanced Drug Delivery Reviews*, 2020, 165-166, pp. 142-154.

attenzione ed intervento efficienti in grado di ridisegnare i contorni della responsabilità dell'agire terapeutico. Infatti, per fare solo un esempio, se si viene forniti di strumenti di monitoraggio con la promessa che le informazioni relative – sebbene processate attraverso sistemi complessi – sono costantemente sotto l'attenzione di un terapeuta, l'inefficienza nella risposta, vuoi dovuta ad un problema tecnico, vuoi dovuta ad un non tempestivo intervento umano, può aprire a pretese di responsabilità semplicemente non immaginabili nel passato anche recente.

In più, l'ambito della salute della persona, specialmente se particolarmente "attenzionata", implica la possibilità di dover prendere decisioni, anche radicali, con grande rapidità che dovrebbero presupporre un quadro informativo il più possibile corretto, completo ed aggiornato. Sicché, diventa cruciale garantire un'efficiente architettura generale di supporto a questa complessità, considerando la facile previsione di aumento continuo e sempre più massivo della produzione e della trasmissione dei dati.

Se tutto questo consente di immaginare nuovi scenari di "sanità diffusa", non va dimenticato, naturalmente, il potenziamento tecnologico e "data-driven" delle stesse strutture sanitarie tradizionali, quali ospedali, ambulatori, centri di analisi e così via.

Anche per essi si profila la necessità appena richiamata di un'architettura che consenta il massimo efficientamento in termini di produzione, elaborazione e supporto alla decisione in un contesto che affronta quotidianamente situazioni critiche ed emergenziali. Ma qui, il contributo dato dalle tecnologie basate sui dati, ed in particolare di quelle che si fanno rientrare nella nozione di "Intelligenza artificiale", si estende potenzialmente ad ogni ambito: dall'organizzazione dell'accesso alle prestazioni, alla gestione documentale e del personale, dei posti letto, delle forniture; dalla diagnostica, alle prestazioni infermieristiche, fino alla chirurgia, ed altro ancora. Per non parlare delle prestazioni ambulatoriali, della riabilitazione (con il connesso tema degli ausili e delle protesi), e delle esigenze di gestione del rischio per finalità assicurative.

Insomma, la promessa delle nuove tecnologie è di rivoluzionare il concetto e le pratiche di mantenimento e miglioramento della salute, quale benessere complessivo dell'individuo.

3. *Cloud computing, Edge computing*

Come si vede, il tema dell'evoluzione del settore sanitario include quello dei possibili utilizzi dell'intelligenza artificiale per efficientarne i servizi ma non si riduce a quello soltanto.

La prospettiva di avere miliardi di dispositivi producenti dati – molti dei quali rientranti nella categoria dei dati personali e meritevoli di particolare protezione – collegati e interoperanti a vari livelli, tra i quali sono distribuite non solo capacità di trasmissione, ma anche di elaborazione e di stoccaggio, comporta la necessità di un'attenzione a tutta questa complessità, posto che un'inefficienza in un punto di essa può potenzialmente risolversi in un esito fatale per la salute individuale o addirittura collettiva.

Il che ci fa porre fin da subito il tema non solo delle potenzialità di questa evoluzione per la realizzazione delle migliori condizioni di salute possibili ma anche quello della sua fragilità in ragione della costitutiva interdipendenza in sistemi sempre più ampi, di complicata gestione, manutenzione, aggiornamento e coinvolgenti i soggetti più disparati (dal medico al capezzale, al fornitore della connessione, a quello/i delle piattaforme e dei servizi online, al gestore delle infrastrutture vicine e lontane, e così via).

Le ricadute di tutto ciò, in termini di responsabilità giuridica sono naturalmente complesse e non soltanto relative alla difficoltà di inquadrare i numerosissimi aspetti di questa realtà nelle categorie classiche e nelle fattispecie specifiche, ma anche – e dati i temi, direi, soprattutto – all'effettività delle risposte giuridiche, posto che il caso di fallimento catastrofico può implicare giudizi di responsabilità soggettiva diversi, non facilmente ricostruibili e non adeguatamente sanzionabili.

Il tutto, naturalmente, in aggiunta alle questioni note in merito ai rischi di una medicina sempre più dipendente dal fattore tecnologico e dai suoi automatismi nel quale l'elemento umano possa apparire secondario e servente, ciò che potrebbe avere effetti contrari alle intenzioni qualora il vasto pubblico verso cui i servizi sono rivolti non riconosca più, in tale complessità, il senso della propria cura (nell'accezione propria del termine inglese *care*), e perda così la fiducia nei servizi preposti al miglioramento della salute.

In questo contesto, dunque, sebbene nel prosieguo di questo lavoro ci si soffermerà in particolare sul tema dell'intelligenza artificiale e, più nello specifico, sulla nuova regolamentazione dell'Unione Europea e sulle questioni relative alla protezione dei dati personali, avendo in mente specifici *stakeholders,* non sarà inopportuno proporre qui, ad uso dei non addetti ai lavori, un sintetico quadro delle questioni infrastrutturali attualmente all'attenzione di studiosi e pratici.

3.1. Cloud computing

Una delle caratteristiche della storia recente della "macchina computante" riguarda l'evoluzione del *design* relativo alla diversa allocazione dei fat-

tori principali che ne connotano l'operatività, vale a dire la capacità e la potenza di calcolo, la memoria e le interfacce *hardware* e *software* necessarie ad un suo utilizzo sempre più diffuso. Il tutto in un percorso che ha previsto e realizzato l'interconnettività generale delle macchine e dei dispositivi in grado di produrre ed elaborare dati.

Così, al modello totalmente accentrato delle origini, quando enormi *mainframes* concentravano in un unico punto tutte le funzionalità e le informazioni elaborate, si sono via via affermati modelli di decentramento delle risorse in grado di scalare le prestazioni e ridurre i rischi di inoperatività legati, in particolare, ai malfunzionamenti di singole unità.

Il modello cui probabilmente anche l'utente comune è oggi abituato è quello che siamo soliti riferire con l'espressione di *cloud computing.* Si tratta di un concetto anticipato sin dagli anni Sessanta del Ventesimo secolo prima da John McCarthy, secondo il quale "computation may someday be organized as a public utility"[9], e poi, esplorato in maggior dettaglio, benché sotto l'etichetta, appunto, di *computer utility*[10]*,* da Douglas Parkhill nel suo testo del 1966 intitolato *The Challenge of Computer Utility.* L'Autore introduce il concetto che il testo esplorerà, non senza presentare il percorso storico e concettuale che vi ha condotto, nel modo seguente:

Tele-data-processing systems (in which many remotely located users are connected via communication links to a central computing facility) have long been familiar in such specialized areas airline reservations, air defense, mail-order tallying, inventory control and department-store point-of-sale recording. More recently, the tele-data-processing concept has been extended to more general-purpose fields with the objective of sharing the use and costs of a digital computer among a number of users, as in any service bureau, but without requiring the physical transport of data and programs between the users and the computing center. In some cases, multiprogramming, so that the central computer can simoultaneously operate on many different programs, is also incorporated. In a few systems, programming, debugging, data introduction and retrieval, and computer control can be performed simultaneously, on-line, at each of the remote sites as though each user had the entire computing facility at his full command. These on-line, general-purpose

9. Citato in Bairagi S. I., Bang A. O., *Cloud Computing: History, Architecture, Security Issues,* in *International Journal of Advent Research in Computer and Electronics (IJARCE),* sp. is., 2015, pp. 102-108 (103).

10. L'accezione acquisita dall'espressione *cloud computing* sarebbe più ampia di quella riferita all'espressione *utility computing* che si configurerebbe come un sottoinsieme della prima, cfr. Daylami N., *The origin and construct of cloud computing,* in *International Journal of the Academic Business World,* 2015, vol. 9, 2, pp. 39-45 (39).

multi-user systems have generated widespread interest and have led to the concept of "computer public utility", the major theme of this book[11].

Non è del tutto chiaro, invece, a chi si debba l'introduzione della fortunata metafora del *cloud computing* che è utilizzata diffusamente oggi. Secondo alcuni essa si dovrebbe ad un *report* interno degli anni Novanta della società *Compaq Computer* ad opera di Sean O'Sullivan nel quale si discuteva di "*cloud computing strategy",* mentre altri ascrivono la paternità all'allora CEO di Google Eric Schmidt in una conferenza del 2006.

La possibilità di utilizzare risorse di calcolo, spazi di memoria, servizi, piattaforme, software in ambienti unitari e messi a disposizione da uno o più fornitori, a prescindere dalla tipologia di dispositivo (mobile, tablet, pc ecc.) come se, per dirla con Parkhill, tutto il sistema fosse a disposizione di ciascuno, è divenuta una realtà largamente utilizzata e nota in particolare dopo l'avvento del *mobile computing* e l'aumento radicale di dispositivi connessi alla rete. L'architettura *cloud* consente, infatti, grande scalabilità, data in particolare dalla possibilità di fornire all'utente le risorse appena indicate *as a service*[12]*,* vale dire senza bisogno che questi disponga in proprio delle dotazioni hardware e software necessarie a realizzare le complesse operazioni di cui abbisogna, ma potendolo svolgerle – spesso dietro remunerazione – attraverso le strutture del fornitore a lui rese accessibili attraverso la rete.

Per la verità, oggi disponiamo di una nozione giuridica di *cloud computing* data dalla Direttiva UE 2022/2555 che – tra le altre cose – ha abrogato la precedente 2016/1148[13], e che definisce un «servizio di cloud computing» come "un servizio digitale che consente l'amministrazione su richiesta di un pool scalabile ed elastico di risorse di calcolo condivisibili e l'ampio ac-

11. Parkhill D.F., *The Challenge of computer utility,* Adison-Wesley pub., Reading Massachusetts, 1966, p. 3.

12. Sulle varie accezioni e utilizzi di questa espressione si veda Duan G. Fu, Zhou N., Sun X. , Narendra N. C. , Hu B., *Everything as a Service (XaaS) on the Cloud: Origins, Current and Future Trends*, in *2015 IEEE 8th International Conference on Cloud Computing*, New York, NY, USA, 2015, pp. 621-628.

13. La Direttiva UE 2022/2555 ha lo scopo di stabilire misure volte a garantire un livello comune elevato di cibersicurezza nell'Unione in modo da migliorare il funzionamento del mercato interno, attraverso obblighi che impongono agli Stati membri di adottare strategie nazionali in materia di cibersicurezza e di designare o creare autorità nazionali competenti, autorità di gestione delle crisi informatiche, punti di contatto unici in materia di sicurezza (punti di contatto unici) e team di risposta agli incidenti di sicurezza informatica (CSIRT); misure in materia di gestione dei rischi di cibersicurezza e obblighi di segnalazione per alcuni soggetti; norme e obblighi in materia di condivisione delle informazioni sulla cibersicurezza; obblighi in materia di vigilanza ed esecuzione per gli Stati membri (art. 1).

cesso remoto a quest'ultimo, anche ove tali risorse sono distribuite in varie ubicazioni" (art. 6, n. 30).

La tipologia di situazioni che nella prassi sono sottese all'espressione *cloud computing* può essere particolarmente complessa non solo quanto agli elementi concreti che vengono forniti *as a service* ma anche alle configurazioni che sono possibili per il migior raggiungimento dell'interesse dei soggetti in gioco. Ad esempio, le esigenze delle attività aziendali possono richiedere l'utilizzo di sistemi cc.dd *multi-cloud* messi a disposizione da diversi fornitori, tali sistemi possono configurarsi come combinazioni "ibride" di *cloud* privati (costituiti specificamente per quella realtà aziendale) o pubblici (potenzialmente accessibili da chiunque). Tale complessità ha impegnato la dottrina che si è interessata di *cloud computing* in un lavoro non semplice di ricostruzione sistematica delle operazioni negoziali messe in atto e della valorizzazione dei loro collegamenti al fine di ricostruire la disciplina applicabile[14]. Tale opera tiene conto oggi della introduzione nel codice del consumo del Capo I-*bis,* nel Titolo II della Parte IV, dedicato alla disciplina dei contratti di fornitura di contenuto digitale o di servizi digitali conclusi tra consumatore e professionista, in tema di conformità del contenuto digitale o del servizio digitale al contratto, di rimedi in caso di difetto di conformità o di mancata fornitura, delle modalità di esercizio degli stessi, nonché della modifica del contenuto digitale o del servizio digitale (art. 135-*octies,* comma 1).

Senza entrare qui nel dettaglio di questa normativa, è comunque opportuno segnalare, per il tema che ci occupa, che tale disciplina generale non si applica ai contratti concernenti servizi di assistenza sanitaria, per i servizi prestati da professionisti sanitari a pazienti, al fine di valutare, mantenere o ristabilire il loro stato di salute, ivi compresa la prescrizione, la somministrazione e la fornitura di medicinali e dispositivi medici, sia essa fornita o meno attraverso le strutture di assistenza sanitaria (art. 135-*novies,* comma2, lett. c).

Per quanto rilevanti siano tutte queste questioni, occorre segnalare che il paradigma sotteso alla architettura della *nuvola,* benché ampiamente usato e certamente destinato a mantenere un suo ruolo essenziale, viene oggi ripensato e affiancato da altri paradigmi. Lo scenario rappresentato nei paragrafi precedenti, si ricorderà, risulta in particolare caratterizzato dall'aumento esponenziale dei dispositivi connessi e dalla necessità di garantire, almeno

14. Un lavoro ricostruttivo completo è svolto, ad esempio, in Trubiani F., *I contratti di cloud computing: natura, contenuti e qualificazione giuridica,* in *Diritto dell'informazione e dell'informatica,* 2022, II(2), pp. 395 ss.

in certe situazioni relative alle decisioni sulla salute, un grado di efficienza del servizio di altissimo livello, in termini di garanzia di efficienza e di immediatezza pressoché istantanea nell'aggiornamento e messa a disposizione dei dati e delle elaborazioni conseguenti. Rispetto a tali esigenze, il *cloud,* sembra non costituire più, da solo, lo strumento migliore.

3.2. Edge Computing

Rispetto ad un universo di dispositivi di varia natura e capacità simultaneamente connessi e in grado quanto meno di rilevare dati e trasmetterli sulla Rete (*Internet of Things*), il modello del *cloud computing* presenta le caratteristiche di un struttura accentrata. La collocazione di grandi *servers* di enorme potenza e in grado di fornire tutti i servizi del *cloud* in luoghi geografici distanti dalle periferie della Rete nelle quali si moltiplicano e operano sempre nuovi dispositivi, nonché l'aumento esponenziale nella produzione di dati che segue alla loro diffusione, producono limitazioni sempre più gravose in ragione, in particolare, dei tempi di comunicazione, elaborazione e risposta tra la "nuvola" e la "terra".

Tale situazione appare del tutto indesiderabile giacché limita fortemente i vantaggi che l'allargamento della datificazione produce in particolare in quelle situazioni che richiedono immediatezza nella risposta (ad es. applicazioni di *Virtual Reality, Augmented Reality,* monitoraggio in tempo reale del paziente e intervento emergenziale in telemedicina, chirurgia robotica ecc.), oppure continuità nel servizio (ad es. servizi di *streaming*), quando l'utente finale si trovi molto lontano dai luoghi delle elaborazioni *cloud* o usufruisca dei servizi in continuo movimento (ad es. veicoli connessi[15]).

Nel 2012 *Cisco Systems Inc.* introduce così un paradigma di ulteriore decentralizzazione, nel quale computazione, conservazione e servizi di rete sono posti più vicino ai dispositivi di produzione dei dati rispetto ai grandi *data centers* dei fornitori di *cloud.* Questo paradigma è stato chiamato *fog computing* "semplicemente perché la nebbia è una nuvola più vicina alla terra"[16]. Si tratta di complementare il *cloud* con un insieme di servizi le cui strutture di elaborazione e fornitura siano più vicine alla periferia sfruttando

15. Sulle problematiche giuridiche connesse alla *smart mobility* cfr. Pisani Tedesco A., *Smart mobility e rischi satellitari e informatici: i possibili scenari di allocazione della responsabilità civile,* in *Diritto del commercio internazionale,* 2019, 4, pp. 801 ss.

16. Bonomi F., Milito R., Zhu J., Addepalli S., *Fog computing and its role in the internet of things*, in *Proceedings of the first edition of the MCC workshop on Mobile cloud computing,* 2012, pp. 13-15 (13).

così vari vantaggi quali: la posizione geografica e la conseguente bassa latenza nella comunicazione, l'ampia distribuzione di nodi di elaborazione in grado di supportare scalabilità e mobilità, interazioni in *real-time,* fornendo supporto alle più imponenti attività analitiche dei grandi server *cloud*[17].

L'idea di base, come si capisce, è quella di spostare una parte del lavoro verso i dispositivi finali sfruttando le potenzialità degli apparati presenti ai nodi di rete diffusi e distribuendo così il carico di lavoro tra *cloud* e periferia: per tale ragione – anche se la terminologia non è univoca – si parla, in generale, di *edge-computing*[18].

Tale paradigma può essere oggi sfruttato ancora di più rispetto al 2012, posto che i dispositivi "finali" risultato sempre più potenti e performanti, addivenendo, quindi, ad una struttura stratificata su più livelli (*edge, fog, cloud*) che, sebbene non presentino tutti il medesimo grado di capacità di elaborazione né le medesime condizioni di sicurezza, possono, però, utilmente collaborare nel distribuire il lavoro computazionale a seconda delle necessità.

Le applicazioni *edge* sono normalmente guidate dall'utente e utilizzano architetture distribuite, in contrasto con le applicazioni guidate dai dati e le architetture centralizzate del *cloud*. Grazie alla sua posizione più vicina al bordo della rete, il modello *edge* ha un consumo di banda e una latenza ridotti che favoriscono il risparmio energetico e il miglioramento della qualità del servizio e dell'esperienza. Nel livello *edge* le risorse sono sono poche, diffuse e con un'elevata eterogeneità, in contrasto con le numerose risorse fornite da *cloud*, che sono localmente raggruppate. Le architetture EC sono molto scalabili per quanto riguarda il numero di dispositivi supportati, il che significa che l'architettura deve sempre essere preparata a registrare un aumento del numero di dispositivi connessi, aggiungendo però complessità al processo di gestione degli stessi[19].

---

17. *Ibidem.*

18. Kong L., et al, *Edge-computing-driven Internet of Things: A Survey*, in *ACM Computing Surveys*, vol. 55, 8, pp. 1-41. L'assimilazione di *fog computing* e *edge computing* è, invece, criticata in OpenFog, *Openfog Reference Architecture for Fog Computing, Openfog Consortium*, 2017, p. 3. Data la flessibilità e l'aumento delle capacità di calcolo dei dispositivi edge la distinzione può essere variabile e ridefinita in funzione del contesto applicativo specifico: "edge of a network and its location highly depend on the context of applications deployment. An edge is a logical border and it can be changed as the data consumer and data generator/provider are varied", così in Mansour Y, Ali Babar M., *A review of edge computing: Features and resources virtualization*, in *Journal of Parallel and Distributed Computing*, 2021, 150, pp. 155-183.

19. Cavalho G., Cabral B., Pereira V., Bernardino J., *Edge computing: current trends, research challenges and future directions,* in *Computing,* 2021, 103, pp. 993-1023 (997-98).

Per contro la maggior disponibilità di risorse sul *cloud* rende questo livello idoneo a compiti più gravosi che richiedono più tempo, oltre che più capacità di processamento, quale l'addestramento dei modelli di apprendimento automatico e l'analisi avanzata dei dati[20].

La possibilità di organizzare la produzione di dati, l'elaborazione e la risposta in modo da potenziare e coordinare il livello *edge,* e quello *cloud,* apre a possibilità importanti di sfruttamento dell'*IoT* nel perseguimento degli obiettivi di miglioramento della salute in un contesto globale caratterizzato dall'invecchiamento della popolazione e l'aumento delle patologie croniche. Poter accedere alla situazione clinica del paziente in tempo reale e da remoto, applicare modelli previsionali per fornire suggerimenti nel contesto del auto-monitoraggio da parte del paziente stesso che possa usufruire di semplici sensori di rilevamento e applicazioni *mobile,* configurano scenari di potenziamento della cura e di "medicina quotidiana" inusitati[21].

4. Profili giuridici generali

Come si vede, il tema fondamentale che emerge da questa trasformazione è, ancora una volta, quello della produzione e della circolazione dei dati, in questo caso, "ad uso sanitario", categoria, questa, che non si identifica *de plano* con quella dei "dati relativi alla salute" di cui al Regolamento UE 2016/679, artt. 4 e 9. Questi ultimi, infatti sono un sottoinsieme dei "dati personali" e si caratterizzano per essere "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" (art. 4, n. 15). I primi, invece, comprendono *tutti* i dati la cui circolazione ed elaborazione tra i vari livelli è funzionale alla organizzazione delle strutture sanitarie e alla prestazione dei servizi, ancorché anonimi e prodotti dai dispositivi per lo svolgimento delle rispettive funzioni o per il loro coordinamento.

I modelli *edge,* e in generale, l'idea stessa della distribuzione delle risorse e delle attività richiedono, tra le altre cose, *standards* di interoperabilità dei dati nonché protocolli condivisi di comunicazione ed elaborazione.

---

20. Reddy Boda V.V., *Edge Computing in Healthcare: What It Is and Why It Matters,* in *MZ Computing Journal,* 2024, vol. 5, 2, pp. 1-18.

21. Ziwei H., *et al., The application of Internet of Things in smart healthcare sector: a bibliometric and deep study,* in *Heliyon,* 2024, Vol. 10, pp. 1-11; Hartmann M., Hashmi U. S., Imran A., *Edge computing in smart Healthcare systems: Review, challenges and research directions,* in *Transactions on Emerging Telecomunications Technologies,* 2019, sp. iss., pp. 1-25.

Si profila, quindi, l'astratta rilevanza di tutta la normazione sui dati prodotta e producenda, e la necessità di un'opera di coordinamento interpretativo che si preannuncia tutt'altro che semplice, in un contesto in cui i temi della sicurezza e della *privacy* divengono ancora più critici.

A tali questioni si aggiungono, inoltre, quelle relative alla individuazione delle operazioni negoziali utilizzate per la fornitura dei servizi digitali quando questi sono potenzialmente l'esito di elaborazioni provenienti da più livelli, coinvolgenti più soggetti e volta a volta variamente interdipendenti sebbene messi in gioco per la funzionalità del singolo servizio richiesto.

Immaginiamo, dunque, che per l'utilizzo di una applicazione di monitoraggio di alcuni parametri clinici del paziente l'elaborazione continua dei dati avvenga: a) in parte sul dispositivo del paziente stesso; b) in parte a livello *fog* e quindi su una "nebbia" di nodi di rete vicini al livello *edge* dei dispositivi di rilevazione e di prima elaborazione in mano al paziente; c) a livello di *cloud* per l'analisi avanzata di grandi quantità di dati provenienti da una pluralità di fonti di base con lo scopo di elaborare le correlazioni significative sulla base delle quali aggiornare i parametri di riferimento di applicarsi, poi, nuovamente d) al livello individuale per fornire i riscontri clinici al singolo paziente.

Immaginiamo, poi, che, in tutto questo, si collochi anche la comunicazione con il medico o l'*équipe* della struttura sanitaria che a sua volta si serva dei dati per la supervisione del paziente e le decisioni terapeutiche fondamentali e che, inoltre, svolga attività di ricerca e, dunque utilizzi i dati anche a tale scopo servendosi, magari, di ulteriori strumenti *edge* e *cloud.*

Come si vede, l'assetto complessivo che si presenta, e che, presumibilmente, è destinato a divenire ordinario nell'evoluzione dei sistemi sanitari tecnologicamente avanzati, implica una enorme complessità giuridica nella quale sono in gioco temi tutti rilevanti per i giudizi di responsabilità, e che vanno dall'adeguata organizzazione della struttura, al livello di assistenza, alla necessaria informazione dei paziente, non solo quanto all'uso dei suoi dati personali ma anche ai fini della sua autodeterminazione terapeutica, fino al giudizio qualitativo sulla prestazione fornita stessa.

Analogamente, quanto al tema specifico dell'intelligenza artificiale nel contesto sanitario, anch'esso va oggi inquadrato in un orizzonte che supera il modo consueto con cui esso è posto, vale a dire con riferimento, in particolare, al tema dell'uso di sistemi di supporto alla (o, idealmente, sostituzione della) decisione umana nel rapporto di cura del paziente[22].

22. Tema, naturalmente, complesso e lungi dall'essere esaurito, sul quale si veda, recentemente, Grasso G. A., *GDPR e intelligenza artificiale: limiti al processo decisionale*

Infatti, elaborazioni complesse, e distribuite su più livelli, dei dati sanitari, aventi scopi specifici, pure differenti, in ragione delle necessità concrete di utilizzo e delle possibilità funzionali proprie a ciascun livello, dispongono ad un utilizzo vario e distribuito anche degli applicativi che racchiudiamo sotto la fortunata etichetta di "intelligenza artificiale". Quest'ultima trova, oggi, una nozione giuridica nell'art. 3 del Regolamento UE 2024/1689, che nel definire che cos'è, ai fini del Regolamento stesso, un "sistema di intelligenza artificiale" lo descrive come "un sistema automatizzato progettato per funzionare con *livelli di autonomia variabili* e che può presentare *adattabilità* dopo la diffusione e che, per obiettivi *espliciti o impliciti*, deduce dall'input che riceve come generare output quali *previsioni, contenuti, raccomandazioni o decisioni* che possono influenzare ambienti *fisici o virtuali*" (corsivi aggiunti).

Una nozione così ampia, si presta ad individuare sistemi del tipo indicato potenzialmente in tutte le articolazioni dell'infrastruttura, sia a livello *cloud,* che *fog* o *edge.*

Il che concretamente significa, di nuovo, il potenziale moltiplicarsi dei soggetti giuridicamente rilevanti e coinvolti nella fornitura di sistemi, di servizi digitali, nel loro utilizzo a vario titolo, nonché, infine, del sovrapporsi a questi ruoli – cui il Regolamento fa corrispondere obblighi differenti – ove ricorresse il caso, anche di quelli essenziali per la gestione dei dati personali (in particolare quelli del titolare del trattamento e del responsabile).

Così, un sistema di supporto alla decisione medica i cui *output* dipendano non solo da dati di cui esso possa disporre sul luogo di operatività ma anche dagli esiti delle elaborazioni su grandi quantità svolte sugli altri livelli, nei quali, di nuovo, operino sistemi di IA, qualora la comunicazione tra i sistemi o la loro performatività non fossero ottimali nel caso di specie, potrebbe generare risposte inadeguate con ricadute gravi in termini di decisione sulla salute e complicate ricostruzioni in tema di responsabilità[23].

---

automatico in sanità, in Salanitro U. (a cura di), *SMART. La persona e l'infosfera,* Pacini Giuridica, Pisa, 2022, pp. 183-223; Scotti R., *La responsabilità civile dei danni cagionati dall'intelligenza artificiale in ambito sanitario,* in *Giustizia civile,* 2024, 1, pp. 158 ss.; Colaruotolo A., *Intelligenza artificiale e responsabilità medica: novità, continuità, criticità,* in *Responsabilità medica,* 2022, 3, pp. 299 ss.; Salito G., *La responsabilità da algoritmo tra (teoria della) finzione e realtà sanitaria: una nuova declinazione della responsabilità medica?*, in *Rivista italiana di medicina legale,* 2022, 4, pp. 849 ss.

23. Non pare inopportuno ricordare che la legge 8 marzo 2017, n. 24, all'art. 7 dispone che "La struttura sanitaria o sociosanitaria pubblica o privata che, nell'adempimento della propria obbligazione, si avvalga dell'opera di esercenti la professione sanitaria, anche se scelti dal paziente e ancorché non dipendenti della struttura stessa, risponde, ai sensi degli articoli 1218 e 1228 del codice civile, delle loro condotte dolose o colpose". Quanto alla

Va da sé, poi, che una tale distribuzione implica l'ampliamento potenziale dell'incidenza di tutte le questioni relative ai rischi dell'utilizzo dell'IA su cui molto si discute (e che saranno brevemente riprese anche nel prosieguo di questo lavoro), quali, in particolare: la ridotta trasparenza dei processi decisionali, il pericolo di deviazioni sistematiche nei loro *output* rispetto allo standard desiderato in ragione delle modalità con cui il sistema è stato costituito, addestrato o impiegato (*bias*), il potenziale impatto discriminatorio delle decisioni, la sostenibilità energetica ed economica dell'addestramento dei modelli più recenti e performanti, ecc.[24].

La costruzione di un quadro giuridico generale relativo all'evoluzione tecnologica contemporanea è tutt'ora in corso, ma, nel momento in cui scriviamo, si deve registrare l'importante novità, per il tema che ci interessa, dell'adozione del Regolamento UE sullo spazio europeo dei dati sanitari, approvato da ultimo, con votazione quasi unanime[25], dal Consiglio dell'Unione Europea nella seduta del 21 gennaio 2025.

Risulta pertanto fondamentale entrare un po' nel dettaglio di questo atto normativo che, in ragione di quanto sopra mostrato, appare cruciale per la costruzione dell'infrastruttura europea di circolazione dei dati sanitari

5. Lo spazio europeo dei i dati sanitari

Il Regolamento del Parlamento Europeo e del Consiglio sullo spazio europeo per i dati sanitari vuole porsi come strumento normativo completo per la disciplina di questa importantissima parte del patrimonio di dati che continuamente viene prodotto. In questo senso, esso non solo interviene complementando la normativa esistente, ed in particolare quella relativa alla protezione dei dati personali, ma predispone anche infrastrutture e strumenti di *governance,* per consentire il riutilizzo dei dati sanitari al fine di trarre da essi tutte le utilità che possono consentire in termini di miglioramento della ricerca e della salute pubblica.

---

responsabilità dell'esercente la professione sanitaria, il terzo comma del medesimo articolo prevede invece che risponda "del proprio operato ai sensi dell'articolo 2043 del codice civile, salvo che abbia agito nell'adempimento di obbligazione contrattuale assunta con il paziente".

24. La letteratura su queste questioni è interdisciplinare e ormai alluvionale, se ne può vedere una sintesi in Sarra C., *Dignità umana nell'era dell'intelligenza artificiale e della datificazione,* Kront, Roma 2025, in particolare, il Cap. 1, con la richiamata bibliografia. Alcuni temi essenziali saranno ripresi nel prosieguo.

25. Il testo è stato approvato con il voto a favore di 25 stati membri su 27, registrandosi il voto contrario solo di Finlandia e Danimarca, cfr. *https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CONSIL:ST_5541_2025_INIT.*

In linea generale, quanto al tema della protezione dei diritti delle persone, il dato sanitario (con le precisazioni sulla definizione di tale categoria che subito faremo) risulta particolarmente problematico. Infatti, esso, per la sua idoneità potenziale a riferire aspetti intimi della persona relativi – innanzi tutto, ma non solo[26] – alle sue condizioni di salute, da un lato, deve godere della più accurata protezione, ma, dall'altro, necessita di circolare e di essere portato alla conoscenza, in particolare, dei professionisti che si succedono nella cura della persona per poter meglio svolgere la propria funzione. Appare fin troppo ovvio che una limitata conoscenza della storia clinica del paziente e dei dati relativi, possono condurre a diagnosi errate, inefficaci, intempestive o addirittura dannose, laddove l'accesso immediato ad una completa rappresentazione può, invece, garantire cure appropriate e tempestive.

Inoltre, la massa di dati prodotti nell'ambito del sistema sanitario nel suo complesso è di enorme importanza per l'elaborazione di analisi avanzate e tempestivi interventi in caso di emergenze sanitarie, o per lo sviluppo della ricerca medica ed epidemiologica.

D'altro canto, però, di nuovo, l'esigenza di circolazione dei dati sanitari deve essere coordinata con il fondamentale rispetto dell'autonomia del paziente, della sua *privacy* informazionale della sua sovranità in tema di trattamenti sanitari che si esprime nel principio dell'autodeterminazione terapeutica e del rifiuto del paternalismo medico che sono conquiste di civiltà etica e giuridica tanto importanti quanto, ahimè, fragili, specialmente in tempi di crisi[27].

Questa doppia necessità – di massima protezione e di agevole circolazione – altro non è che il riflesso sul piano della datificazione della persona del sempre vago confine tra la salute come diritto dell'individuo e "interesse" della collettività sul quale già abbiamo detto. Ma, poiché i benefici della "scoperta di conoscenza" basata sui dati e del "ciclo della datificazione", ivi inclusi quelli di disporre di strumenti di intelligenza artificiale performanti, si mostrano solo alla condizione di poter costantemente contare su grandi quantità di dati, il rischio di una sottovalutazione del dovuto rispetto per l'autonomia dell'individuo è concretamente presente[28].

---

26. Le decisioni prese nell'ambito dei rapporti con i professionisti della salute possono rivelare aspetti extra-sanitari persona ma ugualmente delicati e meritevoli di particolare protezione, quali, ad esempio, le proprie opinioni religiose, le origini etniche ecc.

27. Bontempi M., *Per una ecologia medica: dal paternalismo al personalismo metodologico nel rapporto medico-paziente,* in *Areté,* 2022, 7, pp. 169 ss.

28. Il discorso si farebbe qui importante e delicato, dovendosi chiarire le ragioni per le quali l'avvento della datificazione, quale modalità corrente dello spirito tecnico, sia destinato

Ad ogni modo, vediamo i punti salienti di questo importante atto normativo.

5.1. La struttura del Regolamento sullo spazio europeo dei dati sanitari

In generale, il Regolamento ha lo scopo di istituire il c.d. *spazio europeo dei dati sanitari,* vale a dire di creare le condizioni normative, istituzionali e tecniche per la protezione e circolazione sicura di tali dati. A questo proposito, esso, innanzi tutto, specifica e completa le regole del GDPR in materia, il quale, come accennato e come si vedrà meglio *infra,* ne prevede la disciplina all'art. 9. Come meglio si vedrà nella II parte di questo lavoro, in tale articolo, che riguarda tutte le tipologie di dati meritevoli di particolare protezione, si afferma il principio del divieto di loro trattamento (§1), salvo che ricorra qualcuna delle condizioni di deroga ivi previste.

Inoltre, il nuovo Regolamento stabilisce regole comuni per due componenti software obbligatorie dei sistemi di cartelle cliniche elettroniche (*health record systems*), vale a dire il "componente software europeo di interoperabilità" e il "componente software europeo di registrazione", nonché per le applicazioni di *wellness* che si dichiarino interoperabili con tali sistemi.

L'atto, nel testo al momento disponibile[29], è suddiviso in nove capitoli, 105 articoli e quattro allegati con il consueto corposo apparato di ben 115 *Considerando* e si compone di disposizioni generali (Cap. I), della disciplina del c.d. "uso primario dei dati sanitari" (Cap. II, su cui, brevemente, *infra*), che comprende inoltre la disciplina della *governance* (sez. 2) e dell'infrastruttura transfrontaliera (sez. 3) per garantire la gestione dei dati e i diritti degli interessati con riferimento all'uso primario dei loro dati sanitari.

Seguono le disposizioni uniformi sui sistemi di cartelle cliniche elettroniche e le applicazioni per la salute e il benessere (Cap. III) e l'importantissimo capitolo dedicato al c.d. "uso secondario" dei dati sanitari (Cap. IV), che presenta una disciplina simmetrica a quella relativa all'uso primario ma molto più complessa data la delicatezza del tema, vale a dire il riutilizzo dei dati sanitari dei pazienti per finalità diverse da quelle legate alla prestazione in loro favore di servizi sanitari.

---

a divenire sempre più invasiva rispetto alla persona. Il tema dovrebbe fare i conti con la natura e la consistenza concettuale attuale del principio di dignità umana quale *summa* dei limiti alle pretese sull'individuo. Tal discorso non può essere condotto qui, ho però presentato la questione e aperto alla discussione in Sarra C., *Dignità umana,* cit.

29. Febbraio 2025, si tratta del testo licenziato dal Parlamento Europeo ed approvato dal Consiglio dell'Unione Europea il 21 gennaio 2025, non ancora del tutto rifinita sul piano puramente redazionale.

Così, troviamo disciplinate le condizioni per l'utilizzo, appunto, ultroneo dei dati sanitari (sez. 1), anche in questo caso l'istituzione di una struttura di *governance* (sez. 2), nonché le modalità con cui sarà possibile a certi operatori accedere ai dati sanitari per un loro utilizzo secondario (sez. 3), e la costituzione di una infrastruttura transfrontaliera per l'accesso regolato al di fuori dello stato membro cui appartiene il soggetto (sez. 4); troviamo norme per la costituzione di cataloghi consultabili – nazionali ed europeo – delle serie di dati disponibili e del marchio dell'Unione di qualità e utilità (sez. 5), nonché norme sui reclami agli organismi di accesso ai dati sanitari da parte di persone fisiche o giuridiche (sez. 6).

Seguono una serie di disposizioni relative ad azioni ulteriori (Cap. V) dove si disciplinano, in particolare, tra le altre cose, le possibilità e le modalità di trasferimento dei dati *non personali* verso paesi terzi o organizzazioni internazionali.

Vengono, poi, istituiti e disciplinati organismi a livello unionale di *governance,* tra i quali il "Comitato per lo spazio europeo dei dati sanitari" (*European Health Data Space Board*), il *"forum* dei portatori di interessi" (*stakeholders*) e i "gruppi di interesse" per le piattaforme *MyHealth@EU* e *HealthData@EU* (Ch. 6).

Infine, come di consueto, norme relative alle deleghe di poteri alla Commissione, norme per le determinazioni nazionali sulle sanzioni e, infine, le complesse disposizioni relative alla applicabilità differita delle varie parti del Regolamento che ne spostano la piena operatività fino a sei anni dalla data di entrata in vigore (cfr. art. 105).

Quanto al merito del Regolamento, è interessante notare lo sforzo di configurare un assetto sistematico del "diritto dei dati" che, in questo caso, si manifesta, da un lato, attraverso la dichiarata compatibilità e subordinazione ("Il presente regolamento lascia impregiudicati gli altri atti dell'Unione…") rispetto a numerosi altri Regolamenti, e, dall'altro, nel rinvio a quelli per l'individuazione di molte definizioni essenziali (cfr. art. 2).

Quest'ultimo punto evidenzia come, nonostante le formule presenti in questa tipologia di atti regolativi che introducono definizioni ("ai fini del presente regolamento…"), si stia in realtà determinando un complesso normativo importante e, nelle intenzioni, sistematico, la cui effettiva coerenza sul piano ermeneutico ed applicativo è tutta ancora da verificare[30]. Come si sa, scrivere leggi è solo l'inizio del processo di formazione del diritto.

30. Per un esempio specifico di tali difficoltà, a proposito della compatibilità tra GDPR e AI Act in punto di disciplina delle decisioni automatizzate, si può vedere Sarra C., *Artificial Intelligence in Decision-making: A Test of Consistency between the "EU AI Act" and the "General Data Protection Regulation"*, in *Athens Journal of Law*, 2025, vol. 11, 1, pp. 45-62.

A questo proposito, segnaliamo fin dall'inizio un'articolazione definitoria importante che distingue tra "dati relativi alla salute", per la cui definizione il Regolamento rinvia al GDPR (art. 2, § 1, lett. a); e dati "sanitari elettronici" che possono, a loro volta essere sia "personali" che "non personali" (art. 2, § 2, lett. a), b), c). Di questi ultimi, i primi includono "i dati relativi alla salute e i dati genetici che sono trattati in formato elettronico", e i secondi, invece, "i dati sanitari elettronici diversi dai dati sanitari elettronici personali, compresi sia i dati che sono stati anonimizzati in modo da non riferirsi più a una persona fisica identificata o identificabile ("interessato"), sia i dati che non si sono mai riferiti a un interessato". È importante evidenziare che l'accesso di cui si discute per gli usi, primario e secondario, la cui disciplina costituisce il *core* del Regolamento, è riferito ai "dati sanitari elettronici" nell'insieme delle due categorie sopra evidenziate. In particolare, sono inclusi, non solo i dati prodotti per la prestazione di un servizio sanitario ma anche "dati sui determinanti della salute, quali il comportamento, le influenze ambientali e fisiche, l'assistenza medica e fattori sociali o educativi". Ed inoltre, vi rientrano "dati che sono stati inizialmente raccolti per la ricerca, le statistiche, la valutazione di minacce sanitarie, la definizione delle politiche o finalità normative", e ciò "a prescindere dal fatto che tali dati siano forniti dall'interessato o da altre persone fisiche o giuridiche come i professionisti sanitari, o siano trattati in relazione alla salute o al benessere di una persona fisica e dovrebbero inoltre includere *dati desunti o derivati*, quali diagnosi, test ed esami medici, nonché i dati osservati e registrati con *l'ausilio di strumenti automatizzati*" (*Considerando 6,* corsivi aggiunti).

Come si vede, si tratta di un'enorme quantità potenziale di dati, rispetto ai quali si tratta di capire quali strumenti siano dati agli interessati per tutelare il proprio patrimonio informativo e per interagire con le burocrazie che sono in gioco nella conservazione e nella gestione di essi.

La prassi mostrerà, poi, quanto tali strumenti saranno effettivamente utilizzati e tutelanti.

5.2. Uso "primario" e uso "secondario" dei dati sanitari: nozioni

Rispetto a queste fondamentali questioni, l'aspetto più qualificante dell'atto riguarda senz'altro la distinzione tra "uso primario" e "secondario" dei dati sanitari con riferimento ai quali esso stabilisce regole comuni, sia quanto alla legittimità di usi rientranti in tali categorie, sia quanto alle

infrastrutture transfrontaliere necessarie per gli utilizzi primari e secondari, istituendo meccanismi di *governance* sia livello unionale che statale.

Per "uso primario" deve intendersi il trattamento dei dati sanitari elettronici per la prestazione di assistenza sanitaria al fine di valutare, mantenere o ripristinare lo stato di salute della persona fisica cui si riferiscono tali dati, comprese la prescrizione, la dispensazione e la fornitura di medicinali e dispositivi medici, nonché per i pertinenti servizi sociali, amministrativi o di rimborso (art. 2, § 2, lett. d). In sostanza, si tratta del trattamento dei dati del paziente per la prestazione di servizi sanitari a suo favore e pratiche amministrative relative.

Invece, significativamente, per "uso secondario" si intende il trattamento dei dati sanitari dei pazienti per finalità diverse da quelle iniziali per le quali tali dati sono stati raccolti o prodotti (art. 2, §2, lett. e).

Tra queste si annoverano, innanzi tutto, finalità di pubblico interesse nell'ambito della sanità pubblica o della medicina del lavoro, quali la protezione da gravi minacce per la salute a carattere transfrontaliero, la sorveglianza della sanità pubblica o delle attività per la garanzia di elevati livelli di qualità e sicurezza dell'assistenza sanitaria, inclusa la sicurezza dei pazienti, e di medicinali o dispositivi medici. Vi sono, poi, le finalità relative alla definizione delle politiche e attività regolamentari a sostegno di enti pubblici o di istituzioni, organi e organismi dell'Unione, comprese le autorità di regolamentazione, del settore sanitario o dell'assistenza affinché svolgano i compiti definiti nei rispettivi mandati. Quindi finalità statistiche come le statistiche ufficiali a livello nazionale, multinazionale e dell'Unione, relative al settore sanitario o dell'assistenza. E infine, finalità quali attività d'istruzione o d'insegnamento nel settore sanitario o dell'assistenza al livello della formazione professionale o dell'istruzione superiore, la 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 (art. 53).

Nell'ambito di queste ultime finalità di utilizzo secondario dei dati sanitari, è degno di nota il riferimento esemplificativo alle 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 (art. 53, § 1, lett. e), ii).

Se si considerano tutti gli ambiti di ricerca indicati nell'articolo in termini piuttosto vaghi, si può intravedere una legittimazione delle attività di

utilizzo dei dati sanitari elettronici per uso secondario per lo sviluppo, il test e il miglioramento di applicazioni di intelligenza artificiale in un senso molto ampio, in linea con le aspettative di implementazione che si connettono alle innovazioni relative.

La disposizione appena citata va, poi, coordinata con il Regolamento sull'Intelligenza Artificiale e con le disposizioni relative alla disciplina dei dispositivi medici e medico-diagnostici in vitro (su cui, *infra*).

Infine, costituisce finalità che legittima l'accesso ai dati sanitari elettronici anche il miglioramento della prestazione di assistenza, ottimizzazione delle cure ed erogazione di assistenza sanitaria sulla base dei dati sanitari elettronici di altre persone fisiche (art. 53, § 1, lett. f).

5.3. La disciplina dell'uso "primario" dei dati sanitari elettronici e le applicazioni per la salute

Venendo ora sinteticamente alla disciplina dell'uso "primario", esso, come detto, è riferito all'ambito delle prestazioni sanitarie effettuate in favore dell'interessato stesso a cui il Regolamento, in primo luogo, offre una serie di diritti che specificano o si aggiungono a quelli indicati nel GDPR. Si nota, ad esempio, quanto ai dati personali elettronici, un potenziamento del diritto di accesso, già disciplinato in generale dall'art. 15 del GDPR.

Infatti, il nuovo Regolamento sullo spazio europeo dei dati sanitari, dispone a favore dell'interessato il diritto ad accedere immediatamente e gratuitamente ai propri dati sanitari in formato facilmente leggibile, consolidato, e di scaricare una copia nel formato armonizzato europeo (art. 3). Come precisato dal *Considerando 9,* tale diritto si riferisce ai dati elettronici, lasciando impregiudicate altre modalità di accesso ai propri dati personali secondo la disciplina generale (es. diritto di chiedere una copia cartacea). Tale diritto, può tuttavia, essere limitato, su base nazionale, per maggior tutela della persona fisica, in particolare, della sua sicurezza e sulla base di considerazioni etiche, ritardandone temporaneamente l'accesso ai dati sanitari elettronici personali per garantire che un professionista sanitario possa comunicare e spiegare adeguatamente alla persona interessata il corretto significato clinico di tali dati (art. 3, § 5).

Quanto alle tipologie di dati sanitari cui si riferisce il diritto in parola, esse sono indicate all'art. 14, salvo il potere degli Stati di prevederne altre con legislazione nazionale. Si tratta, in particolare dei dati relativi a profili sanitari sintetici dei pazienti, prescrizioni elettroniche, esenzioni, esami

diagnostici per immagini e relativi referti di immagini, risultati degli esami medici, compresi i risultati di laboratorio e altri risultati diagnostici e relativi referti, lettere di dimissione.

L'accesso ai dati personali elettronici da parte dei soggetti interessati, loro delegati o rappresentanti legali avviene attraverso servizi di accesso organizzati dagli stati membri, e in virtù di un formato europeo di scambio delle cartelle cliniche elettroniche, le cui caratteristiche tecniche saranno elaborate dalla Commissione entro due anni dall'entrata in vigore del Regolamento (art. 15).

Oltre al diritto di accedere ai propri dati, e di avere informazioni sugli accessi da parte dei prestatori di servizi sanitari ad essi (art. 9), gli interessati hanno anche quello di intervenire su di essi e inserire dati volontariamente; in questo caso, poiché queste modifiche non avvengono sotto la supervisione di un professionista della salute, i dati volontariamente immessi devono essere distinti da quelli inseriti dai sanitari (art. 5).

Anche il diritto di rettifica, già previsto dal GDPR, può essere esercitato attraverso i servizi di accesso: in questo caso, il titolare dei dati può far verificare la richiesta di rettifica da un sanitario (art. 6).

L'interessato ha, inoltre, il diritto alla portabilità dei dati, che si sostanzia nella possibilità di richiedere il trasferimento ad altra struttura sanitaria (o identificato servizio sociale o di rimborso) gratuitamente e senza ritardi, anche in altri stati, utilizzando l'infrastruttura transfrontaliera e il formato europeo di scambio della cartelle cliniche elettroniche (art. 7).

Degno di nota è il diritto di limitare l'accesso ai propri dati sanitari elettronici agli stessi sanitari, senza che ciò sia noto a costoro, e con l'avvertimento che una tale limitazione può compromettere la prestazione del servizio (art. 8).

Gli stati membri *possono* attribuire un diritto (reversibile) di "opt-out" dall'accesso ai dati personali elettronici; l'accesso può essere comunque dato al sanitario in casi di emergenza ex art. 9 (2), lett. c), GDPR. Infine, è data possibilità agli stati membri di stabilire regole per disciplinare le tipologie di dati accessibili da differenti operatori sanitari, prevedendo, così degli accessi differenziati (art. 11).

Gli Stati membri identificano una o più "autorità di sanità digitale" come autorità di riferimento e coordinamento tra piano nazionale ed Europeo, che collabori con le altre Autorità di settore (Garante per la protezione dei dati personali, AGCOM ecc.), e che curi l'implementazione tecnica e la diffusione delle informazioni. Tale autorità (o quella eletta di riferimento nel caso fossero più d'una) è tenuta a presentare un *report* biennale sulla propria attività e sui punti di cui all'art. 20.

Gli interessati hanno diritto di presentare reclamo alla "autorità di sanità digitale" per questioni relative all'adempimento degli obblighi e l'esercizio dei diritti sopra menzionati e, nel caso di questioni relative ai dati personali per le quali è competente l'autorità Garante per la protezione dei dati personali, ad essa vengono trasmessi gli atti a cura della autorità di sanità digitale stessa (Art. 21). A quest'ultima autorità è attribuito il compito di vigilare sull'applicazione del Regolamento sullo spazio europeo dei dati sanitari quanto ai diritti degli interessati in merito ai propri dati personali sanitari elettronici.

Infine, quanto alla struttura transfrontaliera per garantire accesso ai dati nell'ambito di prestazioni sanitarie svolte in stati differenti, è prevista l'uso della piattaforma "MyHealth@EU" – da istituirsi secondo specifiche tecniche individuate dalla Commissione entro due anni dall'entrata in vigore del Regolamento – per l'implementazione dei servizi e degli scambi transfrontalieri di dati sanitari elettronici a cura dei punti di contatto" istituiti a livello nazionale.

Questi ultimi costituiscono riferimenti organizzativi e tecnici per i servizi di scambio transfrontaliero dei dati sanitari nel contesto dell'uso primario. In questa veste, quanto alle categorizzazioni di *data protection*, essi agiscono quali contitolari del trattamento per i dati personali sanitari per i trattamenti in cui sono coinvolti, mentre la Commissione agisce quale responsabile del trattamento (art. 23, § 7). Attraverso la medesima piattaforma, gli stati membri possono organizzare la prestazione di ulteriori servizi sanitari, quali, ad esempio, quelli legati alla telemedicina, la sanità mobile, i certificati sanitari, vaccinali e ulteriori servizi di vigilanza della sanità pubblica (art. 24).

Requisito essenziale per tutte le funzioni sopra elencate è l'interoperabilità e la compatibilità software per la costituzione, la registrazione e la gestione dei dati all'interno della cartelle cliniche elettroniche. Per tali ragioni tutti i dispositivi e le applicazioni per la salute che producono dati da inserire nello spazio europeo devono dimostrare la propria conformità ai componenti relativi secondo le indicazioni armonizzate europee e ciò vale anche in particolare per i dispositivi medici, medico-diagnostici in vitro e i sistemi di IA ad alto rischio (art. 27).

L'utilizzo di sistemi di intelligenza artificiale, quindi, per applicazioni dedicate alla generazione di dati sanitari elettronici deve mostrare conformità a questi standard tecnici che si aggiungono a quelli previsti nell'*AI Act*. L'art. 36 contiene delle indicazioni generali circa i contenuti di specifiche comuni a questi sistemi e dispositivi e che la Commissione dovrà emanare.

Secondo uno schema simile a quello contenuto nell'*AI Act* per i sistemi di intelligenza artificiale ad alto rischio, sono presenti obblighi per fornito-

ri, importatori e distributori di sistemi di cartelle cliniche elettroniche che includono la necessità di dettagliata documentazione tecnica, dichiarazione di conformità e apposizione del marchio CE (artt. 36-42), nonché l'individuazione di autorità di vigilanza del mercato che, in particolare, controllino che i sistemi di cartelle cliniche elettroniche non presentino rischi per la salute, la sicurezza, i diritti delle persone e la protezione dei dati personali (artt. 43, 44).

5.4. L'uso "secondario"

La parte sicuramente più significativa e delicata del Regolamento riguarda, come già accennato, la possibilità di usare i dati sanitari elettronici per finalità diverse da quelle relative all'uso primario, vale a dire per scopi che abbiamo già indicato e che non hanno a che fare con la prestazione di servizi per la cura o il miglioramento della salute[31].

Questa parte dell'atto normativo disciplina, in particolare, i soggetti tenuti alla condivisione dei dati sanitari elettronici, le condizioni e le finalità per il loro utilizzo secondario, le modalità con le quali essi sono accessibili e le tutele relative; le infrastrutture transfrontaliera e di *governance* per la condivisione nello spazio europeo (e, in taluni casi anche a soggetti terzi al di fuori di esso).

Quanto ai soggetti, essi sono individuati nei "titolari dei dati sanitari" che sono definiti come le persone fisiche o giuridiche, le autorità pubbliche, le agenzie o altri organismi del settore dell'assistenza sanitaria o delle cure assistenziali, compresi i servizi di rimborso, nonché i soggetti che sviluppino prodotti o servizi destinati al settore sanitario, dell'assistenza sanitaria o delle cure assistenziali, sviluppino o fabbrichino applicazioni per il benessere, svolgano attività di ricerca in relazione al settore dell'assistenza sanitaria o delle cure assistenziali o fungano da registro della mortalità, nonché un'istituzione, un organo o un organismo dell'Unione che abbiano: i) il diritto o l'obbligo, conformemente al diritto dell'Unione o nazionale applicabile e in qualità di titolare o contitolare del trattamento, di trattare dati sanitari elettronici personali per la prestazione di assistenza sanitaria o cure assistenziali o a fini di sanità pubblica, rimborso, ricerca, innovazione, definizione delle politiche, statistiche ufficiali o sicurezza dei pazienti o a fini di regola-

31. Frias I.S., *Secondary Uses of Health Data Under the European Health Data Space. Connections with the Gdpr and the Impact of AI* (April 01, 2024). Available at SSRN: *https://ssrn.com/abstract=5050843.*

mentazione; o la capacità di rendere disponibili dati sanitari elettronici non personali, mediante il controllo della progettazione tecnica di un prodotto e dei servizi correlati, anche in termini di registrazione, fornitura, limitazione dell'accesso o scambio (art. 3, § 2, lett. t).

Come si vede, in buona sostanza, si tratta di tutti i soggetti pubblici o privati che abbiano in qualche modo a che fare con la prestazione di cura o di assistenza sanitaria, di gestione amministrativa o sviluppino prodotti o servizi a tali ambiti destinati.

In linea di principio, costoro hanno l'obbligo di mettere a disposizione per l'uso secondario una lunga serie di dati sanitari elettronici, indicati all'art. 51, tra i quali notiamo in particolare: dati sanitari elettronici provenienti da cartelle cliniche elettroniche; dati genetici, epigenomici e genomici umani; altri dati molecolari umani, quali quelli provenienti dalla proteomica, dalla trascrittomica, dalla metabolomica, dalla lipidomica e altri dati omici; dati sanitari elettronici personali generati automaticamente mediante dispositivi medici; dati provenienti dalle applicazioni per il benessere; dati provenienti da registri medici e da registri della mortalità; dati derivanti da ricerca o sperimentazione clinica; dati sanitari provenienti da biobanche e banche dati associate.

Degno di nota mi sembra anche l'obbligo di mettere a disposizione dati su fattori ritenuti incidenti sulla salute, compresi i determinanti socioeconomici, ambientali e comportamentali.

Posto che ai titolari dei dati sanitari è imposto un obbligo piuttosto gravoso, che si spinge fino al controllo e la segnalazione della presenza di dati protetti da proprietà intellettuale, e che si tratta di una enorme mole di dati, molti dei quali grandemente sensibili, il Regolamento stabilisce, alcune esenzioni e un regime di protezione caratterizzato dalla proibizione di alcuni usi e da una procedura controllata di accesso ai dati.

Quanto alle prime, sono esclusi dagli obblighi le persone fisiche, compresi i singoli ricercatori e le persone giuridiche considerate microimprese ai sensi dell'articolo 2, paragrafo 3, dell'allegato alla Raccomandazione 2003/361/CE della Commissione[32], salvo che gli stati nazionali dispongano diversamente per quei soggetti che rientrino nella loro giurisdizione (art. 50, § 2).

Quanto agli usi vietati (art. 54), si tratta di prescrizioni che si riferiscono agli utenti dei dati sanitari che hanno avuto accesso ad essi per uso secon-

32. Ai sensi di tale disposizione si definisce microimpresa un'impresa che occupa meno di 10 persone e realizza un fatturato annuo oppure un totale di bilancio annuo non superiori a 2 milioni di EUR.

dario attraverso le procedure indicate nel Regolamento. A costoro è proibito servirsi dei dati cui hanno avuto accesso per finalità e a condizioni diverse da quelle indicate negli atti autorizzatori.

Inoltre, è proibito l'accesso e il trattamento dei dati per prendere decisioni pregiudizievoli verso una persona o un gruppo che abbiano effetti giuridici o che incidano significativamente su di essi; offrire condizioni di sfavore nell'ambito del mercato del lavoro, dell'offerta di servizi assicurativi o creditizi, di prodotti o servizi, o discriminatorie sulla base di dati sanitari; per finalità di marketing; per danneggiare la sanità pubblica o la salute delle persone, ad esempio sviluppando prodotti nocivi.

Infine, quanto ai meccanismi di accesso, il Regolamento prevede l'istituzione da parte degli stati membri di organismi pubblici di accesso ai dati sanitari, che possono essere costituiti *ex novo* o essere le relative funzioni assegnate ad organismi esistenti purché sia garantita l'assenza di conflitti di interesse, siano forniti mezzi e personale adeguato e create le condizioni di collaborazione con i portatori di interessi, quali associazioni dei pazienti ecc. (art. 55). Quando i titolari dei dati siano istituzioni o organismi europei, sarà la Commissione a svolgere le funzioni di organismo di accesso ai dati sanitari.

Gli organismi di accesso ai dati svolgono una serie molto complessa di funzioni che sono indicate negli artt. 57-59 del Regolamento. Si tratta di tutte le attività connesse alla raccolta dei dati da parte dei titolari sopra indicati, della gestione delle richieste di accesso ai dati, del monitoraggio degli usi in conformità con il Regolamento, di comunicazione e di informazione pubblica circa le modalità di accesso e delle tipologie di dati accessibili, di gestire l'accesso transfrontaliero, tramite la piattaforma *HealthData@EU*, di cooperazione con l'Unione e gli stati nazionali per l'elaborazione di specifiche tecniche comuni adeguate, di collaborazione con le varie autorità di controllo. Sono titolari, inoltre, della gestione dei reclami in merito a violazioni relative alle disposizioni sull'uso secondario, a meno che non siano di competenza dell'autorità Garante della protezione dei dati personali cui, in questo caso, dovranno essere inviati gli atti (art. 81).

La competenza a decidere circa la richiesta di accesso per uso secondario è dell'organismo responsabile presso il quale è iscritto il titolare dei dati (art. 76).

Sono previsti una serie di obblighi stringenti per i titolari dei dati, ma anche per gli utenti dei dati; obblighi la cui violazione può portare a sanzioni amministrative di particolare gravità. Quanto agli utenti, oltre ad utilizzare i dati cui hanno avuto accesso negli stretti limiti di cui agli atti autorizza-

tori, essi devono, inoltre, tra le altre cose, impedire l'accesso ai dati a terzi, rendere pubblici il risultati degli usi svolti in forma anonima e non devono re-identificare le persone dei cui dati si tratti (art. 61).

Quest'ultima violazione è tra quelle più gravemente sanzionate (fino a 20 000 000 € o il 4% del fatturato mondiale totale annuo se superiore, art. 64).

Interessante è il rapporto tra queste ultime prescrizioni e quelle che impongono agli organismi di accesso di fornire tale facoltà solo ai dati necessari per la finalità per la quale sono richiesti e in forma anonima. Solo laddove sia dimostrato da parte del richiedente l'impossibilità di conseguire tale finalità mediante dati anonimi, l'organismo fornirà una versione comunque pseudonimizzata, trattenendo per sé le informazioni che consentono di ricostruire l'identità delle persone dei cui dati si tratti (art. 66, §§ 2-3). Questo significa che, di fatto, l'utente ottiene sempre e solo dati che, per lui, sono anonimi non potendo disporre delle informazioni idonee ad invertire la pseudonimizzazione. Si comprende, quindi, la ragione della gravità delle sanzioni minacciate per i tentativi di re-identificazione: questi ultimi evidentemente non possono che essere dolosi e sfruttare tecniche di identificazione indiretta.

L'obbligo imposto, a pena di sanzioni, sui titolari dei dati di mettere a disposizione i dati sanitari elettronici implica la possibilità di una maggior accessibilità dei dati sanitari dei pazienti e dei soggetti ultimi destinatari delle prestazioni sanitarie. Il Regolamento riconosce a questi ultimi il diritto di escludere che i propri dati siano resi accessibili per usi secondari sebbene sia data la facoltà agli stati di prevedere norme che, di fatto, ridimensionano grandemente tale diritto. Il diritto nazionale può, infatti, prevedere che alle autorità che esercitano compiti nel settore della sanità pubblica, sia dato comunque accesso ai dati dei soggetti che hanno richiesto l'esclusione se ricorrono le condizioni previste dall'art. 71, § 4.

Leggendo tali ipotesi, non può non aversi l'impressione di uno svuotamento del diritto di esclusione e di una indubbia cessione delle ragioni dell'autonomia del singolo rispetto alle esigenze pubbliche. Infatti, i casi in parola hanno a che fare con la definizione di politiche normative; con l'interesse pubblico nella protezione di gravi minacce, la sicurezza dei prodotti e dispositivi, la garanzia di elevati livelli sanitari; con l'attività statistica ufficiale. Inoltre, significativamente, l'accesso può essere garantito quando i "dati non possono essere ottenuti con mezzi alternativi in modo tempestivo ed efficace in condizioni equivalenti" (*sic!*) e quando il richiedente abbia fornito le giustificazioni richieste dal diritto nazionale che autorizzi la deroga al diritto di esclusione.

Non v'è chi non veda come, in particolare queste ultime condizioni, possano consentire, di fatto, una riduzione significativa del diritto di esclusione. Il legislatore europeo, quindi, di fatto, ammette la possibilità di regimi nazionali più o meno indulgenti verso la *privacy informazionale sanitaria* del singolo, che, però, possono arrivare fino ad un suo completo esautoramento.

L'accesso per uso secondario in un contesto transfrontaliero è reso possibile attraverso il sistema *HealthData@EU*, un assetto di punti di contatto nazionali che agiscono quali contitolari del trattamento per le operazioni cui partecipano e una piattaforma da costituirsi ad opera della Commissione Europea che agirà, invece, da responsabile del trattamento (art. 75).

Informazioni circa le serie di dati raccolti e disponibili a livello nazionale ed europeo devono essere rese pubbliche; le serie di dati possono essere munite di un marchio di qualità ed utilità che le rappresenta in una scala che ne rende così immediatamente evidente il valore (*Considerando 85*).

La correttezza dell'apposizione di tale marchio da parte dei titolari dei dati è rimessa al controllo degli organismi di accesso, cui devono essere fornite tutte le dovute informazioni (art. 60, § 4). I parametri di valutazione per la configurazione del livello di qualità e utilità sono relativi, tra le altre cose, alla documentazione, ai processi di gestione, alla valutazione della copertura, la qualità tecnica (art. 78) e devono coordinarsi con quanto previsto dalle disposizioni dell'*AI Act,* sulla qualità dei processi di gestione dei dati (art. 10; all. IV).

5.5. Osservazioni conclusive

Un aspetto che emerge dal Regolamento e che sembra di particolare interesse è la valorizzazione non solo delle ovvie opportunità ma anche e soprattutto dei pericoli connessi alla circolazione dei dati *non* personali.

Sembra, cioè, che si stia finalmente affermando una maggiore consapevolezza in relazione ad una distinzione che forse, troppo semplicisticamente, era stata in passato sopravvalutata, quasi a ritenersi che una volta predisposta una rigida e sorvegliata disciplina per il trattamento dei dati *personali,* fosse con ciò stesso garantita pienamente la protezione dei diritti persone fisiche.

Invero, la classificazione tra i dati personali, con l'assoggettamento alla relativa normativa, anche delle informazioni che possano identificare la persona fisica *indirettamente* (art. 4, n. 1, GDPR) ha sempre creato difficoltà

pratiche, posto che lo studio tecnico ha mostrato più volte la possibilità di reidentificare i soggetti a partire da dati anonimi e apparentemente sicuri. Sicché la distinzione è sempre apparsa vaga quanto alla capacità di rappresentare una prassi, resa sempre più complessa dal fatto che, ormai, la datificazione della persona è diuturna, estremamente granulare e che l'immagine di un soggetto in una condizione di "sovranità" informazionale consapevole di *tutti* i trattamenti relativi a *tutte* le informazioni che lo riguardano in un modo o nell'altro è una pura astrazione utopica.

La sensazione di una sottovalutazione della pericolosità dei dati non personali era aggravata dallo stesso legislatore europeo che quando il GDPR era appena divenuto applicabile, ha emanato il Regolamento 2018/1807 relativo per l'appunto alla disciplina dei dati *non* personali che adottava per essi un principio opposto a quello del GDPR, vale a dire, incoraggiando la circolazione mediante la proibizione della "localizzazione" dei dati (salve ragioni di sicurezza pubblica, art. 4).

Il tema dei pericoli connessi alla reidentificazione a partire da dati resi anonimi, compare, invece, sempre più frequentemente nel corso degli ultimi anni. Così il Regolamento 2022/868 (*Data Governance Act*), che disciplina, tra le altre cose, le condizioni per il riutilizzo, all'interno dell'Unione, di determinate categorie di dati detenuti da enti pubblici, prevede il divieto per i riutilizzatori di reidentificare gli interessati cui si riferiscono i dati e l'obbligo di adottare misure tecniche e operative per impedire la reidentificazione, nonché di notificare all'ente pubblico qualsiasi violazione dei dati che comporti la reidentificazione degli interessati (art. 5). Inoltre esso prevede che specifici atti legislativi dell'Unione possono qualificare determinate categorie di dati non personali come altamente sensibili, laddove il loro trasferimento a paesi terzi possa, tra l'altro, comportare il rischio di una reidentificazione dei dati non personali anonimizzati. In questo caso la Commissione può adottare atti delegati per stabilire condizioni particolari applicabili ai trasferimenti di tali dati verso paesi terzi (§ 13).

Analogamente, l'art. 32, § 3, del Regolamento 2023/2854 (*Data Act*) prevede che nel caso di sentenza o ordine amministrativo provenienti da un paese terzo di trasferire dati non personali che possano determinare un conflitto tra il destinatario e il diritto dell'Unione o nazionale, in assenza di un accordo internazionale, tale trasferimento potrà avvenire solo a determinate condizioni che possono essere fatte verificare dall'autorità nazionale competente per la cooperazione giudiziaria internazionale in particolare quando vi sia, tra l'altro, il pericolo di reidentificazione.

Il tema è, infine, particolarmente presente nel Regolamento Europeo per la costituzione dello spazio dei dati sanitari, il quale, oltre ai divieti e alle sanzioni già viste, particolarmente gravi per l'ipotesi di reidentificazione, dispone che tali dati siano considerati altamente sensibili ai sensi del già visto *Data Governance Act* ove il loro trasferimento verso paesi terzi presenti un rischio di reidentificazione attraverso mezzi che vanno oltre quelli di cui è ragionevolmente probabile che ci si avvalga, in particolare alla luce del numero limitato di persone fisiche alle quali tali dati sono relativi, del fatto che sono disperse a livello geografico o degli sviluppi tecnologici previsti nel prossimo futuro (art. 88).

Ci si può attendere che questo sarà un tema particolarmente delicato e foriero di numerose controversie.

In conclusione il Regolamento si inserisce in un assetto normativo già molto ricco con il quale dovrà essere coordinato e imporrà una sorta di "educazione" alla condivisione dei dati, non a caso esso prevede obblighi formativi e di alfabetizzazione digitale per gli operatori della sanità coinvolti dalle disposizioni emanate.

Il quadro che ne esce, unito all'evoluzione delle infrastrutture di collegamento, elaborazione e trasferimento dei dati di cui si è detto all'inizio di questa trattazione, presenta un'idea del volto della sanità del futuro e delle complicate rappresentazioni che sarà necessario comporre per valutare la sussistenza delle fattispecie giuridiche in gioco quando qualche disfunzione inevitabilmente si produrrà.

6. L'applicazione dell'Intelligenza Artificiale nel settore sanitario: una rassegna

Nel complicato contesto sopra evidenziato viene a collocarsi oggi il tema dell'utilizzo dell'intelligenza artificiale nel settore sanitario che può trovare applicazione pressoché in ogni ambito della cura e del miglioramento della salute, dalla ricerca alla clinica, alla organizzazione dei mezzi e delle strutture.

Volendo, senza pretesa di esaustività, indicare alcuni dei principali utilizzi che la letteratura sta suggerendo potremmo qui considerare i seguenti.

a) Aspetti gestionali, quali la gestione del personale, delle documentazioni, delle forniture e delle manutenzioni

Gli aspetti organizzatori generali possono essere efficientati con l'ausilio di strumenti di analisi avanzata dei dati, di previsione e di modelli linguistici

per ottenere potenzialmente una serie di benefici[33]. Tra le applicazioni già in uso possiamo trovare senz'altro quelle dedicate ad adiuvare la fase di *recruiting* e, quindi della selezione del personale, amministrativo, medico e infermieristico, in particolare per le realtà operanti nel settore privato, per le quali possono essere più rapidamente implementabili. Nel settore pubblico, tali strumenti dovrebbero essere integrati nelle procedure di selezione e dovrebbero quindi avere un esplicito supporto normativo[34]. Sul punto va ricordato che, da un lato, in linea di principio, l'utilizzo di strumenti di decisione totalmente automatizzata in casi del genere deve rispettare le disposizioni di cui all'art. 22 GDPR, che stabilisce, di principio, un divieto (§ 1), derogabile solo in presenza di determinate condizioni (§ 2) e purché siano garantite adeguate misure di protezione delle libertà, dei diritti e degli interessi legittimi dei destinatari (§ 3). Inoltre, il nuovo Regolamento UE sull'intelligenza artificiale colloca i sistemi utilizzati in questo ambito tra quelli considerati "ad alto rischio", per i quali deve essere garantita la sorveglianza umana (art. 14). Se, e con che limiti, tale previsione che, di fatto, prevede la presenza attiva di una persona fisica nel monitoraggio del sistema con autorità e potere di interropmpere il processo automatico e di modificarne la decisione nel caso singolo, escluda – perciò – sempre e comunque l'applicabilità dell'art. 22 GDPR (che presuppone un totale automatismo), è discusso in letteratura[35]. Vi sono ragioni per ritenere che con l'approvazione dell'*AI Act* l'interpretazione del § 1 del citato articolo debba essere rivista giacché quella tradizionale porterebbe verso la disapplicazione dell'art. 22 ogniqualvolta si sia di fronte ad un sistema ad alto rischio che prenda decisioni che abbiano effetti giuridici o che incidano significativamente sulla persona. In questi casi, infatti, la prevista necessità della supervisione umana renderebbe sempre inapplicabile la disciplina dell'art. 22, ivi inclusa quella relativa alle *safeguard measures* per il caso di deroga al divieto di cui al § 1. Ma poiché si può dubitare che l'*AI Act,* nonostante tutto, offra al destinatario una protezione equivalente, tale conclusione interpretativa deve essere valutata con molta cautela.

---

33. García F. *et al*., *Transforming healthcare with AI*, EIT Health and McKinsey Company, 2020, *https://eithealth.eu/wp-content/uploads/2020/03/EIT-Health-and-McKinsey_Transforming-Healthcare-with-AI.pdf*, p. 73.

34. In modo analogo a come è accaduto con la riforma della disciplina degli appalti pubblici con il d. Lgs. 36/2023 che ha previsto "Per migliorare l'efficienza, le stazioni appaltanti e gli enti concedenti provvedono, ove possibile, ad automatizzare le proprie attività ricorrendo a soluzioni tecnologiche, ivi incluse l'intelligenza artificiale e le tecnologie di registri distribuiti, nel rispetto delle specifiche disposizioni in materia" (art. 30).

35. Cfr. Sarra C., *Artificial Intelligence in Decision-making*, cit.

Appare possibile, in effetti, un'interpretazione aggiornata dell'art. 22, § 1, GDPR che ne concili le esigenze di tutela con il principio di supervisione umana per come espresso nell'*AI Act*, che renda entrambi i regolamenti applicabili nei casi generali in cui la decisione – presa sulla base di elaborazione di dati personali – sia sostanzialmente determinata dalla macchina.

La nuova interpretazione dovrebbe esplicitare le condizioni in cui l'esercizio della supervisione umana è così mirato da escludere che la decisione sia "basata unicamente su un trattamento automatizzato", dato che il mero monitoraggio generale del sistema e il possesso astratto della competenza per fare diversamente non sembrano sufficienti. Questo potrebbe essere realizzato interpretando l'espressione "basata unicamente su un trattamento automatizzato" nell'art. 22, § 1, in un modo che richieda un coinvolgimento specifico e materiale della persona qualificata alla supervisione affinché il caso possa ritenersi escluso dall'ambito di applicazione di tale disposizione.

Sarebbe opportuno, dunque, ritenere che, ai sensi dell'art. 22, § 1, GDPR, una decisione – che abbia effetti giuridici o che incida significativamente in modo analogo sul destinatario – sia considerata completamente automatizzata ogniqualvolta sia presa da una macchina, *nonostante la presenza di una persona qualificata che ne monitora il funzionamento*, a meno che non sia dimostrato che essa sia effettivamente intervenuta in modo specifico e materiale nel processo decisionale individuale con atti significativi in modo che, in assenza di essi, la decisione sarebbe stata diversa[36].

Va inoltre ricordato che lo stesso *AI Act* prevede per le decisioni *supportate* da sistemi di IA "ad alto rischio" (dunque, non necessariamente del tutto automatizzate), il diritto ad avere "spiegazioni chiare e significative sul ruolo del sistema di IA nella procedura decisionale e sui principali elementi della decisione adottata" (art. 86). Sicché, il c.d. "diritto di spiegazione", la cui presenza nel GDPR è stata tanto discussa all'indomani della sua approvazione, trova così esplicito riconoscimento nelle nuove disposizioni normative.

L'intelligenza artificiale, assieme a strumenti che sfruttano la virtualizzazione può intervenire, poi, nella formazione mirata del personale preparandolo per differenti scenari[37]. In questo senso, oltre alla preparazione specifica relativa al settore medico (o amministrativo) di appartenenza, può immaginarsi l'utilizzo per implementare una più accurata formazione gene-

36. *Ibidem.*

37. Zhang W., Cai M., Lee H.J. *et al., AI in Medical Education: Global situation, effects and challenges,* in *Education and Information Technologies,* 2024, 29, pp. 4611 ss.

rale relativa alla sicurezza sui luoghi di lavoro, nonché le buone pratiche e i codici etici adottati dall'organizzazione.

La gestione dei turni, la limitazione delle operazioni ripetitive – sempre più affidabili direttamente all'IA – nonché la rotazione nelle varie mansioni possono essere efficientate garantendo, così, migliore produttività, riducendo lo *stress* e garantendo adeguati tempi di recupero, specialmente in relazione al lavoro notturno, essenziale nelle strutture di ricovero e cura.

L'individuazione di *trend* di consumo in correlazione con eventi ordinari e straordinari possono, poi, migliorare l'organizzazione dell'approvvigionamento delle risorse, mentre l'adozione di modelli di linguaggio può perfezionare la redazione dei documenti amministrativi, l'analisi e la loro gestione.

A questo proposito, può senz'altro segnalarsi la possibilità di utilizzare i *language models* per una resa più ampiamente comprensibile dei documenti medici e ospedalieri a favore dei pazienti, aggiungendo automaticamente alle indicazioni tecniche una sorta di parafrasi semplificata ed esplicatoria. Tale introduzione gioverebbe senz'altro alla crescita e al mantenimento di un rapporto di fiducia consentendo al paziente di sentirsi incluso sempre di più nella relazione di cura, specialmente nelle situazioni in cui abbisogni di prestazioni di alta specialità i cui referti sono spesso a lui incomprensibili. Tale possibilità, potenzierebbe l'autonomia del paziente e potrebbe costituire uno strumento efficace per rafforzare l'alleanza terapeutica con il medico.

L'utilizzo della virtualizzazione e dell'IA possono divenire importanti, inoltre, per il perfezionamento delle esigenze di manutenzione di edifici, dei dispositivi e dei macchinari: l'utilizzo di *digital twins,* in particolare*,* può consentire delle previsioni più accurate sulle attese in termini di *performance* e di durabilità, suggerendo le migliori pratiche per assecondare il loro ciclo vitale[38].

b) Accesso e organizzazione delle prestazioni e dei servizi; telemedicina

Sebbene l'utilizzo di varie forme di automazione delle prenotazioni e di gestione degli appuntamenti siano già in uso, in particolare attraverso l'utilizzo di piattaforme che consentono di svolgere tali operazioni *online,*

38. Un *Digital Twin* è un insieme di costrutti informativi virtuali che descrivono completamente un elemento fisico, sia potenziale che reale, a partire dal livello microatomico fino al livello macro-geometrico. Nella sua forma ottimale, qualsiasi informazione ottenibile dall'ispezione di un prodotto fisico può essere ottenuta dal suo *Digital Twin*, Cfr. Grieves M., Vickers J., *Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Complex Systems*, in Kahlen J., Flumerfelt S., Alves A. (eds), *Transdisciplinary Perspectives on Complex Systems*, Springer, Cham 2017.

l'utilizzo dell'IA, può divenire un fattore di efficientamento importante. Va ricordato che i sistemi di IA destinati a essere utilizzati dalle autorità per valutare l'ammissibilità delle persone fisiche alle prestazioni e ai servizi di assistenza pubblica essenziali, compresi i servizi di assistenza sanitaria, nonché per concedere, ridurre, revocare o recuperare tali prestazioni e servizi, sono classificati, anch'essi, come "ad alto rischio" dall'Allegato III del Regolamento UE sull'intelligenza artificiale. Sicché, per essi, devono trovare applicazioni le più gravose disposizioni che tale atto prevede con riferimento alla catena del valore relativa alla loro messa in opera e gestione.

Tra queste – come già accennato – sono incluse quelle relative agli obblighi di predisporre un efficace sistema di sorveglianza umana (art. 14), sicché vale in questo caso quanto già riferito *supra* in merito al raccordo tra la disciplina ex art. 22 GDPR e l'art. 14 *AI Act*.

Negli ultimi anni si è assistito, poi, ad un aumento della letteratura relativa all'utilizzo di strumenti di intelligenza artificiale per le operazioni di *triage* sebbene una recente revisione generale abbia mostrato come gli studi siano per lo più incentrati sull'elaborazione di *tools* e di valutazione delle *performance* secondo metriche di ricerca ma senza rappresentare il punto di vista dei pazienti o degli stessi operatori sanitari con una informazione molto limitata sui fattori che possano facilitare o ostacolare l'introduzione di questi sistemi di IA. I risultati sullo stato della ricerca in questo settore mostrano un ambito relativamente nuovo e ancora poco sviluppato, condotto principalmente in un ambiente di ricerca non clinico di prototipazione, sviluppo e valutazione[39].

Quanto alla telemedicina, le innovazioni nella comunicazione e nella disponibilità di strumenti di monitoraggio a distanza ed anche indossabili, assieme agli sviluppi di approcci immersivi e di aumento della realtà suggeriscono varie applicazioni, potenzialmente rivoluzionarie in un tempo in cui aumenta la richiesta sanitaria, per l'invecchiamento della popolazione e l'aumento delle malattie croniche. In primo luogo, la telemedicina dotata di monitoraggio remoto avanzato e di analisi predittiva guidata dall'intelligenza artificiale promette un controllo più efficace degli stati patologici cronicizzati. Questo approccio ha il potenziale per ridurre significativamente le ospedalizzazioni e migliorare i risultati dei pazienti, offrendo agli individui una qualità di vita più elevata. In secondo luogo, i programmi di *tele-ICU* sono pronti ad espandersi, mettendo in contatto gli intensivisti con i pazienti

39. Queste le conclusioni in Sira E. *et al., Mapping and Summarizing the Research on AI Systems for Automating Medical History Taking and Triage: Scoping Review,* in *Journal of Internet Medical Research,* 2025, 27, pp. 1-17.

in terapia intensiva in località remote e poco servite. Questo approccio è destinato a migliorare la qualità dell'assistenza in regioni che tradizionalmente hanno dovuto affrontare problemi di accessibilità all'assistenza sanitaria. In terzo luogo, la telemedicina è in grado di facilitare le collaborazioni internazionali e le iniziative di salute globale. Gli esperti di tutto il mondo potranno fornire indicazioni e interventi medici essenziali in aree con infrastrutture sanitarie limitate, favorendo una distribuzione più equa delle competenze mediche. Infine, si sperimentano forme di teleterapia, con *chatbot* per l'auto-aiuto psicologico guidati dall'intelligenza artificiale che offrono un supporto immediato alle persone in difficoltà. Inoltre, gli ambienti di realtà virtuale sono destinati creare le condizioni per interventi terapeutici, anche nell'ambito della salute mentale rispondendo alle diverse esigenze dei pazienti[40].

Va da sé, che la virtualizzazione e il miglioramento delle condizioni tecniche per le esperienze immersive possono portare beneficio anche nello studio dei comportamenti e delle reazioni di pazienti in condizioni cognitive alterate – magari per lo sviluppo di forme di demenza senile, o per l'insorgere di patologie mentali – in differenti contesti e condizioni ambientali garantendo al contempo ampiezza di informazioni e massima sicurezza.

c) Diagnostica, terapeutica, assistenza infermieristica

Le considerazioni avanzate da ultimo ci introducono al tema dell'utilizzo di forme di intelligenza artificiale nel potenziamento degli strumenti di diagnostica, in particolare mediante l'analisi avanzata dei dati forniti dagli strumenti. Pensiamo a sistemi di *pattern recognition* per l'individuazione precoce dei fattori associati all'insorgere o al peggiorare di una patologia applicati alla diagnostica per immagini[41]. O l'individuazione di correlazioni meno studiate finora ed emergenti dall'analisi di dati provenienti da riscontri diagnostici eterogenei[42].

Questo tipo di applicazioni sono sicuramente tra quelle attualmente più discusse e sperimentate e, poiché, quando applicate alla clinica, sono diret-

40. Omaghomi T.T., Elufioye O.A., Akomolafe O. *et al., A Comprehensive Review of Telemedicine Technologies: Past, Presente, Prospects,* in *International Medical Science Research Journal*, 2024, vol. 4, 2, pp. 183-193 (188).

41. Cheng P., Montagnon E. *et al.*, *Deep Learning: An Update for Radiologists*, in *RadioGraphics*, 2021, vol. 41, 5, pp. 1427-1445; Rosen S., Mor S., *Evaluating the Reliability of ChatGPT as a Tool for Imaging TestCheng P.Referral: A Comparative Study with a Clinical Decision Support System*, in *European Radiology,* 2023, vol. 34, 5, pp. 2826-2837.

42. Belard A. *et al*., *Precision Diagnosis: A View of the Clinical Decision Support Systems (CDSS) Landscape through the Lens of Critical Care*, in *Journal of Clinical Monitoring and Computing,* 2017, vol. 31, 2, pp. 261–271.

tamente connesse alla formulazione della decisione medica, esse sono idonee a mettere direttamente in gioco il rapporto medico-paziente toccando, quindi, il punto focale del rapporto di cura, con i suoi risvolti giuridici, etici e deontologici.

Tra le molte questioni problematiche che incidono su questo aspetto, quelle legate alla *opacità* dei sistemi più complessi sono sicuramente tra le più problematiche.

L'opacità collegata a sistemi di elaborazione intelligente appare essere il prodotto di tre fattori: complessità del codice con cui la macchina è programmata, alta dimensionalità dei dati, vale a dire la capacità del sistema di "gestire" milioni di variabili, e nei casi di macchine con capacità di apprendimento, mutevolezza della logica decisionale, giacché i valori di elaborazione della determinazione individuale sono "aggiustati" autonomamente dall'artefatto[43].

L'opacità costituisce un problema molto serio in tutte le situazioni nelle quali non è sufficiente poter garantire – entro delle metriche di efficienza ed accuratezza – un certo comportamento della macchina ma è essenziale poter anche fornire un elevato livello di trasparenza quale base per mostrare compiutamente "perché" essa, in un caso specifico, si è determinata in una data modalità. Ed è ovvio che la decisione su una controversia in merito alla potenziale lesione di diritti fondamentali prodotta dall'azione dell'artefatto richiede un elevato livello di trasparenza.

Nel caso della responsabilità medica, tale questione incide in primo luogo – naturalmente – nel caso dell'errore diagnostico, vale a dire la situazione nella quale il medico formuli una diagnosi supportata da un sistema tale per cui non si sia nella condizione di esplicitare tutte le ragioni che hanno condotto l'artefatto a suggerire una certa individuazione patologica che si riveli errata con conseguenze dannose per il paziente.

Ma, poi, l'opacità rileva anche per il fatto che essa preclude o limita fortemente sia la possibilità di esprimere un consenso realmente informato, sia la possibilità di scelta del paziente, nell'ipotesi che le correlazioni individuate non siano trasparenti e, dunque, non consentano di essere discusse oltre un certo grado.

In generale, sebbene gli algoritmi di *machine learning* si siano dimostrati strumenti preziosi per la diagnosi medica, è concordemente ritenuto che non debbano sostituire l'esperienza e il giudizio umano. Tali strumenti si basano sui dati su cui sono stati addestrati e, di conseguenza potrebbero

43. Burrell J., *How the machine 'thinks:' Understanding opacity in machine learning algorithms*, in *Big Data & Society*, 2016, vol. 3, 1, pp. 1-12.

non considerare tutti i fattori rilevanti nel processo diagnostico del caso specifico. Inoltre, questi algoritmi non sono infallibili e possono commettere errori, sicché la letteratura insiste affinché l'approccio uomo-macchina sia di tipo collaborativo è che gli operatori sanitari esercitino cautela, rivedendo e verificando i risultati generati dai sistemi per garantire diagnosi accurate e affidabili[44].

Va detto, però, che la limitazione dell'uso di tali strumenti al supporto della decisione umana non appare sufficiente ad eliminare tutte le problematiche connesse. In particolare, non va sottovalutata la possibilità che la collaborazione uomo-macchina aggravi le situazioni di *medicina difensiva,* vale a dire di quei comportamenti e di quelle decisioni prese dai sanitari in contesti di cura e giustificate dalle preoccupazioni di precostituirsi una difesa efficace nei giudizi di responsabilità piuttosto che il miglior interesse del paziente[45]. Infatti, la riconosciuta possibilità di dissociarsi dalla valutazione dell'artefatto rischia di non essere sufficiente ad impedire tali comportamenti quando il sanitario che effettivamente lo faccia in scienza e coscienza sia, poi, in caso di esito comunque infausto o dannoso, chiamato a giustificare le ragioni che lo hanno condotto a non fare affidamento su una macchina che, magari, presenta sulla carta coefficienti di performatività particolarmente elevati.

Oltre alla diagnostica, l'IA può intervenire, naturalmente, sulla terapeutica. Oltre all'ausilio nel dosaggio personalizzato e magari variabile di farmaci attraverso l'analisi continuativa dei dati del paziente laddove, magari, accessibili con continuità in maniera non invasiva, essa può intervenire nella più accurata indagine sui miglioramenti, nella predizione di possibili sviluppi, nelle problematiche connesse alla multi-morbilità e l'interazione farmacologica sulle condizioni del singolo paziente e molto altro ancora.

Una menzione particolare va fatta all'integrazione IA-robotica che oltre a consentire lo sviluppo e il perfezionamento di dispositivi innovativi e utilizzabili per interventi molto specifici, troverà sempre maggior impiego in ambiti fondamentali per la salute quali la chirurgia, la riabilitazione, la cura della persona ecc.

Quanto alla prima, si prevede che l'integrazione dell'intelligenza artificiale nella chirurgia robotica medica migliorerà la precisione, l'efficienza e

44. Asif S., Wenhui Y., ur-Rehman S. *et al., Advancements and Prospects of Machine Learning in Medical Diagnostics: Unveiling the Future of Diagnostic Precision,* in *Archive of Computational Methods in Engineering,* 2024, Springer, s.p..

45. Vallini A., *Paternalismo medico, rigorismi penali, medicina difensiva: una sintesi problematica e un azzardo* de jure condendo, in *Rivista italiana di medicina legale,* 2013, 1, pp. 1 ss.

l'accessibilità degli interventi chirurgici, e consentirà di automatizzare compiti ripetitivi come la sutura, l'ottimizzazione i movimenti degli strumenti chirurgici, l'analisi delle immagini intraoperatorie e, perfino il miglioramento della pratica umana attraverso sistemi di *feedback* aptici ai chirurghi. Al momento, l'adozione su larga scala è ostacolata da costi elevati, dipendenza dalla qualità dei dati, e dall'incertezza sulle questioni etiche e giuridiche connesse alla responsabilità: analogamente a quanto si vedrà subito con riferimento alla protesica robotica, tali giudizi divengono problematici laddove il confine tra l'atto umano e quello robotico diventi sfumato[46].

Sul piano dell'impiego a fini riabilitativi, robot dotati di IA possono essere utilizzati non solo per la pratica riabilitativa finalizzata al recupero di funzionalità temporaneamente compromesse ma anche per l'assistenza protesica, e, quindi, per l'ottenimento di prestazioni variamente funzionali nel caso di compromissione definitiva. Quest'ultima ipotesi – in particolare quando si sostanzi in protesi robotiche destinate ad assistere e supportare il movimento del paziente, specialmente quando costui conservi qualche residuo di funzionalità – appare il più interessante perché, come è stato già individuato, al netto dei consueti problemi relativi alla protezione dei dati personali, in particolare biometrici o comunque fisiologici, sembrano entrare in gioco esigenze contrastanti e, al limite, contraddittorie. Da un lato, le necessità di utilizzo semplice e confortevole richiedono che l'azione di supporto robotico sia idealmente in continuità con quella intenzionale e residua del paziente, dall'altro, proprio questa assenza di soluzione di continuità auspicabile, costituisce un problema ai fini della potenziale imputazione di responsabilità nel caso in cui, mediante l'utilizzo dell'arto protesico "intelligente", si produca un danno a terzi[47].

Infine, in merito alle applicazioni di intelligenza artificiale al settore infermieristico ed ostetrico recenti analisi della letteratura – peraltro ancora in sviluppo – hanno individuato diversi ambiti di applicazione. Le principali aree di utilizzo includono, in primo luogo, la cura diretta del paziente sia in ambito critico, come ad esempio lo sviluppo di sistemi di classificazione dei pazienti in terapia intensiva e previsione del rischio di trasferimento in

46. Muhammad I., *et al., Artificial intelligence: revolutionizing robotic surgery: review,* in *Annals of Medicine & Surgery,* 2024, vol. 86, 9, pp. 5401-5409; Zhang C., Hallbeck M. S., Salehinejad H., Thiels C., *The integration of artificial intelligence in robotic surgery: A narrative review*, in *Surgery*, 2024, vol. 176, 3, pp. 552-557.

47. Gli aspetti etici e giuridici di tale ipotesi sono discussi in Sarra C., *Relevant Legal Issues for Hybrid Human-Robotic Assistive Technologies: A First Assessment*, in Frenkel D. A., Chronopoulou A., (eds)*, An Anthology of Law*, ATINER, Athens 2020, pp. 271-291.

unità di terapia intensiva basandosi sui dati delle cartelle cliniche, sia in ambito generale mediante l'utilizzo di algoritmi di elaborazione del linguaggio naturale (NLP) su referti di risonanza magnetica cerebrale per prevedere esiti funzionali nei pazienti con ictus ischemico acuto e monitoraggio delle reazioni avverse ai farmaci. Tali applicazioni includono sistemi autonomi di monitoraggio continuo per pazienti critici, basati su sensori non invasivi, in grado di raccogliere dati ambientali e fisiologici[48].

In secondo luogo, vi sono esperimenti diretti alla gestione del delirio nei pazienti, migliorando la comprensione delle informazioni cliniche e la facilità del loro per gli operatori sanitari, e, più in generale, il miglioramento della raccolta strutturata dei dati e della qualità complessiva della documentazione infermieristica.

In ostetricia, l'IA è utilizzata per migliorare la gestione del rischio ostetrico e monitorare le condizioni delle donne in gravidanza, ad esempio identificando precocemente i segni di sepsi neonatale.

Infine, nell'ambito della formazione, algoritmi di IA sono impiegati per prevedere il successo accademico degli studenti infermieri e ridurre il tasso di abbandono nei corsi di preparazione specifica[49].

d) applicazioni a fini assicurativi

Recenti analisi della letteratura in materia di utilizzo dell'IA nel settore assicurativo[50], in generale, hanno mostrato ampi margini di applicazioni in un ambito nel quale l'analisi dei dati e il calcolo del rischio costituiscono gli elementi essenziali di azione. L'impatto delle nuove tecnologie "intelligenti" si sviluppa, perciò, lungo l'intera catena del valore in cui si muove il settore. Gli individuati ambiti principali di utilizzo includono ad esempio il *marketing*, con la previsione del valore del cliente nel tempo, la segmentazione avanzata per strategie personalizzate, l'analisi delle preferenze dei consumatori per l'innovazione dei prodotti, l'elaborazione di strumenti analitici basati su algoritmi di *machine learning* e statistica predittiva, per identificare i clienti che hanno una probabilità elevata di interrompere il rapporto con un'azienda o un servizio.

---

48. Ruksakulpiwat, S., Thorngthip, S. *et al.*, *A Systematic Review of the Application of Artificial Intelligence in Nursing Care: Where are We, and What's Next?, in Journal of Multidisciplinary Healthcare*, 2024, vol. 17, pp. 1603-1616.

49. Cfr. l'analisi delle pubblicazioni in O'Connor, S., Yan, Y., *et al., Artificial intelligence in nursing and midwifery: A systematic review,* in *Journal of Clinical Nursing*, 2023, vol. 32, pp. 2951–2968.

50. Cfr. per esempio, Owens E., Sheehan B. *et al., Explainable Artificial Intelligence (XAI) in Insurance,* in *Risks,* 2022, vol. 10, 12, pp. 1-50.

Nel settore sanitario, in particolare l'utilizzo di forme di sanità privata, tali applicazioni risultano particolarmente importanti per lo sviluppo di polizze sanitarie a livello individuale o aziendale.

Anche lo sviluppo di prodotti specifici risulta, naturalmente interessato dall'utilizzo di IA, in particolare la creazione di servizi aggiuntivi, come la diagnosi precoce di malattie, l'ingresso in nuovi mercati con ecosistemi basati su IA, per esempio nell'assistenza sanitaria in tempo reale, lo sviluppo di polizze assicurative innovative basate sull'uso di dati dinamici, l'automazione nella gestione delle richieste e nella valutazione dei rischi, la creazione di pool di rischio più piccoli e omogenei per ridurre l'errore sul rischio, la creazione di *chatbot* per la gestione automatizzata delle richieste di assistenza, il supporto per la prevenzione delle perdite attraverso consigli su sicurezza e salute, la comunicazione proattiva con i clienti per migliorare l'*engagement.*

Naturalmente, sono poi presenti applicazioni miranti ad ottimizzare la gestione dei sinistri e la prevenzione delle frodi, l'automazione dei processi di liquidazione con riduzione dei tempi di gestione, il rilevamento avanzato delle frodi tramite modelli di analisi comportamentale e *social network analytics,* la stima dei danni basata su IA per migliorare la gestione delle riserve, la gestione degli *asset* e il controllo del rischio, la reportistica automatizzata sui rischi[51].

Come si vede, si tratta di un amplissimo ambito di applicazioni, molte o tutte delle quali rilevanti anche per lo svolgimento delle pratiche assicurative specifiche per la salute.

Va però ricordato che il recente Regolamento Europeo sull'Intelligenza Artificiale colloca anche i sistemi di IA destinati a essere utilizzati per la valutazione dei rischi e la determinazione dei prezzi in relazione a persone fisiche nel caso di assicurazioni sulla vita e assicurazioni sanitarie tra i sistemi "ad alto rischio" per i quali, dunque, valgono le regole più stringenti previste dalla nuova disciplina. Inoltre, come si vedrà meglio in seguito, il Regolamento dispone il divieto di alcune pratiche (art. 5) che, dunque, non dovrebbero essere messe in atto neppure se utili alle operazioni assicurative appena viste. Tra queste vi sono, in particolare, l'uso di sistemi di categorizzazione biometrica basati sui dati biometrici di persone fisiche, quali il volto o le impronte digitali, per trarre deduzioni o inferenze in merito alle opinioni politiche, all'appartenenza sindacale, alle convinzioni religiose o filosofiche, alla razza, alla vita sessuale o all'orientamento sessuale di una persona. E, infine, importanti limiti sono posti alle operazioni di *social scoring* – vale

51. *Ibidem.*

a dire l'uso "di sistemi di IA per la valutazione o la classificazione delle persone fisiche o di gruppi di persone per un determinato periodo di tempo sulla base del loro comportamento sociale o di caratteristiche personali o della personalità note, inferite o previste" (art. 5, § 1, lett. c). Questi ultimi sono proibiti quando il "punteggio" che esprime la valutazione viene usato per determinare a) un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di gruppi di persone in contesti sociali che non sono collegati ai contesti in cui i dati sono stati originariamente generati o raccolti, oppure b) un trattamento pregiudizievole o sfavorevole di determinate persone fisiche o di gruppi di persone che sia ingiustificato o sproporzionato rispetto al loro comportamento sociale o alla sua gravità (*ibidem*).

Infine, tali disposizioni vanno raccordate con quelle del già discusso Regolamento sullo spazio europeo dei dati sanitari ai sensi del quale – come riferito *supra* – è possibile l'uso secondario di tali dati per attività di ricerca nel settore sanitario che preveda l'addestramento, la prova o la valutazione di algoritmi ma non è lecito l'utilizzo secondario con la finalità di adottare decisioni pregiudizievoli nei confronti di una persona o un gruppo di persone quali l'esclusione dai benefici di un contratto di assicurazione o la modifica delle condizioni contrattuali riferite ai premi.

7. Profili etici

Esistono significative analogie tra l'attuale rivoluzione tecnologica che vede, al momento, nell'intelligenza artificiale il suo *core* più promettente e quanto accaduto a partire dagli anni Sessanta del Ventesimo secolo e che ha portato alla nascita della bioetica.

In entrambi i casi è l'impatto trasformativo dell'innovazione tecnologica a costituire il vettore di riflessioni che toccano gli stessi concetti antropologici di base. La tecnologia, portata a rivoluzionare la medicina, con l'avvento delle tecniche più avanzate di rianimazione, di mantenimento in vita attraverso mezzi artificiali sempre più efficaci, di incisione sul processo procreativo, e molto altro, fa sì che concetti ritenuti fondamentali e sicuri, come quello di vita e di morte, divengano più sfumati. I fenomeni ad essi sottesi si mostrano processi, più che eventi: processi sui quali, in varia misura, si comincia ad avere un qualche controllo grazie al potenziamento tecnologico.

Conseguentemente, assieme alla trasformazione sociale che la ricostruzione e lo sviluppo post-bellico hanno determinato, i fenomeni della vita e

della morte, un tempo vissuti per lo più nell'ambito famigliare e comunitario, si ospedalizzano sempre di più e si medicalizzano, portando tali processi sempre più fuori dall'orizzonte simbolico della famiglia e del corso "naturale" delle cose, per entrare, invece, in quello della gestione professionale e specializzata, che, di per sé, è già un aspetto della tecnica.

Emerge, in questo contesto, un senso della ricerca sul "bene" che non si accontenta della speculazione filosofica e men che meno della sua proiezione metafisica verso un assoluto e che, invece, reclama strumenti di decisione applicabili ai dilemmi che, ormai, divengono quotidiani e, si percepisce rapidamente, non appaiono più gestibili né dentro i puri saperi scientifico-tecnici, né entro la sola deontologia professionale, seppur di venerabile tradizione come quella medica.

Tale "bisogno etico" si presenta progressivamente in tutti gli ambiti di questa società occidentale trasformata: emerge una più netta sensibilità ambientale che, pure, vuole incidere concretamente su quelle che appaiono urgenze (l'inquinamento, lo sfruttamento delle risorse naturali); si pone il problema della compatibilità dell'agire imprenditoriale proiettato al mero profitto con istanze sociali, potenzialmente limitanti la massimazione del guadagno ma ritenute sempre più importanti (la c.d. *business ethics)*, e di lì a poco – alla fine degli anni Sessanta – si porrà anche il tema di un utilizzo etico dei nuovi strumenti informatici che stanno già ormai trasformando la società. Nascerà così la c.d. *Computer Ethics,* prima intesa come deontologia dei professionisti dell'informatica e poi, progressivamente, come ambito di studi specifico della filosofia morale, dedicato alla riflessione, per lo più in chiave di etica applicata, sulle modalità con le quali le nuove tecnologie incidono, trasformano o determinano *ex novo* il modo con cui devono essere affrontati i dubbi morali[52].

Una delle caratteristiche essenziali degli studi di etica applicata più significativi è quella di aver compreso ed accettato l'inevitabile dimensione interdisciplinare – oltre che intervaloriale – delle questione che essi intendono affrontare, dunque, della necessità di trovare modalità e strumenti per un dialogo tra competenze e punti di vista tanto difficile quanto necessario per la considerazione di tutti gli elementi critici che il caso da decidersi presenta.

E va detto che probabilmente l'esperienza più significativa ed esemplare, tanto che, a parere di chi scrive, dovrebbe costituire un modello di riferimento anche per altri settori, è quella che si è affermata con i comitati di

52. Cfr. Sarra C., *Dalla Cibernetica alla Data Ethics. Linee di sviluppo dell'etica applicata alla rivoluzione informatica,* in Moro P. (a cura di), *Etica, Diritto e Tecnologia. Percorsi dell'informatica giuridica contemporanea,* FrancoAngeli, Milano, 2021, pp. 25-43.

bioetica. Si tratta di organismi che costitutivamente si configurano come luoghi di dialogo e decisione dialettica tra portatori di saperi, competenze e punti di vista differenti, che, però, non svolgono una funzione meramente speculativa e di confronto ma si determinano a prendere posizione in merito a specifiche questioni, talvolta davvero drammatiche.

E benché emergano conflitti e spesso punti di vista non conciliabili, pareri che presentano opinioni dissenzienti, non pare possa esservi una via diversa per contemperare pluralismo e applicazione pratica.

Richiamato, sebbene in maniera grandemente sintetica, il contesto di riferimento in cui nasce l'attenzione etica specifica per la rivoluzione informatica, non sorprenderà che a tutt'oggi, nelle sue manifestazioni più note e diffuse, essa si caratterizzi come un settore, appunto, dell'etica applicata e che, nei suoi esiti, spesso presenti forti analogie con quanto la riflessione bioetica ha largamente condiviso proprio per creare un *forum* di discussione che potesse trattenere insieme posizioni che, su un piano fondativo più essenziale, sarebbero, invece, in netto contrasto. Così, principi come il rispetto dell'autonomia dell'uomo, di beneficenza, non maleficenza, giustizia, così importanti nel dibattito bioetico, trovano una simmetria quasi perfetta con quelli indicati nell'ambito specifico dell'intelligenza artificiale, dall'Unione Europea nel famoso documento *Orientamenti etici per un Intelligenza Artificiale affidabile,* prodotto dalla Commissione di Esperti di Alto Livello nominati dalla Commissione Europea nel 2019.

Qui, individuati nella legalità, eticità e robustezza i tre requisiti essenziali per lo sviluppo della fiducia nel sistemi di IA, si richiamano, quali principi essenziali per l'eticità, il rispetto, appunto, dell'autonomia umana, la prevenzione dei danni, l'equità e l'esplicabilità.

Sono molteplici gli aspetti di interesse nell'elaborazione di questo documento: a cominciare dal fatto che esso è stato prodotto nell'ambito di quel processo che ha portato l'Unione ad elaborare, infine, la prima regolamentazione del fenomeno dell'IA con l'emanazione del già più volte citato *AI Act.* Ma, poi, la stessa operazione di istituzionalizzazione dell'etica appare notevole: se una delle accezioni tradizionali del termine fa riferimento alle consuetudini, ai modi abituali di agire riconosciuti in una comunità che nella perpetuazione di essi si riconosce e costituisce la propria identità[53],

53. Il primo significato di *ethos* è dimora, sede, abitazione e dunque attiene allo spazio semantico della casa e, di qui alla famiglia e alla comunità. Per una riflessione sulla condizione dell'uomo tecnologico contemporaneo a partire dalla valorizzazione di questa accezione, cfr. Sartea C., *Ecotecnologia. Sfide etico-giuridiche della civiltà tecnologica,* Giappichelli, Torino, 2024.

appare singolare la predisposizione di un modello *top-down* da parte di "esperti".

In questa operazione, l'eticità dell'IA appare una sorta di connotazione che sta nel mezzo tra la *compliance* giuridica e la performatività tecnica: in effetti, la posizione sposata dagli autori del documento sembra essere quella già presentata in letteratura di un etica c.d. '*soft* e post-compliance'[54]. Si tratta di concepire l'etica dell'IA come una sorta di elaborazione di principi, su vari livelli, che intervengano, quali ausili alla decisione, a colmare gli spazi lasciati vaghi dalla normativa cogente, facendo sì che non si diano conflitti tra le due dimensioni: in questo senso l'etica dell'IA, così presentata, non può che essere *soft, anche* perché è emanata dalla stessa istituzione che, poi, produce anche la norma cogente.

Ci sarebbe da chiedersi come si dovrebbe configurare l'eventuale emersione dalla società di visioni etiche non coincidenti, e magari conflittuali, con quella così istituzionalizzata: ad esse sembrerebbe negato lo spazio di legittimità etico per un eventuale approccio *hard* che voglia, invece, prodursi in un cambiamento normativo.

Sia come sia, il documento prodotto ha oggi una dimensione di valore che non si riduce all'etica ma acquista una dimensione specificamente giuridico-cogente per il fatto di essere richiamata esplicitamente dalla normativa giuridico-regolamentare[55].

Ma la discussione sulle questioni etiche legate all'implementazione di algoritmi in strumenti in grado di elaborare contenuti, decisioni, analisi, previsioni sulla base di dati e di modificare, in qualche misura, la propria azione con vari gradi di autonomia non è certo nata in questi ultimi anni.

Invero, molte delle questioni che si discutono ancora oggi sono state presenti nel dibattito fin dagli albori della *Computer ethics*: basterebbe rileggere i primi numeri della rivista *Ethics and Information Technologies* alla fine degli anni Novanta del secolo scorso per riscontrare come la riflessione si prolunghi ormai da decenni[56].

---

54. Floridi L., *Etica dell'Intelligenza Artificiale. Sviluppi, opportunità, sfide*, Raffaello Cortina, Milano 2022, cap. 4.

55. Cfr. art. 95, § 2, *AI Act.*

56. E, seppur con un dibattito di nicchia, i giuristi non sono stati da meno, in particolare i filosofi del diritto cui si deve l'introduzione dell'*Informatica giuridica* come disciplina. Infatti, già alla fine degli anni Sessanta del Ventesimo secolo possono trovarsi tracce di una nascente discussione tra le pagine della *Rivista Internazionale di Filosofia del Diritto*, dove già si discuteva della possibilità dell'automazione del giudizio o della redazione automatizzata degli atti giuridici, oltre che di questioni filosofiche più pregnanti, cfr. Sarra C., *Ricordare il passato pensando il futuro. Le condizioni di pensabilità della società post-informazionale,* in *Rivista Internazionale di Filosofia del Diritto,* 2021, 4, pp. 865-878.

Volendo, dunque, anche in questo caso, sintetizzare le principali linee critiche, provando a presentarle per la loro potenziale rilevanza nel contesto sanitario, potremmo evidenziare i punti seguenti ampiamente riconosciuti in letteratura.

In due successive revisioni della produzione dottrinale sul tema sono stati evidenziate diverse aree problematiche, suddivise dagli Autori in problematiche derivanti da fattori epistemici e/o normativi, nonché problematiche connesse alla possibilità di giudizio morale in ragione di elementi critici di tracciabilità[57].

Per "fattori epistemici" si intende la rilevanza della qualità e dell'accuratezza dei dati per la giustificabilità delle conclusioni a cui giungono gli artefatti e che, a loro volta, possono dare forma a decisioni non moralmente neutrali. Essi sono relativi, pertanto al rapporto "*in/out"* e hanno a che vedere con la connessone giustificativa dell'*output* rispetto alla base di dati partenza con cui l'artefatto è stato addestrato.

Invece, le preoccupazioni normative si riferiscono esplicitamente all'impatto etico delle azioni e delle decisioni guidate dagli algoritmi: in questo caso il *focus* della discussione è sul modo con cui l'*output* del sistema incide nell'ambiente sociale di riferimento.

Le questioni epistemiche e normative, insieme alla distribuzione della progettazione, dello sviluppo e dell'impiego degli algoritmi, determinano, poi, questioni di tracciabilità con riferimento alla catena di eventi e fattori che portano a un determinato risultato, rendendo difficile la possibilità di identificarne la causa e di, conseguenza, di attribuirne la responsabilità morale.

7.1. Fattori epistemici

Uno dei temi principali sempre ricordato allorché si discuta delle problematiche etiche dell'intelligenza aritificiale riguarda la natura statistico-probabilistica delle correlazioni che l'artefatto è in grado di individuare. In questo senso, la decisione basata su tali connessioni procede mediante l'inclusione del soggetto sul quale la decisione deve essere presa nella gene-

57. Si tratta di Mittelstadt B.D., Allo P., Taddeo M., Wachter S., Floridi L., *The ethics of algorithms: Mapping the debate*, in *Big Data & Society*, 2016, vol. 3, 2, pp. 1-21; Tsamados A., Aggarwal N. *et al., The ethics of algorithms: key problems and solutions*, in *AI & Soc,* 2022, vol. 37, pp. 215–230. Tale impostazione è ripresa in Floridi, *Etica dell'Intelligenza Artificiale,* cit.

ralità per la quale è stata individuata una certa correlazione. Tale struttura, presenta varie limitazioni in termini di giustificabilità della decisione che possono essere giudicate variamente gravi a seconda del settore di implementazione.

Infatti, se si stratta di suggerimenti di *marketing* la cosa può avere conseguenze limitate, ma se si tratta di diagnosticare una patologia e prendere i provvedimenti conseguenti, le questioni diventano molto più delicate.

In primo luogo, vi è il limite di ogni struttura di ragionamento di tipo induttivo: se la correlazione è individuata a livello di popolazione, l'inclusione di ogni nuovo individuo nella classe costruita sconta un margine di imprevedibilità e di errore. Tale questione è rilevante per l'utilizzo delle generalità individuate dalla ricerca medico-scientifica e il loro utilizzo in fase clinico-empirica.

In secondo luogo, artefatti complessi, producono correlazioni che possono derivare dalle proprietà stesse del sistema o dalle modalità di manipolazione dei *dataset* e non necessariamente dal campo analizzato.

Inoltre, e questo è uno dei temi più presenti e sicuramente rilevanti per l'utilizzo nell'ambito della salute, la correlazione individuata non necessariamente è rivelativa, di per sé, di una struttura causale sottostante che la giustifichi e che possa essere usata costruttivamente in fase predittiva.

Quanto agli espedienti per limitare le conseguenze di queste criticità costitutive sono stati suggerite procedure di miglioramento della quantità e qualità dei dati, di *auditing* continuativo e, dove possibile, di valutazione della riproducibilità delle connessioni ritrovate dall'artefatto. Il tutto in un contesto nel quale si suggerisce attenzione al c.d. *automation bias,* vale a dire l'inclinazione a fare troppo affidamento sull'efficacia dell'artefatto piuttosto che alla propria competenza radicata nel settore[58].

Va ricordato che il Regolamento sull'intelligenza artificiale prevede che le persone incaricate della sorveglianza umana (art. 14) siano preparate a (e siano predisposte modalità per) rimanere consapevoli del rischio connesso al "pregiudizio dell'automazione". Inoltre, va ricordato che i sistemi di intelligenza artificiale "ad alto rischio" devono essere soggetti a monitoraggio continuo anche dopo la loro messa in servizio o immissione sul mercato.

Un altro tema, già accennato, riguarda quello della c.d. connessione oc-

58. Goddard K., Roudsari A., Wyatt J.C., *Automation bias: a systematic review of frequency, effect mediators, and mitigators*, in *Journal of the American Medical Informatics Association*, 2012, vol. 19, 1, pp. 121–127; Mosier K.L., Skitka L.J., *Automation Use and Automation Bias*, in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 2019, vol. 43, 3, pp. 344-348.

culta tra dati e conclusione in ragione dell'opacità costitutiva dei sistemi più complessi.

In questo contesto, l'opacità costituisce un limite alla trasparenza – concetto che viene definito come implicante accessibilità e comprensibilità. Il punto è talmente importante che, come si è visto, gli *Orientamenti etici per un'IA affidabile,* includono il principio di esplicabilità tra i quattro fondamentali che connotano l'eticità dello sviluppo di sistemi intelligenti. Eppure, resta discussa la quantità di informazioni che dovrebbero accompagnare una decisione affinché questa possa dirsi comprensibile e, in particolare, se il modello di spiegazione dovrebbe essere configurato oggettivamente, secondo uno standard tecnico, o soggettivamente, vale a dire in relazione alle caratteristiche del caso specifico e dei soggetti coinvolti.

Sul punto, va ricordato che, all'indomani dell'approvazione del Regolamento Europeo sulla protezione dei dati personali, molte discussioni sono state sollevate circa la presenza in tale atto di un vero e proprio diritto alla "spiegazione" della decisione totalmente automatizzata per come essa viene disciplinata in particolare all'art. 22[59]. Nell'ambito di questi dibattiti, una parte della letteratura, ha evidenziato la connessione tra l'esigenza di spiegabilità e l'effettività dei diritti a garanzia del destinatario previsti dall'articolo citato, individuando nel diritto di contestazione, ivi menzionato, la chiave per giustificare la spiegazione ed anche per valutare la quantità necessaria di informazioni che essa dovrebbe contenere. L'importanza di tale connessione ha portato a ritenere incluso nel GDPR, accanto ai più noti principi di "*privacy by design", "privacy by default" e "accountability",* anche il principio di "*contestability by design"*[60].

---

59. Cfr *amplius* Sarra, C., *Defenceless? An Analytical Inquiry into the Right to Contest Fully Automated Decisions in the GDPR*, in Frenkel D. A., Chronopoulou A. (eds.), *An Anthology of Law*, ATINER, Athens 2020, pp. 235-252; Larus J., Hankin C., Carson G.S., *et al*., *When Computers Decide: European Recommendations on Machine-Learned Automated Decision Making*. ACM 2018; Brkan M., *Do Algorithms Rule the World? Algorithmic Decision-Making in the Framework of the GDPR and Beyond*, in *International Journal of Law and Information Technology*, 2019, vol. 27, 2, pp. 91-121; Mendoza I., Bygrave L.A., *The Right Not to Be Subject to Automated Decisions Based on Profiling*, in Synodinou T.-E., Jougleux P., Markou C., Prastitou T. (eds.), *EU Internet Law: Regulation and Enforcement*, Springer International Publishing, Cham 2017, pp. 77–98; Veale M., Edwards L., *Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling*, in *Computer Law & Security Review*, 2018, vol. 34, 2, pp. 398-404.

60. Almada M.*, Human intervention in automated decision-making: Toward the construction of contestable systems,* in *Proceedings of the Seventeenth International Conference on Artificial Intelligence and Law,* 2019, pp. 2–11. ICAIL '19. Montreal, QC, Canada: Association for Computing Machinery; Mulligan K.D., Kluttz D.N., Kohli N.*,*

Nonostante il permanere di dubbi sul punto, negli anni a seguire si è affermata da più parti l'esigenza di poter contare su una dimensione giuridica dell'esplicabilità: in particolare, una posizione netta sul punto, quanto alla necessità di trasparenza per la valutazione della legittimità dell'azione amministrativa che si sia servita di strumenti di IA è stata presa, con grande risonanza mediatica, dal Consiglio di Stato italiano[61].

Da ultimo, dopo l'emanazione degli *Orientamenti etici,* come ricordato *supra,* il Regolamento sull'IA ha stabilito formalmente il diritto di spiegazione (art. 86), anche se per il modo con cui è formulato si può presumere che non sarà certo idoneo a placare la discussione né a prevenire le criticità.

Ovviamente, l'opacità è un limite alla possibilità di scrutinio e all'individuazione della responsabilità, ciò che appare decisivo nell'ambito clinico. In particolare, la trasparenza, intesa come sopra ricordato, è stata individuata prima ancora che come un elemento etico, come una condizione "pro-etica", vale a dire, come un presupposto per poter esercitare il proprio agire etico.

Nell'ambito, infine, dei fattori epistemici, uno dei temi più discussi e all'attenzione di tutte le comunità di studiosi, quale che sia il loro ambito specifico di *expertise,* ritroviamo le preoccupazioni relative alla possibilità che l'artefatto si produca in deviazioni sistematiche (e, dunque, potenzialmente su larga scala) rispetto ad uno standard desiderabile, in particolare per ragioni etiche. Si tratta del tema – anche questo già accennato – dei *bias* dell'algoritmo che taluni distinguono da quello della c.d. *fairness* che nello schema qui seguito viene incluso nel fattori normativi. Va detto, però, che sul punto il dibattito non è perspicuo e facilmente si vedono le due questioni trattate come fossero una sola.

La letteratura sul tema dei *bias* – partendo dal presupposto che nessuna produzione tecnica è mai moralmente neutrale perché comunque riflette i valori di chi l'ha posta in essere – evidenzia come essi possano sorgere da tre fattori in particolare: da problemi di datificazione (es. presenza di valori sociali nelle pratiche datificate; *sampling* sottorapresentativo o comunque inadeguato); da limitazioni tecniche o dalle modalità specifiche con cui è determinata la logica decisoria o da difetti nel *design* complessivo (es. utilizzo di liste alfabetiche che avvantaggiano, di fatto, coloro che si trovano all'ini-

---

Shaping Our Tools: Contestability as a Means to Promote Responsible Algorithmic Decision Making in the Professions, in Werbach K. (ed.), *After the Digital Tornado. Networks, Algorithm, Humanity,* Cambridge University Press, Cambridge 2020, pp. 137-151*;* Alfrink K., Keller I., Kortuem G., Doorn N.*, Contestable AI by Design: Towards a Framework*, in Minds & Machines, 2023, 33, pp. 613-639.

61. Sui cui pronunciamenti si dirà *infra.*

zio; utilizzo di *proxy* inadeguati), o da aspetti emergenti nell'uso, come ad esempio, l'impiego in un settore diverso da quello originale degli artefatti.

Il punto significativo è che sebbene siano continuamente sviluppati approcci per l'eliminazione di tali difetti – approcci che possono riguardare i dati di partenza (*pre-processing*), il modo in cui l'artefatto decide (*in-processing*) o implicare pratiche di controllo e correzione *ex post* (*post-processing*)[62] – l'eliminazione del problema appare molto più difficile di quanto si potrebbe immaginare. Infatti, la semplice esclusione di alcune variabili sensibili, può non essere né praticabile sempre né sufficiente: talvolta tale pratica potrebbe inficiare l'efficacia dell'algoritmo, e comunque tali variabili possono essere incorporate altrove, per es. negli usi linguistici datificati.

Talvolta un *bias* "noto" può, invece, essere sfruttato per mitigare altri *bias* presenti nei dati; altre volte possono essere usati "synthetic data" – vale a dire dati generati da simulazioni o modelli statistici, invece che essere raccolti direttamente dal campo di riferimento – per creare *data-set* migliori (correggere difetti di distribuzione, eliminare correlazioni spurie ecc.).

Nell'ambito sanitario, il tema è particolarmente rilevante: dall'accesso alle prestazioni, alla sperimentazione mediante modelli di IA, alla clinica, fino alla valutazione dell'efficacia farmacologica, il tema del rischio di errori sistematici è presente ovunque.

7.2. Fattori normativi

Problematica relativa ai possibili *bias* nell'azione dell'artefatto è quasi sempre associata al pericolo di decisioni automatizzate che possano concretizzare forme di discriminazione algoritmica e, di conseguenza, si configurino come *unfair.* Il termine *fairness* e l'aggettivazione connessa (*fair/unfair*) è presente in molta parte della letteratura anche di lingua italiana *quo talis,* ed in effetti risulta di difficile traduzione ed anche di non banale concettualizzazione. Anche l'utilizzo del termine "equità" (e, dunque, anche la coppia "equo/iniquo"), se certamente non del tutto errato, non presenta esattamente lo stesso spazio semantico e può risultare, inoltre, addirittura fuorviante nelle applicazioni giuridiche nelle quali è richiamato specialmente con riferimento a certe modalità del giudizio che non necessariamente tro-

62. Cfr. Oneto L., Chiappa S., *Fairness in Machine Learning*, in Oneto L., Navarin N., Sperduti A., Anguita D. (eds), *Recent Trends in Learning From Data. Studies in Computational Intelligence*, Springer, Cham, 2020, pp. 155-196

vano il loro *focus* nel tema antidiscriminatorio che è, invece, particolarmente all'attenzione nell'uso "laico".

Sebbene nella pratica siano spesso considerati parti dello stesso tema, come accennato c'è chi distingue tra la problematica dei *bias* e quella degli impatti discriminatori dell'*output* che viene, in questi casi, ascritta alla *fairness.*

In effetti, anche il diritto conosce un'articolazione analoga, o comunque una doppia connotazione del tema discriminatorio che, almeno per certe situazioni, probabilmente può essere fatta corrispondere ai due momenti cui specificamente questa parte della letteratura riferisce i termini sopra ricordati.

Alludo alla distinzione tra discriminazione *diretta* e *indiretta:* la prima sarebbe riferita a quelle situazioni nelle quali una persona è trattata meno favorevolmente di quanto sia, sia stata o sarebbe trattata un'altra in una situazione analoga, in base ad un elemento sensibile e che non dovrebbe fare la differenza, mentre la seconda sarebbe determinata da quelle situazioni nelle quali una disposizione, un criterio o una prassi apparentemente neutri possono mettere in una situazione di particolare svantaggio alcune tipologie di soggetti. Tale distinzione si ritrova nel nostro diritto positivo in materia giuslavoristica ed in particolare nell'art. 2 del D. Lgs. 9 luglio 2003, n. 216 che recepisce la Direttiva europea 2000/78/CE.

Come si vede, la prima situazione è esattamente quella di una "logica decisoria" viziata dall'utilizzo di un criterio che, invece, non dovrebbe essere utilizzato per differenziare il trattamento delle persone, determinando così una diseguaglianza irragionevole. Invece, la seconda situazione si riferisce a situazioni nelle quali i criteri utilizzati per la decisione, benché di per sé neutrali, e cioè non implicanti condizioni sensibili quali il genere, l'origine etnica, le credenze religiose, ecc., tuttavia producono esiti che impattano in maniera irragionevolmente diseguale nei destinatari. Un esempio di questa situazione potrebbe vedersi nell'utilizzo di un criterio che faccia riferimento all'altezza minima per accedere a certe posizioni, cosa che, benché apparentemente neutrale, almeno rispetto ai più noti attributi sensibili, si può risolvere "indirettamente" in una discriminazione di genere, se, mediamente, le persone di sesso maschile risultano superare più comunemente detto criterio.

Una delle difficoltà maggiori su queste questioni, oltre alla non coincidente categorizzazione etica, tecnica e giuridica, è che la stessa letteratura risulta non uniforme. In effetti, si sono contate fino a ventuno definizioni diverse di *fairness* utilizzate dagli studiosi e questo certamente non agevola

una condivisa gestione dei fenomeni sottesi[63]. Peraltro, di tutte queste nozioni, ve ne sono quattro che sembrano essere le più richiamate e precisamente:

a) *anti-classificazione:* si riferisce alle categorie protette, come l'origine etnica e il genere, e ai loro *proxy* che non vengono utilizzati esplicitamente nel processo decisionale;
b) *parità di classificazione:* considera un modello *fair* se le misure comuni di performance predittiva, compresi i tassi di falsi positivi e negativi, sono uguali tra i gruppi protetti;
c) *calibrazione:* considera la *fairness* come misura di quanto ben-calibrato è un modello rispetto ai gruppi protetti;
d) *parità statistica:* definisce la *fairness* come una stima di probabilità media uguale per tutti i membri dei gruppi protetti[64].

Nell'ambito sanitario, ciascuna di queste nozioni può avere un ruolo a seconda della particolare situazione. In particolare, data la materia, non pare possibile esprimere un giudizio unico e *a priori* circa, ad esempio, l'esclusione di certe variabili "proibite", giacché molte di queste sono, invece, rilevanti per la salute. D'altronde è esattamente per questa particolare connessione con la sfera più intima dei soggetti che tali dati sono considerati meritevoli di particolare protezione. Così, per fare solo qualche esempio, oltre all'ovvia differenza biologica tra i sessi, anche parametri apparentemente meno diretti possono essere significativi, per esempio le credenze religiose, nella misura in cui prescrivono certi comportamenti (o impongono certi divieti, per es. trasfusioni di sangue), possono essere decisive per la diagnosi e la scelta terapeutica del paziente.

Dunque, il tema, già molto delicato in generale, risulta ancora più sensibile quando sia in gioco la salute, specialmente se intesa come "benessere totale".

A questo proposito, va sottolineato come l'incidenza massiva del fenomeno della datificazione, accompagnato dalla possibilità di utilizzare algoritmi di gestione dei dati prodotti, di estrazione di conoscenza e, infine, di decisione in un contesto che vuole essere "totale", comporti una seria sfida

63. Tale numero è riportato in Wong P.H., *Democratizing Algorithmic Fairness,* in *Philosophy of Technology,* 2020, 33, pp. 225-244 (nota 5), nel quale si sottolinea giustamente l'impossibilità di un algoritmo di essere *fair* secondo qualsiasi nozione e che *fairness* ed efficienza possono andare in conflitto dovendosi quindi ricorrere ad un'ulteriore scala di valori per stabilire come bilanciarli. In altri termini, l'accordo su una qualche nozione di *fairness* è una questione *politica* prima che tecnica.

64. Tsamados *et al, The ethics of algorithm,* cit., § 6.

all'autonomia dei soggetti. Come si è visto all'inizio di queste riflessioni, il rapporto tra libertà individuale e salute collettiva costituisce il vero nodo profondo e problematico attorno al quale si gioca la costruzione delle politiche pubbliche, incluse quelle normative, relative alla salute. Ed è chiaro che, sul piano morale, ogni accentuazione della dimensione pubblica si traduce in una potenziale limitazione all'autonomia del singolo. Sebbene la nostra Costituzione sia molto chiara nel fissare il limite di ogni intervento pubblico, anche legislativo, nel "rispetto per la persona umana" (art. 32, comma 2, Cost.), tale indicazione – essenziale sul piano dei principi – non riesce a rendere più agevole il difficilissimo compito di trovare il punto di mediazione tra le diverse esigenze. Accade, così, che la ricerca del "benessere totale" attraverso la tecnologia dei dati, rischia di connotare l'esistenza tutta delle persone dalla potenziale presenza costante di artefatti della salute, che monitorano, analizzano, suggeriscono comportamenti, e condizionano lo stile di vita della persona in maniera pervasiva senza che il soggetto abbia la possibilità di valutare con cognizione di causa l'effettiva utilità (per le ragioni dette finora) o addirittura sopprimendo del tutto il suo senso critico e realizzando così un "paternalismo sanitario" di ritorno attraverso l'oracolo tecnico.

Così, se la personalizzazione che l'algoritmo "totale" promette, attraverso l'analisi dei dati specifici del soggetto e la sua inclusione nelle classi rilevanti ai fini della previsione e del suggerimento del comportamento ritenuto più salutare, può, effettivamente, portare a dei vantaggi per i soggetti che vedono la loro situazione scrutata con maggior dettaglio rispetto ad una prassi omogeneizzante, va detto che, a sua volta tale personalizzazione influisce sui comportamenti, paradossalmente, portando il soggetto ad "aderire" *ex post* alle classificazioni entro cui è incluso, creando una sorta di "previsione autoavverantesi".

L'esito di questo "ciclo della datificazione" rischia, così, di andare contro le intenzioni e mortificare, invece che promuovere, l'autonomia morale delle persone. In questo scenario, va ricordato che vi sono vari fattori che incidono su quest'ultima, tra questi, senz'altro: l'azione degli algoritmi che modellano le possibilità di scelta; la loro già ricordata opacità e la scarsa conoscenza da parte dei destinatari dei sistemi e la mancanza di partecipazione nel *design* degli artefatti che occulta la scelte morali che si incorporano nello strumento[65].

Infine, l'autonomia morale delle persone è strettamente influenzata dalla loro capacità di controllo delle informazioni e dei dati che vi si riferiscono,

65. Le cc.dd. *invisible choices* su cui si veda il pionieristico Moor. J.H., *What is Computer Ethics*?, in *Metaphilosophy*, 1985, vol. 16, 4, pp. 266-275.

ciò che, come si è ricordato, si usa definire come *privacy* informazionale. Questo tema è sempre presente in tutta la letteratura qui considerata, sia etica che più specificamente dedicata al tema sanitario, compresa quella che lavora sul *design* delle nuove infrastrutture di computazione distribuita. In effetti, se l'incremento della complessità e la distribuzione delle operazioni di processamento dei dati, aumentano la performatività nelle condizioni attuali di rischio di "congestione" dovuto alla produzione massiva di dati, esse determinano anche maggiori problematiche di sicurezza e di rischio per la *privacy*.

In tema di dati sanitari, sarà cruciale seguire la progressiva applicazione del Regolamento sullo spazio europeo dei dati sanitari di cui si è già parlato, nonché concentrarsi sull'informazione comprensibile alle persone coinvolte e sulle misure organizzative e le tutele che la normativa generale sulla protezione dei dati personali, e il nuovo regolamento sull'intelligenza artificiale prevedono. A questi due atti sono dedicati gli approfondimenti nel prosieguo di questo lavoro.

7.3. Responsabilità

Il tema della responsabilità per l'azione determinata o, comunque, influenzata dall'artefatto, è naturalmente presente nel dibattito etico ed è, anzi, uno di quelli presenti fin dall'inizio della riflessione sulla rivoluzione informatica. Sebbene vi siano indubbiamente riflessioni talvolta analoghe a quelle che sono offerte dalla letteratura giuridica, in etica il respiro è decisamente più ampio, essendo determinato più dalla posizione teorica di riferimento che dal comparto normativo positivo di un certo ordinamento, cosa dalla quale, invece, il giurista non può prescindere.

Sul punto, dunque, la discussione è ampia e contempla posizioni "rivoluzionarie" che, ad esempio, insistono per la proposizione del tema etico entro una ricostruzione "ontologica" che rifiuti l'antropocentrismo con cui – asseritamente – la questione dell'agire morale sarebbe stata sempre posta.

In grande sintesi, il giudizio di responsabilità etica sarebbe sempre stato riferito alla persona umana come unica protagonista della vicenda morale e del tutto determinato dal modo con cui, nella storia, costei abbia teorizzato il proprio destino nel perseguimento del "bene".

Traendo ispirazione dalle etiche ambientalistiche più radicali, e in particolare dall'idea di un "egualitarismo biosferico", vale a dire della parità ontologica di tutte le forme di vita, l'*information ethics* propone una visione

nella quale ogni "organismo informazionale" – naturale o artificiale – ha dignità morale ed ogni azione viene giudica sulla base della sua capacità di aumentare o ridurre l'entropia[66]. Tale prospettiva, che non è possibile approfondire ulteriormente qui, ha il vantaggio di porre entro un quadro generale consistente il tema della responsabilità dello stesso artefatto, verso cui vari studiosi propendono ma che altrimenti risulta estremamente problematica. Va detto che il diritto, in ragione della "virtualità" che connota l'ascrizione della personalità giuridica, dispone, in effetti, in astratto delle categorie per immaginare una costruzione del genere, almeno al di fuori dell'ambito penalistico dove il principio personalistico risulta ancora molto radicato, nonostante la discussione che alcuni interventi normativi molto noti hanno suscitato in passato[67]. Ed infatti non mancano proposte tese ad immaginare l'artefatto come una persona giuridica, magari connotata dalla disponibilità di un patrimonio quale condizione per l'ascrizione della personalità.

Sia come sia, al di fuori delle proposte complessive e "rivoluzionarie", il tema principale allorché si discuta della possibilità di ascrizione di una responsabilità per le conseguenze dell'azione dell'artefatto, è quello della difficoltà di ricostruire la serie di eventi rilevanti moralmente e che hanno determinato l'esito finale in un contesto in cui partecipano numerosi attori (progettatori, sviluppatori, programmatori, distributori, utenti ecc.) la cui azione è, inoltre, possibilmente inframezzata di vari automatismi più o meno complessi ed opachi. Tale situazione rende problematica l'individuazione di ogni responsabilità "lineare" e financo sfida la sensatezza di tale giudizio, giacché laddove l'automa presenti forme avanzate di autonomia, lo stesso nesso di causalità verso le azioni umane appare difficilmente ricostruibile.

Il rischio è quello, duplice, di non riuscire a riconoscere la responsabilità in casi socialmente ritenuti gravi e meritevoli quantomeno di stigma morale se non proprio di azioni riparatorie, oppure, dall'altro lato, di sanzionare pretestuosamente qualcuno purchessia sebbene la richiesta di diligenza nei suoi confronti possa apparire, nel contesto di riferimento, del tutto supererogatoria.

---

66. Floridi L., *Information Ethics: On the philosophical foundation of computer ethics*, in *Ethics and Information Technology*, 1999, vol. 1, pp. 37-56; Floridi L., *On the intrinsic value of informational object and the infosphere*, in *Ethics and Information Technology*, 2002, 4, pp. 287-304.

67. In particolare con l'introduzione del D. Lgs 231/2001 e della responsabilità, ivi definita "amministrativa", delle persone giuridiche per reati commessi nel suo interesse o a suo vantaggio da persone con funzioni di direzione, rappresentanza o amministrazione o di soggetti a questi sottoposti.

In questo contesto, emerge anche l'idea di abbandonare nozioni ancestrali quali quella di "colpa" o di "retribuzione" in favore di categorie ritenute più adeguate quale quella del prendersi cura delle conseguenze trasformative di un'azione complessa quale che sia la sua derivazione, umana, artificiale o una combinazione difficilmente valutabile di entrambe[68].

Quale che sia la valutazione sul piano morale di tali proposte, c'è da chiedersi se esse possano immaginarsi idonee a penetrare nel tessuto giuridico, e se la società sia pronta a rinunziare del tutto alle categorie "ancestrali" senza che ciò si risolva, invece, in una maggiore disaffezione nei confronti del diritto con conseguenze sociali ancora peggiori.

D'altro canto, e fuori da queste ultime considerazioni, la riflessione bioetica ci ha presentato l'idea di una "etica della cura"[69], che si faccia carico delle condizioni di imperfezione e di dolore ineluttabili in ragione della fragilità della natura umana, nel contesto di un concetto di salute, quale stato di benessere, che non necessariamente presuppone la perfezione fisica ma include la possibilità di un equilibrio vivibile, nella dignità della persona umana, anche nella condizione di patologia inevitabile o cronica.

In conclusione, la sfida morale e giuridica nella attuale condizione di trasformazione tecnologica resta aperta ed appare caratterizzata, profondamente, dalla modulazione della stessa autocomprensione dell'uomo contemporaneo, che, ancora una volta, si mostra in cerca di sé stesso.

Bibliografia

Alfrink K., Keller I., Kortuem G., Doorn N.*, Contestable AI by Design: Towards a Framework, in* Minds & Machines, 2023, 33, pp. 613-639 9, pp. 5401-5409.

Almada M.*, Human intervention in automated decision-making: Toward the construction of contestable systems,* in *Proceedings of the Seventeenth International Conference on Artificial Intelligence and Law,* 2019, pp. 2-11. ICAIL '19. Montreal, QC, Canada: Association for Computing Machinery.

Asif S., Wenhui Y., ur-Rehman S. *et al., Advancements and Prospects of Machine Learning in Medical Diagnostics: Unveiling the Future of Diagnostic Precision,* in *Archive of Computational Methods in Engineering,* 2024, Springer, s.p.

Bairagi S.I., Bang A.O., *Cloud Computing: History, Architecture, Security Issues,* in *International Journal of Advent Research in Computer and Electronics (IJARCE),* sp. is., 2015, pp. 102-108.

68. Floridi, *On the intrinsic value,* cit.

69. Palazzani L., *Cura e giustizia. Tra teoria e prassi,* Ed. Studium, Roma 2017.

Belard A. *et al*., *Precision Diagnosis: A View of the Clinical Decision Support Systems (CDSS) Landscape through the Lens of Critical Care*, in *Journal of Clinical Monitoring and Computing,* 2017, vol. 31, 2, pp. 261-271.

Bonomi F., Milito R., Zhu J., Addepalli S., *Fog computing and its role in the internet of things,* in *Proceedings of the first edition of the MCC workshop on Mobile cloud computing,* 2012, pp. 13-15.

Bontempi M., *Per una ecologia medica: dal paternalismo al personalismo metodologico nel rapporto medico-paziente,* in *Areté,* 2022, 7, pp. 169 ss.

Brkan M., *Do Algorithms Rule the World? Algorithmic Decision-Making in the Framework of the GDPR and Beyond*, in *International Journal of Law and Information Technology*, 2019, vol. 27, 2, pp. 91-121.

Burrell J., *How the machine 'thinks:' Understanding opacity in machine learning algorithms*, in *Big Data & Society*, 2016, vol. 3, 1, pp. 1-12.

Cavalho G., Cabral B., Pereira V., Bernardino J., *Edge computing: current trends, research challenges and future directions,* in *Computing,* 2021, 103, pp. 993-1023.

Cheng P., Montagnon E. *et al.*, *Deep Learning: An Update for Radiologists*, in *RadioGraphics*, 2021, vol. 41, 5, pp. 1427-1445.

Colaruotolo A., *Intelligenza artificiale e responsabilità medica: novità, continuità, criticità,* in *Responsabilità medica,* 2022, 3, pp. 299 ss.

Collingridge D., *The Social Control of Technology,* Frances Printer, London 1980.

Daylami N., *The origin and construct of cloud computing,* in *International Journal of the Academic Business World,* 2015, 9, 2, pp. 39-45.

Duan G. Fu, Zhou N., Sun X. , Narendra N. C. , Hu B., *Everything as a Service (XaaS) on the Cloud: Origins, Current and Future Trends*, in *2015 IEEE 8th International Conference on Cloud Computing*, New York, NY, USA, 2015, pp. 621-628.

Floridi L., *Etica dell'Intelligenza Artificiale. Sviluppi, opportunità, sfide*, Raffaello Cortina, Milano, 2022.

Floridi L., *Information Ethics: On the philosophical foundation of computer ethics*, in *Ethics and Information Technology*, 1999, vol. 1, pp. 37-56.

Floridi L., *On the intrinsic value of informational object and the infosphere*, in *Ethics and Information Technology,* 2002, 4, pp. 287-304.

García F. *et al*., *Transforming healthcare with AI*, EIT Health and McKinsey Company, 2020, *https://eithealth.eu/wp-content/uploads/2020/03/EIT-Health-and-McKinsey_Transforming-Healthcare-with-AI.pdf*.

Giglioni F*., Manuale di diritto sanitario,* Neldiritto Editore, Ba, 2024, Cap. 1.

Grasso G.A., *GDPR e intelligenza artificiale: limiti al processo decisionale automatico in sanità,* in Salanitro U. (a cura di), *SMART. La persona e l'infosfera,* Pacini Giuridica, Pisa 2022, pp. 183-223.

Grieves M., Vickers J.*, Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Complex Systems*, in Kahlen J., Flumerfelt S., Alves A. (eds), *Transdisciplinary Perspectives on Complex Systems,* Springer, Cham 2017.

Hartmann M., Hashmi U.S., Imran A., *Edge computing in smart Healthcare systems: Review, challenges and research directions,* in *Transactions on Emerging Telecomunications Technologies,* 2019, sp. iss., pp. 1-25.

Kong L.*, et al, Edge-computing-driven Internet of Things: A Survey,* in *ACM Computing Surveys*, vol. 55, 8, pp. 1-41.

Larus J., Hankin C., Carson G.S., *et al*., *When Computers Decide: European Recommendations on Machine-Learned Automated Decision Making*, ACM 2018.

Luzzi S., *Salute e sanità nell'Italia repubblicana,* Donzelli, Roma, 2004.

Mandsberg N.K., *et al*, *Orally ingestible medical devices for gut engineering, Advanced Drug Delivery Reviews*, 2020, 165-166, pp. 142-154.

Mansour Y, Ali Babar M., *A review of edge computing: Features and resources virtualization,* in *Journal of Parallel and Distributed Computing,* 2021*,* 150, pp. 155-183.

Mendoza I., Bygrave L.A., *The Right Not to Be Subject to Automated Decisions Based on Profiling*, in Synodinou T.-E., Jougleux P., Markou C., Prastitou T. (eds.), *EU Internet Law: Regulation and Enforcement*, Springer International Publishing, Cham 2017, pp. 77-98.

Mittelstadt B.D., Allo P., Taddeo M., Wachter S., Floridi L.*, The ethics of algorithms: Mapping the debate,* in *Big Data & Society,* 2016, vol. 3, 2, pp. 1-21.

Moor. J.H., *What is Computer Ethics*?, in *Metaphilosophy*, 1985, vol. 16, 4, pp. 266-275.

Muhammad I., *et al., Artificial intelligence: revolutionizing robotic surgery: review,* in *Annals of Medicine & Surgery,* 2024, vol. 86, 9, pp. 5401-5409.

Mulligan K.D., Kluttz D.N., Kohli N.*, Shaping Our Tools: Contestability as a Means to Promote Responsible Algorithmic Decision Making in the Professions,* in Werbach K. (ed.), *After the Digital Tornado. Networks, Algorithm, Humanity,* Cambridge University Press, Cambridge 2020, pp. 137-151.

O'Connor, S., Yan, Y., *et al., Artificial intelligence in nursing and midwifery: A systematic review,* in *Journal of Clinical Nursing*, 2023, vol. 32, pp. 2951-2968.

Omaghomi T.T., Elufioye O.A., Akomolafe O. *et al., A Comprehensive Review of Telemedicine Technologies: Past, Presente, Prospects,* in *International Medical Science Research Journal*, 2024, vol. 4, 2, pp. 183-193.

Oneto L., Chiappa S.*, Fairness in Machine Learning,* in Oneto L., Navarin N., Sperduti A., Anguita D. (eds)*, Recent Trends in Learning From Data. Studies in Computational Intelligence, Springer,* Cham 2020, pp. 155-196.

OpenFog, *Openfog Reference Architecture for Fog Computing,* Openfog Consortium, 2017.

Owens E., Sheehan B. *et al., Explainable Artificial Intelligence (XAI) in Insurance,* in *Risks,* 2022, vol. 10, 12, pp. 1-50.

Palazzani L., *Cura e giustizia. Tra teoria e prassi,* Ed. Studium, Roma, 2017.

Parkhill D.F., *The Challenge of computer utility,* Adison-Wesley pub., Reading Massachusetts, 1966.

Reddy Boda V.V., *Edge Computing in Healthcare: What It Is and Why It Matters,* in *MZ Computing Journal,* 2024, vol. 5, 2,, pp. 1-18.

Rosen S., Mor S., *Evaluating the Reliability of ChatGPT as a Tool for Imaging TestCheng P.Referral: A Comparative Study with a Clinical Decision Support System*, in *European Radiology,* 2023, vol. 34, 5, pp. 2826-2837.

Ruksakulpiwat, S., Thorngthip, S. *et al.*, *A Systematic Review of the Application of Artificial Intelligence in Nursing Care: Where are We, and What's Next?,* in *Journal of Multidisciplinary Healthcare*, 2024, vol. 17, pp. 1603-1616.

Salito G., *La responsabilità da algoritmo tra (teoria della) finzione e realtà sanitaria: una nuova declinazione della responsabilità medica?*, in *Rivista italiana di medicina legale,* 2022, 4, pp. 849 ss.

Sarra C., *Artificial Intelligence in Decision-making: A Test of Consistency between the "EU AI Act" and the "General Data Protection Regulation",* in *Athens Journal of Law,* 2025, vol. 11, 1, pp. 45-62.

Sarra C.*, Dalla Cibernetica alla Data Ethics. Linee di sviluppo dell'etica applicata alla rivoluzione informatica,* in Moro P. (a cura di), *Etica, Diritto e Tecnologia. Percorsi dell'informatica giuridica contemporanea,* FrancoAngeli, Milano, 2021, pp. 25-43.

Sarra C., *Il mondo-dato,* CLEUP, II ed., Padova, 2022.

Sarra C., *La dignità della persona nell'era della datificazione e dell'intelligenza artificiale,* KRONT, Roma, 2025.

Sarra C., *Relevant Legal Issues for Hybrid Human-Robotic Assistive Technologies: A First Assessment,* in Frenkel D.A.*,* Chronopoulou A. (eds)*, An Anthology of Law,* ATINER*,* Athens, 2020, pp. 271-291.

Sarra C., *Ricordare il passato pensando il futuro. Le condizioni di pensabilità della società post-informazionale,* in *Rivista Internazionale di Filosofia del Diritto,* 2021, 4, pp. 865-878.

Sarra C., *Defenceless? An Analytical Inquiry into the Right to Contest Fully Automated Decisions in the GDPR*, in Frenkel D.A., Chronopoulou A. (eds.), *An Anthology of Law*, ATINER, Athens, 2020, pp. 235-252.

Sartea C., *Ecotecnologia. Sfide etico-giuridiche della civiltà tecnologica,* Giappichelli, Torino 2024.

Scotti R., *La responsabilità civile dei danni cagionati dall'intelligenza artificiale in ambito sanitario,* in *Giustizia civile,* 2024, 1, pp. 158 ss.

Sira E. *et al, Mapping and Summarizing the Research on AI Systems for Automating Medical History Taking and Triage: Scoping Review,* in *Journal of Internet Medical Research,* 2025, 27, pp. 1-17.

Trubiani F., *I contratti di cloud computing: natura, contenuti e qualificazione giuridica,* in *Diritto dell'informazione e dell'informatica,* 2022, II(2), pp. 395 ss.

Tsamados A., Aggarwal N. *et al., The ethics of algorithms: key problems and solutions,* in AI & Soc, 2022, vol. 37, pp. 215-230.

Veale M., Edwards L., *Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling*, in *Computer Law & Security Review*, 2018, Vol. 34, 2, pp. 398-404.

Zhang C., Hallbeck M.S., Salehinejad H., Thiels C., *The integration of artificial intelligence in robotic surgery: A narrative review*, in *Surgery*, 2024, vol. 176, 3, pp. 552-557.

Ziwei H., *et al., The application of Internet of Things in smart healthcare sector: a bibliometric and deep study,* in *Heliyon,* 2024, 10, pp. 1-11.

II. La disciplina del trattamento dei dati personali in ambito sanitario

di *Anna Zilio*

1. Privacy e sanità: concetti e istituti

1.1. La definizione di dato personale e il perimetro di applicazione del GDPR

Il concetto di "dato personale" è attualmente definito dal Regolamento UE 2016/679 (di seguito anche solo "Regolamento" o "GDPR") che all'art. 4 lo definisce come "qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»). Si considera identificabile la persona fisica che può essere "identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale"[1]. Tale definizione risulta fondamentale al fine di comprendere e definire l'ambito di applicazione del

1. Regolamento Generale sulla Protezione dei dati, Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016.

Regolamento poiché lo stesso andrà preso in considerazione in tutte – ed esclusivamente – le attività di trattamento che comprenderanno un dato, per l'appunto, personale e, quindi, in tutte le ipotesi in cui vi sia la necessità di tutela di persone fisiche interessate al trattamento.

Sul punto, al fine di definire il perimetro di applicazione del GDPR, nonché di fornire delle linee guida per i soggetti coinvolti nella gestione delle attività di trattamento, si può ricordare quanto il *Working Party art. 29* (di seguito anche solo "WP 29") ha stabilito con il Parere n. 4 del 2007[2], individuando i quattro elementi fondamentali che caratterizzano il dato personale, ovverosia "qualsiasi informazione", "concernente", una "persona fisica", "identificata o identificabile".

Per quanto concerne il primo elemento, ovvero "qualsiasi informazione", il WP 29 precisa che il concetto di dato personale comprende qualsiasi tipo di informazione su una persona e, dunque, può includere sia informazioni "oggettive" come la presenza di una data sostanza nel sangue di una persona, sia informazioni "soggettive" come opinioni o valutazioni. In merito, si precisa che affinché l'informazione diventi un "dato personale" non è necessario che la stessa sia vera o dimostrata. In tal senso, infatti, le norme sulla protezione dei dati disciplinano in modo specifico l'ipotesi in cui le informazioni non siano corrette, conferendo all'interessato il diritto di accesso a quelle informazioni, nonché il diritto di contestarle mediante gli adeguati mezzi d'impugnazione. Inoltre, dal punto di vista del contenuto dell'informazione, il concetto di dato personale comprende qualsiasi tipo d'informazione, ovvero sia le informazioni personali, considerate "dati sensibili"[3] sia le informazioni di ordine più generale. L'espressione "dati personali", infatti, comprende sicuramente informazioni sulla vita privata e familiare in senso stretto, ma anche sulle attività di qualunque tipo, come quelle in merito ai rapporti di lavoro o al comportamento economico e sociale di una persona.

I dati personali comprendono quindi informazioni sulle persone, a prescindere dalla posizione o dalle capacità delle stesse (ovvero in quanto consumatori, pazienti, lavoratori, clienti, ecc.)[4].

Infine, dal punto di vista del formato dell'informazione o del supporto usato per la raccolta e il trattamento della stessa, la definizione di dato personale comprende le informazioni disponibili in qualsiasi forma, sia essa

2. Gruppo di Lavoro Art. 29, *Parere 4/2007 sul concetto di dati personali*, 20 giugno 2007 p. 2.

3. Direttiva UE 95/46/CE sulla protezione dei dati personali Direttiva, 24 ottobre 1995, art. 8.

4. Gruppo di Lavoro Art. 29, *Parere 4/2007 sul concetto di dati personali*, 20 giugno 2007, pp. 7-8.

alfabetica, numerica, grafica, fotografica o acustica, nonché le informazioni registrate su carta e le informazioni conservate nella memoria di un computer attraverso un codice binario o in una videocassetta. Quindi, in tal senso, anche i dati in forma di suoni e immagini costituiscono dati personali ai sensi del Regolamento, poiché gli stessi costituiscono informazioni relative a una persona fisica determinata o determinabile.

Con riferimento al secondo elemento, il WP 29 specifica che, in linea generale, un'informazione si può considerare "concernente" una persona se la riguarda. In molte situazioni questa relazione può essere stabilita facilmente come, ad esempio, nel caso dei dati ricavabili dai risultati di un test medico di un paziente contenuti nella sua cartella clinica. Vi sono, tuttavia, delle differenti situazioni in cui non è sempre facile determinare se le informazioni oggetto del trattamento "concernono" una persona. In alcuni casi, infatti, le informazioni trasmesse dai dati concernono oggetti e non persone.

Tali oggetti appartengono di solito a qualcuno e, dunque, solo indirettamente tali informazioni possono essere considerate come "concernenti" le persone o gli oggetti. Allo scopo di fornire delle linee guida sul punto, si potrebbe affermare che, per stabilire se i dati "concernono" dovremmo ricorrere a un elemento di "contenuto" oppure di "finalità" oppure ancora di "risultato".

L'elemento di "contenuto" è presente nei casi in cui l'informazione riguardante una particolare persona sia fornita a prescindere dalla finalità del responsabile del trattamento o di terzi, o dal suo impatto sulla persona interessata. Un'informazione "concerne", quindi, una persona quando la "riguarda", e questo deve essere valutato alla luce delle circostanze del caso di specie.

Anche un elemento di "finalità" può far sì che le informazioni "concernano" una data persona. Tale elemento può essere considerato presente quando i dati sono o saranno probabilmente utilizzati, tenendo conto di tutte le circostanze del caso di specie, al fine di valutare, trattare in un dato modo o influire sullo stato o sul comportamento di una persona.

Una terza eventualità in cui possiamo dire con certezza che un dato personale è "concernente" una persona specifica emerge quando vi è un elemento di "risultato". Nonostante l'assenza di elementi di "contenuto" o di "finalità" è, infatti, possibile dire che i dati "concernono" una persona quando il loro impiego può avere un impatto sui diritti e sugli interessi di quella persona, tenendo conto di tutte le circostanze del caso di specie.

In linea generale, secondo quanto definito nel Parere 4/2007 si può considerare "identificata" la persona fisica che, all'interno di un gruppo,

è "distinta" da tutti gli altri membri e, quindi, la persona fisica è "identificabile" quando, sebbene non sia stata ancora identificata, è comunque possibile identificarla in un secondo momento e mediante l'analisi dei dati che la riguardano.

L'identificazione si fonda di norma su informazioni particolari che possiamo chiamare "identificatori" e che hanno un rapporto particolarmente stretto e privilegiato con la persona interessata. Ad esempio, segni esterni identificativi riguardano l'aspetto, l'altezza, il colore dei capelli, l'abbigliamento, ecc., oppure una qualità che non può essere percepita immediatamente, come la professione, una funzione o un nome. La Direttiva UE 95/46/CE, cui si riferiva il parere citato, faceva riferimento a questi "identificatori" nella definizione di "dati personali" di cui all'articolo 2 che affermava, appunto, che una persona fisica "può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale"[5].

Il considerando 26 della Direttiva[6] prestava particolare attenzione al termine "identificabile", quando disponeva che "per determinare se una persona sia tale, è opportuno prendere in considerazione l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri per identificare detta persona". Ciò significa che la sola possibilità, in via ipotetica, di distinguere una persona non basta per considerare tale persona "identificabile" se, tenendo conto dell'"insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri per identificare detta persona", quella possibilità non esiste o è trascurabile. In tal caso, la persona non dovrebbe dunque essere considerata "identificabile" e le informazioni non configurerebbero quindi "dati personali", nemmeno ai sensi dell'attuale Regolamento.

Il criterio dell'"insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri" deve, in particolare, tenere conto di tutti i fattori in gioco. Il costo dell'identificazione è sicuramente uno di questi fattori fondamentali, ma non può essere considerato in via esclusiva. La finalità, il modo in cui viene strutturato il trattamento, il vantaggio atteso dal responsabile del trattamento, gli interessi dei singoli, nonché il rischio di disfunzioni organizzative (es. violazioni degli obblighi

5. Direttiva UE 95/46/CE sulla protezione dei dati personali Direttiva, 24 ottobre 1995, art. 2.

6. Direttiva UE 95/46/CE sulla protezione dei dati personali Direttiva, 24 ottobre 1995, Considerando 26.

di riservatezza) e tecniche sono tutti elementi da prendere in considerazione. Per altro verso, trattandosi di un'analisi che richiede della dinamicità, non possiamo non considerare che bisognerebbe senza dubbio valutare anche lo stato dell'arte della tecnologia impiegata al momento del trattamento, così come le possibilità di sviluppo della stessa nel periodo di riferimento in cui saranno trattati i dati.

Il WP 29 specifica, in aggiunta, che attualmente l'identificazione può non essere possibile con tutti i mezzi di cui è ragionevolmente possibile avvalersi oggi. Se i dati sono destinati a essere conservati per un mese, forse l'identificazione non è possibile nell' "arco di vita" dell'informazione e in tal caso i dati non dovrebbero essere considerati dati personali. Se, invece, l'intenzione è conservare i dati per 10 anni, il responsabile del trattamento dovrebbe considerare la possibilità che l'identificazione avvenga anche al nono anno, il che li renderebbe dati personali in quel preciso momento e non fin dall'inizio del trattamento. È importante, quindi, che il sistema implementato e adottato per il trattamento dei dati sia in grado di adattarsi a questi sviluppi via via che gli stessi si verificano, integrando le misure tecniche e organizzative più appropriate in tempo utile[7].

Come si è già detto, un fattore rilevante per valutare "tutti i mezzi che possono essere ragionevolmente utilizzati" per identificare le persone sarà, di fatto, la finalità perseguita dal responsabile del trattamento nel trattare i dati. Le autorità nazionali per la protezione dei dati si sono trovate di fronte a casi in cui, da un lato, il responsabile del trattamento sostiene che vengono trattate solo informazioni sparse, senza riferimenti a nomi o altro identificatore diretto, ritenendo che i dati non dovrebbero essere assimilati a dati personali, né dovrebbero essere soggetti alle norme di protezione dei dati. Dall'altro lato però, il trattamento di quelle informazioni ha senso soltanto se permette di identificare persone specifiche e di trattarle in un determinato modo. Nei casi, quindi, in cui la finalità del trattamento implichi l'identificazione di persone si può facilmente presumere che il responsabile del trattamento o qualunque altra persona coinvolta ha – o avrà – i mezzi che "possono essere ragionevolmente utilizzati" per identificare l'interessato. In effetti, pretendere che le persone non siano identificabili quando la finalità del trattamento è precisamente identificarle sarebbe una contraddizione in termini, precisa il WP 29. Pertanto, è opportuno considerare le informazioni concernenti persone identificabili come rientranti nel perimetro di operatività e tutela del Regolamento e, di conseguenza, subordinarne il trattamento alle norme sulla protezione dei dati.

7. Op. cit., p. 1.

Il concetto di identificabilità è fondamentale al fine di definire che cosa rientri nella definizione di dato personale e, dunque, nel perimetro di applicazione del GDPR.

L'art. 4, par. 1 del GDPR differenzia l'identificazione diretta, quale ad esempio il nome e cognome, ovvero un dato personale che permette di individuare direttamente la persona fisica a cui si riferisce, dall'identificazione indiretta, quale ad esempio il numero di telefono o il codice fiscale che, pur trattandosi indubbiamente di dati personali, si tratta di dati personali che permettono di indentificare uno specifico individuo solo mediante l'accesso a un apposito registro o, in ogni caso, mediante un'azione specifica e ulteriore. In aggiunta, il Considerando 26 del GDPR sancisce che "[...] per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente. Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici. [...]"[8].

Secondo quanto previsto dal Regolamento, quindi, i principi relativi alla tutela dei dati personali non troverebbero applicazione nel caso di informazioni anonime, ovverosia informazioni che non si riferiscono a una persona fisica identificata o identificabile, nonché ai dati personali sottoposti a processi di anonimizzazione che non consentono l'identificazione dell'interessato a cui si riferiscono.

Pur non fornendo il GDPR una specifica definizione di che cosa debba intendersi per anonimizzazione dei dati personali, la stessa può essere ricavata sia dal Considerando 26[9], sia dal confronto con la definizione di dato pseudonimizzato fornita dal GDPR all'art. 4, n. 5)[10]. Nel dettaglio, pseudonimizzare un dato personale significa trattare lo stesso in modo tale che non possa più essere attribuito a un interessato specifico senza l'utilizzo di informazioni aggiuntive e, a condizione, che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile. Dunque, differentemente dai dati anonimi,

8. Regolamento Generale sulla Protezione dei dati, Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, Considerando 26.

9. Op. cit., p. 1.

10. Ivi, art. 4, n. 5.

i dati pseudonimizzati, essendo stati sottoposti a una procedura reversibile, seppure mediante un'azione aggiuntiva, possono essere ricondotti a una persona fisica e, alla luce di ciò, rientreranno nell'ambito di applicazione del Regolamento.

1.2. I principi del Regolamento UE 2016/679 (cenni)

Prima di concentrare la trattazione sul trattamento dei dati in ambito sanitario, al fine di definire brevemente i principi e i concetti generali relativi al trattamento dei dati sanitari disciplinati dalla normativa di riferimento, ci è utile ripercorrere i principi fondamentali applicabili al trattamento dei dati personali, disciplinati dall'art. 5 del GDPR[11].

Ogni trattamento di dati personali deve avvenire nel rispetto dei seguenti principi:

1. il principio di liceità, correttezza e trasparenza del trattamento, nei confronti dell'interessato;
2. il principio di limitazione della finalità del trattamento, compreso l'obbligo di assicurare che eventuali trattamenti successivi non siano incompatibili con le finalità della raccolta dei dati;
3. il principio di minimizzazione dei dati: ossia, i dati devono essere adeguati pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento;
4. il principio di esattezza e aggiornamento dei dati, compresa la tempestiva cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento;
5. il principio di limitazione della conservazione, ovvero, è necessario provvedere alla conservazione dei dati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento;
6. il principio di integrità e riservatezza poiché occorre garantire la sicurezza adeguata dei dati personali oggetto del trattamento.

Sul punto, il Regolamento oltre a richiedere che il Titolare del trattamento rispetti tali principi fondamentali, specifica che lo stesso deve essere essere "in grado di comprovarlo". Tale principio, detto di "responsabilizzazione" (o accountability) viene specificatamente esplicato anche dall'articolo 24, paragrafo 1, del GDPR che afferma "il Titolare mette in atto misure tecni-

11. Ivi, art. 4, n. 5.

che e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente Regolamento"[12]. Quindi, la normativa europea in materia di protezione dei dati affida al Titolare del trattamento il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto di alcuni criteri specifici indicati nel Regolamento.

Il primo fra tali criteri è la cd. *data protection by default and by design*, prevista dall'articolo 25 del GDPR, ossia la necessità di prevedere delle garanzie nell'attività di trattamento "al fine di soddisfare i requisiti"[13] del Regolamento e tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati. Tutto questo, ovvero le considerazioni in materia di data *protection by design and by default*, devono avvenire a monte, prima di procedere al vero e proprio trattamento dei dati. Secondo l'art. 25 paragrafo 1 del Regolamento deve avvenire "sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso", richiedendo un'analisi preventiva da parte dei titolari, ovvero delle attività in tal senso specifiche e dimostrabili.

Tra le attività fondamentali che il Titolare del trattamento è chiamato a porre in essere vi sono le attività connesse alla gestione del rischio inerente al trattamento, ossia il rischio di impatti negativi sulle libertà e i diritti degli interessati[14]. Tali impatti dovranno essere analizzati attraverso il processo di valutazione previsto dagli artt. 35 e 36[15]. All'esito di tale attività di valutazione del rischio, il Titolare del trattamento potrà:

- decidere se iniziare il trattamento, adottando delle misure tecniche e organizzative adeguate alla mitigazione del rischio;
- oppure, se il rischio continuerà a risultare elevato, consultare l'autorità di controllo competente che avrà il compito di indicare le misure ulteriori da implementare a cura del Titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell'articolo 58 del Regolamento[16].

I principi sopracitati, dunque, dovranno essere sempre considerati dal Titolare nella gestione delle attività di trattamento e, in particolare, assu-

12. Ivi, art. 24.
13. Ivi, art. 25.
14. Ivi, Considerando nn. 75 e 77.
15. Ivi, artt. 35 e 36.
16. Ivi, art. 58.

meranno un ruolo di rilievo nella gestione delle attività di trattamento che coinvolgono categorie particolari di dati personali[17], quali i dati relativi alla salute.

1.3. I dati personali in ambito sanitario (definizioni)

L'articolo 9 del Regolamento disciplina il trattamento dei dati cd. particolari, tra i quali rientrano anche i dati relativi alla salute, unitamente ai dati genetici e biometrici.

Per quanto riguarda, dunque, il trattamento delle "categorie particolari di dati personali", lo stesso è generalmente vietato, a meno che il Titolare del trattamento non dimostri, in conformità al sopracitato principio di *accountability*, di soddisfare almeno una delle condizioni fissate all'articolo 9, paragrafo 2[18] del Regolamento, ovverosia:

- l'interessato abbia prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche;
- il trattamento sia effettuato da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali;
- il trattamento riguardi dati personali resi manifestamente pubblici dall'interessato;
- il trattamento sia necessario per specifici scopi, ovvero:
  i. per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell''interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale;
  ii. 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;
  iii. per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali;
  iv. per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri;
  v. per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o

17. Ivi, art. 9.
18. Ivi, art. 9, par. 2.

terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali;
vi. per motivi di interesse pubblico nel settore della sanità pubblica;
vii. per il perseguimento di fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

Premesse, quindi, le prime indicazioni fornite dal GDPR in materia di trattamento dei dati relativi alla salute, al fine di perimetrare l'attività di analisi, dobbiamo fornire una definizione degli stessi. In merito, per la nozione di dati "genetici", "biometrici" e "relativi alla salute" è opportuno fare riferimento all'art. 4 del GDPR[19].

I "dati genetici" ai sensi dell'art. 4 punto 13) del Regolamento sono definiti come "i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione"[20]. In aggiunta, il Considerando 34 specifica che per dati genetici devono essere intesi i dati personali relativi alle caratteristiche genetiche, ereditarie o acquisite, di una persona fisica, che "risultino dall'analisi di un campione biologico della persona fisica in questione, in particolare dall'analisi dei cromosomi, dell'acido desossiribonucleico (DNA) o dell'acido ribonucleico (RNA), ovvero dall'analisi di un altro elemento che consenta di ottenere informazioni equivalenti"[21]. In tale ambito si è, inoltre, pronunciato anche il Garante Privacy con il Provvedimento n. 146/2019 "recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del D.lgs. 101/2018"[22] che, oltre a riprendere la definizione fornita dal GDPR, prevede delle specifiche misure e strumenti di cautela da adottare per la custodia e la sicurezza dei dati genetici e dei campioni biologici.

Per quanto concerne i "dati biometrici", gli stessi sono definiti dall'art. 4 n. 14 del GDPR come i "i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici"[23]. Oggetto di partico-

19. Ivi, art. 4.
20. Ivi, art. 4, n. 13.
21. Ivi, Considerando 34.
22. Autorità Garante per la protezione dei dati personali, *Provvedimento n. 146/2019 "recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del D.lgs. 101/2018"*, 22 luglio 2019.
23. Ivi, art. 4, n. 14.

lare attenzione è stato, in particolare, l'elemento testuale che specifica che, affinché un dato biometrico possa essere considerato parte della categoria così come definita dal GDPR, esso deve essere sottoposto a un "trattamento tecnico specifico" che consente o confermi l'identificazione univoca della persona. In merito, si è espresso sia il Garante Privacy, anteriormente all'entrata in vigore del GDPR, con il Provvedimento n. 345/2017[24] specificando che "il presupposto perché il trattamento delle immagini possa essere qualificato come biometrico è che i confronti finalizzati al riconoscimento dell'individuo siano automatizzati mediante appositi strumenti hardware o software", sia lo stesso Regolamento che al Considerando 51 chiarisce che "il trattamento di fotografie non dovrebbe costituire sistematicamente un trattamento di categorie particolari di dati personali, poiché esse rientrano nella definizione di dati biometrici soltanto quando siano trattate attraverso un dispositivo tecnico specifico che consente l'identificazione univoca o l'autenticazione di una persona fisica [...]".

Passando, infine, alla definizione di dati relativi alla salute fornita dal GDPR, all'art. 4, n. 15 gli stessi sono definiti come "i 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"[25], mentre al Considerando 35 prevede che "nei dati personali 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"[26] Precisamente, questi comprendono:

- informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria o della relativa prestazione;
- un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco a fini sanitari;
- le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici;
- qualsiasi informazione riguardante, a titolo esemplificativo una malattia, una disabilità, il rischio di malattie, l'anamnesi medica, i trattamenti cli-

24. Autorità Garante per la protezione dei dati personali, *Provvedimento n. 345/2017 "Verifica preliminare. Riconoscimento via webcam dei partecipanti a corsi di formazione in diretta streaming"*, 26 luglio 2017.

25. Ivi, art. 4, n. 15.

26. Ivi, Considerando 35.

nici o lo stato fisiologico o biomedico dell'interessato, indipendentemente dalla fonte, quale un medico o altro operatore sanitario, un ospedale, un dispositivo medico o un test diagnostico in vitro.

Con riferimento alla normativa italiana e, in particolare, al D.lgs. 101/2018 si specifica che lo stesso si esprime, all'art. 2-*septies*, in materia di trattamento di dati relativi alla salute richiamando l'art. 9 del GDPR e chiarendo che per gli stessi sono previste delle misure di garanzia ulteriori rispetto a quanto disciplinato a livello europeo[27].

Fornita, quindi, una chiara definizione di che cosa debba intendersi per dato genetico, biometrico e dato relativo alla salute, si precisa che l'art. 9 del GDPR, in generale, vieta il trattamento di tali dati, salvo poi indicare delle specifiche eccezioni a tale divieto. Il trattamento di tali dati è, infatti, consentito nel caso in cui:

- l'interessato abbia prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche;
- il trattamento sia necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che 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;
- 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, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;
- 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;

27. D.lgs. 10 agosto 2018, n. 101, Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)", G.U. 4 settembre 2018.

- il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici.

Concluse, quindi, le dovute premesse relative al perimetro di applicazione della normativa privacy in materia di dati personali in ambito sanitario, sarà necessario approfondirne la disciplina, le misure e le tutele previste sia dalla normativa in materia che dai provvedimenti e dalle linee guida fornite dalle autorità di riferimento.

2. La disciplina del trattamento dei dati personali in ambito sanitario

2.1. I provvedimenti dell'Autorità Garante Privacy italiana

Come anticipato, nel panorama legislativo nazionale con il D.lgs. 101/2018 il legislatore si è posto l'obiettivo di recepire quanto previsto dal GDPR e adeguare, modificandolo, il D.lgs. 193/2003 ("Codice della Privacy")[28]. Sul punto, è opportuno evidenziare che il Codice della Privacy mette in luce il ruolo dell'Autorità Garante per la protezione dei dati personali, ovvero il cd. Garante Privacy, chiamato a ricoprire un ruolo di indirizzo e garanzia in materia. In particolare, il nuovo art. 2-*quater* del Codice della Privacy[29] prevede espressamente che il Garante Privacy promuova l'adozione di regole deontologiche con riguardo al trattamento dei dati relativi alla salute, genetici e biometrici. Inoltre, l'art. 2-*septies*[30] del Codice della Privacy, introdotto dal D.lgs. 101/2018, prevede che l'autorità sia chiamata ad emanare un provvedimento, con cadenza almeno biennale, che esplichi le linee guida, le raccomandazioni e le migliori prassi in materia di protezione dei dati personali, nonché dell'evoluzione scientifica e tecnologica e dell'interesse alla libera circolazione dei dati nell'Unione Europea.

È chiaro, quindi, il tentativo dell'autorità italiana incaricata della tutela dei dati personali di adeguare e attualizzare il panorama legislativo nazionale alle nuove disposizioni previste dal Regolamento e dagli indirizzi dell'Unione Europea. Nonostante il tentativo di un intervento legislativo esaustivo,

28. D.lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonchè alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE. G.U. 29 luglio 2003

29. Ivi, art. 2-quater.

30. Ivi, art. 2-septies.

dall'entrata in vigore del GDPR, gli operatori del settore sanitario si sono più volte rivolti al Garante Privacy al fine di ottenere degli indirizzi chiarificatori in materia di trattamento dei dati in ambito sanitario, nonché delle precisazioni in merito alle misure da adottare e agli adempimenti da porre in essere.

Con il Provvedimento n. 55/2019 "Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario"[31] il Garante Privacy ha, quindi, fornito delle prime istruzioni operative per il personale sanitario.

In tale documento il Garante Privacy si esprime, in primo luogo, sulle informazioni da fornire all'interessato coinvolto nel trattamento dei dati personali. L'autorità richiama, infatti, il principio di trasparenza previsto dall'art. 5, par. 1, lett. a) del Regolamento che impone ai titolari di informare l'interessato sui principali elementi del trattamento che li coinvolge, al fine di renderli consapevoli sulle principali caratteristiche dello stesso. A tal riguardo viene precisato che, nel rispetto dell'obbligo di comunicare gli elementi di cui agli artt. 13 e 14 del Regolamento, le informazioni da rendere all'interessato vanno rese in forma concisa, trasparente, intelligibile e facilmente accessibile, con linguaggio semplice e chiaro[32]. Inoltre, per quanto concerne le modalità con cui deve essere fornita l'informativa, alla luce del principio di responsabilizzazione di cui all'art. 5 del Regolamento, spetta al Titolare scegliere le modalità più appropriate al caso di specie, posto che tale modalità dovrà sempre tenere in considerazione le circostanze del trattamento, nonché il contesto in cui viene effettuato (ad esempio, il dispositivo utilizzato, la natura dell'interazione con il titolare e le eventuali limitazioni che implicano tali fattori[33]).

Per quando riguarda il contenuto dell'informativa da fornire all'interessato, invece, il Regolamento specifica e integra quelli che erano gli elementi informativi già previsti dall'art. 13 del Codice della Privacy. Pertanto, l'informativa, predisposta in passato dai titolari dovrebbe essere aggiornata e integrata solo con riferimento agli elementi di novità previsti dagli artt. 13 e 14 del Regolamento.

Con specifico riferimento all'attività posta in essere da Titolari del trattamento operanti in ambito sanitario che effettuano una pluralità di opera-

31. Autorità Garante Privacy, *Provvedimento n. 55/2019 "Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario"*, 7 marzo 2019.

32. Cfr. art. 12, par. 1, del Regolamento Ue 2016/679 e art. 78 del Codice della Privacy.

33. Ivi, Considerando 58.

zioni particolarmente complesse (es. aziende sanitarie), il Garante Privacy ritiene opportuno suggerire di fornire all'interessato le informazioni previste dall'art. 13 del Regolamento in modo progressivo. In tal senso, quindi, i pazienti di una struttura sanitaria potrebbero in prima battuta ricevere solo le informazioni relative ai trattamenti che rientrano nell'ordinaria attività di erogazione delle prestazioni sanitarie, mentre le informazioni relative a particolari attività di trattamento (es. fornitura di presidi sanitari, modalità di consegna dei referti medici *on-line*, finalità di ricerca) potrebbero essere rese successivamente e solo ai pazienti effettivamente interessati da tali servizi e da tali ulteriori trattamenti.

Infine, per quanto riguarda il tempo di conservazione dei dati personali trattati in ambito sanitario, il Garante Privacy ricorda che, con riferimento alla documentazione sanitaria, l'ordinamento giuridico fornisce differenti indicazioni circa i tempi di conservazione della stessa (ad esempio: la documentazione inerente agli accertamenti effettuati nel corso delle visite per il rilascio del certificato di idoneità all'attività sportiva agonistica deve essere conservato, a cura del medico visitatore, per almeno cinque anni, le cartelle cliniche, unitamente ai relativi referti, vanno conservate illimitatamente[34], la documentazione iconografica radiologica, deve essere conservata per un periodo non inferiore a dieci anni)[35].

Nell'ipotesi in cui, d'altro canto, i tempi di conservazione di specifici documenti sanitari non siano stabiliti da una disposizione normativa, il titolare del trattamento, in virtù del principio di responsabilizzazione, dovrà individuare tale periodo in modo che i dati siano conservati, in una forma che consenta l'identificazione degli interessati, per un arco di tempo non superiore al conseguimento delle finalità per le quali i dati sono trattati e indicare tale periodo (o i criteri per determinarlo) tra le informazioni da rendere all'interessato ai sensi dell'art. 13 GDPR.

La secondo misura su cui si sofferma il Garante Privacy nel sopracitato provvedimento riguarda la designazione del Responsabile della protezione dei dati (RDP, *Data Protection Officer,* DPO) ai sensi dell'art. 37 del Regolamento[36]. Si ritiene, infatti, che i trattamenti dei dati personali relativi a pazienti effettuati da un'azienda sanitaria appartenente al SSN devono essere ricondotti a quelli per i quali è prevista la designazione obbligatoria del RPD, per due ordini di ragioni. Da un lato, infatti, gli stessi potrebbero, in genere, avere natura giuridica di "organismo pubblico", mentre dall'altro lato gli stes-

34. Circolare del Ministero della Sanità del 19 dicembre 1986 n.900 2/AG454/260.
35. Art. 4, d.m. 14 febbraio 1997.
36. Ivi*,* art. 37.

si potrebbero essere ricondotti alla condizione prevista dall'art. 37, par. 1, lett. c), considerato che le attività principali delle aziende sanitarie, in qualità di Titolari del trattamento consistono nel trattamento, su larga scala, di dati sulla salute. In ogni caso, anche il trattamento dei dati relativi a pazienti svolto da un ospedale privato, da una casa di cura o da una residenza sanitaria assistenziale (RSA) rientrerebbe in linea generale, nel concetto di larga scala.[37]

Circa il singolo professionista sanitario che opera in regime di libera professione a titolo individuale, il provvedimento chiarisce che lo stesso non è tenuto alla designazione del Responsabile della Protezione dei dati personali, ovvero il DPO, poiché, secondo quanto indicato nel Considerando n. 91 del Regolamento[38], i trattamenti dallo stesso effettuati non possono essere classificati come dati personali trattati su larga scala.

Infine, il Garante Privacy si esprime anche sull'adozione del Registro dei trattamenti ex art. 30 del GDPR[39], precisando che la tenuta del registro costituisce un elemento essenziale per la corretta gestione e tracciabilità dei trattamenti, nonché per l'efficace e necessaria individuazione di quelli a maggior rischio per gli interessati.

L'adozione del Registro dei trattamenti in ambito sanitario risulta, quindi, obbligatoria. Infatti, essendo le fattispecie di esenzione di cui all'art. 30, par. 5 del Regolamento tra loro alternative[40], la deroga alla tenuta del registro non opera in presenza anche di uno solo degli elementi indicati dal predetto par. 5, ovvero: il trattamento che presenta un rischio per i diritti e le libertà per l'interessato; il trattamento non occasionale; il trattamento che include categorie particolari di dati di cui all'art. 9 o dati relativi a condanne penali e a reati. Tutto ciò, in aggiunta, in coerenza con la circostanza che il registro delle attività del trattamento costituisce uno strumento di *accountability* e di gestione del rischio.

Per le suddette ragioni, si ritiene, quindi, che non ricadono nelle ipotesi di esenzione dall'obbligo di tenuta del registro i singoli professionisti sanitari che agiscano in libera professione, i medici di medicina generale/pediatri di libera scelta, gli ospedali privati, le case di cura, le RSA e le aziende sanitarie appartenenti al SSN, nonché le farmacie, le parafarmacie e le aziende ortopediche.

---

37. Comitato Europeo per la protezione dei dati, *Linee guida sui Responsabili della protezione dei dati*, adottate il 13 dicembre 2016, versione emendata e adottata in data 5 aprile 2017.

38. Ivi, Considerando 91.

39. Cfr. Regolamento Ue 2016/679, Considerando n. 82.

40. Cfr. Gruppo di lavoro Art. 29 per la protezione dei dati, *Position paper related to article 30(5)*, 19 aprile 2018.

2.2. I ruoli privacy coinvolti nel trattamento dei dati personali

Il provvedimento del 2019 del Garante Privacy mette, quindi, in luce una serie di primi adempimenti che i Titolari del trattamento di dati personali in ambito sanitario sono chiamati a porre in essere, ovvero fornire un'idonea informativa agli interessati rispetto alle finalità, alle modalità e ai tempi di conservazioni dei dati personali, l'individuazione di un Responsabile per la Protezione dei Dati (DPO) e la tenuta di un Registro dei trattamenti ai sensi dell'art. 30 del GDPR.

Una corretta gestione della privacy richiede, tuttavia, anche una definizione dei ruoli dei soggetti coinvolti nelle attività di trattamento[41], ovvero, oltre al Titolare del trattamento, anche i contitolari, il Responsabile, il subresponsabile e gli autorizzati al trattamento.

Partendo dal Titolare del trattamento, lo stesso viene definito dall'art. 4, punto 7 del GDPR, come la "persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali"[42].

L'*European Data Protection Board*, con le "Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR"[43] fornisce alcune specifiche indicazioni utili al fine di agevolare l'identificazione del Titolare del trattamento. In particolare, l'EDPB specifica che per quanto concerne i soggetti che possono assumere il ruolo di Titolare del trattamento, non sono previste delle specifiche limitazioni, anche se operativamente è di solito l'organizzazione in quanto tale e non una persona fisica, quale l'amministratore delegato o un dipendente, ad agire in qualità di Titolare del trattamento. In aggiunta, per individuare la titolarità del trattamento, possono essere seguite diverse strade. Infatti, se in alcuni casi è chiaro che la stessa può essere definita a norma di legge e in altri può essere ricavata da un'analisi degli elementi fattuali o del caso concreto, in altri ancora, vi sono delle attività di trattamento che sono naturalmente connesse e riconducibili al ruolo ricoperto da un determinato soggetto (es. il datore di lavoro rispetto al trattamento dei dati dei dipendenti, l'editore rispetto agli abbonati o un'associazione rispetto ai membri della stessa). Infine, per essere qualificato come Titolare del trattamento non è necessario che tale

41. Fiordalisi G., *Inquadramento e istituti di base,* in Bolognini L. e Zipponi S. (a cura di), *Privacy e diritto dei dati sanitari,* Giuffrè, Milano, 2024, pp. 8-18.

42. Regolamento Ue 2016/679, art. 4, n. 7.

43. Comitato Europeo per la protezione dei dati, *Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR*, versione 2, 7 luglio 2021.

soggetto abbia accesso effettivo ai dati trattati, poiché il suo ruolo chiave si concretizza nella determinazione delle finalità e dei mezzi del trattamento.

Per quanto concerne, invece, la definizione di contitolarità, la stessa si configura nel caso in cui il trattamento coinvolga più di un soggetto, ovvero quando ai sensi dell'art. 26 del GDPR "*due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento*". La partecipazione congiunta dei due soggetti può derivare da una decisione comune, oppure può derivare da decisioni convergenti di due o più soggetti.[44] Al fine di trovare un criterio che permetta di determinare se il trattamento comprenda una contitolarità, l'EDPB suggerisce di valutare se il trattamento sarebbe o meno possibile senza la partecipazione di entrambi i soggetti, nel senso che i trattamenti svolti da ciascun soggetto sono tra loro indissociabili, indissolubilmente legati.

Una volta stabilito che si è in presenza di una contitolarità di trattamento, tra i contitolari del trattamento viene stipulato un vero e proprio "accordo di contitolarità" in cui sono determinate le rispettive responsabilità. Tale ripartizione deve riguardare il rispetto dei principi generali in materia di protezione dei dati, la base giuridica del trattamento, le misure di sicurezza, l'obbligo di notifica di violazione dei dati, le valutazioni d'impatto sulla protezione dei dati, il ricorso a responsabili del trattamento, i trasferimenti verso paesi terzi e i contatti con gli interessati e le autorità di controllo.

Il Responsabile del trattamento è, ai sensi dell'art. 4 punto 8) del GDPR "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organo che tratta dati personali per conto del titolare del trattamento"[45]. Quindi, per assumere il ruolo di Responsabile del trattamento, è necessario essere un soggetto distinto rispetto al Titolare del trattamento e trattare dati personali per conto di quest'ultimo. Il Responsabile del trattamento riceve, ai sensi dell'art. 28 del GDPR[46], delle specifiche istruzioni rispetto al trattamento da parte del Titolare. Il trattamento di dati personali da parte di un Responsabile del trattamento sarà, dunque, regolato da un contratto o da un atto giuridico di altra natura, redatto per iscritto, anche in formato elettronico. L'EDPB specifica che "Il titolare e il responsabile del trattamento possono negoziare un contratto specifico, comprensivo di tutti gli elementi obbligatori, oppure basarsi, in tutto o in parte, su clausole contrattuali tipo"[47]. Infine, il GDPR prevede all'art. 28 tutti gli elementi che devono essere disciplinati nella nomina del Responsabile anche se, in ogni caso, dovrebbe comprendere delle

44. Ivi, p. 3.
45. Regolamento Ue 2016/679, art. 4, n. 8.
46. Regolamento Ue 2016/679, art. 28.
47. Ivi, pp. 4-5.

istruzioni coerenti rispetto alle specifiche attività di trattamento condotte dal Responsabile per conto del Titolare.

L'art. 28 del GDPR prevede, inoltre, che "il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del Titolare del trattamento". È quindi espressamente prevista dal Regolamento la possibilità che il Responsabile del trattamento ricorra, a sua volta, a un sub-responsabile del trattamento per adempiere agli impegni presi con il Titolare del trattamento. Tale possibilità è, tuttavia, sancita solo laddove vi sia una autorizzazione scritta da parte del Titolare del trattamento.

Infine, l'art. 29 del GDPR statuisce che "il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento" e l'art. 2-quaterdecies del Codice Privacy "il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità"[48]. Tutti i soggetti che entrano in contatto con i dati personali e sono coinvolti nelle attività di trattamento (es. i dipendenti di un'organizzazione), ma che non ricoprono un ruolo di determinazione delle finalità, dei mezzi e delle modalità di trattamento – ruolo ricoperto dal Titolare del trattamento o dal Responsabile del trattamento per conto del Titolare – saranno nominati Autorizzati al trattamento ai sensi dell'art. 29 del Regolamento.

Anche, quindi, nel caso di attività di trattamento che coinvolgono dati relativi alla salute è chiaro che una delle prime attività che dovranno essere svolte allo scopo di verificare e garantire la compliance del trattamento dei dati personali rispetto alla normativa e alle *best practice* sarà l'identificazione e la determinazione – anche mediante atti formali – dei ruoli privacy coinvolti nel processo.

Sul punto, il Garante Privacy si è espresso nel 2020 con specifico riferimento al ruolo privacy e agli adempimenti *data protection* richiesti al medico competente che opera in materia di salute e sicurezza nei luoghi di lavoro[49] in conformità agli obblighi previsti dal D.lgs. 81/2008, cd. T.U. in materia di salute e sicurezza nei luoghi di lavoro.

---

48. Regolamento Ue 2016/679, art. 29.

49. Autorità Garante per la protezione dei dati personali, *Il ruolo del "medico competente" in materia di sicurezza sul luogo di lavoro, anche con riferimento al contesto emergenziale*, 2020.

Le modalità e le finalità delle operazioni di trattamento poste in essere dal medico competente sono determinate dalla legge che richiede al professionista di trattare i dati in modo autonomo, nel rispetto della disciplina di protezione dei dati e dei principi che regolano l'attività diagnostica e delle regole di deontologia professionale. Peraltro, dato che le sue valutazioni non possono in alcun modo essere condizionate dalle scelte organizzative e gestionali dell'ente e/o del Datore di lavoro ai sensi dell'art. 2 del D.lgs. 81/2008, il medico competente non tratterà i dati in alcuno modo "per conto" del Datore di lavoro – e, quindi, in qualità di Responsabile del trattamento – ma anzi, in qualità di Titolare del trattamento ai sensi degli artt. 4, n. 7 e 24 del Regolamento, sarà lui stesso a determinare mezzi e finalità. Lo stesso Regolamento, infatti, considera autonomamente i trattamenti necessari per le finalità di "medicina del lavoro"[50], nell'ambito della quale è riconducibile la funzione del medico e che devono, infatti, essere effettuati "sotto la responsabilità di un professionista soggetto al segreto professionale conformemente al diritto dell'Unione o degli stati membri […]"[51]. Tali trattamenti gestiti dal medico competente sono disciplinati separatamente dai trattamenti che deve porre in essere il Datore di lavoro, poiché – spiega il Garante Privacy – questi sono necessari per assolvere i propri obblighi normativi in materia di "salute e sicurezza sul lavoro"[52] e, dunque, ciò appare sufficiente a identificare il medico competente come un autonomo titolare del trattamento.

Come tale, il medico è quindi tenuto a regolare le attività di trattamento poste sotto il suo controllo in conformità alle prescrizioni della normativa privacy e del GDPR. Tra gli adempimenti che dovrà porre essere vi sono:

- l'obbligo di tenere un Registro delle attività di trattamento svolte dal Titolare sotto la propria responsabilità[53], distinto da quello del Datore di lavoro che gli ha conferito l'incarico e anche nel caso in cui sia un dipendente che svolge il ruolo di medico competente per il proprio Datore di lavoro, alla luce del fatto che tratta, in maniera non occasionale, categorie particolari di dati relativi allo stato di salute[54];
- gli obblighi informativi nei confronti degli interessati, poiché il medico competente riceve i dati anagrafici dei lavoratori dal Datore di lavoro e,

50. Regolamento Ue 2016/679, art. 9 lett. h).
51. Regolamento Ue 2016/679, art. 9, par. 3.
52. Regolamento Ue 2016/679, art. 9, lett. b) e art. 88.
53. Regolamento Ue 2016/679, art. 30, par. 1.
54. Regolamento Ue 2016/679, art. 30, paragrafo 5.

di conseguenza, potrà e dovrà fornire le informazioni richieste dal Regolamento al momento della prima comunicazione e/o incontro con l'interessato al trattamento;

- obbligo di adottare misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio[55]. In particolare, il Garante Privacy precisa che "nei casi in cui vengano utilizzati strumenti (ad es. applicativi informatici) del datore di lavoro, nel rispetto del principio di responsabilizzazione, dovranno essere adottate le misure tecniche e organizzative affinché il trattamento sia conforme alla normativa di settore in materia di salute e sicurezza sui luoghi di lavoro, garantendo, ad esempio, che i dati personali relativi alla diagnosi dei dipendenti non entrino, anche accidentalmente, nella disponibilità del datore di lavoro, predisponendo a tal fine misure che assicurino l'accesso selettivo ai dati o che li rendano non comprensibili ai soggetti non autorizzati, ad esempio mediante ricorso alla cifratura degli stessi dati"[56] In tali casi, in aggiunta, dovrà essere disciplinato anche il rapporto tra le parti ai sensi dell'art. 28 del Regolamento, prevedendo "specifiche misure organizzative volte a escludere l'accesso ai dati da parte del personale preposto agli uffici, o analoghe funzioni aziendali, che svolgono compiti datoriali (es. risorse umane, uffici disciplinari) e in generale a uffici o altro personale che trattano i dati dei dipendenti per finalità di gestione del rapporto di lavoro"[57].

Infine, per quanto riguarda l'obbligo di designazione del Responsabile della Protezione dei Dati (DPO)[58] con riferimento allo svolgimento della propria attività[59] il Garante Privacy indica, tra gli esempi di trattamento da non considerare su larga scala, quelli svolti da un singolo professionista sanitario[60]. Dunque, il medico competente non sarà tenuto a nominare un DPO.

---

55. Regolamento Ue 2016/679, art. 32.

56. Autorità Garante per la protezione dei dati personali, *Il ruolo del "medico competente" in materia di sicurezza sul luogo di lavoro, anche con riferimento al contesto emergenziale*, 2020, p. 11.

57. Ivi, pp. 11-12.

58. Regolamento Ue 2016/679, art. 37.

59. Cfr. Provvedimento n. 55/2019, Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario – n. 55 del 7 marzo 2019; nonché Considerando n. 91 del Regolamento Ue 2016/679; sul punto anche il Gruppo di lavoro Art. 29 per la protezione dei dati.

60. Gruppo di Lavoro art. 29, *Linee guida sui Responsabili della protezione dei dati*, 5 aprile 2017.

Tali adempimenti, previsti nel sopracitato documento di indirizzo del Garante Privacy con riferimento al medico competente e alle attività di trattamento dei dati personali svolti dallo stesso nei suoi adempimenti in materia di salute e sicurezza nei luoghi di lavoro, possono essere considerati dei riferimenti per quanto riguarda, in generale, gli adempimenti che ciascun Titolare o Responsabile del trattamento, coinvolto nel trattamento dei dati personali in ambito sanitario, è chiamato a considerare.

2.3. Altri adempimenti privacy

Il principio di *accountability* previsto dal GDPR, come anticipato, prevede che il Titolare e il Responsabile del trattamento non siano esclusivamente tenuti al rispetto delle prescrizioni previste dal Regolamento e, in generale, della disciplina in materia di protezione dei dati personali, ma anche a dimostrare di aver adempiuto agli obblighi e di operare in conformità.

Oltre agli adempimenti che già si sono citati perché richiesti al medico competente (ovvero Registro dei trattamenti, informative privacy e misure tecniche e organizzative adeguate), gli enti e i soggetti, sia pubblici che privati, che assumo un ruolo nel trattamento dei dati in ambito sanitario, sono chiamati a:

- adottare un Modello Organizzativo Privacy (cd. MOP), ovvero l'insieme delle procedure di *data protection*, del Registro dei trattamenti, delle informative privacy, delle misure tecniche e organizzative e dell'organigramma dei ruoli privacy, al fine di implementare un sistema di gestione degli adempimenti di *data protection* che permetta agilmente di individuare ruoli e responsabilità;
- svolgere una valutazione d'impatto sulla protezione dei dati personali (*Data Protection Impact Assessment*, cd. DPIA)[61] che, ai sensi del Regolamento, deve essere svolta dai Titolari del trattamento di valutare i rischi per i diritti e le libertà degli interessati coinvolti nelle attività di trattamento;
- adottare delle specifiche procedure *data protection* (quali le procedure per la gestione delle istanze degli interessati) e, nel dettaglio, una procedura relativa alla gestione di eventuali *data breach*, ovvero delle eventuali violazioni della sicurezza del sistema informativo che comportano la distruzione, la perdita, l'alterazione o la divulgazione di dati perso-

61. Regolamento Ue 2016/679, art. 35.

nali, al fine di formalizzare delle indicazioni e delle istruzioni operative sulle azioni da svolgere in conformità delle disposizioni dell'art. 33 del GDPR[62].

Tali attività, che dovranno, quindi, essere considerate ogni qualvolta ci si trovi a disciplinare le attività sanitarie che comprendo un trattamento di dati personali relativi alla salute, dovranno poi essere integrate con ulteriori considerazioni e approfondimenti di *compliance* qualora il trattamento sia reso più complesso dall'utilizzo di strumenti che possono rientrare nell'ampio concetto di "sanità digitale". L'impiego sempre più diffuso e articolato di software e sistemi digitali che ottimizzano le attività svolte dai soggetti operanti nel settore sanitario richiede, infatti, delle considerazioni ulteriori, alla luce delle normative specificatamente adottate e dei maggiori rischi che comportano per gli interessati.

3. La sanità digitale

3.1. L'utilizzazione dei software in ambito sanitario

Come accennato, gli operatori del settore sanitario, sia pubblici che privati (es. ospedali, cliniche, medici di base, laboratori di analisi e centri di ri-

62. Regolamento Ue 2916/679, art. 33 "1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo. 2. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione. 3. La notifica di cui al paragrafo 1 deve almeno: a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione; b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni; c) descrivere le probabili conseguenze della violazione dei dati personali; d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi. 4. Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo. 5. Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente articolo".

cerca) utilizzano, per finalità amministrative e cliniche, con sempre maggiore frequenza e concentrazione, dei software sviluppati per l'area medicale[63].

Tali software comprendono inevitabilmente il trattamento di dati personali, ovvero sia dati comuni del personale medico che dati relativi alla salute dei pazienti. Dunque, per disciplinare l'utilizzo degli stessi dovrà essere considerata sia la normativa in materia di dati personali, sia la specifica normativa di settore applicabile ai *software* e agli strumenti digitali.

Alcuni *software* utilizzati in ambito medicale appartengono, in particolare, alla categoria dei dispositivi medici e, in quanto tali, sono disciplinati dal Regolamento UE 2017/745 sui dispositivi medici, il cd. *Medical Device Regulation* (anche solo "MDR") e definiti come "qualunque strumento, apparecchio, apparecchiatura o *software* destinato dal fabbricante a essere impiegato sull'uomo, da solo o in combinazione, per una o più destinazioni d'uso mediche specifiche" di diagnosi e cura[64]. Dal punto vista degli adempimenti di *data protection* che discendono dall'utilizzo di tali *software*, le prime considerazioni da svolgere riguardano la corretta individuazione del ruolo privacy ricoperto dal fornitore di tali *software*[65], ruolo che potrebbe essere diverso a seconda dell'attività concretamente svolta nei confronti del committente.

Il fornitore sarà, infatti, qualificato come Responsabile del trattamento ai sensi dell'art. 28 del GDPR nel caso in cui il contratto di servizi stipulato con il committente includa un'attività di *hosting* dei dati personali presso i sistemi e le infrastrutture IT del fornitore del *software*[66]. Lo stesso si verificherà anche nell'ipotesi in cui, pur non essendo prevista un'attività di *hosting* da parte del fornitore, questo presti delle attività di installazione e/o manutenzione del *software* nei confronti del committente. L'individuazione e la nomina, in questi casi, del provider come Responsabile del trattamento, confermata anche nelle citate Linee Guida 7/2020 dell'*European Data Protection Board*, chiede dunque che l'ospedale, la clinica o il medico di

63. Zipponi S., Biondi S., *Tutela dei dati personali nel settore dei software di area medicale e dei dispositivi medici*, in Bolognini L.,e Zipponi S. (a cura di), *Privacy e diritto dei dati sanitari,* Giuffrè, Milano, 2024, p. 57.

64. 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, art. 2.

65. Stefanelli S., Di Nunzio A., *La governance in ambito sanitario nell'ottica del GDPR*, in M. Iaselli (a cura di), *La tutela dei dati personali in ambito sanitario*, Giuffrè, Milano, 2020.

66. *ex plurimis,* Autorità Garante per la protezione dei dati personali, Ordinanza ingiunzione nei confronti di Roma Capitale, 17 dicembre 2020.

base formalizzino un atto di nomina e/o di designazione del fornitore come Responsabile del trattamento, chiedendo allo stesso di ottemperare agli obblighi previsti dal GDPR e, in particolare, di garantire l'implementazione di misure di sicurezza adeguate a garantire la sicurezza dei dati personali coinvolti del trattamento. Tale formale designazione, quindi, servirà anche a delimitare i profili di responsabilità in capo al *software provider*. In alcuni casi, come pronunciatosi il Garante Privacy nel Provvedimento sanzionatorio erogato nei confronti di "Roma servizi per la mobilità", alcuni obblighi e adempimenti sono posti a carico del Responsabile del trattamento, e ciò a prescindere dal fatto che gli siano impartite delle specifiche istruzioni da parte del Titolare mediante la nomina[67].

Vi sono, tuttavia, delle ipotesi in cui non è così pacifica la classificazione del fornitore come Responsabile del trattamento ma, al contrario, lo stesso viene individuato come Titolare autonomo del trattamento. È il caso, ad esempio, del provider che presti il servizio di *customer support* nei confronti del cliente. Tale attività, infatti, comprende il trattamento sia dei dati personali del personale ospedaliero e/o dei pazienti, che dei dati del soggetto che richiede l'attività di manutenzione, ovvero dei dati del cliente. In tal caso, avendo questo secondo trattamento come base giuridica l'esecuzione del contratto tra fornitore e committente, lo stesso sarà eseguito dal *provider* in qualità di Titolare autonomo del trattamento.

In aggiunta, un'ulteriore ipotesi in cui il fabbricante del *software* dovrà essere qualificato come Titolare del trattamento, riguarda il trattamento dei dati personali svolto dallo stesso in adempimento degli obblighi di vigilanza che gli sono richiesti dagli artt. 87 ss. del MDR. Tale regolamento, infatti, prevede che il fabbricante dei dispositivi messi a disposizione nel mercato dell'Unione Europea sia tenuto a fare una segnalazione alle autorità competenti qualora si verifichi un incidente grave relativo a tali dispositivi. Trattandosi di adempimenti, finalità di trattamento, modalità di svolgimento dello stesso e tipologia dei dati trattati, richiesti al fornitore e definiti direttamente dalla legge, in questo caso il fabbricante sarà individuato come Titolare del trattamento.

Per quanto riguarda gli adempimenti e le accortezze richieste al fabbricante di un dispositivo medico è chiaro che gli stessi saranno piuttosto rilevanti alla luce dei dati personali che potrebbe trattare nelle attività di gestione delle segnalazioni circa gli eventi e gli incidenti relativi ai dispo-

67. Zipponi S., Biondi S., *Tutela dei dati personali nel settore dei software di area medicale e dei dispositivi medici*, in Bolognini L., Zipponi S. (a cura di), *Privacy e diritto dei dati sanitari,* Giuffrè, Milano, 2024, pp. 63-64.

sitivi stessi. Tali dati potrebbero includere, oltre ai dati personali comuni del segnalante (nome, cognome, contatto), anche e indirettamente i dati del paziente, seppur non necessari al completamento della segnalazione alle autorità competenti. Il fabbricante dovrà, dunque, adottare le misure tecniche e organizzative adeguate a limitare i rischi e a tutelare le libertà degli interessati e, a titolo esemplificativo e non esaustivo:

- il fabbricante dovrà fornire al segnalante l'informativa ai sensi dell'art. 13 del GDPR, sia nel caso in cui si tratti di un paziente che di un operatore sanitario;
- invitare il segnalante a fornire a sua volta l'informativa del fabbricante ai terzi le cui informazioni sia presenti nella segnalazione.

In aggiunta al ruolo del fabbricante, vi sarà anche quello degli ulteriori soggetti coinvolti nella commercializzazione dei software medicali, ovverosia il mandatario, l'importatore e il distributore. Tali soggetti, con riferimento all'obbligo normativo previsto dal MDR di informare il fabbricante nel caso in cui ricevano delle segnalazioni di sospetti, potrebbero essere individuati quali Titolari autonomi del trattamento. Dall'altro lato, invece, svolgendo attività di fornitura nei confronti del fabbricante che, dunque, fornirebbe loro delle specifiche istruzioni, potrebbero essere qualificati come Responsabili del trattamento. In tale situazione di incertezza normativa, gli adempimenti e la qualifica del *provider* in materia di *data protection*, non potrà che essere gestita e valutata caso per caso, sulla base delle esigenze concrete.

Un ulteriore requisito che dovrà, infine, essere considerato al fine di garantire la *compliance data protection* della progettazione dei *software* di area medicale riguarda il rispetto dei principi di *privacy by design* e *by default* previsti dell'art. 25 del GDPR.

Il primo principio, previsto dal primo paragrafo dell'art. 25 richiede che il Titolare del trattamento metta in atto delle misure tecniche e organizzative adeguate, come la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati. Tali misure devono, inoltre, tenere conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento

di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento[68].

Al secondo paragrafo, invece, il GDPR chiede al Titolare del trattamento di mettere "in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica"[69].

I commercianti e produttori dei software medicali sono, pertanto, chiamati, in virtù dei principi illustrati a porre in essere tutti gli accorgimenti tecnici e organizzativi necessari a garantire la compliance normativa dei software. Dovranno perciò essere adottate le procedure di data protection, implementate idonee misure di sicurezza e di prevenzione dei data breach, formalizzati gli atti di designazione degli autorizzati e dei responsabili del trattamento.

Dal punto di vista degli adempimenti tecnici, il Considerando 78 del GDPR specifica che "In fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati. I principi della protezione dei dati fin dalla progettazione e della protezione dei dati per impostazione predefinita dovrebbero essere presi in considerazione anche nell'ambito degli appalti pubblici"[70]. L'adempimento di tali obblighi, che in via generale gravano sul Titolare del trattamento, potrà essere contrattualmente previsto anche in capo al Responsabile del trattamento che, a seconda delle eventuale tipologia di violazione, potrà rispondere ai sensi di una responsabilità contrattuale con conseguente richiesta di risarcimento del danno, ma – ad avviso anche di Zipponi e Biondi[71] – non gli sarà addebitabile una sanzione

68. Regolamento Ue 2016/679, art. 25 par. 1.

69. Regolamento Ue 2016/679, par. 2.

70. I*vi*, Considerando 78.

71. Zipponi S., Biondi S., *Tutela dei dati personali nel settore dei software di area medicale e dei dispositivi medici*, in Bolognini L., Zipponi S. (a cura di), *Privacy e diritto dei dati sanitari,* Giuffrè, Milano, 2024, p. 72.

amministrativa per violazione del GDPR. In tal senso, infatti, si esprimono anche le Linee Guida 4/2019 dell'*European Data Protection Board*[72] chiarendo che è il Titolare a dover assicurare il rispetto dei principi di *privacy by design* e *by default* in merito al trattamento svolto dai suoi Responsabili e Sub-responsabili del trattamento, tenendone conto anche in fase di stipula dei contratti con gli stessi.

Dall'altra parte, il produttore, in qualità di Responsabile del trattamento, seppur non considerabile un diretto destinatario degli obblighi di cui l'art. 25 del Regolamento, sarà considerato una figura essenziale e a supporto del Titolare, e sarà chiamato a utilizzare le proprie competenze al fine per instaurare un clima di fiducia e orientare il cliente, Titolare del trattamento, verso la progettazione di prodotti e servizi che rispondono alle esigenze normative.

3.2. Refertazione online, il dossier sanitario elettronico e il Fascicolo Sanitario Elettronico

Un altro aspetto della cd. sanità digitale che merita un approfondimento dal punto di vista della *data protection* è l'implementazione e l'utilizzo di sistemi di refertazione *online*, del dossier sanitario elettronico e del Fascicolo Sanitario Elettronico.

Sul punto, il Garante Privacy si è espresso per la prima volta nel 2009 con le "Linee Guida in tema di referti online", intendendosi per "referto online" la possibilità di accedere al referto tramite modalità digitali (ovvero tramite Fascicolo sanitario elettronico, sito Web, posta elettronica anche certificata, supporto elettronico). Tali linee guida, integrate nel 2013[73], già prevedevano l'obbligatorietà del consenso informato dell'interessato come base giuridica del trattamento. Sul punto, come già precedentemente accennato, il Garante Privacy è tornato ad esprimersi nel 2019[74] confermando che il trattamento dei dati personali relativi alla salute per finalità di cura mediante l'utilizzo della refertazione *online* richiede la prestazione di un consenso informato, libero e specifico da parte dell'interessato.

---

72. Comitato Europeo per la protezione dei dati personali, *Linee guida 4/2019 sull'articolo 25 Protezione dei dati fin dalla progettazione e per impostazione predefinita,* 20 ottobre 2020.

73. Melchionna S., *Sanità digitale e innovazione*, in Bolognini L., Zipponi S. (a cura di), *Privacy e diritto dei dati sanitari,* Giuffrè, Milano 2024, p. 92.

74. Comitato Europeo per la protezione dei dati personali, *Linee guida 4/2019 sull'articolo 25 Protezione dei dati fin dalla progettazione e per impostazione predefinita,* 20 ottobre 2020.

La mancata prestazione del consenso non deve, tuttavia, precludere in alcun modo la possibilità di accedere alla prestazione medica richiesta e deve essere, in ogni caso, concesso all'interessato che abbia scelto di aderire ai servizi di refertazione *online*, in relazione ai singoli esami clinici a cui si sottoporrà di volta in volta, di manifestare una volontà contraria ovvero che i relativi referti non siano oggetto del servizio di refertazione *online*, diversamente da quanto in precedenza deciso e comunicato. Al fine di informare opportunamente l'interessato rispetto alle attività e alle finalità di trattamento che lo coinvolgono, nonché raccogliere lecitamente il suo consenso, il Titolare del trattamento deve, dunque, fornire un'informativa idonea e specifica, distinta rispetto a quella relativa al trattamento dei dati personali per finalità di cura e che esponga, con un linguaggio chiaro e comprensibile, le caratteristiche del servizio di refertazione *online*, sempre in conformità agli artt. 13 e 14 del GDPR.

Il Garante Privacy specifica anche che, ai fini di tutelare e garantire la sicurezza dei dati personali trattati, la struttura sanitaria è tenuta ad adottare dei protocolli di comunicazione sicuri (https) e dei sistemi di autenticazione forte dell'interessato (cd. *strong authentication*). Il referto *online* deve essere, inoltre, reso disponibile sul sito web per un massimo di 45 giorni, nonché garantire all'utente la possibilità di cancellare dal sistema di consultazione, in modo complessivo o selettivo, i referti che lo riguardano[75].

Per quanto riguarda l'implementazione di idonee misure di sicurezza, le Linee Guida in materia di refertazione *online* dell'autorità nazionale in materia di tutela dei dati personali prevedono la necessità di adottare idonei sistemi di autenticazione e autorizzazione per i soggetti autorizzati a seconda dei ruoli e delle finalità dei trattamenti coinvolti nel sistema di refertazione *online*, nonché la definizione di diversi livelli di protezione dei dati a seconda che la consultazione online dei referti avvenga tramite servizi web, tramite posta elettronica anche certificata o un altro supporto elettronico.

Inoltre, tutti gli operatori che accedono ai sistemi di refertazione devono ricevere una idonea formazione anche e soprattutto al fine di gestire eventuali incidenti e episodi di violazione dei dati personali.

Infine, sempre nell'ottica di definire tutti gli adempimenti privacy richiesti al Titolare del trattamento che voglia svolgere servizi di refertazione *online*, è opportuno ricordare che, anche in questo caso:

- la refertazione *online*, con le sue specifiche caratteristiche e le misure di sicurezza necessarie, deve essere prevista nel Registro dei trattamenti adottato dal Titolare del trattamento ai sensi dell'art. 30 del GDPR;

75. Autorità Garante per la protezione dei dati, *Referti online - le FAQ del Garante*, 2020.

- qualora il Titolare intenda implementare l'uso di nuove tecnologie per offrire su larga scala nuovi servizi digitali di refertazione deve effettuare, prima di procedere al trattamento, la valutazione d'impatto in conformità all'art. 35 del Regolamento.

Un'altra fondamentale struttura operativa dell'ecosistema della sanità digitale su cui si è espresso il Garante Privacy riguarda il dossier sanitario. Nel 2015, infatti, con le Linee guida in materia di Dossier sanitario[76] si è espresso con riferimento ai trattamenti di dati personali effettuati dalle strutture sanitarie mediante tale strumento.

Secondo la definizione resa nelle "Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario" del 2009[77], il dossier sanitario è lo strumento costituito presso un organismo sanitario quale Titolare del trattamento (ad esempio un ospedale, un'azienda sanitaria, una casa di cura), mediante il quale sono rese accessibili "informazioni, inerenti allo stato di salute di un individuo, relative ad eventi clinici presenti e trascorsi (es., referti di laboratorio, documentazione relativa a ricoveri, accessi al pronto soccorso), volte a documentarne la storia clinica". Il dossier sanitario, dunque, comprende tutte le informazioni circa gli eventi e i trattamenti clinici occorsi all'interessato esclusivamente presso un'unica struttura sanitaria. Come approfondiremo successivamente in questo paragrafo il dossier sanitario si differenzia dal FSE poiché i documenti e le informazioni sanitarie accessibili tramite tale strumento sono stati generati da un unico Titolare del trattamento e non da più strutture sanitarie. Il dossier sanitario si distingue anche dalla cartella clinica, poiché in questo caso si tratta di uno strumento che riguarda un singolo episodio di ricovero dell'interessato.

Nelle Linee Guida pubblicate nel 2015, dunque, il Garante Privacy si esprime innanzi tutto riguardo all'informativa privacy che deve essere fornita all'interessato ai sensi dell'art. 13 del GDPR. In particolare, nell'informativa al dossier deve essere fornita evidenza all'interessato:

- delle finalità del trattamento, ovvero che il Titolare del trattamento desidera costituire un insieme di informazioni personali riguardanti l'interessato al fine di documentarne la storia sanitaria dello stesso e permettere agli operatori sanitari coinvolti di accedere alle informazioni necessarie così da ottimizzare i trattamenti e l'attività di cura;

76. Autorità Garante per la protezione dei dati, *Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario*, 4 giugno 2015.

77. Ivi.

- che l'eventuale mancato consenso al trattamento dei dati personali mediante il dossier sanitario non incide sulla possibilità di accedere alle cure mediche richieste;
- che, nel caso in cui lo stesso presti il consenso al trattamento dei suoi dati personali mediante il dossier sanitario, questo potrà essere consultato, nel rispetto dell'Autorizzazione generale del Garante, anche qualora ciò sia ritenuto indispensabile per la salvaguardia della salute di un terzo o della collettività[78];
- in merito ai soggetti ai quali i dati personali trattati mediante il dossier possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o autorizzati al trattamento;
- circa il divieto di diffusione dei suoi dati relativi allo stato di salute.

Per quanto riguarda la prestazione del consenso, nello specifico, il Garante Privacy fornisce delle precisazioni riguardanti la revoca dello stesso. Ai fini dell'accesso al dossier da parte del personale sanitario non è necessario, infatti, che l'interessato presti volta per volta il consenso, poiché il dossier sarà accessibile nel tempo da parte di tutti gli operatori sanitari che lo prenderanno in cura sulla base del consenso che l'interessato avrà inizialmente prestato.

Nel caso, invece, di revoca del consenso, la stessa è liberamente manifestabile in qualsiasi momento e, se manifestata, determina che il dossier sanitario non debba più essere ulteriormente implementato. Dalla revoca, quindi, le informazioni sanitarie presenti dovranno rimanere accessibili al professionista o alla struttura interna al titolare che le ha redatte e per eventuali conservazioni per obbligo di legge, ma non potranno più essere condivise con i professionisti degli altri reparti che prenderanno successivamente in cura l'interessato. Sempre in materia di consenso, infine, si specifica che vi sono delle informazioni che potrebbero richiedere delle maggiori tutele dell'interessato. In tal caso, come ad esempio, nell'eventualità di informazioni relative ad atti di violenza sessuale o pedofilia, all'infezione da HIV o all'uso di alcool o di stupefacenti, le stesse dovranno espressamente menzionate nell'informativa e sottoposte a un consenso specifico dell'interessato. L'interessato può, infatti, in ogni caso decidere di oscurare taluni dati o documenti sanitari, che non saranno visibili e consultabili tramite il dossier.

---

78. Autorità Garante per la protezione dei dati, *Autorizzazione generale n. 2/2014 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale*, 11 dicembre 2014.

Proprio in materia di dossier sanitario, il Garante Privacy si è recentemente pronunciato con il provvedimento del 22 febbraio 2024[79], sanzionando per 75mila euro l'Azienda sanitaria dell'Alto Adige per non aver configurato correttamente le modalità di accesso al dossier sanitario elettronico. Nel caso di specie, alla luce delle violazioni determinate da accessi non autorizzati ai dossier sanitari, il Garante Privacy ha citato le Linee Guida del 2015, richiamando i Titolari del trattamento a svolgere un'attività di monitoraggio e di verifica rispetto agli accessi da parte del personale sanitario ai dossier. Tali accessi, devono infatti essere limitati – anche nel tempo – mediante degli idonei processi autorizzativi, tenuto conto, in ogni caso, anche del diritto di oscuramento esercitabile dall'interessato.

Nel caso dell'azienda sanitaria sanzionata, è emerso che la configurazione del dossier sanitario consentiva al personale sanitario di accedere alle informazioni di qualunque paziente fosse stato assistito dalla stessa, dichiarando la sussistenza di una pluralità di casistiche preordinate[80]. Le misure messe in atto non risultavano pienamente idonee a garantire che potesse accedere al dossier sanitario di un paziente solo il personale sanitario che lo avesse in cura, rendendo quindi di fatto possibile che attraverso l'utenza di un professionista sanitario operante presso la stessa si potesse accedere al dossier sanitario di interessati che non erano in cura presso il titolare dell'utenza e che non risultavano associati a "eventi clinici amministrativi tracciati a livello informatico". In aggiunta, l'autorità ha anche accertato – tra le mancate misure tecniche che l'azienda avrebbe dovuto implementare – la mancata predisposizione di un sistema di *alert*, volto ad individuare comportamenti anomali o a rischio relativi alle operazioni eseguite dagli incaricati al trattamento (ad esempio, relativi al numero degli accessi eseguiti, alla tipologia o all'ambito temporale degli stessi).

Da ultimo, ma non per importanza, il Garante Privacy si è anche più volte espresso, a partire dal 2009, fornendo delle linee guida e delle indicazioni specifiche in materia di Fascicolo Sanitario Elettronico (cd. Fse). L'ultima edizione del vademecum informativo è di Luglio 2024[81].

Partendo dalla definizione, il Fse è l'insieme di dati e documenti digitali relativi all'intera storia clinica di una persona generati ora, oltre che dalle strutture sanitarie pubbliche, anche da quelle private[82]. Il Fse permette di

79. Autorità Garante per la tutela dei dati personali, Provvedimento n. 130 del 22 febbraio 2024.

80. Nanni S., *Dossier sanitario, il Garante Privacy sanziona un'Asl per accessi non autorizzati: cosa impariamo,* in *Cybersecurity360*, 10 aprile 2024.

81. Autorità Garante per la tutela dei dati personali, *Fascicolo Sanitario Elettronico – Vademecum*, ed. luglio 2024.

82. Cfr. Il FSE è stato previsto dall'art. 12, del d.l. n. 179/2012 e successivamente disciplinato dal Dpcm n. 178/2015 e dal decreto del 7 settembre 2023 (FSE 2.0).

consultare molti documenti sanitari rilevanti, come le prescrizioni mediche e farmaceutiche, le prenotazioni, le cartelle cliniche, i referti anche di pronto soccorso, le schede di dimissioni ospedaliere, i certificati medici e le esenzioni. Nello stesso è presente anche il *patient summary* (ovverosia il profilo sanitario sintetico del paziente) che riassume la storia clinica dell'assistito e contiene i dati necessari a gestire un'emergenza sanitaria, nonché il taccuino personale, ovvero una sezione riservata all'assistito in cui inserire dati, anche generati dai dispositivi medici e/o *wearable*, e documenti personali relativi ai propri percorsi di cura.

Il Fse persegue, inoltre, delle specifiche finalità, ovvero di diagnosi, di cura e di riabilitazione, di studio e ricerca scientifica in campo medico, biomedico ed epidemiologico, di governo (programmazione sanitaria, verifica della qualità delle cure e valutazione dell'assistenza sanitaria), di prevenzione e di profilassi internazionale. Una caratteristica fondamentale, garantita dal sistema nazionale della tessera sanitaria, del Fse è che lo stesso viene automaticamente alimentato con i documenti e le informazioni del paziente, così che lo stesso possa sempre facilmente consultare i propri documenti socio-sanitari, generati da diverse strutture sanitarie sia pubbliche che private, nonché situate al di fuori della Regione di appartenenza.

Per quanto riguarda gli adempimenti necessari a garantire la conformità del trattamento dei dati personali nell'ambito di utilizzo del Fascicolo Sanitario Elettronico, il Garante Privacy si è, innanzi tutto e anche in questo caso, espresso circa la necessità di informare gli interessati ai sensi dell'art. 13 del GDPR. L'informativa deve, dunque:

- essere formulata con linguaggio chiaro e indicare, oltre a tutti gli elementi richiesti dal Regolamento, ovvero indicazione del Titolare del trattamento, delle finalità, del periodo di conservazione ecc., anche che i dati che andranno a integrare il Fse sono relativi allo stato di salute dell'interessato e dunque rientrano nella categoria di cui all'art. 9 del GDPR;
- indicare il diritto di oscuramento dell'interessato, nonché l'idoneo diritto di conoscere quali accessi sono stati effettuati al proprio fascicolo.

Sul punto, allo scopo di fornire delle indicazioni pratiche e uniformi per gli operatori del sistema sanitario nazionale, l'autorità italiana ha recentemente reso il proprio parere favorevole[83] su un modello di informativa nazionale relativo ai trattamenti effettuati attraverso il FSE 2.0.

83. Autorità Garante per la protezione dei dati personali, *Faq in tema di fascicolo sanitario elettronico*, 2020.

Per quando concerne la prestazione del consenso, lo stesso deve essere reso una tantum dall'interessato e può essere sempre revocato, senza in ogni caso alcun pregiudizio rispetto alla garanzia di ricevimento della prestazione sanitaria.

Il Garante Privacy chiarisce e differenzia con specificità quali sono i soggetti che possono accedere al Fse e quali i soggetti ai quali l'accesso è negato. I primi sono: l'assistito, affinché possa consultare i propri documenti sanitari sia clinici che amministrativi, come le ricette o i referti; tutti gli esercenti le professioni sanitarie, con il consenso dell'assistito, che intervengono nel suo processo di cura, compreso il medico di base; i professionisti sanitari che hanno in cura l'interessato e secondo livelli diversificati a seconda dell'attività svolta; le Regioni/province autonome, il Ministero della salute e l'Agenas nei limiti delle rispettive competenze attribuite dalla legge, senza l'utilizzo dei dati identificativi degli assistiti, secondo livelli di accesso, modalità e logiche di organizzazione ed elaborazione dei dati conformi ai principi di proporzionalità, necessità e indispensabilità nel trattamento dei dati personali e delle misure tecniche e organizzative previste dalla normativa di riferimento. Non possono, invece, accedere al Fse i periti, le compagnie di assicurazione, i datori di lavoro, le associazioni scientifiche e gli organismi amministrativi pur se operanti in ambito sanitario, e comunque i terzi non autorizzati non possono accedere al fascicolo.

In caso di emergenza, ovvero in caso di impossibilità fisica, incapacità di agire o incapacità di intendere o di volere e di rischio grave, imminente ed irreparabile per la sua salute o incolumità fisica, inoltre, il personale sanitario che prenderà in cura l'interessato può accedere prioritariamente al profilo sanitario sintetico e, ove necessario, agli ulteriori dati e documenti del fascicolo – ad eccezione dei dati e documenti per i quali l'assistito abbia richiesto l'oscuramento – e comunque per il tempo strettamente necessario ad assicurare le cure in emergenza.

Il Garante Privacy si è espresso anche in materia di *data retention* del Fse, specificando che l'indice dei dati e documenti del fascicolo viene cancellato dal titolare del trattamento decorsi 30 anni dalla data del decesso dello stesso, con periodicità annuale.

Per quanto riguarda, infine, i cd. dati a "maggior tutela", ovvero ad esempio i documenti sanitari e socio-sanitari relativi a persone sieropositive, donne che si sottopongono a un'interruzione volontaria di gravidanza, vittime di atti di violenza sessuale o di pedofilia, persone che fanno uso di sostanze stupefacenti, di sostanze psicotrope e di alcool, donne che decidono di partorire in anonimato, nonché quelli riferiti ai servizi offerti dai consultori

familiari, gli stessi sono di default oscurati, ovvero resi visibili solo all'assistito, il quale potrà però decidere liberamente e in qualsiasi momento di renderli visibili a terzi.

L'importanza delle disposizioni previste dalle normative di riferimento e dei documenti di indirizzo forniti dal Garante Privacy in materia di Fse è evidenziata anche dalle recenti attività istruttorie e dai provvedimenti del Garante Privacy.

A fine gennaio 2024, infatti, il Garante Privacy ha concluso un'attività istruttoria i cui esiti hanno rilevato che 18 Regioni e le due Province autonome del Trentino Alto Adige hanno modificato, anche significativamente, il citato modello di informativa predisposto dal Ministero, previo parere del Garante, al fine di coordinamento nazionale. Il Garante Privacy ha riscontrato, nel dettaglio, che alcuni diritti come il diritto di oscuramento, delega e consenso specifico e le misure di sicurezza, i livelli di accesso differenziati, la qualità dei dati non erano garantite dalle aziende sanitarie.

Per concludere, con il provvedimento del 27 Novembre 2024[84] il Garante Privacy ha irrogato tre sanzioni di 10mila euro ciascuna, irrogate rispettivamente alla Regione Molise, alla Società Molise dati, e a Engineering ingegneria informatica S.p.A., definendo i procedimenti aperti dopo l'intrusione nel Portale regionale del Fascicolo Sanitario Elettronico verificatasi a fine 2022. Il Garante ha, nel dettaglio, accertato che la violazione era stata provocata da un *bug* di sicurezza nel sistema di autenticazione con cui si accedeva al Fse della regione. Sono stati, quindi, sanzionati la Regione Molise in quanto titolare del Portale e la Società Molise dati, in qualità di responsabile dell'attività di implementazione tecnica del fascicolo, per non aver effettuato delle specifiche verifiche per valutare la presenza di criticità nel software sviluppato da *Engineering*, ovvero il fornitore che aveva sviluppato le componenti tecniche del Portale. Tali sistemi, infatti, privi delle idonee misure di sicurezza necessarie per limitare l'accesso da parte degli utenti esclusivamente alle informazioni che li riguardavano, avevano consentito l'illecito da parte di un soggetto terzo che era riuscito a utilizzare funzionalità a cui non era autorizzato, mediante la modifica della URL.

3.3. App e sanità

Illustrati, quindi, i principali strumenti attivi nell'ambito della sanità digitale oramai consolidati nell'attività degli operatori del settore, appare

84. Autorità Garante per la protezione dei dati personali, *Provvedimento n. 736 del 2024.*

opportuno concludere la trattazione approfondendo le implicazioni privacy scaturenti dai più recenti strumenti, quali l'utilizzo di app.

Quelle che Giannini definisce le *mobile application* mediche[85] possono essere utilizzate per favorire la comunicazione tra specialisti e staff del team medico ma anche per far sì che il paziente abbia un ruolo più centrale nel proprio percorso terapeutico personale. Ecco, quindi, che vi saranno applicazioni utilizzate per servizi strettamente amministrativi quali le prenotazioni alle visite mediche, nonché applicazioni relative al *wellness* e alla prestazioni di servizi più legati alla cura del paziente e alla prestazione di consulenze mediche online.

Il Garante Privacy si è chiaramente espresso sulla materia, sia con il provvedimento del 2019[86], con cui ha ribadito che il trattamento dei dati personali svolto mediante app mediche è un trattamento che deve considerarsi distinto rispetto al trattamento svolto dal Titolare per finalità di cura del paziente e che, dunque, richiederà uno specifico e chiaro consenso da parte dell'interessato che sarà anche in questo caso opportunamente informato ai sensi dell'art. 13 del GDPR, sia con il recente "Compendio sul trattamento dei dati personali effettuato attraverso piattaforme volte a mettere in contatto i pazienti con i professionisti sanitari accessibili via web e app"[87] pubblicato a marzo 2024.

In tale documento informativo interviene, *in primis*, delineando il perimetro delle attività svolte mediante tali strumenti e le finalità dei trattamenti coinvolti.

Alla luce delle attività che le app mediche consentono di svolgere, ovvero inviare e archiviare documenti sanitari, anche al fine di condividerli con il professionista sanitario, visualizzare lo storico degli appuntamenti e ricevere via email informazioni sulla salute pubblica e comunicazioni promozionali sui servizi offerti, appare indiscutibile che i proprietari e gestori di tali piattaforme non siano legittimati a trattare i dati relativi alla salute degli utenti per finalità di diagnosi, assistenza e terapia sanitaria. Tali dati, infatti, in conformità al Regolamento e a tutte le indicazioni già fornite nella presente trattazione, sono autorizzate esclusivamente a un professionista sanitario soggetto al segreto professionale. I trattamenti dei

85. Giannini A., *Le mobile applications mediche*, Iaselli M. (a cura di), *La tutela dei dati personali in ambito sanitario*, Giuffrè, Milano, 2020.

86. Autorità Garante per la protezione dei dati personali, *Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario,* marzo 2019

87. Autorità Garante per la protezione dei dati personali, *Compendio sul trattamento dei dati personali effettuato attraverso piattaforme volte a mettere in contatto i pazienti con i professionisti sanitari accessibili via web e app*, marzo 2024.

dati personali saranno quindi effettuabili dai proprietari e dai gestori delle piattaforme solo qualora siano strettamente necessari ad offrire servizi funzionali al rapporto medico paziente, quali quelli di natura amministrativa (ad esempio il pagamento delle prestazioni sanitarie) o tecnologica (ad esempio la gestione degli account e degli appuntamenti delle visite specialistiche).

Premesso il quadro operativo delle app mediche che, innegabilmente, coinvolgono una molteplicità di trattamenti dei dati personali relativi alla salute per mano di diversi soggetti, è chiaro ed essenziale che sia rispettato il principio di responsabilizzazione in base al quale il Titolare del trattamento deve conformarsi ed essere in grado di comprovare la conformità ai principi e agli adempienti previsti dal Regolamento fin dalla progettazione.

Nel dettaglio, attraverso le suddette piattaforme possono essere effettuati tre tipologie di trattamenti, caratterizzati da distinte finalità, con riferimento alle quali rilevano specifiche basi giuridiche.

La prima tipologia di trattamento riguarda l'ipotesi in cui sia previsto un trattamento di dati relativi alla salute degli utenti che utilizzano un'applicazione o una piattaforma per effettuare la prenotazione di una visita medica. In tal caso, non trattandosi di un trattamento finalizzato alla diagnosi o alla cura del paziente, il Titolare del trattamento sarà chiamato a raccogliere il consenso informato dell'utente. In aggiunta, il Garante Privacy specifica che nel caso in cui i dati personali dell'utente siano raccolti per il perseguimento di finalità ulteriori, ovvero a titolo esemplificativo inviare comunicazioni commerciali o di *marketing*, il consenso dovrà essere raccolto in modo specifico per ciascuna finalità di trattamento[88].

La seconda ipotesi di trattamento riguarda, invece, l'operazione di trattamento posta in essere dai professionisti sanitari (es. medici) che utilizzano in prima persona la piattaforma per gestire le prenotazioni delle visite da parte dei loro pazienti. In tal caso, si precisa che il trattamento risulta lecito alla luce della base giuridica del trattamento prevista dall'art. 6, par. 1 lett. b) del Regolamento, ovvero il contratto stipulato tra il professionista sanitario e la società che fornisce e gestisce la piattaforma.

Infine, per quanto concerne il trattamento dei dati relativi alla salute dei pazienti che potrebbero aver contattato il professionista sanitario mediante la piattaforma, ma potrebbero essere comunque soggetti a un trattamento per finalità di cura, in questo caso, trattandosi di un'ipotesi rientrante nella casistica prescritta dall'art. 9, par. 2, lett. h) e par. 3 del

88. Comitato Europeo per la protezione dei dati, *Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679*, maggio 2020.

GDPR, non sarà necessario che il professionista sanitario raccolga il consenso del paziente.

L'Autorità Garante in materia di protezione dei dati, inoltre, nel citato Compendio in materia, nel fornire delle disposizioni clarificatorie circa l'utilizzo di tali piattaforme in ambito medico, evidenzia che le stesse devono essere tenute distinte dai cd. strumenti di telemedicina, ovverosia le tecniche mediche e informatiche tramite le quali il medico può curare e/o visitare da remoto il paziente. Secondo il Garante, i due strumenti perseguono, infatti, diverse finalità di trattamento. Da una parte, vi è il perseguimento delle finalità di cura nel caso dell'utilizzo degli strumenti di telemedicina, mentre dall'altra, nel caso delle app mediche, vi è la finalità di fornire un servizio mediante l'utilizzo della tecnologia. Da non dimenticare che, tuttavia, se è vero che la progettazione di tali piattaforme dovrà tenere in considerazione le differenze con la telemedicina, è pur vero che dovrà essenzialmente considerare le disposizioni previste per strumenti che – seppur differenti – presentano dei punti di contatto, ossia la già trattata disciplina in materia di refertazione online e di Fascicolo Sanitario Elettronico.

Per quanto concerne l'implementazione delle misure tecniche e organizzative adeguate a progettare un'applicazione medica che garantisca la tutela dei dati personali degli utenti riguarda poi il divieto di diffusione dei dati personali, va specificato che:

- per quanto concerne il divieto di diffusione dei dati personali relativi alla salute[89], le piattaforme dovranno garantire delle modalità di accesso e di registrazione dell'utente idonee a scongiurare il rischio che soggetti non autorizzati possano accedere alle informazioni inserite dagli utenti per la scelta del professionista sanitario, in assenza di un idoneo presupposto giuridico;
- il Titolare del trattamento dovrà individuare delle misure tecniche e organizzative finalizzate a ridurre il rischio di distruzione, perdita, modifica, divulgazione non autorizzata o accesso, in modo accidentale o illegale, ai dati personali trasmessi, conservati o comunque trattati. A tal fine, potrà considerare di adottare sistemi di cifratura dei dati personali, oppure, a titolo esemplificativo: delle procedure di adesione alla piattaforma da parte dello specialista che preveda la verifica dell'identità dello stesso e delle sue qualifiche professionali, una procedura di verifica o convalida del dato di contatto scelto dall'utente (es. indirizzo di posta elettronica,

89. *Cfr.* artt. 2-septies, comma 8 e art. 166, comma 2, del Codice della Privacy e art. 9 Regolamento Ue 2016/679.

numero di cellulare), delle misure per ridurre ipotesi di errori di omonimia/omocodia, delle procedure di autenticazione informatica a più fattori, dei meccanismi di blocco della app in caso di inattività, nonché dei sistemi di monitoraggio anche automatici per rilevare accessi non autorizzati o anomali alle piattaforme.

In aggiunta, il Garante Privacy si è espresso in relazione alla necessità di svolgere una valutazione di impatto ai sensi dell'art. 35 del GDPR. L'autorità, in particolare, chiarisce che considerata la tipologia dei dati personali coinvolti nelle attività di trattamento delle piattaforme mediche, nonché del numero dei soggetti interessati al trattamento, non si può che considerare obbligatorio lo svolgimento di una preventiva valutazione di impatto. Tale obbligatorietà è prevista, infatti, anche dalle "Linee guida concernenti la valutazione di impatto sulla protezione dei dati" che richiamano i criteri per stabilire se un trattamento "possa presentare un rischio elevato"[90].

Infine, anche in materia di app mediche, occorre svolgere una riflessione in materia di *governance* dei dati, ovvero circa l'individuazione dei corretti ruoli privacy dei soggetti coinvolti nelle operazioni di trattamento. Posto che ogni caso specifico richiede delle considerazioni e delle analisi che non possono essere con superficialità evitate, il Garante della Privacy riesce a definire tre casi – scuola che ci concedono di avere delle linee guida in materia.

Nel caso dei trattamenti dei dati personali degli utenti della piattaforma necessari all'utilizzo della stessa, è chiaro che il gestore dell'app dovrà essere individuato quale Titolare del trattamento, poiché sarà lui a determinare le modalità e le finalità di un trattamento imprescindibile al corretto funzionamento della piattaforma e all'erogazione dei servizi.

Anche nel caso delle operazioni di trattamento dei dati personali relativi ai professionisti sanitari che utilizzano la piattaforma per erogare loro stessi dei servizi ai pazienti, il gestore dell'app sarà Titolare del trattamento con riferimento ai dati personali considerabili "necessari" a garantire l'esecuzione del contratto di servizi stipulato tra le parti.

Per quanto concerne, invece, il trattamento dei dati relativi alla salute dei pazienti che sono entrati in contatto con il professionista grazie all'utilizzo dell'app ma è stato poi svolto dal professionista per il perseguimento della finalità di cura nell'ambito della prestazione medica, sarà il professionista a ricoprire il ruolo di Titolare del trattamento. In tal caso, quindi, il gestore della piattaforma ricoprirà un ruolo differente, ovvero quello di

90. Gruppo di Lavoro Articolo 29, *Linee-guida in materia di valutazione di impatto sulla protezione dei dati,* 4 ottobre 2017.

Responsabile del trattamento ai sensi dell'art. 28 GDPR, poiché lo stesso nello svolgimento di attività di tipo tecnico – amministrativo per conto del professionista sanitario (es. attività di conservazione dei documenti) tratterà i dati personali per conto del Titolare. È chiaro, quindi, che alla luce delle particolarità del trattamento dei dati coinvolti e del numero e della vulnerabilità degli interessati, nella predisposizione dell'atto di nomina del Responsabile del trattamento, il professionista sanitario dovrà opportunamente e formalmente indicare le misure tecniche e organizzative che il gestore della piattaforma dovrà implementare per garantire la sicurezza e la tutela dei dati personali dei pazienti.

4. Il futuro della sanità digitale

4.1. IA e dati sintetici

Chiariti, quindi, gli aspetti di *compliance* relativi agli strumenti e alle implementazioni della sanità digitale oramai consolidati, non possiamo che concludere la trattazione con un approfondimento circa i più recenti ambiti in cui la tecnologia applicata alla gestione del mondo sanitario esplica la sua potenzialità. Anche tali aspetti non possono, infatti, prescindere da delle considerazioni in materia di conformità del trattamento dei dati personali coinvolti.

Innanzi tutto, le prime considerazioni devono riguardare l'utilizzo innovativo delle tecniche di Intelligenza Artificiale in campo medico. Lasciando per ora da parte la disciplina prevista dal Regolamento Ue sull'Intelligenza Artificiale (cd. AI Act)[91] che verrà maggiormente approfondita nella Parte III del presente lavoro, occorre in questa fase specificare che la nuova normativa entrata in vigore in materia appare necessariamente connessa con la disciplina prevista in materia dei dati personali[92]. L'AI Act, in particolare, adotta un approccio definito "risk-based", classificando i sistemi di IA in base al livello di rischio – inteso come la combinazione della probabilità del verificarsi di un danno e la gravità del danno stesso – agli stessi connesso. Tra i sistemi di IA considerati ad alto rischio, il Regolamento europeo sull'Intelligenza Artificiale comprende anche i sistemi utilizzati in ambito

91. Regolamento UE 2024/1689 del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale).

92. Iaselli M., *AI Act Principi, regole ed applicazioni pratiche del Reg. UE 1689/2024,* Maggioli Editore, Santarcangelo di Romagna, p. 77.

medico, fornendo così delle disposizioni applicabili agli operatori del settore, ovvero sia i produttori di tali sistemi, sia ai loro distributori e rivenditori, sia i loro "deployer"[93].

Proprio sulle interazioni tra la normativa ad oggi prevista in materia di IA e la normativa in materia di tutela dei dati personali, il Garante della Privacy si è pronunciato nel 2023 pubblicando il "Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di Intelligenza Artificiale"[94]. Ancora una volta, dunque, l'autorità specifica che, ai sensi del citato principio della "protezione dei dati fin dalla progettazione" previsto dall'art. 25, par. 1, del Regolamento, anche nella realizzazione di sistemi di intelligenza artificiale in ambito sanitario devono essere adottate misure tecniche e organizzative adeguate a garantire la conformità del trattamento ai principi di protezione dei dati, così da tutelare i diritti e le libertà degli interessati. Anche per tali operazioni di trattamento saranno, inoltre, richieste delle riflessioni sulla definizione la cd. *governance* dei dati, individuando il Titolare del trattamento e nominando formalmente gli eventuali Responsabili del trattamento ai sensi dell'art. 28 coinvolti nell'attività di trattamento relativa al sistema di IA applicato in materia sanitaria.

Il Garante Privacy enuclea poi, ai sensi di quanto previsto dal GDPR e delle pronunce del Consiglio di Stato[95], quelli che possono essere considerati i tre principi cardine che devono governare l'utilizzo di algoritmi e di strumenti di IA nell'esecuzione di compiti di rilevante interesse pubblico[96].

Il primo è il principio di conoscibilità che prevede che "l'interessato ha il diritto di conoscere l'esistenza di processi decisionali basati su trattamenti automatizzati e, in tal caso, di ricevere informazioni significative sulla logica utilizzata, sì da poterla comprendere"[97];

Alla luce del secondo principio, ovvero il principio di non esclusività della decisione algoritmica, ciascun processo decisionale deve comprendere un intervento umano capace di controllare, validare ovvero smentire la decisione automatica, ovvero il c.d. *human in the loop*.

---

93. L'art. 3 del AI Act definisce chiunque (persona fisica o giuridica) utilizzi un sistema di IA nell'ambito di un'attività "professionale".

94. Autorità Garante per la protezione dei dati personali, *Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di Intelligenza Artificiale,* 2023.

95. Cfr. sentenze VI sez., nn. 2270/2019, 8472/2019, 8473/2019, 8474/2019, 881/2020, e 1206/2021.

96. Autorità Garante per la protezione dei dati personali, *Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di Intelligenza Artificiale,* 2023, p. 3.

97. Autorità Garante per la protezione dei dati personali, *Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di Intelligenza Artificiale,* 2023, p. 6.

Il terzo principio, invece, è il principio di non discriminazione algoritmica. Tale principio richiede al Titolare del trattamento coinvolto nell'utilizzo di sistemi di IA, di ricorrere a sistemi di IA considerati affidabili ovvero sistemi che riducano opportunamente le opacità, gli errori dovuti a cause tecnologiche e/o a cause derivanti dall'intervento umano. Tali adempimenti devono essere posti in essere mediante delle verifiche periodiche in merito all'evoluzione delle tecnologie implicate, ai processi matematici e statistici appropriati per l'attività di profilazione, alle misure tecniche e organizzative adottare. Tali verifiche devono essere poste in essere per minimizzare il rischio di errori e di utilizzo discriminatorio degli algoritmi[98].

Definiti, quindi, in principi considerabili quali punti fermi del trattamento dei dati sanitari coinvolti nei sistemi di IA in ambito medico, appare opportuno precisare quali tra gli altri requisiti previsti dal GDPR in materia di trattamento dei dati relativi alla salute, devono essere considerati per garantire la tutela degli interessati a tali trattamenti, proprio alla luce delle criticità, degli impatti e dei rischi che ne possono derivare.

In primis, dovranno essere considerati i requisiti di esattezza, correttezza e aggiornamento dei dati personali, poiché i dati raccolti per finalità di cura potrebbero essere stati sottoposti a modificazione, rettifica o integrazione da parte personale sanitario che ha svolto delle attività nel corso delle cure destinate all'interessato[99].

L'autorità nazionale, infatti, nel richiamare il suddetto principio, specifica che il dato non aggiornato o inesatto potrebbe influenzare l'efficacia e la correttezza dei servizi forniti dai sistemi di IA, poiché tali sistemi si basano sulla rielaborazione di tali dati personali.

In secondo luogo, un principio ai sensi dell'art. 5 par. 1 lett. f) del GDPR da considerarsi fondamentale nella progettazione e nell'utilizzo dei sistemi di Intelligenza Artificiale è certamente il principio di integrità e riservatezza, in base al quale "i dati personali devono essere "trattati in maniera da garantire un'adeguata sicurezza (…), compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali"[100]. La tutela dei dati personali degli interessati e gli eventuali rischi per gli stessi devono, quindi, essere valutati in concreto svolgendo una analisi sulle banche dati utilizzate come base del sistema di elaborazione e dei modelli di analisi. L'utilizzo di modelli di analisi deterministica mediante tecniche di *machine learning* può

98. Considerando 71 GDPR.
99. Regolamento Ue 2016/679, Art. 5, par. 1, lett. d).
100. Regolamento Ue 2016/679, par. 1.

infatti comportare degli errori o delle distorsioni, nonché dei risultati discriminatori per gli interessati. Per mitigare tali rischi, quindi, i trattamenti dei dati personali dovranno essere descritti in modo puntuale, al fine di rendere noti gli interessati circa le logiche utilizzate per la generazione di dati e servizi, nonché le metriche di addestramento del modello, le verifiche svolte per essere sicuri che non vi siano eventuali *bias*.

Dunque, per garantire la conformità dell'impiego delle tecniche di IA alla normativa in materia di trattamento dei dati personali, l'interessato dovrà essere reso noto delle misure poste in essere per tutelare i suoi diritti fondamentali e i suoi interessi, tra le quali devono essere indicate anche le misure adeguate a mitigare i rischi correlati all'uso di tecniche di IA sui dati relativi alla salute.

Per quanto concerne, in particolare, i "rischi di discriminazione" che possono derivare da una selezione impropria, incompleta e non accurata dei dati utilizzati dai sistemi di IA, un *case study*[101] accaduto negli Stati Uniti può essere considerato a titolo esemplificativo. Nel caso di specie, il sistema di IA utilizzato per stimare il rischio sanitario di oltre 200 milioni di americani tendeva erroneamente ad assegnare un livello di rischio inferiore ai pazienti afroamericani a parità di condizioni di salute, negandogli dunque l'accesso alle cure sanitarie. Dalle analisi svolte dai ricercatori era emerso che tale discriminazione derivava dall'erronea applicazione della metrica utilizzata per la stima del rischio, che era basata sulla spesa sanitaria media individuale. L'appartenenza a uno specifico gruppo etnico, quindi, non era una caratteristica utilizzata direttamente dal sistema di IA per determinare il risultato, ma era piuttosto la spesa media pro-capite ad influenzare indirettamente i risultati. Per evitare, quindi, tali rischi di discriminazione, il Garante Privacy evidenzia che dovrà innegabilmente essere mantenuto e garantito il ruolo centrale dell'intervento umano nell'utilizzo del sistema di IA, ovvero del professionista sanitario, così da garantire l'equità e l'inclusività delle cure fornite ai pazienti.

Per implementare quella che viene definita come una *trustworthy* IA, lo stesso Garante della Privacy elenca degli spunti di misure e adempimenti che nella predisposizione dei sistemi di IA in sanità devono essere implementate:

- assicurare che la base giuridica del trattamento sia chiara, prevedibile e resa conoscibile agli interessati anche attraverso specifiche campagne di informazione;
- consultare gli *stakeholder* e gli interessati nell'ambito dello svolgimento della valutazione d'impatto;

101. Obermeyer Z., Powers B., Vogeli C., Mullainathan S., *Dissecting racial bias in an algorithm used to manage the health of populations*, Science, 2019.

- pubblicare, anche solo per estratto, la valutazione d'impatto;
- predisporre le informazioni da rendere agli interessati, con gli elementi di cui agli artt. 13 e 14 del Regolamento in termini chiari, concisi e comprensibili;
- informare non solo in merito agli elementi di cui ai richiamati artt. 13 e 14 del Regolamento ma anche evidenziando se il trattamento sia effettuato nella fase di apprendimento dell'algoritmo (sperimentazione e validazione) ovvero nella successiva fase di applicazione dello stesso, nell'ambito dei servizi sanitari, rappresentando le logiche e le caratteristiche di elaborazione dei dati, se sussistono eventuali obblighi e responsabilità dei professionisti sanitari, a cui si rivolge l'interessato, ad utilizzare servizi sanitari basati sull'IA, i vantaggi, in termini diagnostici e terapeutici, derivanti dall'utilizzo di tali nuove tecnologie;
- assicurare modalità efficaci di esercizio dei diritti degli interessati previsti dal Regolamento e dalle specifiche discipline di settore, tenuto anche conto dei diversi ruoli rivestiti dai soggetti coinvolti nel trattamento;
- nel caso di perseguimento di finalità di cura, garantire che i servizi di elaborazione dei dati basati su sistemi di IA, siano realizzati solo a seguito di una espressa richiesta di attivazione del professionista sanitario e non in modo automatico;
- regolamentare i profili di responsabilità professionale connessi alla scelta del professionista sanitario di affidarsi o meno ai servizi di elaborazione dei dati sanitari dei propri pazienti effettuati sulla base di sistemi di IA[102].

Sull'importanza di considerare la protezione dei dati personali come la cornice entro cui i sistemi di IA devono operare, si è espressa anche l'Organizzazione Mondiale della Sanità[103], precisando che si rende necessario delineare un quadro giuridico e di *governance* dei dati che deve essere conforme al GDPR.

Tra le ulteriori novità applicative digitali che sia affacciano al settore sanitario e meritano un approfondimento, vi sono anche quelli che vengono definiti "dati sintetici". I dati sintetici sono definiti dall'*European Data Protection Regulation* come "dati non originali generati da dati originali e da un modello che viene addestrato a riprodurre le caratteristiche e la struttura dei dati originali"[104].

---

102. Autorità Garante per la protezione dei dati personali, *Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di Intelligenza Artificiale,* 2023, pp. 10-11.

103. World Health Organizatoin, *Regulatory Considerations on artificial intelligence for health*, 2023.

104. European Data Protection Supervisor, *Synthetic Data* (pagina informativa); cfr.

La particolarità dei dati sintetici risiede nel fatto che, a livello statistico il loro valore è lo stesso dei dati personali "reali", ma essendo generati attraverso un modello di IA, non possono essere direttamente ricondotti a una persona fisica determinata. Tale caratteristica permetterebbe, quindi, di analizzare i dati in un modo più sicuro e tutelante per gli interessati, consentendo a enti di ricerca e ospedali di implementare sistemi di IA nel pieno rispetto della normativa prevista in materia di dati personali[105]. In ambito sanitario, infatti, le applicazioni dei dati sintetici possono essere numerose, dalla previsione dell'insorgenza di patologie, come l'insufficienza cardiaca, utilizzando i dati delle cartelle cliniche elettroniche, all'innovazione dei servizi di teleassistenza e telemonitoraggio a vantaggio di persone fragili o anziane.

Da un lato dunque, dal punto di vista della conformità alla normativa relativa alla *data protection*, l'utilizzo dei dati sintetici correttamente elaborati non comporta particolare criticità per la compliance al GDPR, poiché i dati sintetici sottoposti a un processo di anonimizzazione non sarebbero più considerabili quali dati idonei a identificare una persona fisica determinata e, dunque, non sarebbero dati personali. Dall'altro lato, tuttavia, necessarie riflessioni devono essere svolte per quanto concerne la fase preliminare, ovvero la fase del processo in cui il dato personale viene elaborato per costruire un modello che consentirà al sistema di IA di elaborare dati sintetici. Per quanto riguarda le finalità di trattamento dei dati personali riconducibili a questa fase di trasformazione dei dati personali in dati sintetici, la dottrina specifica che le stesse potrebbero rientrare, a seconda del caso, nelle finalità di trattamento per fini statistici o di ricerca scientifica, per finalità didattiche o di pubblicazione scientifica e nelle finalità di trattamento per scopi giornalistici o di manifestazione del pensiero[106].

Circa le basi giuridiche del trattamento dei dati personali nella fase di propedeutiche allo sviluppo di un modello necessario alla generazione dei dati sintetici, la dottrina distingue due casistiche.

La prima ipotesi riguarda il caso in cui il trattamento dei dati personali si esaurisce con l'elaborazione degli stessi necessaria alla sintetizzazione. In tal caso, il trattamento può essere considerato legittimo ai sensi dell'art.

Raghunathan T.E., *Synthetic data, Annual Review of Statistics and Its Application,* pp. 8, 129-140, 2021.

105. Panfilo D., *I dati sintetici, una nuova frontiera per la ricerca sanitaria* in *Sole 24 Ore,* 24 novembre 2023.

106. Bolognini L., Zipponi S., *Prospettive future in sanità: spazio europeo dei dati sanitari e regolazione dei dati sintetici*, Bolognini L., Zipponi S., *Privacy e diritto dei dati sanitari*, 2024, Giuffrè, Milano, p. 280.

89 del GDPR ovvero della normativa in materia di trattamento dei dati per finalità di ricerca scientifica, pubblicazione scientifica o manifestazione del pensiero. Optare, infatti, per le basi giuridiche del legittimo interesse e del consenso non apparirebbe, infatti, proporzionato rispetto alla tipologia di trattamento[107]. Nella seconda ipotesi, invece, ovvero il caso in cui il processo di ottenimento dei dati sintetici non comporti una anonimizzazione immediata degli stessi, ma passi per un procedimento di elaborazione degli stessi in forma di dato personale, sarà richiesta un'applicazione stringente di cui agli artt. 6 e ss. del GDPR.

È chiaro, dunque, che se da un lato l'utilizzo dei dati sintetici rappresenta una frontiera ricca di opportunità per il settore della ricerca scientifica e per la stessa tutela dei dati personali relativi alla salute, dall'altra parte lo stesso richiede un intervento normativo, anche in termini di *soft law*, poiché, ad oggi, non è fornito un quadro esaustivo e maturo[108].

Da quanto finora discusso emerge che nonostante le potenzialità applicative dall'IA e dei dati sintetici, l'utilizzo di tali modelli e applicazioni nel settore sanitario ci costringe ad affrontare delle nuove sfide. Infatti, voler garantire la qualità e la certezza dei dati "primari" utilizzati come base di sviluppo dei modelli di IA e dei dati sintetici, porta inevitabilmente con sè i rischi di amplificazione dei *bias* insiti nei dataset originali, nonché del rischio di "allucinazione", ovvero del rischio che il modello inventi delle risposte o delle decisioni.

4.2. Un panorama normativo in continua evoluzione: il Data Act e il Regolamento sullo spazio europeo dei dati sanitari

Se lo scopo è fornire una panoramica quanto più completa con riferimento alle nuove prospettive in materia di trattamento dei dati personali, non possiamo non fare cenno al Regolamento Ue 2023/2854 riguardante norme armonizzate sull'accesso equo ai dati e sul loro utilizzo, ovvero il cd. Data Act[109].

---

107. Ivi, p. 281.

108. Cappellaro G., *AI e dati sintetici cambieranno la Sanità, ma solo con le giuste regole,* in *Agenda Digitale*, 22 novembre 2023.

109. 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 (regolamento sui dati).

Tale Regolamento, pubblicato in Gazzetta Ufficiale dell'Unione Europea in data 22 dicembre 2023 e che, ai sensi dell'art. 50 dello stesso, sarà applicabile a partire dal 12 settembre 2025, ha come obiettivo fondamentale la creazione di un ecosistema legislativo, uniforme a livello comunitario, per favorire e regolamentare la condivisione di dati tra privato e privato, nonché tra pubblico e privato.

Tale normativa, nel dettaglio, avrà degli impatti anche nel settore sanitario, trovando applicazione su tutti quelli che vengono definiti come "prodotti connessi", ovvero prodotti "presenti in tutti gli aspetti dell'economia e della società, tra cui infrastrutture private, civili o commerciali, veicoli, attrezzature sanitarie e legate allo stile di vita, navi, aeromobili, apparecchiature domestiche e beni di consumo, dispositivi medici e sanitari". Il Data Act richiede al Titolare (che non sempre coinciderà con il Titolare del trattamento ai sensi del GDPR) di porre essere i seguenti principali adempimenti, ovvero:

- ai sensi dell'art. 3 i "prodotti connessi" devono essere progettati e fabbricati in maniera tale che i dati (compresi i metadati) siano, per impostazione predefinita, "accessibili all'utente in modo facile, sicuro, gratuito, in un formato completo, strutturato, di uso comune e leggibile da dispositivo automatico e, ove pertinente e tecnicamente possibile, in modo diretto", dunque progettati e realizzati "*accessibili by design e by default*";
- ai sensi dell'art. 4 qualora l'Utente non deve poter accedere ai dati direttamente attraverso il "prodotto connesso" e il Titolare ha l'obbligo di mettere a disposizione dell'Utente dati (e metadati) "senza indebito ritardo, con la stessa qualità di cui dispone il titolare dei dati, in modo facile, sicuro, gratuitamente, in un formato completo, strutturato, di uso comune e leggibile da dispositivo automatico e, ove pertinente e tecnicamente possibile, modo continuo e in tempo reale";
- ai sensi dell'art. 5, nel caso in cui l'Utente ne faccia richiesta, il Titolare è obbligato a mettere i dati a disposizione di un terzo indicato dall'utente, sempre "senza indebito ritardo, con la stessa qualità di cui dispone il titolare dei dati, in modo facile, sicuro, a titolo gratuito per l'utente, in un formato completo, strutturato, di uso comune e leggibile da dispositivo automatico e, ove pertinente e tecnicamente possibile, in modo continuo e in tempo reale".

È chiaro, quindi, che con l'entrata in vigore del Data Act, si renderanno necessarie alcune attività di compliance anche nel settore *healthcare*, ad

esempio attuando delle modifiche contrattuali e coordinando la compliance al GDPR con i contenuti della nuova normativa[110].

Per concludere, un ulteriore tassello nel panorama normativo della disciplina del trattamento dei dati nel settore sanitario, sarà posto dalla pubblicazione del Regolamento sullo spazio europeo dei dati sanitari (*European Health Data Space – "EHDS"*). Tale atto, di cui si è già detto nella Parte I di questo lavoro, mira a creare "*common rules, standards and infrastructures and a governance framework*", che consentano lo scambio transfrontaliero di dati sanitari per migliorare l'assistenza ai pazienti, nonché per incentivare ricerca e innovazione. Il Regolamento – attualmente in fase di pubblicazione – renderà semplice l'accesso e il controllo sui dati sanitari personali, permettendo ai cittadini europei un accesso immediato, gratuito e sicuro alle proprie informazioni sanitarie in formato elettronico, indipendentemente dallo Stato membro in cui si trovano e mediante l'uso di piattaforme protette[111].

5. Conclusioni: linee guida per gli stakeholders di riferimento

Per trarre, dunque, le conclusioni da quanto emerso nel corso della trattazione appare opportuno ripercorrere i punti salienti di quanto discusso al fine di tentare una definizione di alcune linee guida per gli stakeholder di riferimento del settore sanitario che si trovino coinvolti nelle attività di trattamento dei dati personali relativi alla salute e debbano garantire la compliance normativa della stessa.

La definizione di alcune linee guida operative non può prescindere da una prima attività di *stakeholder categorization*, poiché diversi adempimenti in materia di *data protection* saranno richiesti a seconda del soggetto considerato e del ruolo privacy ricoperto.

Chiaro è, quindi, che la prima necessaria attività riguarderà la definizione di una corretta *governance* dei dati, che dovrà essere formalizzata analizzando di volta in volta l'impatto che ciascun *stakeholder* ha nell'operazione di trattamento.

Avremo, quindi:

- soggetti che opereranno in qualità di Titolari del trattamento (ospedali, infrastrutture pubbliche, governi e pubbliche amministrazioni, medici);

110. Stefanelli S., *L'impatto del Data Act sulla Sanità: obblighi e opportunità per le aziende*, in *Agenda Digitale*, 12 gennaio 2024.

111. Michinelli A., *Spazio europeo dei dati sanitari: arriva la rivoluzione europea, ecco di che si tratta*, in *Cybersecurity 360*, 27 gennaio 2025.

- soggetti che saranno nominati Responsabili del trattamento ai sensi dell'art. 28 del GDPR (fornitori di servizi digitali, consulenti esterni ecc.) e che, dunque, tratteranno i dati per conto dei Titolari del trattamento;
- soggetti che opereranno in qualità di autorizzati al trattamento (es. dipendenti delle strutture cliniche con ruoli amministrativi);
- soggetti che saranno interessati al trattamento dei loro dati relativi alla salute (es. i pazienti) e che avranno diritto a ricevere le tutele e le garanzie previste dalla normativa nazionale e comunitaria in materia.

Una volta definita la *governance* dei dati, sarà necessario procedere alla verifica del rispetto dei principi previsti dal GDPR e dell'adempimento degli obblighi dagli stessi derivanti, ovvero:

- l'individuazione della corretta base giuridica del trattamento, a seconda della finalità di trattamento perseguita dal Titolare;
- l'adozione di misure tecniche e organizzative adeguate ad attuare i principi di protezione dei dati;
- la corretta informazione degli interessati ai sensi degli artt. 13 e 14 del GDPR;
- lo svolgimento di una valutazione di impatto ai sensi dell'art. 35 del GDPR;
- la nomina di un DPO ai sensi dell'art. 37 del GDPR;
- la formalizzazione di adeguate procedure data protection al fine di fornire delle istruzioni operative a tutti i soggetti coinvolti attivamente nelle attività di trattamento o che potrebbero trovarsi a gestire richieste di esercizio dei diritti da parte degli interessati o episodi di violazione dei dati personali;
- la formalizzazione di un Registro dei trattamenti ai sensi dell'art. 30 GDPR.

Tali adempimenti dovranno, chiaramente, essere posti essere e calibrati nell'intensità a seconda di un'analisi pratica dell'operazione di trattamento in atto, nonché degli strumenti tecnologici coinvolti nell'attività di trattamento dei dati personali relativi alla salute. Quanto più, infatti, i diritti degli interessati saranno impattati e messi in una posizione di rischio rispetto al trattamento, tanto più gli operatori dovranno valutare con attenzione le misure tecniche e organizzative da implementare.

Infine, tali considerazioni non potranno prendere a riferimento la sola disciplina prevista in materia di protezione dei dati personali, ma necessite-

ranno sempre di più un approccio coordinato con altre normative nazionali e comunitarie[112], ad esempio in materia di Intelligenza Artificiale.

Il corretto Modello Organizzativo *Data Protection* funge, infatti, da cornice entro cui le attività medico-sanitario devono essere svolte, sempre in coerenza con il cambiamento in atto e lo sviluppo delle nuove tecnologie, affinché lo stesso possa essere al tempo stesso un punto fermo e un confine malleabile alle necessità manifestate dal mondo dei servizi.

Bibliografia

Normativa

D.lgs. 10 Agosto 2018, n. 101 **"**Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)", G.U. 4 settembre 2018.

D.lgs. 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonchè alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE. G.U. 29 luglio 2003.

Regolamento Generale sulla Protezione dei dati, Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016.

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 (regolamento sui dati).

Provvedimenti e linee guida

Autorità Garante per la protezione dei dati personali, Provvedimento n. 345/2017 "*Verifica preliminare. Riconoscimento via webcam dei partecipanti a corsi di formazione in diretta streaming*", 26 luglio 2017.

Autorità Garante per la protezione dei dati personali, Provvedimento n. 146/2019 "*recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del D.lgs. 101/2018*", 22 Luglio 2019.

112. Tra queste, il Data Act, il Regolamento sullo spazio europeo dei dati sanitari, il Data Governance Act e la Direttiva NIS 2.

Autorità Garante per la protezione dei dati personali, Provvedimento n. 55/2019 "*Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario*", 7 marzo 2019.

Autorità Garante per la protezione dei dati personali, *Il ruolo del "medico competente" in materia di sicurezza sul luogo di lavoro, anche con riferimento al contesto emergenziale*, 2020.

Autorità Garante per la protezione dei dati personali, *Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di Intelligenza Artificiale,* 2023.

Autorità Garante per la protezione dei dati personali, *Compendio sul trattamento dei dati personali effettuato attraverso piattaforme volte a mettere in contatto i pazienti con i professionisti sanitari accessibili via web e app*, marzo 2024.

Gruppo di Lavoro Articolo 29, *Linee-guida in materia di valutazione di impatto sulla protezione dei dati,* 4 ottobre 2017.

Comitato Europeo per la protezione dei dati, *Linee guida sui Responsabili della protezione dei dati,* adottate il 13 dicembre 2016, versione emendata e adottata in data 5 aprile 2017.

Comitato Europeo per la protezione dei dati, *Linee guida 5/2020 sul consenso ai sensi del regolamento (UE) 2016/679*, maggio 2020.

Comitato Europeo per la protezione dei dati personali, *Linee guida 4/2019 sull'articolo 25 Protezione dei dati fin dalla progettazione e per impostazione predefinita,* 20 ottobre 2020.

Comitato Europeo per la protezione dei dati, *Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR*, versione 2, 7 luglio 2021.

Gruppo di Lavoro Art. 29, *Parere 4/2007 sul concetto di dati personali*, 20 giugno 2007.

Gruppo di Lavoro art. 29, *Linee guida sui Responsabili della protezione dei dati,* 5 aprile 2017.

Gruppo di lavoro Art. 29 per la protezione dei dati, *Position paper related to article 30(5)*, 19 aprile 2018.

Contributi

Bolognini L., Zipponi S., *Prospettive future in sanità: spazio europeo dei dati sanitari e regolazione dei dati sintetici*, Bolognini L., Zipponi S., *Privacy e diritto dei dati sanitari*, 2024, Giuffrè, Milano, p. 280.

Bolognini L., Mannelli S., *L'arte della privacy: metafore sulla (non) conformità alle regole nell'era data-driven,* in R. D'Orazio (a cura di) *Codice della privacy e data protection*, Rubbettino, Milano, 2021.

Bongiovanni S., *Il formulario del dpo: norme, giurisprudenza, strumenti operativi e modelli di atti,* Giappichelli Editore, Torino, 2021.

Beccara J.L.A., C*ompendio breve sulla privacy: guida alla lettura del GDPR con esempi e casi pratici,* Santarcangelo di Romagna, Maggioli, 2021.

Cappellaro G., *AI e dati sintetici cambieranno la Sanità, ma solo con le giuste regole,* in *Agenda Digitale*, 22 novembre 2023.

Chizzola E., Guarda P., Maroni V., Rufo L., *Ricerca in sanità e protezione dei dati personali: scenari applicativi e prospettive future,* Università di Trento, Atti del convegno del 29 settembre 2023.

Fimiani M., *Compendio di normativa sulla privacy per il trattamento dei dati personali: guida alla lettura del codice della privacy e del GDPR,* Neldiritto editore, Roma, 2022.

Fiordalisi G., *Inquadramento e istituti di base,* in Bolognini L. e Zipponi S. (a cura di), *Privacy e diritto dei dati sanitari,* Giuffrè, Milano, 2024, pp. 8-18.

Giannini A., *Le mobile applications mediche*, Iaselli M. (a cura di), *La tutela dei dati personali in ambito sanitario*, Giuffrè, Milano, 2020.

Melchionna S., *Sanità digitale e innovazione*, in Bolognini L., Zipponi S. (a cura di), *Privacy e diritto dei dati sanitari,* Giuffrè, Milano 2024, p. 92.

Michinelli A., *Spazio europeo dei dati sanitari: arriva la rivoluzione europea, ecco di che si tratta* in Cybersecurity 360, 27 gennaio 2025.

Nanni S., *Dossier sanitario, il Garante Privacy sanziona un'Asl per accessi non autorizzati: cosa impariamo,* in *Cybersecurity360*, 10 aprile 2024.

Obermeyer Z, Powers B, Vogeli C, Mullainathan S., *Dissecting racial bias in an algorithm used to manage the health of populations*, Science, 2019.

Stefanelli S., Di NunzioA., *La governance in ambito sanitario nell'ottica del GDPR*, in M. Iaselli (a cura di), *La tutela dei dati personali in ambito sanitario*, Giuffrè, Milano 2020.

Stefanelli S., *L'impatto del Data Act sulla Sanità: obblighi e opportunità per le aziende*, in *Agenda Digitale*, 12 gennaio 2024.

S. Amato, *Biodiritto 4.0 Intelligenza artificiale e nuove tecnologie*, Giappichelli, Milano, 2020.

Zipponi S. e Biondi S., *Tutela dei dati personali nel settore dei software di area medicale e dei dispositivi medici*, in Bolognini L., Zipponi S. (a cura di), *Privacy e diritto dei dati sanitari,* Giuffrè, Milano, 2024, p. 57.

III. Sanità ed intelligenza artificiale: i sistemi di diagnostica medica alla luce dell'AI ACT

di *Giulia De Bona*

1. Opportunità e rischi dell'Intelligenza Artificiale

Nel suo percorso di sviluppo, l'Intelligenza Artificiale ha conosciuto numerose fasi, tutte caratterizzate dalla discontinuità: a momenti di forte entusiasmo sono succeduti periodi di crisi e di disincanto[1]. Ciononostante, è indubbio che a partire dal primo decennio del XXI secolo l'intelligenza artificiale abbia ottenuto risultati scientifici e tecnologici senza precedenti, presentandosi prima di tutto come «una sfida imitativa diretta non verso le creazioni umane, ma verso l'essere umano stesso, considerato come mente e cervello»[2].

1. Si parla dei cosiddetti "inverni dell'Intelligenza Artificiale". Cfr. Sartor G., *L'informatica Giuridica e le tecnologie dell'informazione. Corso di informatica giuridica*, Giappichelli, Torino, 2022, pp. 291-300.

2. Cit. Del Pizzo A., *IA e medicina*, in Iaselli M. (a cura di), *AI ACT. Principi, regole ed applicazioni pratiche del Reg. UE 1689/2024*, Maggioli, Santarcangelo di Romagna, 2024, p. 347. Ardigò A., *Un nuovo processo mimetico: le ricerche di "intelligenze artificiali". Interrogativi ed ipotesi di rilevanza*, in Negrotti M. (a cura di), *Intelligenze artificiali e scienze sociali*, FrancoAngeli, Milano, 1984, pp. 30-47.

In tal modo, robot e sistemi di IA hanno iniziato a diffondersi in svariati campi come, ad esempio, nei sistemi bancari e finanziari, nella difesa militare, nel ramo dei trasporti terrestri ed aerei, nell'ambito sanitario ed anche nei processi produttivi, operativi e distributivi del settore secondario. In questo moto acceleratorio, l'Unione Europea mira a dare maggior forza alle imprese e ai cittadini in un futuro digitale sostenibile, prospero ed incentrato sulla persona.

Sin dal 2020, con la strategia per *Plasmare il futuro digitale dell'Europa*, si punta sulle tecnologie a vantaggio delle persone, promuovendo i valori democratici, rispettando i diritti fondamentali e contribuendo a un'economia sostenibile, a impatto climatico zero ed efficiente nell'impiego delle risorse. In particolare, tre sono gli obiettivi fondamentali che ci si è posti: «1. Una tecnologia al servizio delle persone: sviluppare, diffondere e adottare tecnologie che migliorino sensibilmente la vita quotidiana delle persone (…). 2. Un'economia equa e competitiva: un mercato unico senza attriti, in cui le imprese di tutte le dimensioni e in qualsiasi settore possano competere in condizioni di parità e possano sviluppare, commercializzare e utilizzare tecnologie, prodotti e servizi digitali su una scala tale da rafforzare la loro produttività e la loro competitività a livello mondiale, e in cui i consumatori possano essere certi che i loro diritti vengano rispettati. 3. Una società aperta, democratica e sostenibile: un ambiente affidabile in cui i cittadini siano autonomi e responsabili nel modo in cui agiscono e interagiscono, anche in relazione ai dati che forniscono sia online sia offline (…)»[3].

Per approdare, poi, nell'anno successivo, alla *Bussola per il digitale: il modello europeo per il decennio digitale*, il quale, reduce dalla pandemia da COVID-19, definisce gli obiettivi digitali dell'UE per il 2030 in materia di competenze, governo, imprese e infrastrutture, facendo molta attenzione anche alla digitalizzazione in campo socio-sanitario ed assistenziale[4].

---

3. Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, *Plasmare il futuro digitale dell'Europa*, COM (2020) 67 final, 19.2.2020, Bruxelles, p. 2-3. Reperibile al link: *https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52020DC0067*. Si anticipi sin da ora, con riferimento al settore sanitario in senso ampio, che tra gli obiettivi principali vi è anche: «La promozione di cartelle cliniche elettroniche basate su un formato comune europeo di scambio per consentire ai cittadini europei di accedere a dati sanitari e scambiarli in tutta l'UE in modo sicuro. Uno spazio europeo dei dati sanitari per migliorare la sicurezza dell'accessibilità dei dati sanitari, che consentirà una ricerca, una diagnosi e un trattamento mirati e più rapidi (dal 2022)», p. 13.

4. Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, *Bussola per il digitale: il modello europeo per il decennio digitale*, COM(2021) 118 final, 9.3.2021, Bruxelles. Reperibile al link: *https://eur-lex.europa.eu/resource.html?uri=cellar:12e835e2-81af-11eb-9ac9-01aa75ed71a1.0021.02/DOC_1&format=PDF*.

Risulta evidente il ruolo decisivo delle nuove tecnologie, ed in particolare dell'intelligenza artificiale, nel miglioramento di ogni aspetto della vita quotidiana; tuttavia, affinché la trasformazione digitale divenga effettiva, si dovranno creare quadri normativi appropriati che garantiscano il diritto indiscriminato di accesso al mondo digitale e, soprattutto, l'affidabilità delle tecnologie stesse anche di fronte ai possibili usi distorti che se ne possono fare.

Così, per arginare i rischi correlati all'impiego dell'intelligenza artificiale, senza però limitare l'avanzamento della ricerca nonché, appunto, i vantaggi da essa derivanti, sono state adottate delle iniziative destinate a delineare un quadro etico e giuridico di carattere antropocentrico[5].

Dal punto di vista etico, esemplare è la sintesi elaborata da un ristretto gruppo di lavoro costituito su iniziativa dell'Unione Europea, l'*AI4People*, il quale afferma la necessità che l'IA consenta la realizzazione dell'essere umano nel pieno delle sue capacità, che si ponga solo a supporto dell'azione umana escludendo una sua deresponsabilizzazione, e che agevoli la coesione sociale senza limitare la autodeterminazione umana.

A tale scopo, per il raggiungimento di un' IA affidabile sarebbe necessario rispettare i seguenti sette principi: 1) iniziativa e controllo umano; 2) robustezza tecnica e sicurezza dei sistemi; 3) rispetto della *privacy* e *governance* dei dati; 4) trasparenza, tracciabilità, spiegabilità e comunicazione; 5) diversità, non discriminazione ed equità; 6) benessere sociale e ambientale; 7) responsabilità, verificabilità minimizzazione e comunicazione degli impatti negativi, mezzi risarcitori[6].

A ciò si aggiungono i lavori condotti da un gruppo di esperti sull'intelligenza artificiale, istituito dalla Commissione Europea, che ha di recente pubblicato una serie di linee guida etiche per una intelligenza artificiale degna di fiducia. Secondo l'AI-HLEG[7], le basi di un IA rispettosa del diritto,

---

5. Regolamento UE 2024/1689, Considerando 1: «Lo scopo del presente regolamento è migliorare il funzionamento del mercato interno istituendo un quadro giuridico uniforme in particolare per quanto riguarda lo sviluppo, l'immissione sul mercato, la messa in servizio e l'uso di sistemi di intelligenza artificiale (sistemi di IA) nell'Unione, in conformità dei valori dell'Unione, promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea («Carta»), compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, proteggere contro gli effetti nocivi dei sistemi di IA nell'Unione, nonché promuovere l'innovazione».

6. Floridi L., Cowls J., Beltrametti M., Chatila R., Chazerand P., Dignum V., Luetge C., Medeline R., Pagallo U., Rossi F., Schafer B., Valcke P., Vayena E., *AI4People - An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations*, in "Minds and Machines", n. 28, 2018, pp. 689-707.

7. AI-HLEG è l'acronimo di High Level Expert Group on Artificial Intelligence, e rappresenta un gruppo di 52 esperti nominati dalla Commissione Europea per individuare

etica e robusta, sono i seguenti principi: 1) rispetto dell'autonomia; 2) prevenzione del danno; 3) equità procedurale e sostanziale; 4) spiegabilità delle decisioni algoritmiche[8].

Se la parola chiave, nel rapporto tra l'essere umano ed i sistemi di intelligenza artificiale, è *fiducia*, di non trascurabile rilevanza è anche l'intervento in ambito giuridico concretizzatosi di recente con l'AI Act[9], il quale individua una regolamentazione funzionale a plasmare i sistemi di IA, in modo che gli stessi siano affidabili ed in linea con i diritti e i valori dell'UE, garantendo imprescindibilmente il controllo umano, la sicurezza, la *privacy,* la trasparenza, la non discriminazione e il benessere sociale e ambientale[10]. Con questa aspirazione garantistica e di tutela, anche dei valori della democrazia e dello Stato di diritto, l'AI Act fondandosi su un approccio basato sul rischio, in ragione del quale i sistemi di IA sono classificati in diverse categorie di rischio a seconda di quanto possano incidere negativamente sui diritti fondamentali ed i valori dell'Unione, stabilisce norme armonizzate per l'immissione sul mercato, la messa in servizio e l'uso dell'intelligenza artificiale in tutto il territorio unionale.

2. L'IA nel settore sanitario: I sistemi robotici e di intelligenza artificiale per uso diagnostico

Uno dei fenomeni più rilevanti del XXI secolo è l'invecchiamento della popolazione; si stima, infatti, che circa il 12% della popolazione mondiale

---

delle misure attuative della strategia operativa in merito all'Intelligenza Artificiale adottata nel 2018 dalla Commissione stessa.

8. AI-HLEG, *Orientamenti etici per un'IA affidabile*, 2019.

9. Regolamento UE 1689/2024, esso si basa sul principio che l'IA deve essere sviluppata e utilizzata in modo sicuro, etico e rispettoso dei diritti fondamentali e dei valori europei.

10. In riferimento a ciò si veda anche il contenuto del Considerando 47 dell'AI Act: «I sistemi di IA potrebbero avere un impatto negativo sulla salute e sulla sicurezza delle persone, in particolare quando tali sistemi sono impiegati come componenti di sicurezza dei prodotti. Coerentemente con gli obiettivi della normativa di armonizzazione dell'Unione di agevolare la libera circolazione dei prodotti nel mercato interno e di garantire che solo prodotti sicuri e comunque conformi possano essere immessi sul mercato, è importante che i rischi per la sicurezza che un prodotto nel suo insieme può generare a causa dei suoi componenti digitali, compresi i sistemi di IA, siano debitamente prevenuti e attenuati. Ad esempio, i robot sempre più autonomi, sia nel contesto della produzione sia in quello della cura e dell'assistenza alle persone, dovrebbero essere in misura di operare e svolgere le loro funzioni in condizioni di sicurezza in ambienti complessi. Analogamente, nel settore sanitario, in cui la posta in gioco per la vita e la salute è particolarmente elevata, è opportuno che i sistemi diagnostici e i sistemi di sostegno delle decisioni dell'uomo, sempre più sofisticati, siano affidabili e accurati».

ha più di 65 anni e che entro il 2050 tale percentuale salirà, quasi duplicandosi, al 21%[11].

Non a caso il settore sanitario costituisce una delle principali fonti di finanziamento e conseguente sviluppo tecnologico ed informatico degli ultimi anni[12]. Le applicazioni spaziano dai sistemi di chirurgia robotica, ai sistemi di supporto alle diagnosi, alla ricerca farmaceutica, al monitoraggio dei pazienti, sino alle terapie personalizzate e così via. Difatti, l'IA, grazie ai sofisticati algoritmi *self learning* che la caratterizzano, è capace di processare e analizzare importanti complessi di dati, individuando *pattern* articolati e fornendo, a titolo di risposta, *insight* preziosi; ciò fa sì che tali sistemi si pongano come delle componenti indispensabili nel funzionamento e nel perfezionamento del settore sanitario.

Con lo scopo di meglio implementare l'ecosistema sanitario con le innovative tecnologie di cui si può oggi disporre, già nel 2018 la Commissione Europea, con una comunicazione al Parlamento, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, sosteneva che: «(…) solo con una nuova concezione dei nostri sistemi sanitari e assistenziali potremmo garantire che questi si mantengano adeguati al loro scopo. Ciò significa concepire sistemi che mirino a continuare a promuovere la sanità, prevenire malattie e fornire assistenza incentrata sul paziente che soddisfi i bisogni dei cittadini. I sistemi sanitari e assistenziali necessitano di riforme e soluzioni innovative per diventare maggiormente resilienti, accessibili ed efficaci nel fornire assistenza di qualità ai cittadini europei»[13].

Il campo della medicina si è sempre dimostrato profondamente recettivo all'introduzione di sistemi tecnologici; difatti, conformemente a quanto rilevato dal Parlamento Europeo nelle due Risoluzioni in materia di diritto

---

11. Galluzzo L., Gandin C., Ghirini S., Scafato E., *L'invecchiamento della popolazione: opportunità o sfida?*, Centro Nazionale di Epidemiologia, Sorveglianza e Promozione della Salute, Istituto Superiore di Sanità, Roma.

12. Ad esempio si consideri il contenuto del documento prodotto dall'EuRobotic, *Strategic research agenda for robotics in europe 2014-2020*. Reperibile al link: https*://old.eurobotics.net/sparc/upload/topic_groups/SRA2020_SPARC.pdf*. Si veda anche: *EU4Health: Programma Europeo Salute 2021-2027*, reperibile al link: *https://www.salute.gov.it/portale/rapportiInternazionali/dettaglioContenutiRapportiInternazionali.jsp?area=rapporti&id=1948&lingua=italiano&menu=programmi.*

13. Comunicazione della Commissione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni *relativa alla trasformazione digitale della sanità e dell'assistenza nel mercato unico digitale, alla responsabilizzazione dei cittadini e alla creazione di una società più sana*, COM (2018) 233 final, 25.4.2018, Bruxelles, p. 1. Reperibile al link: *https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52018DC0233*.

civile e intelligenza artificiale[14], e come anche ribadito successivamente dalla Commissione Europea nel Libro Bianco sull'Intelligenza Artificiale[15], i dispositivi medici[16] dotati di intelligenza artificiale si prestano ad essere particolarmente adatti a svolgere operazioni chirurgiche ad alta precisione, eseguire operazioni ripetitive ed a portare a termine compiti di assistenza personalizzata. Sia le Risoluzioni, che il Libro Bianco, inoltre, sottolineano come la collaborazione tra intelligenza artificiale e diagnosi formulata da un essere umano, riduca considerevolmente il tasso di errore e le tempistiche rispetto al caso in cui ciò fosse svolto esclusivamente da un operatore umano[17].

Più precisamente, se in origine già rivoluzionario è apparso l'avvento dello stetoscopio, quale primo strumento in grado di far sentire i suoni interni del corpo umano in modo non invasivo; il percorso evolutivo delle tecnologie in ambito medico, molto dinamico e diversificato, ha raggiunto livelli di sofisticatezza tali da introdurre non solo soluzioni all'avanguardia, ma anche promettenti innovazioni, funzionali al miglioramento della qualità, dell'efficienza e dell'efficacia delle cure mediche[18].

Passando attraverso sistemi avanzati di documentazione elettronica, i quali facilitano la raccolta, la registrazione, la gestione e la conservazione

---

14. Risoluzione del Parlamento Europeo del 16 febbraio 2027 recante raccomandazioni alla Commissione concernenti norme di diritto civile della robotica e Risoluzione del Parlamento Europeo del 12 febbraio 2019 su una politica industriale globale in materia di robotica e intelligenza artificiale.

15. Commissione Europea, *Libro Bianco sull'intelligenza artificiale - Un approccio europeo all'eccellenza e alla fiducia*, Reperibile al link: *https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:52020DC0065*.

16. Si tenga presente che la definizione di «dispositivi medici» a livello europeo è contenuta all'interno dell'art. 1 paragrafo 2 della Direttiva 93/42/CEE: «qualunque strumento, apparecchio, impianto, software, sostanza o altro prodotto, utilizzato da solo o in combinazione, compreso il software destinato dal fabbricante ad essere impiegato specificamente con finalità diagnostiche e/o terapeutiche e necessario al corretto funzionamento del dispositivo, destinato dal fabbricante ad essere impiegato sull'uomo a fini di: diagnosi, prevenzione, controllo, terapia o attenuazione di una malattia; diagnosi, controllo, terapia, attenuazione o compensazione di una ferita o di un handicap; studio, sostituzione o modifica dell'anatomia o di un processo fisiologico; — intervento sul concepimento, la cui azione principale voluta nel o sul corpo umano no sia conseguita con mezzi farmacologici né immunologici né mediante metabolismo, ma la cui funzione possa essere assistita da questi mezzi».

17. Cfr. Lupton M., *Some ethical and legal consequences of the application of artificial intelligence in the fiel of medicine*, in *Trends Med*, vol. 18, n. 4, 2018, pp. 1-7; De Menech C., *Intelligenza artificiale e autodeterminazione in materia sanitaria*, in *BioLaw Journal-Rivista di BioDiritto*, 1, 2022, p. 183.

18. Del Pizzo A., *IA e medicina*, in Iaselli M. (a cura di), *AI ACT. Principi, regole ed applicazioni pratiche del Reg. UE 1689/2024*, Maggioli, Santarcangelo di Romagna, 2024, p. 345.

delle informazioni cliniche dei pazienti, si è giunti alla semplificazione, per i professionisti, dell'accesso e della condivisione dei dati clinici, con conseguente snellimento e miglioramento della prestazione medica erogata.

Ad oggi, i protagonisti indiscussi del progresso tecnologico nell'ambito qui preso in esame sono i sistemi di robotica medica e i sistemi di supporto alle decisioni cliniche (CDSS, *Clinical Decision Support Systems*); simili strumenti, assumendo il ruolo di validi alleati del professionista sanitario, sono in grado di offrire raccomandazioni fondate su dati precisi, migliorando considerevolmente la qualità delle decisioni cliniche[19].

In sintesi, pertanto, si può concludere che la robotica e i sistemi di IA in ambito sanitario sono sviluppati per svolgere diverse tipologie di compiti come, ad esempio, migliorare il lavoro svolto dagli operatori sanitari, estendere la possibilità di intervento nelle operazioni chirurgiche, supportare il medico in ambito diagnostico e terapeutico, assistere i pazienti nelle attività riabilitative, fare previsioni sul decorso di una malattia o sulla probabilità di sviluppare certe patologie, supportare le campagne di prevenzione, migliorare le capacità fisiche degli esseri umani o assisterli nell'esecuzione di determinati compiti (si pensi alle protesi robotiche)[20].

Sin da ora è utile ribadire che si è comunque di fronte ad un settore che merita particolari attenzioni, in quanto riguarda prevalentemente l'accesso a servizi e prestazioni essenziali, tanto pubbliche quanto private, necessarie affinché l'intera comunità possa partecipare pienamente alla vita sociale e migliorare anche il proprio tenore di vita.

Più precisamente, «le persone fisiche che chiedono o ricevono prestazioni e servizi essenziali di assistenza pubblica dalle autorità pubbliche, vale a dire servizi sanitari, prestazioni di sicurezza sociale, servizi sociali che forniscono protezione in casi quali la maternità, la malattia, gli infortuni sul lavoro, la dipendenza o la vecchiaia e la perdita di occupazione e l'assistenza sociale e abitativa, sono di norma dipendenti da tali prestazioni e servizi e si trovano generalmente in una posizione vulnerabile rispetto alle autorità responsabili»[21].

Proprio per questo motivo, i sistemi programmati secondo l'intelligenza artificiale utilizzati per simili prestazioni e servizi, potendo avere un impatto

19. Cfr. Azzi S., Gagnon S., Ramirez A., Richards G., *Healthcare applications of artificial intelligence and analytics: A review and proposed framework*, in *Applied sciences*, 10(18), 6553, 2020, pp. 1-21; Kitsios F., Kamariotou M., Syngelakis A.I., Talias M.A., *Recent advances of artificial intelligence in healthcare: A systematic literature review*, in *Applied sciences*, 13(13), 7479, 2023, pp. 1-22.

20. Lagioia F., *L'intelligenza artificiale in sanità: un'analisi giuridica*, Giapichelli, Torino, 2020, pp. 21-23.

21. Regolamento UE 1689/2024 Considerando 58.

significativo sul sostentamento delle persone e violare i loro diritti fondamentali, quali il diritto alla protezione sociale, alla non discriminazione, alla dignità umana, dovrebbero essere classificati come sistemi ad alto rischio e di conseguenza, dovrebbero essere concessi, negati, ridotti, revocati o recuperati dalle autorità, una volta compreso se i beneficiari abbiano legittimamente diritto a tali prestazioni o servizi, oppure no.

2.1. I sistemi esperti nel settore medico-diagnostico

Per una analisi più approfondita, si consideri che i sistemi di IA sono, anzitutto, *software* che non differiscono dai comuni programmi che si compongono di una pluralità di algoritmi, ossia sequenze di istruzioni, definite in modo univoco, per eseguire efficacemente un compito[22]; con la precisazione che solo i sistemi IA sono in grado di eseguire compiti che sarebbero considerati intelligenti, se venissero assolti da un essere umano.

Date queste premesse, occorre, altresì, chiarire che i *software* di IA si articolano nel seguente modo: da un lato, in robot e bot[23], a seconda che siano incorporati o meno in un automa, ossia in un apparato meccanico e elettronico che, avendo una propria dimensione fisica, opera materialmente nella realtà concreta e non virtuale; dall'altro lato, in sistemi di rappresentazione formale della conoscenza, qualificati pure come sistemi simbolici, e sistemi connessionisti[24], in base alla relativa struttura e alle proprie modalità di funzionamento[25]. Inoltre, queste due diverse categorie sono rappresentative di altrettanti diversi approcci funzionalisti: il *top down* e il *bottom up*[26]; mentre

22. Moro P., *Macchine come noi. Natura e limiti della soggettività robotica*, in Ruffolo U. (a cura di), *Intelligenza artificiale – Il diritto, i diritti, l'etica*, Milano, 2020, p. 51; Sartor G., Lagioia F., *Le decisioni algoritmiche tra etica e diritto*, in Ruffolo U. (a cura di), *Intelligenza artificiale – Il diritto, i diritti, l'etica*, Milano, 2020, pp. 63 ss.

23. Russell S. J., Norvig P., *Intelligenza artificiale. Un approccio moderno*, vol. 2, II ediz., Milano, 2005, pp. 55 ss.

24. Russell S., Norvig P., *Intelligenza artificiale-Un approccio moderno*, vol. 1, IV ediz. Milano, 2021, pp. 26 s.; Sartor G., Lagioia F., *Le decisioni algoritmiche tra etica e diritto*, in Ruffolo U. (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020, pp. 68 ss.

25. Si precisa sin da ora, ai fini della più chiara argomentazione, che le nozioni di sistemi connessionisti e reti neurali sono interscambiabili.

26. L'approccio *top down* si basa sull'elaborazione simbolica introdotta da Newell e Simon nel XX secolo, in concreto si introduce la conoscenza nella *knowledge base* e la macchina la traduce in dati e simboli logici: a partire da una serie di conoscenze, dichiarazioni o affermazioni, il sistema deduce gli effetti. Ciò significa che la conoscenza viene rappresentata tramite frasi dichiarative secondo la logica del primo ordine o un altro linguaggio logico-

il primo prende le mosse dalla comprensione dei processi intellettivi del cervello umano per poi riproporli, la seconda tipologia di approccio principia dalla disamina analitica del cervello, mirando alla sua riproduzione sintetica.

Quali espressioni del metodo *top down* si trovano i sistemi simbolici, i quali manifestano l'abilità di riproporre gli stessi ragionamenti logici che danno forma all'attività intellettiva umana; al proposito, il sistema di rappresentazione formale della conoscenza per eccellenza è il sistema esperto, programma che si comporta proprio come un "esperto" in determinati ambiti, fornendo risposte, in termini di *output*, coerenti, precise e approfondite con la stessa sicurezza di uno specialista in materia[27].

Ciascun sistema esperto si compone di due elementi: «un elemento strutturale, in ragione del quale il sistema è basato sulla conoscenza, cioè si compone di una base di conoscenza distinta dal motore inferenziale; e, un elemento funzionale, in ragione del quale il sistema deve essere in grado di fornire prestazioni che richiedano notevoli competenze»[28].

---

matematico, ed è proprio in questo modo che il processo di ragionamento produce nuova conoscenza. Più precisamente, questi sistemi sono composti da tre parti fondamentali: il "livello di conoscenza", secondo il quale nella macchina sono introdotte le informazioni di un particolare dominio di conoscenza (es. il dominio della medicina); il "livello dei simboli", ossia la conoscenza reale viene rappresentata e organizzata secondo strutture e linguaggi simbolici che permettono sia la memorizzazione dei dati e dei nessi logici, che l'elaborazione tramite processi inferenziali; per ultimo si presenta il "livello sub-simbolo", secondo il quale al di sotto del livello dei simboli, le informazioni sono trasformate in segnali.

L'approccio *bottom up*, come suggerisce la nomenclatura stessa, è un processo che segue un percorso dal basso verso l'alto; ciò significa che al sistema viene innanzitutto insegnato ad interagire con l'ambiente ed a rispondere agli *input* esterni, ed una volta realizzata tale base di conoscenza, si procede con la realizzazione dello stato di sviluppo successivo, seguendo, per così dire, le stesse tappe evolutive avvenute in natura. Tentando un paragone con la biologia evoluzionista, per la quale l'uomo è il prodotto di una lunga evoluzione, iniziata con la nascita, la crescita e l'evoluzione in base all'esperienza; parimenti dovrebbe accadere con i sistemi programmati secondo l'intelligenza artificiale, ove l'ente interagendo con l'ambiente dinamico costruisce dei comportamenti imparando dall'esperienza e migliorandosi progressivamente. Cfr. Di Stasio G., *Machine learning e reti neurali nel diritto civile. Applicazione del machine learning a casi di diritto condominiale*, in *i-lex, 2018;* Lagioia F., *L'intelligenza artificiale in sanità: un'analisi giuridica*, Giappichelli, Torino, 2020; Newell A., Simon H. A., *Human problem solving*, Prentice Hall-Inc., Englewood Cliffs, New Jersey, 1972; Sartor G., *L'intelligenza artificiale e il diritto*, Giappichelli, Torino, 2022.

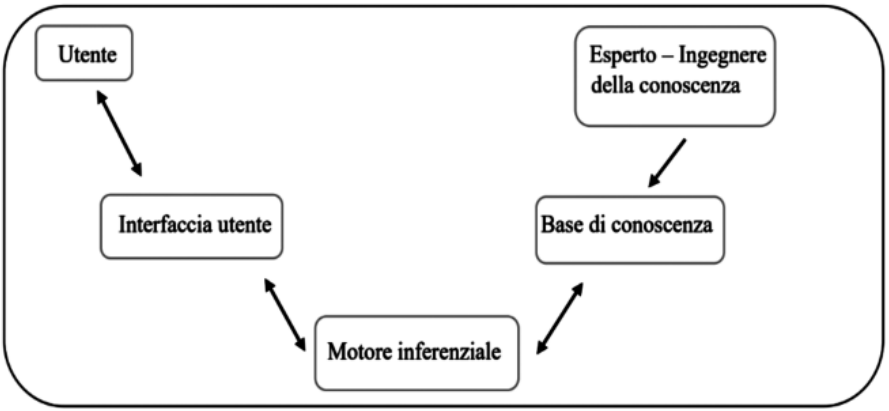
27. Sartor G., Lagioia F., *Le decisioni algoritmiche tra etica e diritto*, in Ruffolo U. (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020, 68 ss.

28. Iaselli M., *Le origini dell'IA, evoluzione e rapporti con il diritto*, in Iaselli M. (a cura di) *AI ACT. Principi, regole e applicazioni pratiche del Reg. UE 1689/2024*, Maggioli, Santarcangelo di Romagna, 2024, p. 19. Cfr. Sartor G., *Intelligenza artificiale e diritto. Un'introduzione*, Giuffrè, Milano, 1996, pp. 15 ss.; Sartor G., *L'intelligenza artificiale e il diritto*, Giappichelli, Torino, 2022, pp. 35 ss.

Tali sistemi sono programmi in cui l'utente interagisce con il sistema con una sorta di dialogo, similmente a quanto avviene in una normale conversazione con un essere umano, in cui viene esposto un problema e vengono rivolte domande sulle soluzioni proposte; per queste loro caratteristiche, possono essere visti come veri e propri intermediari tra gli esperti umani che interagiscono con il sistema per acquisire conoscenza, e l'utente umano che interagisce con il sistema a titolo di consultazione[29].

Si comprende, pertanto, che l'elemento distintivo del sistema esperto è quello che lo stesso dovrebbe essere in grado di riproporre il ragionamento che un esperto umano farebbe nelle stesse circostanze; le soluzioni presentate, difatti, dovrebbero essere di alta qualità e caratterizzate anche da una maggior rapidità di prospettazione.

Fig. 1 – Schema di sistema basato sulla conoscenza



Di non trascurabile rilevanza è l'ulteriore caratteristica che connota tali sistemi esperti: la loro capacità di spiegare e giustificare i propri comportamenti, *rectius* gli *output* prodotti, fornendo delucidazioni in merito al ragionamento seguito. Inoltre, il sistema esperto può anche rispondere ad impulsi sulla base di informazioni incomplete o addirittura incerte, sforzandosi di ricavare delle soluzioni attingendo a diverse combinazioni delle informazioni impartite *ab origine*.

Sintetizzando, pertanto, un sistema di questo tipo si dovrebbe presentare come trasparente, ossia in grado di giustificare e/o spiegare l'*iter* logico per-

29. Iaselli M., *Le origini dell'IA, evoluzione e rapporti con il diritto*, in Iaselli M. (a cura di) *AI ACT. Principi, regole e applicazioni pratiche del Reg. UE 1689/2024*, Maggioli, Santarcangelo di Romagna, 2024, pp. 19-20.

seguito per il raggiungimento della soluzione; flessibile, vale a dire capace di fronteggiare dinamiche modificazioni delle loro basi di conoscenza; capace di utilizzare il metodo euristico nella ricerca delle soluzioni ai problemi posti, al pari di un esperto umano.

Scendendo più nel particolare, con riferimento specifico ai sistemi robotici e di intelligenza artificiale per uso diagnostico, si rileva che il sistema esperto, ossia, appunto un sistema informatico basato su un modello di comportamento intelligente, capace di effettuare attività che richiedono particolari competenze e cognizioni[30], sia lo strumento che meglio soddisfa le esigenze che la disciplina medica pone alle scienze informatiche e tecnologiche. Difatti, grazie a tali sofisticate tipologie di sistemi si raggiungono importanti obiettivi diagnostici in termini di assistenza alla decisione clinica: organizzando opportunamente la conoscenza medica secondo criteri e strategie definite da esperti, il sistema sarà in grado di fornire spiegazioni precise dei procedimenti compiuti, dei ragionamenti effettuati e delle conclusioni raggiunte[31].

E ciò, a titolo esemplificativo, è proprio quello che accade chiedendo un consulto a *Mycin*[32], sistema esperto, progettato al fine della identificazione di batteri alla base di infezioni gravi quali la batteriemia e la meningite, e della individuazione del relativo trattamento farmacologico.

L'utente, nel caso in esame l'operatore medico, dovrà rispondere ad una prima serie di domande, poste dal sistema *Mycin*, relativamente ai sintomi

---

30. Sartor G., *Intelligenza artificiale e diritto. Un'introduzione*, Giuffrè, Milano, 1996, pp. 22-23.

31. Lagioia F., *L'intelligenza artificiale in sanità: un'analisi giuridica*, Giapichelli, Torino, 2020, pp. 32-33. In particolare, le loro caratteristiche tecniche principali sono, cit.: «a) esplicito riferimento a un modello metodologico convalidato; b) la facilità di archiviazione e recupero dei dati preesistenti; c) la disponibilità di aiuti in linea; d) la giustificazione delle richieste e delle conclusioni raggiunte; e) l'aggiornamento frequente delle basi di conoscenza; f) la verifica e la validazione clinica delle prestazioni». Cfr. Paparella F., *Sistema esperto per la diagnosi delle malattie del fegato e delle vie biliari con gestione dell'incertezza*, Bari, 2010, pp. 48 ss.

32. *Mycin* è uno dei primi esempi innovativi di intelligenza artificiale nel settore sanitario. Sviluppato negli anni '70 presso l'Università di Stanford, è stato progettato come un sistema esperto per assistere i medici nell'identificazione dei batteri che causano gravi infezioni e nella raccomandazione degli antibiotici. La sua notorietà ed importanza non risiede solo nella sua applicazione, ma anche nel modo in cui ha rivoluzionato l'uso dell'intelligenza artificiale nella diagnosi e nel trattamento medico. Nonostante le sue promettenti capacità, *Mycin* non è molto impiegato nella pratica clinica reale; difatti, come si diceva poc'anzi, la sua importanza risiede piuttosto nel suo ruolo di precursore, mostrando che l'intelligenza artificiale poteva assistere i medici nelle decisioni cliniche. Cfr. Gorry G.A., *Computer-assisted clinical decision-making,* in *Methods Inf Med*, 1973, vol. 12, n. 1, pp. 45–51; Shortliffe, E.H., *Mycin: a knowledge-based computer program applied to infectious diseases*, AMIA Annual Symposium Proceedings Archive, 1977, pp. 66-69.

che il paziente presenta, in questo modo si individuano delle iniziali ipotesi diagnostiche potenzialmente valide. Dopodiché, il *software* formula tutta un'ulteriore serie di domande sempre più direzionali alla precisa identificazione della diagnosi, fintanto che non si approda alla diagnosi finale, la quale si porrà come l'unica "risposta" che è perfettamente sussumibile a quel singolo caso clinico. Infine, il programma procede alla prescrizione della terapia da seguire.

Dal momento che il sistema esperto di Standford porta a termine il proprio compito avvalendosi del ragionamento per esclusione, non deve stupire: né che di fronte a settori di particolare complessità, il sistema stesso impieghi un lasso di tempo apprezzabile per l'elaborazione di un *output*, dovendo attingere ad una vastissima gamma di regole/informazioni impartite, abbisognando, altresì, di conseguenza, di una continua implementazione da parte dei programmatori; e neppure, che terminato l' "interrogatorio", il caso concreto possa sussumersi in più "regole" diagnostiche diverse. In quest'ultima ipotesi, il sistema *Mycin* potrà solo indicare quale delle diagnosi individuate riterrà più probabile, attribuendo a ciascuna un grado di priorità sulle altre.

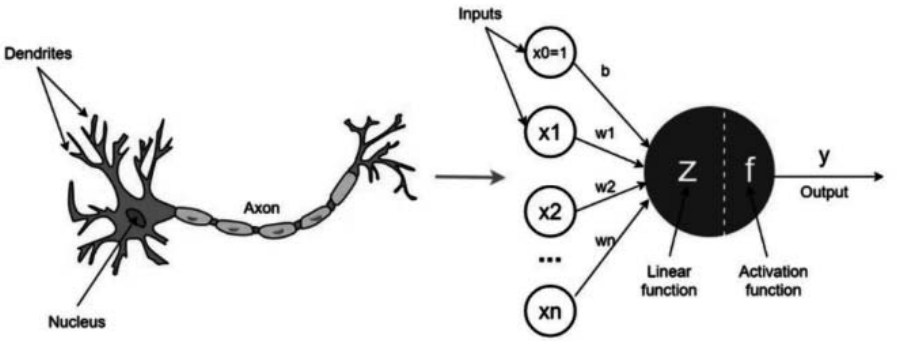
2.2. Le reti neurali nel settore medico-diagnostico

I sistemi connessionisti, o reti neurali, sono invece espressione dell'approccio *bottom up* e, traendo la propria ragion d'essere dalle strutture fisiologiche del cervello umano, presentano delle evidenti affinità con quest'ultimo: il percettrone[33], ossia la loro unità elementare è nient'altro che la

33. Dal punto di vista squisitamente informatico, il percettrone è nient'altro che una funzione matematica, elaborata per la prima volta nel 1943 da Warren McCulloch e Walter Pitts: secondo il loro modello, si ha un certo numero di *input*, un determinato peso per ogni *input* e un valore di *bias*. In particolare, rispetto alla somma dei prodotti di ogni *input* per il relativo peso va sottratto il valore di *bias*: quando il saldo è pari o positivo, il percettrone emette l'*output* e si lega ad un suo simile; nel momento in cui, invece, il saldo risulti negativo, nessun segnale viene emesso e nessun collegamento tra percettroni viene creato. In altre parole, si pensi di avere un *input* A, di valore 1 e con peso pari a 1, un *input* B, di valore 2 e peso 2, e un valore di *bias*, corrispondente a 3. Se si moltiplicano gli *input* A e B per il loro corrispondente peso si otterrà il seguente risultato: 1 e 4. La loro somma è maggiore del valore di *bias* 3, pertanto il percettrone emetterà un segnale, e così facendo si legherà al percettrone successivo. Esclusivamente in presenza di una molteplicità di strati di percettroni potrà parlarsi di rete neurale di base, nel caso in cui vi siano due o tre livelli di percettroni, o profonda, in presenza di più strati. Cfr. Sartor G., Lagioia F., *Le decisioni algoritmiche tra etica e diritto*, in Ruffolo U. (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè Francis Lefebvre, Milano, 2020.

riproduzione digitale del neurone, inoltre, l'unione di più percettroni conduce alla nascita di una rete neurale, in tutto similare a quella umana. Difatti, al pari di ciascuna cellula neurale umana, la quale si compone di un nucleo dal quale partono una serie di collegamenti, i dendriti, che trasportando impulsi da un neurone all'altro danno poi vita alla rete neurale in quanto tale, anche il percettrone è dotato di una unità elementare che viene sollecitata dagli *input* che la raggiungono per il tramite della rete di collegamenti che la lega ad altri percettroni.

Fig. 2 – Confronto tra neurone umano e percettrone[34]



Tali sistemi, a differenza dei sistemi simbolici, basano il loro funzionamento sull'apprendimento automatico[35], e ciò significa che a loro viene fornito, non tanto un insieme di conoscenze da cui muovere per generare *output* in termini di risposta/comportamento; bensì, un vero e proprio metodo di apprendimento[36],

34. Sartor G., *Intelligenza artificiale e diritto. Un'introduzione*, Gappichelli, Torino, 2022, p. 56.

35. Sartor G., Lagioia F., *Le decisioni algoritmiche tra etica e diritto*, in Ruffolo U. (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè Francis Lefebvre, Milano, 2020, pp. 68 ss.

36. Tre sono i metodi per l'apprendimento automatico: l'apprendimento supervisionato, l'apprendimento non supervisionato e l'apprendimento per rinforzo. Nel primo caso, si inserisce all'interno della macchina un training set, ossia un insieme di informazioni che forniscono la rappresentazione di un oggetto, qualificandolo. In questo modo, ad esempio, su richiesta il sistema, procedendo alla profilazione di immagini di specifiche piante ed all'analisi dei dati del training set, sarà in grado di sussumere l'immagine al nome della pianta che più le assomiglia. Il secondo metodo di apprendimento, prevede che nella macchina si immettano una importante quantità di dati non elaborati, sul presupposto che sia la macchina stessa a procedere a raggruppare ed ordinare i dati che tra loro presentano delle affinità. In ultimo, il metodo di apprendimento automatico, prevede che la macchina impari ad agire facendo tentativi, sbagliando e riprovando fintanto che non si raggiunga l'obiettivo impartito, incidendo sull'ambiente circostante. Cfr. Sartor G., Lagioia F., *Le decisioni algoritmiche tra etica e diritto,* in Ruffolo U. (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè Francis Lefebvre, Milano, 2020, p. 69. Marmo, R., *Algoritmi per l'intelligenza*

grazie al quale il sistema stesso potrà autonomamente rielaborare i dati carpiti dal mondo circostante.

Un esempio concreto di rete neurale applicata alla diagnostica medica è il sistema *Watson for Oncology*[37], quale sistema di intelligenza artificiale, sviluppato all'interno del progetto *DeepQA* di IBM, rappresentante un'applicazione avanzata di elaborazione del linguaggio naturale, recupero delle informazioni, rappresentazione della conoscenza, ragionamento automatico e tecnologie di apprendimento automatico nel campo dell' *open domain question answering*[38].

Il funzionamento del sistema è il seguente: nella macchina viene inserita la cartella clinica elettronica di un paziente che viene approfonditamente analizzata dal sistema stesso il quale avrà, così, piena contezza del completo quadro clinico, comprensivo di risultati dei test di laboratorio, referti di visite sostenute in passato e così via. A questo punto il sistema attinge alle numerose informazioni che le sono state "date in pasto"[39] precedentemente, e che la stessa ha attentamente raggruppato in modelli, formulando tutte le possibili diagnosi potenzialmente adattabili alla specificità del caso concreto, in termini di "raccomandazioni". Il sistema procederà, poi, ad una prima scrematura: per mezzo di *scoring algorithms*, accorda a ciascuna ipotesi un grado di plausibilità, eliminando quelle che non raggiungono un certo coefficiente prestabilito. Superata questa fase, le ipotesi diagnostiche che ancora possono essere tenute in considerazione vengono affiancate da materiale specifico deducibile a loro sostegno, che il sistema ricava dalla propria "memoria"; più precisamente, l'ipotesi alla quale viene associata il più alto

---

artificiale. Progettazione dell'algoritmo. Dati e machine learning. Neural network. Deep learning, Hoepli, Milano, 2020, pp. 149-153. Jori A., *Principi di roboetica. Filosofia pratica e Intelligenza Artificiale*, Nuova Ipsa, Palermo, 2019.

37. Per ulteriori approfondimenti sul tema, si rimanda alle seguenti letture: Di Nucci E., Tupasela A., *Concordance as evidence in the Watson for Oncology decisiom-support system*, in *Ai and Society*, 2020, pp. 811-818; Yu Z., Wang Z., Ren X., Lou D., Li X., Liu H., Zhang X., *Practical exploration and research of Watson for Oncology clinical decision support system in real world and localized practise*, in *Journal of Clinical Oncology - An American Society of Clinical Oncology Journal*, vol. 37, n. 15, 2019, pp. 115 ss.; Somashekhar S.P., Sepúlveda M.-J., Puglielli S., Norden A.D., Shortliffe E. H., Rohit Kumar C., Rauthan A., Arun Kumar N., Patil P., Rhee K., Ramya Y., *Watson for oncology and breast cancer treatment reccomendations: Agreement with an expert multidisciplinary tumor board*, in *Annals of Oncology*, n. 29, 2018, pp. 418-423;

38. Ferrucci D., Brown E., Chu-Carroll J., Fan J., Gondek D., Kalyanpur A.A., Lally A., Murdock J.W., Nyberg E., Prager J., Schlaefer, N., Welty D., *The AI Behind Watson - The Technical Article. Building Watson: An Overview of the DeepQA Project*, in *AI Magazine Fall*, 2010.

39. Ossia a casi repertoriati di cancro, ad articoli di rinomate riviste inerenti alle neoplasie o, ancora, ad estratti di manuali di medicina inerenti alle questioni tumorali.

grado di probabilità, viene classificata come "*recommended*", mentre, l'ipotesi con un coefficiente comunque considerevole, se esistente, è etichettata come "*for consideration*". Giunto alla individuazione di una diagnosi finale, il sistema suggerisce anche la cura più idonea da adottarsi.

Illustrato, quindi, il funzionamento tanto di un sistema esperto, quanto di una rete neurale, appare ora possibile individuare le differenze che li contraddistinguono: con riferimento ai sistemi esperti, di cui si è trattato nel paragrafo 2.1., la base conoscitiva, data dall'insieme delle leggi scientifiche che regolano una determinata materia, è impartita dai programmatori o dai loro collaboratori[40]; per la rete neurale, invece, il bagaglio cognitivo è formato proprio dal sistema stesso, ricavando le leggi scientifiche che governano una specifica materia direttamente dalla enorme quantità di dati che gli sono assicurati dall'ingegnere informatico o dal *domain expert*[41]. In quest'ultimo aspetto è ravvisabile la somiglianza dei sistemi connessionisti con gli esseri umani: entrambi non solo riescono ad estrarre le leggi ordinatrici dell'apparente confusione della realtà, ma rendono anche tali leggi delle vere e proprie premesse maggiori per i ragionamenti sussuntivi che sono chiamati a svolgere in determinati settori identificati, come può essere, appunto, quello medico-diagnostico[42].

In ultimo, particolare attenzione va posta sul fatto che i sistemi esperti e i sistemi connessionisti addestrati con il metodo d'apprendimento supervisionato, nella risoluzione dei problemi loro sottoposti, non escogitano mai soluzioni innovative, limitandosi, piuttosto, a valersi delle conoscenze

40. Sartor G., Lagioia F., *Le decisioni algoritmiche tra etica e diritto*, in Ruffolo U. (a cura di), *Intelligenza artificiale - Il diritto, i diritti, l'etica,* Giuffrè Francis Lefebvre, Milano, 2020, p. 68.

41. Più precisamente, il loro compito è esclusivamente quello di selezionare accuratamente i materiali, a partire dai quali la macchina dovrà risalire alle leggi scientifiche di settore, cui è preposta.

42. Tradizionalmente, il ragionamento induttivo era quello che riconduceva il particolare al generale, mentre il ragionamento deduttivo, compiendo il passaggio inverso, procedeva dal generale al particolare. Una simile posizione, oramai abbandonata, ha lasciato spazio al criterio discretivo del nesso di consequenzialità, in ragione del quale quando si è in presenza di un risultato assolutamente certo si è dinanzi ad un ragionamento di tipo deduttivo; qualora, invece, si sia al cospetto di un risultato più o meno probabile si dovrà parlare di ragionamento induttivo. La stessa rete neurale di cui si è trattato sinora quando viene applicata alla diagnostica, riconducendo uno specifico quadro clinico ad una o più patologie probabili, ricorre evidentemente alla logica induttiva. Che l'attività di tipo diagnostico sia connaturata ad un ragionamento di tipo induttivo è pacifico, ponendosi le leggi medico-scientifiche come di tipo statistico, i ragionamenti diagnostici non possono che essere induttivi. Sul rilievo che dalla natura probabilistica della loro premessa maggiore discende immancabilmente la natura soltanto probabilistica del relativo nesso di conseguenzialità. Cfr. Carcaterra G., *Presupposti e strumenti della scienza giuridica*, II ediz., Torino, 2012, pp. 171 ss.

umane correnti[43]. Ciò conduce alla conseguenza che il contributo umano si presenta ancora come assolutamente imprescindibile per affrontare quesiti inediti e individuare soluzioni non ancora pensate[44], necessitando, tali sistemi, di continui aggiornamenti, a maggior ragione di fronte a settori in continua evoluzione, come quello medico-diagnostico. È chiaro, quindi, come gravi sui programmatori, ingegneri informatici, *domain expert*, il compito di revisionare opportunamente la base cognitiva: per i sistemi esperti, fornendo loro le inedite leggi scientifiche che sono state appena scoperte; per le reti neurali, dando loro "in pasto" i dati etichettati dai quali siano deducibili le innovative regole diagnostiche. Ciò conduce alla conclusione che, a fronte della evidente utilità pratica di tali sistemi, rappresentata soprattutto dal minor tempo di individuazione della soluzione diagnostica e dal miglior risultato ottenibile[45], si pongono importanti obblighi di controllo e coordinamento del costante aggiornamento e della continua revisione dei sistemi stessi al fine di evitarne la loro – negligente – obsolescenza.

3. Sfide etiche e giuridiche: trasparenza, affidabilità e spiegabilità

I vantaggi nella somministrazione delle cure e nell'assistenza al paziente a tutto tondo dovuti alla progressiva integrazione tra IA e settore sanitario, di

43. Costanza M., *L'AI: de iure condito e de iure condendo*, in Ruffolo U. (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè Francis Lefebvre, Milano, 2020, p. 408.

44. Sartor G., Lagioia F., *Le decisioni algoritmiche tra etica e diritto*, in Ruffolo U. (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè Francis Lefebvre, Milano, 2020, p. 81.

45. A titolo puramente esemplificativo, si citino due esperimenti condotti: un primo test, condotto in India ha riguardato ben 638 casi di metastasi al seno, i quali sono stati sottoposti all'attenzione tanto di un team di oncologi del Manipal Comprehensive Cancer Center di Bengaluru, quanto del sistema Watson for Oncology. Nel 93% dei casi le diagnosi e le prescrizioni teraupetiche sono coincise. Somashekhar S.P., Sepúlveda M.-J., Puglielli S., Norden A. D., Shortliffe E. H., Rohit Kumar C., Rauthan A., Arun Kumar N., Patil P., Rhee K., Ramya Y., *Watson for oncology and breast cancer treatment reccomendations: Agreement with an expert multidisciplinary tumor board*, in *Annals of Oncology*, n. 29, 2018, pp. 419 ss. Un secondo test è stato condotto in Cina e ha avuto ad oggetto 57 casi di tumori di diverso genere, in questo caso a "sfidare" il sistema Watson for Oncology erano un gruppo di oncologi dell'Oncology Department of Beijing Chaoyang Integrative Medicine Emergency Medical Center. Il risultato fu che i pareri combaciavano nel 100% dei casi. Yu Z., Wang Z., Ren X., Lou D., Li X., Liu H., Zhang X., *Practical exploration and research of Watson for Oncology clinical decision support system in real world and localized practise*, in *Journal of Clinical Oncology-An American Society of Clinical Oncology Journal*, vol 37, n. 15, 2019, pp. 115 ss.; Miller A., *The future of health care could be elementary with Watson*, in *CMAJ*, vol. 11, 2013, pp. 185-186.

cui si trattava nei paragrafi precedenti, non si presentano disgiunti da rischi o complessità tecniche, limiti etici e preoccupazioni giuridiche[46].

Il paradigma tecnologico, infatti, si distingue per una notevole opacità, la quale risulta legata in parte alla necessità di mantenere il segreto industriale, ed in parte alla imperscrutabilità del linguaggio computazione di cui il sistema stesso si avvale[47]; ciò, rende, da un lato, in molti casi difficile (se non impossibile) motivare e verificare le decisioni clinico-diagnostiche, e dall'altro lato, complicato l'affidamento incondizionato all'*ouput* del sistema[48].

Ulteriore questione emergente è quella legata alla presenza di eventuali errori o *bias* nel processo decisionale stesso, che compromettono altamente l'affidabilità del sistema. I sistemi di IA, soprattutto quelli maggiormente sofisticati del calibro del *machine learning* o delle reti neurali profonde, apprendono sulla base di grandi *set* di dati che vengono loro forniti durante l'addestramento. Se tali dati di addestramento sono affetti da distorsioni o pregiudizi, che possono derivare da scelte metodologiche durante l'elaborazione dei dati o, ancora, dalla presenza di "naturali" disuguaglianze nella società, si parla appunto di *bias*[49]*,* che possono condurre ad errori nei risultati forniti in termini di previsioni e/o classificazioni.

A questo si aggiunge anche il rischio di un possibile disequilibrio tra la decisione del medico ed il sistema di IA; laddove il primo, appoggiandosi troppo al sistema stesso riduca l'attenzione necessaria, non fa altro che ab-

46. Al proposito, per una panoramica, si veda: Palazzani L., *AI and health: ethical aspects for regulation*, in *Teoria e critica della Regolazione Sociale*, 1, 2021, pp. 1-16; Schoenberger D., *Artificial Intelligence in healthcare: a critical analysis of the legal and ethical implications*, in *International Journal of Law and Information Technology*, 27, 2018, pp. 171-203.

47. De Menech C., *Intelligenza artificiale e autodeterminazione in materia sanitaria,* in *BioLaw Journal-Ruvista di BioDiritto*, 1, 2022, p. 185.

48. Cfr. Lo Sapio G., *La black-box: l'esplicabilità delle scelte algoritmiche quale garanzia di buona amministrazione*, in *Federalismi.it*, 16, 2021; Smith H., *Clinical AI: opacity, accountability, responsability and liability*, in *AI&Society*, 36, 2021, 535-545.

49. Ad esempio proprio in ambito sanitario interessante è lo studio condotto da Obermeyer ed altri studiosi in: Obermeyer Z. et al., *Analisi dei pregiudizi razziali in un algoritmo utilizzato per gestire la salute della popolazione*, in *Scienza*, 2019. In particolare, degli algoritmi di previsione utilizzati negli Stati Uniti per l'individuazione di pazienti con esigenze sanitarie complesse ha mostrato una specifica tendenza: i sintomi dei pazienti di colore, nonostante avessero problemi di salute maggiori, se comparati con i pazienti bianchi, venivano spesso trascurati. Si trattava proprio di un errore di progettazione dell'algoritmo: lo stesso era stato addestrato sulla base dei dati riguardanti i costi sanitari passati come indicatori dei costi futuri. Dal momento che i pazienti di colore, anche a causa di fattori storici e socioeconomici, tendono ad avere costi sanitari inferiori, l'algoritmo interpretava erroneamente tale fatto come segno di minore bisogno sanitario. Cfr. Stradella E., *Stereotipi e discriminazioni: dall'intelligenza umana all'intelligenza artificiale*, in *Liber Amicorum per Pasquale Costanzo*, 2020.

bassare il livello di competenza richiesta con conseguente "responsabilizzazione", in termini operativi, del sistema programmato secondo l'intelligenza artificiale (cd. *deskilling*)[50].

Infine, di non trascurabile rilevanza è l'aspetto della tutela del trattamento dei dati personali: tali sistemi necessitano di importantissime quantità di dati per poter essere massimamente efficienti ed efficaci e, per di più, si tratta di specifiche categorie di dati, anche sensibili, che abbisognano di iter di raccolta, elaborazione e conservazione molto complessi, che rischiano di violare la disciplina in materia.

In questo scenario, l'adozione di regole precise e trasparenti è di fondamentale importanza, anche e soprattutto, per accrescere la fiducia nei cittadini rispetto alle nuove tecnologie, a maggior ragione nell'ambito della cura della salute ove, lo si ribadisca, vengono coinvolti beni essenziali come la salute e la vita[51]. Inoltre, come già accennato, trattandosi di sistemi sofisticati si costruiscono sulla premessa teorica di una autonomia ed imprevedibilità intrinseche del loro funzionamento, le quali rendono parzialmente oscuri i processi interni di elaborazione delle decisioni, tale per cui gli *output* non solo non sono determinabili *ex ante*, ma non sono nemmeno ricostruibili *ex post*[52]. È chiaro come ciò sia direttamente funzionale a ledere gravemente il diritto del paziente ad ottenere la spiegazione delle decisioni del sistema di IA adoperato[53].

---

50. Chen Y. Et al., *Professionals' responses to the introduction of AI innovations in radiology and their implications for future adoption: a qualitative study*, in *BMC Health Services Research*, 21, 2021.

51. Regolamento UE 2024/1689, Considerando 47: «(…) nel settore sanitario, in cui la posta in gioco per la vita e la salute è particolarmente elevata, è opportuno che i sistemi diagnostici e i sistemi di sostegno delle decisioni dell'uomo, sempre più sofisticati, siano affidabili e accurati». Non va dimenticato che nell'ambito sanitario i fattori di vulnerabilità e di rischio sono certamente acuiti, in particolare, con riferimento alla stretta relazione di cura e fiducia tra medico e paziente. Daverio M., Macioce F., *Intelligenza artificiale e diritto alla salute nella regolazione europea: aspetti emergenti al riguardo alla relazione medico-paziente*, in *Teoria e Critica della Regolazione Sociale*, 1, 2023, p. 2.

52. Casonato C., Marchetti B., *Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale*, in *BioLaw-Rivista di BioDiritto*, 3, 2021, pp. 415-437.

53. Per ultimo, Regolamento UE 1689/2024, Considerando 171: «Le persone interessate dovrebbero avere il diritto di ottenere una spiegazione qualora la decisione di un deployer si basi principalmente sugli output di determinati sistemi di IA ad alto rischio che rientrano nell'ambito di applicazione del presente regolamento e qualora tale decisione produca effetti giuridici o in modo analogo incida significativamente su tali persone in un modo che esse ritengano avere un impatto negativo sulla loro salute, sicurezza o sui loro diritti fondamentali. Tale spiegazione dovrebbe essere chiara e significativa e fornire una base su cui le persone interessate possano esercitare i loro diritti. Il diritto di ottenere una spiegazione non dovrebbe applicarsi all'uso di sistemi di IA per i quali il diritto dell'Unione o nazionale prevede

Per queste ragioni l'UE ha deciso di adottare un approccio aperto e flessibile, in ragione del quale la disciplina e regolamentazione giuridica di tali sistemi non si realizza a partire dalle caratteristiche tecniche dell'IA o dagli effetti che la stessa è in grado di produrre; bensì, si struttura sulla base dei rischi che sono collegati all'utilizzo di simili tecnologie, articolando i diversi sistemi in tre categorie: sistemi a rischio inaccettabile, sistemi ad alto rischio e sistemi a basso rischio, di cui si dirà meglio in seguito.

4. Strumenti normativi a supporto dell'IA nell'ambito sanitario

Di fronte alle sfide che l'interazione dei sistemi programmati secondo l'intelligenza artificiale con il settore sanitario pone, diversi sono gli strumenti che l'UE ha elaborato negli ultimi anni al fine di supportarne l'utilizzo eticamente e giuridicamente corretto.

Nella consapevolezza che il *file rouge* che deve condurre alla definizione di un perimetro normativo e disciplinare relativo ai dispositivi medici di intelligenza artificiale deve essere quello della sicurezza dei pazienti, è innanzitutto necessario valutare se delle norme settoriali basate su un approccio di rischio possano meglio riconoscere le peculiarità del settore, consentendo di stabilire requisiti specifici per garantire che le applicazioni dell'IA nell'ambito sanitario siano sicure ed efficaci, ma favorendo al contempo l'innovazione.

A livello europeo, anteriormente all'intervento del Regolamento UE 1689/2024, i principi per una possibile disciplina dei sistemi di intelligenza artificiale per uso sanitario venivano individuati nella Risoluzione del Parlamento Europeo del 16 febbraio 2017 recante raccomandazioni concernenti norme di diritto civile sulla robotica. Questo intervento riguardava principalmente la responsabilità per danni prodotti dai robot, individuando, altresì, due principi fondamentali da rispettare nell'utilizzo di sistemi robotici in ambito socio-sanitario: l'impiego delle tecnologie nei servizi di cura non deve in alcun modo disumanizzare le pratiche di accudimento sostituendosi al contatto umano; inoltre, deve essere rispettato il principio dell'autonomia supervisionata del sistema intelligente impiegato, che implica che sia sempre il medico a prendere la decisione finale in termini di cura ed esecuzione della stessa[54].

---

eccezioni o restrizioni e dovrebbe applicarsi solo nella misura in cui tale diritto non sia già previsto dal diritto dell'Unione».

54. Ferioli E. A., *L'intelligenza artificiale nei servizi sociali e sanitari: una nuova sfida*

Oltre a ciò, il quadro normativo appariva molto frammentato, ed in materia trovava applicazione anche: la normativa europea sui dispositivi medici[55], la disciplina europea sull'identificazione elettronica[56], la disciplina sulla sicurezza di reti e sistemi informativi[57], nonché ovviamente la disciplina sulla protezione dei dati personali[58].

Nell'aprile 2021 la Commissione europea ha presentato la proposta per l'adozione di un Regolamento contenente regole per l'armonizzazione della disciplina sull'intelligenza artificiale, con l'obiettivo di promuovere uno sviluppo etico dell'IA, in linea con i valori fondamentali dell'UE, ed in grado di garantire alla stessa il ruolo di leader nel panorama dello sviluppo tecnico scientifico mondiale, rafforzando, di conseguenza, anche la fiducia dei cittadini verso le nuove tecnologie[59]. Il 12 giugno 2024 viene così pubblicato nella Gazzetta Ufficiale dell'Unione Europea il testo definitivo dell'*Artificial Intelligence Act (AI ACT)*, il quale si propone di dar vita ad un nuovo quadro normativo completo e puntuale, capace di far fronte alle diverse problematiche ed alle necessità correlate allo sviluppo dell'intelligenza artificiale, con l'aspirazione di favorire un utilizzo responsabile ed etico delle nuove tecnologie e con l'obiettivo dichiarato di: «[…] migliorare il funzionamento del mercato interno e promuovere la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea, compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, contro gli effetti nocivi dei sistemi di IA nell'Unione, e promuovendo l'innovazione»[60].

4.1. L'IA ed i sistemi medico-diagnostici alla luce del Regolamento UE 1689/2024

Il primo passo da compiersi per affrontare un'approfondita analisi dell'AI Act è quello di individuare il suo ambito di applicazione. Privilegiando un

al ruolo delle istituzioni pubbliche nel welfare italiano?, in "BioLaw Journal – Rivista di BioDiritto", n. 1/2019, pp. 163-175.

55. Regolamento UE 2017/746 sui dispositivi medico-diagnostici in vitro ("IVDR").

56. Regolamento UE 910/2014; integrato di recente dal Regolamento UE 2024/1183 che istituisce il quadro europeo per l'identità digitale.

57. Direttiva NIS 2016/1148, sulla sicurezza delle reti e dei sistemi informativi.

58. Regolamento 2016/679 – GDPR.

59. Commissione europea, *Proposta di Regolamento del Parlamento europeo e del Consiglio che stabilisce regole di armonizzazione sull'intelligenza artificiale*, p. 1.

60. Art. 1 AI ACT.

approccio il più omnicomprensivo possibile, al fine di evitare una possibile obsolescenza normativa nel breve termine[61], il legislatore ha, innanzitutto, scelto di fornire una definizione di «sistema di IA», ove per tale si intende: «un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali»[62]. Una definizione che si articola in sette elementi chiave:

1. *Sistema basato su macchina*. Un sistema di IA deve essere implementato e operare su macchine, includendo tanto componenti *hardware*, quanto componenti *software*.
2. *Autonomia.* Il sistema deve essere progettato per operare con un certo grado di autonomia e indipendenza rispetto alla possibilità di intervento umano. Ciò significa che il sistema è in grado di produrre *output* senza necessità di una interazione umana.
3. *Adattabilità.* In seguito alla sua implementazione il sistema può esibire la capacità di modificare il proprio comportamento sulla base dell'esperienza acquisita.
4. *Obiettivi*. Il sistema di IA opera per obiettivi impliciti o espliciti, ove i primi possono essere dedotti direttamente dal comportamento del sistema, mentre i secondi sono individuati in modo chiaro e preciso dal programmatore.
5. *Inferenza.* Un sistema di IA deve essere capace di svolgere un'attività inferenziale a partire dagli *input* che riceve, generando *output*[63].

---

61. Cfr. Ruschemeier, H., *AI as a challenge for legal regulation – the scope of application of the artificial intelligence act proposal*, in *ERA Forum*, 2023; Bobev, T., *Defining AI in the AI Act: Pin the Tail on the System*, reperibile al link: *https://www.law.kuleuven.be/citip/blog/defining-ai-in-the-ai-act-pin-the-tail-on-the-system/.*

62. Art. 3, par. 1, n. 1 AI Act. Si precisi, al proposito, che proprio per far fronte alla rapida evoluzione tecnologica, l'art. 112, n. 1, dell' AI Act prevede la possibilità di modificare e/o aggiornare l'elenco degli utilizzi vietati: «La Commissione valuta la necessità di modificare l'elenco stabilito nell'allegato III e l'elenco di pratiche di IA vietate di cui all'articolo 5 una volta all'anno dopo l'entrata in vigore del presente regolamento e fino al termine del periodo della delega di potere di cui all'articolo 97. La Commissione trasmette i risultati della valutazione al Parlamento europeo e al Consiglio».

63. La capacità inferenziale è un elemento cruciale nella distinzione dei sistemi di IA dai software tradizionali. Tale capacità si basa su tecniche di IA come l'apprendimento automatico o gli approcci logico-simbolici, che conferiscono al sistema l'attitudine di generare output quali previsioni, contenuti o raccomandazioni incidenti sulla realtà fisica (o anche virtuale), dimostrando grande adattabilità e autonomia; mentre, i *software* tradizionali seguo-

6. *Output*. I sistemi di IA generano output quali previsioni, contenuti, raccomandazioni o decisioni capaci di influenzare l'ambiente reale o virtuale circostante.
7. *Capacità di influenzare ambienti fisici o virtuali*. Tale capacità evidenzia il ruolo attivo del sistema di IA sull'ambiente in cui opera, potendo produrre, con i suoi *output*, conseguenze tangibili o digitali.

Si noti che non è necessario che tutti questi sette elementi siano presenti contemporaneamente affinché si parli di sistema di IA ai sensi della definizione dell'AI Act: a tal fine, difatti, è sufficiente che il sistema si basi su macchine e che sia in grado di esibire la capacità inferenziale.

Dopodiché, sempre con l'obiettivo di una precisa identificazione del perimetro di applicabilità del Regolamento, funzionale a garantire una diffusa applicazione dell'intelligenza artificiale ed un corretto grado di tutela delle persone dell'Unione Europea, conformemente a quanto già compiuto con riferimento al Regolamento UE 679/2016 (GDPR), è apparso utile svincolare l'ambito di applicazione territoriale dell'AI Act dal luogo in cui si trovano i fornitori dei sistemi. L'art. 2 dell'AI Act, precisa, infatti, che il Regolamento si applica: "a) ai fornitori che immettono sul mercato o mettono in servizio sistemi di IA o immettono sul mercato modelli di IA per finalità generali nell'Unione, indipendentemente dal fatto che siano stabiliti o ubicati nell'Unione o in un paese terzo; b) ai *deployer* dei sistemi di IA che hanno il loro luogo di stabilimento o sono situati all'interno dell'Unione; c) ai fornitori e ai *deployer* di sistemi di IA che hanno il loro luogo di stabilimento o sono situati in un paese terzo, laddove l'output prodotto dal sistema di IA sia utilizzato nell'Unione; d) agli importatori e ai distributori di sistemi di IA; e) ai fabbricanti di prodotti che immettono sul mercato o mettono in servizio un sistema di IA insieme al loro prodotto e con il loro nome o marchio; f) ai rappresentanti autorizzati di fornitori, non stabiliti nell'Unione; g) alle persone interessate che si trovano nell'Unione (…)»[64].

---

no regole definite, limitandosi ad eseguire, in modo automatico, delle operazioni prestabile, dimostrandosi privi della capacità di apprendere e adattare il proprio comportamento in modo indipendente. Per fare un esempio concreto, si pensi ad esempio ad un sistema di diagnostica medica: il sistema di IA potrebbe analizzare immagini e dati clinici al fine di suggerire delle possibili diagnosi, individuando anche quella più probabile; il *software* tradizionale potrebbe semplicemente fornire delle letture in termini statistici, o dei risultati precalcolati.

64. Art. 2, par. 1, AI Act. Con riferimento al presente articolo è, inoltre, fondamentale precisare che ai sensi dell'art. 3, n. 3 dell'AI Act, per «fornitore» si intende: «una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che sviluppa un sistema di IA o un modello di IA per finalità generali o che fa sviluppare un sistema di IA o un modello di IA per finalità generali e immette tale sistema o modello sul mercato o mette

Le previsioni di cui alla lettera a) ove si può leggere che il Regolamento in analisi è applicabile ai fornitori indipendentemente dal fatto che siano stabiliti o ubicati nell'Unione o in un paese terzo, nonché alla lettera c) ove si trova precisato che lo stesso avviene anche a favore dei fornitori e dei *deployer* che hanno il loro luogo di stabilimento o sono situati in un paese terzo, ma anche alla lettera f) ove si fa riferimento ai rappresentanti autorizzati di fornitori che non siano stabiliti nell'Unione, esplicitano a chiare lettere la volontà del legislatore unionale di regolare anche l'attività di soggetti non europei, essendo ardua, unicamente in ragione delle sue caratteristiche distintive e identificative, una delimitazione geografica dell'utilizzo dell'IA[65].

Un ulteriore passo da effettuarsi è porre l'attenzione sulle modalità di costruzione della regolamentazione di riferimento: si tratta di una normativa *in primis* di carattere orizzontale, ossia strutturata in maniera tale da essere

---

in servizio il sistema di IA con il proprio nome o marchio, a titolo oneroso o gratuito». Ai sensi dell'art. 3, n. 9 dell'AI Act, per «immissione sul mercato» si intende: «la prima messa a disposizione di un sistema di IA o di un modello di IA per finalità generali sul mercato dell'Unione». Ai sensi dell'art. 3, n. 11 dell'AI Act, per «messa in servizio» si intende: «la fornitura di un sistema di IA direttamente al deployer per il primo uso o per uso proprio nell'Unione per la finalità prevista». Ai sensi dell'art. 3, n. 4 per «deployer» si intende: «una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che utilizza un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale». Ai sensi dell'art. 3, n. 5 dell'AI Act, per «rappresentante autorizzato» si intende: «una persona fisica o giuridica ubicata o stabilita nell'Unione che ha ricevuto e accettato un mandato scritto da un fornitore di un sistema di IA o di un modello di IA per finalità generali al fine, rispettivamente, di adempiere ed eseguire per suo conto gli obblighi e le procedure stabiliti dal presente regolamento». Ai sensi dell'art. 3, n. 6 dell'AI Act, per «importatore» si intende: «una persona fisica o giuridica ubicata o stabilita nell'Unione che immette sul mercato un sistema di IA recante il nome o il marchio di una persona fisica o giuridica stabilita in un paese terzo». Ai sensi dell'art. 3, n. 7 dell'AI Act, per «distributore» si intende: «una persona fisica o giuridica nella catena di approvvigionamento, diversa dal fornitore o dall'importatore, che mette a disposizione un sistema di IA sul mercato dell'Unione».

65. Ciò, perfettamente in linea anche con il Considerando 22 il quale afferma: «Alla luce della loro natura di sistemi digitali, è opportuno che determinati sistemi di IA rientrino nell'ambito di applicazione del presente regolamento anche quando non sono immessi sul mercato, né messi in servizio, né utilizzati nell'Unione. È il caso, ad esempio, di un operatore stabilito nell'Unione che appalta alcuni servizi a un operatore stabilito in un paese terzo in relazione a un'attività che deve essere svolta da un sistema di IA che sarebbe classificato ad alto rischio. In tali circostanze il sistema di IA utilizzato dall'operatore in un paese terzo potrebbe trattare dati raccolti nell'Unione e da lì trasferiti nel rispetto della legge, e fornire all'operatore appaltante nell'Unione l'output di tale sistema di IA risultante da tale trattamento, senza che tale sistema di IA sia immesso sul mercato, messo in servizio o utilizzato nell'Unione. Al fine di impedire l'elusione del presente regolamento e di garantire una protezione efficace delle persone fisiche che si trovano nell'Unione, è opportuno che il presente regolamento si applichi anche ai fornitori e ai deployer di sistemi di IA stabiliti in un paese terzo, nella misura in cui l'output prodotto da tali sistemi è destinato a essere utilizzato nell'Unione».

applicabile a tutti i sistemi di IA, a prescindere dal settore in cui gli stessi siano impiegati[66], ed in ragione di ciò non si troverà una disciplina specifica e destinata solo alla regolamentazione dei sistemi medici di IA, ma la stessa apparirà, per certi versi, diffusa e frammentata all'interno del Regolamento; e, *in secundis* si tratta di una normativa "a strati", vale a dire che impone obblighi differenziati in base al livello di rischio attribuito ai diversi sistemi di IA, ove per «rischio» si intende «la combinazione della probabilità del verificarsi di un danno e la gravità del danno stesso»[67]. Viene così a delinearsi un sistema flessibile ed allo stesso tempo robusto, introduttivo di principi di portata generale, denotato da norme proporzionate ed efficaci, che intervengono limitatamente a situazioni portatici di un rischio concreto, e capaci di contemperare anche i futuri sviluppi dell'intelligenza artificiale[68].

Pertanto, focalizzandosi brevemente sul settore dell'assistenza sanitaria in senso ampio, sin da ora preme solo precisare che il legislatore al Considerando 4 cita tale ambito come un campo sul quale l'IA, quale famiglia di tecnologie in rapida evoluzione, potrebbe garantire una vasta gamma di benefici a livello economico, ambientale e sociale[69]. Ad integrazione di ciò, al Considerando 58 viene, tuttavia, sottolineato come i sistemi di IA applicati ai settori come quello dell'accesso ad alcuni servizi e prestazioni essenziali, pubblici o privati, necessari affinché le persone possano partecipare pienamente alla vita sociale o migliorare il proprio tenore di vita, nonché i sistemi utilizzati per la valutazione dei rischi e la determinazione dei prezzi

66. Mandarà, E., *Il Regolamento UE sull'intelligenza artificiale*, in (a cura di Iaselli M.) *AI ACT. Principi, regole ed applicazioni pratiche del Reg. UE 1689/2024*, Maggioli, Santarcangelo di Romagna, 2024, p. 57.

67. Art. 3, n. 2, AI Act.

68. Mandarà, E., *Il Regolamento UE sull'intelligenza artificiale*, in (a cura di Iaselli M.) *AI ACT. Principi, regole ed applicazioni pratiche del Reg. UE 1689/2024*, Maggioli, Santarcangelo di Romagna, 2024, p. 57; Nikolinakos, N.T., *EU Policy and Legal Framework for Artificial Intelligence, Robotics and Related Tachnologies – the AI Act in Law, Governance and Technology*, Spinger, 2023, pp. 336-337.

69. Considerando 4, AI Act: «L'IA consiste in una famiglia di tecnologie in rapida evoluzione che contribuisce al conseguimento di un'ampia gamma di benefici a livello economico, ambientale e sociale nell'intero spettro delle attività industriali e sociali. L'uso dell'IA, garantendo un miglioramento delle previsioni, l'ottimizzazione delle operazioni e dell'assegnazione delle risorse e la personalizzazione delle soluzioni digitali disponibili per i singoli e le organizzazioni, può fornire vantaggi competitivi fondamentali alle imprese e condurre a risultati vantaggiosi sul piano sociale e ambientale, ad esempio in materia di assistenza sanitaria, agricoltura, sicurezza alimentare, istruzione e formazione, media, sport, cultura, gestione delle infrastrutture, energia, trasporti e logistica, servizi pubblici, sicurezza, giustizia, efficienza dal punto di vista energetico e delle risorse, monitoraggio ambientale, conservazione e ripristino della biodiversità e degli ecosistemi, mitigazione dei cambiamenti climatici e adattamento ad essi».

per assicurazioni sulla vita o sanitarie, ed anche i sistemi utilizzati per la classificazione delle chiamate di emergenza o per la selezione dei pazienti, serbando intrinsecamente il rischio di gravi discriminazioni e lesioni dei diritti fondamentali, abbisognano di essere trattati con grande attenzione.

Per questo motivo, per quanto attiene alla specifica disciplina dei sistemi medici di IA, la stessa sarà analizzata ai paragrafi successivi in considerazione degli approfondimenti che si effettueranno per ciascuna categoria di rischio.

4.1.1. Sistemi di IA a rischio inaccettabile

La prima categoria di sistemi individuata dall'AI Act è quella dei sistemi a rischio "inaccettabile". L'art. 5, rubricato «Pratiche di IA vietate», individua un elenco di intelligenze artificiali vietate in ragione del loro impatto sui diritti fondamentali e sulle libertà delle persone, nonché in ragione della loro contrarierà rispetto ai principi cardine dell'UE quali la dignità umana, l'uguaglianza e la democrazia. Tale divieto è supportato da due cardini normativi: l'articolo 16 del Trattato sul Funzionamento dell'Unione Europea, che funge da base giuridica per le norme specifiche sul trattamento dei dati personali in relazione al divieto di utilizzare sistemi di identificazione biometrica a distanza a fini di contrasto, sistemi di categorizzazione biometrica a fini di contrasto e valutazioni del rischio individuale a fini di contrasto; e l'articolo 114 del Trattato sul Funzionamento dell'Unione Europea, il quale funge da base giuridica per tutti gli altri divieti[70].

Più precisamente, a titolo riassuntivo, è vietata l'immissione sul mercato, messa in servizio o l'uso:

1. di sistemi di IA che utilizzano tecniche subliminali o che sfruttino la vulnerabilità di una persona, o di un gruppo di persone capaci di distorcere il comportamento delle stesse, pregiudicandone la capacità di assumere delle decisioni consapevoli tanto da provocare loro un danno significativo[71];

---

70. Communication to the Commission Approval of the content of the draft Communication from the Commission - *Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), C(2025) 884 final, 04.02.2025, Bruxelles.*

71. Per approfondimenti si rimenda a: Bermudez J. P., Nyrup R., Deterding S., Mougenot C., Moradbakhti L., You F., Calvo R. A., *The AI Act needs a practical definition of 'subliminal techniques'*, 2023, reperibile al link: *https://www.euractiv.com/section/artificial-intelligence/*

2. di sistemi di IA per la valutazione o la classificazione di persone sulla base del loro comportamento sociale, delle loro caratteristiche personali o della loro personalità;
3. di sistemi di polizia predittiva, quindi per valutare o prevedere il rischio di compimento di un reato da parte di una persona fisica, basandosi esclusivamente sulle sue caratteristiche personali; ad esclusione dei casi in cui tali sistemi siano utilizzati a supporto e conferma di una valutazione già effettuata da un operatore umano;
4. di sistemi che introducano la pratica dello *scraping* di immagini facciali da internet o da sistemi di videosorveglianza, ciò al fine di evitare la crescita del fenomeno della sorveglianza di massa con conseguente violazione dei diritti fondamentali;
5. di sistemi di riconoscimento delle emozioni delle persone in relazione ai loro dati biometrici. Tale divieto opera solo con riferimento a sistemi impiegati in ambienti e contesti specifici, in cui emerga la particolare vulnerabilità dei soggetti coinvolti; e viene escluso quando tale tipologia di sistemi venga utilizzato per motivi medici o di sicurezza;
6. di sistemi di IA per il riconoscimento biometrico in tempo reale, ossia di quei sistemi adoperati nella ricerca di potenziali vittime di reato o di persone scomparse, nella prevenzione di una minaccia specifica per la vita delle persone, nella identificazione e localizzazione di potenziali autori di reati; sempreché il loro utilizzo non sia autorizzato dall'autorità giudiziaria o amministrativa competente tenendo conto della natura della situazione concreta ed avendo riguardo della gravità, dell'entità e della probabilità del danno che verrebbe causato in difetto del ricorso al sistema di IA;
7. di sistemi di categorizzazione biometrica, ovvero sistemi che utilizzano i dati biometrici delle persone fisiche al fine di assegnarle a categorie specifiche, che possono riguardare aspetti quali il sesso, l'età, il colore degli occhi o dei capelli, i tratti della personalità, la lingua, la religione, l'orientamento sessuale o politico. L'immissione di questi sistemi è vietata qualora sia finalizzata a classificare le persone fisiche per effettuare deduzioni o inferenze con riferimento alle peculiarità personali di cui prima; in tutti gli altri casi, simili sistemi sono identificati come sistemi ad alto rischio.

---

opinion/the-ai-act-needs-a-practical-definition-of-subliminal-techniques/; Bermudez J. P., Nyrup R., Deterding S., Mougenot C., Moradbakhti L., You F., Calvo R.A., *What Is a Subliminal Technique? An Ethical Perspective on AI-Driven Influence*, 2023, reperibile al link: *https://philarchive.org/rec/BERWIA-9*; Casaburo D., Guliotta L., *The EU AI Act proposal(s): Manipulative and exploitative AI practices*, 2023, reperibile al link: *https://www.law.kuleuven.be/citip/blog/the-eu-ai-act-proposals-manipulative-and-exploitative-ai-practices/.*

A regolare minuziosamente la categoria dei sistemi di IA vietati è intervenuta di recente la Commissione Europea la quale ha pubblicato il "*Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act)",* ossia delle linee guida, concepite per garantire un'applicazione coerente, efficace e uniforme dell'AI Act in tutta l'Unione europea, che offrono preziose indicazioni sull'interpretazione dei divieti da parte della Commissione, fornendo spiegazioni giuridiche ed esempi pratici per aiutare le parti interessate a comprendere e rispettare i requisiti della legge sull'IA.

Calando la disciplina generale al caso concreto dei dispositivi medici programmati secondo l'intelligenza artificiale, presi in considerazione nella trattazione in esame, si consideri, ad esempio, un dispositivo programmato secondo l'IA utilizzato nella riabilitazione dei pazienti portatori di una disabilità fisica, il quale esibisca la capacità di interpretare ed adattarsi alle esigenze dell'utente. In tali circostanze, potrebbe, ad esempio, residuare il pericolo che il sistema interpreti in maniera distorta il desiderio di miglioramento del suo utilizzatore, spingendolo ad intensificare eccessivamente gli esercizi e giungendo a provocare infortuni o complicazioni di vario genere. Risulta, difatti, evidente che le persone in contesti sanitari, siano essi pazienti o soggetti partecipanti ad un *trial* clinico, versano in condizioni di vulnerabilità (più o meno accentuata), ed il loro comportamento può essere più facilmente condizionato e distorto proprio in ragione di tale posizione da loro ricoperta.

O ancora, si pensi ad un sistema di *social scoring*, utilizzato per determinare l'accesso a determinati servizi sanitari, il quale si porrebbe, residuando un alto rischio che i risultati forniti dal sistema potrebbero essere non corretti o comunque viziati da *bias*, come evidentemente in violazione del diritto alla dignità e alla non discriminazione, nonché ai valori di uguaglianza e giustizia.

È opportuno chiarire che, conformemente alle neo introdotte Linee Guida ed in accordo con il Considerando 29 dell'AI Act, i divieti posti rispetto ai sistemi di IA destinati a compiere pratiche manipolative o di sfruttamento della vulnerabilità non pregiudicano il loro utilizzo in modo lecito e costruttivo; come, ad esempio, nel caso in cui le tecniche subliminali abilitate dall'intelligenza artificiale siano utilizzate per il trattamento psicologico di una malattia mentale o per la riabilitazione fisica, in conformità alla legge e agli standard medici applicabili[72].

72. Communication to the Commission Approval of the content of the draft

Allo stesso modo, il divieto di cui all'articolo 5, paragrafo 1, lettera f), della legge sull'IA contiene, come si anticipava poc'anzi, un'eccezione esplicita per i sistemi di riconoscimento delle emozioni utilizzati nell'ambito dei luoghi di lavoro e degli istituti di istruzione per ragioni mediche o di sicurezza, come ad esempio i sistemi per uso terapeutico. Alla luce dell'obiettivo del Regolamento 1689/2024 di garantire un elevato livello di protezione dei diritti fondamentali, questa eccezione dovrebbe essere interpretata in modo restrittivo. Non a caso, la stessa non comprende l'uso di sistemi di riconoscimento delle emozioni per rilevare aspetti generali di benessere, come il monitoraggio generale dei livelli di stress sul posto di lavoro; piuttosto, il riconoscimento delle emozioni può essere utilizzato per ragioni mediche per assistere dipendenti o studenti affetti da autismo e migliorare l'accessibilità per le persone non vedenti o sorde[73].

In conclusione, si ribadisca che tali Linee Guida, sforzandosi di interpretare i divieti in modo proporzionato per raggiungere gli obiettivi dell'AI Act di proteggere i diritti fondamentali e la sicurezza, mirano ad aumentare la chiarezza giuridica e a fornire indicazioni sull'interpretazione della Commissione dei divieti di cui all'articolo 5 dell'AI Act, servendo da bussola pratica per assistere le autorità competenti nelle loro attività di applicazione, nonché i fornitori, i *deployer* e gli implementatori di sistemi di IA nel garantire il rispetto dei loro obblighi ai sensi dell'AI Act. In aggiunta, non si tratta di Linee Guida vincolanti, difatti, qualsiasi interpretazione autorevole dell'AI Act potrà essere data, in ultima analisi, solo dalla Corte di giustizia dell'Unione europea[74].

4.1.2. Sistemi di IA ad alto rischio e loro classificazione

La seconda categoria, quella identificata dai sistemi di IA "ad alto rischio", risulta quella con maggior rilevanza, in quanto dalla stessa derivano importanti obblighi a carico di diversi ordini di soggetti.

Communication from the Commission - *Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act),* C(2025) 884 final, 04.02.2025, Bruxelles, pp. 50 ss.

73. Communication to the Commission Approval of the content of the draft Communication from the Commission - *Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act),* C(2025) 884 final, 04.02.2025, Bruxelles, pp. 93 ss.

74. Communication to the Commission Approval of the content of the draft Communication from the Commission - *Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act),* C(2025) 884 final, 04.02.2025, Bruxelles, pp. 1-2.

L'art. 6 dell'AI Act distingue due diverse categorie: la prima categoria comprende tutti i sistemi di IA che soddisfino entrambe le seguenti condizioni: « a) il sistema di IA è destinato a essere utilizzato come componente di sicurezza di un prodotto, o il sistema di IA è esso stesso un prodotto, disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'allegato I; b) il prodotto, il cui componente di sicurezza a norma della lettera a) è il sistema di IA, o il sistema di IA stesso in quanto prodotto, è soggetto a una valutazione della conformità da parte di terzi ai fini dell'immissione sul mercato o della messa in servizio di tale prodotto ai sensi della normativa di armonizzazione dell'Unione elencata nell'allegato I». In altre parole, sono da considerarsi ad alto rischio, i sistemi di IA che sono componenti di sicurezza di un prodotto, o un prodotto stesso disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'allegato I, ossia, a titolo esemplificativo i regolamenti UE 2017/745 e 2017/746 relativi, rispettivamente, ai dispositivi medici ed ai dispositivi medico-diagnostici in vitro[75], nonché il regolamento (UE) 2016/425 sui dispositivi di protezione individuale[76] ed anche il regolamento UE 2023/1230 cd "Regolamento Macchine", e così via.

La seconda categoria, invece, ricomprende tutti i sistemi di IA inclusi nell'allegato III. Quest'ultima elencazione si fonda sul settore di utilizzo, e ricomprende ad esempio quello dell'istruzione e della formazione professionale; quello dell'occupazione, gestione dei lavoratori e accesso al lavoro autonomo; quello dell'accesso a servizi privati essenziali e a prestazioni e servizi pubblici essenziali e fruizione degli stessi; quello della migrazione, asilo e gestione del controllo delle frontiere; quello dell'amministrazione della giustizia ed altri ancora. Anche in questo caso, esemplificando, si possono trovare i sistemi di IA destinati a essere utilizzati dalle autorità pubbliche o per conto di autorità pubbliche per valutare l'ammissibilità delle persone fisiche alle prestazioni e ai servizi di assistenza pubblica essenziali, compresi i servizi di assistenza sanitaria, nonché per concedere, ridurre, revocare o recuperare tali prestazioni e servizi[77]; o ancora, i sistemi di IA

75. Allegato I, Sezione A, nn. 11 e 12: «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, p. 1)»; «regolamento (UE) 2017/746 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medico-diagnostici *in vitro* e che abroga la direttiva 98/79/CE e la decisione 2010/227/UE della Commissione (GU L 117 del 5.5.2017, p. 176)».

76. Allegato I, Sezione A, n. 9: «regolamento (UE) 2016/425 del Parlamento europeo e del Consiglio, del 9 marzo 2016, sui dispositivi di protezione individuale e che abroga la direttiva 89/686/CEE del Consiglio (GU L 81 del 31.3.2016, p. 51)».

77. Allegato III, n. 5, lettera a), AI Act.

destinati a essere utilizzati per determinare l'accesso, l'ammissione o l'assegnazione di persone fisiche agli istituti di istruzione e formazione professionale a tutti i livelli[78]. In deroga a quanto appena descritto, un sistema di IA di cui all'allegato III può non essere considerato ad alto rischio nel caso in cui non presenti un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche, anche nel senso di non influenzare materialmente il risultato del processo decisionale[79].

La disposizione normativa di cui all'art. 6 dell'AI Act procede, poi, elencando una serie di ipotesi nelle quali deve ritenersi che un sistema di IA non presenti un rischio significativo, e che quindi possa qualificarsi come non ad alto rischio: «a) il sistema di IA è destinato a eseguire un compito procedurale limitato; b) il sistema di IA è destinato a migliorare il risultato di un'attività umana precedentemente completata; c) il sistema di IA è destinato a rilevare schemi decisionali o deviazioni da schemi decisionali precedenti e non è finalizzato a sostituire o influenzare la valutazione umana precedentemente completata senza un'adeguata revisione umana; o d) il sistema di IA è destinato a eseguire un compito preparatorio per una valutazione pertinente ai fini dei casi d'uso elencati nell'allegato III»[80].

Resa questa breve panoramica sulla modalità di classificazione dei sistemi di IA ad alto rischio, si passi ad esaminare come vengono qualificati, alla luce delle predette considerazioni, i dispositivi medici programmati secondo l'IA. Sul tema, il Considerando 50 è lapidario, includendo i dispositivi medici e medico-diagnostici in vitro nella categoria dei sistemi ad alto rischio: «Per quanto riguarda i sistemi di IA che sono componenti di sicurezza di prodotti, o che sono essi stessi prodotti, e rientrano nell'ambito di applicazione di una determinata normativa di armonizzazione dell'Unione elencata nell'allegato al presente regolamento, è opportuno classificarli come sistemi ad alto rischio a norma del presente regolamento se il prodotto interessato è sottoposto alla procedura di valutazione della conformità con un organismo terzo di valutazione della conformità a norma della suddetta pertinente normativa di armonizzazione dell'Unione. Tali prodotti sono, in particolare, macchine, giocattoli, ascensori, apparecchi e sistemi di pro-

78. Allegato III, n. 3, lettera a), AI Act.

79. Art. 6, n. 3, AI Act.

80. Art. 6, n. 3, AI Act. In particolare, a norma dell'art. 6, n. 4 dell'AI Act, laddove i fornitori ritengano che il proprio sistema non integri un rischio significativo nel senso descritto dal dettato normativo, dovranno documentare la valutazione del sistema di IA prima che lo stesso sia immesso nel mercato o in servizio; gli stessi saranno comunque tenuti all'obbligo di registrazione di cui l'art. 49, nonché a quello di esibizione della documentazione relativa alla valutazione su richiesta delle autorità competenti.

tezione destinati a essere utilizzati in atmosfera potenzialmente esplosiva, apparecchiature radio, attrezzature a pressione, attrezzature per imbarcazioni da diporto, impianti a fune, apparecchi che bruciano carburanti gassosi, dispositivi medici, dispositivi medico-diagnostici in vitro, veicoli automobilistici e aeronautici»[81]. Inoltre, il rimando limpido contenuto all'interno dell'Allegato I, Sezione A, nn. 11 e 12, ai Regolamenti europei di disciplina dei dispositivi medici e dei dispositivi medico-diagnostici in vitro, supporta questa qualificazione.

Rimanendo nell'ambito sanitario, si torni agli esempi di sistemi di IA di diagnostica medica resi nei paragrafi 2.1. e 2.2., ossia i sistemi *Mycin* e *Watson for Oncology*, rispetto ai quali ci si potrebbe chiedere se essi siano da considerarsi sistemi ad alto rischio oppure no.

In considerazione del fatto che nella definizione di dispositivo medico rientrano anche i *software* utilizzati, da soli o in combinazione, con finalità diagnostiche e/o terapeutiche[82], si tratta, in entrambi i casi di prodotti che rientrano nell'ambito di applicazione di una determinata normativa di armonizzazione dell'UE, ed in particolare, del Regolamento 745/2017. In aggiunta, ai sensi della lettera a) dell'art. 6 n. 1 dell'AI Act sono da considerarsi sistemi ad alto rischio i prodotti disciplinati dalla normativa di armonizzazione dell'UE di cui l'allegato I, nella cui elencazione rientra anche il Regolamento del 2017 appena citato. In ragione di queste considerazioni, a parere della scrivente, è da concludersi che i sistemi come *Mycin* e *Watson for Oncology* siano da considerarsi ad alto rischio, con tutte le conseguenze che ne derivano.

4.1.2.1. I requisiti dei sistemi ad alto rischio

I sistemi ad alto rischio devono necessariamente rispettare specifici requisiti descritti dettagliatamente dal Regolamento 1689/2024, alla Sezione 2, artt. 8-15. Sin da ora è opportuno precisare che l'onere di garantire il rispetto di tali requisiti spetta ai fornitori (Art. 3, par. 3, n. 1), i quali sono altresì tenuti a presentare, su richiesta, alle autorità competenti una dichiarazione di conformità del sistema[83].

---

81. Regolamento UE 1689/2024. A maggior precisazione, sempre con riferimento all'ambito sanitario in senso ampio, l'Allegato III al punto 5, lettera a), annovera tra i sistemi ad alto rischio: «i sistemi di IA destinati ad essere utilizzati delle autorità pubbliche o per conto di autorità pubbliche per valutare l'ammissibilità delle persone fisiche alle prestazioni o ai servizi di assistenza pubblica essenziali, compresi i servizi di assistenza sanitaria (…)».

82. Per la definizione completa si veda la nota 16 di questo elaborato.

83. Art. 47, AI Act: «1. Il fornitore compila una dichiarazione scritta di conformità UE

Tali requisiti, che costituiscono il sostrato normativo minimo che deve guidare i fornitori nello sviluppo dei sistemi ad alto rischio, favorendo la realizzazione di tecnologie in linea con i valori europei, sono:

1. costruzione di un sistema di gestione del rischio: il fornitore è tenuto a implementare, in maniera documentata, un sistema che consenta di identificare e analizzare i possibili rischi derivanti dal suo impiego, farne una stima e adottare idonee misure;
2. precisione in tema di *data governance* e qualità dei *dataset*: i *dataset* utilizzati dal fornitore in fase di addestramento, validazione e test devono essere gestiti in maniera appropriata, e rispondere ad elevati requisiti in materia di pertinenza, rappresentatività, correttezza e completezza, onde limitare la possibilità di incorrere in *bias* dannosi e discriminatori;
3. adottare un'adeguata documentazione tecnica: i fornitori devono redigere e mantenere una documentazione tecnica completa e aggiornata che sia in grado di dimostrare il rispetto della normativa;
4. fornire adeguate informazioni in ossequio dell'obbligo di tracciabilità: il fornitore deve garantire la verificabilità e tracciabilità delle decisioni e dei processi posti in essere dai sistemi ad alto rischio prevedendo meccanismi di registrazione automatica dei log, al fine di attenuare l'effetto "*black-box*" e la conseguente opacità del funzionamento del *software*;
5. fornire adeguate informazioni in ossequio dell'obbligo di trasparenza: la

---

leggibile meccanicamente, firmata a mano o elettronicamente, per ciascun sistema di IA ad alto rischio e la tiene a disposizione delle autorità nazionali competenti per dieci anni dalla data in cui il sistema di IA ad alto rischio è stato immesso sul mercato o messo in servizio. La dichiarazione di conformità UE identifica il sistema di IA ad alto rischio per il quale è stata redatta. Su richiesta, una copia della dichiarazione di conformità UE è presentata alle pertinenti autorità nazionali competenti. 2. La dichiarazione di conformità UE attesta che il sistema di IA ad alto rischio interessato soddisfa i requisiti di cui alla sezione 2. La dichiarazione di conformità UE riporta le informazioni di cui all'allegato V ed è tradotta in una lingua che può essere facilmente compresa dalle autorità nazionali competenti degli Stati membri nei quali il sistema di IA ad alto rischio è immesso sul mercato o messo a disposizione. 3. Qualora i sistemi di IA ad alto rischio siano soggetti ad altra normativa di armonizzazione dell'Unione che richieda anch'essa una dichiarazione di conformità UE, è redatta un'unica dichiarazione di conformità UE in relazione a tutte le normative dell'Unione applicabili al sistema di IA ad alto rischio. La dichiarazione contiene tutte le informazioni necessarie per identificare la normativa di armonizzazione dell'Unione cui si riferisce la dichiarazione. 4. Redigendo la dichiarazione di conformità UE, il fornitore si assume la responsabilità della conformità ai requisiti di cui alla sezione 2. Il fornitore tiene opportunamente aggiornata la dichiarazione di conformità UE. 5. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 97 al fine di modificare l'allegato V aggiornando il contenuto della dichiarazione di conformità UE di cui a tale allegato per introdurre elementi che si rendano necessari alla luce del progresso tecnico».

trasparenza del sistema nei confronti degli utenti deve essere garantita mediante predisposizione di istruzioni per l'uso chiare, concise e comprensibili, che contengano almeno una serie di elementi specificamente individuati dal legislatore;
6. implementare idonee misure di controllo umano: i fornitori devono porre in essere misure appropriate a consentire un'effettiva supervisione umana sul funzionamento dei sistemi ad alto rischio;
7. raggiungere elevati *standard* di accuratezza, robustezza e sicurezza informatica: i sistemi ad alto rischio devono essere progettati e sviluppati in modo da garantire un elevato livello di accuratezza, robustezza e sicurezza informatica durante l'intero ciclo di vita del *software*.

Si evidenzi che non sempre risulta facile per i fornitori soddisfare tali richieste, e proprio per questo motivo l'AI Act stesso, all'art. 40, prevede una presunzione di conformità, a favore di tutti quei sistemi di IA che rispettino i requisiti stabiliti dalle norme di armonizzazione o parti di esse, nella misura in cui tali norme implementino i medesimi requisiti dettati dall'AI Act. Peraltro, un'ulteriore presunzione opera, a norma dell'art. 42 e limitatamente ai requisiti di cui l'art. 10 AI Act per i set di dati di addestramento utilizzati dai sistemi di IA, con riferimento a tutti quei sistemi che siano stati allenati e testati su dati che riflettono lo specifico contesto geografico, comportamentale, contestuale e funzionale in cui sono destinati ad essere utilizzati.

Si tratta evidentemente di una disciplina caratterizzata dalla voluta genericità, la quale tuttavia non permette di cogliere a pieno le specificità dei sistemi robotici destinati alla diagnostica medica, qui presi in considerazione, se non per il tramite di una attenta attività di sussunzione dello specifico sistema da analizzarsi nella disciplina delineata.

4.1.2.2. Sistemi di IA ad alto rischio e adempimenti a carico dei fornitori

Concentrando l'attenzione sui sistemi ad alto rischio, la cornice normativa prevista dal Regolamento appare decisamente complessa e onerosa, rivolgendosi precisamente a tutti i soggetti coinvolti tanto nello sviluppo, quanto nella successiva fase di commercializzazione dei sistemi stessi. Nonostante la stragrande maggioranza degli obblighi dettati dal Regolamento siano diretti ai fornitori (i "*providers*"), ossia i soggetti che sviluppano il sistema di IA oppure che dispongono di un sistema sviluppato con l'intenzione di immetterlo sul mercato o metterlo in servizio sotto il proprio nome

o marchio, anche a titolo gratuito[84], obblighi specifici sono previsti anche a carico degli utenti, importatori e distributori, il cui ruolo viene dettagliatamente delineato dal Regolamento.

A carico dei fornitori, è previsto l'obbligo di rispettare dei requisiti obbligatori, e ciò sin dalla genetica fase di progettazione e sviluppo; nonché, di verificare la conformità del sistema prima della sua commercializzazione[85]. Difatti, prima che il sistema di IA sia immesso sul mercato i fornitori dovranno: garantire che i sistemi di IA ad alto rischio siano conformi ai requisiti previsti per tale categoria di sistemi, dimostrandone la loro conformità nel caso di richiesta da parte dell'autorità nazionale competente[86]; fornire i propri dati di contatto e disporre di un sistema di gestione della qualità conforme all'articolo 17[87]; conservare la documentazione di cui all'articolo

84. Art. 3, n. 3 AI Act.

85. Sezione 3 – artt. 16-27.

86. Art. 21, AI Act: «1. I fornitori di sistemi di IA ad alto rischio, su richiesta motivata di un'autorità competente, forniscono a tale autorità tutte le informazioni e la documentazione necessarie per dimostrare la conformità del sistema di IA ad alto rischio ai requisiti di cui alla sezione 2, in una lingua che può essere compresa facilmente dall'autorità in una delle lingue ufficiali delle istituzioni dell'Unione indicata dallo Stato membro interessato. 2. Su richiesta motivata di un'autorità competente, i fornitori concedono inoltre all'autorità competente richiedente, a seconda dei casi, l'accesso ai log generati automaticamente del sistema di IA ad alto rischio di cui all'articolo 12, paragrafo 1, nella misura in cui tali log sono sotto il loro controllo. 3. Qualsiasi informazione ottenuta da un'autorità competente a norma del presente articolo è trattata in conformità degli obblighi di riservatezza di cui all'articolo 78».

87. Art. 17, AI Act: «1. I fornitori di sistemi di IA ad alto rischio istituiscono un sistema di gestione della qualità che garantisce la conformità al presente regolamento. Tale sistema è documentato in modo sistematico e ordinato sotto forma di politiche, procedure e istruzioni scritte e comprende almeno gli aspetti seguenti: a) una strategia per la conformità normativa, compresa la conformità alle procedure di valutazione della conformità e alle procedure per la gestione delle modifiche dei sistemi di IA ad alto rischio; b) le tecniche, le procedure e gli interventi sistematici da utilizzare per la progettazione, il controllo della progettazione e la verifica della progettazione del sistema di IA ad alto rischio; c) le tecniche, le procedure e gli interventi sistematici da utilizzare per lo sviluppo e per il controllo e la garanzia della qualità del sistema di IA ad alto rischio; d) le procedure di esame, prova e convalida da effettuare prima, durante e dopo lo sviluppo del sistema di IA ad alto rischio e la frequenza con cui devono essere effettuate; e) le specifiche tecniche, comprese le norme, da applicare e, qualora le pertinenti norme armonizzate non siano applicate integralmente, o non includano tutti i requisiti pertinenti di cui alla sezione 2, i mezzi da usare per garantire che il sistema di IA ad alto rischio sia conforme a tali requisiti; f) i sistemi e le procedure per la gestione dei dati, compresa l'acquisizione, la raccolta, l'analisi, l'etichettatura, l'archiviazione, la filtrazione, l'estrazione, l'aggregazione, la conservazione dei dati e qualsiasi altra operazione riguardante i dati effettuata prima e ai fini dell'immissione sul mercato o della messa in servizio di sistemi di IA ad alto rischio; g) il sistema di gestione dei rischi di cui all'articolo 9; h) la predisposizione, l'attuazione e la manutenzione di un sistema di monitoraggio successivo all'immissione sul mercato a norma dell'articolo 72; i) le procedure relative alla segnalazione di un incidente grave a norma dell'articolo 73; j) la gestione della comunicazione con le autorità nazionali competenti, altre autorità pertinenti, comprese quelle che

18[88]; conservare i log generati automaticamente dai loro sistemi di IA ad alto rischio di cui all'articolo 19[89]; rispettare gli obblighi di registrazione di cui all'articolo 49, paragrafo 1; assicurare il rispetto della procedura di valutazione della conformità di cui all'articolo 43 prima che sia immesso sul mercato o messo in servizio, ed elaborare una dichiarazione di conformità UE a

---

forniscono o sostengono l'accesso ai dati, gli organismi notificati, altri operatori, clienti o altre parti interessate; k) i sistemi e le procedure per la conservazione delle registrazioni e di tutte le informazioni e la documentazione pertinenti; l) la gestione delle risorse, comprese le misure relative alla sicurezza dell'approvvigionamento; m) un quadro di responsabilità che definisca le responsabilità della dirigenza e di altro personale per quanto riguarda tutti gli aspetti elencati nel presente paragrafo. 2. L'attuazione degli aspetti di cui al paragrafo 1 è proporzionata alle dimensioni dell'organizzazione del fornitore. I fornitori rispettano, in ogni caso, il grado di rigore e il livello di protezione necessari per garantire la conformità dei loro sistemi di IA ad alto rischio al presente regolamento. 3. I fornitori di sistemi di IA ad alto rischio soggetti agli obblighi relativi ai sistemi di gestione della qualità o a una funzione equivalente a norma del pertinente diritto settoriale dell'Unione possono includere gli aspetti elencati al paragrafo 1 nell'ambito dei sistemi di gestione della qualità stabiliti a norma di tale diritto. 4. Per i fornitori che sono istituti finanziari soggetti a requisiti in materia di governance, dispositivi o processi interni stabiliti a norma del diritto dell'Unione in materia di servizi finanziari, l'obbligo di istituire un sistema di gestione della qualità, ad eccezione del paragrafo 1, lettere g), h) e i), del presente articolo, si considera soddisfatto se sono soddisfatte le regole sui dispositivi o i processi di governance interna a norma del pertinente diritto dell'Unione in materia di servizi finanziari. A tal fine, si tiene conto delle norme armonizzate di cui all'articolo 40».

88. Art. 18, AI Act: «1. Il fornitore, per un periodo che termina 10 anni dopo che il sistema di IA ad alto rischio è stato immesso sul mercato o messo in servizio, tiene a disposizione delle autorità nazionali competenti: a) la documentazione tecnica di cui all'articolo 11; b) la documentazione relativa al sistema di gestione della qualità di cui all'articolo 17; c) la documentazione relativa alle modifiche approvate dagli organismi notificati, ove applicabile; d) le decisioni e gli altri documenti rilasciati dagli organismi notificati, ove applicabile; e) la dichiarazione di conformità UE di cui all'articolo 47. 2. Ciascuno Stato membro stabilisce le condizioni alle quali la documentazione di cui al paragrafo 1 resta a disposizione delle autorità nazionali competenti per il periodo indicato in tale paragrafo nel caso in cui il prestatore o il rappresentante autorizzato stabilito nel suo territorio fallisca o cessi la sua attività prima della fine di tale periodo. 3. I fornitori che sono istituti finanziari soggetti a requisiti in materia di governance, dispositivi o processi interni stabiliti a norma del diritto dell'Unione in materia di servizi finanziari, conservano la documentazione tecnica nell'ambito della documentazione conservata a norma del pertinente diritto dell'Unione in materia di servizi finanziari».

89. Art. 19, AI Act: «1. I fornitori di sistemi di IA ad alto rischio conservano i log di cui all'articolo 12, paragrafo 1, generati automaticamente dai loro sistemi di IA ad alto rischio, nella misura in cui tali log sono sotto il loro controllo. Fatto salvo il diritto dell'Unione o nazionale applicabile, i log sono conservati per un periodo adeguato alla finalità prevista del sistema di IA ad alto rischio, della durata di almeno sei mesi, salvo diversamente disposto dal diritto dell'Unione o nazionale applicabile, in particolare dal diritto dell'Unione in materia di protezione dei dati personali. 2. I fornitori che sono istituti finanziari soggetti a requisiti in materia di governance, a dispositivi o a processi interni stabiliti a norma del diritto dell'Unione in materia di servizi finanziari, conservano i log generati automaticamente dai loro sistemi di IA ad alto rischio nell'ambito della documentazione conservata a norma del pertinente diritto in materia di servizi finanziari».

norma dell'articolo 47; adottare le necessarie misure correttive e fornire le informazioni necessarie in conformità dell'articolo 20[90].

Gli obblighi dei fornitori, tuttavia, non si esauriscono nella fase antecedente alla immissione nel mercato di un sistema di IA; invero, gli stessi sono tenuti ad adempiere a doveri di monitoraggio e scambio di informazioni per tutta la durata della vita del sistema stesso. Più precisamente, i fornitori, ai sensi dell'art. 72 dell'AI Act, sono tenuti a istituire e documentare un sistema di monitoraggio che sia proporzionato alla natura delle tecnologie di IA e ai rischi del sistema di IA ad alto rischio; tale sistema raccoglie, documenta e analizza i dati pertinenti che possono essere forniti dai *deployer* o che possono essere raccolti tramite altre fonti sulle prestazioni dei sistemi di IA ad alto rischio per tutta la durata del loro ciclo di vita e consente al fornitore di valutare la costante conformità dei sistemi di IA.

Ultimo, ma non meno importante, è l'obbligo condiviso con i *deployer*, sancito dall'art. 4 dell'AI Act, secondo il quale i fornitori devono adottare misure idonee a garantire «un livello sufficiente di alfabetizzazione in materia di IA del loro personale nonché di qualsiasi altra persona che si occupa del funzionamento e dell'utilizzo dei sistemi di IA per loro conto, prendendo in considerazione le loro conoscenze tecniche, la loro esperienza, istruzione e formazione, nonché il contesto in cui i sistemi di IA devono essere utilizzati, e tenendo conto delle persone o dei gruppi di persone su cui i sistemi di IA devono essere utilizzati», il quale dovrà adempiersi già a partire dal 2 febbraio 2025.

4.1.2.3. Sistemi di IA ad alto rischio e adempimenti a carico dei *deployer*

Ai sensi dell'art. 3 n. 4 dell'AI Act per *deployer* si intende: «una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che

90. Art. 20, AI Act: «1. I fornitori di sistemi di IA ad alto rischio che ritengono o hanno motivo di ritenere che un sistema di IA ad alto rischio da essi immesso sul mercato o messo in servizio non sia conforme al presente regolamento adottano immediatamente le misure correttive necessarie per rendere conforme tale dispositivo, ritirarlo, disabilitarlo o richiamarlo, a seconda dei casi. Essi informano di conseguenza i distributori del sistema di IA ad alto rischio interessato e, ove applicabile, i *deployer*, il rappresentante autorizzato e gli importatori. 2. Qualora il sistema di IA ad alto rischio presenti un rischio ai sensi dell'articolo 79, paragrafo 1, e il fornitore ne venga a conoscenza, tale fornitore indaga immediatamente sulle cause, in collaborazione con il *deployer* che ha effettuato la segnalazione, se del caso, e ne informa le autorità di vigilanza del mercato competenti per il sistema di IA ad alto rischio interessato e, ove applicabile, l'organismo notificato che ha rilasciato un certificato per il sistema di IA ad alto rischio in conformità dell'articolo 44, in particolare in merito alla natura della non conformità e all'eventuale misura correttiva pertinente adottata».

utilizza un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale». L'art. 26 dell'AI Act elenca dettagliatamente gli obblighi cui sono tenuti i *deployer* di sistemi di IA ad alto rischio, che possono essere sintetizzati come segue.

I *deployer* svolgono il compito primario di adottare tutte le misure tecniche ed organizzative idonee all'utilizzazione dei sistemi secondo quanto previsto dalle istruzioni che li accompagnano; detengono, altresì, la competenza, sulla base delle appena citate istruzioni, di garantire che il funzionamento del sistema sia monitorato da una persona fisica in possesso delle adeguate capacità tecniche, formazione ed autorità; ed, in ultimo, saranno tenuti a sospendere l'utilizzo del sistema qualora ritengano che l'uso dello stesso in conformità alle istruzioni possa determinare un rischio ai sensi dell'art. 79 dell'AI Act. Nell'ipotesi in cui si identifichi un incidente grave, saranno i *deployer* a dover informare il fornitore e, successivamente, anche il distributore o importatore, nonché le autorità competenti. Sempre ai *deployer* spetta di garantire la conservazione dei *log* generati autonomamente per un periodo adeguato alle finalità del sistema, e comunque per un periodo di almeno sei mesi, nel caso in cui tali *log* siano sotto il loro controllo, salvo che sia diversamente previsto dalla legge nazionale o dall'UE o dalla disciplina sulla protezione dei dati personali.

Se i sistemi di IA ad alto rischio sono impiegati all'interno dei luoghi di lavoro, i *deployer* che siano anche datori di lavoro dovranno informare i rappresentanti dei lavoratori e i lavoratori interessati. Laddove, invece, i sistemi siano utilizzati per assumere decisioni, o assistere all'assunzione di decisioni, riguardanti persone fisiche, queste ultime devono essere informate del fatto di interagire con tali sistemi, nonché delle finalità e della natura della decisione assunta dalla macchina, e dell'esistenza del proprio diritto alla spiegazione.

Uno degli obblighi di maggior rilevanza riconosciuti in capo ai *deployer* è sicuramente quello di eseguire, preventivamente[91] all'immissione nel mercato dei sistemi ad alto rischio, una valutazione di impatto sul rispetto dei diritti fondamentali. Tale obbligo, da alcuni messo in discussione[92] per la sua criticità intrinseca e concreta di dimostrare se, ed eventualmente in che modo, un sistema possa direttamente cagionare un danno ai diritti fondamentali, è previsto a carico di *deployer* che siano organismi di dirit-

91. E poi di volta in volta soggetta ad aggiornamenti.

92. Hacker P., *AI Regulation in Europe: from the AI Act to future regulatory challenges*, in *Oxford Handbook of Algorithmic Governance and the Law*, Oxford University Press, 2024.

to pubblico, privati che erogano servizi pubblici o che forniscano sistemi destinati ad essere utilizzati per valutare l'affidabilità creditizia delle persone fisiche o per la valutazione dei rischi e la determinazione dei prezzi di assicurazioni sulla vita e assicurazioni sanitarie[93]. Con la precisazione che all'interno della categoria dei soggetti privati che erogano servizi di natura pubblica vi rientrano, ad esempio, coloro che svolgono un ruolo nel settore dell'istruzione, dell'assistenza sanitaria, dei servizi sociali, degli alloggi e dell'amministrazione della giustizia[94].

Con l'evidente obiettivo di consentire al *deployer* di rilevare i rischi specifici per i diritti delle persone o dei gruppi di persone che potrebbero essere interessati e di individuare, di conseguenza, le misure da adottare al concretizzarsi di tali rischi, la valutazione in esame dovrà contenere una serie di elementi minimi:

1. la descrizione dei processi in cui il sistema di IA sarà utilizzato, in linea con la finalità prevista;
2. la descrizione del periodo di tempo e della frequenza di utilizzo del sistema di IA;
3. l'indicazione delle categorie di persone o gruppi di persone fisiche interessate dall'uso del sistema;
4. l'individuazione dei rischi specifici di danno che possono incidere sui diritti fondamentali di tali persone o gruppi, in particolare, tenendo conto delle informazioni pertinenti per un'adeguata valutazione dell'impatto, comprese, tra l'altro, le informazioni trasmesse dal fornitore del sistema di IA ad alto rischio nelle istruzioni per l'uso;
5. stabilire le misure da adottare al concretizzarsi di tali rischi, compresi, ad esempio, i meccanismi di *governance* in tale contesto specifico di utilizzo, quali le modalità di sorveglianza umana secondo le istruzioni per l'uso, o le procedure di gestione dei reclami e di ricorso, dato che potrebbero essere determinanti nell'attenuare i rischi per i diritti fondamentali in casi d'uso concreto.

I risultati ottenuti dalla valutazione, dovranno essere comunicati dal *deployer* alla pertinente autorità di vigilanza del mercato per il tramite del modulo fornito dall'Ufficio per l'IA; quest'ultimo avrà, altresì, il compito di elaborare un modello di questionario al fine di agevolare l'adempimento dell'obbligo da parte dei *deployer*, riducendone così gli oneri amministrativi.

93. Allegato III, art. 5 lett. b) e c) dell'AI Act.
94. Considerando 96 dell'AI Act.

In aggiunta, al fine di ottimizzare il coordinamento con la normativa UE, qualora il *deployer* debba eseguire una valutazione d'impatto che coinvolga i dati personali, a norma dell'art. 35 del GDPR, la stessa dovrà integrarsi in quella resa sui diritti fondamentali.

Infine, anche i *deployer*, come in precedenza accennato, di concerto con i fornitori, sono tenuti, ai sensi dell'Art. 4 dell'AI Act ad adempiere agli obblighi di alfabetizzazione in materia di IA.

4.1.3. Sistemi di IA a basso rischio

In via residuale e a titolo di completezza espositiva, la normativa in esame prende in considerazione anche i sistemi a basso rischio, ossia coloro che non rientrano nelle altre due categorie appena descritte in quanto non rappresentativi di possibili gravi danni per i diritti fondamentali degli esseri umani. Al fine di favorire l'adeguamento su base volontaria ai requisiti previsti per i sistemi di IA ad alto rischio, si incoraggia la redazione, da parte di fornitori e *deployer,* di codici di condotta e meccanismi di *governance* per i sistemi che non rientrano nella categoria "ad alto rischio" con il chiaro obiettivo di diffondere un livello di sicurezza più elevato di tutti i sistemi immessi sul mercato a conseguente garanzia di maggior tutela per le persone fisiche. L'adeguamento deve avvenire tenendo conto delle soluzioni tecniche disponibili e delle migliori pratiche del settore, individuando gli obiettivi precisi da conseguire, come ad esempio: la valutazione e la riduzione al minimo dell'impatto dei sistemi di IA sulla sostenibilità ambientale, la promozione dell'alfabetizzazione in materia di IA, la facilitazione di una progettazione inclusiva e diversificata dei sistemi di IA, la valutazione e la prevenzione dell'impatto negativo dei sistemi di IA sulle persone vulnerabili[95].

Al di là dell'auspicata introduzione dei codici di condotta appena citati, per l'utilizzazione di tali dispositivi a basso rischio, sarà sufficiente rispettare dei requisiti di trasparenza i quali consentono agli utenti di essere consapevoli di interagire con un sistema di IA, salvo che ciò risulti evidente, così da comprenderne anche le caratteristiche distintive e le limitazioni eventuali. Più precisamente, essendo la trasparenza un requisito fondamentale ed allo stesso tempo imprescindibile per incrementare la fiducia dei cittadini nell'utilizzo consapevole dei sistemi di IA, l'art. 50 dell'AI Act, a prescindere del livello di rischio accordabile al sistema stesso, prescrive per tutti i sistemi destinati ad interagire direttamente con le persone fisiche il rispetto di un

95. Art. 95 AI Act.

certo livello di trasparenza, funzionale a garantire: la verifica che i risultati forniti dai sistemi di IA siano privi di errori, la carenza di vizi nel processo decisionale, nonché che il sistema stesso sia utilizzato esclusivamente per le finalità consentite per tutto il suo ciclo di vita[96].

Al proposito va comunque evidenziato che, sebbene le informazioni debbano essere rese, nel rispetto del principio dell'accessibilità, tempestivamente, al più tardi al momento della prima interazione tra l'essere umano e la macchina, ed in maniera chiara ed intellegibile, è frequente che a causa della complessità del sistema non sia comunque possibile avere una limpida e precisa panoramica delle loro modalità di funzionamento[97].

Giungendo al caso concreto, nell'ambito sanitario, simili sistemi possono essere, ad esempio, quelli destinati al monitoraggio e al tracciamento dell'uso di attrezzature ospedaliere, ove l'IA potrebbe aiutare nell'ottimizzazione della disponibilità e della manutenzione delle apparecchiature; oppure si pensi anche ad un sistema di IA che aiuta nella gestione degli appuntamenti, il quale non accede direttamente alle informazioni ed ai dati dei pazienti[98].

5. Conclusioni: linee guida per gli stakeholders di riferimento

Nel panorama sanitario attuale, l'adozione ed implementazione di soluzioni basate sull'intelligenza artificiale non è più un'eccezione, ma la normalità. Questa incisività è dovuta alla forte capacità di tali sistemi di fungere da validi assistenti, e talvolta addirittura sostituti, degli operatori sanitari in diversi ambiti operativi. Punto fondamentale è che la macchina deve sempre essere considerata come un'estensione della capacità dell'operatore sanitario, chiunque esso sia, e non come un mero sostituto. Difatti, la supervisione umana rispetto ai sistemi di intelligenza artificiale è da considerarsi presidio a garanzia del controllo e del corretto funzionamento dei sistemi stessi, nonché funzionale a garantire che il loro utilizzo non influisca negativamente sul grado di autonomia delle persone fisiche e non causi ulteriori effetti

96. Iaselli M., *Le origini dell'IA, evoluzione e rapporti con il diritto*, in Iaselli M. (a cura di) *AI ACT. Principi, regole e applicazioni pratiche del Reg. UE 1689/2024*, Maggioli, Santarcangelo di Romagna, 2024, p. 94.

97. Varošanec I., *On the path to the future: mappingthe notion of transparency in the EU regulatory framework for IA*, in *International Review of Law, Computers & Technology*, 2022, p. 98.

98. Del Pizzo A., *IA e medicina*, in Iaselli M. (a cura di) *AI ACT. Principi, regole ed applicazioni pratiche del Reg. UE 1689/2024*, Maggioli, Santarcangelo di Romagna, 2024, p. 362.

negativi. Si tratta di un precipitato logico della prospettiva antropocentrica con la quale ci si approccia all'intelligenza artificiale: non solo le nuove tecnologie devono restare al servizio degli esseri umani, ma questi ultimi dovranno anche restare al centro di qualsiasi interazione con i sistemi di IA, e loro evoluzioni, in considerazione del fatto che solo agli esseri umani viene incontestabilmente riconosciuta la capacità di assumere decisioni in particolari circostanze[99].

Per questo motivo, aspetto centrale del requisito di sorveglianza umana, di cui all'articolo 14 dell'AI Act, è che i sistemi ad alto rischio contengano strumenti idonei a consentire l'effettiva supervisione umana durante il loro utilizzo. Funzionalmente, queste misure di salvaguardia supportano gli obiettivi generali di trasparenza e contribuiranno alla prevenzione ed alla riduzione dei rischi per la salute, la sicurezza ed i diritti fondamentali, tanto nell'ipotesi in cui il sistema venga direttamente utilizzato per le finalità previste, quanto nel caso di loro utilizzo improprio.

L'impianto dell'AI Act è volto alla costruzione di un sistema tale da prevenire il concretizzarsi dei rischi correlati ai sistemi di IA, mediante l'imposizione di obblighi in capo ai diversi attori che operano lungo tutta la catena di progettazione, sviluppo e distribuzione e da attuare prima dell'immissione dei sistemi nel mercato.

Prendendo in considerazione alcuni possibili *stakeholders* impegnati nella prestazione di servizi sanitari, si rileva che gli stessi possono facilmente rientrare nella categoria dei *deployer*, assumendo, quindi gli obblighi relativi. Per fare alcuni esempi, tanto gli amministratori e dirigenti ospedalieri; quanto le unità operative ospedaliere non cliniche: reparto tecnico/sistemi informativi/settore innovazione/cyber security, comunicazione con pubblico e pubblicità e segnalazioni, ufficio legale; quanto i professionisti della salute interni all'ospedale: primari dei reparti, medici, operatori sanitari, infermieri, staff ambulanza, addetti alle radiografie, ostetrici, studenti/specializzandi, sono astrattamente riconducibili, alla luce delle definizioni dettate dallo stesso AI Act al suo articolo 3, alla categoria di coloro che, persone fisiche o giuridiche, autorità pubbliche, agenzie o un altro organismi, utilizzano un sistema di IA sotto la propria autorità, nella misura in cui quest'ultima condizione sia presente.

---

99. Lend E., *Human oversight in the EU artificial intelligence act: what, when and by whom?*, in *Law, Innovation and Technology*, 2023, pp. 511 e ss.; Onitiu D., *The Limits of Explainability & Human Oversight in the EU Commission's Proposal for the Regulation on AI - a Critical Approach Focusing on Medical Diagnostic Systems*, in *Information & Communications Technology Law*, 2022.

Ferma restando l'utilizzabilità e l'applicabilità solo dei sistemi di IA ad alto rischio e a basso rischio, con i crismi analizzati nel paragrafo 4.1.1. dedicato ai sistemi di IA a rischio inaccettabile, tali categorie di soggetti saranno tenuti agli obblighi già analizzati ai paragrafi dal 4.1.2. al 4.1.3, che possono così sintetizzarsi:

1. attività preventiva di valutazione dell'impatto del sistema sul rispetto dei diritti fondamentali, se ricorrono le condizioni sopra ricordate; nonché, di predisposizione tecnica ed organizzativa delle condizioni idonee di utilizzazione del sistema, conformemente alle istruzioni impartite dai fornitori, di cui il sistema stesso è corredato;
2. continuo monitoraggio della conformità del sistema, durante tutto il suo ciclo di vita. Tale compito si articola in diverse mansioni: verificare il persistente rispetto delle istruzioni, rilevare eventuali danni cagionati dal sistema, aggiornare periodicamente i fornitori sul funzionamento del sistema e sugli eventuali danni;
3. in adempimento del dovere di trasparenza, informare opportunamente gli utenti di interagire con il sistema di IA.

Con riferimento alla categoria dei pazienti e partecipanti ai *trial* clinici, gli stessi dovranno essere considerati alla stregua di meri utenti finali dell'applicazione di un sistema di IA, con riferimento ai quali dovranno essere garantiti il rispetto dei diritti fondamentali e dei principi della non discriminazione, della qualità e sicurezza dei sistemi di IA con i quali interagiscono, nonché il principio della trasparenza, imparzialità ed equità identificabili con il diritto alla spiegabilità della decisione del sistema. Tutti aspetti decisivi e strettamente correlati all'adempimento degli obblighi prescritti dall'IA Act ai fornitori, *deployer*, distributori, rappresentanti e così via, per portare a compimento l'iniziativa europea di promozione di un panorama di IA sicuro ed etico.

In conclusione, gli obiettivi concorrenti fra loro di protezione dei consumatori e/o utenti finali, intesi non solo quali utilizzatori dei sistemi programmati secondo l'intelligenza artificiale, ma anche quali soggetti passivi dell'azione di tali sistemi, e di promozione dell'innovazione tecnico-informatica devono divenire la priorità del legislatore, tanto europeo quanto nazionale.

Affinché l'ecosistema normativo possa dirsi efficace, è imprescindibile che lo stesso si fondi sulla combinazione di norme giuridiche, codici di condotta, *standard* tecnici e *best practice*. Solo con tale compenetrazione di elementi si potrà dar vita ad un quadro metodologico e sostanziale capace

di garantire certezza, flessibilità, trasparenza e corretta interpretazione di fronte a situazioni problematiche e dilemmatiche.

Bibliografia

AI-HLEG, *Orientamenti etici per un'IA affidabile*, 2019.

Ardigò A., *Un nuovo processo mimetico: le ricerche di "intelligenze artificiali". Interrogativi ed ipotesi di rilevanza*, in Negrotti M. (a cura di*), Intelligenze artificiali e scienze sociali*, FrancoAngeli, Milano, 1984, pp. 30-47.

Azzi S., Gagnon S., Ramirez A., Richards G., *Healthcare applications of artificial intelligence and analytics: A review and proposed framework*, in *Applied sciences*, 10(18), 6553, 2020, pp. 1-21.

Bermudez J.P., Nyrup R., Deterding S., Mougenot C., Moradbakhti L., You F., Calvo R.A., *The AI Act needs a practical definition of 'subliminal techniques'*, 2023.

Bermudez J.P., Nyrup R., Deterding S., Mougenot C., Moradbakhti L., You F., Calvo R.A., *What Is a Subliminal Technique? An Ethical Perspective on AI-Driven Influence*, 2023.

Bobev, T., *Defining AI in the AI Act: Pin the Tail on the System*.

Carcaterra G., *Presupposti e strumenti della scienza giuridica*, II ediz., Torino, 2012, pp. 171 ss.

Casaburo D., Guliotta L., *The EU AI Act proposal(s): Manipulative and exploitative AI practices*, 2023.

Casonato C., Marchetti B., *Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale*, in *BioLaw-Rivista di BioDiritto*, 3, 2021.

Chen Y. Et al., *Professionals' responses to the introduction of AI innovations in radiology and their implications for future adoption: a qualitative study*, in *BMC Health Services Research*, 21, 2021.

Communication to the Commission Approval of the content of the draft Communication from the Commission – *Commission Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), C(2025) 884 final, 04.02.2025, Bruxelles.*

Commissione Europea, *Libro Bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia.*

Commissione Europea, comunicazione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, *Bussola per il digitale: il modello europeo per il decennio digitale*, COM(2021) 118 final, 9.3.2021, Bruxelles.

Commissione Europea, comunicazione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni, *Plasmare il futuro digitale dell'Europa*, COM (2020) 67 final, 19.2.2020, Bruxelles.

Commissione Europea, comunicazione al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo e al Comitato delle Regioni *relativa alla trasformazione digitale della sanità e dell'assistenza nel mercato unico digitale, alla responsabilizzazione dei cittadini e alla creazione di una società più sana*, COM (2018) 233 final, 25.4.2018, Bruxelles.

Costanza M., *L'AI: de iure condito e de iure condendo*, in Ruffolo U. (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè Francis Lefebvre, Milano, 2020, p. 407-418.

Daverio M., Macioce F., *Intelligenza artificiale e diritto alla salute nella regolazione europea: aspetti emergenti al riguardo alla relazione medico-paziente*, in *Teoria e Critica della Regolazione Sociale*, 1, 2023, pp. 1-14.

Del Pizzo A., *IA e medicina*, in Iaselli M. (a cura di) *AI ACT. Principi, regole ed applicazioni pratiche del Reg. UE 1689/2024*, Maggioli, Santarcangelo di Romagna, 2024, pp. 345-373.

De Menech C., *Intelligenza artificiale e autodeterminazione in materia sanitaria*, in *BioLaw Journal-Rivista di BioDiritto*, 1, 2022, pp. 181-203.

Direttiva NIS 2016/1148, sulla sicurezza delle reti e dei sistemi informativi; Direttiva 93/42/CEE.

Di Nucci E., Tupasela A., *Concordance as evidence in the Watson for Oncology decision-support system*, in *Ai and Society*, 2020.

Di Stasio G., *Machine learning e reti neurali nel diritto civile. Applicazione del machine learning a casi di diritto condominiale*, in *i-lex,* 2018, pp. 1-24.

EU4Health: *Programma Europeo Salute 2021-2027.*

EuRobotic, *Strategic research agenda for robotics in europe 2014-2020*.

Ferioli E. A., *L'intelligenza artificiale nei servizi sociali e sanitari: una nuova sfida al ruolo delle istituzioni pubbliche nel welfare italiano*?, in "BioLaw Journal – Rivista di BioDiritto", n. 1/2019, pp. 163-175.

Ferrucci D., Brown E., Chu-Carroll J., Fan J., Gondek D., Kalyanpur A.A., Lally A., Murdock J.W., Nyberg E., Prager J., Schlaefer, N., Welty D., *The AI Behind Watson - The Technical Article. Building Watson: An Overview of the DeepQA Project*, in *AI Magazine Fall*, 2010.

Floridi L., Cowls J., Beltrametti M., Chatila R., Chazerand P., Dignum V., Luetge C., Medeline R., Pagallo U., Rossi F., Schafer B., Valcke P., Vayena E., *AI4People - An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations*, in "Minds and Machines", n. 28, 2018, pp. 689-707.

Galluzzo L., Gandin C., Ghirini S., Scafato E., *L'invecchiamento della popolazione: opportunità o sfida?*, Centro Nazionale di Epidemiologia, Sorveglianza e Promozione della Salute, Istituto Superiore di Sanità, Roma.

Gorry G. A., *Computer-assisted clinical decision-making,* in *Methods Inf Med*, 1973, Vol. 12, n. 1, pp. 45–51.

Hacker P., *AI Regulation in Europe: from the AI Act to future regulatory challenges*, in *Oxford Handbook of Algorithmic Governance and the Law*, Oxford University Press, 2024.

Iaselli M., *Le origini dell'IA, evoluzione e rapporti con il diritto*, in Iaselli M. (a cura di) *AI ACT. Principi, regole e applicazioni pratiche del Reg. UE 1689/2024*, Maggioli, Santarcangelo di Romagna, 2024, pp. 13-43.

Jori, A., *Principi di roboetica. Filosofia pratica e Intelligenza Artificiale*, Nuova Ipsa, Palermo, 2019.

Kitsios F., Kamariotou M., Syngelakis A.I., Talias M.A., *Recent advances of artificial intelligence in healthcare: A systematic literature review*, in *Applied sciences*, 13(13), 7479, 2023, pp. 1-22.

Lagioia F., *L'intelligenza artificiale in sanità: un'analisi giuridica*, G.Giapichelli, Torino, 2020.

Lend E., *Human oversight in the EU artificial intelligence act: what, when and by whom?*, in *Law, Innovation and Technology*, 2023, pp. 511 e ss.

Lo Sapio G., *La black-box: l'esplicabilità delle scelte algoritmiche*
quale garanzia di buona amministrazione, in *Federalismi.it*, 16, 2021, pp. 114-127.

Lupton M., *Some ethical and legal consequences of the application of artificial intelliogence in the fiel of medicine*, in *Trends Med*, Vol. 18, n. 4, 2018, pp. 1-7.

Mandarà E., *Il Regolamento UE sull'intelligenza artificiale*, in (a cura di Iaselli M.) *AI ACT. Principi, regole ed applicazioni pratiche del Reg. UE 1689/2024*, Maggioli, Santarcangelo di Romagna, 2024, p. 57.

Marmo R., *Algoritmi per l'intelligenza artificiale. Progettazione dell'algoritmo. Dati e machine learning. Neural network. Deep learning*, Hoepli, Milano, 2020.

Miller A., *The future of health care could be elementary with Watson*, in *CMAJ*, vol. 11, 2013, pp. 185-186.

Moro P., *Macchine come noi. Natura e limiti della soggettività robotica*, in Ruffolo U. (a cura di), *Intelligenza artificiale – Il diritto, i diritti, l'etica*, Milano, 2020, pp. 45-61.

Newell A., Simon H.A., *Human problem solving*, Prentice Hall-Inc., Englewood Cliffs, New Jersey, 1972.

Nikolinakos, N.T., *EU Policy and Legal Framework for Artificial Intelligence, Robotics and Related Tachnologies - the AI Act in Law, Governance and Technology*, Spinger, 2023, pp. 336-337.

Obermeyer Z. et al., *Analisi dei pregiudizi razziali in un algoritmo utilizzato per gestire la salute della popolazione*, in Scienza, 2019.

Onitiu D., *The Limits of Explainability & Human Oversight in the EU Commission's Proposal for the Regulation on AI- a Critical Approach Focusing on Medical Diagnostic Systems*, in *Information & Communications Technology Law*, 2022.

Palazzani L., *AI and health: ethical aspects for regulation*, in *Teoria e critica della Regolazione Sociale*, 1, 2021.

Paparella F., *Sistema esperto per la diagnosi delle malattie del fegato e delle vie biliari con gestione dell'incertezza*, Bari, 2010, pp. 48 ss.

Regolamento UE 2024/1689.

Regolamento 2016/679 – GDPR.
Regolamento UE 2024/1183.
Regolamento UE 2017/746 sui dispositivi medico-diagnostici in vitro ("IVDR").
Regolamento UE 910/2014.
Risoluzione del Parlamento Europeo del 16 febbraio 2027 recante raccomandazioni alla Commissione concernenti norme di diritto civile della robotica e Risoluzione del Parlamento Europeo del 12 febbraio 2019 su una politica industriale globale in materia di robotica e intelligenza artificiale.
Ruschemeier, H., *AI as a challenge for legal regulation – the scope of application of the artificial intelligence act proposal*, in *ERA Forum*, 2023.
Russell S., Norvig P., *Intelligenza artificiale. Un approccio moderno*, vol. 1, IV ediz., Milano, 2021.
Sartor G., *Intelligenza artificiale e diritto. Un'introduzione*, Giuffrè, Milano, 1996.
Sartor, G., *L'informatica Giuridica e le tecnologie dell'informazione. Corso di informatica giuridica*, Giappichelli, Torino, 2022.
Sartor G., *Intelligenza artificiale e diritto. Un'introduzione*, Gappichelli, Torino, 2022.
Sartor G., Lagioia F., *Le decisioni algoritmiche tra etica e diritto*, in Ruffolo U. (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, 2020.
Schoenberger D., *Artificial Intelligence in healthcare: a critical analysis of the legal and ethical implications*, in *International Journal of Law and Information Technology*, 27, 2018, pp. 171-203.
Shortliffe, E.H., *Mycin: a knowledge-based computer program applied to infectious diseases*, AMIA Annual Symposium Proceedings Archive, 1977, pp. 66-69.
Smith H., *Clinical AI: opacity, accountability, responsability and liability*, in *AI&Society*, 36, 2021, pp. 535-545.
Somashekhar S.P., Sepúlveda M.-J., Puglielli S., Norden A.D., Shortliffe E.H., Rohit Kumar C., Rauthan A., Arun Kumar N., Patil P., Rhee K., Ramya Y., *Watson for oncology and breast cancer treatment reccomendations: Agreement with an expert multidisciplinary tumor board*, in *Annals of Oncology*, n. 29, 2018, pp. 418-423.
Stradella E., *Stereotipi e discriminazioni: dall'intelligenza umana all'intelligenza artificiale*, in *Liber Amicorum per Pasquale Costanzo*, 2020.
Varošanec I., *On the path to the future: mappingthe notion of transparency in the EU regulatory framework for IA*, in *International Review of Law, Computers & Technology*, 2022, p. 98.
Yu Z., Wang Z., Ren X., Lou D., Li X., Liu H., Zhang X., *Practical exploration and research of Watson for Oncology clinical decision support system in real world and localized practise*, in *Journal of Clinical Oncology-An American Society of Clinical Oncology Journal*, vol. 37, n. 15, 2019.

Sitografia

eur-lex.europa.eu – Commissione Europea, *Libro Bianco sull'intelligenza artificiale – Un approccio europeo all'eccellenza e alla fiducia.*

old.eu-robotics.net – EuRobotic, *Strategic research agenda for robotics in europe 2014-2020*.

www.salute.gov.it – *EU4Health: Programma Europeo Salute 2021-2027*.

www.law.kuleuven.bem/ – Bobev, T., *Defining AI in the AI Act: Pin the Tail on the System*.

www.euractiv.com – Bermudez J.P., Nyrup R., Deterding S., Mougenot C., Moradbakhti L., You F., Calvo R.A., *The AI Act needs a practical definition of 'subliminal techniques'*.

www.philarchive.org – Bermudez J.P., Nyrup R., Deterding S., Mougenot C., Moradbakhti L., You F., Calvo R.A., *What Is a Subliminal Technique? An Ethical Perspective on AI-Driven Influence*, 2023.

www.law.kuleuven.bes/ – Casaburo D., Guliotta L., *The EU AI Act proposal(s): Manipulative and exploitative AI practices*, 2023.

Copyright © 2025 by FrancoAngeli s.r.l., Milano, Italy. Isbn: 9788835178699

Vi aspettiamo su:

www.francoangeli.it

per scaricare (gratuitamente) i cataloghi delle nostre pubblicazioni

DIVISI PER ARGOMENTI E CENTINAIA DI VOCI: PER FACILITARE
LE VOSTRE RICERCHE.

Management, finanza, marketing, operations, HR
Psicologia e psicoterapia: teorie e tecniche
Didattica, scienze della formazione
Economia, economia aziendale
Sociologia
Antropologia
Comunicazione e media
Medicina, sanità

Architettura, design, territorio
Informatica, ingegneria
Scienze
Filosofia, letteratura, linguistica, storia
Politica, diritto
Psicologia, benessere, autoaiuto
Efficacia personale
Politiche e servizi sociali

FrancoAngeli

La passione per le conoscenze

FrancoAngeli

DIRITTO ALLA SALUTE, PROTEZIONE DEI DATI PERSONALI E IA

L'innovazione tecnologica sta trasformando radicalmente il settore sanitario, ponendo nuove sfide giuridiche, etiche e organizzative. Questo volume analizza il rapporto tra diritto alla salute, protezione dei dati personali e impiego dell'intelligenza artificiale, esaminando le implicazioni normative e le questioni aperte nel contesto europeo. Attraverso un approccio interdisciplinare, il libro affronta temi cruciali quali l'evoluzione della sanità nell'era della datificazione e le potenzialità dell'intelligenza artificiale nel settore medico, analizzando in questa prospettiva i tre regolamenti europei dedicati alla creazione di uno spazio europeo dei dati sanitari, alla protezione dei dati personali e all'intelligenza artificiale con un *focus* sull'applicazione al settore sanitario. Viene inoltre rappresentato in modo chiaro, sintetico e completo il quadro delle questioni etiche all'attenzione degli studiosi con uno sguardo alle prospettive future. Frutto di un progetto di ricerca interdisciplinare, il volume si rivolge a giuristi, professionisti della sanità, *policy maker* e studiosi interessati a comprendere l'impatto delle tecnologie emergenti sulla tutela della salute e dei diritti fondamentali.

Claudio Sarra è professore di Etica e Informatica giuridica nella Scuola di Giurisprudenza dell'Università di Padova. Per questo editore ha pubblicato la monografia *Lo scudo di Dioniso. Contributo allo studio della metafora giuridica* e ha co-curato i volumi *Positività e Giurisprudenza. Teoria e prassi nella formazione giudiziale del diritto, e Tecnodiritto. Temi e problemi di informatica e robotica giuridica contemporanea*.

Anna Zilio è Avvocato del Foro di Padova, collabora con uno studio legale internazionale fornendo supporto a società sia italiane che estere in materia di data protection e nuove tecnologie, responsabilità amministrativa degli enti ai sensi del D.lgs. 231/2001, corporate governance e corporate social responsibility.

Giulia De Bona è dottoranda di ricerca in Ciencia Sociales y Jurídica presso il Dipartimento di Ciencias Jurídicas Internacionales e Históricas y Filosofía del Derecho dell'Università di Córdoba (ES), in regime di Cotutela con l'Università degli Studi di Padova.

FrancoAngeli
La passione per le conoscenze