



UNIVERSITÀ DEGLI STUDI DI PAVIA

Dipartimento di Giurisprudenza

Diritto della Prevenzione, dell'Innovazione e della Sicurezza per
le imprese e l'Amministrazione pubblica

La digitalizzazione del Servizio Sanitario Nazionale tra
governance dei dati sanitari e intelligenza artificiale

Relatore: Chiar.ma Prof. Valentina Buratti

Tesi di laurea di

Tommaso Marise

Matr. 563720

Anno accademico 2025/2026

Indice

INTRODUZIONE	6
--------------------	---

CAPITOLO I

I DATI SANITARI: DEFINIZIONE, TUTELA E FUNZIONE NEL QUADRO DELLA TRASFORMAZIONE DIGITALE DELLA SANITÀ

1. I dati relativi alla salute: profili definitori ed evoluzione normativa.	11
1.1. I dati relativi alla salute nel GDPR: definizione, ambito applicativo e tutela.....	12
2. I principi del trattamento dei dati relativi alla salute e l'autodeterminazione informativa.....	18
3. Lo Spazio Europeo dei Dati sanitari: finalità e obiettivi.....	23
3.1 Utilizzo primario e secondario dei dati sanitari.	26
3.2 <i>L'European Health Data Space</i> : tensioni tra interesse individuale e collettivo...	32
4. La controversa natura dei dati sanitari: tra bene pubblico e funzione di interesse generale.	33

CAPITOLO II

LA GESTIONE DEL DATO SANITARIO TRA *GOVERNANCE* E INNOVAZIONE

1. La sanità digitale: un'introduzione.	37
2. La nuova <i>governance</i> dei dati sanitari tra diritto dell'Unione europea e disciplina interna.	39
2.1. Il ruolo della Commissione Europea e l'intervento normativo delle autorità italiane nel delicato equilibrio tra atti di <i>hard</i> e <i>soft law</i>	43
3. La digitalizzazione dei servizi sanitari: il ruolo di AGENAS.....	45

4. Verso una nuova gestione dei dati sanitari: <i>OpenData</i> , principi <i>Fair</i> e <i>Trust</i>	48
5. La telemedicina come strumento di <i>e-Health</i>	51
6. Tecnologia <i>blockchain</i> e telemedicina quali strumenti per una circolazione sicura del dato sanitario.....	56
7. Strumenti di <i>e-Health</i> : il Fascicolo Sanitario Elettronico e la Cartella Clinica Elettronica.....	58
7.1 Istituzione dell'Ecosistema dei Dati Sanitari in Italia e il parere negativo da parte del Garante della <i>Privacy</i>	64
7.2 Il FSE e il problema dell'interoperabilità.....	67
8. Conclusioni.....	69

CAPITOLO III

INTELLIGENZA ARTIFICIALE E SANITÀ PUBBLICA: OPPORTUNITÀ E CRITICITÀ

1. L'impiego dell'intelligenza artificiale nella sanità pubblica: prime coordinate. .	71
2. Intelligenza artificiale e sanità: profili definitori.....	72
2.1. Le applicazioni pratiche dei sistemi di I.A. in sanità: tra opportunità e limiti.....	75
3. Il Regolamento europeo 2024/1689: il primo tentativo di regolamentazione dell'AI	81
3.1 L'intervento del legislatore italiano: la nuova legge quadro n. 132/2025 sull'intelligenza artificiale.	86
4. La trasformazione digitale della sanità: il modello <i>Value-Based Healthcare</i>	91
4.1. L'Intelligenza Artificiale come strumento essenziale nella transizione verso il modello <i>Value Based HealthCare: il caso Babylon Health</i>	95
5. I rischi legati al fenomeno della discriminazione algoritmica.....	96

5.1. Dal primo caso giurisprudenziale all'art. 30 d.lgs. n. 36/2023: la positivizzazione della non discriminazione algoritmica.	100
6. Il futuro della medicina? Neurotecnologie e <i>Brain Computer Interface</i> : tra applicazioni pratiche ed esigenze di regolamentazione.	103
6.1 Un accenno ai c.d. neurodiritti.	108
BIBLIOGRAFIA	111

INTRODUZIONE

La progressiva digitalizzazione del Servizio Sanitario Nazionale ha modificato profondamente le modalità di raccolta, gestione, circolazione e utilizzo delle informazioni sanitarie, ponendo questioni che investono tanto la tutela dei diritti fondamentali della persona quanto l'organizzazione e il funzionamento dei sistemi sanitari. Muovendo da questa trasformazione, la presente tesi si propone di analizzare il rapporto tra *governance* dei dati sanitari e innovazione tecnologica, concentrando l'attenzione sulle principali evoluzioni normative e istituzionali che stanno accompagnando la costruzione della sanità digitale.

L'indagine prende le mosse dal tentativo di fornire una definizione di dato sanitario; quest'ultimo costituisce contestualmente una risorsa strategica della società contemporanea e un'informazione caratterizzata dalla capacità di incidere sulla sfera più intima e vulnerabile della persona.

La duplice natura del dato impone di interrogarsi sulle condizioni alle quali la crescente circolazione e valorizzazione del dato possano conciliarsi con la tutela della riservatezza, dell'autodeterminazione e, più in generale, dei diritti fondamentali dell'individuo. La tesi esamina, pertanto, l'evoluzione della disciplina della protezione dei dati personali, soffermandosi in particolare sulla nozione di "dato relativo alla salute", sulle difficoltà applicative derivanti dalla sua ampiezza e sul progressivo superamento di un modello fondato prevalentemente sul consenso quale strumento di controllo individuale sull'informazione.

Su tali premesse, si innesta l'analisi del Regolamento sullo Spazio Europeo dei Dati Sanitari (EHDS - Regolamento UE 2025/327), che rappresenta un passaggio decisivo nella costruzione di un sistema europeo di circolazione e riutilizzo dei dati sanitari. Grazie all'approvazione di tale atto, il quadro regolatorio ha compiuto un salto qualitativo, muovendosi in sinergia con il *Data Governance Act* e il *Data Act* per la costruzione di un mercato unico dei dati. Particolare attenzione è dedicata alla distinzione tra uso primario e uso secondario dei dati sanitari, nonché al rapporto tra tutela della dimensione individuale dell'informazione sanitaria e perseguimento di finalità di interesse generale,

quali la ricerca, l'innovazione, la programmazione sanitaria e la tutela della salute collettiva.

La progressiva valorizzazione del dato sanitario rende, tuttavia, necessario interrogarsi non soltanto sulle regole che ne disciplinano la protezione e la circolazione, ma anche sui soggetti e sulle strutture chiamati a governarne la gestione. Per tale ragione, la tesi si sofferma sull'architettura istituzionale della sanità digitale e della *governance* dell'innovazione tecnologica, esaminando la distribuzione di competenze tra livello europeo e livello nazionale e il ruolo assunto dalle diverse autorità pubbliche coinvolte nel processo di trasformazione digitale. In questo quadro, particolare attenzione è dedicata all'esigenza di combinare fonti di *hard law* con strumenti di *soft law*, nonché alle funzioni e ai caratteri di AgID, ACN, Garante per la protezione dei dati personali e AGENAS, quali soggetti chiamati a concorrere, secondo competenze differenziate, alla governance dei dati e all'innovazione tecnologica in ambito sanitario.

All'interno di tale sistema, AGENAS, designata quale Autorità di sanità digitale (Agenzia nazionale per la sanità digitale), è chiamata a evolvere da mero organo tecnico-operativo a cerniera istituzionale per la gestione delle piattaforme pubbliche e l'implementazione dell'intelligenza artificiale a supporto dei servizi territoriali.

L'analisi della governance consente così di mettere in luce come la trasformazione digitale non costituisca soltanto un processo tecnologico, ma richieda una corrispondente evoluzione delle strutture istituzionali e delle modalità di coordinamento tra i diversi attori coinvolti.

La governance del dato presuppone, inoltre, la disponibilità di infrastrutture e standard idonei a garantirne qualità, interoperabilità, sicurezza e conservazione nel tempo. Vengono, pertanto, esaminati gli strumenti attraverso i quali il patrimonio informativo sanitario viene organizzato e reso progressivamente interoperabile, soffermandosi sull'applicazione estensiva della disciplina sugli *OpenData* e l'integrazione tra i principi *FAIR* (*Findable, Accessible, Interoperable, Reusable*) e *TRUST* (*Transparency, Responsibility, User Focus, Sustainability, Technology*) consentono di realizzare *repository* sicuri e duraturi. Tali presupposti metodologici sono indispensabili per sorreggere l'evoluzione dell'*e-Health* e consentire il passaggio a modelli assistenziali

avanzati, garantendo al contempo che la circolazione e il riutilizzo dei dati avvengano nel pieno rispetto della riservatezza e dell'integrità delle informazioni.

In questo contesto di profonda trasformazione, spinto in modo decisivo dalle risorse del Piano Nazionale di Ripresa e Resilienza (PNRR - Missione 6), la telemedicina e le tecnologie emergenti come la *blockchain* si configurano quali strumenti essenziali per superare la frammentazione territoriale e ripensare la relazione terapeutica. La possibilità di effettuare televisite, teleconsulti e monitoraggi a distanza mediante dispositivi integrati trasforma il paziente da destinatario passivo a soggetto attivo del percorso di cura. Tuttavia, l'implementazione di questi strumenti richiede una costante attenzione critica verso i rischi di *digital divide*, il pericolo di depersonalizzazione del rapporto medico-paziente e la necessità di garantire standard di sicurezza informatica idonei a prevenire accessi abusivi e violazioni della *privacy*.

In questa prospettiva, particolare attenzione è dedicata al perno dell'intera infrastruttura di sanità digitale, che è rappresentato dal Fascicolo Sanitario Elettronico (FSE), e alla Cartella Clinica Elettronica (CCE). La distinzione delle rispettive funzioni consente di evidenziare il passaggio da una gestione frammentata delle informazioni cliniche a un modello orientato alla progressiva integrazione e interoperabilità dei dati. In particolare, Il definitivo superamento delle storiche criticità del sistema, legate alla frammentazione regionalistica e alla mancanza di dialogo tra i *database* territoriali, è affidato al potenziamento dell'Infrastruttura Nazionale per l'Interoperabilità (INI) e alla realizzazione dell'Ecosistema dei Dati Sanitari (EDS).

Preso atto dell'architettura organizzativa della sanità digitale, la riflessione si concentra sulle straordinarie opportunità e sulle complesse criticità poste dall'ingresso dell'intelligenza artificiale e delle neurotecnologie nella sanità pubblica. L'analisi si sofferma sulle applicazioni operative di *machine* e *deep learning*, dal supporto diagnostico alla riorganizzazione dei processi mediante strumenti di *Business Intelligence*, per evidenziare come l'opacità delle cd. *black box* imponga una rigorosa tutela dell'alleanza terapeutica, della *explainability* e del principio di centralità della decisione medica.

Tali dinamiche vengono vagliate alla luce della recente evoluzione normativa, segnata a livello sovranazionale dall'approccio basato sul rischio dell'*AI Act* (Regolamento UE

2024/1689) e, nel contesto nazionale, dall'approvazione della Legge n. 132/2025. Il confronto tra i due interventi normativi consente di verificare come la disciplina dell'intelligenza artificiale stia progressivamente costruendo strumenti volti a governare i rischi derivanti dall'impiego di sistemi automatizzati, soprattutto nei settori caratterizzati da un elevato impatto sui diritti fondamentali.

Lo studio approfondisce poi il ruolo centrale dell'algoritmo all'interno del paradigma della *Value-Based Healthcare*, in cui l'efficienza organizzativa e il disinvestimento strategico convergono verso la massimizzazione del valore clinico per il paziente. Rispetto a ciò, si evidenzia tuttavia il rischio della discriminazione algoritmica derivante da *bias* nei *dataset*: un tema affrontato analizzando l'evoluzione giurisprudenziale del Consiglio di Stato e la sua positivizzazione nel principio di "riserva di umanità" e non discriminazione *ex* articolo 30 del nuovo Codice dei Contratti Pubblici.

L'ultima parte della tesi estende lo sguardo alle frontiere più avanzate della medicina, esaminando le applicazioni delle neurotecnologie e delle *Brain-Computer Interface* (BCI). Tra esigenze di *compliance by design*, *cybersecurity* e tutela dei dati neurali, la trattazione si conclude riflettendo sull'emergere dei cd. "neurodiritti" (dalla *privacy* mentale alla continuità psicologica), intesi come nuova barriera a presidio dell'integrità e della dignità della persona umana di fronte all'avanzare della tecnologia.

CAPITOLO I

I DATI SANITARI: DEFINIZIONE, TUTELA E FUNZIONE NEL QUADRO DELLA TRASFORMAZIONE DIGITALE DELLA SANITÀ

SOMMARIO: 1. I dati relativi alla salute: profili definitori ed evoluzione normativa – 1.1 I dati relativi alla salute nel GDPR: definizione, ambito applicativo e tutela - 2. I principi del trattamento dei dati relativi alla salute e l'autodeterminazione informativa – 3. Lo spazio europeo dei dati sanitari: finalità e obiettivi – 3.1. Utilizzo primario e secondario dei dati sanitari – 3.2. *L'European Health data space*: tensioni tra interesse individuale e collettivo – 4. La controversa natura dei dati sanitari: tra bene pubblico e funzione di interesse generale

1. I dati relativi alla salute: profili definitori ed evoluzione normativa.

La progressiva digitalizzazione e la rapida evoluzione tecnologica hanno elevato il dato personale a risorsa strategica della società contemporanea. In questo scenario, i dati sanitari assumono un rilievo del tutto peculiare, per la loro capacità intrinseca di svelare gli aspetti più intimi e vulnerabili della persona fisica, attinenti alla sfera psicofisica, patologica o assistenziale, gli stessi si collocano al crocevia tra la tutela dei diritti fondamentali dell'individuo e il perseguimento di cruciali interessi della collettività.

Inquadrare rigorosamente il dato sanitario sotto il profilo definitorio rappresenta, tuttavia, una sfida complessa. Il Codice della *Privacy* definiva i dati sensibili come “*dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale*”¹. Il Codice riservava ai dati sulla salute e sulla vita sessuale garanzie e cautele ulteriormente rafforzate rispetto

¹ Art. 4, comma 1, l. d), Codice Privacy, Decreto legislativo 30/06/2003, n. 196.

agli altri dati sensibili², ad esempio, all'articolo 22, comma 8, imponeva il divieto assoluto di diffusione dei dati idonei a rivelare lo stato di salute.

Il Codice della *Privacy* rappresenta, quindi, un punto di partenza fondamentale per definire a livello normativo i dati sanitari, ma, con la, sempre più rapida, evoluzione delle tecnologie e la continua integrazione di queste ultime nella vita quotidiana di tutti i cittadini, si è avvertita sempre più l'esigenza di un intervento normativo di rango europeo in grado di armonizzare la disciplina. Questo tipo di intervento è avvenuto a partire dal 2016 attraverso l'emanazione del GDPR, *General Data Protection Regulation*³. Ad oggi, l'intera materia è plasmata dal diritto dell'Unione Europea, il cui intervento avviene tramite lo strumento del Regolamento⁴. L'uso del Regolamento è fondamentale perché permette di garantire un'effettiva uniformazione della disciplina, basato su regole armonizzate, nei vari Stati membri.

1.1. I dati relativi alla salute nel GDPR: definizione, ambito applicativo e tutela.

Il dato personale è oramai un elemento essenziale all'interno della società moderna. La protezione del dato personale è un diritto fondamentale della persona, questo principio viene affermato tramite l'emanazione, da parte dell'Unione Europea, del GDPR, *General Data Protection Regulation*⁵. Si tratta della principale normativa europea in materia di protezione dei dati personali. Il Regolamento è entrato in vigore nel 2016 e disciplina il trattamento dei dati personali delle persone fisiche e la libera circolazione dei dati. Il regolamento ha due finalità principali: innanzitutto “*persegue un obiettivo di uniformazione della disciplina europea sulla privacy*”, in secondo luogo, permette di superare la direttiva madre del 1995⁶, la quale era “*imperniata su una concezione*

² Da qui la dicitura di dati “supersensibili”.

³ Regolamento della comunità Europea 27/04/2016, n. 2016/679/UE.

⁴ Verranno analizzati più avanti i Regolamenti che permettono di completare il quadro normativo di riferimento.

⁵ Regolamento della comunità Europea 27/04/2016, n. 2016/679/UE.

⁶ Direttiva 24 ottobre 1995, n. 95/46/CE.

*sostanzialmente statica del trattamento dei dati personali e, soprattutto, per lo più binaria, in cui le informazioni procedono prevalentemente dall'interessato al titolare*⁷.

Il dato personale diventa, quindi, elemento essenziale nel Regolamento, a causa della continua evoluzione tecnologica che ha portato ad un “*mutamento qualitativo*” e ha, di conseguenza, permesso alla tutela della privacy di evolversi nel “*diritto di ogni persona al mantenimento del controllo sui propri dati, ovunque essi si trovino*”⁸.

La definizione di dato personale fornita dal Regolamento è molto ampia. È l'art. 4 a definire il dato personale come “*qualsiasi informazione riguardante una persona fisica identificata o identificabile; si considera identificabile una persona fisica che può essere identificata, direttamente o indirettamente*”⁹. L'elemento fondamentale che caratterizza il dato personale è, quindi, la sua idoneità a identificare una persona fisica.

Il dato deve, innanzitutto, portare con sé gli elementi necessari per essere associato ad un determinato soggetto, e, in secondo luogo, permettere l'identificazione anche attraverso il collegamento con altri dati¹⁰. Il Regolamento persegue l'obiettivo di bilanciamento tra la protezione e la circolazione dei dati, e, nell'ambito della disciplina europea in materia di protezione dei dati personali.

Ai fini che interessano, particolare rilievo assumono i dati relativi alla salute, in ragione della loro capacità di rivelare aspetti particolarmente sensibili della sfera individuale. Proprio la natura delicata delle informazioni concernenti lo stato di salute delle persone ha indotto il legislatore europeo a prevedere per tali dati uno specifico regime di tutela, collocandoli tra le categorie particolari di dati personali disciplinate dal GDPR.

Per quanto riguarda il trattamento dei dati relativi alla salute emergono due criticità: la prima è dovuta alle “*tendenze interpretative che fanno prevalere le esigenze di protezione su quelle di circolazione dei dati*”¹¹, ciò emerge nell'ambito sanitario a causa della natura sensibile del dato che attiene alla salute dell'individuo. La seconda criticità deriva dalla

⁷ C. COLAPIETRO, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in *Federalismi.it*, 2018, p. 13.

⁸ *Ivi*, p. 14.

⁹ Art. 4, par. 1, Regolamento della comunità Europea 27/04/2016, n. 2016/679/UE.

¹⁰ Dato personale (Artt. 2-4; 9-10).

¹¹ S. FRANCA, *Il trattamento dei dati sanitari nel contesto della sanità digitale. Verso una governance equilibrata?*, In *Federalismi.it*, 2025, p. 324.

crisi dell'autodeterminazione informativa, difatti, le regole del GDPR non permettono di assicurare un'autodeterminazione del soggetto nelle proprie scelte di trattamento e, di conseguenza, le regole del trattamento *“appaiono come pilastri di un'impalcatura che sostiene un modello di protezione di tipo eminentemente formale che nella sostanza non è idoneo a garantire in modo effettivo l'individuo”*¹².

Sotto un profilo definitorio, il GDPR non fornisce una definizione di dato sanitario, ma piuttosto quella di *“dati relativi alla salute”*. Questi ultimi sono considerati come *“dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute”*¹³. Si tratta di dati attinenti alle condizioni psicofisiche, fisiologiche o patologiche, di una persona identificata o identificabile, riferite al passato al presente o al futuro. La norma qualifica anche i dati concernenti le prestazioni di assistenza sanitaria erogate all'interessato e anche i numeri, i simboli e gli altri elementi che ne consentono il riconoscimento ai fini sanitari¹⁴. Il Regolamento, però, non fa alcun riferimento ai dati indirettamente relativi alla salute, cioè quei dati che, pur non riguardando l'ambito sanitario, consentono di desumere lo stato di salute dell'interessato in seguito ad un ragionamento logico di tipo deduttivo. Questi ultimi vanno considerati come dati relativi alla salute per due motivi: innanzitutto, l'utilizzo nel Regolamento sia del termine *“attinenti”* sia dell'espressione *“che rivelano”* suggerisce un'interpretazione estensiva della nozione di dato sanitario. Questa categoria, infatti, non comprende solo le informazioni strettamente medico-scientifiche o legate alle prestazioni assistenziali, ma si estende anche a quei dati apparentemente neutri da cui si possono comunque dedurre le condizioni psicofisiche dell'individuo. In secondo luogo, questi vanno ricompresi nella definizione di dati relativi alla salute in modo da evitare l'indebolimento della tutela dei diritti fondamentali dell'interessato¹⁵. La definizione di dati relativi alla salute va integrata con il considerando n. 35, in base al quale questi ultimi comprendono *“tutti i dati riguardanti lo stato di salute dell'interessato che rivelino informazioni connesse allo*

¹² *Ibidem*.

¹³ Art. 4, par. 15, Regolamento della comunità Europea 27/04/2016, n. 2016/679/UE.

¹⁴ L. D'ALEO, *La definizione di dato relativo alla salute nel GDPR: una questione ancora aperta*, in Dirittoesanita.unipv.it, 2025.

¹⁵ *Ibidem*.

stato di salute fisica o mentale passata, presente o futura dello stesso”¹⁶. La particolarità della nozione, oltre all’ampiezza della stessa, riguarda la capacità di “*qualificare dati personali apparentemente non riconducibili alla categoria di dati relativi alla salute*”¹⁷. Si tratta di un tipo di interpretazione estensiva, che trova conferma anche nella giurisprudenza, la quale ha qualificato come dato relativo alla salute l’informazione resa da un operatore sanitario ad un terzo relativa al ricovero in un determinato reparto, indipendentemente dalla menzione della specifica malattia¹⁸. Il riferimento è al caso deciso da Cass. n. 28417/2023¹⁹, nel quale una paziente, recatasi in ospedale per una interruzione volontaria della gravidanza, aveva espressamente chiesto che non fossero fornite informazioni sul suo stato di salute a soggetti terzi e che per ogni contatto fosse utilizzato esclusivamente il suo numero di telefono personale. Successivamente alle dimissioni, basandosi su un numero telefonico registrato in occasione di un precedente ricovero, l’infermiera di reparto aveva contattato il marito, informandolo del ricovero della moglie nel reparto di ginecologia e della necessità di assumere una generica terapia, senza fornire, però, specifiche indicazioni in merito al tipo di intervento svolto. La Corte ha stabilito che “*il fatto stesso di comunicare l’esigenza di un trattamento sanitario e, quindi, l’esigenza di una “malattia” in senso lato – intesa, dunque, come situazione che renda necessario un trattamento sanitario – attiene a dato sulla salute: non occorre cioè, a tal fine, che sia specificato di quale trattamento o di quale malattia si tratti*”.

Se l’ampiezza della nozione risponde all’esigenza di garantire all’interessato una protezione effettiva dei suoi diritti, allo stesso tempo, è importante evitare restrizioni eccessivamente rigide che potrebbero compromettere alcuni settori, come quello della ricerca²⁰. Inoltre, l’applicazione di questo assetto regolatorio porta con sé una problematica: diverse tipologie di dati assumono lo stesso grado di protezione e ciò si traduce nell’applicazione di un livello di tutela uniforme in situazioni molto differenti²¹.

¹⁶ Considerando n. 35, Regolamento della comunità Europea 27/04/2016, n. 2016/679/UE.

¹⁷ S. FRANCA, *Il trattamento dei dati sanitari nel contesto della sanità digitale. Verso una governance equilibrata?*, In *Federalismi.it*, p. 325.

¹⁸ A. IULIANI, *Gli incerti confini della nozione di “dati relativi alla salute”*, in *Autodeterminazione, cura e ricerca nell’era digitale*, 2026, p. 238.

¹⁹ Cass. 11 ottobre 2023, n. 28417, in *Foro.it*, 2023, I, c. 3062.

²⁰ L. D’ALEO, *La definizione di dato relativo alla salute nel GDPR: una questione ancora aperta*, in [Dirittoesanità.unipv.it](https://dirittoesanità.unipv.it), 2025.

²¹ S. FRANCA, *Il trattamento dei dati sanitari nel contesto della sanità digitale. Verso una governance equilibrata?*, In *Federalismi.it*, p. 325.

Sarebbe, di conseguenza, ottimale individuare un criterio pressoché univoco da poter utilizzare per stabilire se il dato, preso in considerazione, sia indirettamente relativo alla salute, in modo da valorizzarne l'idoneità a fornire informazioni sulle condizioni psicofisiche dell'interessato. In assenza di questo criterio si svilupperebbe il rischio di imbattersi in un'interpretazione eccessivamente ampia e potenzialmente lesiva del concetto di dato relativo alla salute.

A tal fine, può essere utile l'analisi di una recente sentenza della Corte di giustizia dell'Unione europea²² che ha avuto modo di esprimersi sulla nozione di dato relativo alla salute. Il caso aveva ad oggetto l'attività di vendita online di medicinali riservati alle farmacie, ma non soggetti a prescrizione medica, posta in essere da un gestore di una farmacia tedesca, attraverso la piattaforma online *"Amazon Marketplace"*. Durante la procedura d'acquisto, la piattaforma richiedeva l'inserimento di dati personali come nome e indirizzo di spedizione e altre informazioni personali. Il nodo centrale della controversia consiste nello stabilire se le informazioni richieste durante la procedura di acquisto possano essere qualificate come dati relativi alla salute ai sensi del GDPR.

La questione risulta particolarmente complessa, in quanto i medicinali oggetto della vendita non sono soggetti a prescrizione medica e, pertanto, non è possibile presumere con certezza che essi siano destinati all'utilizzo dell'acquirente, anziché di soggetti terzi. Ora, l'esigenza che i dati relativi alla salute riflettano lo stato patologico o fisiologico di uno specifico interessato solleva una problematica: ci si chiede se tale qualificazione sussista anche laddove manchi la certezza assoluta sul legame tra il dato e il soggetto. Poiché i farmaci venduti online non richiedono ricetta, la Corte ammette che i prodotti potrebbero essere ordinati per conto di terzi non identificabili. La soluzione offerta dalla Corte persegue la finalità di garantire la massima tutela ai diritti e alle libertà fondamentali degli individui di fronte a rischi significativi, quest'ultima, ritiene sufficiente che i dati consentano di desumere informazioni sulla salute *"mediante un'operazione intellettuale di raffronto o di deduzione"* in modo da ottenere *"la creazione di un nesso tra un medicinale, le sue indicazioni terapeutiche o i suoi usi e una persona fisica identificata o identificabile"*²³. In questo senso, la Corte qualifica i dati indicati dai clienti sulla

²² Corte Gius. UE, 4 ottobre 2024, C-21/23.

²³ A. AMIDEI, *Dati relativi alla salute e acquisto di farmaci online* (Corte giust. UE, 4 ottobre 2024, C-21/23, ND c. DR), in [Dirittoesanita.unipv.it](https://www.dirittoesanita.unipv.it), 2025.

piattaforma come relativi alla salute a prescindere dal fatto che le informazioni inserite riguardino l'utente interessato o qualsiasi altra persona. Ma, in questo modo, l'esigenza di protezione assume una valenza “astratta” perché non si riferisce più alla specifica situazione di trattamento²⁴. Bisognerebbe invece, secondo l'Avvocato Generale²⁵, tutelare l'autodeterminazione informativa dell'utente per evitare che venga protetto da rischi “ipotetici”, in modo da individuare uno specifico rapporto per bilanciare le esigenze di protezione e circolazione²⁶. Considerata la portata delle problematiche derivanti dall'ampiezza della definizione di dati relativi alla salute, si potrebbe pensare di fare ricorso solamente a dati anonimi per aggirare il regime del trattamento. Tramite l'anonimizzazione i dati sono sottoposti a un procedimento in grado di privarli del carattere personale, per poi poter essere liberamente trattati. Ma, la completa anonimizzazione è complicata da ottenere. Citando il caso *Breyer* della Corte di giustizia, un dato non può essere considerato anonimizzato qualora la reidentificazione sia solo “ragionevolmente possibile”²⁷. Il dato pseudonimizzato è quindi, secondo quest'ultima lettura, da considerare come un dato che non perde mai la natura personale, se non alla cancellazione irreversibile delle chiavi di pseudonimizzazione²⁸. In realtà, la Corte ha, successivamente, ridimensionato questa interpretazione negando l'equivalenza tra dato pseudonimizzato e personale, e, ha, invece, stabilito come sia necessaria una valutazione caso per caso²⁹. L'anonimizzazione presenta comunque delle criticità ulteriori, legate al traffico enorme di dati relativi alla salute e soprattutto al fatto che la privazione del carattere personale del dato può portare ad un impoverimento del dato stesso ed un allontanamento dagli obiettivi di ricerca³⁰.

²⁴ S. FRANCA, *Il trattamento dei dati sanitari nel contesto della sanità digitale. Verso una governance equilibrata?*, In *Federalismi.it*, p. 326.

²⁵ Cfr. Conclusioni dell'Avv. Generale Maciej Szpunar presentate il 25 aprile 2024, causa C-21/23.

²⁶ *Ibidem*.

²⁷ 19 ottobre 2016, *Breyer*, C-582/14.

²⁸ *Ivi*, p. 328.

²⁹ Corte di Giustizia, 4 settembre 2025, Causa C-413/23 P, EDPS v SRB.

³⁰ *Ivi*, p. 329.

2. I principi del trattamento dei dati relativi alla salute e l'autodeterminazione informativa.

L'articolo 5 del GDPR disciplina i principi fondamentali e applicabili al trattamento dei dati personali che verranno di seguito, brevemente, analizzati. Quest'ultimo riproduce il contenuto dell'art. 6 della Direttiva 95/46/CE, ma con una nuova visione; infatti, *“raccolge l'esperienza europea degli ultimi venti anni, con particolare riferimento agli approdi della Corte di Giustizia dell'Unione europea e, soprattutto, alla progressiva trasformazione dell'approccio delle istituzioni europee in materia, che passa da «una configurazione prevalentemente market-driven ad una fundamental rights-oriented»*³¹.

Il regolamento prevede delle regole generali applicabili a ogni forma di trattamento e delle regole specifiche per tipologie di dati e di trattamento particolari, l'ambito di applicazione è circoscritto solo ai trattamenti legati ad un'attività professionale o commerciale³².

Il principio fondamentale con il quale si apre l'art. 5 è quello della liceità del trattamento. L'attuazione di tale principio impone il rispetto di due requisiti alternativi: la necessità del trattamento o il consenso dell'interessato. La disposizione va interpretata anche ai sensi dell'art. 6 e del considerando n. 40 del Regolamento stesso, da due ipotesi di natura alternativa: l'espressione del consenso e il caso di trattamenti che trovino un fondamento normativo.³³

La c.d. *“funzione tipica del consenso”*³⁴ si trae dalla lettura dell'art. 9 del Regolamento che impone un divieto generale di trattamento, senza l'esplicito consenso dell'interessato per quanto riguarda i dati sensibili. Procedendo con i principi enunciati dall'art. 5, il primo comma si occupa dei principi di correttezza e di trasparenza. Questi ultimi si esprimono tramite un'adeguata informativa che viene considerata *“funzionale alla formazione ed espressione di un consenso al trattamento autenticamente libero e consapevole, nonché*

³¹ C. COLAPIETRO, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in *Federalismi.it*, 2018, p. 20.

³² *Ibidem*.

³³ *Ibidem*.

³⁴ *Ivi*, p. 21.

*all'eventuale esercizio di tutti i diritti dell'interessato*³⁵. Il principio di liceità (anche lealtà) è stato oggetto di interpretazione con riferimento alla questione dei *cookies*: in particolare, si è ritenuto fondamentale che le informative date agli utenti siano adeguate a far sì che, questi ultimi, siano in grado di comprendere le modalità e gli effetti ulteriori del trattamento³⁶. In altre parole, *“il leale comportamento del titolare si dovrebbe concretizzare in una libera scelta dell'interessato, anche mediante un duplice grado di informativa (breve ed estesa) che consenta «agli utenti di esprimere scelte realmente consapevoli sull'installazione dei cookie mediante la manifestazione di un consenso espresso e specifico»*³⁷.

La lettera b) dell'art. 5 c. 1, stabilisce che *“i dati personali devono essere raccolti per finalità determinate, esplicite e legittime”*³⁸ e queste ultime devono risultare espressamente dall'informativa. Il principio di finalità si collega con quello di liceità, dato che il consenso si rivela, da solo, insufficiente a tutelare i dati personali in seguito alla continua e incessante evoluzione della tecnologia. Tale presa d'atto conduce alla necessità di introdurre il principio di finalità, stabilendo le finalità per le quali i dati devono essere trattati³⁹. Anche da questo tipo di principio, si comprende come il Regolamento sia orientato verso una tutela dei dati personali che possa essere al passo con i tempi, si tratta del problema del trattamento svolto per finalità diverse da quelle per cui i dati sono stati raccolti: il trattamento secondario⁴⁰.

Il principio di necessità è disciplinato all'art. 5, l. c): innanzitutto, in base a questo principio, *“i dati devono essere caratterizzati da un nesso di pertinenza e adeguatezza rispetto alle finalità, in modo tale che non possano essere raccolti dati eccedenti le finalità predeterminate. In particolare, i sistemi di trattamento dei dati devono ridurre al minimo l'utilizzazione dei dati personali, laddove i medesimi obiettivi possano essere raggiunti mediante dati anonimi o che non consentano l'immediata identificazione*

³⁵ *Ibidem*.

³⁶ C. COLAPIETRO, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in *Federalismi.it*, 2018, p. 22.

³⁷ *Ibidem*.

³⁸ Art. 5, par. 1, l. b), Regolamento della comunità Europea 27/04/2016, n. 2016/679/UE.

³⁹ *Ivi*, p. 23.

⁴⁰ *Ibidem*.

dell'interessato"⁴¹. Gli ultimi principi contenuti nel Regolamento si occupano di valorizzare la responsabilità del titolare del trattamento. Si rivengono, quindi, i principi di integrità e riservatezza⁴² e il principio di responsabilizzazione del titolare⁴³ in base al quale le regole del trattamento devono essere osservate dal titolare stesso, sul quale grava l'onere della prova⁴⁴.

Dopo aver, brevemente, descritto i principi alla base del trattamento è fondamentale soffermarsi sul tema dell'autodeterminazione. Si tratta di un tema critico all'interno della disciplina del trattamento dei dati relativi alla salute e ha rilievi rispetto all'applicazione del principio di trasparenza. Il legame tra questi due principi fondamentali rientra nell'esercizio dei diritti sul trattamento, ma i dubbi emergono in merito al fatto che il consenso debba essere informato. Già prima del GDPR il consenso era la regola generale per la fondatezza della liceità del trattamento e l'autodeterminazione informativa avveniva tramite la previa informazione e la successiva espressione del consenso⁴⁵. Il GDPR ha modificato la disciplina in merito ai trattamenti relativi alla salute stabilendo che per questi ultimi il consenso non è più necessario, optando quindi per una decentralizzazione del consenso stesso. Il consenso è una forte base giuridica in grado di assicurare l'autodeterminazione informativa e di garantire all'interessato il controllo dei propri dati⁴⁶. Questa affermazione non è priva di criticità. Innanzitutto, considerando che il consenso deve essere libero (oltre che espresso, inequivoco e informato) bisogna chiedersi quanto si possa parlare di un consenso effettivamente libero in un contesto come quello delle prestazioni sanitarie. Inoltre, in merito all'informativa all'interessato, la lettura delle informazioni relative alle cure esprime una *"fotografia in via preventiva del trattamento e basata su contenuti standardizzati che non consente di acquisire un quadro completo del trattamento anche per come effettivamente si svolge"*. Infine, non convince l'adempimento agli obblighi informativi, considerato non adeguato a causa della

⁴¹ Ivi, p. 24.

⁴² Art. 5, par. 1, l. f), Regolamento della comunità Europea 27/04/2016, n. 2016/679/UE.

⁴³ Art. 5, par. 2, Regolamento della comunità Europea 27/04/2016, n. 2016/679/UE.

⁴⁴ C. COLAPIETRO, *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in Federalismi.it, 2018, p. 26.

⁴⁵ S. FRANCA, *Il trattamento dei dati sanitari nel contesto della sanità digitale. Verso una governance equilibrata?*, In Federalismi.it, p. 330.

⁴⁶ Ivi, p. 331.

manca di elementi fondamentali⁴⁷. L'analisi condotta fin ora fa emergere le criticità del trattamento dei dati relativi alla salute, sia sul piano definitorio che sul piano dell'autodeterminazione. Per garantire la liceità del trattamento bisogna appoggiarsi a due modelli, il primo sull'autonomia, basato sulla manifestazione di volontà del soggetto, il secondo sull'eteronimia, fondato sul principio di legalità⁴⁸. Il primo modello si basa sulla manifestazione del consenso e può essere considerato alla luce del *Data Governance Act* nella parte dedicata all'istituto dei servizi di intermediazione dei dati⁴⁹, considerato come *“un servizio che mira a instaurare, attraverso strumenti tecnici, giuridici o di altro tipo, rapporti commerciali ai fini della condivisione dei dati tra un numero indeterminato di interessati e di titolari dei dati, da un lato, e gli utenti dei dati, dall'altro, anche al fine dell'esercizio dei diritti degli interessati in relazione ai dati personali”*, e i servizi di cooperative di dati, cioè servizi *“offerti da una struttura organizzativa costituita da interessati, imprese individuali o da PMI, che sono membri di tale struttura, avente come obiettivi principali quelli di aiutare i propri membri nell'esercizio dei loro diritti in relazione a determinati dati, anche per quanto riguarda il compiere scelte informate prima di acconsentire al trattamento dei dati, di procedere a uno scambio di opinioni sulle finalità e sulle condizioni del trattamento dei dati che rappresenterebbero al meglio gli interessi dei propri membri in relazione ai loro dati, o di negoziare i termini e le condizioni per il trattamento dei dati per conto dei membri prima di concedere l'autorizzazione al trattamento dei dati non personali o prima che essi diano il loro consenso al trattamento dei dati personali”*⁵⁰. Si tratta di servizi adeguati al raggiungimento di determinati obiettivi come quello di *“rafforzare la posizione dei singoli individui, affinché compiano scelte informate prima di acconsentire all'utilizzo dei dati.”*⁵¹ In merito all'intermediazione dei dati, la cooperativa è tenuta a seguire determinate regole previste dall'articolo 12 DGA mantenendo separate le attività di intermediazione e di utilizzo dei dati.⁵² Il modello cooperativo permette di appoggiarsi ad

⁴⁷ *Ibidem*.

⁴⁸ S. FRANCA, *Il trattamento dei dati sanitari nel contesto della sanità digitale. Verso una governance equilibrata?*, In *Federalismi.it*, p. 333.

⁴⁹ Art 2, par. 1, n. 11, Regolamento UE 30/05/2022 n. 868.

⁵⁰ Art 2, par. 1, n. 15, Regolamento UE 30/05/2022 n. 868.

⁵¹ Considerando n. 31, Regolamento UE 30/05/2022 n. 868.

⁵² S. FRANCA, *Il trattamento dei dati sanitari nel contesto della sanità digitale. Verso una governance equilibrata?*, In *Federalismi.it*, p. 336.

un intermediario (cooperativa) per utilizzare i dati in modo da favorire l'autodeterminazione informativa e la circolazione dei dati stessi. Il modello si basa sulla difficoltà, in capo all'interessato, di poter esercitare pienamente la propria autodeterminazione informativa, difficilmente raggiungibile senza un intermediario⁵³.

Per quanto riguarda il modello eteronomo, bisogna ricordare che, in merito ai dati relativi alla salute, i trattamenti, possono essere necessari per differenti ipotesi⁵⁴. Si tratta di ipotesi di liceità, che richiedono che *“il trattamento sia necessario 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.”*⁵⁵ In questo senso interviene il Regolamento sullo Spazio Europeo dei Dati Sanitari che si occupa di rinnovare il regime dei dati sanitari, in merito all'utilizzo primario e secondario. Riguardo agli usi secondari, essi possono riguardare diverse finalità ed è il versante relativo a questi ultimi, all'interno del Regolamento, a considerare il modello eteronomo per il trattamento dei dati⁵⁶. È il considerando n. 52 a stabilire che l'attribuzione, da parte del regolamento, di compiti di interesse pubblico agli organismi responsabili dell'accesso ai dati sanitari va adeguata ai sensi dell'articolo 6, par. 1, lettera e) del GDPR in ottemperanza con l'articolo 9, par. 2 lettera da g) a j)⁵⁷. Significa che la disciplina del Regolamento è già di per sé una solida base giuridica per quest'ultimo. Inoltre, lo stesso considerando, invita gli Stati membri a non utilizzare il consenso come *“ulteriore condizione”* ai sensi dell'art. 9, par. 4, per quanto attiene a trattamenti per l'uso secondario di dati sanitari elettronici personali⁵⁸. Le problematiche legate a questo modello sono amplificate nel settore sanitario, di fatti il rischio è quello di *“condurre alla proliferazione di ecosistemi isolati e non comunicanti causando una frammentazione nel sistema informativo sanitario e, conseguentemente, minando le ragioni dell'interoperabilità.”*⁵⁹

⁵³ *Ibidem*.

⁵⁴ Motivi di: interesse pubblico rilevante, interesse pubblico nel settore della sanità pubblica o per finalità di ricerca.

⁵⁵ *Ivi*, p. 338.

⁵⁶ *Ibidem*.

⁵⁷ S. FRANCA, *Il trattamento dei dati sanitari nel contesto della sanità digitale. Verso una governance equilibrata?*, In *Federalismi.it*, p. 336.

⁵⁸ *Ibidem*.

⁵⁹ *Ivi*, p. 340.

3. Lo Spazio Europeo dei Dati sanitari: finalità e obiettivi.

Il Regolamento UE 2025/327⁶⁰, (EHDS), nasce con l'obiettivo di valorizzare pienamente l'uso primario e secondario dei dati personali e non personali⁶¹. Il Regolamento va considerato anche alla luce di altri interventi normativi dedicati alla materia dei dati, quali il Regolamento (UE) 2022/868 (*Data Governance Act*) e Regolamento (UE) 2023/2854 (*Data Act*). Questi ultimi hanno un rapporto di sinergia con il Regolamento EHDS, creando uno “*Spazio europeo dei dati*”⁶².

L'esistenza di uno spazio europeo dei dati sanitari permette di rafforzare l'idea del mercato unico e della libera circolazione. Inoltre, la possibilità di avere accesso ai dati, di utilizzarli in modo armonizzato, interoperabile e sicuro, di fare affidamento sulle tutele e sui diritti garantiti alle persone fisiche⁶³ e di poter garantire la protezione dei dati personali, permettono di mirare ad obiettivi quali “*innovazione, la crescita e il benessere della società europea potendo apportare benefici trasversali a diversi settori e un'economia basata sulla condivisione delle informazioni*”⁶⁴.

Attraverso l'emanazione del Regolamento il legislatore europeo ha introdotto il concetto di “*dato sanitario elettronico*”, che si sovrappone a quello di “*dato relativo alla salute*” delineato dal GDPR di cui si è dato conto in precedenza.

Al concetto di dato relativo alla salute possono essere ricondotte due tipologie di dato che “*potrebbero essere immaginate come due insiemi tra loro distinti, ma dotati di alcuni elementi in comune*”⁶⁵. Il primo insieme include i dati relativi alla salute e i dati genetici trattati in formato elettronico, nonché i “*dati sanitari elettronici non personali*” (e, cioè, i dati relativi alla salute anonimizzati o, per loro natura, non riferibili ad una persona fisica

⁶⁰ Regolamento della comunità Europea 11/02/2025, n. 2025/327/UE.

⁶¹ Per una lettura complessiva S. Corso, Lo spazio europeo dei dati sanitari. Prime riflessioni sul Regolamento UE 2025/327, in *Le Nuove leggi civili commentate*, 3/2025, pp. 563-603.

⁶² F. TRUBIANI, F. CASCINI, *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, luogo, 2025, p. 135.

⁶³ Soprattutto sulla base del GPDR, già precedentemente affrontato.

⁶⁴ *Ivi*, p. 136.

⁶⁵ L. D'ALEO, *La definizione di dato relativo alla salute nel GDPR: una questione ancora aperta*, in [Dirittoesanità.unipv.it](https://www.dirittoesanità.unipv.it), 2025.

identificata o identificabile, anch'essi elaborati in formato elettronico). Nel secondo insieme rientrano, invece, tutti i dati relativi alla salute, a prescindere dalla modalità del loro trattamento. Le due nozioni si intrecciano⁶⁶ e, di conseguenza, l'utilizzo di tali dati è disciplinato, oltre che dal GDPR, dal Regolamento EHDS.

Il Regolamento ha due impronte particolari, la prima economica e la seconda pubblicistica. L'implicazione economica è basata su due valori già affrontati e di difficile bilanciamento: la tutela della persona e la libera circolazione dei dati⁶⁷. Questo perché il dato si frappone in due lati, da una parte rappresenta l'espressione della persona, intesa come sua intimità e suoi diritti fondamentali, dall'altro, è un bene avente valore economico. Da questo punto di vista è fondamentale rinvenire un equilibrio tra la tutela della persona e la circolazione dei dati, cercando di creare spazi unici europei dei dati in modo da poter permettere, a parità di condizioni, a tutti gli operatori economici di accedere⁶⁸. La seconda impronta, di tipo pubblicistica, favorisce *“la circolazione e l'utilizzazione dei dati sanitari elettronici nell'interesse generale (l'uso secondario disciplinato dagli artt. 50 ss.), svincolate dalla manifestazione del consenso dell'interessato, nella consapevolezza dell'importanza fondamentale che hanno assunto la raccolta e la gestione dei dati nello svolgimento della funzione sanitaria”*⁶⁹. L'impronta pubblicistica deriva dal richiamo alla funzione sociale, presente nel considerando n. 4 del GDPR, secondo il quale, la protezione dei dati va considerata *“alla luce della sua funzione sociale e va temperata con altri diritti fondamentali”*⁷⁰. Il, già citato, *Data Governance Act*⁷¹, disciplina tra i suoi obiettivi la *“destinazione altruistica dei dati per finalità di interesse generale”*⁷². Nel Capo V del Data Act, il legislatore europeo, all'art. 15, disciplina due ipotesi eccezionali in cui la condivisione dei dati viene imposta per legge, rispetto ad una base volontaria. In questo modo il legislatore configura delle esigenze solidaristiche e un interesse pubblico all'utilizzazione dei dati superiore

⁶⁶ La nozione di “dato sanitario elettronico” è più ampia della nozione di “dato relativo alla salute”.

⁶⁷ A. MORACE PINELLI, *Lo spazio europeo dei dati sanitari (reg. UE n. 327/2025)*, in *La Nuova Giurisprudenza Civile Commentata*, n. 4, 1° luglio 2025, p. 1016.

⁶⁸ *Ibidem*.

⁶⁹ *Ivi*, p. 3.

⁷⁰ Considerando n. 4, Regolamento della comunità Europea 27/04/2016, n. 2016/679/UE.

⁷¹ Regolamento della comunità Europea 30/05/2022, n. 2022/868/UE.

⁷² A. MORACE PINELLI, *Lo spazio europeo dei dati sanitari (reg. UE n. 327/2025)*, in *La Nuova Giurisprudenza Civile Commentata*, n. 4, 1° luglio 2025, p. 1016, in *Banca dati OneLegale*, p. 3.

rispetto a quello dei titolari⁷³. L'obbligo di condivisione grava sui titolari dei dati che non siano enti pubblici e presuppone la sussistenza di "*necessità eccezionali*", cioè, "*circostanze imprevedibili e limitate nel tempo*"⁷⁴ che richiedano l'utilizzo dei dati detenuti dai soggetti privati, da parte di enti pubblici, istituzioni e organismi dell'Unione europea. La finalità è quella di consentire a tali soggetti di esercitare efficacemente le proprie funzioni istituzionali e perseguire obiettivi di interesse generale. La prima ipotesi ricorre in presenza di un'emergenza pubblica, come nel caso di una crisi sanitaria, quando le autorità competenti non siano in grado di ottenere tempestivamente i dati necessari attraverso strumenti alternativi per prevenire, gestire o superare la situazione emergenziale. La seconda ipotesi riguarda esclusivamente i dati non personali e si configura quando un soggetto pubblico, nell'esercizio di compiti di interesse pubblico espressamente previsti dalla legge, abbia individuato dati indispensabili allo svolgimento delle proprie funzioni e abbia previamente esaurito ogni altro mezzo ragionevolmente disponibile per acquisirli, compreso l'acquisto sul mercato o il ricorso ad altri strumenti normativi. In tal modo, il regolamento realizza un bilanciamento tra la tutela delle prerogative dei titolari dei dati e l'esigenza di garantire il perseguimento di finalità pubbliche di particolare rilevanza⁷⁵. Il Regolamento EHDS persegue quest'ultimo obiettivo, normando l'utilizzo primario e secondario dei dati sanitari. Difatti, le norme relative all'utilizzo primario possono tradursi nella creazione di un sistema basato su tecnologie uniformi e integrate, in modo da consentire un accesso facile, immediato e sicuro ai dati, e, inoltre, ridurre la frammentazione tra i sistemi Europei e nazionali⁷⁶. Per quanto riguarda l'utilizzo secondario, il Regolamento EHDS disciplina l'istituzione di un ecosistema digitale gestito da enti del settore pubblico, che dovranno fornire, successivamente alla verifica di requisiti previsti dalla normativa, l'accesso ai dati sanitari⁷⁷.

⁷³ *Ivi*, p. 4.

⁷⁴ *Ibidem*.

⁷⁵ *Ibidem*.

⁷⁶ F. TRUBIANI, F. CASCINI, *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, 2025, p. 136.

⁷⁷ *Ivi*, p. 137.

3.1 Utilizzo primario e secondario dei dati sanitari.

L'utilizzo dei dati sanitari, primario e secondario, va calibrato anche, e soprattutto, in merito alle implicazioni per gli Stati membri dell'Unione Europea nell'attuazione delle norme. In merito all'utilizzo primario, e le sue naturali implicazioni, il Regolamento EHDS lo considera come *“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”*⁷⁸. Diventa di fondamentale importanza considerare la disciplina della condivisione in merito all'utilizzo primario dei dati sanitari. Quest'ultima si raggiunge con *“il miglioramento dell'accesso e del controllo delle persone fisiche sui propri dati sanitari a livello transfrontaliero, e con la facilitazione dello scambio tra professionisti”*⁷⁹. L'art. 23 del Regolamento disciplina l'infrastruttura *“MyHealth@EU”* (LaMiaSalute@UE), fondamentale per la condivisione dei dati per l'uso primario. Si tratta dell'infrastruttura guida per la circolazione europea dei dati sanitari elettronici e delle cartelle cliniche, cruciale per scopi legati all'accesso dei dati da parte dei pazienti, in modo da poter esercitare i propri diritti, e per l'inserimento, la modifica e l'esclusione delle informazioni presenti nelle cartelle cliniche elettroniche⁸⁰. Il paragrafo n. 2 disciplina i c.d. Punti di contatto nazionale, stabilendo che *“ciascuno Stato membro designa un punto di contatto nazionale per la sanità digitale quale sportello organizzativo e tecnico per la fornitura di servizi connessi allo scambio transfrontaliero di dati sanitari elettronici personali nel contesto dell'uso primario. Ogni punto di contatto nazionale per la sanità digitale si collega a tutti gli altri punti di contatto nazionali per la sanità digitale negli altri Stati membri e alla piattaforma centrale di interoperabilità per la sanità digitale nelle infrastrutture transfrontaliere LaMiaSalute@UE (MyHealth@EU)”*⁸¹.

⁷⁸ Art 2, par. 2, l. b), Regolamento della comunità Europea 11/02/2025, n. 2025/327/UE.

⁷⁹ *Ivi*, p. 138.

⁸⁰ *Ivi*, p. 139.

⁸¹ Art. 23, par. 2, Regolamento della comunità Europea 11/02/2025, n. 2025/327/UE.

Si richiede, quindi, ad ogni Stato membro di garantire la disponibilità al collegamento della propria infrastruttura (MyHealth@EU) con tutte le infrastrutture riconosciute dal servizio sanitario di ogni Stato membro. Il PCN (Punto di contatto nazionale) è, quindi, un servizio di accesso ai dati; quest'ultimo deve essere designato, da ogni Stato membro, entro il 26 marzo 2027, e la sua operatività deve avvenire entro il 26 marzo 2029. L'obiettivo è descritto al par. 5 dell'art. 23, nel senso che *“Gli Stati membri garantiscono che tutti i prestatori di assistenza sanitaria siano collegati ai rispettivi punti di contatto nazionali per la sanità digitale. Gli Stati membri garantiscono che i prestatori di assistenza sanitaria collegati siano in grado di effettuare scambi bidirezionali di dati sanitari elettronici con il punto di contatto nazionale per la sanità digitale.”*⁸² Le Autorità di Sanità Digitale hanno il compito di organizzare l'utilizzo primario in ogni Stato membro. Affronteremo il tema nel secondo capitolo, per ora è sufficiente osservare che si tratta di autorità istituite dagli Stati membri per la gestione dell'utilizzo primario dei dati sanitari, sia in territorio nazionale sia tramite la cooperazione con altri Stati membri⁸³. Come bilanciamento nei confronti dei diritti dell'interessato, quest'ultimo ha un potere diretto di governo sui propri dati sanitari: oltre al diritto di accesso, gratuito e interoperabile dei propri dati sanitari elettronici, il diritto alla rettifica e all'integrazione dei dati inesatti o incompleti e il diritto alla notifica in caso di accesso ai propri dati da parte di soggetti terzi, si aggiunge il diritto di opposizione selettiva⁸⁴. Si tratta di un diritto all'oblio selettivo di tipo *“soggettivo e funzionale”*, a impedire a determinati soggetti l'accesso alla propria cartella clinica elettronica. Il diritto di opposizione selettiva trova il suo unico limite nella necessità del professionista a tutelare gli interessi vitali dell'interessato o di altra persona fisica⁸⁵. Continuando con i diritti e i poteri in capo all'interessato, è necessario considerare il potere di delega. Quest'ultimo permette al proprietario dei dati sanitari di nominare uno o più rappresentanti (a tempo determinato o indeterminato) per accedere a tutti i suoi dati e agire per nome suo. Si tratta di un potere esercitabile tramite il portale nazionale di accesso ai dati o tramite la presentazione di una

⁸² Art. 23, par. 5, Regolamento della comunità Europea 11/02/2025, n. 2025/327/UE.

⁸³ F. TRUBIANI, F. CASCINI, *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, 2025, p. 140.

⁸⁴ F. TRUBIANI, M. DI NUZZO, *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, 2025, p. 183.

⁸⁵ F. TRUBIANI, M. DI NUZZO, *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, 2025, p. 183.

dichiarazione all'autorità competente. L'ampiezza della disciplina del potere di delega è, ulteriormente dimostrata, dalla portata di natura aggiuntiva (e non sostitutiva), del potere di delega stesso. In base a ciò, la delega può essere, in ogni momento, revocata.⁸⁶ Ma, l'eventuale attribuzione a tempo indeterminato, collegata con la portata estesa delle norme relative la gestione delle autorizzazioni a terzi non convince: la delega è di tipo generale e comprendendo quindi il massimo dell'ampiezza, può essere limitata solo dall'interessato. Inoltre, il delegato non ha requisiti, doveri o oneri specificati, si tratta, quindi, di un potere attribuito in capo all'interessato, che presenta ancora delle zone dubbiose. Infatti, considerando anche il potere di opposizione selettiva e quello di oscuramento temporaneo dei dati la regola *“non appare coerente con il dinamismo delle relazioni personali e fiduciarie che caratterizzano la società in questo momento storico con il concreto rischio di indebolire il principio del pieno governo dei dati sanitari da parte del soggetto cui si riferiscono”*. La dottrina⁸⁷, qui, considera opportuna la predisposizione e forme o presidi del potere delegato che siano in grado di minimizzare il rischio sopra esposto, ad esempio: nella fase di attuazione si può prevedere che l'attribuzione della delega abbia la forma di atto pubblico, senza il quale la durata sarebbe limitata, oppure, si potrebbe predisporre un collegamento di parentela o di una relazione stabile tra delegato e delegante⁸⁸. In merito al precedentemente citato diritto di oscuramento, temporaneo o permanente, di specifici dati è necessario affermare che quest'ultimo potere permette all'interessato di “mascherare” alcune categorie di dati sensibili all'interno della propria cartella clinica elettronica per limitarne l'accesso a professionisti sanitari o prestatori di assistenza sanitaria. In base al GDPR, colui che esercita questo potere, cioè l'interessato, ha il solo diritto ad ottenere l'informazione relativa alle conseguenze che la limitazione all'accesso potrebbe avere sulla prestazione dell'assistenza sanitaria⁸⁹. Il contenuto dell'informativa dovrebbe consentire all'interessato di comprendere, in maniera corretta, i rischi legati alla limitazione da lui esercitata, ma, nella realtà, l'avvertimento è generico ed astratto e non permette all'interessato di essere pienamente consapevole dei rischi, che, non possono essere

⁸⁶ *Ibidem*.

⁸⁷ *Ibidem*.

⁸⁸ *Ivi*, p. 184.

⁸⁹ F. TRUBIANI, M. DI NUZZO, *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, 2025, p. 183.

comunicati nemmeno dal professionista sanitario, il quale, non può visionare la limitazione⁹⁰. Risulta complicato riuscire a ritenere la limitazione valida, efficace e idonea *“a fondare un principio di autoresponsabilità del paziente con assoluto esonero del professionista o del prestatore dei servizi sanitari”* considerando che, l’interessato esercita un potere rilevante, ma, in *“assenza di consapevolezza e di assistenza in merito alle conseguenze pratiche che possano derivargli”*⁹¹. In ogni caso, la problematica esposta viene considerata difficilmente superabile, considerando che, il potere di oscuramento può essere superato dalla necessità del professionista di accedere ai dati per la salvaguardia degli interessi vitali dell’interessato. Bisogna, quindi, chiedersi se l’esistenza della cartella clinica elettronica, con il relativo accesso ai dati sanitari, non giustifichi il professionista o il prestatore del servizio sanitario dallo svolgere una *“piena e completa anamnesi dell’interessato cercando di ottenere comunque tutte le informazioni rilevanti al fine del corretto svolgimento della propria prestazione senza che l’assenza di quel dato nella cartella clinica elettronica possa di per sé costituire, appunto, causa di limitazione o esonero da responsabilità”*⁹².

L’analisi della disciplina riguardante l’utilizzo secondario dei dati sanitari è fondamentale per dare coerenza e linearità al sistema nel suo complesso. L’art. 53 del Regolamento lo disciplina e individua l’obiettivo di garantire un quadro europeo adeguato al riutilizzo dei dati personali per finalità di uso secondario. Secondo l’art. 2, par. 2, l. e) del Regolamento l’uso secondario comprende gli utilizzi ulteriori a quelli riguardanti la raccolta e/o il trattamento iniziale dei dati⁹³. Tale articolo rimanda al Capo IV del Regolamento stesso, quest’ultimo presenta delle differenti finalità rispetto a quelle legate alla raccolta o produzione dei dati. Tra gli utilizzi permessi troviamo (art. 53) sanità pubblica, prevenzione e gestione delle emergenze sanitarie, innovazione dei dispositivi medici e delle tecnologie applicate alla salute, attività di ricerca scientifica e storica, di medicina personalizzata, interventi per la sicurezza e qualità delle cure. Rimane escluso l’utilizzo per finalità commerciali e azioni in contrasto con la salute individuale o pubblica, oltre alle finalità discriminatorie, il reimpiego dei dati per profilazioni sanitarie non autorizzate

⁹⁰ *Ibidem*.

⁹¹ *Ibidem*.

⁹² *Ivi*, p. 185.

⁹³ Art. 2, par. 2, l. e), Regolamento della comunità Europea 11/02/2025, n. 2025/327/UE.

e qualunque uso che re-identifichi l'interessato⁹⁴. Per ottenere l'accesso ai dati adibiti all'uso secondario è necessario avanzare una richiesta⁹⁵ con il rispetto, da parte del soggetto richiedente, di determinati requisiti di affidabilità scientifica, infrastrutture adeguate alla protezione dei dati e garanzie tecniche e organizzative conformi ai profili europei di sicurezza e anonimizzazione⁹⁶. A concedere l'autorizzazione è l'*Health Data Access Body* (HDAB): si tratta di un'autorità nazionale che si occupa di valutare la coerenza tra le richieste e le finalità previste dal Regolamento e, in caso di conformità, concede un'autorizzazione. Quest'ultima, concede all'interessato un "diritto condizionato d'uso dei dati". Non viene conferita nessuna titolarità esclusiva in capo al soggetto, i dati rimangono sotto il controllo dell'autorità pubblica che può modificarne l'accesso, l'uso o imporre condizioni⁹⁷. Dopo aver concesso e rilasciato l'autorizzazione, il soggetto richiedente deve poter accedere ai dati sanitari, per farlo, questi ultimi, vengono rilasciati in un ambiente digitale controllato e chiuso (*secure processing environment*) che ne impedisce accessi non autorizzati, copie o esportazioni vietate⁹⁸. La particolarità dell'utilizzo secondario dei dati sanitari rispetto al, già citato, utilizzo primario deriva dalla consapevolezza del valore economico dei dati, che in questa forma, diventano sia beni informativi personali (da proteggere), sia risorse pubbliche da sfruttare. Infatti, la differenza sostanziale tra i due utilizzi è che l'utilizzo primario rimane gratuito per l'interessato, mentre l'utilizzo secondario è condizionato a tariffe a carico dell'interessato stesso. Si può quindi optare per una distinzione soprattutto in merito alla tipologia dell'utilizzo, nella quale si distingue l'accesso come diritto (per quanto riguarda l'utilizzo primario) e l'accesso come servizio regolato (per quanto riguarda l'utilizzo secondario)⁹⁹. Ciò che precede è la rappresentazione del sistema disciplinato dal Regolamento, ma, nonostante la precisione del modello normativo, sono comunque possibili azioni di elusione rispetto alle norme previste (es. attacchi hacker diretti o accedere tramite terzi) in modo da ottenere fraudolentemente l'accesso ai dati. Secondo la dottrina è, quindi,

⁹⁴ F. TRUBIANI, M. DI NUZZO, *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, 2025, p. 186.

⁹⁵ A farlo, possono essere diversi soggetti come enti pubblici nazionali o europei, centri di ricerca, industrie farmaceutiche ecc.

⁹⁶ *Ibidem*.

⁹⁷ *Ibidem*.

⁹⁸ *Ibidem*.

⁹⁹ F. TRUBIANI, M. DI NUZZO, *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, 2025, p. 186.

necessario accompagnare *“la protezione normativa con un’intensa attività di vigilanza ex post, ed un efficace cooperazione internazionale in materia di sicurezza informatica e rafforzamento del potere sanzionatorio delle autorità pubbliche”*, perché, in assenza di queste garanzie *“la neutralità dell’uso secondario rischia di divenire, nei fatti, una forma occulta di selezione su base sanitaria, lesiva della parità e dignità delle persone”*¹⁰⁰. Procedendo con la disciplina dell’utilizzo secondario, il Regolamento si rifà all’art 6, par.1, l. a), c), e) o f) del GDPR in combinato con l’art. 9, par. 2, l. da g) a j) sempre del GDPR, per creare una solida base giuridica e una governance affidabile per l’utilizzo secondario dei dati sanitari elettronici. Viene istituito un *“meccanismo comune europeo”* in base al quale *“i titolari dei dati sanitari elettronici sono obbligati a mettere a disposizione i dati in loro possesso in conformità a un’autorizzazione ai dati, rilasciata da un organismo responsabile dell’accesso ai dati a fronte di una domanda di accesso promossa di un richiedente i dati che soddisfi le prescrizioni e le condizioni stabilite nel Capo IV del Regolamento”*¹⁰¹. In questo senso, *“lo spazio europeo porta al superamento di condizioni imposte a livello nazionale, comprese limitazioni e disposizioni specifiche che richiedano il consenso delle persone fisiche per quanto riguarda il trattamento per l’uso secondario dei dati sanitari elettronici personali.”*¹⁰² A livello di governance, ogni Stato membro deve istituire un organismo responsabile dell’accesso ai dati sanitari¹⁰³. Questi organismi nazionali devono cooperare nell’UE attraverso un’infrastruttura condivisa: DatiSanitari@UE (art. 75) che permette lo scambio e il riutilizzo dei dati sanitari nei differenti Stati membri. Si tratta di organismi di mediazione tra gli utenti dei dati sanitari e i titolari di questi ultimi. Gli organismi hanno compiti relativi all’autorizzazione per l’accesso ai dati e devono occuparsi de *“la preparazione e compilazione di tali dati ove richiesti dai titolari dei dati sanitari e la pseudonimizzazione o l’anonimizzazione di tali dati”*¹⁰⁴.

¹⁰⁰ Ivi, p. 187.

¹⁰¹ F. TRUBIANI, F. CASCINI, *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, 2025, p. 143.

¹⁰² Ibidem.

¹⁰³ Art. 55, Regolamento della comunità Europea 11/02/2025, n. 2025/327/UE.

¹⁰⁴ Art 57, Regolamento della comunità Europea 11/02/2025, n. 2025/327/UE.

3.2 *L'European Health Data Space*: tensioni tra interesse individuale e collettivo.

L'European Health Data Space è, quindi, un progetto ambizioso portato avanti dall'Unione Europea e mira a “*facilitare l'accesso e il controllo delle persone sui propri dati sanitari elettronici e a consentirne, promuovendone l'interoperabilità, il riutilizzo per finalità di interesse pubblico, come il sostegno alle politiche, la ricerca scientifica e la statistica. Ciò a beneficio altresì dell'innovazione e del buon funzionamento del mercato interno*”¹⁰⁵. L'art. 51 elenca le “*categorie minime di dati sanitari elettronici per l'uso secondario*”¹⁰⁶, per poi permettere ad ogni Stato membro di aggiungerne di ulteriori. L'elenco, molto ampio previsto all'art. 51, è volutamente esteso in modo da evitare problemi di armonizzazione tra normative unitarie e nazionali, visto che, si tratta di un elenco molto esaustivo. Va inoltre considerata la natura complementare del Regolamento EHDS rispetto al GDPR: ciò significa che il Regolamento va applicato e interpretato in combinato con il GDPR stesso in modo da armonizzare, il più possibile, le norme di rango europeo¹⁰⁷. La difficoltà che il legislatore europeo incontra è quella del necessario bilanciamento tra diritti. Per comprenderne la portata, basta considerare che l'utilizzo secondario dei dati sanitari è relativo a diverse finalità altamente sensibili, tra cui, il diritto alla salute e la libertà di ricerca scientifica, oltre, ai diritti alla protezione dei dati personali e alla riservatezza¹⁰⁸. Ma, ancor più problematico è il fatto che è necessario bilanciare i diritti individuali con la tutela della salute della collettività. Il caso più semplice è quello relativo ad un'emergenza sanitaria: anche di fronte al diritto dell'interessato di negare l'accesso ai propri dati sanitari, in caso di una situazione urgente, individuale o collettiva, quest'ultimo può essere sospeso in modo da accedere ai dati stessi, anche se oscurati. Infatti, “*la volontà espressa dall'interessato sui propri*

¹⁰⁵ F. TRUBIANI, C. DI SOMMA, *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, 2025, p. 168.

¹⁰⁶ Art. 51, Regolamento della comunità Europea 11/02/2025, n. 2025/327/UE.

¹⁰⁷ F. TRUBIANI, M. DI NUZZO, *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, 2025, p. 176.

¹⁰⁸ F. TRUBIANI, C. DI SOMMA, *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, 2025, p. 161.

*dati...cede di fronte alla necessità di tutelare beni di interesse superiore...*¹⁰⁹. Inoltre, il Regolamento prevede deroghe relative all'intervento dello Stato membro con misure straordinarie per ragioni di sanità pubblica. Sarà, quindi, importante evolvere la disciplina in modo da garantire la prevalenza dell'interesse collettivo, con il minor sacrificio possibile per l'interesse individuale¹¹⁰.

4. La controversa natura dei dati sanitari: tra bene pubblico e funzione di interesse generale.

Non esiste una vera e propria definizione di beni comuni, ma, questi ultimi, sono individuati come strumenti che possono portare benefici alla collettività¹¹¹. Si pone l'interrogativo se i dati sanitari, a seguito del processo di digitalizzazione, possano essere considerati tali¹¹². Il limite riguarda la tutela dei diritti dei portatori, parliamo di consenso, trattamento, riservatezza, etc.; garanzie che sono fondamentali, ma che non possono impedire il progresso scientifico. I dati sanitari sono essenziali, perché permettono una rapida evoluzione in termini di cure, comunicazione e condivisione in ambito sanitario; insomma, la circolazione di questi ultimi dovrebbe essere limitata il meno possibile. Ciò avviene già, in parte, con la tutela alla riservatezza¹¹³, ma l'obiettivo del legislatore è, anche, quello di evitare che la tutela della riservatezza del titolare dei dati possa, in qualche modo, prevalere sull'esigenza comune di perseguimento dell'interesse pubblico¹¹⁴.

L'analisi va svolta partendo dalla definizione di beni, presente all'articolo 810 del Codice civile: i beni sono le cose che possono costituire oggetto di diritti. Bisogna distinguere,

¹⁰⁹ F. TRUBIANI, M. DI NUZZO, *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, 2025, p. 188.

¹¹⁰ *Ivi*, p. 189.

¹¹¹ F. TRUBIANI, R. CARLEO, *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, 2025, p. 193.

¹¹² Sul tema si veda altresì G. Di Filippo, *I dati come beni giuridici. Dati personali e dati non personali: regime di appartenenza e di circolazione*, in P. Stanzione (a cura di), *I poteri privati delle piattaforme e le nuove frontiere della privacy*, Giappichelli, Torino, 2022. E. Cremona, *Quando I dati diventano beni comuni: modelli di data sharing e prospettive di riuso*, in *Riv. it. inform. dir.*, 2023, 2, pp. 111-130.

¹¹³ Es. favorendo la circolazione pseudonimizzata, anonimizzata o de-identificata dei dati.

¹¹⁴ *Ivi*, p. 194.

quindi, i beni e le cose. Per farlo, è necessario considerare l'esempio relativo alla disciplina del patrimonio culturale che permette ai beni culturali di essere considerati come tali solo successivamente all'apposizione del vincolo, dato che, precedentemente all'apposizione, vengono considerati come cose. La differenziazione poggia “*non sull'idoneità della cosa a costituire oggetto di diritti (ex art. 810 c.c.), ma sull'intensità del suo legame con il soddisfacimento dell'interesse pubblico*”¹¹⁵. Da questo punto di vista, ci si chiede se i dati in possesso della pubblica amministrazione possano essere considerati beni a destinazione pubblica. Per capirlo, bisogna definire il dato, quest'ultimo è “*qualunque elemento (espresso, tra l'altro, in forma di numero, testo, immagine, video o audio), che può essere riprodotto e memorizzato con formati diversi (tanto digitali, quanto materiali) e, sebbene abbia un valore proprio, può assumere significati differenti in ragione alla sua contestualizzazione*”¹¹⁶. Si tratta di una definizione che si differenzia da quella di dato personale, già riportata in precedenza. La questione va posta sull'esercizio di un diritto della personalità sul proprio patrimonio informativo da parte dell'interessato e non, sulla semplice considerazione del dato personale come un bene. Ovviamente, gli enti pubblici hanno e possiedono un patrimonio informativo immenso composto da informazioni di diverso tipo utilizzate nello svolgimento delle attività istituzionali¹¹⁷, e, “*il fatto stesso che le informazioni entrino nella disponibilità di soggetti vincolati, nello svolgimento della loro attività, al perseguimento dell'interesse della collettività rende i dati in loro possesso “a destinazione pubblica”*”¹¹⁸. La destinazione pubblica può essere di tipo oggettivo, nel momento in cui la collettività sia titolare di un diritto di accesso ai dati, diritto al quale corrisponde il dovere dell'amministrazione di renderli fruibili. Oppure, può essere di tipo soggettivo, nel momento in cui l'autorità sia depositaria di dati senza l'obbligo di metterli a disposizione della collettività. Da qui, sorge un nuovo problema, quello relativo alla titolarità dei dati: è incerto se appartengano al soggetto privato di riferimento o a quello pubblico. Per quanto riguarda l'ente pubblico, l'appartenenza può essere riscontrata nel

¹¹⁵ A. SIMONATI, *I dati personali in possesso della pubblica amministrazione: beni a destinazione pubblica?*, in Ceridap, 2025, 3, pp. 208-238.

¹¹⁶ *Ibidem*.

¹¹⁷ Sui dati detenuti dalla pubblica amministrazione si veda S. FRANCA, *I dati personali nell'amministrazione pubblica*, Trento, 2023.

¹¹⁸ *Ibidem*.

regime dei beni pubblici in senso stretto, per il soggetto privato, i dati detenuti dalla pubblica amministrazione potrebbero essere assimilati ai beni privati di interesse pubblico. Secondo la Corte di Cassazione, in merito alla demanialità, quest'ultima *“esprime una duplice appartenenza, alla collettività ed al suo ente esponentiale, dovendosi intendere la titolarità in senso stretto come appartenenza di servizio, nel senso che l'ente esponentiale può e deve assicurare il mantenimento delle specifiche rilevanti caratteristiche del bene e la sua concreta possibilità di fruizione”*¹¹⁹. Si può, quindi, cercare di affermare che i dati in possesso della pubblica amministrazione possano assumere un'attitudine sia patrimonialistica che solidaristica e che, di conseguenza, *“la (parziale) appartenenza dei dati all'autorità, allorché essa ne entra in possesso, è strumentale o alla loro fruizione da parte della comunità, oppure comunque al loro utilizzo nel perseguimento dell'interesse generale”*¹²⁰.

¹¹⁹ Cass. civ., s.u., 14 febbraio 2011, n. 3665.

¹²⁰ *Ibidem*.

CAPITOLO II

LA GESTIONE DEL DATO SANITARIO TRA *GOVERNANCE* E INNOVAZIONE

SOMMARIO: 1. La sanità digitale: un'introduzione - 2. La nuova *governance* dei dati sanitari tra diritto dell'Unione europea e disciplina interna - 2.1 Il ruolo della Commissione Europea e l'intervento normativo delle autorità italiane nel delicato equilibrio di atti di *hard* e *soft law* - 3. La digitalizzazione dei servizi sanitari: il ruolo di AGENAS - 4. Verso una nuova gestione dei dati sanitari: *OpenData*, principi *Fair* e *Trust* - 5. La telemedicina come strumento di *e-Health* - 6. Tecnologia blockchain e telemedicina quali strumenti per una circolazione sicura del dato sanitario - 7. Strumenti di *e-Health*: il Fascicolo Sanitario Elettronico e la Cartella Clinica Elettronica - 7.1 Istituzione dell'Ecosistema dei Dati Sanitari in Italia e il parere negativo da parte del Garante della *Privacy* - 7.2 Il FSE e il problema dell'interoperabilità - 8. Conclusioni

1. La sanità digitale: un'introduzione.

La possibilità di accedere, elaborare e condividere i dati sanitari si configura oggi come una risorsa strategica fondamentale per l'innovazione del Servizio Sanitario Nazionale. A livello nazionale, il processo di trasformazione digitale della sanità si è tradotto, in particolare a partire dal 2008, nell'adozione di una strategia orientata alla diffusione dell'*e-Health* quale strumento ordinario a disposizione di operatori, pazienti e cittadini, con l'obiettivo di elevare la qualità dell'assistenza e l'efficienza del sistema¹²¹. La spinta verso la realizzazione di servizi integrati in rete è stata ulteriormente alimentata dalle tendenze sociodemografiche in atto e dalla crescente esigenza di ottimizzare l'erogazione delle prestazioni; in questo scenario, strumenti come il Fascicolo Sanitario Elettronico (FSE) e la telemedicina hanno assunto un ruolo centrale. Successivamente, la crisi pandemica da COVID-19 ha evidenziato con drammatica urgenza la necessità di accedere, scambiare e valorizzare i dati sanitari in modo tempestivo. In tale contesto, l'impiego delle risorse del Piano Nazionale di Ripresa e Resilienza (PNRR) si è rivelato decisivo. In particolare, la Missione VI del PNRR nasce dall'esigenza di “*colmare il divario tra le disparità territoriali ed offrire maggiore integrazione tra i servizi sanitari*”

¹²¹ A. MAZZA LABOCCETTA, *Telemedicina: sfide, problemi, opportunità*, in *Federalismi.it*, 2023, p. 146.

nei diversi ambiti assistenziali. La Componente 1, dedicata a “Reti nazionale, puntae, puntaintermedie e telemedicina per l’assistenza territoriale”, tra gli altri obiettivi diretti a potenziare il Servizio sanitario nazionale ,punta ad allineare i servizi ai bisogni della comunità e dei pazienti e a rafforzare le strutture e i servizi sanitari di prossimità e i servizi domiciliari, e in questa direzione si propone di “sviluppare la telemedicina e superare la frammentazione e la mancanza di omogeneità dei servizi sanitari offerti sul territorio” e di rafforzare “soluzioni di telemedicina avanzate a sostegno dell’assistenza domiciliare”¹²². Si tratta della Missione Salute, alla quale il PNRR ha destinato 15,63 miliardi di euro (misura pari all’8,16% dell’importo totale) per sostenere riforme e investimenti a beneficio del Servizio Sanitario Nazionale. Gli interventi della Missione si dividono in due aree principali: ridisegnare la rete di assistenza sanitaria territoriale con professionisti e prestazioni disponibili in modo capillare su tutto il territorio nazionale, per una sanità che sia vicina e prossima alle persone; e innovare il parco tecnologico ospedaliero, digitalizzare il SSN, investire in ricerca e formazione del personale sanitario per una sanità più sicura, equa e sostenibile. Oltre alla già citata Componente 1, incentrata sul rafforzamento dei servizi e delle prestazioni erogate sul territorio, risulta fondamentale la Componente 2: “Innovazione, ricerca e digitalizzazione del Servizio Sanitario Nazionale”. Gli interventi relativi a tale Componente sono incentrati sul rinnovamento e ammodernamento delle strutture tecnologiche e digitali esistenti. Si vuole ottenere ciò completando la diffusione del Fascicolo Sanitario Elettronico e migliorando la capacità di erogazione e monitoraggio dei Livelli Essenziali di Assistenza (LEA) attraverso più efficaci sistemi informativi, oltre ad un potenziamento della ricerca scientifica¹²³.

Muovendo da queste premesse e alla luce della nozione di dato sanitario precedentemente delineata, il presente capitolo intende analizzare la dimensione più strettamente organizzativa della sanità digitale: la trattazione si concentrerà sull’architettura della *governance* dei dati, sui principali attori istituzionali coinvolti e sui concreti strumenti operativi dell’*e-Health*.

¹²² A. MAZZA LABOCCETTA, *Telemedicina: sfide, problemi, opportunità*, in *Federalismi.it*, p. 149.

¹²³ MINISTERO DELLA SALUTE, *Piano nazionale di ripresa e resilienza. Cos'è la Missione Salute*, [Ministero della Salute](#).

2. La nuova *governance* dei dati sanitari tra diritto dell'Unione europea e disciplina interna.

Nel capitolo precedente è emerso quanto la digitalizzazione sia entrata sempre di più a far parte della vita dei cittadini e come questa innovazione abbia spinto l'Unione Europea a regolamentare le nuove tecnologie. L'intervento europeo è divenuto fondamentale per *“favorire lo sviluppo tecnologico, ma anche a garantire che i diritti fondamentali della persona siano tutelati nel contesto online con la stessa intensità assicurata nel mondo offline”*¹²⁴. Ora, dato che gli operatori economici digitali privati si trovano in una situazione di vantaggio che permette loro di mantenere il potere economico in una cerchia ristretta e, quindi, di incidere pesantemente sulla sfera pubblica e sui diritti individuali, è stato necessario un intervento a livello sovranazionale. Questo perché *“le logiche del mercato digitale, fondato sull'uso gratuito dei servizi e sulla valorizzazione economica dei dati personali, hanno reso obsoleta la normativa antitrust di tipo classico, basata sulla teoria del prezzo e sull'analisi dei mercati rilevanti”*¹²⁵. L'intervento pubblico è, quindi, fondamentale per imporre limiti al potere di questi soggetti in modo da salvaguardare il sistema europeo. Questa spinta ha portato il legislatore a adottare Regolamenti, tra cui il già richiamato GDPR. Allo stesso tempo, l'interventismo dell'UE ha portato anche ad un accentramento delle funzioni di esecuzione normativa e amministrativa *“sempre più frequentemente sottratte agli Stati membri e attribuite alla Commissione europea”*¹²⁶. Tutto ciò ha un rilievo particolare dal punto di vista del diritto sanitario e dello, anch'esso già citato, Spazio Europeo dei Dati Sanitari. L'attività di regolazione incontra, infatti, il limite dell'obsolescenza normativa nel momento in cui si confronta con l'evoluzione tecnologica. In questo senso, la regolazione deve essere flessibile, in modo da potere cambiare ed essere modificabile. In tutto ciò è fondamentale mantenere un equilibrio tra le fonti primarie, più rigide e, quindi, più adatte ad accompagnare un'evoluzione della tecnica, e le fonti secondarie, più adatte a

¹²⁴ L. DEL CORONA, A. GIUBILEI, M. LADU, V. MONTOSZI, *Intelligenza artificiale, sanità digitale ed esigenze di regolazione*, in *Federalismi.it.*, 2025, p. 3.

¹²⁵ *Ivi*, p. 4.

¹²⁶ *Ibidem*.

regolamentare gli aspetti di dettaglio¹²⁷. Il ricorso a fonti secondarie, elaborate a livello unionale, è preferibile visto che l'esigenza di flessibilità si accompagna a quella di accentrimento dell'intervento pubblico¹²⁸. Deriva da queste esigenze l'utilizzo del ricorso alla Commissione Europea¹²⁹, in questo senso *“si tratta di un modello che deroga alla regola dell'attuazione nazionale, rispondendo a precise necessità: da un lato, garantire l'uniformità dell'azione regolatoria nel territorio UE; dall'altro, evitare l'obsolescenza delle norme tramite l'utilizzo di fonti secondarie dotate di flessibilità”*¹³⁰. Attraverso l'emanazione dell'EHDS, la tendenza a fare ricorso ai poteri della Commissione è cresciuta sempre più, ma ciò ha sollevato sempre più dubbi relativi al rischio di far prendere delle decisioni che comportano l'esercizio di discrezionalità politica ad un organo non direttamente rappresentativo come la Commissione¹³¹. Ma, a causa della natura politica propria della Commissione nonché del legame fiduciario con il Parlamento europeo, è possibile ravvisare una legittimazione *“all'esercizio di poteri normativi che implicino l'esercizio di una discrezionalità non puramente tecnica”*¹³². Ora, è necessario riportare come la maggior parte delle regole necessarie all'attuazione della disciplina generale impartita dall'UE, in merito alla società digitale, siano elaborate da soggetti privati tramite atti di autoregolazione e co-regolazione¹³³. Ciò, in alcuni casi, comporta l'attribuzione di funzioni in capo alla Commissione Europea¹³⁴. È il caso delle norme tecniche armonizzate che, grazie al meccanismo della presunzione di conformità¹³⁵ acquisiscono forza *“quasi vincolante”*¹³⁶. Il rinvio ai codici di condotta, strumenti di *soft-law* che promuovono comportamenti conformi ai principi normativi, è considerato un atto

¹²⁷ *Ivi*, p. 5.

¹²⁸ *Ibidem*.

¹²⁹ Il ricorso agli atti della Commissione si riscontra in quasi tutti i recenti regolamenti in materia digitale.

¹³⁰ L. DEL CORONA, A. GIUBILEI, M. LADU, V. MONTOSI, *Intelligenza artificiale, sanità digitale ed esigenze di regolazione*, in *Federalismi.it*, 2025, p. 5.

¹³¹ *Ibidem*.

¹³² *Ibidem*.

¹³³ G. PISTORIO, *La co-regolazione nell'ecosistema digitale tra etero-regolazione e auto-regolazione. Questioni definitorie*, in *Osservatorio sulle fonti*, n. 1, 2024, pp. 137 ss.

¹³⁴ Ricordo che la Commissione non si occupa dell'elaborazione diretta della norma, ma può rivestire un ruolo di rilievo nella produzione normativa.

¹³⁵ Meccanismo in base al quale chi aderisce alle norme tecniche armonizzate si presume abbia tenuto un comportamento conforme agli obblighi di legge.

¹³⁶ *Ivi*, p. 6.

di co-regolazione¹³⁷. Tuttavia, l'attività di rinvio degli atti ai privati pone problematiche legate alla trasparenza e all'accessibilità delle norme, è, anche, per questo motivo che è possibile ipotizzare al fatto che *“in futuro si assista a una progressiva riduzione del ricorso all'autoregolazione e alla co-regolazione, a vantaggio di una maggiore ricorso agli atti secondari direttamente adottati dalla Commissione”*. Lo Spazio Europeo dei Dati Sanitari interviene in questo senso, *“avendo sostanzialmente sostituito i rinvii alle norme armonizzate con il riferimento a specifiche tecniche da inserirsi negli atti esecutivi della Commissione europea”*¹³⁸. Oltre alla centralizzazione normativa si ha un consolidamento delle competenze amministrative in capo dalle istituzioni europee. Uno dei primi segnali è stata l'istituzione del Comitato europeo per la protezione dei dati¹³⁹, quale organo di raccordo e coordinamento tra le autorità nazionali, incaricato di assicurare uniformità di applicazione e coerenza interpretativa. Il rafforzamento del ruolo della Commissione c'è poi stato nel DSA, dove viene stabilito che la Commissione dispone di poteri diretti di vigilanza e di intervento nei confronti delle piattaforme di grandi dimensioni e nel *Digital Markets Act* (“DMA”), secondo il quale, la Commissione è l'unica autorità responsabile della designazione dei *gatekeeper* e del controllo delle loro condotte¹⁴⁰. Il rafforzamento dei poteri si nota anche nell'*AI Act* rispetto alle funzioni di controllo e supervisione sui sistemi ad alto rischio, e nel Regolamento sullo spazio europeo dei dati sanitari, che assegna alla Commissione europea compiti di gestione delle infrastrutture digitali comuni, quale la piattaforma *MyHealth@EU*, già vista in precedenza¹⁴¹. Ma, non è

¹³⁷ Sulla tendenza a forme di co-regolazione nei mercati digitali cfr. E. Bruti Liberati, Poteri privati e nuova regolazione pubblica, in *Dir. pubbl.*, 2023, 1, pp. 475-532. O. Pollicino, I codici di condotta tra self-regulation e hard law: esiste davvero una terza via per la regolazione digitale? Il caso della strategia europea contro la disinformazione on line, in *Rivista trimestrale di diritto pubblico*, 4, 2022, p. 1051; A. Simoncini, La co-regolazione delle piattaforme digitali, in *Rivista trimestrale di diritto pubblico*, 4, 2022, p. 1031. In materia di salute C. Di Costanzo, La co-regolazione delle nuove tecnologie nel settore della salute: ambiti di applicazione, caratteristiche e prospettive, in *Osservatorio sulle fonti*, 2024, 1, pp. 285-316.

¹³⁸ *Ibidem*.

¹³⁹ Sul ruolo e sui poteri esercitabili dal Comitato EDPB cfr. L. BOLOGNINI, P. BONETTI, E. GUARNIERI, *The super powers of the European Data Protection Board (EDPB) and the principle of due administrative procedure*, in *Diritto, Economia e Tecnologie della Privacy*, 2025, 1, pp. 1-25; F. PARODO, *La tutela del diritto alla protezione dei dati personali: l'effettività dei rimedi e il ruolo nomofilattico del Comitato europeo per la protezione dei dati personali*, in *Federalismi.it*, 2021, 25, pp. 106-151; C. FIGLIOLIA, M. MACCHIA, *Autorità per la “privacy” e Comitato europeo nel quadro del “General Data Protection Regulation”*, in *Giorn. dir. amm.*, 4, 2018, pp. 423-438.

¹⁴⁰ *Ivi*, p. 7.

¹⁴¹ L. DEL CORONA, A. GIUBILEI, M. LADU, V. MONTOSZI, *Intelligenza artificiale, sanità digitale ed esigenze di regolazione*, 2025, in *Federalismi.it*, 2025, p.7.

semplice garantire la fondatezza delle competenze tecniche adeguate da parte della Commissione successivamente all'estensione delle funzioni amministrative in capo a quest'ultima. Per cercare di arginare il problema sono stati istituiti organismi di supporto tecnico e consultivo (es. Comitato europeo per i servizi digitali o il Consiglio europeo per l'IA) in modo da assistere la Commissione nell'espletamento delle sue funzioni¹⁴². Un'ulteriore problematica relativa all'esercizio di funzioni amministrative in capo alla Commissione potrebbe derivare dal rischio di compromettere l'imparzialità della funzione amministrativa a causa del carattere politico della Commissione. Infine, va considerato che l'attribuzione di competenze normative e amministrative alla Commissione ha come conseguenza la produzione di effetti significativi nel processo di integrazione europea, a causa del consolidamento del ruolo della Commissione di *“principale titolare del potere esecutivo dell'UE”*¹⁴³. Di fatti, *“l'affermarsi della Commissione come esecutivo dell'Unione europea impone una riflessione complessiva sul sistema istituzionale europeo e sull'equilibrio dei poteri al suo interno, al fine di garantire un'adeguata ripartizione delle funzioni tra i diversi organi”*¹⁴⁴.

In conclusione, l'accentramento delle funzioni normative ed esecutive in capo alla Commissione Europea risponde alla priorità assoluta di tutelare i diritti fondamentali dei cittadini di fronte allo strapotere economico delle *Big Tech* e al rischio di obsolescenza normativa.

Per la sanità digitale, tale svolta garantisce una cornice di protezione uniforme a livello dell'Unione Europea e la flessibilità necessaria per adeguarsi al rapido sviluppo tecnologico mediante fonti secondarie. Ciò produce rilevanti conseguenze sul piano della *governance*: la Commissione diventa il principale organo esecutivo europeo dotato di poteri diretti di vigilanza e gestione dei rischi, superando la dipendenza dall'autoregolazione privata. Tuttavia, questa concentrazione solleva dubbi circa l'imparzialità amministrativa e la discrezionalità politica, rendendo indispensabile il supporto di organismi tecnici consultivi. Questo modello si collega alla gestione del dato sanitario tramite il Regolamento sullo Spazio Europeo dei Dati Sanitari (EHDS): l'UE ha infatti affidato alla Commissione la gestione delle infrastrutture digitali comuni (come

¹⁴² *Ibidem.*

¹⁴³ *Ibidem.*

¹⁴⁴ *Ibidem.*

MyHealth@EU) e la definizione diretta delle specifiche tecniche, sottraendo il controllo dei dati di salute agli standard privati.

2.1. Il ruolo della Commissione Europea e l'intervento normativo delle autorità italiane nel delicato equilibrio tra atti di *hard* e *soft law*

Dopo aver analizzato il “nuovo” ruolo della Commissione Europea è necessario affrontare la questione relativa alla sanità digitale, ma interessandoci alla normativa nazionale e agli interventi delle autorità amministrative italiane in merito alla governance dell'IA sanitaria.

La sempre più frenetica adozione di strumenti di IA nel settore sanitario “*da una parte, introduce nuove opportunità di efficienza, personalizzazione e accessibilità delle prestazioni sanitarie, ma dall'altra solleva interrogativi profondi in termini di responsabilità, trasparenza, equità e tutela dei diritti fondamentali*”¹⁴⁵. Partendo da questa affermazione, l'esigenza di un nuovo assetto regolatorio è molto presente: quest'ultimo deve essere “*prudente ma flessibile, attento a non limitare o imbrigliare gli sviluppi delle nuove tecnologie, senza tuttavia lasciarli privi di controllo*”¹⁴⁶.

La risposta dell'UE è arrivata tramite l'emanazione di strumenti di *hard law*, tra cui il GDPR e il Regolamento EHDS, già richiamati. La complessità tecnico-scientifica degli strumenti tecnologici utilizzati, la specificità dei diversi settori interessati dal fenomeno nonché la notevole eterogeneità tra gli Stati membri (in termini di capacità amministrative, grado di digitalizzazione, cultura giuridica e sensibilità etica), sono i fattori che hanno reso evidente come gli strumenti di *hard law*, da soli, non siano sufficienti per regolare l'intera disciplina sull'IA¹⁴⁷. Secondo la dottrina, l'utilizzo di sistemi di IA e di algoritmi nel settore sanitario solleva tre tipi di criticità: “*epistemiche*”, in merito all'affidabilità e la trasparenza dei sistemi, “*etico-giuridiche*”, per quanto

¹⁴⁵ *Ivi*, p. 10.

¹⁴⁶ *Ibidem*.

¹⁴⁷ *Ivi*, p. 11.

riguarda le questioni di responsabilità in caso di errori diagnostici algoritmici e sulla garanzia del consenso informato, e, come ultime, “*tecnicoprocedurali*”, in merito ai minimi requisiti in termini di sicurezza, robustezza e protezione dei dati che i sistemi di IA devono garantire¹⁴⁸. Inoltre, a causa della continua evoluzione tecnologica, normare questi sistemi e, soprattutto, farlo per tempo, è molto complicato. Osservando questo punto di vista gli interventi di *hard law*, come i Regolamenti, non sono abbastanza adeguati a regolare il fenomeno dell’IA, visto che si tratta di questioni “*che richiedono interventi regolatori, da una parte, tempestivi, dall’altra, che siano frutto di un’attenta ponderazione e di una costante rivalutazione proprio in funzione dei delicati e complessi equilibri che si rischia di compromettere*”¹⁴⁹. In relazione a tale profilo, si avverte una sempre più crescente necessità di un’architettura regolatoria “*multilivello*” in grado di accostare le, già presenti, fonti di *hard-law* con delle fonti di *soft-law*, più adattabili rispetto ai continui cambiamenti dei sistemi di IA. In questo contesto le autorità di governo nazionali e le autorità amministrative indipendenti assumono un ruolo sempre più importante. Difatti, a queste ultime spetta il compito di “*vigilare sul rispetto dei diritti costituzionali e sovranazionali, in modo da garantire che l’innovazione tecnologica in ambito sanitario non produca nuove forme di esclusione o diseguaglianza*”, e di svolgere “*un ruolo cruciale nel fornire linee guida, regolamenti attuativi, pareri tecnici e norme secondarie che rendono applicabili nella pratica le previsioni legislative europee, tenendo anche conto delle diversità afferenti a ciascuno Stato che, si ricorda, conserva competenza legislativa in materia sanitaria*”¹⁵⁰. In Italia già diversi attori hanno contribuito alla regolazione della sanità digitale: innanzitutto, il Ministero della Salute, il quale, in linea con la Strategia nazionale per la Sanità Digitale ha approvato le Linee Guida per i servizi di Telemedicina¹⁵¹ attraverso le quali vengono definiti i modelli e gli standard per lo sviluppo dell’assistenza territoriale nel Servizio Sanitario Nazionale, oltre alla promozione in merito all’utilizzo dell’intelligenza artificiale per migliorare l’efficienza e l’accessibilità dell’assistenza sanitari¹⁵². L’ultimo intervento a livello

¹⁴⁸ L. DEL CORONA, A. GIUBILEI, M. LADU, V. MONTOSI, *Intelligenza artificiale, sanità digitale ed esigenze di regolazione*, 2025, in *Federalismi.it.*, 2025, p.11.

¹⁴⁹ *Ivi*, p, 12.

¹⁵⁰ *Ibidem*.

¹⁵¹ Predisposte da AGENAS, e il D.M. n. 77/2022.

¹⁵² *Ivi*, p. 13.

temporale è stato l'approvazione della legge n. 132/2025 in materia di intelligenza artificiale¹⁵³, in linea con il Regolamento europeo sull'IA (*AI Act*), che affronteremo più avanti. Viene affidato un ruolo importante ad autorità nazionali quali l'Agenzia per l'Italia Digitale (AgID) e all'Agenzia per la Cybersicurezza Nazionale (ACN), alle quali spettano compiti di vigilanza, coordinazione e monitoraggio in merito all'attuazione della disciplina, in raccordo con il Governo e altre autorità indipendenti, soprattutto il Garante per la protezione dei dati personali¹⁵⁴. Si riscontra anche il contributo dell'Agenzia Italiana del Farmaco (AIFA) nel regolare l'uso dell'IA nelle terapie farmacologiche e i due provvedimenti rappresentati dal “Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di Intelligenza Artificiale”, approvato dal Garante per la protezione dei dati personali e le “Linee guida per l'adozione di IA nella pubblica amministrazione”, adottate dall'AgID. Si tratta di atti di normazione secondaria adeguati al completare la normativa primaria¹⁵⁵. In particolare, le Linee Guida AgID, “*si configurano come strumenti di soft law finalizzati a fornire indicazioni operative alle amministrazioni, in questo caso sanitarie, per l'implementazione di sistemi di IA conformi al quadro normativo vigente e a individuare uno specifico modello di governance aziendale*”, oltre ai “*requisiti tecnici stringenti che i sistemi di IA destinati all'utilizzo nel settore sanitario devono rispettare, prestando attenzione anche alla documentazione tecnica che deve accompagnare ogni fase dello sviluppo e dell'implementazione dei sistemi di IA, garantendo la tracciabilità delle decisioni algoritmiche*”¹⁵⁶

3. La digitalizzazione dei servizi sanitari: il ruolo di AGENAS.

Considerando la, sempre più crescente, importanza e centralità delle autorità nazionali, diventa fondamentale affrontare un'importante novità sul piano della *governance* dei dati

¹⁵³ L. 23 settembre 2025, n. 132.

¹⁵⁴ Sul ruolo del Garante nella sanità digitale si veda G. Cerrina Feroni, Sanità digitale, tra innovazione e tutela dei dati sanitari: il ruolo del garante privacy, in Corti Supreme e Salute, 2025, 1, pp. 225-251.

¹⁵⁵ L. DEL CORONA, A. GIUBILEI, M. LADU, V. MONTOSI, *Intelligenza artificiale, sanità digitale ed esigenze di regolazione*, 2025, in Federalismi.it., 2025, p.14.

¹⁵⁶ *Ibidem*.

sanitari quale l'istituzione dell'Autorità di sanità digitale nazionale¹⁵⁷. Quest'ultima è stata istituita nel 1993¹⁵⁸ e, ad opera della legge 28 marzo 2022, n. 25, ha assunto il ruolo di autorità di sanità digitale nazionale. L'obiettivo è quello di garantire omogeneità e coerenza nell'attuazione delle politiche di digitalizzazione del Servizio Sanitario Nazionale.

Prima di affrontare l'argomento è necessario fare una premessa in merito alla centralità dei dati personali nella digitalizzazione dei dati sanitari. La digitalizzazione della sanità incide profondamente sul rapporto tra i cittadini e i sistemi sanitari, sia in merito allo sviluppo di sistemi di IA per diagnosi e svolgimento delle cure, sia per l'utilizzo dei dati sanitari. Infatti, il paziente *“tende a configurarsi sempre meno come destinatario passivo di prestazioni e sempre più come soggetto attivamente coinvolto nei processi di cura”*¹⁵⁹. La tecnologia passa quindi da mero mezzo a *“fattore costitutivo della salute contemporanea”*¹⁶⁰. Senza i dati il sistema sanitario non può funzionare, è quindi importante affermare che per sfruttare i mezzi, sempre più innovativi, che la tecnologia permette di utilizzare in modo da migliorare i servizi di cura e assistenza sanitaria è necessario valorizzare i dati sanitari e favorirne la circolazione, anche se, questo comporta un aumento dei rischi legati al movimento dei dati che portano con loro informazioni relative alla salute. In merito a questa nuova visione interviene il Regolamento EHDS: infatti, *“la circolazione del dato cessa di essere demonizzata quale mera opportunità economica da limitare per non compromettere la riservatezza degli interessati, a fronte delle possibilità che essa offre in termini di innovazione, concorrenza e accesso a servizi pubblici essenziali.”*¹⁶¹ Ed è in questo clima di innovazione che il legislatore europeo istituisce l'Autorità di sanità digitale, AGENAS. Quest'ultima è disciplinata dall'art. 19 del Regolamento, il quale stabilisce che gli Stati membri sono tenuti a istituire o designare l'Autorità come soggetto istituzionalmente responsabile dell'attuazione e dell'applicazione delle disposizioni del regolamento. In combinato con il considerando n. 30, il compito principale dell'Autorità è quello di pianificare e attuare le norme per

¹⁵⁷ Sull'architettura dei poteri pubblici nel settore e sul ruolo di Agenas si veda F. GIGLIONI, *Manuale di diritto sanitario*, Molfetta, 2024, pp. 69-71.

¹⁵⁸ Tramite d.lgs. n. 266/1993.

¹⁵⁹ *Ivi*, p. 19.

¹⁶⁰ *Ibidem*.

¹⁶¹ *Ivi*, p. 21.

l'accesso ai dati sanitari elettronici, per la loro trasmissione e per l'applicazione dei diritti delle persone fisiche e dei professionisti sanitari tutelati dal regolamento¹⁶². Quest'ultimo disciplina poteri complessi in capo alle autorità. Partendo dall'art. 19, par. 1, all'Autorità spetta garantire l'attuazione dei diritti e degli obblighi relativi all'uso primario dei dati sanitari, adottando le soluzioni tecniche necessarie a livello nazionale, regionale o locale e *“stabilendo le norme e i meccanismi pertinenti”*¹⁶³.

Il Regolamento si sofferma in particolare sui profili legati alla gestione dei dati sanitari: l'Autorità deve *“garantire l'attuazione a livello nazionale del formato europeo di scambio delle cartelle cliniche elettroniche, in cooperazione con le autorità nazionali e i portatori di interesse”*¹⁶⁴, *“dare attuazione alle prescrizioni in materia di interoperabilità e sicurezza dei dati sanitari elettronici”*¹⁶⁵ e *“svolgere attività di vigilanza del mercato delle cartelle cliniche elettroniche, avendo cura nel contempo di evitare qualsiasi conflitto di interessi”* alla lettera i). L'art. 19 chiede, inoltre, agli Stati membri di informare *“la Commissione in merito all'identità delle autorità di sanità digitale entro il 26 marzo 2027”*¹⁶⁶. In questo senso, il legislatore italiano si è già mosso attraverso l'emanazione della recente legge 23 settembre 2025, n. 132, recante *«Disposizioni e deleghe al Governo in materia di intelligenza artificiale»*. Quest'ultima prevede norme importanti in merito alla sanità digitale e sullo strumento del fascicolo sanitario elettronico, stabilendo che, attraverso uno o più decreti del Ministro della salute, vengano disciplinate le *“soluzioni di intelligenza artificiale”* che supportano le finalità perseguite dal fascicolo sanitario elettronico¹⁶⁷. Seguendo gli scopi perseguiti dall'EHDS, il legislatore italiano ha previsto che *“per il supporto alle finalità di cura, e in particolare per l'assistenza territoriale, è istituita una piattaforma di intelligenza artificiale. La progettazione, la realizzazione, la messa in servizio e la titolarità della piattaforma [...] sono attribuite all'AGENAS in qualità di Agenzia nazionale per la sanità digitale”*¹⁶⁸. L'art. 10 della legge 132/2025 impone all'AGENAS di erogare servizi di supporto ai professionisti sanitari, ai medici

¹⁶² L. DEL CORONA, A. GIUBILEI, M. LADU, V. MONTOSZI, *Intelligenza artificiale, sanità digitale ed esigenze di regolazione*, 2025, in *Federalismi.it.*, p.22.

¹⁶³ Art. 19, par. 2, l. a), Regolamento della comunità Europea 11/02/2025, n. 2025/327/UE.

¹⁶⁴ Art. 19, par. 2, l. g), Regolamento della comunità Europea 11/02/2025, n. 2025/327/UE.

¹⁶⁵ Art. 19, par. 2, l. j), Regolamento della comunità Europea 11/02/2025, n. 2025/327/UE.

¹⁶⁶ Art. 19, par. 1, Regolamento della comunità Europea 11/02/2025, n. 2025/327/UE.

¹⁶⁷ *Ivi*, p. 24.

¹⁶⁸ *Ibidem*.

nella pratica clinica quotidiana e agli utenti per l'accesso ai servizi, divenendo sostanzialmente, il titolare del trattamento dei dati sanitari. Inoltre, ad AGENAS spetta specificare i tipi di dati trattati e le operazioni svolte nella piattaforma, oltre all'adeguamento di misure tecniche e organizzative per arginare i rischi¹⁶⁹. Il legislatore italiano ha quindi designato AGENAS nello svolgere i compiti previsti dall'art. 19 dell'EHDS alle Autorità nazionali di sanità digitale. Ma, la particolarità di AGENAS in Italia è che non si tratta di un'autorità amministrativa indipendente, ma di una agenzia sottoposta alla vigilanza del Ministero della salute. Le motivazioni che hanno spinto il legislatore a compiere questa scelta derivano dalla volontà di valorizzare un ente già esistente, evitando di crearne uno *ex novo*. Ciò comporta delle problematiche: ci si chiede se l'AGENAS sia in grado di svolgere un potere regolatorio (attribuito dall'EHDS all'Autorità di sanità nazionale) rispetto allo svolgimento di funzioni tecniche e gestionali; è poi presente il rischio di sovrapposizioni con attività svolte da soggetti come il Ministero e il Garante oltre ai dubbi relativi alla finanza dell'Autorità. Infatti, l'EHDS chiede che le Autorità abbiano delle adeguate risorse umane e finanziarie, ma la legge italiana prevede che le nuove attribuzioni AGENAS siano esercitate gratuitamente¹⁷⁰. Per risolvere i precedenti dubbi sarà necessario attendere l'approvazione dei decreti attuativi, per ora ci basta affermare che il nuovo impianto regolatorio *“sembrerebbe richiedere all'AGENAS, in qualità di Autorità di sanità digitale, di trasformarsi da mero organo tecnico-operativo con funzioni gestionali a “cerniera istituzionale” tra digitalizzazione dei servizi sanitari e salvaguardia delle garanzie costituzionali a tutela della persona.”*¹⁷¹ Si tratta, senza dubbio, di un progetto ambizioso, che però, è di fondamentale importanza per preservare il ruolo dei soggetti pubblici in un settore sempre più dominato dai privati.

4. Verso una nuova gestione dei dati sanitari: *OpenData*, principi *Fair e Trust*.

¹⁶⁹ L. DEL CORONA, A. GIUBILEI, M. LADU, V. MONTOSI, *Intelligenza artificiale, sanità digitale ed esigenze di regolazione*, in *Federalismi.it.*, 2025, p.25.

¹⁷⁰ *Ibidem*.

¹⁷¹ *Ibidem*.

L'efficacia dell'operato delle nuove Autorità di sanità digitale e la realizzazione di un simile progetto istituzionale dipendono inevitabilmente dalla qualità e dalle modalità di gestione della materia prima su cui esse sono chiamate a vigilare: i dati sanitari

L'esigenza di poter contare su sistemi rapidi, efficaci e sicuri in merito allo scambio e alla gestione dei dati sanitari si è resa particolarmente urgente in occasione della crisi da Covid-19.

Per poter salvaguardare le vite e la salute dei cittadini si è reso necessario uno scambio continuo di dati sanitari e, quindi, di una normativa sulla gestione di questi ultimi che fosse all'altezza del compito. Ma, *“la mancanza di criteri uniformi di raccolta e trasmissione, insieme alla carenza di trattamento adeguato in termini di formazione e conservazione, ha reso complessa la trasformazione dei dati in informazioni utili, mettendo spesso a repentaglio la sicurezza dei dati stessi”*¹⁷². La carenza di regole uniformi e precise, che puntano a garantire affidabilità, autenticità, integrità, leggibilità e reperibilità ai dati sanitari, si configura come un *“vulnus”* normativo importante¹⁷³. L'analisi va letta considerando i più recenti sviluppi in tema dei principi di *FAIR* (*Findable, Accessible, Interoperable, Reusable*): elaborati nel 2014 per ottimizzare la riutilizzabilità dei dati della ricerca, rappresentano un insieme di linee guida per garantire la rintracciabilità, l'accessibilità, l'interoperabilità e la riutilizzabilità dei dati. Come è già stato rilevato, uno degli obiettivi del Regolamento EHDS è quello di predisporre una nuova *“governance dei dati sanitari finalizzata ad abilitare nuovi modelli di cura, migliorare la prevenzione attraverso l'individuazione di percorsi sanitari mirati nonché indirizzata allo sviluppo, alla ricerca e alla definizione di policy governative e normative basate sull'evidenza”*¹⁷⁴. Il dato sanitario diventa, quindi, uno strumento fondamentale, ma molto vulnerabile a violazioni esterne. In questo scenario, l'UE si muove per sviluppare un mercato unico per i servizi e i prodotti di sanità digitale, creando un ecosistema che dovrà fornire *“nuove frontiere per la ricerca e l'innovazione, favorendo*

¹⁷² E. SORRENTINO, A.F. SPAGNUOLO, *Gestione e conservazione dei dati sanitari. Il vulnus normativo che impatta su sicurezza e data protection*, in *Federalismi.it*, 2024, p. 138.

¹⁷³ *Ivi*, p. 139.

¹⁷⁴ *Ivi*, p. 143.

la creazione di dataset di dimensioni consistenti e facilitare così la conduzione di studi multicentrici su scala europea”¹⁷⁵.

È in questo senso che devono essere intesi i principi di *Fair* in merito alla disciplina sugli *open data*. Andando ad analizzare la normativa relativa agli *open data* e i principi di *fair* si può ipotizzare una “*interpretazione estensiva*” della norma anche ai dati sanitari in modo da “*iniziare a configurare una politica di corretta gestione e conservazione che vada ad aumentare significativamente la sicurezza dei dati, minimizzando il rischio di violazioni*”, inoltre, “*applicare i principi open data e FAIR ai dati sanitari, in una prospettiva di completa apertura e condivisione, potrebbe risultare funzionale all’implementazione di una solida politica di conservazione, aumentando al contempo la valorizzazione di questa preziosa risorsa informativa nonché i livelli di sicurezza*”¹⁷⁶. Inoltre, è la natura pubblica del patrimonio informativo che eleva i dati al rango di bene comune imponendo che siano resi aperti, fruibili e disponibili¹⁷⁷. Il quadro normativo internazionale e sovranazionale si evolve verso politiche di maggiore apertura e condivisione dei dati pubblici sottolineando come la condivisione del patrimonio informativo sia fondamentale per ampliare le conoscenze e sviluppare la ricerca¹⁷⁸. I principi *FAIR* vengono, ultimamente, associati ai principi *TRUST* (*Transparency, Responsibility, User Focus, Sustainability, Tecnology*) per l’implementazione di *repository* in grado di conservare i dati di ricerca a lungo termine. In sostanza, l’idea è quella di utilizzare i principi di *FAIR* sin dalla progettazione per rendere i dati facilmente identificabili, rintracciabili, accessibili e interoperabili, e, in parallelo, utilizzare un sistema di *repository TRUST* in modo da ottenere la fiducia degli utenti¹⁷⁹. Per sintetizzare, i principi *FAIR* e *TRUST* assicurano una gestione e una conservazione dei dati corrette e a lungo termine. Questo avviene grazie a *repository* funzionali e durevoli nel tempo, all’interno dei quali anche i dati sanitari, se adeguatamente anonimizzati,

¹⁷⁵ *Ivi*, p. 145

¹⁷⁶ *Ivi*, p. 150.

¹⁷⁷ A. F. SPAGNUOLO, E. SORRENTINO, *Open data per l’e-democracy*, in *Rivista italiana di informatica e diritto*, 4, 1 (mag. 2022), pp. 273-282.

¹⁷⁸ Un esempio importante è il progetto dell’Unione Europea “*Open Research Data Pilot*” che persegue gli obiettivi di creare un piano di gestione dei dati e di fornire un accesso aperto e un riutilizzo dei dati in conformità con i principi di *FAIR*.

¹⁷⁹ *Ivi*, p. 153.

possono essere liberamente condivisi per il riutilizzo secondario, azzerando i rischi per la sicurezza degli interessati.

5. La telemedicina come strumento di *e-Health*.

La creazione di un ecosistema sicuro e interoperabile basato sui principi *FAIR* e *TRUST* trova la sua applicazione più concreta ed emergente nell'ambito dell'*e-Health*, laddove la gestione del dato diventa il presupposto operativo per erogare servizi di cura a distanza.

A partire dalla crisi pandemica da Covid-19, il ricorso a prestazioni sanitarie a distanza è stato giustificato dalla necessità di erogare servizi a differenti tipologie di persone obbligate in quarantena o, in ogni caso, in isolamento. In questo contesto è emerso con forza il tema della telemedicina che, da un lato, ha permesso di contrastare la diffusione del virus, dall'altro, ha garantito la continuità della cura e dell'assistenza dei pazienti che ne avevano diritto, all'interno dei loro luoghi di domicilio¹⁸⁰. Il termine telemedicina appare per la prima volta nella letteratura scientifica negli anni '70, definita come “*la pratica della medicina senza l'usuale confronto fisico tra medico e paziente, utilizzando un sistema di comunicazione interattivo multimediale*”¹⁸¹. Successivamente, è possibile ravvisare una definizione ufficiale nella Comunicazione del 4 novembre 2008 della Commissione europea, in cui viene identificata nella “*prestazione di servizi di assistenza sanitaria, tramite il ricorso alle TIC, in situazioni in cui il professionista della salute e il paziente (o due professionisti) non si trovano nella stessa località*”. Una prestazione che si caratterizza per “*la trasmissione sicura di informazioni e dati di carattere medico grazie a testi, suoni, immagini o altre forme necessarie per la prevenzione, la diagnosi, il trattamento e il successivo controllo dei pazienti*”¹⁸².

Con il termine telemedicina si allude a una pluralità di prestazioni – televisita, teleconsulto, teleassistenza, tele refertazione – che possono avvenire mediante due principali modalità operative: telemonitoraggio e telecontrollo. Si distingue inoltre a

¹⁸⁰ M. CAMPAGNA, *Linee guida per la Telemedicina: considerazioni alla luce dell'emergenza Covid-19*, in *Corti Supreme e Salute*, 2020, p. 601.

¹⁸¹ A. MAZZA LABOCCETTA, *Telemedicina: sfide, problemi, opportunità*, in *Federalismi.it*, 2023, p. 139.

¹⁸² *Ibidem*.

seconda che la telemedicina sia utilizzata dal professionista sanitario per fornire prestazioni sanitarie agli assistiti ovvero per servizi di consulenza o supporto a favore di altri sanitari.

Nel periodo pandemico, l'obbligo del distanziamento per ridurre il contagio ha accelerato la digitalizzazione. Le tecnologie dell'informazione e della comunicazione (TIC) sono diventate la principale alternativa al contatto umano, rivoluzionando la comunicazione nella sanità, nella pubblica amministrazione, nelle imprese e nelle professioni.

In merito alla nascita e allo sviluppo della telemedicina, in Italia il primo intervento volto a regolare questo fenomeno è stato nel 1990: fu istituito, tramite decreto¹⁸³, un “Comitato Nazionale per la Telemedicina” e nel 1999 fu presentato in Parlamento un disegno di legge¹⁸⁴ con l’obiettivo di diffondere la telemedicina di emergenza e potenziare i sistemi di monitoraggio a distanza¹⁸⁵. Nel 2008 la Commissione Europea, tramite Comunicazione (COM-2008-689) del 4 novembre, ha attribuito centralità alla telemedicina incoraggiando azioni, a livello comunitario e di governo dei singoli Stati membri, volte a favorire una maggiore integrazione dei servizi di telemedicina nella pratica clinica. Negli anni successivi, nonostante l’interesse manifestato sia a livello nazionale che europeo, la prestazione sanitaria tramite la telemedicina non è riuscita a imporsi con fermezza nello scenario dell’assistenza clinica. Come già accennato, la pandemia da Covid-19 ha reso la telemedicina uno strumento fondamentale per garantire la continuità delle cure e contrastare la diffusione del virus. Di conseguenza, il Sistema Sanitario Nazionale è stato *“chiamato a garantire quanto più possibile la regolare erogazione dei servizi nel contesto pandemico anche sfruttando le opportunità derivanti dall’utilizzo di strumenti digitali, sia nell’assistenza dei pazienti a distanza sia nel facilitare la collaborazione e lo scambio di informazioni fra i professionisti coinvolti”*¹⁸⁶. Di seguito, la VI missione del Piano

¹⁸³ Ministero dell’Università e della ricerca, decreto del 20 aprile 1990.

¹⁸⁴ D.l. n. 3775.

¹⁸⁵ S. SAMO, *La telemedicina alla luce dell’avvento della robotica e dell’Intelligenza Artificiale*, in *Federalismi.it*, 2025, p. 228.

¹⁸⁶ *Ivi*, p. 229.

Nazionale di Ripresa e Resilienza (PNRR) ha destinato un miliardo di euro per favorire la diffusione e lo sviluppo della telemedicina tramite interventi mirati¹⁸⁷.

La telemedicina è considerata quell'approccio *“innovativo alla pratica sanitaria, caratterizzata dall'erogazione di servizi a distanza mediante dispositivi digitali, software, reti di comunicazione e sistemi di intelligenza artificiale”*¹⁸⁸. La diffusione della telemedicina e il suo potenziamento sono fondamentali per rafforzare il Servizio Sanitario Nazionale. Questo strumento permette, infatti, di garantire prestazioni di alta qualità, ottimizzare la gestione delle risorse economiche e assicurare un accesso più equo e uniforme alle cure su tutto il territorio nazionale. Uno degli aspetti di maggiore importanza è rappresentato dalla necessità di utilizzare la telemedicina come unica soluzione in circostanze nelle quali potrebbe essere difficile garantire l'assistenza sanitaria. Inoltre, tale strumento permette al paziente di ricevere cure specifiche nella propria abitazione senza dover ricorrere allo studio del proprio medico oppure ad una struttura ospedaliera, generando due effetti positivi: il primo nei confronti del paziente, il secondo sul SSN. In merito al paziente, quest'ultimo può acquisire maggiore autonomia nella gestione della propria situazione sanitaria, invece, per quanto riguarda il SSN, la telemedicina permette di ridurre la degenza e il ricorso al pronto soccorso, favorendo un intervento dei medici ospedalieri più tranquillo e mirato, e riducendo eventuali sprechi di risorse pubbliche.

Dal punto di vista operativo, similmente a quanto avvenuto con il fascicolo sanitario elettronico, il supporto infrastrutturale del servizio di telemedicina viene modulato dal PNRR sulla base di un approccio di tipo federalista: infatti, la competenza alla realizzazione delle piattaforme di telemedicina è stata rimessa alle singole Regioni, in conformità alle Linee di indirizzo per la realizzazione dei servizi di telemedicina di cui al D.M. 21 settembre 2022 e a fronte della predisposizione di una Piattaforma Nazionale di Telemedicina (PNT), posta sotto la gestione di Agenas.

¹⁸⁷ N. POSTERARO, *La telemedicina*, in V. BONTEMPI (a cura di), *Lo stato digitale nel Piano nazionale di ripresa e resilienza*, Roma, 2022, pp. 187-200. Sul punto anche P. DE ANGELIS, *Il PNRR e la telemedicina*, in *Sanità Pubblica e Privata*, 2024, 2, pp. 6-12.

¹⁸⁸ S. SAMO, *La telemedicina alla luce dell'avvento della robotica e dell'Intelligenza Artificiale*, cit., p. 230.

A fronte di un sistema di telemedicina e, più in generale, di *e-health*, caratterizzato da una struttura spiccatamente regionalistica, la Piattaforma Nazionale di Telemedicina è stata investita di un ruolo di primaria importanza per la garanzia dell'uniformità sul territorio nazionale della complessiva offerta di cura. Infatti, stando a quanto affermato da Agenas nel comunicato del 1 ottobre 2024, la PNT è chiamata a garantire l'interoperabilità con l'architettura applicativa del fascicolo sanitario elettronico e con l'ecosistema dei dati sanitari, nell'intento di perseguire una serie obiettivi di più ampio respiro che toccano trasversalmente l'intero comparto della sanità e cercano di porre rimedio ad alcune delle intrinseche deficienze del sistema sanitario nazionale: prima fra tutte la disparità territoriale nell'erogazione delle prestazioni di cura¹⁸⁹. La telemedicina viene, quindi, potenzialmente immaginata non solo quale mezzo funzionale all'attività assistenziale, ma anche come strumento di programmazione e di governo del servizio sanitario¹⁹⁰.

La scelta di adottare un approccio di tipo regionalistico, in parte temperata dalla predisposizione di una piattaforma nazionale, suscita alcune perplessità, soprattutto se si considera che uno dei principali obiettivi attribuito allo strumento di *e-health* sia l'implementazione omogenea di percorsi di telemedicina sull'intero territorio nazionale. Non si può tralasciare che le Regioni si siano mosse e si stiano muovendo in maniera disarmonica, modulando, in modo diverso, le prestazioni e le modalità operative della telemedicina¹⁹¹.

D'altra parte, esistono anche dei veri e propri limiti allo sviluppo e alla diffusione di questo strumento. Primo tra tutti, il *digital divide*, termine che allude al divario digitale sussistente tra chi può accedere a *internet* e chi non può. Si distingue tra tre differenti tipologie di *digital divide*: la prima forma è di tipo globale e mira ad evidenziare la differenza di accesso e utilizzo di *internet* tra i paesi più sviluppati economicamente ed i più arretrati; la seconda è di tipo sociale, in questo caso le differenze riguardano l'accesso a prestazioni di ogni tipo; la terza è democratica, viene limitata la partecipazione alla vita

¹⁸⁹ Sul tema A. Coiante, L'implementazione della telemedicina come elemento strutturale del SSN: dalla frammentarietà all'uniformità. La stabilizzazione post-PNRR e il possibile ruolo dei LEA, in *federalismi.it*, 2025, 28, pp. 44-66 e A. Ciafardini, Telemedicina e livelli essenziali di assistenza nel prisma dei divari territoriali, in *Italian Papers On Federalism*, 2/2025, pp. 162-176.

¹⁹⁰ Su tale profilo R. CAVALLO PERIN, *L'interesse della collettività alla tutela della salute*, in *Dir. amm.*, 2024, 3, p. 758.

¹⁹¹ Sul punto V. BURATTI, *La riforma della sanità territoriale: luci e ombre dei nuovi modelli organizzativi e assistenziali*, in *Ceridap*, 2025, 2, pp. 36-63.

politica e sociale. Il divario digitale è causato dalla carenza di strumentazioni tecnologiche o alla mancanza di conoscenze informatiche adeguate a poter utilizzare tali strumenti, oltre che a fattori come età, istruzione, reddito o posizione geografica¹⁹². Un altro problema legato alla diffusione della telemedicina riguarda il saper gestire il rapporto medico paziente, evitando che si instauri nel malato una sensazione di abbandono o solitudine, questo perché *“è soltanto nella relazione in presenza tra medico e paziente che può nascere quell’empatia, elemento fondamentale di un rapporto che si fonda sull’ascolto, sulla percezione emotiva della paura, della fiducia e dell’umanità. Dunque, la presenza fisica con il medico è quella condicio sine qua non affinché si produca quel carattere palliativo inalienabile per il paziente che non può essere sostituita da alcun progresso tecnologico”*¹⁹³. In questo senso va avvertito il principale timore legato allo sviluppo della telemedicina, cioè l’eliminazione di quell’elemento umano che caratterizza il rapporto tra medico e paziente.

Oltre alle criticità derivanti dal regionalismo del sistema, che si ripercuotono sulla funzione organizzativa attribuita alla telemedicina, non meno controversa è la reale efficacia con riferimento all’effettiva erogazione delle prestazioni di cura. A tal propositivo, si deve osservare che, anche alla luce di quanto previsto dal d.lgs. 15 marzo 2024, n. 29, i principali beneficiari della telemedicina sono pazienti con una malattia cronica e un’età superiore a sessantacinque anni, cioè soggetti che tendenzialmente hanno scarsa dimestichezza e naturale ritrosia all’utilizzo dei mezzi tecnologici e che necessiteranno presumibilmente dell’ausilio di un “caregiver”. Tale notazione di natura demografica impone una seria riflessione sulla modulazione dei servizi: ad oggi, le linee guida del 2022 attribuiscono a una scelta discrezionale del medico di medicina generale il ricorso alla telemedicina per la cura di un paziente¹⁹⁴. Si tratta di un giudizio che non si limita all’analisi di aspetti clinici, ma si estende anche alla verifica delle conoscenze informatiche del paziente e della dotazione tecnologica di cui lo stesso dispone, elementi questi ultimi che esulano dall’ambito delle competenze proprie del professionista. Si

¹⁹² S. SAMO, *La telemedicina alla luce dell’avvento della robotica e dell’Intelligenza Artificiale*, cit., p. 233.

¹⁹³ *Ivi*, p. 234.

¹⁹⁴ V. BURATTI, *La riforma della sanità territoriale: luci e ombre dei nuovi modelli organizzativi e assistenziali*, in *Ceridap*, 2025, 2, pp. 36-63.

profila, dunque, un serio rischio in ordine all'effettività di un godimento uniforme dei diritti sul territorio nazionale nonché alla diffusione di pratiche di medicina difensiva¹⁹⁵.

6. Tecnologia *blockchain* e telemedicina quali strumenti per una circolazione sicura del dato sanitario.

Proprio per superare le riserve legate alla sicurezza dei dati, all'integrità dei sistemi e ai rischi di medicina difensiva, la dottrina e il legislatore rivolgono crescente attenzione a nuove architetture tecnologiche in grado di blindare il flusso informativo. Prima fra tutte, la *blockchain*.

Quest'ultima, tra le altre cose, permette di creare un *database* per la gestione dei dati e, inoltre, può essere molto utile riguardo al tema della telemedicina. Bisogna però prima inquadrare questa nuova tecnologia, che può essere considerata come uno storico di tutte le transazioni o operazioni, che avvengono al suo interno¹⁹⁶. Si tratta di un registro digitale cronologico composto da una lista di dati in cui i *computer* collegati alla rete possono inserire informazioni secondo le regole del sistema. Il contenuto è poi verificabile da qualsiasi dispositivo che possa accedere a *Internet*. Le informazioni inserite vengono crittografate e organizzate in più gruppi, chiamati blocchi, che contengono “*le “notizie” relative a un certo numero di operazioni, un riferimento al blocco precedente, nonché una risposta a un complesso algoritmo matematico, che viene utilizzato per validare i dati associati con quel blocco.*” L'accesso al contenuto del database è vincolato all'autorizzazione da parte di tutti i partecipanti alla *blockchain* e, inoltre, una copia di quest'ultima viene memorizzata su tutti i *computer* in rete, creando un *database* condiviso. Ciò che garantisce sicurezza al sistema *blockchain* è la decentralizzazione del sistema e la trasparenza delle informazioni contenute in quest'ultimo. Il connubio con la

¹⁹⁵ F. APERIO BELLA, *Telemedicina tra decentramento ed esigenze di uniformità*, in C. Bottari, P. J. Tárraga López, J. Cantero Martínez (a cura di), *Sanità rurale e assistenza sanitaria decentrata*, Napoli, 2024, p. 355 prefigura il rischio di una vera e propria «telemedicina difensiva».

¹⁹⁶ E. SIGNORINI, F. ZAMBARDINO, *La blockchain e la telemedicina: quali opzioni per la sicurezza e l'integrità dei dati sanitari*, in *Federalismi.it*, 2025, p. 206.

telemedicina, strumento fondamentale che permette di fornire servizi di assistenza sanitaria in contesti di distanza fisica tra il paziente e la struttura sanitaria, è il più promettente. In questo senso, ci si muove verso un tipo di cura basato su un approccio personalizzato: infatti, le informazioni sanitarie, grazie a queste nuove tecnologie, non si troveranno più soltanto nelle cartelle cliniche, ma, verranno aggiornate a livello giornaliero tramite l'acquisizione dei dati raccolti da dispositivi indossabili (come cerotti e non solo) che consentiranno di monitorare la condizione di salute dei pazienti¹⁹⁷. Si tratta di un'innovazione importante, in questo modo il paziente da soggetto passivo diventa anche soggetto attivo e, grazie all'attivazione da parte del soggetto in cura di questi nuovi sistemi, sarà possibile prevedere il rischio di sviluppare determinate malattie. Ma, oltre a migliorare l'esperienza di cura per il paziente, il collegamento tra intelligenza artificiale e telemedicina può portare a degli sviluppi fondamentali anche in merito a tutti quei soggetti che intervengono e assistono i pazienti nei percorsi di cura, si intendono i *caregiver*. Difatti, *“l'adozione di sistemi di telemedicina nel settore sanitario comporta nuove dinamiche di cooperazione tra pazienti e operatori, contribuendo a un contestuale miglioramento delle prestazioni offerte”*¹⁹⁸. I benefici si articolano su quattro livelli: innanzitutto, la qualità dell'assistenza migliora grazie al monitoraggio costante e a distanza dei parametri dei pazienti. In secondo luogo, si amplia la copertura sanitaria, garantendo interventi tempestivi anche a chi risiede in aree isolate o lontane dagli ospedali. Terzo, l'interazione continua tra i vari attori del sistema accresce l'efficacia e l'efficienza del servizio. Infine, dal punto di vista economico, l'ottimizzazione delle risorse razionalizza i processi sociosanitari, traducendosi in una significativa riduzione dei costi. Il lato critico di questa evoluzione tecnologica riguarda le problematiche che potrebbero emergere in seguito ad attacchi *hacker* che potrebbero minare la *privacy* dei pazienti. Inoltre, per ottenere dei livelli di efficienza ed efficacia adeguati è necessario che il sistema del Fascicolo Sanitario Elettronico sia integro, dato che, quest'ultimo include la storia medica, farmaceutica e di diagnosi del paziente.

¹⁹⁷ E. SIGNORINI, F. ZAMBARDINO, *La blockchain e la telemedicina: quali opzioni per la sicurezza e l'integrità dei dati sanitari*, in *Federalismi.it*, 2025, p. 208.

¹⁹⁸ *Ivi*, p. 211.

7. Strumenti di *e-Health*: il Fascicolo Sanitario Elettronico e la Cartella Clinica Elettronica.

Dal piano delle tecnologie emergenti e della gestione sicura dei flussi dati si giunge così ai fondamentali strumenti operativi dell'*e-Health* che ne costituiscono il supporto informativo: il Fascicolo Sanitario Elettronico e la Cartella Clinica Elettronica¹⁹⁹.

La digitalizzazione della sanità incide sia sulle modalità di erogazione delle prestazioni sanitarie sia sull'organizzazione delle amministrazioni. Risulta, quindi, necessario analizzare il Fascicolo Sanitario Elettronico (FSE), il quale costituisce uno dei principali strumenti di *e-Health*. Si tratta di una raccolta digitale di tutti i dati e documenti sanitari e sociosanitari relativi alla storia clinica di un soggetto, operando come una carta d'identità digitale sanitaria del singolo cittadino e come un archivio della salute dell'assistito²⁰⁰. Il FSE si configura come il punto unico di aggregazione e condivisione della documentazione sanitaria e sociosanitaria del cittadino, alimentato dai diversi attori del SSN e dai servizi regionali²⁰¹. Tale strumento costituisce la concreta applicazione di un'architettura di sistema orientata a supportare pienamente l'interazione tra gli operatori sanitari e il rapporto tra medico e paziente.

Sul piano normativo, il FSE è stato introdotto²⁰² dall'articolo 12 del d.l. 18 ottobre 2012 n. 179²⁰³, ma con il decreto “del Fare” (d.l. 21 giugno 2013, n. 69), il legislatore, modificando l'articolo 12 del decreto crescita, ha stabilito un termine entro il quale ciascuna Regione e Provincia Autonoma dovesse provvedere all'attivazione del FSE nel proprio territorio (il termine massimo era fissato al 30 giugno 2015). Tuttavia, l'iter previsto dalla norma ha subito diversi rallentamenti, e il decreto che regola nel

¹⁹⁹ L. Ferraro, *Il Regolamento UE 2016/679 tra Fascicolo Sanitario Elettronico e Cartella Clinica Elettronica: il trattamento dei dati di salute e l'autodeterminazione informativa della persona*, in *BioLaw Journal - Rivista di BioDiritto*, 2021, 4, pp. 91-114.

²⁰⁰ N. POSTERARO, *La digitalizzazione della sanità in Italia: uno sguardo al Fascicolo Sanitario Elettronico (anche alla luce del Piano Nazionale di Ripresa e Resilienza)*, in *Federalismi.it*, 2021, p. 192.

²⁰¹ A. AMORE, *Il fascicolo sanitario elettronico nella prospettiva dell'eguaglianza territoriale: una proposta di inquadramento giuridico tra LEA e LEP*, in *Ia, sanità – territorio, pubbliche amministrazioni*, 2026, pp. 61-65.

²⁰² In realtà, diverse Regioni avevano avviato attività progettuali per la realizzazione di sistemi di FSE a livello locale ben prima che lo strumento acquisisse rilievo nazionale.

²⁰³ Cd. decreto crescita, poi convertito in l. 17 dicembre 2012, n. 221.

dettaglio il FSE è stato infatti adottato soltanto nel settembre 2015, si tratta del d.p.c.m. 29 settembre 2015, n. 178, “Regolamento in materia di fascicolo sanitario elettronico”.

Ora, prima di analizzare le caratteristiche di questo strumento, è necessario soffermarsi sulle differenze che intercorrono tra esso e la Cartella Clinica Elettronica (CCE). Le cartelle cliniche sono state colpite dal processo di dematerializzazione²⁰⁴ della documentazione sanitaria, assieme a referti e ricette mediche. In quest’ottica, a seguito dell’adozione di una serie di linee guida in tema di dematerializzazione²⁰⁵, è stato emanato il d.l. 13 maggio 2011 n. 70, il quale ha stabilito l’obbligo per tutte le aziende sanitarie del SSN di adottare procedure telematiche per consentire la consegna di referti medici tramite web, posta elettronica certificata o altre modalità digitali. In seguito, all’articolo 13 del d.l. n. 179/2012, viene disposta la sostituzione delle prescrizioni in formato cartaceo con le equivalenti in formato elettronico e la conservazione delle cartelle cliniche “anche solo in formato digitale”²⁰⁶. La digitalizzazione è stata bruscamente accelerata dalla pandemia da Covid-19. Con lo scopo di ridurre l’afflusso dei pazienti negli studi dei professionisti è stato emanato il d.m. 25 marzo 2020²⁰⁷ attraverso il quale è stato modificato il d.m. 2 novembre 2011²⁰⁸, introducendo l’articolo 3-*bis*, il quale prevede canali alternativi di consegna del promemoria cartaceo della ricetta, tra cui: il portale del Sistema di Accoglienza Centrale (SAC), il FSE dell’assistito, la posta elettronica e gli SMS.

Riguardo alla Cartella Clinica Elettronica, quest’ultima si configura come un documento informatico redatto dalla struttura sanitaria di riferimento per la gestione integrata dei dati clinici del paziente, finalizzato a garantire la continuità assistenziale nel tempo. È un atto pubblico “*avente fede privilegiata*”²⁰⁹ che risulta fondamentale non solo per la

²⁰⁴ E. CATELANI, *La digitalizzazione dei dati sanitari: un percorso ad ostacoli*, in *Corti Supreme e Salute*, 2023, p. 427.

²⁰⁵ “Linee guida per la dematerializzazione della documentazione clinica in laboratorio e diagnostica per immagini – Normativa e prassi” adottate dal ministero della salute nel 2007; le “Linee guida in tema di fascicolo sanitario elettronico e di dossier sanitario” adottate dal Garante della Privacy nel 2009; le “Linee guida nazionali per il sistema CUP”, adottate dal Ministero della salute il 27 ottobre 2009.

²⁰⁶ *Ivi*, p. 196.

²⁰⁷ Recante “Estensione della dematerializzazione delle ricette e dei piani terapeutici e modalità alternative al promemoria cartaceo della ricetta elettronica”.

²⁰⁸ Recante “Dematerializzazione della ricetta medica cartacea, di cui all’articolo 11, comma 16, del decreto-legge n. 78 del 2010”.

²⁰⁹ *Ivi*, p. 196.

documentazione e per la storia clinica del paziente, ma anche per garantire la tutela giurisdizionale nei giudizi di risarcimento danni promossi da pazienti o terzi, in relazione a condotte mediche ritenute lesive. La differenza fondamentale tra FSE e CCE è che il primo, contiene tutta la storia clinica del paziente, mentre la seconda descrive solo un singolo episodio di ricovero dell'interessato. La cartella elettronica è tra le tecnologie maggiormente in uso in tutta Europa con una percentuale di utilizzo dell'81% (69% in Italia), tuttavia, molte strutture sanitarie italiane continuano a gestire in formato cartaceo le cartelle cliniche, ciò dimostra quanto sia necessario investire sulla digitalizzazione dei documenti sanitari.

Tornando al FSE, la finalità principale dello stesso è quella di creare una base informativa organica, a continua implementazione, che possa favorire il miglioramento delle attività di cura, diagnosi, prevenzione e riabilitazione dei pazienti. Tale strumento permette la condivisione informatica di dati e documentazione sanitaria, integrati e aggiornati nel tempo da una pluralità di soggetti. Ciò consente di ricostruire fedelmente l'intera storia clinica dell'assistito, mettendone in luce i diversi eventi sanitari e garantendo, di conseguenza, un più efficiente processo di cura²¹⁰. Attraverso il FSE, il paziente può monitorare e consultare la propria storia clinica per intero, condividendola con i professionisti sanitari per ricevere un'assistenza più efficace ed efficiente. Lo strumento offre un supporto fondamentale per la continuità delle cure: permette infatti ai diversi operatori che assistono il paziente di conoscere tempestivamente le iniziative diagnostiche e terapeutiche già avviate dai colleghi. Il FSE è stato sviluppato proprio per superare le carenze dei canali tradizionali nella trasmissione dei dati clinici, garantendo una disponibilità informativa ideale per la continuità assistenziale. In quest'ottica, esso rappresenta il principale fattore abilitante per un sistema di Sanità Digitale (*e-Health*) realmente incentrato sulla centralità dell'assistito. Risulta fondamentale riportare la necessità del consenso da parte del paziente, il quale, può decidere di permettere la visualizzazione del proprio FSE e in ogni momento può modificare le indicazioni in merito a chi può accedere e consultare il suo FSE. Ma, in deroga al generale divieto di trattare i dati particolari (art. 9, par. 1, GDPR), i paragrafi 2, lett. h) e 3 del medesimo articolo consentono oggi al professionista sanitario di trattare i dati sanitari del paziente

²¹⁰ N. POSTERARO, *La digitalizzazione della sanità in Italia: uno sguardo al Fascicolo Sanitario Elettronico (anche alla luce del Piano Nazionale di Ripresa e Resilienza)*, in *Federalismi.it*, 2021, p. 197.

anche in assenza di un esplicito consenso, purché ciò sia necessario all'erogazione della prestazione richiesta. Tuttavia, come opportunamente chiarito dal Garante per la protezione dei dati personali, i trattamenti effettuati tramite il Fascicolo Sanitario Elettronico (FSE) per finalità di cura continuano a richiedere, quale imprescindibile condizione di liceità, la previa acquisizione del consenso dell'interessato²¹¹. Il FSE è fondamentale anche come strumento di supporto per la ricerca nonché per la programmazione e pianificazione sanitaria. In caso di finalità diverse da quella della cura della persona, nel rispetto dei principi di proporzionalità, necessità e indispensabilità del trattamento dei dati personali, è indispensabile utilizzare informazioni che non siano in grado di identificare i pazienti²¹². Da questo punto di vista, il FSE costituisce un chiaro esempio di come si debbano bilanciare due esigenze opposte: da un lato, la libera circolazione dei dati (essenziale per la sanità pubblica e l'efficienza burocratica) e, dall'altro, il diritto alla riservatezza a tutela della dignità della persona. Procedendo con l'analisi relativa al Fascicolo Sanitario Elettronico, questo strumento deve comprendere un nucleo minimo di elementi. Al suo interno debbono essere obbligatoriamente inseriti i dati identificativi e amministrativi dell'assistito, i referti, i verbali del pronto soccorso, le lettere di dimissione e il consenso alla donazione degli organi. In ordine, in merito ai dati identificativi il FSE deve garantire l'allineamento di questi ultimi con quelli contenuti nell'Anagrafe Nazionale degli Assistiti (ANA) in modo da evitare errori di riconoscimento del paziente. Per quanto riguarda i dati amministrativi, essi sono composti dalle informazioni relative alla posizione dell'assistito nei confronti del Servizio Sanitario Nazionale. All'interno del nucleo minimo troviamo il *dossier* farmaceutico, sezione aggiornata a cura della farmacia in grado di tracciare e ricostruire la storia farmacologica dell'assistito, e il *patient summary*, un "riassunto" del profilo medico del paziente redatto dal medico di famiglia. Quest'ultimo fornisce un supporto fondamentale in situazioni, soprattutto, di emergenza²¹³. Il *patient summary* è stato criticato a causa del fatto che potrebbe contenere dati sanitari differenti rispetto a quelli inseriti nel FSE e, a causa di questa mancata sincronia, potrebbero emergere dubbi relativi alla cura del paziente.

²¹¹ *Ivi*, p. 199.

²¹² La tecnica più utilizzata è la pseudonimizzazione. Permette di de-identificare i dati eliminando l'associazione tra uno specifico paziente e le informazioni che lo riguardano.

²¹³ Pensiamo all'operatore sanitario che, trovandosi di fronte ad un paziente sconosciuto, può ottenere informazioni sulla salute di quest'ultimo.

Inoltre, se previsto dalla Regione, il FSE può comporsi di elementi integrativi, tra i quali il taccuino personale²¹⁴. Si tratta di un'area specifica nella quale ciascun paziente può inserire dati e documenti relativi alle proprie cure, va specificato che grazie a questo strumento l'assistito può partecipare attivamente alla creazione del proprio *database* sanitario personale. Il ruolo del professionista sanitario che si occupa di considerare le informazioni inserite dal paziente è quello di prendere in considerazione le informazioni con la maggiore cautela possibile. Va detto che i dati inseriti personalmente nel taccuino non vengono certificati dal SSN. Questo strumento rimane parzialmente utilizzato a causa del fatto che il componimento del taccuino personale viene disposto dalle scelte delle singole Regioni.

Dopo aver analizzato le finalità e gli utilizzi del FSE, è necessario soffermarsi sulle difficoltà, in tema di attuazione, che questo strumento ha incontrato. Infatti, successivamente all'introduzione del FSE nell'ordinamento italiano nel 2012, il primo bilancio fu deludente. Nonostante fosse formalmente attivo in tutte le Regioni italiane, l'utilizzo da parte di medici e pazienti si attestò su percentuali molto basse, ciò a causa di fattori culturali (popolazione prevalentemente anziana, con scarsa alfabetizzazione digitale e desiderosa di un confronto personale con il professionista) ed economico-organizzativi (assenza o scarsità delle infrastrutture informatiche e mancanza di organico specializzato nelle strutture sanitarie)²¹⁵. Peraltro, il suo stesso funzionamento era condizionato dal fatto che l'istituzione e la gestione del Fascicolo spettavano alle singole Regioni, oltre che dalla scarsa interoperabilità dei sistemi²¹⁶; criticità, queste ultime, che hanno storicamente caratterizzato l'intero processo di digitalizzazione della Pubblica Amministrazione.

Grazie al, precedentemente citato, PNRR, precisamente Missione VI, Componente 2, è stato possibile persistere nell'investimento dello strumento del FSE. Infatti, il PNRR, ha elevato il FSE a *“pietra angolare per l'erogazione dei servizi sanitari digitali e la valorizzazione dei dati clinici nazionali”* attraverso l'attribuzione di tre principali funzioni: punto di accesso per la fruizione dei servizi sanitari, base dati contenente

²¹⁴ N. POSTERARO, *La digitalizzazione della sanità in Italia: uno sguardo al Fascicolo Sanitario Elettronico (anche alla luce del Piano Nazionale di Ripresa e Resilienza)*, in *Federalismi.it*, 2021, p. 205.

²¹⁵ V. BURATTI, *Fascicolo sanitario elettronico: verso la piena operatività?* In [Diritto e sanità](#).

²¹⁶ Il tema dell'interoperabilità verrà affrontato nel paragrafo successivo.

informazioni omogenee sulla storia clinica di ciascun paziente, strumento per l'analisi di dati, al fine del miglioramento della prestazione dei servizi sanitari. Nelle intenzioni del Piano, il FSE è destinato a subire, come del resto molte altre banche dati pubbliche, una transizione da strumento informativo a struttura centrale abilitante idonea all'erogazione di servizi²¹⁷.

Risulta necessario, in questa sede, rilevare gli interventi da parte del Garante della *Privacy*. Quest'ultimo è intervenuto perché l'adozione dell'applicativo in ambito sanitario richiede un delicato bilanciamento tra la libera circolazione dei dati, essenziale per efficientare l'azione pubblica e tutelare la salute collettiva, e il diritto alla riservatezza. In merito a ciò, è già stato citato il Provvedimento n. 294 del 22 agosto 2022. I profili controversi rilevati in tale parere sono stati considerati risolti dal Garante tramite parere positivo²¹⁸. Precisamente, l'Autorità ha specificato alcune necessarie condizioni affinché il parere si debba intendere favorevole, prima fra tutti il coordinamento tra schema di decreto e Linee guida per i servizi di telemedicina. Il riferimento è, poi, all'obbligo di stabilire i termini entro cui Ministero ed enti locali dovranno fornire agli interessati le informazioni relative ai trattamenti di dati personali effettuati attraverso il FSE ed effettuare campagne di informazione circa l'alimentazione della banca dati, adempimenti a cui si è data attuazione con valutazione positiva del Garante²¹⁹.

In conclusione, *“nonostante il via libera alla nuova versione del Fascicolo (Decreto attuativo 7 settembre 2023), persistono alcuni dubbi sulle scelte effettuate che, peraltro, riflettono le criticità da tempo emerse in materia: mantenimento di un approccio federato-regionalistico, eccessiva attenzione ad aspetti di stretta informatica e mancato coinvolgimento degli stakeholders. Soprattutto, desta perplessità l'eliminazione di qualsiasi riferimento all'Ecosistema dei dati sanitari, strumento essenziale per garantire un sistema centralizzato di raccolta e analisi dei dati e l'erogazione di servizi omogenei sul territorio. Se l'espunzione dell'EDS ha reso più agevole il rilascio di un parere positivo da parte del Garante e, quindi, la prosecuzione dell'iter legislativo del Fascicolo, nella misura in cui era certamente l'aspetto più delicato dell'intera architettura, allo*

²¹⁷ V. BURATTI, *Fascicolo sanitario elettronico: verso la piena operatività?* In [Diritto e sanità](#).

²¹⁸ Provvedimento n. 256 del 8 giugno 2023.

²¹⁹ Provvedimento n. 600 del 21 dicembre 2023.

*stesso tempo rischia di costituire un limite per il nuovo sistema di servizi di sanità digitale che si presenta ora privo di un organo fondamentale*²²⁰.

7.1 Istituzione dell'Ecosistema dei Dati Sanitari in Italia e il parere negativo da parte del Garante della *Privacy*.

Il legislatore italiano è intervenuto realizzando l'Ecosistema dei Dati Sanitari (EDS) attraverso l'emanazione del decreto del Ministero della Salute del 31 dicembre 2024²²¹. Si tratta di un'infrastruttura tecnologica di notevoli dimensioni, progettata per comprendere al proprio interno i dati trasmessi al Fascicolo sanitario elettronico (FSE) dalle strutture sanitarie e sociosanitarie e dagli enti del Servizio sanitario nazionale (SSN), nonché i dati resi disponibili tramite il sistema Tessera sanitaria²²². Attraverso la raccolta e il trattamento di tali informazioni, l'EDS si propone di fornire, in modo omogeneo sul territorio nazionale, servizi di supporto alle cure, alla prevenzione, alla profilassi internazionale, al governo dell'assistenza sanitaria e alla ricerca scientifica in campo medico, biomedico ed epidemiologico. Ad esempio, l'istituzione dell'EDS consentirà la realizzazione del *dossier* farmaceutico, contenente i dati relativi a prescrizioni, erogazioni e somministrazioni di farmaci all'assistito, estratti dai documenti de FSE. Il FSE è composto da più unità di archiviazione di dati tra loro indipendenti²²³, alle quali possono accedere solo determinati soggetti, avuto riguardo al ruolo da essi esercitato e alle esigenze del trattamento²²⁴. Le strutture sanitarie, sociosanitarie e gli enti del SSN sono tenuti a estrarre i dati dal FSE e dal sistema Tessera Sanitaria per trasmetterli

²²⁰ V. BURATTI, *Fascicolo sanitario elettronico: verso la piena operatività?* In [Diritto e sanità](#).

²²¹ Sul ruolo dell'EDS a livello nazionale M. MATASSA, *Colmare i divari. Come le nuove tecnologie promettono di rivoluzionare la sanità italiana*, in *Federalismi.it*, 12, 2025, p. 173 ss.; S. CORSO, *Il fascicolo sanitario elettronico 2.0. Spunti per una lettura critica*, in *Nuove leggi civ.*, 2, 2024, pp. 334 ss.; N. POSTERARO, *La digitalizzazione della sanità in Italia: uno sguardo al Fascicolo Sanitario Elettronico (anche alla luce del Piano Nazionale di Ripresa e Resilienza)*, in *Federalismi.it*, 26, 2021, p. 189 ss.

²²² L. D'ALEO, *L'ecosistema dei dati sanitari (EDS)*, in [Diritto e sanità](#), 2025.

²²³ Precisamente: ventuno dedicate alla gestione dei dati "in chiaro" (cioè non sottoposti alla tecnica di anonimizzazione o pseudonimizzazione) associati a ciascuna regione e provincia autonoma; una contenente i dati relativi ai servizi di assistenza sanitaria erogati al personale navigante (SASN); una riservata ai dati pseudonimizzati (vale a dire non attribuibili a un interessato specifico senza l'utilizzo di informazioni aggiuntive); una finalizzata alla raccolta di dati anonimi.

all'EDS. In tale ambito, le Regioni e le Province Autonome operano come titolari del trattamento, mentre spetta all'Agenas, in qualità di responsabile, predisporre le soluzioni tecnologiche idonee a garantire uno scambio dati corretto. Deve essere assicurato il completo allineamento tra i documenti dei FSE regionali e le informazioni presenti nell'EDS, evitando duplicazioni inutili in rispetto del principio di minimizzazione. In caso il trattamento persegua una finalità di cura, di prevenzione o di profilassi internazionale, il consenso informato dell'interessato costituisce una condizione di accesso all'EDS. Quest'ultimo può anche essere prestato per via telematica o tramite delegato. In caso di revoca il soggetto precedentemente autorizzato non potrà usufruire dei servizi EDS. In merito all'accesso, questo è consentito a soggetti determinati, individuati in base alla finalità perseguita dal trattamento, precisamente²²⁵: per finalità di diagnosi, cura e riabilitazione possono consultare l'EDS le strutture sociosanitarie, i medici convenzionati e gli esercenti le professioni sanitarie che prendono in cura l'interessato, oltre ai medici di medicina generale e ai pediatri di libera scelta per il periodo in cui gli prestano assistenza; per finalità di prevenzione, l'accesso è riservato ai soggetti del SSN e dei servizi sociosanitari regionali, nonché ai professionisti sanitari che hanno in carico o assistono l'interessato; per finalità di profilassi internazionale, può procedere alla consultazione la direzione generale del Ministero della salute designata quale Centro italiano per il regolamento sanitario internazionale; per finalità di governo dell'assistenza sanitaria e per finalità di studio e di ricerca scientifica in campo medico, biomedico ed epidemiologico, infine, può accedere all'EDS il personale degli uffici del Ministero della salute, di Agenas, delle regioni e delle province autonome competenti in materia. A garanzia di un livello di sicurezza adeguato al rischio per i diritti e le libertà fondamentali degli individui, è prevista l'adozione di specifiche misure tecniche e organizzative. Tra queste rientrano l'uso di rigorosi sistemi di autorizzazione, l'impiego di protocolli di comunicazione basati su *standard* crittografici e la cifratura o separazione dei dati relativi allo stato di salute. Risulta inoltre fondamentale garantire il tracciamento puntuale degli accessi e delle operazioni effettuate all'interno dell'EDS.

L'istituzione dell'EDS risulta fondamentale per la digitalizzazione della sanità, tuttavia, il primo intervento di regolazione, mediante decreto istitutivo del FSE, ha ricevuto un

²²⁵ L. D'ALEO, *L'ecosistema dei dati sanitari (EDS)*, in [Diritto e sanità](#), 2025.

parere negativo da parte del Garante della *Privacy*²²⁶ che ha sostenuto che l'EDS *“comporta di fatto la duplicazione di dati e documenti sanitari già presenti nel FSE e determina la costituzione della più grande banca dati sulla salute del nostro Paese”*, si tratterebbe di un *database* che, sempre secondo il Garante *“raccolgerebbe a livello centralizzato, senza garanzie di anonimato per gli assistiti, dati e documenti sanitari relativi a tutte le prestazioni sanitarie erogate sul territorio nazionale”*²²⁷. Il Garante ha sottolineato l'opportunità di acquisire il previo parere dell'Agenzia per la Cybersicurezza Nazionale (ACN) ai fini dell'individuazione di misure di sicurezza adeguate al trattamento dei dati sanitari. L'Autorità evidenzia inoltre diverse criticità e profili di non conformità al GDPR, riconducibili a quattro ambiti principali²²⁸: contenuto, nel senso che manca chiarezza circa la tipologia di dati trasmessi all'EDS da parte delle strutture sanitarie, sociosanitarie, degli enti del SSN e del sistema Tessera Sanitaria; alimentazione, occorre precisare con maggiore trasparenza quali soggetti debbano alimentare l'EDS e secondo quali modalità; principi generali del trattamento, in questo senso il Garante rileva una carenza nelle garanzie per gli interessati, evidenziando come il mancato aggiornamento dei dati violi i principi stabiliti dall'articolo 5 del GDPR; valutazione del rischio, dato che, i trattamenti effettuati nell'EDS necessitano di una preventiva Valutazione di Impatto ai sensi dell'articolo 35 del GDPR, indispensabile per individuare le misure di tutela idonee a salvaguardare i diritti e le libertà degli utenti. L'intervento da parte dell'autorità è in linea con le autorità europee, infatti, il Garante rivolge un richiamo al legislatore affinché *“armonizzi il quadro normativo con la disciplina sulla privacy, bilanciando così le esigenze di digitalizzazione, trasparenza e apertura con il diritto fondamentale alla protezione dei dati personali. L'obiettivo è tutelare l'individuo non solo nella sua dimensione di utente e cittadino, ma prima di tutto come persona”*²²⁹. Infine, i profili controversi sono stati considerati risolti dal Garante che ha reso parere positivo²³⁰ sul nuovo schema di decreto. L'Autorità, dopo aver analizzato le criticità del precedente

²²⁶ Garante per la protezione dei dati personali, *Parere al Ministero della Salute sullo schema di decreto da adottare assieme al Ministro delegato per l'innovazione tecnologica e la transizione digitale, di concerto con il Ministro dell'economia e delle finanze, sull'Ecosistema Dati Sanitari (EDS)* - 22 agosto 2022 [9802752].

²²⁷ *Ivi*, p. 146.

²²⁸ *Ibidem*.

²²⁹ F. FAINI, *Governo dei dati personali nell'impiego dell'intelligenza artificiale e della blockchain da parte della sanità pubblica*, in *Diritto Mercato Tecnologia*, 2023 p. 34.

²³⁰ Tramite provvedimento n. 256 del 8 giugno 2023.

schema di decreto (provvedimento n. 294/2022) e le contromisure del Ministero, ha subordinato il parere favorevole a specifiche condizioni. La principale riguarda il coordinamento tra il decreto e le Linee guida per i servizi di telemedicina. Vengono inoltre richiesti precisi termini affinché Ministero ed enti locali informino gli utenti sui trattamenti dei dati personali tramite il FSE e promuovano campagne informative sull'alimentazione della banca dati, adempimenti già attuati e valutati positivamente dal Garante con il provvedimento n. 600 del 21 dicembre 2023.

7.2 Il FSE e il problema dell'interoperabilità.

Nel precedente paragrafo è emerso come una delle principali finalità del FSE sia quella di poter raggruppare in un'unica sede e ripercorrere la storia clinica del paziente. Ciò dipende fortemente dal mantenimento, da parte dei documenti contenuti nel FSE, delle caratteristiche di affidabilità, autenticità, integrità e leggibilità stabilite dal CAD²³¹. Diventa, quindi, fondamentale poter conservare i dati in maniera sicura e corretta. Ma, il FSE ha bisogno di rispettare una caratteristica fondamentale, cioè l'interoperabilità²³². Viene stabilito, dal d.p.c.m. n. 178/2015 che ciascuna Regione e Provincia Autonoma deve istituire il Fascicolo Sanitario Elettronico attraverso un'infrastruttura in grado di interoperare con altre soluzioni regionali di FSE²³³. In sostanza, è fondamentale che tra i sistemi regionali ci sia “dialogo”, soprattutto in casi di mobilità sanitaria interregionale²³⁴. L'interoperabilità risulta essenziale: *“da un punto di vista pratico, per consentire a un paziente di rivolgersi a differenti professionisti e strutture, ubicati in Regioni diverse da quelle di residenza, o fuori dal territorio nazionale, favorendo un approccio multiprofessionale e multidisciplinare alle cure e consentendo la prevenzione e la*

²³¹ Codice dell'amministrazione digitale, i principi enunciati sono presenti all'art. 44 del dlgs 3 marzo 2005, n. 82.

²³² Più in generale sull'interoperabilità nelle politiche di digitalizzazione della pubblica amministrazione G. CARULLO, *Interoperabilità dei dati e riflessi organizzativi*, in R. CAVALLO PERIN, *L'amministrazione pubblica con i big data*, Torino, 2021, pp. 251-259.

²³³ E. SORRENTINO, A.F. SPAGNUOLO, *La sanità digitale in emergenza Covid-19. Uno sguardo al fascicolo sanitario elettronico*, in *Federalismi*, 2020.

²³⁴ N. POSTERARO, *La digitalizzazione della sanità in Italia: uno sguardo al Fascicolo Sanitario Elettronico (anche alla luce del Piano Nazionale di Ripresa e Resilienza)*, in *Federalismi.it*, 2021, p. 206.

diagnosi precoce. Secondo una prospettiva più ampia, l'interoperabilità risulta funzionale al governo del sistema sanitario, in termini di programmazione e monitoraggio, nonché a esigenze di studio e ricerca scientifica"²³⁵.

L'interoperabilità tocca tutto il processo di digitalizzazione della pubblica amministrazione e l'Unione Europea ha emanato il Quadro europeo d'Interoperabilità che fornisce principi e modelli adeguati a garanzia del raggiungimento di quest'ultima. A livello nazionale il CAD si occupa del tema a partire dall'art. 12, co. 2, in base al quale *"Le pubbliche amministrazioni utilizzano, nei rapporti interni, in quelli con le altre amministrazioni e con i privati, le tecnologie dell'informazione e della comunicazione, garantendo l'interoperabilità dei sistemi e l'integrazione dei processi di servizio fra le diverse amministrazioni..."*. Ma, a causa dell'eterogeneità dei dati è complicato riuscire a creare sistemi totalmente interoperabili tra le amministrazioni pubbliche. Proprio per questa ragione, il PNRR ha disposto il potenziamento delle infrastrutture tecnologiche e dell'interoperabilità delle banche dati della Pubblica Amministrazione. L'obiettivo è snellire le procedure pubbliche applicando pienamente il principio europeo del *"once only"*, che evita al cittadino l'onere di fornire più volte le stesse informazioni a diverse amministrazioni. A tal fine, è stata istituita tramite l'articolo 50-ter del CAD, la Piattaforma Nazionale Dati: un'infrastruttura che offrirà alle PA un catalogo centralizzato di connettori automatici²³⁶ (le cosiddette API – *Application Programming Interface*), accessibili tramite un servizio dedicato e operanti in un contesto di totale conformità alle normative europee sulla *privacy*²³⁷. Con specifico riferimento al FSE, e proprio per rispondere alla necessità di garantirne l'interoperabilità, la Legge di Bilancio 2017 ha modificato l'art. 12 del d.l. n. 179/2012. La norma ha affidato all'AgID, d'intesa con i Ministeri della Salute e dell'Economia e delle Finanze, la progettazione dell'Infrastruttura Nazionale per l'Interoperabilità (INI), concepita come macro-modello di gestione dell'intera rete dei FSE regionali. Nello specifico, i diversi sistemi regionali dialogano con l'infrastruttura INI per raccogliere, richiedere e trasmettere dati e documenti sanitari. Tali flussi avvengono in modalità sicura e nel pieno rispetto delle scelte di consenso

²³⁵ V. BURATTI, *Fascicolo sanitario elettronico: verso la piena operatività?* In [Diritto e sanità](#).

²³⁶ Sul punto, G. BUTTARELLI, *Dati e interoperabilità nella pubblica amministrazione*, in *Osservatorio IRPA sullo Stato Digitale*.

²³⁷ N. POSTERARO, *La digitalizzazione della sanità in Italia: uno sguardo al Fascicolo Sanitario Elettronico (anche alla luce del Piano Nazionale di Ripresa e Resilienza)*, in *Federalismi.it*, 2021, p. 208.

espresse dagli assistiti. Nel 2018 è stata completata l'Infrastruttura nazionale per l'Interoperabilità e ciò ha permesso di passare da un modello federato, in cui appena 10 Regioni risultavano collegate, ma senza una reale interoperabilità, in favore di un sistema centralizzato nazionale. La nuova architettura è, infatti, in grado di connettere stabilmente tutte le Regioni e di rendere finalmente comunicanti i rispettivi fascicoli sanitari territoriali²³⁸.

8. Conclusioni.

In conclusione, l'evoluzione della sanità digitale si configura come un processo complesso in cui le opportunità offerte dall'innovazione tecnologica e dalle risorse del PNRR si intrecciano con la necessità di una *governance* solida e bilanciata²³⁹. Il progressivo accentramento normativo ed esecutivo in capo alla Commissione Europea, affiancato a livello nazionale da fonti di *soft law* e da autorità di settore come l'AGENAS, mira a garantire uniformità, flessibilità e sicurezza nella gestione dei dati sanitari. La piena valorizzazione del patrimonio informativo, guidata dai principi *FAIR* e *TRUST* e dall'apertura agli *OpenData*, trova applicazione concreta in strumenti chiave quali il Fascicolo Sanitario Elettronico (FSE), la Cartella Clinica Elettronica, la telemedicina e la *blockchain*. Tuttavia, il perseguimento dell'interoperabilità dei sistemi e la creazione di grandi banche dati come l'Ecosistema dei Dati Sanitari (EDS) impongono di superare il *digital divide* e le frammentazioni regionali, richiedendo un costante bilanciamento tra l'efficienza dell'azione pubblica e le tutele fondamentali della *privacy*, al fine di porre sempre al centro la dignità della persona e la relazione di cura.

²³⁸ *Ibidem*.

²³⁹ F. VALENTINI, *La sanità digitale tra regolazione, organizzazione amministrativa e azione terapeutica*, in *Munus*, 2023, 2, pp. 449-486.

CAPITOLO III

INTELLIGENZA ARTIFICIALE E SANITÀ PUBBLICA: OPPORTUNITÀ E CRITICITÀ

SOMMARIO: 1. L'impiego dell'intelligenza artificiale nella sanità pubblica: prime coordinate - 2. Intelligenza artificiale e sanità: profili definitori - 2.1 Le applicazioni pratiche dei sistemi di I.A. in sanità: tra opportunità e limiti - 3. Il Regolamento europeo 2024/1689: il primo tentativo di regolamentazione dell'IA – 3.1 L'intervento del legislatore italiano: la nuova legge quadro n. 132/2025 sull'intelligenza artificiale - 4. La trasformazione digitale della sanità: il modello *Value-Based Healthcare* - 4.1 L'Intelligenza Artificiale come strumento essenziale nella transizione verso il modello *Value Based HealthCare: il caso Babylon Health* - 5. I rischi legati al fenomeno della discriminazione algoritmica – 5.1 Dal primo caso giurisprudenziale all'art. 30 d.lgs n. 36/2023: la positivizzazione della non discriminazione algoritmica - 6. Il futuro della medicina? Neurotecnologie e *Brain Computer Interface*: tra applicazioni pratiche ed esigenze di regolamentazione - 6.1 Un accenno ai c.d. neurodiritti - 7. Conclusioni.

1. L'impiego dell'intelligenza artificiale nella sanità pubblica: prime coordinate.

Una grande quantità di dati rappresenta un substrato conoscitivo utile per l'impiego di strumenti di intelligenza artificiale che, nel settore della sanità pubblica, può rappresentare un importante strumento idoneo al perseguimento di innumerevoli funzioni.

Il presente capitolo analizza l'impatto trasformativo e le criticità legate all'integrazione dell'intelligenza artificiale e delle nuove tecnologie nella sanità pubblica. L'indagine prende avvio dall'esame delle implicazioni etiche e delle applicazioni pratiche dell'IA, sia organizzative sia diagnostiche, bilanciando le opportunità di innovazione con i rischi legati all'opacità algoritmica e alla tutela della privacy. Viene, poi, approfondito il quadro normativo di riferimento, fondato sull'approccio basato sul rischio dell'*AI Act* europeo e sulle recenti disposizioni nazionali (L. 132/2025) a garanzia della centralità della decisione medica e dell'inclusione. La trattazione prosegue esaminando la transizione verso il modello *Value-Based Healthcare* e l'adozione strategica di soluzioni *data-driven*, per poi affrontare il tema della discriminazione algoritmica e dei *bias* nei dataset. Infine, lo sguardo si estende alle frontiere più avanzate della medicina, analizzando le

neurotecnologie e le *Brain Computer Interface* (BCI), unitamente alle complesse sfide regolatorie e alla nascita dei cosiddetti "neurodiritti" a tutela dell'integrità e della riservatezza mentale dell'individuo.

2. Intelligenza artificiale e sanità: profili definitori.

Risulta complicato dare una definizione unitaria del termine *eHealth* a causa del fatto che, questa espressione comprende diversi istituti e categorie, tra cui la telemedicina e il Fascicolo Sanitario Elettronico²⁴⁰, ma anche l'impiego di strumenti di intelligenza artificiale. È importante, prima di soffermarsi sull'aspetto specifico, cioè di come l'intelligenza artificiale ha impattato sulla sanità, parlare delle questioni etiche connesse all'uso dell'intelligenza artificiale in questo ambito²⁴¹. Innanzitutto, la *privacy*: rimane fondamentale (e obbligatorio per legge) proteggere i dati personali della persona. Nei capitoli precedenti è stato affrontato il discorso relativo al necessario bilanciamento dei diritti, ora, sappiamo che l'accesso a grandi quantità di dati è decisivo al fine di tutelare la salute pubblica, e che, quest'uso potrebbe portare a conflitti con la libertà individuale²⁴². Rimane necessario ribadire l'importanza del tema della sicurezza, cioè l'esigenza di poter proteggere i dati da abusi e violazioni da parte di terzi. Se il Regolamento EHDS è nato come risposta dell'Unione Europea per bilanciare i diritti individuali e l'interesse pubblico, oggi emerge la necessità di riconoscerne una portata più profonda. Oltre a fornire gli strumenti tecnici per la gestione e la condivisione dei dati, il Regolamento ha infatti consacrato la *privacy* come espressione piena e compiuta della libertà, sia individuale sia collettiva. Infatti, “*non si tratta semplicemente di tutelare un diritto fondamentale, bensì di custodire un bene relazionale che riguarda il modo in cui ciascuno di noi si offre o si sottrae allo sguardo altrui, anche quando questo sguardo è mediato da algoritmi o da pratiche cliniche guidate dall'intelligenza dei dati (in gergo*

²⁴⁰ T. BALDUZZI, D. MORANA, F. MORGANTI, *La salute “intelligente”: eHealth, consenso informato e principio di non-discriminazione*, in *Federalismi.it*, 2022, p. 129.

²⁴¹ F. TRUBIANI, L. GRION, *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, 2025, p. 4.

²⁴² Intesa sia come diritto alla riservatezza che come autonomia decisionale.

data-driven)”²⁴³. In questo senso, la trasparenza, il consenso informato e la possibilità di controllare l’accesso ai propri dati diventano prima presidi morali e, successivamente, garanzie giuridiche. La problematica riguarda la difficoltà a coniugare ciò che precede con l’obiettivo di difendere e promuovere la salute pubblica. È necessario ricordare che non si è di fronte ad un problema tecnico, anche se alcuni lo considerano come tale²⁴⁴, ma si tratta di una problematica legata al bilanciamento dei diritti. Per riuscire a trovare una soluzione, sono necessari due presupposti fondamentali: la fiducia e il riconoscimento di un dovere. La fiducia negli altri soggetti è fondamentale, nell’ottica in cui ognuno deve rinunciare a qualcosa per il bene degli altri, mentre il riconoscimento di un dovere è il corrispettivo necessario di ogni diritto²⁴⁵ ed è quindi di primaria importanza per evitare di tramutare ogni rivendicazione in una pretesa unilaterale. In merito al bilanciamento dei diritti bisogna soffermarsi sulla qualità e sulla rappresentatività dei dati impiegati nell’addestramento dei sistemi di *machine learning*. Analizzare questi sistemi è fondamentale, considerando che, apprendono a partire da dati storici (anche incompleti, parziali o distorti) per incorporare le disuguaglianze preesistenti nel contesto dal quale provengono²⁴⁶. Il *machine learning* è utilizzato per costruire modelli predittivi basati sui dati storici. Inoltre, nel *machine learning* supervisionato, i modelli vengono addestrati su un insieme di dati etichettati, dove ogni esempio di *input* è associato a un’etichetta corretta. In questo modo, i modelli possono apprendere le relazioni tra le caratteristiche dei dati e le rispettive classi, in modo da poter svolgere delle predizioni su nuovi dati²⁴⁷. Si tratta di una metodologia molto utilizzata nel settore biomedico soprattutto per l’analisi delle immagini diagnostiche. Si tratta, quindi, di un problema di *dataset*, infatti, da una parte possono contenere pregiudizi e dall’altra possono rappresentare categorie minoritarie. A causa della composizione dei *dataset* si riduce la capacità predittiva dell’algoritmo e si rischia, quindi, di ritardare o compromettere diagnosi per intere fasce di popolazione. Un altro problema riguarda la trasparenza: nei sistemi di *deep learning*, nei quali si usano reti neurali profonde, la capacità di raggiungere risultati accurati è

²⁴³ *Ivi*, p. 5.

²⁴⁴ La soluzione potrebbe essere quella di affidarsi ad architetture informatiche che riducano il rischio di ricondurre dati anonimizzati agli individui che li avevano prodotti.

²⁴⁵ *Ivi*, p. 7.

²⁴⁶ *Ivi*, p. 8.

²⁴⁷ F. TRUBIANI, M. CESARELLI, F. MERCALDO, *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, 2025, p. 16.

comparabile a quella di uno specialista umano, il problema riguarda però il modo in cui pervengono alle conclusioni. La difficoltà a comprendere il “ragionamento” (da parte dei fruitori) dietro le scelte dei sistemi deriva dalla complessità della loro architettura matematica, si parla delle *black box* (scatole nere), sistemi che forniscono risultati ma senza spiegazioni²⁴⁸. In questo senso, nell’ambito sanitario²⁴⁹, emergono i lati negativi di questa opacità. Infatti, nel contesto delle professioni di cura *“un’indicazione algoritmica priva di giustificazioni comprensibili non può essere sufficiente, tanto più se si considera che tali professioni sono vincolate da precisi obblighi deontologici. Per un medico, infatti, agire “in scienza e coscienza” non è una formula retorica, ma un principio fondamentale, che implica la capacità di comprendere e motivare ogni scelta clinica.”*²⁵⁰ Da queste premesse emerge la necessità di garantire la trasparenza e l’intellegibilità delle decisioni algoritmiche (*explainability*). Nel contesto della pratica medica, infatti, non è sufficiente disporre di un responso automatizzato di cui si conosca solo la percentuale di affidabilità statistica; l’azione clinica richiede di comprenderne le logiche sottostanti. Si tratta di una sfida complicata, affinché l’intelligenza artificiale possa essere integrata totalmente nella pratica clinica, sarà necessaria la collaborazione tra differenti esperti nei vari settori (ingegneri, medici, giuristi, economisti etc.). Sarà sempre più necessario rendere le decisioni prese dai sistemi di IA affidabili, sicure e accessibili per ottenere la fiducia da parte di professionisti e pazienti. L’intelligenza artificiale ha le potenzialità per poter trasformare la medicina e migliorare la salute globale, per farlo, bisognerà puntare ad un approccio equilibrato tra innovazioni tecnologiche ed etica.

La dottrina amministrativistica si sta interrogando sull’impiego di strumenti di IA in sede procedimentale²⁵¹ e con riferimento ai servizi pubblici. Infatti, *“l’intelligenza artificiale rende possibile una conoscenza minuziosa del comportamento delle persone in un dato*

²⁴⁸ *Ivi*, p. 9.

²⁴⁹ Va specificato che in altri ambiti la mancata trasparenza delle decisioni da parte dei sistemi può essere tollerabile o irrilevante, ad esempio la scelta del percorso più rapido da parte di un navigatore.

²⁵⁰ F. TRUBIANI, L. GRION, *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, 2025, p. 9.

²⁵¹ Sul punto, senza pretesa di esaustività, G. Avanzini, *Decisioni amministrative e algoritmi informatici*, Napoli, 2019, G. GALLONE, *Riserva di umanità e funzioni amministrative*, Milano, 2023, B. MARCHETTI, *Intelligenza artificiale, poteri pubblici e rule of law*, in *Riv. It. Dir. Pubblico Comunitario*, 2024, 1, pp.49-64. S. C. MATTEUCCI, *Umano troppo umano. Decisioni amministrative automatizzate e principio di legalità*, in *Diritto pubblico*, 2019, 1, pp. 5-41, E. Carloni, *Critica dell’amministrazione artificiale*, Bologna, 2026.

contesto (es. un'area metropolitana) o settore (le community), consentendo di ripensare integralmente la soddisfazione dei bisogni sociali, comprese le prestazioni di servizio pubblico, con soluzioni che paiono mettere seriamente in crisi le impostazioni finora prevalenti. Non si tratta solo di un aspetto conoscitivo del tipo di bisogni sociali delle comunità locali, ma altresì delle risposte che le persone provano a dare ai medesimi, con l'autorganizzazione o la fruizione di prestazioni a titolo gratuito, che gli algoritmi presenti in rete consentono di rilevare e definire in vario modo (es. BlaBlaCar per il trasporto; lezioni di storia o di economia per l'istruzione; ecc.)”²⁵².

2.1. Le applicazioni pratiche dei sistemi di I.A. in sanità: tra opportunità e limiti.

L'intelligenza artificiale è uno strumento essenziale per sanità moderna e ha permesso l'evoluzione di quest'ultima, difatti gli ambiti applicativi sono vari.

Il primo campo applicativo riguarda la gestione dei processi organizzativi. Infatti, una buona sanità deve avere alla propria base una gestione efficiente dei processi organizzativi sia dal punto di vista nazionale che territoriale, risulta quindi di fondamentale importanza poter contare su dati disponibili in tempo reale, accessibili e interpretabili. In questo senso si sviluppano i sistemi di *business intelligence* (BI), algoritmi in grado di organizzare, analizzare, e contestualizzare i dati, fino a trasformarli, da dati grezzi, in informazioni significative. I sistemi BI si sviluppano su tre libelli di complessità: il livello descrittivo che permette di aggregare i dati e fornire informazioni in merito ai processi in atto; il livello predittivo, un software capace di eseguire proiezioni statistiche basate sull'andamento tendenziale dei dati passati; e, infine, un livello prescrittivo, basato su agenti IA, che compie azioni autonome²⁵³. Nell'organizzazione sanitaria, i sistemi di *Business Intelligence* (BI) offrono un supporto strategico a due livelli: centralmente, consentono alla direzione di pianificare il fabbisogno di personale e apparecchiature sulla

²⁵² Sul punto, R. C. PERIN, C. JACOD, *I servizi pubblici con l'intelligenza artificiale*, in *Il Diritto dell'Amministrazione Pubblica digitale*, 2025, p. 193.

²⁵³ F. TRUBIANI, A. LAGHI, *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, 2025, p. 23.

base delle reali esigenze del territorio. A livello periferico, ottimizzano l'efficienza delle singole aziende sanitarie, migliorando la gestione del *triage* nei dipartimenti d'emergenza, i ricoveri ospedalieri e l'organizzazione delle liste d'attesa.

In merito a queste ultime, dal primo agosto 2024 sono entrate in vigore nuove regole per la gestione delle liste d'attesa nelle prestazioni sanitarie²⁵⁴. Questo perché la garanzia di un tempestivo accesso alle cure rappresenta uno degli strumenti fondamentali di tutela del diritto alla salute. Tra gli interventi più significativi troviamo il potenziamento dei Centri Unici di Prenotazione (CUP) e l'incremento dell'offerta di visite mediche e specialistiche²⁵⁵. Risulta necessario soffermarsi sull'istituzione, da parte di AGENAS, della Piattaforma nazionale delle liste d'attesa, presentata come uno degli strumenti più innovativi introdotti dal legislatore, in quanto in grado di verificare in tempo reale i tempi di attesa e il rispetto delle priorità nell'erogazione delle prestazioni sanitarie su tutto il territorio nazionale²⁵⁶.

Tali sistemi sono utili anche per alleggerire il carico burocratico in capo al medico, permettono di automatizzare le attività amministrative e routinarie. Inoltre, si tratta di sistemi integrati con la Cartella Clinica Elettronica e con il Fascicolo Sanitario Elettronico, e possono consentire di velocizzare la comunicazione tra paziente e medico. In ultimo troviamo anche gli *ambient scribe*, sistemi che, “ascoltando” il dialogo tra professionista sanitario e paziente, riescono a sintetizzare le informazioni ed inviarle in via telematica all'interessato²⁵⁷. In sostanza, il BI permette di migliorare l'esperienza di cura sia per il medico che per il paziente e migliorare l'efficienza operativa nel settore della sanità.

In ambito di diagnosi e cura l'utilizzo dei sistemi di IA è sempre più presente. Spesso, si tratta di un apporto non visibile agli utenti/pazienti, ad esempio l'utilizzo nella radiologia per l'analisi delle immagini. Esistono, però, anche sistemi visibili come quelli che sono in grado di interpretare il tracciato dell'elettrocardiogramma, o che possono supportare il

²⁵⁴ Attraverso la L. n. 107 del 29 luglio 2024 è stato convertito, con modifiche, il D.L. 7 giugno 2024, n. 73.

²⁵⁵ È l'articolo 4, al comma 1, a prevedere che le visite possono essere effettuate anche nei giorni di sabato e domenica e che per l'erogazione di tali prestazioni la fascia oraria possa essere prolungata.

²⁵⁶ G. AVANZINI, *Liste d'attesa sanità: nuove regole dal 1° agosto, 2024*, in [Centro studi Diritto e Sanità](#).

²⁵⁷ *Ivi*, p. 24.

lavoro del radiologo evidenziando specifici reperti negli esami diagnostici. Tali sistemi sono in grado di ridurre gli errori diagnostici, di rendere prioritaria l'analisi di immagini contenenti reperti potenzialmente gravi e di ridurre i tempi di lavoro, migliorando l'efficienza delle procedure diagnostiche.

La comunicazione tra medico e paziente è cambiata con l'avvento dei sistemi di IA. Innanzitutto, è fondamentale affermare che la relazione tra il medico e il paziente è la solida base dell'alleanza terapeutica e della medicina centrata sulla persona²⁵⁸. Di conseguenza, se da un lato delegare interamente la comunicazione all'intelligenza artificiale solleva forti perplessità, dall'altro il suo impiego come supporto nelle attività routinarie rappresenta una valida soluzione, specialmente per alleggerire l'elevato carico di lavoro dei professionisti. Un'applicazione pratica è rappresentata dai *chatbot* algoritmici, impiegati per rispondere ai quesiti dei pazienti per garantire risposte più rapide e precise. Tuttavia, nella realtà clinica, la necessità di una costante supervisione medica per prevenire i frequenti errori degli algoritmi fa sì che, al momento, non sia ancora dimostrato un effettivo risparmio di tempo per i professionisti. Un altro esempio riguarda gli algoritmi in grado di semplificare il linguaggio dei referti radiologici, rendendo il paziente autonomo nella comprensione del risultato evitando termini tecnici difficilmente comprensibili. Trattandosi di tecnologie mediatrici tra medico e paziente, il loro impiego comporta inevitabili rischi. Innanzitutto, l'uso dell'IA rischia di compromettere il senso di prossimità e l'ascolto empatico percepiti dal paziente, impoverendo la qualità relazionale del colloquio clinico. Inoltre, questi sistemi richiedono regole d'ingaggio rigorose per evitare che comunicazioni cruciali per la vita del paziente vengano gestite in modo impersonale da un algoritmo. Risulta quindi fondamentale che l'adozione dell'IA, nel settore sanitario, sia accompagnata da un'adeguata formazione dei professionisti sanitari, sia in merito alle capacità tecniche che alle abilità comunicative e le riflessioni etiche²⁵⁹. L'obiettivo, non è quello di sostituire la relazione terapeutica, ma è quello di potenziarla tramite l'integrazione di sistemi di IA adeguati.

²⁵⁸ F. TRUBIANI, A. LAGHI, *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, 2025, p. 26.

²⁵⁹ F. TRUBIANI, A. LAGHI, *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, 2025, p. 27.

Il tema della formazione è, anch'esso, di primaria importanza. Integrare l'IA nella formazione medica permette di puntare ad un'innovazione su più fronti: la possibilità di personalizzare i percorsi formativi, tramite un adattamento dei contenuti in base alle esigenze dei singoli studenti, permette di aumentare l'efficacia dell'apprendimento. Inoltre, le opportunità legate all'utilizzo di simulazioni virtuali (come la realtà aumentata, tramite visori) sono varie e *“permettono di replicare scenari clinici complessi in un ambiente controllato, offrendo agli studenti la possibilità di esercitarsi in sicurezza e sviluppare competenze pratiche senza rischi per i pazienti”*²⁶⁰. Si tratta di strumenti simulativi che sono diventati, sempre più, fondamentali per la formazione in aree critiche (chirurgia, procedure interventistiche etc.). Infine, tramite i sistemi di IA, la formazione continua dei professionisti viene supportata con continui aggiornamenti e ciò permette di mantenere un elevato standard di cura, è in questo senso che diventa necessario affermare come la sinergia tra formazione medica e IA sia un'occasione primaria per innovare l'educazione sanitaria, migliorare le competenze cliniche ed elevare la qualità dell'assistenza ai pazienti.

L'intelligenza artificiale ricopre ormai un ruolo centrale nella ricerca biomedica, grazie a strumenti avanzati in grado di analizzare grandi volumi di dati, accelerare la scoperta di nuovi farmaci e favorire la personalizzazione delle terapie. In questo senso, l'ambito più promettente riguarda le cd. scienze “-omiche” (radiomica, genomica etc.) nelle quali i sistemi di IA sono utilizzati come supporto per l'interpretazione dei dati. Inoltre, nell'ambito della *drug discovery* (scoperta dei farmaci) l'implementazione di sistemi di IA permette di ridurre i costi ed i tempi di sviluppo. Forse, la novità più interessante riguarda il concetto di *digital twin* (DT)²⁶¹. Il DT si riferisce alla creazione di una controparte digitale e dinamica di un'entità fisica, aggiornata costantemente tramite i dati in tempo reale provenienti da sensori e simulazioni. Attraverso l'impiego di algoritmi predittivi e apprendimento automatico, l'IA contribuisce fortemente allo sviluppo e all'evoluzione dei DT²⁶². Questi ultimi sono impiegati per costruire modelli personalizzati di pazienti, basati su dati clinici, genetici e biometrici con l'obiettivo di

²⁶⁰ Ivi, p. 28.

²⁶¹ F. TRUBIANI, A. LAGHI, *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, 2025, p. 29.

²⁶² Sull'uso dei *digital twin* in sanità G. Capilli, Digital Twin in sanità: innovazioni, opportunità e sfide giuridiche, in *Rivista italiana di medicina legale e del diritto in campo sanitario*, 2024, 3-4, pp. 527-535.

simulare l'effetto di terapie specifiche, monitorare l'evoluzione delle patologie e supportare la decisione clinica²⁶³.

Le soluzioni precedentemente citate ed affrontate sono il frutto dell'evoluzione tecnologica all'interno del settore sanitario e, oltre ad essere efficaci, sono commercialmente disponibili. Occorre, tuttavia, considerare l'esistenza di limiti oggettivi che ostacolano la concreta implementazione delle soluzioni analizzate. In primo luogo, l'efficacia di tali modelli è strettamente vincolata alla qualità del patrimonio informativo sanitario: la disponibilità, l'organizzazione, la classificazione e la corretta gestione dei dati rappresentano prerequisiti imprescindibili affinché gli algoritmi possano operare. In questo senso, viene sviluppato il Fascicolo Sanitario Elettronico, già precedentemente affrontato, strumento digitale attraverso il quale è possibile raccogliere e gestire i dati sanitari in modo integrato e sicuro. L'obiettivo principale è quello dell'interoperabilità tra i sistemi tra pazienti, operatori sanitari, istituzioni di ricerca, aziende tecnologiche e Stati membri.

Per quanto riguarda il livello operativo locale, l'applicazione dei sistemi di IA in ambito sanitario locale non si può basare solamente sull'innovazione tecnologica; infatti, quest'ultimo per funzionare richiede interventi organizzativi, culturali e normativi per favorire l'interoperabilità e una corretta gestione dei dati²⁶⁴. Ciò comporta delle difficoltà: la mancanza di *standard* condivisi, la frammentazione dei sistemi e la presenza di dati sanitari, spesso, distribuiti su sistemi non centralizzati, ostacolano la condivisione dei dati ed il raggiungimento dell'obiettivo, cioè la creazione di un *dataset* di qualità. Inoltre, a causa della separazione tra pubblico e privato a livello locale e dell'assenza di una *governance* unificata l'efficacia complessiva dei sistemi di IA viene ridotta. Per far fronte alla complessità organizzativa delle strutture sanitarie sarà necessaria una sinergia tra diverse figure professionali (ingegneri clinici, medici, informatici, *data scientist* etc).

L'evoluzione e lo sviluppo dell'IA nell'ambito sanitario incontra questioni regolatorie ed etiche. Per quanto riguarda la normativa, dal punto di vista regolatorio, è fondamentale poter garantire la sicurezza, l'efficacia e l'affidabilità dei sistemi. Per farlo, sono necessari dei processi di validazione e certificazione che devono tenere conto della natura evolutiva

²⁶⁴ Ivi, p. 32.

dell'IA in grado di apprendere e modificarsi nel tempo, oltre a sistemi di monitoraggio delle prestazioni. Gli interventi più recenti riguardano il Regolamento Europeo per i Dispositivi Medici (MDR)²⁶⁵ e l'*Artificial Intelligence Act*²⁶⁶, normative che si occupano di creare un quadro giuridico specifico per i produttori di soluzioni di IA in sanità.

Rimane fondamentale il tema della protezione dei dati personali, va rispettato il GDPR, assicurando un trattamento corretto dei dati, promuovendo l'anonimizzazione e il consenso informato.

In merito all'etica, emergono delle problematiche riguardanti le decisioni automatizzate che devono essere comprensibili, spiegabili e verificabili sia per i pazienti che per i professionisti sanitari²⁶⁷.

L'equità, anch'essa, deve essere garantita nel senso che gli algoritmi devono essere sviluppati e allenati su dati rappresentativi, per evitare eventuali pregiudizi che possano comportare discriminazioni future²⁶⁸.

Infine, l'utilizzo di soluzioni di IA in sanità impatta, e non poco, sulla sostenibilità ambientale ed economica. Per quanto riguarda la prima, l'IA può favorire una logistica ospedaliera più ottimizzata, permette anche di minimizzare i ricoveri e, di conseguenza, abbattere i consumi che derivano da questi ultimi. Consente anche un'importante riduzione dei materiali cartacei e degli spostamenti fisici favorendo un sistema sanitario più improntato al rispetto e alla tutela dell'ambiente. Sul piano della sostenibilità economica, la definizione di nuove politiche sanitarie sarà determinante per prevenire disparità nell'accesso alle cure. I sistemi di intelligenza artificiale richiedono ingenti investimenti finanziari; di conseguenza, la limitatezza delle risorse disponibili, che penalizza in particolare le strutture sanitarie locali minori, rischia di generare asimmetrie territoriali e diseguaglianze nell'erogazione delle prestazioni.

In ultima istanza, è necessario affrontare il tema dell'interazione tra IA e i professionisti sanitari, quest'ultima sarà efficiente nel momento in cui si riuscirà a creare un sistema

²⁶⁵ Regolamento UE 2017/745.

²⁶⁶ Regolamento UE 13 giugno 2024, n. 1689.

²⁶⁷ Ritorna il tema, precedentemente affrontato, dell'opacità delle decisioni algoritmiche.

²⁶⁸ F. TRUBIANI, A. LAGHI, *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, 2025, p. 33.

fondato sulla fiducia reciproca, sulla formazione continua e su una adeguata distribuzione delle responsabilità²⁶⁹. Il c.d. *digital gap* (divario digitale) è alla base delle resistenze all'adozione dei sistemi di IA in ambito sanitario. L'adozione dei sistemi di IA può portare i professionisti a temere una sostituzione del lavoro umano o una perdita di autonomia, è quindi necessario accompagnare il cambiamento tramite operazioni di formazione continua e di aggiornamento digitale. È importante affermare che gli algoritmi non possono sostituire, interamente, il lavoro del professionista sanitario, dato che, nella realtà clinica molti eventi sono frutto di situazioni imprevedibili o di emergenza che non possono essere affidate al calcolo di un algoritmo e per le quali sono necessari altri elementi come l'esperienza.

In conclusione, l'intelligenza artificiale rappresenta già una solida realtà nel settore sanitario, destinata a offrire opportunità sempre più significative a vantaggio di pazienti e professionisti. Tuttavia, il suo consolidamento richiede una *governance* rigorosa, fondata su pilastri imprescindibili: imparzialità, equità, tutela della privacy, sicurezza, responsabilità e sostenibilità ecologico-ambientale.

3. Il Regolamento europeo 2024/1689: il primo tentativo di regolamentazione dell'AI

Nelle pagine precedenti si è accennato a un intervento normativo dell'Unione Europea in merito alla regolamentazione dei sistemi di IA. Si tratta dell'*AI Act*²⁷⁰, il Regolamento costituisce la prima disciplina organica sull'IA e ha un duplice scopo: da un lato, stimolare lo sviluppo e l'adozione di sistemi di IA che siano innovativi, sicuri e affidabili in tutto il mercato unico europeo; dall'altro, garantire la tutela dei diritti fondamentali, della sicurezza e della salute dei cittadini²⁷¹. Il principio base sul quale si fonda il Regolamento

²⁶⁹ Ivi, p. 34.

²⁷⁰ Regolamento UE n. 2024/1689.

²⁷¹ M. MILAN, *Intelligenza artificiale e diritto positivo: dal Regolamento (UE) 2024/1689 alla legge italiana 23 settembre 2025, n. 132*, Guide pratiche in *Banca Dati OneLegale*.

è quello di proporzionalità, in base al quale, più il rischio che deriva da un sistema è elevato, più rigorose saranno le regole che lo governano²⁷².

L'intelligenza artificiale è definita dal Regolamento come un sistema automatizzato capace di operare con gradi diversi di autonomia, che riceve dati o input e produce output, come previsioni, decisioni o contenuti, in funzione di obiettivi espliciti o impliciti²⁷³. La definizione comprende tutto il ciclo di progettazione, addestramento, validazione e utilizzo, di fatti, il rischio non deriva solo dal prodotto finale, ma può derivare anche dal modo in cui il sistema viene gestito e concepito. Il Regolamento si fonda su un approccio basato sul rischio (*risk-based*) dove gli usi dell'IA vengono classificati in funzione del loro potenziale danno sociale o individuale. Il Regolamento riserva gran parte delle proprie norme ai sistemi di IA reputati ad alto rischio, in quanto maggiormente suscettibili di incidere su diritti fondamentali delle persone, sul processo democratico, sulla salute, sulla sicurezza e sulle libertà individuali²⁷⁴. I rischi sono suddivisi in livelli: i sistemi "ad alto rischio" (disciplinati all'articolo 5 del Regolamento) comprendono quelli impiegati nei settori più sensibili (sicurezza, istruzione, accesso ai servizi etc) e devono rispettare requisiti stringenti di accuratezza, trasparenza, sorveglianza umana, gestione dei dati e sicurezza informatica, oltre a essere registrati in un'apposita banca dati europea; successivamente viene individuato un "*rischio inaccettabile*" (disciplinati all'articolo 5 del Regolamento) che comporta il divieto assoluto dello svolgimento di differenti pratiche. Tali sono i sistemi che manipolano il comportamento umano attraverso tecniche subliminali o ingannevoli, che sfruttano vulnerabilità individuali (legate all'età, alla disabilità o alla condizione economica), che attribuiscono punteggi sociali o prevedono la propensione criminale delle persone basandosi su dati di personalità. Inoltre, è vietato l'uso indiscriminato del riconoscimento facciale in tempo reale in spazi pubblici, salvo eccezioni rigidamente circoscritte per la sicurezza nazionale o la ricerca di persone scomparse, previa autorizzazione giudiziaria. Il Regolamento ricomprende nel novero dei sistemi ad alto rischio anche quelli destinati ad essere impiegati in ambito sanitario. È l'articolo 6 dell'AI Act ad includere tra i sistemi di IA reputati ad alto rischio quelli che

²⁷² Rimangono esclusi sistemi militari o di difesa.

²⁷³ Art. 3, par. 1, Regolamento UE n. 2024/1689.

²⁷⁴ A. AMIDEI, *L'AI Act in Gazzetta Ufficiale: l'impatto sul settore sanitario e il contesto italiano (in divenire)*, in [Diritto e Sanità](#), 2024.

costituiscono prodotti, o componenti di prodotti, già soggetti a valutazione preventiva di conformità ai sensi delle norme eurounitarie elencate all'Allegato I del Regolamento; ove tra esse è espressamente ricompreso anche il Regolamento UE 2017/745 in materia di dispositivi medici, nonché il Regolamento UE 2017/746 concernente i dispositivi medici *in vitro*. L'inclusione dei sistemi di IA destinati all'impiego in ambito medico tra quelli classificati come ad alto rischio comporta delle conseguenze per gli operatori del settore, intesi come produttori e sviluppatori (*deployer*) dei sistemi. Il Regolamento, all'articolo 3, definisce con tale locuzione chiunque utilizzi un sistema di IA nell'ambito di un'attività professionale, definizione, quest'ultima, che ben potrebbe applicarsi sia alle strutture sanitarie (pubbliche e private), sia ai singoli esercenti la professione medica, nel momento in cui si avvalgano nella propria di sistemi di IA qualificabili come dispositivi medici. Chi sviluppa questi sistemi deve metterne a disposizione la documentazione tecnica, mappare i dati impiegati per l'addestramento e fornire le informazioni necessarie a chi li integrerà in software successivi. Per i modelli più potenti, suscettibili di innescare rischi sistemici per il mercato o la sicurezza pubblica, scattano severi protocolli di gestione del rischio, monitoraggio continuo e protezione informatica. Questa sezione del regolamento declina in disposizioni giuridiche il principio etico fondamentale secondo cui i sistemi di intelligenza artificiale non possono, in nessun caso, essere impiegati per la sorveglianza di massa o per finalità discriminatorie. La normativa impone specifici obblighi di trasparenza per i contesti in cui l'utilizzo dell'IA non è immediatamente evidente, anch'esso è un livello di rischio, legato alla necessità di trasparenza in merito all'uso dell'IA. I *chatbot* che imitano l'interazione umana devono dichiarare la propria natura, così come i contenuti automatizzati (testi, immagini e video) e i *deepfake* richiedono una chiara etichettatura²⁷⁵. L'obiettivo è tutelare la fiducia reciproca nei rapporti digitali e preservare l'integrità dell'informazione da possibili manipolazioni²⁷⁶. Un intero capitolo della normativa (il Capo V) è riservato ai modelli di IA per finalità generali (i cosiddetti *foundation models*), caratterizzati da grandi dimensioni e versatilità applicativa.

²⁷⁵ All'interno del Regolamento non sono presenti norme per l'IA ritenute a rischio minimo o nullo, ma è necessario riportare che la maggioranza dei sistemi utilizzati nell'UE rientra in questa categoria (ne sono un esempio i videogiochi abilitati all'IA).

²⁷⁶ M. MILAN, *Intelligenza artificiale e diritto positivo: dal Regolamento (UE) 2024/1689 alla legge italiana 23 settembre 2025, n. 132*, Guide pratiche in *Banca Dati OneLegale*.

In merito alla *governance*, ogni Stato membro nomina delle autorità nazionali per garantire l'applicazione e la vigilanza del Regolamento. La supervisione centrale è affidata al nuovo Ufficio europeo per l'intelligenza artificiale (istituito presso la Commissione UE), incaricato di monitorare i modelli AI e di coordinare i singoli Stati tramite un Comitato per l'IA composto da delegati nazionali. L'intero impianto istituzionale è supportato da un *panel* scientifico di esperti indipendenti e da un forum consultivo degli *stakeholder*, garantendo un costante allineamento della normativa all'evoluzione tecnica ed empirica²⁷⁷. Il Regolamento europeo punta con forza sulla trasparenza e sulla difesa dei diritti dei cittadini. Per questo motivo, le pubbliche amministrazioni che intendono adottare sistemi di IA ad alto rischio devono prima eseguire una rigorosa valutazione del loro impatto sulle persone. In più, ogni *software* di questa categoria e chiunque lo utilizzi dovranno essere registrati in una banca dati pubblica a livello UE. Accanto a questi severi obblighi, l'*AI Act* prevede anche misure per sostenere l'innovazione: ne sono un esempio le *sandbox* normative, ossia degli spazi di prova controllati dove le aziende possono sviluppare e collaudare le nuove tecnologie in situazioni reali, lavorando a stretto contatto con i regolatori.

Risulta fondamentale soffermarsi sull'impatto che la *compliance* alle regole europee avrà in termini di *governance* delle amministrazioni sanitarie. Ciò è rivolto all'organizzazione amministrativa, la quale è chiamata ad assicurare le migliori condizioni affinché l'interazione tra personale sanitario e sistemi di IA sia corretta. Innanzitutto, è necessario considerare le decisioni che rilevano nella fase di programmazione: *"l'amministrazione deve anzitutto comprendere i bisogni tecnologici per lo svolgimento dei propri compiti e servizi, deve poi decidere come questi bisogni possano o debbano essere soddisfatti e, infine, disporre le attività necessarie per l'acquisizione delle applicazioni migliori a soddisfarli"*²⁷⁸. In questa fase l'amministrazione deve soppesare differenti fattori. Infatti, oltre ad una valutazione costi/benefici, quest'ultima deve stabilire come procurarsi tali applicazioni e deve valutare il grado di rischio legato all'uso dell'IA.

²⁷⁷ *Ibidem*.

²⁷⁸ B. MARCHETTI, *L'uso di sistemi di IA in ambito medico: qualche strategia per un'amministrazione sanitaria "compliant" con le regole europee e capace di affrontare la sfida*, in *BioLaw Journal - Rivista di BioDiritto*, 2/2025, pp. 331-334.

Un secondo tema è relativo alle politiche rivolte al personale sanitario. È l'articolo 4 del Regolamento, intitolato "Alfabetizzazione in materia di IA", a stabilire che *"I fornitori e i deployer di sistemi di IA adottano misure per sostenere lo sviluppo dell'alfabetizzazione in materia di IA del loro personale e delle altre persone che si occupano del funzionamento e dell'uso dei sistemi per loro conto, tenendo conto delle loro conoscenze tecniche, della loro esperienza, della loro istruzione e formazione, del contesto d'uso e delle persone o dei gruppi di persone su cui i sistemi saranno utilizzati"*. L'aspetto relativo alla formazione e alle competenze è, dunque, fondamentale: *"Le strutture sanitarie si devono confrontare apprestando percorsi convincenti che mirino a dotare il proprio personale delle conoscenze necessaria comprendere l'IA, ma anche a garantirne il continuo aggiornamento, in considerazione della costante e rapida evoluzione della tecnologia"*²⁷⁹.

Relativamente all'organizzazione amministrativa, recentemente (27 luglio 2026) è entrato in vigore il Regolamento (UE) 2026/1744 (*Digital Omnibus*). Quest'ultimo offre una semplificazione mirata del *corpus* normativo sull'IA, preservando allo stesso tempo solide garanzie per la sicurezza delle persone e i diritti fondamentali. Si occupa, inoltre, di sostenere l'innovazione e la competitività facilitando la conformità per le imprese più piccole, estendendo i tempi, ampliando le opportunità di sperimentazione e fornendo maggiore chiarezza giuridica alle imprese che sviluppano e implementano l'IA in Europa²⁸⁰. Tra le modifiche, troviamo un intervento relativo all'articolo 4 del Regolamento (affrontato sopra): nel testo, l'obbligo di garantire un livello di alfabetizzazione, viene sostituito dall'obbligo di adottare misure per sostenere lo sviluppo. Infatti, tra le modifiche relative alla riduzione degli oneri amministrativi, in tema di alfabetizzazione, il precedente requisito di alfabetizzazione all'IA per le imprese viene semplificato e, la Commissione e gli Stati membri, assumono un ruolo più incisivo nella promozione dell'alfabetizzazione all'IA.

²⁷⁹ B. MARCHETTI, *L'uso di sistemi di IA in ambito medico: qualche strategia per un'amministrazione sanitaria "compliant" con le regole europee e capace di affrontare la sfida*, in *BioLaw Journal - Rivista di BioDiritto*, 2/2025, pp. 331-334.

²⁸⁰ Unione Europea, *Entra in vigore AI Omnibus, reperibile al seguente link <https://digital-strategy.ec.europa.eu/it/news/ai-omnibus-enters-force>*.

Rispetto la materia sanitaria, il regolamento incide in maniera diretta²⁸¹. Attraverso i livelli di rischio è possibile classificare la maggior parte dei sistemi basati su IA, e destinati all'utilizzo medico, come ad alto rischio. I software basati su IA devono rispettare diversi requisiti, tra i quali la trasparenza, l'obbligo di sorveglianza umana e l'uso di sistemi di attenuazione dei rischi. L'impatto sul settore sanitario si concretizza anche attraverso la disciplina dei prodotti farmaceutici, un esempio è l'introduzione di spazi di sperimentazione normativa (*sandbox*) per testare i nuovi trattamenti in modo sicuro. Un punto di forza fondamentale riguarda la sinergia con l'EHDS, in merito all'utilizzo secondario dei dati sanitari elettronici. Infine, l'*AI Act*, fornisce la base legale per promuovere l'adozione dell'IA nella medicina e nella prevenzione. Ne è un esempio l'iniziativa *AICare@EU* la quale prevede una serie di interventi coordinati, come il programma *EU4Health* ("UE per la salute, programma di lavoro 2024), che mira ad accelerare la diffusione sicura ed efficace dei sistemi di IA in contesti clinici, contribuendo ad una più ampia integrazione dell'IA nell'assistenza sanitaria²⁸².

3.1 L'intervento del legislatore italiano: la nuova legge quadro n. 132/2025 sull'intelligenza artificiale.

Risulta fondamentale dare conto anche il primo intervento organico del legislatore italiano in merito all'IA, la Legge 23 settembre 2025, 132. Tale intervento normativo è stato adottato a seguito dell'emanazione dell'*Ai Act* ed è composto da sei Capi, distinti per finalità. L'obiettivo primario della Legge è quello di promuovere un uso corretto, trasparente e responsabile dell'IA, fondato sui diritti fondamentali della persona²⁸³ (si tratta del c.d. rapporto antropocentrico).

Prima di analizzare la legge risulta necessario soffermarsi sull'impatto che gli algoritmi hanno sul diritto alla salute. L'IA è una nuova dimensione del potere amministrativo che

²⁸¹ Commissione europea, *Public Health, L'intelligenza artificiale nel settore dell'assistenza sanitaria*, reperibile al seguente link https://health.ec.europa.eu/chealth-digital-health-and-care/artificial-intelligence-healthcare_it.

²⁸² *Public Health, L'intelligenza artificiale nel settore dell'assistenza sanitaria*, [qui](#).

²⁸³ M. MILAN, *Intelligenza artificiale e diritto positivo: dal Regolamento (UE) 2024/1689 alla legge italiana 23 settembre 2025, n. 132*, Guide pratiche in *Banca Dati OneLegale*.

incide sui criteri di legittimazione dell'azione pubblica e sulla stessa definizione dell'interesse generale²⁸⁴. Infatti, *“la Costituzione italiana colloca la salute in un punto nevralgico dell'ordinamento, al crocevia tra l'interesse individuale (come diritto fondamentale della persona) e l'interesse generale (come garanzia di tutela collettiva). Da questa duplice dimensione emerge una tensione giuridica delicata, nella quale il diritto inviolabile del singolo ad accedere a cure efficaci e tempestive si intreccia con la responsabilità pubblica di preservare il bene comune, secondo criteri di universalità, equità e solidarietà”*. E, di conseguenza, *“la dimensione pubblicistica della salute, in questa prospettiva, non si esaurisce nella prestazione sanitaria in senso stretto, ma si estende all'organizzazione, alla programmazione e alla regolazione dei processi decisionali, attraverso i quali la tutela viene concretamente realizzata”*. L'introduzione dell'IA in sanità ridefinisce le modalità di tutela della salute, sostituendo al solo intuito umano un'elaborazione algoritmica spesso poco trasparente per utenti e operatori. A fronte di innegabili benefici teorici, come diagnosi più rapide, efficienza operativa e gestione ottimale delle risorse, l'uso dei dati comporta forti rischi: *dataset* incompleti o distorti possono celare, dietro un'illusoria neutralità tecnica, l'amplificazione di disuguaglianze e discriminazioni strutturali. Il settore sanitario si differenzia da altre aree di azione amministrativa, nelle quali la correttezza dell'algoritmo può essere accertata *ex post*. Infatti, nel campo della sanità, l'errore algoritmico incide immediatamente sulla vita e sull'integrità fisica della persona²⁸⁵. Da questa osservazione deriva il fatto che la tutela può diventare fragile ogni qual volta che il contenuto della decisione non sia immediatamente riconducibile a un procedimento controllato e guidato. In questo nuovo contesto, l'efficacia dell'art. 32 Cost. non riguarda più soltanto l'atto sanitario in sé fornito dall'algoritmo, ma richiede un'estensione della tutela costituzionale. Si afferma così il diritto a un'amministrazione sanitaria "giusta nell'uso della tecnologia", fondato su processi controllati e sulla centralità della responsabilità umana²⁸⁶. Risulta quindi fondamentale affermare come l'IA, oltre a modificare l'assetto tecnico delle decisioni sanitarie, incide sulla struttura relazionale della cura. In questo senso, *“l'IA rappresenta una soglia critica del costituzionalismo sanitario: promette una medicina più precisa e*

²⁸⁴ S. GARDINI, *L'intelligenza artificiale nell'amministrazione sanitaria. Riflessioni a margine della recentissima Legge n. 132/2025*, in *Il diritto dell'economia*, 2-3/2025, pp. 417-457.

²⁸⁵ *Ibidem*.

²⁸⁶ *Ibidem*.

predittiva, ma al tempo stesso rischia di ridurre la cura a un processo impersonale, in cui la valutazione clinica potrebbe essere sempre più sovrastata dalle correlazioni algoritmiche e il medico potrebbe diventare un supervisore di output automatizzati. La tutela costituzionale del diritto alla salute non può tollerare una simile deriva, perché l'oggetto della protezione non è solo la funzionalità biologica, ma anche la relazione umana della cura"²⁸⁷.

Tornando all'analisi della Legge 23 settembre 2025, 132, è il Capo I a stabilire che l'adozione, lo sviluppo e la sperimentazione dell'IA devono allinearsi ai principi costituzionali, alle norme dell'Unione Europea e ai valori cardine di trasparenza, sicurezza, tutela dei dati e della *privacy*, parità di genere, non discriminazione e sostenibilità. Senza imporre nuovi vincoli rispetto al regolamento europeo, la normativa nazionale punta a garantire la coerenza del sistema, focalizzandosi sulla *cybersicurezza* e sulla costante supervisione umana in ogni fase del ciclo di vita delle tecnologie. Il Capo II raccoglie le disposizioni di settore, articolandosi in una serie di norme che disciplinano l'impiego dell'intelligenza artificiale in ambiti specifici della vita pubblica e privata, è in questo Capo che viene disciplinato l'utilizzo dell'IA nel settore sanitario.

Riguardo a quest'ultimo, la Legge individua l'esigenza di unire l'innovazione tecnologica e la protezione dei diritti fondamentali della persona, soprattutto il diritto alla salute, alla dignità e alla riservatezza dei dati. L'articolo 7 enuncia i principi generali sull'uso dell'IA in ambito sanitario: l'intelligenza artificiale si configura come uno strumento di supporto per migliorare il sistema sanitario, contribuendo a prevenzione, diagnosi e cura nel pieno rispetto dei diritti e delle libertà individuali. Il suo impiego non deve mai tradursi in discriminazioni, selezioni o esclusioni nell'accesso alle prestazioni. Ai pazienti è garantito il diritto di sapere se e come l'intelligenza artificiale intervenga nel loro percorso clinico. In ogni caso, la decisione medica rimane centrale: la tecnologia assiste ma non sostituisce il giudizio del professionista, e deve basarsi su sistemi affidabili, aggiornati e sottoposti a periodici controlli di qualità su dati e algoritmi, si tratta del principio della centralità della decisione medica. Il legislatore riserva inoltre una specifica attenzione al ruolo dell'IA a supporto delle persone con disabilità. Questa disposizione riflette una politica di

²⁸⁷ S. GARDINI, *L'intelligenza artificiale nell'amministrazione sanitaria. Riflessioni a margine della recentissima Legge n. 132/2025*, in *Il diritto dell'economia*, 2-3/2025, pp. 417-457.

inclusione sociale, elevando la tecnologia a vero e proprio strumento abilitante. L'IA non si limita così a essere un mezzo per migliorare l'efficienza o l'accuratezza diagnostica, ma si traduce in un fattore di accessibilità e autonomia, capace di potenziare le capacità individuali e abbattere barriere sia fisiche sia comunicative. Questa scelta normativa segna un passaggio culturale rilevante: la disabilità non è più considerata limite da compensare, bensì ambito di valorizzazione della tecnologia in chiave costituzionalmente solidale²⁸⁸.

L'art. 8 disciplina il quadro della ricerca e della sperimentazione scientifica: la nuova disciplina qualifica come attività di rilevante interesse pubblico, con solido fondamento negli articoli 32 e 33 della Costituzione, i trattamenti di dati personali, anche sensibili, svolti per finalità di ricerca da enti pubblici o privati non profit. Questa qualificazione, in linea con il GDPR, offre maggiore flessibilità nella raccolta e nell'elaborazione delle informazioni. Tra le novità più rilevanti vi è la legittimazione dell'uso secondario dei dati privi di identificativi diretti: per procedere non è richiesto un nuovo consenso del paziente, a patto che sia garantita un'adeguata informativa generale. Sono inoltre autorizzati i trattamenti volti all'anonimizzazione, alla pseudonimizzazione e alla generazione di dati sintetici, favorendo la creazione di *dataset* scientifici di alto valore nel rispetto dei diritti fondamentali. Sotto il profilo della *governance*, l'AGENAS assume un ruolo di coordinamento tecnico, con il potere di emanare linee guida su anonimizzazione e dati sintetici previo parere del Garante *Privacy*. Infine, viene introdotto un meccanismo di comunicazione preventiva al Garante: in caso di mancato blocco entro trenta giorni dall'invio, il trattamento può essere avviato, fermi restando i successivi poteri ispettivi e sanzionatori dell'Autorità.

L'articolo 10 estende la portata della riforma integrando l'IA all'interno del Fascicolo Sanitario Elettronico (FSE) e della sanità digitale. Attraverso l'inserimento del nuovo articolo 12-bis nel D.L. n. 179/2012, viene istituita una piattaforma nazionale di intelligenza artificiale, la cui gestione è affidata ad AGENAS nel suo ruolo di Agenzia nazionale per la sanità digitale. Questa infrastruttura offrirà servizi di supporto non vincolanti sia ai medici sia ai cittadini. Per i professionisti sanitari si configurerà come un

²⁸⁸ M. MILAN, *Intelligenza artificiale e diritto positivo: dal Regolamento (UE) 2024/1689 alla legge italiana 23 settembre 2025, n. 132*, Guide pratiche in *Banca Dati OneLegale*.

ausilio nella pratica clinica e nella presa in carico dei pazienti; per gli utenti, invece, rappresenterà un canale per facilitare l'accesso ai servizi territoriali e alle Case della comunità. Sotto il profilo della tutela dei dati, AGENAS assume la titolarità del trattamento, con l'obbligo di alimentare la piattaforma esclusivamente con le informazioni strettamente necessarie. Progettazione e gestione del sistema avverranno sotto la vigilanza congiunta del Ministero della Salute, del Garante Privacy e dell'ACN (Agenzia per la Cybersicurezza Nazionale), garantendo elevati standard di sicurezza. Il tutto avverrà nel rispetto del principio di invarianza finanziaria, senza nuovi o maggiori oneri per la finanza pubblica.

Concludendo il discorso precedentemente iniziato, al Capo III della Legge 132 viene delineata la strategia nazionale e l'assetto di *governance*. La legge delinea una *governance* strutturata a livello centrale, prevedendo l'adozione di una Strategia Nazionale per l'Intelligenza Artificiale. Redatta dalla Presidenza del Consiglio d'intesa con i ministeri competenti, la strategia viene periodicamente approvata dal Comitato interministeriale per la transizione digitale con l'obiettivo di stimolare la sinergia pubblico-privato, promuovere la ricerca e coordinare le politiche di innovazione. A presidio di queste attività viene istituito un Comitato di coordinamento che riunisce i principali ministri e le autorità delegate, con compiti di indirizzo e vigilanza sugli enti dell'ecosistema digitale. Sul piano operativo, la gestione e il controllo della materia sono affidati a due Autorità nazionali per l'IA: L'AgID (Agenzia per l'Italia Digitale), incaricata di promuovere l'innovazione e definire le procedure di notifica e valutazione della conformità dei sistemi, e L'ACN (Agenzia per la Cybersicurezza Nazionale), responsabile di vigilanza, ispezioni e sanzioni, oltre che del coordinamento con i partner europei. Per garantire la massima coerenza d'azione, le due agenzie collaborano in modo strutturato attraverso un comitato congiunto istituito presso la Presidenza del Consiglio. Il Capo IV si occupa della tutela del diritto d'autore nelle opere realizzate con l'ausilio dell'IA, stabilendo che la protezione riguarda solo le opere dell'ingegno umano, anche se create con strumenti IA. Ciò si traduce nel fatto che l'opera è protetta se costituisce espressione del lavoro intellettuale dell'autore umano, mentre l'apporto automatizzato non può generare, di per sé, un diritto d'autore autonomo²⁸⁹. Il Capo V si occupa delle

²⁸⁹ M. MILAN, *Intelligenza artificiale e diritto positivo: dal Regolamento (UE) 2024/1689 alla legge italiana 23 settembre 2025*, n. 132, Guide pratiche in *Banca Dati OneLegale*.

disposizioni penali mirate a contrastare gli abusi dei sistemi di IA e, infine, il Capo VI contiene le disposizioni finanziarie e di coordinamento. La legge afferma il principio di invarianza finanziaria, prevedendo che le nuove funzioni siano esercitate con le risorse già disponibili, salvo le spese specificamente autorizzate.

4. La trasformazione digitale della sanità: il modello *Value-Based Healthcare*.

Il concetto di *Value-Based Healthcare* (VBHC) è sempre più utilizzato nell'ambito dell'innovazione sanitaria, ed è considerato il “*paradigma dominante attorno al quale dovrebbero essere organizzati e strutturati i sistemi sanitari, le aziende ospedaliere e, più in generale, tutti gli attori che operano nel settore della salute*”²⁹⁰. Ciò che contraddistingue i modelli VBHC è la centralità del dato, elemento fondamentale attraverso il quale è possibile fondare i percorsi di cura, e, in sostanza, migliorare l'efficienza dell'assistenza sanitaria. L'introduzione dell'IA all'interno dei processi sanitari comporta un cambiamento nelle dinamiche organizzative e nei ruoli professionali, cambiamento che deve essere affrontato con un approccio rivolto al *technological change management*. Si tratta dell'insieme delle pratiche, delle strategie e degli strumenti adottati per governare l'introduzione e l'implementazione efficace delle innovazioni tecnologiche all'interno delle organizzazioni sanitarie²⁹¹. Data la natura articolata dell'ambito sanitario, occorre determinare se l'introduzione di nuove tecnologie costituisca un beneficio concreto per il paziente oppure un fattore penalizzante per la sostenibilità economica e gli standard qualitativi delle prestazioni. Innanzitutto, l'integrazione delle nuove tecnologie determina l'adozione di un approccio *data-driven*, nel quale l'analisi sistematica dei dati permette di identificare *pattern*, prevedere scenari e prendere decisioni, riducendo l'incertezza e aumentando l'efficienza del sistema, favorendo una personalizzazione delle cure. Inoltre, la grande quantità di dati disponibili permette alle organizzazioni sanitarie di monitorare l'efficacia delle cure e l'andamento dei costi in tempo reale, consentendo un monitoraggio continuo rispetto alla qualità e alla

²⁹⁰ A. GARGIULO, D. LEONE, F. SCHIAVONE, *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, 2025, p. 116.

²⁹¹ *Ivi*, p. 118.

sostenibilità dei servizi. È in questo senso che va inteso il valore: grazie a una riduzione degli sprechi e a una maggiore capacità di pianificazione strategica, è possibile generare un valore tangibile per il paziente, in termini di *outcome* clinici migliori, e per il sistema²⁹². Ciò non è esente da rischi: innanzitutto, il problema dei *bias* nei dati, è importante creare *database* privi di distorsioni (anche se complicato) per evitare un'amplificazione delle disuguaglianze esistenti, infatti, in presenza di *dataset*, non equi e non rappresentativi, gli algoritmi possono penalizzare interi gruppi di pazienti; un'altra problematica riguarda l'accessibilità ai dati per fini di ricerca, i problemi legati alla *privacy*, alla protezione dei dati e alla mancanza di interoperabilità tra i sistemi possono ostacolare la possibilità di ottenere informazioni su scala regionale o nazionale.

In questo contesto, il *Value Based Health Care* si propone come un modello sostenibile, innovativo e centrato sui risultati di salute ottenuti sui pazienti. In contrapposizione all'impostazione tradizionale, orientata all'offerta di servizi e alla suddivisione in branche specialistiche, il paradigma VBHC propone una ristrutturazione dell'assistenza sanitaria basata sui segmenti di pazienti con esigenze cliniche comuni. Ciò consente alle organizzazioni sanitarie di intercettare preventivamente le necessità ricorrenti e di erogare soluzioni cliniche integrate e personalizzate, con benefici diretti sul percorso d'cura del paziente e sull'efficienza operativa del sistema. Centrale, nel paradigma VBHC, è la misurazione sistematica degli esiti clinici e dei costi sostenuti nel percorso di cura. Si tratta di pratiche fondamentali per il monitoraggio della *performance* e per il miglioramento dell'assistenza sanitaria. Tuttavia, in mancanza di una trasformazione culturale profonda all'interno della professione medica, il modello VBHC non potrà avere successo. La soluzione principale potrebbe essere quella di investire ed integrare i principi della VBHC nei programmi di formazione sanitaria.

Il modello VBHC permette di compiere alcune osservazioni in merito alla storica definizione del concetto di salute fornita dall'Organizzazione Mondiale della Sanità, nel 1948, intesa come “*uno stato di completo benessere fisico, mentale e sociale e non la semplice assenza di malattia.*” La definizione risulta, al giorno d'oggi, difficile da attuare, dato che, la salute è sempre più intesa come “*la capacità della persona di funzionare e*

²⁹² A. GARGIULO, D. LEONE, F. SCHIAVONE, *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, 2025, p. 121.

vivere una vita soddisfacente anche in presenza di malattie”²⁹³. In questo senso il modello VBHC modifica la valutazione del successo nei sistemi sanitari, infatti, quest’ultimo, non è più basato sul volume dei servizi, ma sui risultati ottenuti concretamente sui pazienti. Ciò consente un cambiamento di paradigma che incentiva e richiede ai sistemi sanitari di ridefinire il concetto di valore all’interno della cura. Negli ultimi anni, sono stati due gli eventi che hanno permesso, ed accelerato, l’implementazione del modello VBHC: innanzitutto, la pandemia Covid-19 che ha spinto i sistemi sanitari verso un approccio più tempestivo e soprattutto molto più incentrato sulle soluzioni innovative e orientate agli esiti²⁹⁴; in secondo luogo, l’adozione accelerata dell’Intelligenza Artificiale si è dimostrata come un’opportunità fondamentale per migliorare vari aspetti dell’assistenza sanitaria, infatti, l’utilizzo dei sistemi di IA per diagnosi, prognosi e monitoraggio ha permesso una gestione più mirata delle risorse e ha comportato la personalizzazione delle cure e la prevenzione. Un altro tassello fondamentale è composto dall’importanza di un ecosistema integrato e orientato all’innovazione, sfociato nella collaborazione tra attori pubblici e privati per lo sviluppo di applicazioni intelligenti²⁹⁵. L’emergenza pandemica da Covid-19 e la rapida diffusione dell’IA in medicina hanno evidenziato la centralità di tre pilastri: le competenze professionali, la *governance* dei dati e le infrastrutture digitali. Questi elementi si rivelano cruciali per trasformare l’IA in un reale supporto alla *Value-Based Healthcare* (VBHC). Di conseguenza, *“la pandemia è stata la spinta propulsiva che ha reso l’adozione delle nuove tecnologie un passo essenziale da intraprendere. Se prima le nuove tecnologie digitali erano percepite come un mero supporto al business sanitario, ora sono diventate un pilastro imprescindibile per la trasformazione dei sistemi sanitari verso modelli più centrati sul valore, sostenibili e resilienti”*²⁹⁶.

In merito al concetto di VBHC emerge una distinzione fondamentale, si tratta di quella tra l’efficacia operativa e la strategia. Se per la prima si intende il miglioramento dei processi esistenti (come la riduzione dei tempi di attesa o il miglioramento dell’igiene ospedaliera), per la seconda si intendono le scelte deliberatamente orientate (ad esempio

²⁹³ A. GARGIULO, D. LEONE, F. SCHIAVONE, *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, 2025, p. 121.

²⁹⁴ Ad esempio, molti degli elementi tipici del modello VBHC sono stati implementati per necessità in un momento di enorme difficoltà, come ad esempio la misurazione standardizzata degli esiti.

²⁹⁵ *Ibidem*.

²⁹⁶ *Ivi*, p. 122.

quali servizi offrire, oppure, come strutturare i percorsi di cura), cioè quelle scelte che, connesse ad una visione di lungo termine che connetta le *performance* operative con obiettivi centrati sul paziente e sull'uso sostenibile delle risorse, possono integrare una strategia vincente di VBHC²⁹⁷. Un esempio di strategia VBHC deriva dal concetto di disinvestimento, cioè la rimozione di pratiche sanitarie inefficaci o troppo onerose rispetto ai benefici prodotti. Tramite l'attività di disinvestimento si mira a liberare risorse da interventi a basso valore per reinvestirle in pratiche clinicamente più efficaci ed economicamente sostenibili. Si tratta di una strategia per migliorare la qualità dell'assistenza ed è considerato un vero e proprio elemento strategico della VBHC, in quanto permette di riallocare le risorse verso le pratiche di alto valore rafforzando il sistema sanitario. Nella pratica, per attuare il disinvestimento sono necessari degli strumenti di valutazione come l'*Health Technology Assessment* (HTA) che analizza l'efficacia clinica delle tecnologie sanitarie²⁹⁸.

Rimane da compiere un'osservazione in modo da poter comprendere al meglio il concetto di valore nella VBHC, bisogna distinguerlo dal solo valore economico. Se in sanità il valore si misura sulla capacità di risolvere i problemi del paziente e soddisfarne le aspettative, il valore economico si concentra sulla sostenibilità finanziaria e sull'efficienza operativa. La VBHC unisce queste due visioni: solamente coniugando valore clinico, esperienza del paziente ed efficienza economica, i sistemi sanitari possono offrire cure più eque e orientate alla persona²⁹⁹.

In conclusione, il modello VBHC rappresenta una delle più rilevanti e recenti trasformazioni nell'ambito della sanità. Attraverso lo spostamento dell'attenzione dal volume delle prestazioni al valore generato per il paziente è stato possibile migliorare gli esiti clinici e i livelli di assistenza. A oggi, l'adozione del modello VBHC *“non è più solamente un'opzione innovativa ma una condizione imprescindibile per affrontare sfide strutturali come l'invecchiamento della popolazione, l'aumento delle cronicità, la crescente pressione sui bilanci pubblici e la richiesta sociale di cure più*

²⁹⁷ A. GARGIULO, D. LEONE, F. SCHIAVONE, *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, 2025, p. 122.

²⁹⁸ Un esempio fondamentale è quello della *Malaysian Health Technology Assessment Section* (MaHTAS) che sta esplorando l'integrazione di un framework di disinvestimento nel ciclo di vita delle tecnologie sanitarie.

²⁹⁹ *Ivi*, p. 123.

personalizzate”³⁰⁰. Ma, per ottenere risultati sempre più considerevoli, sarà necessaria un’evoluzione culturale orientata agli esiti, sostenuta da infrastrutture tecnologiche, capacità analitiche e *governance* dei dati. L’adozione del modello VBHC deve diventare un obiettivo strategico condiviso. Spetta alle organizzazioni sviluppare competenze adeguate in grado di garantire continuità, coordinamento e personalizzazione, in modo da generare valore non solo nell’erogazione della prestazione, ma durante tutto il percorso del paziente. Infatti, l’adozione del VBHC comporta ad una ridefinizione del concetto di valore in sanità: non si tratta più di massimizzare la produttività o minimizzare i costi, ma di generare valore clinico, basato sugli esiti, valore esperienziale, basato sulla soddisfazione del paziente e valore allocativo, tramite un efficiente utilizzo delle risorse³⁰¹.

4.1. L’Intelligenza Artificiale come strumento essenziale nella transizione verso il modello *Value Based HealthCare: il caso Babylon Health*.

Nel paragrafo precedente è stato affrontato il tema del modello VBHC ed è emersa la centralità dei sistemi di IA all’interno del paradigma. L’adozione dei sistemi di IA permette infatti di analizzare grandi volumi di dati, facilitando la personalizzazione dei trattamenti e non solo. L’utilizzo dell’IA è basato su un approccio *human-centered* in merito alla progettazione delle tecnologie che non intende sostituire il giudizio clinico, ma potenziarlo. Tuttavia, da un lato, l’impiego dell’IA offre potenzialità significative ma, dall’altro, è necessario mantenere l’autonomia la competenza del personale sanitario, evitano di delegare le scelte e le decisioni ai sistemi automatizzati. Risulta necessario considerare l’IA come un’integrazione all’intelligenza clinica e come uno strumento che

³⁰⁰ A. GARGIULO, D. LEONE, F. SCHIAVONE, *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, 2025, p. 130.

³⁰¹ DOMENICO RUSSO, DANIELE AVENOSO, LUIGI DE ANGELIS, ANNA LA SALVIA, ELENA TRATTA, ELENA GUERRA, LORENZO ROMAGNOLI, DAVIDE RUFFO, GIORGIO LORENZO COLOMBO, *Ripensare l’evidenza: approccio multidisciplinare all’uso dei dati sintetici in ambito sanitario – Parte II*, in *BioLaw Journal - Rivista di BioDiritto*, 2025, 3, pp. 343-372.

*“libera tempo per l’interazione umana e migliora la capacità decisionale, senza mai sostituirla”*³⁰².

È utile soffermarsi sul caso di studio *Babylon Health*, che rappresenta perfettamente il paradigma di VBHC ponendo il paziente al centro del sistema. La sua piattaforma, basata sull’integrazione del *Knowledge Graph* e di algoritmi di *Natural Language Processing*, trasforma i sintomi inseriti dagli utenti in concetti clinici standardizzati permettendo delle diagnosi predittive supportate da *real-world evidence*. Si tratta di un approccio *data-driven* che permette di personalizzare i percorsi di cura in base al profilo di rischio individuale e di monitorare l’efficacia delle cure. Grazie alla piattaforma i pazienti possono usufruire di un servizio costantemente disponibile che, tra le altre cose, decongestiona i canali tradizionali, libera risorse e riduce i tempi di attesa. Attraverso *Babylon* è stato possibile attuare anche delle pratiche di disinvestimento strategico (precedentemente affrontato), pratica che rispecchia la filosofia VBHC. Infatti, la piattaforma è in grado di monitorare indicatori come la riduzione delle ospedalizzazioni evitabili o i livelli di controllo glicemico, in modo da garantire che ogni interazione tecnologica sia guidata da dati concreti e orientata a risultati tangibili³⁰³. La strategia a lungo termine di *Babylon* combina efficacia operativa e scelte deliberate di posizionamento, e, oltre ad essere un canale digitale, si concretizza come un ecosistema in cui la tecnologia e la *governance* dei dati convergono per la creazione di un valore clinico, per migliorare l’esperienza del paziente e per sostenere economicamente il sistema sanitario. *Babylon Health* è l’esempio lampante di come l’IA possa trasformare la sanità rendendola più efficace ed equa.

5. I rischi legati al fenomeno della discriminazione algoritmica.

L’automazione, parziale, delle procedure decisionali rappresenta uno dei settori più promettenti in merito alla digitalizzazione della sanità, ma costituisce un settore molto sensibile a causa delle eventuali conseguenze che potrebbero derivare da una decisione

³⁰² *Ivi*, p. 126.

³⁰³ A. GARGIULO, D. LEONE, F. SCHIAVONE, *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, 2025, p. 128.

automatizzata, conseguenze che possono tradursi in pregiudizi, oppure in, *bias*. Con quest'ultimo termine ci si riferisce normalmente a una "*distorsione cognitiva, un costrutto derivante ad percezioni errate, automatismi mentali che generano credenze, che inducono a veloci valutazioni e decisioni, che, in ultima analisi, comportano la formazione di un pensiero che contiene stereotipie e, appunto, pregiudizi*"³⁰⁴. Dato che i *bias* sono in grado di influenzare anche i processi mentali umani, sia valutativi che decisionali, anche nei sistemi di IA possono essere presenti tali distorsioni.

I *bias* possono essere presenti in tutte le fasi di vita dell'algoritmo: possono essere introdotti a partire dalla selezione dei dati, nell'elaborazione degli stessi oppure, non essere presenti nel dato di partenza ma essere generati successivamente e comunque incidere sull'*output* finale, inficiandone l'imparzialità. Di fatti, algoritmi viziati conducono a decisioni errate, inadeguate, non corrispondenti all'effettiva configurazione della realtà sottoposta³⁰⁵. Va esclusa l'idea di considerare i *bias* come meri errori di implementazioni dell'algoritmo, si tratta infatti dello specchio dei pregiudizi insiti in una società. Rimane, comunque, di primaria importanza la selezione dei criteri e l'individuazione degli elementi su cui sviluppare le basi per la creazione dell'algoritmo.

Una problematica importante riguarda il modo in cui si percepiscono gli algoritmi, infatti, il problema dei *bias* è legato alla reale possibilità di accorgersi di tali distorsioni. Spesso, gli algoritmi sono percepiti come oggetti indiscutibili, e di conseguenza anche i loro risultati, ma, va aggiunto che, a causa dell'opacità di questi sistemi, gli algoritmi sono considerati indecifrabili. Il tema dell'opacità è già stato affrontato in precedenza, e assume un rilievo importante in questa sede. Si distingue tra l'opacità intenzionale, fenomeno che indica le barriere regolamentari volontariamente erette dagli sviluppatori degli algoritmi (es. diritti di proprietà individuale), e, opacità intrinseca, intesa come la difficoltà, o impossibilità, di tradurre, in forma umanamente intelleggibile, lo sviluppo del processo decisionale algoritmico. Inoltre, il problema legato all'opacità è amplificato dalla frammentazione delle informazioni che sono solitamente da ricostruire a partire dall'analisi dei documenti predisposti a corredo dei contratti di fornitura di servizi di

³⁰⁴ ALBERTO. M. GAMBINO, E. MAGGIO, *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, 2025, p. 38.

³⁰⁵ *Ivi*, p. 39.

IA³⁰⁶. L'opacità è un tema fondamentale, perché, a causa di quest'ultima, emerge il rischio inconsapevole di discriminazione algoritmica.

Il diritto alla non discriminazione è ampiamente riconosciuto, in ambito nazionale è l'articolo 3 della Costituzione a stabilire che *“Tutti i cittadini hanno pari dignità sociale e sono eguali davanti alla legge, senza distinzione di sesso, di razza, di lingua, di religione, di opinioni politiche, di condizioni personali e sociali. È compito della Repubblica rimuovere gli ostacoli di ordine economico e sociale, che, limitando di fatto la libertà e l'eguaglianza dei cittadini, impediscono il pieno sviluppo della persona umana e l'effettiva partecipazione di tutti i lavoratori all'organizzazione politica, economica e sociale del Paese”*. Il compito relativo alla rimozione degli ostacoli che limitano l'uguaglianza tra cittadini va inteso come direttamente applicabile anche alle attività di sviluppo ed utilizzo dei sistemi di IA³⁰⁷. In ambito europeo, all'articolo 21 della Carta dei diritti fondamentali dell'Unione Europea viene stabilito: *“È vietata qualsiasi forma di discriminazione fondata, in particolare, sul sesso, la razza, il colore della pelle o l'origine etnica o sociale, le caratteristiche genetiche, la lingua, la religione o le convinzioni personali, le opinioni politiche o di qualsiasi altra natura, l'appartenenza ad una minoranza nazionale, il patrimonio, la nascita, la disabilità, l'età o l'orientamento sessuale”*. Inoltre, il GDPR, Regolamento (UE) 679/2016, vieta il trattamento di dati personali che possa comportare *“effetti discriminatori nei confronti di persone fisiche sulla base della razza o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dello status genetico, dello stato di salute o dell'orientamento sessuale”*³⁰⁸, e, all'articolo 22, pone degli obblighi specifici a tutela degli interessati i cui dati sono trattati nell'ambito di processi decisionali automatizzati. In merito all'IA, successivamente alla Risoluzione del Parlamento europeo del 16 febbraio 2017, la Commissione ha stabilito che la non-discriminazione deve essere intesa non solo come divieto per i sistemi di IA di produrre effetti discriminatori e

³⁰⁶ ALBERTO. M. GAMBINO, E. MAGGIO, *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, 2025, p. 41.

³⁰⁷ *Ivi*, p. 42.

³⁰⁸ Considerando n. 71, Regolamento (UE) 679/2016.

pregiudizi vietati, ma anche nel senso di realizzare sistemi in grado di essere utilizzati in modo da includere soggetti diversi e promuovere l'uguaglianza³⁰⁹.

È invece l'*Ai Act*, nella consapevolezza che l'uso dei sistemi di IA potrebbe avere impatti negativi sui diritti fondamentali, a imporre ai *deployer* di sistemi di IA di svolgere una valutazione d'impatto sui diritti fondamentali, in modo da individuare eventuali rischi specifici per i soggetti interessati. Quest'ultima deve essere svolta prima del primo impiego di ogni sistema di IA e deve essere aggiornata, si tratta di un obbligo che ricade sia sui *deployer* pubblici che privati, visto che, anch'essi si ritenga perseguano una finalità di interesse pubblico³¹⁰.

Sul piano pratico, il rispetto dell'obbligo di non discriminazione, gravante su tutti i soggetti pubblici e privati che adottano sistemi di IA nell'esecuzione delle proprie attività, si concretizza nell'esigenza di *“prevenire che i bias siano importati in fase di progettazione e sviluppo nei sistemi di Intelligenza Artificiale e nella pari ordinata necessità di consentire la verifica ex post di tali sistemi, così da appurare se bias si siano, anche involontariamente, comunque successivamente creati, consentendo un controllo diffuso da parte dei cittadini e dei vari portatori di interesse”*³¹¹. Per riuscire a raggiungere gli obiettivi prefissati è necessario attuare azioni di natura tecnica e di approccio legale. Per quanto riguarda le prime, la Commissione europea ha disposto come i cittadini, oltre ai soggetti interessati e a coloro che utilizzeranno i sistemi, debbano essere coinvolti sin dalla selezione dei dati e dalla progettazione, dato che, su di loro si riverserebbero le decisioni assunte in via automatizzata. Un rimedio che si colloca a metà tra il piano giuridico e il piano tecnico è il ricorso agli algoritmi *open source*, nel rispetto del principio di apertura e riuso dei *software* sviluppati dalle amministrazioni. Di fatti, un algoritmo aperto consente un controllo più diffuso. Un altro tema fondamentale riguarda la trasparenza, è necessario assicurare un'adeguata documentazione di ogni aspetto riguardante il sistema algoritmico.

³⁰⁹ ALBERTO. M. GAMBINO, E. MAGGIO, *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, 2025, p. 41.

³¹⁰ Questa affermazione deriva dal Considerando n. 96, *Ai Act*, che stabilisce che: *“Gli enti privati che forniscono tali servizi pubblici sono legati a compiti di interesse pubblico, ad esempio nei settori dell'istruzione, dell'assistenza sanitaria, dei servizi sociali, degli alloggi e dell'amministrazione della giustizia”*.

³¹¹ *Ivi*, p. 45.

5.1. Dal primo caso giurisprudenziale all'art. 30 d.lgs. n. 36/2023: la positivizzazione della non discriminazione algoritmica.

Questo percorso di progressiva sensibilizzazione tecnica e normativa trova una delle sue prime e fondamentali applicazioni pratiche nelle aule di giustizia e nel settore dei contratti pubblici, dove il legislatore ha dovuto tradurre i principi astratti in regole stringenti per le procedure di gara. Il Consiglio di Stato, con sentenza 2270/2019, ha sancito il principio di non discriminazione. Ciò è avvenuto in seguito all'impugnazione di una procedura nazionale di mobilità da parte di alcuni docenti di scuola superiore, i quali lamentavano che la procedura di assunzione fosse gestita da un sistema informatico che operava attraverso un algoritmo, il cui funzionamento era sconosciuto, e che avrebbe emesso una decisione amministrativa senza tenere conto delle preferenze espresse nelle rispettive domande³¹². Dopo un rigetto da parte del TAR lazio (sent. 12026/2016), il Consiglio di Stato ha, in primo luogo, rimarcato i numerosi vantaggi relativi all'automazione in relazione alle quali l'utilizzo di procedure automatizzate è conforme ai canoni di efficienza ed economicità dell'azione amministrativa, a loro volta declinazione del principio costituzionale di buon andamento dell'azione amministrativa (art. 97 Cost.). Successivamente, la Corte ha ritenuto la tecnica applicata all'algoritmo come una regola amministrativa con piena valenza giuridica, e, di conseguenza, soggetta ai principi relativi allo svolgimento dell'attività amministrativa. Spetta quindi alla P.A. temperare preventivamente i diversi interessi, senza lasciar margine ad alcune discrezionalità. È in questo modo che l'algoritmo viene classificato come "atto amministrativo informatico", classificazione dalla quale derivano diverse conseguenze in tema di conoscibilità: da un lato, il meccanismo che porta alla decisione deve essere pienamente conoscibile, e la correttezza del processo informatico è soggetta al sindacato giurisdizionale del giudice amministrativo, il quale deve averne piena cognizione al fine di sindacare la legittimità della decisione automatizzata³¹³. Il Consiglio di Stato ha quindi accolto l'appello e

³¹² Consiglio di Stato – sent. 2270/2019: Il procedimento automatizzato utilizzato dalla P.A. deve essere conoscibile e rispettare i principi dell'azione amministrativa, in Biodiritto, [qui](#).

³¹³ Consiglio di Stato – sent. 2270/2019: Il procedimento automatizzato utilizzato dalla P.A. deve essere conoscibile e rispettare i principi dell'azione amministrativa, in Biodiritto, [qui](#).

riformato la sentenza impugnata, riscontrando la violazione dei principi di imparzialità, pubblicità e trasparenza in relazione alla inconoscibilità del funzionamento dell'algoritmo in merito all'assegnazione dei posti disponibili e riconoscendo l'interesse degli appellanti all'assunzione nella classe di concorso nella quale era stato maturato il maggior punteggio.

Ma, il principio di non discriminazione, viene positivizzato all'interno del nuovo Codice appalti (d.lgs. 31 marzo 2023, n. 36) introduce per la prima volta il tema dell'utilizzo delle procedure automatizzate, è rubricato *“Uso di procedure automatizzate nel ciclo di vita dei contratti pubblici”*³¹⁴ e punta a diventare la prima norma che, a livello nazionale, identifica i principi da rispettare in caso di utilizzo di procedure amministrative automatizzate e di tecnologie avanzate³¹⁵. Oltre al comma primo, il quale stabilisce che *“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...”*, al comma terzo dello stesso articolo si stabilisce come *“Le decisioni assunte mediante automazione rispettano i principi di: a) conoscibilità e comprensibilità, per cui ogni operatore economico ha diritto a conoscere l'esistenza di processi decisionali automatizzati che lo riguardino e, in tal caso, a ricevere informazioni significative sulla logica utilizzata; b) non esclusività della decisione algoritmica, per cui comunque esiste nel processo decisionale un contributo umano capace di controllare, validare ovvero smentire la decisione automatizzata; c) non discriminazione algoritmica, per cui il titolare mette in atto misure tecniche e organizzative adeguate al fine di impedire effetti discriminatori nei confronti degli operatori economici.”*

Il punto centrale è la trasparenza, sia per conoscere le modalità di assunzione della decisione, sia per realizzare il diritto dell'interessato di conoscere eventuali processi

³¹⁴ Si veda il commento di G. Avanzini, *Uso di procedure automatizzate nel ciclo di vita dei contratti pubblici*. Commento ad art. 30, in R. Villata, M. Ramajoli, *Commentario al codice dei contratti pubblici*, Pisa, 2025.

Sul tema G. Mancini Palamoni, *Il paradigma digitale dei contratti pubblici*, in *Ceridap*, 2024, 2.

³¹⁵ Sul punto, D. U. GALETTA, *Digitalizzazione, Intelligenza artificiale e pubbliche amministrazioni: il nuovo Codice dei contratti pubblici e le sfide che ci attendono*, in *Federalismi*, 2023.

decisionali automatizzati che lo riguardano³¹⁶. Viene, successivamente, affermato il principio di “riserva di umanità”, il quale comporta il fatto di consentire sempre l’intervento umano per controllare, validare e modificare la decisione automatizzata. Secondo la dottrina, *“La riserva di umanità oltre che presidio per una intelligenza artificiale al servizio dell’amministrazione più giusta, efficace ed equa, è quindi, in questo senso anzitutto un fondamentale fattore di legittimazione sociale dell’automazione avanzata a mezzo di intelligenza artificiale... prevede in particolare che il risultato computazionale raggiunto dal software, prima di rifluire in una decisione, possa essere sottoposto a revisione da parte di una persona che sia a ciò preposta. In altri termini si passa da una scelta “autonoma” del software ad una scelta “assistita, ovvero assunta dall’uomo ma con il supporto dello strumento dell’intelligenza artificiale”*³¹⁷. Infine, il comma 3 si conclude con la lettera c) che richiama il principio di non discriminazione algoritmica, in forza del quale il titolare della procedura dovrà assicurare misure tecniche e organizzative adeguate al fine di impedire effetti discriminatori nei confronti degli operatori economici. Questo principio si collega al comma quarto del medesimo articolo, nella parte in cui impone alle P.A. di adottare ogni misura tecnica e organizzativa idonea a garantire che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori, nonché a impedire effetti discriminatori nei confronti di persone fisiche sulla base della nazionalità o dell'origine etnica, delle opinioni politiche, della religione o delle convinzioni personali, dell'appartenenza sindacale, dei caratteri somatici o dello status genetico, dello stato di salute, del genere o dell'orientamento sessuale³¹⁸.

In conclusione, è d’interesse l’analisi di quello che è considerato uno dei primi casi di discriminazione algoritmica. Negli anni ’80 la *St. George Hospital Medical School* di Londra valutava gli studenti che si candidavano per l’ammissione tramite un algoritmo innovativo che aveva il compito di essere più imparziale. L’idea era quella di risparmiare

³¹⁶ A. CORRADO, *I nuovi contratti pubblici, intelligenza artificiale e blockchain: le sfide del prossimo futuro*, in *Federalismi*, 2023, p. 133.

³¹⁷ G. GALLONE, *Riserva di umanità...cit. L’A. chiarisce che l’espressione “riserva di umanità”, coniata, dalla dottrina iberica la si deve a J. PONCE SOLE*, *Inteligencia artificial, Derecho administrativo y reserva de humanidad algoritmos y procedimiento administrativo debido tecnologico*, in *Revista General de Derecho Administrativo*, 50, 2019 [1]; Si veda anche, H. FRY, *Hello World. Essere umani nell’era delle macchine*, Torino, 2018.

³¹⁸ Art. 30. Comma 4, d.lgs 31 marzo 2023, n. 36.

tempo e forza lavoro, oltre che rendere il processo di selezione equo, estromettendo l'intervento potenzialmente arbitrario dell'essere umano rispetto ai singoli casi concreti. Nel 1986 alcuni professori notarono poca "diversità" tra gli iscritti selezionati. Avvenne una discriminazione a causa dell'algoritmo, che era stato progettato per dare punteggi più bassi alle donne e alle persone con nomi non europei. Infatti, il caso arrivò davanti alla *U.K. Commission for Racial Equality*, la quale accertò che ogni anno, su 2500 esclusi circa, 60 venivano penalizzati e discriminati in quanto non europei (-15 punti), e/o donne (-3 punti)³¹⁹.

A quarant'anni di distanza dal caso appena citato, le tecnologie hanno subito uno sviluppo impressionante (nel 2019 gli utenti mensili di *Facebook* erano stimati attorno ai 2,41 miliardi, poco meno di 1 essere umano su 3³²⁰). Questo deve far ragionare, se negli anni '80 le discriminazioni algoritmiche potevano avere un determinato impatto, comunque altamente discriminatorio, oggi possono assumere proporzioni planetarie.

6. Il futuro della medicina? Neurotecnologie e *Brain Computer Interface*: tra applicazioni pratiche ed esigenze di regolamentazione.

Le neurotecnologie (NT) e le tecnologie di *Brain Computer Interface* (BCI) rappresentano un ambito potenzialmente trasformativo per la salute umana. Le BCI, attraverso adeguati dispositivi e procedure, sono in grado di monitorare, analizzare, predire il sistema nervoso per comprenderne la struttura, l'attività o le intenzioni³²¹. Dal punto di vista tecnico, la BCI è un'interfaccia neurale che mette in comunicazione diretta il cervello con i dispositivi esterni. Permette, ad esempio, di controllare un computer con il pensiero o di ripristinare funzioni motorie e sensoriali compromesse. Ovviamente, è un tipo di tecnologia innovativa e forse tra le più promettenti dell'era digitale, che incontra

³¹⁹ G. GIORGINI PIGNATIELLO, *Il contrasto alle discriminazioni algoritmiche: dall'anarchia giuridica alle Digital Authorities?* in *Federalismi.it*, 2021, p.169.

³²⁰ ANSA, 2019, [qui](#).

³²¹ M. C. GAETA, *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, 2025, p. 255.

però dei limiti sul piano etico-legale e non solo. In questo senso, emerge un nuovo concetto che riguarda la condizione di vulnerabilità di ogni essere umano rispetto allo sviluppo tecnologico: la vulnerabilità tecnologica. Se da una parte l'avvento di queste nuove tecnologie apre a scenari futuri che, fino a poco fa, non erano immaginabili³²², dall'altra emergono nuove sfide etiche e legali che richiedono un'adeguata regolamentazione. Ad esempio, sono importanti le questioni legate alla sicurezza fisica e informatica, come gli attacchi all'utente e al dispositivo BCI tramite la rete internet, e ancora, il tema della privacy è fondamentale: in caso di accesso illecito ai dati neurali e mentali potrebbero configurarsi discriminazioni o profilazioni psicologiche. In più, la sicurezza delle tecnologie BCI incide anche sul pensiero e sulle decisioni, in caso di tecniche manipolative potrebbe concretizzarsi una violazione del diritto di autodeterminazione del soggetto. Per arginare e limitare i rischi appena riportati potrebbe essere necessaria un'attività di compliance sin dalla fase della progettazione, che tenga conto dei principi etici e delle regole giuridiche, in modo da far sì che la tutela dei diritti fondamentali dell'uomo sia un elemento intrinseco alla tecnologia, e non una eventuale e successiva verifica³²³.

Le concrete applicazioni nel settore sanitario in merito alle BCI sono rivolte allo sviluppo di tecnologie in grado di migliorare la vita, soprattutto in merito alla gestione di patologie che ostacolano la comunicazione verbale³²⁴. È, inoltre, risultato di primaria importanza l'approccio collaborativo ed etico da parte delle istituzioni internazionali ed europee in merito allo sviluppo delle BCI³²⁵; anche in Italia, attraverso i d.d.l. n. 1245/2024³²⁶, è stato evidenziato il potenziale rivoluzionario delle neurotecnologie, comprese le BCI.

Data la potenzialità enorme delle neurotecnologie, e di conseguenza anche gli enormi rischi che potrebbero derivare da un'assenza normativa, risulta necessario una regolamentazione che tuteli l'individuo in una prospettiva di sviluppo sempre più ampia

³²² Ad esempio, in ambito di neurotecnologie, è possibile migliorare la mobilità di una persona paralizzata tramite un esoscheletro guidati dagli impulsi cerebrali del paziente.

³²³ M. C. GAETA, *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, 2025, p. 258.

³²⁴ Oppure, alcune società hanno creato dei dispositivi da impiantare nel cervello con la promessa di restituire capacità motorie a soggetti disabili.

³²⁵ Ad esempio, i programmi *Horizon 2020* e *Horizon Europe* che incentivano la ricerca nel settore.

³²⁶ D.d.l Istituzione dell'Autorità nazionale per l'intelligenza artificiale e le neurotecnologie, 25 settembre 2024, n. 1245.

e sostenibile. Sono due gli interventi del legislatore europeo che possono fornire una base giuridica per le neurotecnologie e le BCI: il già citato, *Ai Act*, e il nuovo Regolamento sulla responsabilità del produttore³²⁷. Anche le neurotecnologie sono “prodotti” e, di conseguenza, possono rientrare nell’ambito della tutela del consumatore. Tuttavia, negli anni, le esigenze di tutela degli individui rispetto all’avvento delle nuove tecnologie ha accelerato l’esigenza di una regolamentazione più mirata. Infatti, è stata adottata una più severa regolamentazione che, partendo dal concetto di sicurezza dei prodotti giunge a quello di rischio, e si basa sulla valutazione dell’impatto del rischio (*risk impact assessment*) e sulla gestione del rischio (*risk management*) dei prodotti tecnologici³²⁸ in modo da ridurre i possibili danni per gli esseri umani. Precisamente, il requisito della sicurezza comprende sia la *safety* che la *cybersecurity* e riguarda anche gli individui che utilizzano le applicazioni neurotecniche. La sicurezza informatica (*cybersecurity*) è invece legata al funzionamento dei sistemi IT (*Information Technology*) e, in questo settore, risultano fondamentali le misure di *cybersecurity* per proteggere i prodotti intelligenti da attacchi *hacker* e *bias* algoritmici. Oltre a ciò, rimane fondamentale la tutela della *privacy*, visto che, i dati devono essere protetti anche attraverso adeguate misure tecniche e organizzative in grado di assicurare la salvaguardia dei prodotti. Per quanto riguarda l’approccio basato sul rischio, è l’*Ai Act*, all’articolo 9, a prevedere un sistema di gestione dei rischi per i sistemi ad alto rischio, e a disporre, all’articolo 27, una valutazione d’impatto sui diritti fondamentali per i soli sistemi ad alto rischio espressamente indicati. Si tratta di una modalità di misurazione e gestione fondata sull’approccio *risk based* e che si trova, sempre di più, al centro delle tecniche di regolamentazione. Inoltre, il meccanismo eccede i requisiti di sicurezza già previsti a livello europeo, di fatti, adatta la regolamentazione in base al livello di rischio dell’IA correlato all’impatto che il sistema ha sui diritti umani³²⁹. Ogni livello di rischio va gestito con un’attività di *compliance by design* adatta e da compiere prima dell’immissione sul mercato dei dispositivi BCI.

³²⁷ Regolamento 2024/2853/UE – Nuova PLD.

³²⁸ Ivi, p. 261.

³²⁹ M. C. GAETA, *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, 2025, p. 264.

Il modello descritto è chiaramente improntato alla tutela dell'utente, ma la regolamentazione deve essere applicata alle tecnologie caso per caso. Infatti, per esempio, le tecnologie BCI possono rientrare nella definizione di tecnologie di IA proibite (articolo 5 *Ai Act*) quando le tecnologie utilizzano tecniche subliminali che agiscono senza che una persona ne sia consapevole, o tecniche manipolative con l'effetto di distorcere il comportamento umano³³⁰. In questo senso agiscono le Linee guida sui sistemi di IA vietati³³¹ che si soffermano sui rischi legati alle neurotecnologie, soprattutto in merito alle interfacce cervello-computer, che possono comportare un aumento significativo del pericolo di una sofisticata manipolazione della mente umana.

La regolamentazione delle neurotecnologie passa per il tema della *privacy*, con riferimento specifico ai dati neurali e mentali: visto che, i progressi nelle neuroscienze e nelle interfacce cervello-computer consentono l'accesso e la manipolazione delle informazioni neurali, è necessario stabilire delle linee guida chiare per proteggere la *privacy* mentale degli individui. Attualmente la tutela della *privacy* è disciplinata dal GDPR: tuttavia, mentre è certo che i dati neurali rientrino nel suo ambito di applicazione, l'inclusione dei dati mentali resta ancora incerta. Questo perché i dati neurali riguardano la struttura e il funzionamento del sistema nervoso e sono quindi in grado di rivelare informazioni sulla condizione clinica umana (salute e benessere), ciò permette loro di rientrare nell'ambito di applicazione dell'art. 9 del GDPR. Invece, per quanto riguarda i dati mentali, essi riguardano la sfera più intima e personale del soggetto (emozioni, ricordi etc) e, di conseguenza, dovrebbero essere classificati come dati sensibili. Si tratta di un ambito difficile da regolamentare, a causa del fatto che, nel momento in cui si ha a che fare con dati neurali e mentali, la normativa *privacy* si trova a dover affrontare questioni ancora aperte, come il consenso o la protezione dei dati.

In merito al tema della regolamentazione, è necessario riportare la disciplina normativa che regola le neurotecnologie di BCI³³², attualmente è composta da due Regolamenti: il Regolamento sui dispositivi medici (MDR)³³³ e il, già affrontato,

³³⁰ Ibidem.

³³¹ 4 febbraio 2025 C (2025) 844 final.

³³² M. C. GAETA, *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, 2025, p. 266.

³³³ Regolamento 2017/745/UE.

Regolamento sullo Spazio Europeo dei Dati Sanitari (EHDS)³³⁴. Il Regolamento MDR comprende i dispositivi di NT con scopi medici utilizzati, all'articolo 2 viene fornita la definizione di dispositivo medico: *“qualunque strumento, apparecchio, apparecchiatura, software, impianto, reagente, materiale o altro articolo, destinato dal fabbricante a essere impiegato sull'uomo, da solo o in combinazione, per una o più delle seguenti destinazioni d'uso mediche specifiche: diagnosi, prevenzione, monitoraggio, previsione, prognosi, trattamento o attenuazione di malattie; diagnosi, monitoraggio, trattamento, attenuazione o compensazione di una lesione o di una disabilità, studio, sostituzione o modifica dell'anatomia oppure di un processo o stato fisiologico o patologico, fornire informazioni attraverso l'esame in vitro di campioni provenienti dal corpo umano, inclusi sangue e tessuti donati, e che non esercita nel o sul corpo umano l'azione principale cui è destinato mediante mezzi farmacologici, immunologici o metabolici, ma la cui funzione può essere coadiuvata da tali mezzi (...)”*³³⁵. Si tratta di una definizione molto ampia, spesso, le BCI rientrano nelle predette finalità e vanno quindi considerate come dispositivi medici.

Per quanto riguarda il trattamento dei dati sanitari, inclusi quelli gestiti tramite tecnologie BCI, il Regolamento EHDS disciplina i dati elettronici e la loro condivisione. Ciò garantisce la continuità assistenziale e il perseguimento di finalità di interesse collettivo, creando così un quadro giuridico uniforme all'interno dello Spazio Europeo dei Dati Sanitari con l'obiettivo di fornire un sistema integrato per la condivisione, l'accesso e la gestione dei dati sanitari tra gli Stati membri.

Sul piano nazionale è stato proposto il d.d.l. n. 1245/2024 per l'introduzione dell'Autorità nazionale per l'Intelligenza Artificiale e le neurotecnologie. In questo senso, si nota un'importante attenzione da parte del governo verso il settore, all'articolo 1, comma 3, del testo si trova la definizione di neurotecnologie, la quale include le tecnologie BCI: *“Per neurotecnologie si intendono i sistemi elettronici posizionati all'esterno o all'interno del cervello o di altre componenti del sistema nervoso al fine di registrare o stimolare l'attività cerebrale, anche attraverso l'uso di interfacce cervello-computer, ovvero un tipo di canale neuroinformatico di comunicazione diretta tra il cervello e un dispositivo di*

³³⁴ Regolamento 2025/327/UE.

³³⁵ Art. 2, Regolamento 2017/745/UE.

calcolo che non utilizza il sistema periferico e neuro-muscolare”³³⁶. Rilevano anche gli articoli 7 e 8 della, precedentemente citata, legge n. 135/2025, che, in ottica di salvaguardare i diritti fondamentali dell’individuo, mira a bilanciare le opportunità relative all’utilizzo dell’IA in ambito sanitario³³⁷. L’articolo 7 evidenzia il ruolo dell’IA come strumento di supporto per il sistema sanitario, mentre l’articolo 8 considera di rilevante interesse pubblico i trattamenti di dati per la ricerca scientifica nella realizzazione di sistemi di IA e consente, l’uso secondario di tali dati personali purché pseudonimizzati, senza ulteriore consenso specifico. Tale disposizione è in contrasto con i principi del Codice *privacy*. Quest’ultima è sicuramente orientata verso l’idea di facilitare la ricerca e lo sviluppo di nuove terapie, ma, a causa di un’assenza di specifiche regole giuridiche di base, solleva interrogativi in merito al tema della *privacy*. Risulta, quindi, necessario un attento bilanciamento tra il progresso scientifico e la protezione della sfera più intima dell’individuo³³⁸.

6.1 Un accenno ai c.d. neurodiritti.

Il termine “neurodiritti” nasce in seguito allo sviluppo delle NT e comprende i diritti fondamentali, legati alla sfera mentale e neurocognitiva, emersi in seguito a tale innovazione e in risposta “*alle crescenti sfide etiche, legali e sociali poste dai progressi nello sviluppo e nell’accessibilità delle neurotecnologie (NT)*”³³⁹. Si tratta di diritti umani neurali e vengono suddivisi in quattro classificazioni³⁴⁰: libertà cognitiva, *privacy* mentale, integrità mentale e continuità psicologica. Il diritto alla *privacy* mentale ha lo scopo di proteggere “*le informazioni private o sensibili nella mente di una persona dalla raccolta, archiviazione, utilizzo o addirittura cancellazione non autorizzati*”. Risulta necessario difendere le informazioni prima che si materializzino, proteggendo così anche la fonte e fornendo una tutela maggiore. Per quanto riguarda il diritto all’integrità mentale,

³³⁶ Art. 1, d.d.l. n. 1245/2024.

³³⁷ M. C. GAETA, *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, 2025, p. 268.

³³⁸ *Ibidem*.

³³⁹ PARLAMENTO EUROPEO, *The protection of mental privacy in the area of neuroscience*, studio, cit., pp. 38-51.

³⁴⁰ G. BELISARIO, *Neurodiritti: nuovi diritti o diritti già esistenti?* in *Federalismi*, 2024, p. 72.

quest'ultimo dovrebbe proteggere tutte le intrusioni non autorizzate³⁴¹. Il diritto alla continuità psicologica ha lo scopo di proteggere “*i substrati mentali dell'identità personale da alterazioni inconsce e non consentite da parte di terze parti attraverso l'uso di neurotecnologie invasive o meno*”. Quest'ultimo mira a prevenire l'alterazione del funzionamento neurale, non solo l'accesso ai dati cerebrali. Infine, il diritto alla libertà cognitiva mira a tutelare l'individuo dall'uso coercitivo e non consenziente delle neurotecnologie³⁴².

Tali diritti sono definiti come “nuovi”, ma, potrebbero essere già disciplinati nelle Carte fondamentali esistenti e nelle normative europee e nazionali. Il quadro normativo cogente, infatti, sembrerebbe fornire già le risposte necessarie alle questioni di tutela della mente umana in applicazione dell'articolo 12 disp. prel c.c.³⁴³ In questa prospettiva, pur passando dai diritti tradizionali ai c.d. neurodiritti, il quadro normativo esistente garantirebbe un'adeguata tutela dei soggetti coinvolti, che potrà essere poi integrato da normative settoriali, legislazione tecnica o principi etici.

³⁴¹ Quest'ultimo potrebbe rientrare nella sfera di tutela dell'articolo 3 della CEDU.

³⁴² M. IENCA, R. ANDORNO, N. Hertz, *Neurorights - Do we Need New Human Rights? A Reconsideration of the Right to Freedom of Thought in Neuroethics*, 16/2023, p. 5

³⁴³ M.C. GAETA, L. AULINO, E. TROISI, *The possible relationships between law and ethics in the context of artificial intelligence regulation*, in *Humana.Mente*, XXXIV, 2023, p. 163-167.

BIBLIOGRAFIA

- ALBERTI I., *L'accesso documentale alla cartella clinica del defunto per ragioni diagnostico-terapeutiche al tempo del Regolamento sullo spazio europeo dei dati sanitari*, in *Federalismi.it*, 2025, 33, pp. 260-279.
- AMIDEI, A., *Dati relativi alla salute e acquisto di farmaci online (Corte giust. UE, 4 ottobre 2024, C-21/23, ND c. DR)*, in *Dirittoesantità.unipv.it*, 2025.
- AMIDEI, A., *L'AI Act in Gazzetta Ufficiale: l'impatto sul settore sanitario e il contesto italiano (in divenire)*, in *Dirittoesantità.unipv.it*, 2024.
- AMORE, A., *Il fascicolo sanitario elettronico nella prospettiva dell'eguaglianza territoriale: una proposta di inquadramento giuridico tra LEA e LEP*, in *Ia, sanità – territorio, pubbliche amministrazioni*, 2026.
- APERIO BELLA, F., *Telemedicina tra decentramento ed esigenze di uniformità*, in C. Bottari, P. J. Tárraga López, J. Cantero Martínez (a cura di), *Sanità rurale e assistenza sanitaria decentrata*, Napoli, 2024.
- APERIO BELLA F., *La telemedicina entro e oltre il territorio: verso un diritto alla salute digitale?*, in *Istituzioni del Federalismo*, 4/2025, pp. 833-856.
- AVANZINI G., *Decisioni amministrative e algoritmi informatici*, Napoli, 2018.
- AVANZINI, G., *Liste d'attesa sanità: nuove regole dal 1° agosto, 2024*, in *Centro studi Diritto e Sanità*.
- AVANZINI G., *Intelligenza artificiale e discrezionalità*, in AA. VV., *Annuario AIPDA 2022. Discrezionalità e amministrazione. Atti del convegno annuale, Bologna 7-8 ottobre 2022*, Napoli, 2023, pp. 119-147.
- BALDUZZI, T., MORANA, D., MORGANTI, F., *La salute "intelligente": eHealth, consenso informato e principio di non-discriminazione*, in *Federalismi.it*, 2022.
- BELISARIO, G., *Neurodiritti: nuovi diritti o diritti già esistenti?* in *Federalismi*, 2024.
- BOLOGNINI, L., BONETTI, P., GUARNIERI, E., *The super powers of the European Data Protection Board (EDPB) and the principle of due administrative procedure*, in *Diritto, Economia e Tecnologie della Privacy*, 2025, 1.
- BURATTI, V., *Fascicolo sanitario elettronico: verso la piena operatività?* in *Diritto e sanità*.

BURATTI, V., *La riforma della sanità territoriale: luci e ombre dei nuovi modelli organizzativi e assistenziali*, in *Ceridap*, 2025, 2.

BUTTARELLI, G., *Dati e interoperabilità nella pubblica amministrazione*, in *Osservatorio IRPA sullo Stato Digitale*.

CAMPAGNA, M., *Linee guida per la Telemedicina: considerazioni alla luce dell'emergenza Covid-19*, in *Corti Supreme e Salute*, 2020.

CAPILLI G., *Digital Twin in sanità: innovazioni, opportunità e sfide giuridiche*, in *Rivista italiana di medicina legale e del diritto in campo sanitario*, 2024, 3-4, pp. 527-535.

CARLONI E., *I principi di legalità algoritmica. Le decisioni automatizzate di fronte al giudice amministrativo*, in *Diritto amministrativo*, 2020, 2, pp. 271-304.

CARLONI E., *Critica dell'amministrazione artificiale*, Bologna, 2026.

CARULLO G., *L'amministrazione quale piattaforma dei servizi digitali*, Napoli, 2022.

CARULLO G., *Dati personali e fini pubblici: dubbi di compatibilità europea del Codice Privacy*, in *Ceridap*, n. 3, 2024,

CASSESE S., *La pubblica amministrazione dinanzi alle transizioni*, in *Giornale di Diritto Amministrativo*, 2024, 6, pp.818-820.

CATELANI, E., *La digitalizzazione dei dati sanitari: un percorso ad ostacoli*, in *Corti Supreme e Salute*, 2023.

CAVALLO PERIN, R., JACOD, C., *I servizi pubblici con l'intelligenza artificiale*, in CAVALLLO PERIN, R., GALETTA D.U., *Il Diritto dell'Amministrazione Pubblica digitale*, Torino, 2025.

CIAFARDONI A., *Telemedicina e livelli essenziali di assistenza nel prisma dei divari territoriali*, in *Italian Papers On Federalism*, 2/2025, pp. 162-176.

COIANTE A., *L'implementazione della telemedicina come elemento strutturale del SSN: dalla frammentarietà all'uniformità. La stabilizzazione post-PNRR e il possibile ruolo dei LEA*, in *Federalismi.it*, 2025, 28, pp. 44-66.

COLAPIETRO, C., *I principi ispiratori del Regolamento UE 2016/679 sulla protezione dei dati personali e la loro incidenza sul contesto normativo nazionale*, in *Federalismi.it*.

CORRADO, A., *I nuovi contratti pubblici, intelligenza artificiale e blockchain: le sfide del prossimo futuro*, in *Federalismi*, 2023.

CORSO S., *Relazione di cura e protezione dei dati. I nuovi scenari della telemedicina*, in *Federalismi.it*, 33/2025, pp. 304-317.

CORSO S., *Lo spazio europeo dei dati sanitari. Prime riflessioni sul Regolamento UE 2025/327*, in *Le Nuove leggi civili commentate*, 3/2025, pp. 563-603.

CREMONA E., *Quando i dati diventano beni comuni: modelli di data sharing e prospettive di riuso*, in *Riv. it. inform. dir.*, 2023, 2, pp. 111-130.

D’ALEO, L., *L’ecosistema dei dati sanitari (EDS)*, in *Diritto e sanità*, 2025.

D’ALEO, L., *La definizione di dato relativo alla salute nel GDPR: una questione ancora aperta*, in *Dirittoesantità.unipv.it*, 2025.

DE ANGELIS P., *Il PNRR e la telemedicina*, in *Sanità Pubblica e Privata*, 2024, 2, pp. 6-12.

DEL CORONA, L., GIUBILEI, A., LADU, M., MONTOSZI, V., *Intelligenza artificiale, sanità digitale ed esigenze di regolazione*, in *Federalismi.it*, 2025.

DE MENECH C., FOGLIA M. (a cura di), *Cura e ricerca nell’era digitale. Interessi antagonisti e modelli di bilanciamento*, Torino, 2026.

DE MENECH C., *IA e consenso informato: reciproci condizionamenti e implicazioni giuridiche*, in *Giurisprudenza italiana*, 2/2025, pp. 457-460.

DI COSTANZO C., *La co-regolazione delle nuove tecnologie nel settore della salute: ambiti di applicazione, caratteristiche e prospettive*, in *Osservatorio sulle fonti*, 2024, 1, pp. 285-316.

DI FILIPPO G., *I dati come beni giuridici. Dati personali e dati non personali: regime di appartenenza e di circolazione*, in P. STANZIONE (a cura di), *I poteri privati delle piattaforme e le nuove frontiere della privacy*, Giappichelli, Torino, 2022.

FAINI, F., *Governo dei dati personali nell’impiego dell’intelligenza artificiale e della blockchain da parte della sanità pubblica*, in *Diritto Mercato Tecnologia*, 2023.

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

FERONI G. C., *Sanità digitale, tra innovazione e tutela dei dati sanitari: il ruolo del garante privacy*, in *Corti Supreme e Salute*, 1/2025, pp. 225-251.

FIGLIOLIA, C., MACCHIA, M., *Autorità per la “privacy” e Comitato europeo nel quadro del “General Data Protection Regulation”*, in *Giorn. dir. amm.*, 4, 2018.

FRANCA S., *I dati personali nell'amministrazione pubblica: attività di trattamento e tutela del privato*, Trento, 2023.

FRANCA, S., *Il trattamento dei dati sanitari nel contesto della sanità digitale. Verso una governance equilibrata?* in *Federalismi.it.*, 2025, 33, pp. 318-342.

FRANCA S., *Principi e regole del trattamento di dati personali tramite profilazione sanitaria*, in *Nuova Giur. Civ. Comm.*, 5, 2025,

GAETA, M. C., *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, 2025.

GAETA, M.C., AULINO, L., TROISI, E., *The possible relationships between law and ethics in the context of artificial intelligence regulation*, in *Humana.Mente*, XXXIV, 2023.

GALLONE, G., *Riserva di umanità...* [J. PONCE SOLÉ, *Inteligencia artificial, Derecho administrativo y reserva de humanidad algoritmos y procedimiento administrativo debido tecnologico*, in *Revista General de Derecho Administrativo*, 50, 2019; H. FRY, *Hello World. Essere umani nell'era delle macchine*, Torino, 2018].

GAMBINO, A. M., MAGGIO, E., *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*.

GARGIULO, A., LEONE, D., SCHIAVONE, F., *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, 2025.

GIARDINI S., *L'intelligenza artificiale nell'amministrazione sanitaria. Riflessioni a margine della recentissima Legge n. 132/2025*, in *Il diritto dell'economia*, 2-3/2025, pp. 417-457.

GIGLIONI, F., *Manuale di diritto sanitario*, Molfetta, 2024.

GIORGINI PIGNATIELLO, G., *Il contrasto alle discriminazioni algoritmiche: dall'anarchia giuridica alle Digital Authorities?* in *Federalismi.it*, 2021.

IULIANI A., *Gli incerti confini della nozione di "dati relativi alla salute", in Autodeterminazione, cura e ricerca nell'era digitale*, 2026, p. 238.

IENCA, M., ANDORNO, R., HERTZ, N., *Neurorights - Do we Need New Human Rights? A Reconsideration of the Right to Freedom of Thought*, in *Neuroethics*, 16/2023.

MACCABIANI N., *Tra coordinamento informativo e livelli essenziali delle prestazioni: il caso del Fascicolo Sanitario Elettronico*, in *federalismi.it*, 12/2023, pp. 251-270.

MARCHETTI B., *L'uso di sistemi di IA in ambito medico: qualche strategia per un'amministrazione sanitaria "compliant" con le regole europee e capace di affrontare la sfida*, in *BioLaw Journal - Rivista di BioDiritto*, 2/2025, pp. 331-334.

MATASSA M., *Colmare i divari. Come le nuove tecnologie promettono di rivoluzionare la sanità italiana*, in *federalismi.it*, 12/2025, pp. 162-197.

MAZZA LABOCCETTA, A., *Telemedicina: sfide, problemi, opportunità*, in *Federalismi.it*, 2023.

MILAN, M., *Intelligenza artificiale e diritto positivo: dal Regolamento (UE) 2024/1689 alla legge italiana 23 settembre 2025*, n. 132, *Guide pratiche in Banca Dati OneLegale*.

MORACE PINELLI, A., *Lo spazio europeo dei dati sanitari (reg. UE n. 327/2025)*, in *La Nuova Giurisprudenza Civile Commentata*, n. 4, 1° luglio 2025, p. 1016.

MORGANTI F., *Intelligenza artificiale costituzionalmente orientata come veicolo positivo di eguaglianza: algoritmi "riparativi" e programmazione sanitaria*, in *Corti Supreme e Salute*, 2025, 3, pp. 1045-1065.

PARODO, F., *La tutela del diritto alla protezione dei dati personali: l'effettività dei rimedi e il ruolo nomofilattico del Comitato europeo per la protezione dei dati personali*, in *Federalismi.it*, 2021, 25.

PIOGGIA A., *La sanità nel PNRR tra riforme e attuazione: territorialità, domiciliarità e telemedicina*, in *Istituzioni del Federalismo*, 4/2025, pp. 741-748.

PISTORIO, G., *La co-regolazione nell'ecosistema digitale tra etero-regolazione e auto-regolazione. Questioni definitorie*, in *Osservatorio sulle fonti*, n. 1, 2024.

PITINO A., *Sfide e prospettive nell'era del FSE 2.0 e della telemedicina*, in *Corti Supreme e Salute*, 3/2025, pp. 977-982.

POSTERARO, N., *La digitalizzazione della sanità in Italia: uno sguardo al Fascicolo Sanitario Elettronico (anche alla luce del Piano Nazionale di Ripresa e Resilienza)*, in *Federalismi.it*, 2021.

POSTERARO, N., *La telemedicina*, in V. BONTEMPI (a cura di), *Lo stato digitale nel Piano nazionale di ripresa e resilienza*, Roma, 2022.

RE FERRE G., *Il fascicolo sanitario elettronico nello spazio europeo dei dati sanitari tra diritti del paziente e utilizzo secondario dei dati*, in *Diritto amministrativo*, 2025, 4, pp. 1237-1266.

RUSSO D., AVENOSO D., DE ANGELIS L., LA SALVIA A., TRATTA E., GUERRA E., ROMAGNOLI L., RUFFO D., COLOMBO L. R., *Ripensare l'evidenza: approccio multidisciplinare all'uso dei dati sintetici in ambito sanitario – Parte II*, in *BioLaw Journal - Rivista di BioDiritto*, 2025, 3, pp. 343-372.

SAMO, S., *La telemedicina alla luce dell'avvento della robotica e dell'Intelligenza Artificiale*, in *Federalismi.it*, 2025.

SENIGAGLIA R., *Giudizio di eleggibilità e condizioni di accesso ai servizi di telemedicina*, in *Persona e Mercato*, 4/2025, pp. 1095-1113.

SIGNORINI, E., ZAMBARDINO, F., *La blockchain e la telemedicina: quali opzioni per la sicurezza e l'integrità dei dati sanitari*, in *Federalismi.it*, 2025.

SILVANO C., *La digitalizzazione dei servizi sanitari alla luce del riparto di competenze tra Stato e Regioni. Il caso del Fascicolo Sanitario Elettronico*, in *federalismi.it*, 26/2023, pp. 228-249.

SIMONATI, A., *I dati personali in possesso della pubblica amministrazione: beni a destinazione pubblica?*, in *Ceridap*, 2025.

SORRENTINO, E., SPAGNUOLO, A.F., *Gestione e conservazione dei dati sanitari. Il vulnus normativo che impatta su sicurezza e data protection*, in *Federalismi.it*, 2024.

SORRENTINO, E., SPAGNUOLO, A.F., *La sanità digitale in emergenza Covid-19. Uno sguardo al fascicolo sanitario elettronico*, in *Federalismi.it*, 2020.

SPAGNUOLO, A. F., SORRENTINO, E., *Open data per l'e-democracy*, in *Rivista italiana di informatica e diritto*, 4, 1 (mag. 2022).

TRUBIANI, F., CARLEO, R., *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, 2025.

TRUBIANI, F., CASCINI, F., *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, 2025.

TRUBIANI, F., CESARELLI, M., MERCALDO, F., *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, 2025.

TRUBIANI, F., DI NUZZO, M., *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, 2025.

TRUBIANI, F., DI SOMMA, C., *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, 2025.

TRUBIANI, F., GRION, L., *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, 2025.

TRUBIANI, F., LAGHI, A., *Sistemi di intelligenza artificiale in medicina verso lo spazio europeo dei dati sanitari*, 2025.

VALENTINI F., *La sanità digitale tra regolazione, organizzazione amministrativa e azione terapeutica*, in *Munus*, 2/2023, pp. 449-486.

VITERBO F. G., *Principi di trattamento e di "governance" dei dati personali in ambito sanitario*, in *Rassegna di diritto civile*, 4/2023, pp. 1443-1476.