SANITÀ DIGITALE E DIRITTI FONDAMENTALI: CRITICITÀ E PROSPETTIVE TRA EQUITÀ E PROTEZIONE DEI DATI*

di Candida Conti**

Sommario. 1. Evoluzione del rapporto di cura. – 2. Le macchine possono sbagliare: la necessità di supervisione umana e di empatia. – 3. La sicurezza dei dati e il *digital divide*. – 4. Riflessioni conclusive.

1. Evoluzione del rapporto di cura. Alle origini della tradizione ippocratica, il rapporto tra medico e paziente era fondato su un modello essenzialmente paternalistico, caratterizzato da due presupposti fondamentali: da un lato, il dovere professionale del medico di perseguire il bene del paziente; dall'altro, la pacifica accettazione dell'assistito rispetto alle decisioni diagnostiche e terapeutiche assunte dal curante. La convinzione che il medico operasse sempre nell'interesse del malato si è consolidata nel corso dei secoli, contribuendo a conferirgli il ruolo di autorità morale e, per certi aspetti, una sostanziale immunità sul piano giuridico. Tale impostazione si ritrova anche nella tradizione cristiana, all'interno della quale il medico era assimilato a una figura quasi sacerdotale, chiamata a preservare la salute in quanto bene affidato da Dio. Investito dell'autorevolezza derivante dalle proprie competenze professionali, il medico, era pertanto considerato il soggetto più idoneo a orientare il paziente verso le scelte ritenute migliori per la tutela della salute; mentre il malato, al contrario, era privo delle conoscenze mediche necessarie per comprendere appieno la propria condizione clinica e per assumere autonomamente decisioni terapeutiche, per tale ragione il suo consenso risultava sostanzialmente irrilevante, poiché la richiesta stessa di assistenza implicava l'affidamento alle valutazioni e alle decisioni del medico[1]. Per lungo tempo, dunque, l'*ars medica*, legittimata non soltanto dal sapere scientifico ma anche dall'autorità religiosa, si è sviluppata in uno spazio sostanzialmente sottratto al controllo giuridico. Soltanto a seguito della scoperta degli esperimenti condotti sugli esseri umani nei campi di concentramento nazisti emerse con chiarezza la necessità di sottoporre la ricerca medica ai limiti giuridici ed etici compatibili con il rispetto della dignità delle persone[2]. Da questa nuova sensibilità è emersa una diversa concezione del rapporto di cura, fondata non più sulla sola beneficenza del medico, bensì sul riconoscimento dell'autonomia decisionale dei singoli. Il quadro normativo nazionale ha progressivamente attribuito centralità al principio di autodeterminazione, ponendo al contempo il limite del rispetto della persona umana allo stesso intervento, legittimo[3], del legislatore[4]. L'art. 32, c. 2, Cost. riconosce, infatti, il diritto

* *Sottoposto a referaggio.*

** Dottoranda di ricerca in Diritto costituzionale – Università della Tuscia.

[1] Tale approccio implica la sottomissione del paziente «alla sacra decisione del medico», cfr. V. Mallardi, *Le origini del consenso informato,* in *Acta Otorhinolaryngol Italica*, 25, 2005, 313.

[2] C. Casonato, *La scienza come parametro interposto di costituzionalità,* in *Rivista AIC*, 2, 2016, 4.

[3] Rispetto alla legittimità del trattamento cfr. P. Veronesi, *L'eccezione alla regola: il caso dei trattamenti sanitari obbligatori,* in *Rivista AIC*, 6, 2021, 233.

[4] S. Mangiameli, *Autodeterminazione: diritto di spessore costituzionale?*, in *Forum di Quaderni costituzionali*, Relazione tenuta al IV Laboratorio Sublacense su «La comunità familiare e le scelte di fine vita», 3-5 luglio 2009, 18, ove

dell'individuo di decidere liberamente in ordine ai trattamenti sanitari che lo riguardano, consentendo l'imposizione di trattamenti obbligatori soltanto nei casi previsti dalla legge e nel rispetto della dignità umana[5]. Tale libertà di cura si traduce, pertanto, nella facoltà di accettare o rifiutare le cure proposte in conformità ai propri valori, alle proprie convinzioni e al proprio personale progetto di vita. L'autodeterminazione terapeutica non è in ogni caso da intendersi come una libertà astratta o meramente formale, ma come la concreta possibilità di orientare le decisioni riguardanti il proprio corpo[6] e la propria salute. Il fondamento costituzionale di tale diritto, infatti, non è da rinvenire esclusivamente nell'art. 32 Cost.[7] ma anche negli artt. 2 e 13 Cost.; dal combinato disposto di questi articoli emerge il legame inscindibile tra tutela della salute, libertà personale e libero sviluppo della personalità. La giurisprudenza costituzionale ha progressivamente valorizzato questa lettura sistematica, riconoscendo nel consenso informato uno strumento essenziale per la tutela della dignità della persona e per l'effettivo esercizio della libertà di autodeterminazione[8]. Tuttavia, tale capacità, per essere efficace come massima espressione della libertà in capo al singolo, implica una riflessione sul grado di consapevolezza del soggetto sottoposto a trattamento, che deve conoscersi e sapere porsi in relazione alle scoperte scientifiche del tempo. Solo in questa prospettiva la conoscenza scientifica non si pone in antitesi rispetto all'autonomia individuale, ma ne costituisce un presupposto essenziale, potendo essere considerata «architetto della libertà dei singoli»[9]. La piena realizzazione dell'autodeterminazione presuppone inevitabilmente l'esistenza di condizioni organizzative che consentano al paziente di compiere scelte realmente consapevoli. Il rispetto delle decisioni del paziente, infatti, spesso richiede l'adozione di specifici protocolli assistenziali e di informazione, la cui attuazione richiede ulteriori risorse professionali ed economiche[10] perché solo attraverso una conoscenza adeguata della propria condizione clinica e delle opzioni terapeutiche disponibili il paziente può decidere liberamente se sottoporsi o meno a un trattamento e revocare in qualsiasi momento il consenso precedentemente prestato. L'effettivo esercizio di tale libertà, dunque, dipende da fattori economici, culturali e sociali. Ne deriva il rischio che ciò che risulta biologicamente possibile e giuridicamente consentito non sia concretamente accessibile a tutti in eguale misura, con conseguenti effetti discriminatori[11]. Potrebbero crearsi

si evidenzia come, grazie all'intervento dell'on. Moro in Assemblea costituente, si sia giunti a una formulazione che impedisce alla legge di «violare i limiti imposti dal rispetto della persona umana».

[5] Sul concetto di rispetto della persona umana, cfr. A.A. Negroni, *Art. 32 della Costituzione e superamento delle vaccinazioni obbligatorie*, in *Forum di Quaderni costituzionali*, 2, 2020, 813-815.

[6] Sul progressivo ridimensionamento del divieto di atti di disposizione del proprio corpo previsto dall'art. 5 c.c., cfr. A. D'Aloia, *Al limite della vita: decidere sulle cure*, in *Quaderni costituzionali*, 2, 2010, 241.

[7] La circostanza in base alla quale il consenso informato trova il suo fondamento negli artt. 2, 13 e 32 della Cost. pone in risalto la sua funzione di sintesi di due diritti fondamentali della persona: quello all'autodeterminazione e quello alla salute, in quanto, se è vero che ogni individuo ha il diritto di essere curato, egli ha, altresì, il diritto di ricevere le opportune informazioni in ordine alla natura e ai possibili sviluppi del percorso terapeutico, nonché delle eventuali terapie alternative; informazioni che devono essere le più esaurienti possibili, proprio al fine di garantire la libera e consapevole scelta da parte del paziente anche rispetto alla scelta del medico e del luogo di cura.

[8] Cfr. Corte cost., sent. n. 438/2008, punto 4 del *Considerato in diritto*, ove si afferma che il consenso informato costituisce una sintesi dei diritti fondamentali all'autodeterminazione e alla salute, trovando il proprio fondamento negli artt. 2, 13 e 32 Cost.

[9] Espressione ripresa da A. Gusmai, *Il diritto all'autodeterminazione: una libertà «perimetrata» dal sapere scientifico?*, in *Diritti fondamentali*, 1, 2019, 2. L'Autore spiega tale espressione osservando che biologi e genetisti, attraverso la ricerca scientifica, possono spingere la vita oltre la sua «storia naturale».

[10] F. Minni, A. Morrone, *Il diritto alla salute nella giurisprudenza della Corte costituzionale*, in *Rivista AIC*, 3, 2023, 8-11.

[11] Trib. Modena, decreto 14 maggio 2009, in Giurisprudenza di merito, 11, 2009, 2693, secondo cui l'intervento sociale rimane funzionale alla persona e alla sua sfera di autodeterminazione.

tensioni derivanti dalla limitazione della capacità di scelta di alcuni per il limitato accesso alle innovazioni clinico-terapeutiche, che si traducano in nuove forme di disuguaglianza. Appare pertanto auspicabile un processo legislativo maggiormente capace di confrontarsi con l'innovazione scientifica fin dalle sue prime fasi, valorizzando il contributo degli esperti all'interno del procedimento parlamentare. Ciò non significherebbe attribuire agli scienziati un potere decisionale sostitutivo di quello politico, che deve rimanere nelle mani delle istituzioni democraticamente legittimate, ma consentirebbe di elaborare regole più consapevoli e adeguate alle sfide poste dal progresso tecnologico e biomedico, evitando al singolo di trovarsi senza supporto al confronto con la scienza nella fase giudiziale[12]. In ogni caso, al di là delle modalità attraverso cui l'ordinamento è chiamato a governare l'innovazione scientifica, il principio del consenso informato costituisce ormai un valore consolidato tanto a livello nazionale quanto internazionale. Ad esempio, la Convenzione sui diritti dell'uomo e la biomedicina, adottata a Oviedo nel 1997 e ratificata in Italia con la l. n. 145/2001 stabilisce che ogni intervento sanitario richiede il consenso libero e informato della persona interessata, la quale può revocarlo in qualsiasi momento[13]. Analogamente, la Carta dei diritti fondamentali dell'Unione europea riconosce il consenso informato quale presupposto imprescindibile di legittimità dell'intervento sanitario[14]. La costruzione di un'effettiva alleanza terapeutica, quindi, presuppone un rapporto di fiducia tra medico e paziente, fondato su un'informazione corretta, completa e comprensibile[15]. Tuttavia, il rapido progresso scientifico e tecnologico, oltre a moltiplicare le opportunità diagnostiche e terapeutiche, accresce la complessità delle informazioni necessarie affinché il paziente possa esercitare in modo effettivo il proprio diritto all'autodeterminazione. In questo sistema di già fragili equilibri del rapporto di cura l'impiego crescente di sistemi di intelligenza artificiale impone una riflessione ulteriore sulla centralità della persona assistita. Proprio con riferimento all'istituto del consenso informato si concentra, infatti, uno dei principali interrogativi sollevati dall'introduzione di tali tecnologie: fino a che punto il diritto all'informazione richiede che il paziente sia reso edotto del funzionamento degli strumenti algoritmici impiegati nel processo clinico? La questione assume particolare rilevanza nei casi in cui i sistemi di intelligenza artificiale incidano in misura significativa sulle decisioni diagnostiche o terapeutiche. In tali ipotesi, infatti, il paziente potrebbe legittimamente richiedere di conoscere non soltanto l'esito della valutazione algoritmica, ma anche il ruolo concretamente svolto dal sistema nel processo decisionale e l'incidenza che esso ha avuto sulla scelta finale del professionista sanitario. Se il rapporto medico-paziente è da sempre caratterizzato da una sfida epistemologica connessa alla difficoltà, per il paziente, di comprendere informazioni tecniche e specialistiche, l'impiego dell'intelligenza artificiale introduce, dunque, un ulteriore livello di complessità. Il problema non riguarda soltanto la comprensione delle informazioni cliniche, ma anche l'individuazione del contenuto

Per approfondimento, cfr. A. De Vita, *Il diritto all'autodeterminazione in ambito sanitario e il testamento biologico: verso nuove frontiere del diritto?,* in *Giustizia amministrativa*, 2020.

[12] A. Gusmai, *Il diritto all'autodeterminazione: una libertà «perimetrata» dal sapere scientifico?*, cit., 9-10.

[13] Art. 5, c. 2, Convenzione di Oviedo, che riconosce il diritto dell'interessato a ricevere informazioni adeguate sullo scopo, sulla natura, sulle conseguenze e sui rischi dell'
intervento, nonché a revocare liberamente il consenso in qualsiasi momento.

[14] Art. 3 della Carta dei diritti fondamentali dell'Unione europea, ai sensi del quale «ogni individuo ha diritto alla propria integrità fisica e psichica» e deve essere rispettato, tra l'altro, «il consenso libero e informato della persona interessata, secondo le modalità definite dalla legge». Sul dovere del medico di rispettare le scelte terapeutiche del paziente, cfr. Codice di deontologia medica, Titolo III, artt. 20 ss.; in particolare, l'art. 35 impone al medico di astenersi da trattamenti sanitari in presenza di un valido rifiuto dell'interessato.

[15] Sul punto v. Cass. civ., sez. III, sent. n. 364/199, cfr. *ex multis* Cass. civ., sez. III, sent. n. 2847/2010 e Cass. civ., sez. III, sent. n. 27751/2013.

dell'informazione tecnologica da fornire all'interessato. Ci si interroga, in particolare, su quali elementi relativi al funzionamento dei sistemi algoritmici debbano essere comunicati affinché il consenso possa dirsi realmente informato e l'autodeterminazione del paziente effettivamente garantita.

L'art. 78 del Codice di deontologia medica, pur non disciplinando espressamente l'intelligenza artificiale, afferma il dovere del medico di assicurare un'adeguata informazione e di acquisire il consenso informato del paziente anche nell'impiego di strumenti e innovazioni tecnologiche. La disposizione conferma come l'introduzione di nuove tecnologie non attenui gli obblighi informativi gravanti sul professionista sanitario, ma richieda, al contrario, una rinnovata attenzione alla qualità e alla comprensibilità delle informazioni fornite alla persona assistita[16]. Ugualmente, il Comitato Nazionale di Bioetica e il Comitato Nazionale per la Biosicurezza, le Biotecnologie e le Scienze della Vita sostengono il dovere del medico di informare il paziente qualora l'uso dell'AI abbia portato a una diagnosi o a una proposta terapeutica[17]. Il regolamento (UE) n. 2024/1689 (*AI Act*), all'art. 50 introduce infatti specifici obblighi di trasparenza, imponendo che le persone fisiche siano informate quando interagiscono con un sistema di intelligenza artificiale, salvo che tale circostanza risulti evidente per una persona ragionevolmente informata. Nella medesima prospettiva si colloca la l. n. 132/2025 in materia di intelligenza artificiale, la quale si spinge oltre quanto previsto dall'*AI Act* perché quest'ultimo prevede soprattutto un obbligo di trasparenza sull'interazione con l'IA, mentre la l. n. 132/2025 sposta l'attenzione sulla relazione professionista-paziente e sulla qualità dell'informazione, avvicinandosi molto di più alle logiche del consenso informato[18]. Nell'ambito della relazione terapeutica che prevede l'impiego di strumenti dotati di intelligenza artificiale, l'estensione dell'informazione dovuta al paziente dipende dunque dal ruolo concretamente svolto da tali sistemi nel processo decisionale clinico. Inoltre, la funzione dell'informazione rispetto alla conoscenza implica che l'estensione e il contenuto della comunicazione debbano essere calibrati sulle effettive esigenze del paziente e spetta al medico individuare e selezionare le informazioni rilevanti, essendo il soggetto maggiormente in grado di valutare le capacità cognitive, il livello culturale e le condizioni psicologiche dell'assistito. In questo contesto assumono pertanto rilievo i principi di ragionevolezza e proporzionalità: il primo costituisce un criterio flessibile, idoneo a contemperare i molteplici interessi coinvolti nel rapporto di cura; il secondo opera come parametro di valutazione dell'obbligo informativo, assicurando che la comunicazione del sanitario risulti adeguata alle concrete necessità del destinatario delle cure. L'obiettivo è quello di porre il paziente nelle condizioni di maturare una decisione realmente libera e consapevole, fondata sulla comprensione delle informazioni rilevanti per il trattamento sanitario. Ne consegue che l'ampiezza del consenso informato non può essere definita in termini assoluti, ma varia in relazione alle circostanze del caso concreto, tenendo conto, da un lato, dell'incidenza concretamente esercitata dal sistema di intelligenza artificiale sul procedimento diagnostico o terapeutico e, dall'altro, dell'età, del livello culturale e delle capacità di

[16] In tale prospettiva, è stato osservato che l'art. 78, collocato nel Titolo XVIII, rubricato «Informazione e innovazione sanitaria», sembra riferirsi principalmente all'informativa relativa al trattamento dei dati sanitari e non direttamente al consenso alle cure, F. Ferretti, *La relazione di cura e il consenso informato nell'era della Medical Artificial Intelligence*, in *Corti supreme e salute*, 1, 2025, 108.

[17] Comitato nazionale per la Bioetica, Comitato nazionale per la Biosicurezza, le Biotecnologie e le Scienze della Vita, *Intelligenza artificiale e medicina: aspetti etici*, 29 maggio 2020, 14, ove si afferma che sussiste un «obbligo etico e giuridico» di informare adeguatamente il paziente che si sottoponga a trattamenti sanitari fondati sull'impiego dell'intelligenza artificiale.

[18] Art. 13, c. 2, l. n. 132/2025, secondo cui «per assicurare il rapporto fiduciario tra professionista e cliente, le informazioni relative ai sistemi di intelligenza artificiale utilizzati dal professionista sono comunicate al soggetto destinatario della prestazione intellettuale con linguaggio chiaro, semplice ed esaustivo».

comprensione del paziente. Va, infine, comunque, ribadito che nonostante i rilevanti progressi compiuti nel settore della *Explainable Artificial Intelligence*, permane una considerevole distanza rispetto all'obiettivo di una piena spiegabilità dei sistemi più complessi, in particolare di quelli fondati su tecniche avanzate di *deep learning.* Gli strumenti di *auditing* algoritmico, le tecniche di *reverse engineering* e i metodi di interpretazione *ex post* consentono frequentemente di ottenere soltanto ricostruzioni approssimative del percorso decisionale seguito dal sistema[19]. Nella realtà il diritto all'informazione non può essere interpretato nel senso di imporre una completa conoscenza del funzionamento tecnico dell'algoritmo[20] perché ciò che assume rilevanza è che il paziente sia posto nelle condizioni di comprendere gli elementi essenziali che hanno inciso sulla decisione clinica e il peso specifico del sistema tecnologico[21] diversamente non è invece necessario conoscere nel dettaglio il codice sorgente, l'architettura del modello, il flusso dei dati o i meccanismi computazionali interni dell'algoritmo, così come non è mai stato richiesto di comprendere i processi neurobiologici sottesi al ragionamento del medico umano[22].

2. Le macchine possono sbagliare: la necessità di supervisione umana e di empatia.

Per preservare la fiducia nel paradigma della cura non è sufficiente garantire il diritto di trasparenza e di informazione, ma è necessario anche comprendere i rischi connessi all'impiego delle nuove tecnologie, così da sviluppare una consapevolezza critica sul fatto che anche i sistemi di intelligenza artificiale, al pari degli esseri umani, possono commettere errori. Partendo da questo assunto, diventa centrale interrogarsi sui rischi sistemici dei procedimenti automatizzati, primo fra tutti quello delle discriminazioni algoritmiche. Tali criticità assumono particolare rilievo nel contesto del sistema sanitario italiano, fondato, tra gli altri, sul principio di equità che può essere declinato sia come uguaglianza nell'uso delle cure sia come uguaglianza nell'accesso alle stesse. Quello che si vuole dimostrare è che eventuali errori diagnostici o terapeutici possono incidere negativamente sulla fiducia dei cittadini nei confronti del sistema sanitario. Di conseguenza, la capacità dell'intelligenza artificiale di incidere in modo significativo sulle decisioni relative all'accesso, alla qualità e alla priorità delle cure rende imprescindibile l'introduzione di adeguati meccanismi di supervisione umana, volti a prevenire, individuare e correggere esiti distorsivi o ingiustamente discriminatori[23]. I

---

[19] F. Ferretti, *La relazione di cura e il consenso informato nell'era della Medical Artificial Intelligence*, cit., 114, riporta l'esempio di MYCIN, sistema esperto sviluppato presso l'Università di Stanford per supportare i medici nella diagnosi e nel trattamento delle infezioni batteriche. Tale sistema, progettato per essere comprensibile, si basava su regole di conoscenza di tipo *if-then*, consentendo agli esperti di codificare protocolli diagnostici. Per approfondimenti in merito alla trasparenza algoritmica, cfr. Y. Zhang, S. Kang, R. Meng, M. Böhme, A. Roychoudhury, *VeriGrey: Greybox Agent Validation*, 2026; H. Zhang, Y. Rong, Y. He, H. Chen, *LLAMAFUZZ: Large Language Model Enhanced Greybox Fuzzing*, in *7th ACM/IEEE International Conference on Automation of Software Test (AST 2026)*, Rio de Janeiro, 2026.

[20] Come spiegato nell'ordinanza Cass. a n. 28358 del 10 ottobre 2023.

[21] L. Piva, Cassazione Civile, sez. I – ord. n. 28358/2023: lecito il *rating* reputazionale a mezzo di algoritmo quando l'utente ne conosce il procedimento, in *Rivista di BioDiritto*, 2023.

[22] B. Mittelstadt, *The Impact of Artificial Intelligence on the Doctor-Patient Relationship*, in Consiglio d'Europa, dicembre 2021, 48.

[23] Il termine «*bias*», utilizzato per indicare i c.d. algoritmi discriminatori, si riferisce a pregiudizi incorporati nei sistemi informatici che determinano discriminazioni sistematiche e ingiuste a danno di determinati individui o gruppi. La definizione è ripresa da V. Molaschi, *Algoritmi e discriminazione*, in *Fundamental Rights*, 2, 2022, 28-29, il quale precisa che tali discriminazioni si verificano soprattutto nei processi algoritmici connessi ad attività di profilazione, ove per profilazione si intende, ai sensi del GDPR, «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la

modelli predittivi costruiti su basi dati non inclusivi possono produrre risultati meno accurati per specifiche categorie di pazienti, con conseguenze negative in termini di diagnosi, prognosi o accesso alle cure. Relativamente alla discriminazione algoritmica occorre rilevare l'importanza della fase iniziale del processo di valutazione, costituita dalla selezione dei *dataset*, in quanto, come sappiamo i sistemi di intelligenza artificiale si basano sull'analisi dei *big data*, ovvero di grandi quantità di dati aggregati, per formulare le proprie decisioni; di conseguenza, la scelta dei dati di addestramento risulta fondamentale per prevenire il rischio di discriminazioni algoritmiche. In tale contesto assume particolare rilievo il principio del *garbage in*, *garbage out*, secondo il quale l'utilizzo di dati incongrui, inesatti o non affidabili conduce inevitabilmente a decisioni errate, inaffidabili e potenzialmente discriminatorie. Un ulteriore rischio di *bias* e, conseguentemente, di risultati discriminatori, può derivare non solo dall'impiego di dati «contaminati» per progettare sistemi medicali ma anche dall'impiego di *dataset* incompleti, capaci di offrire una rappresentazione solo parziale e distorta della realtà. Nello studio *Geographic Distribution of US Cohorts Used to Train Deep Learning Algorithms* dell'Università di Stanford del settembre 2020 si rende noto il fatto che la maggior parte degli algoritmi diagnostici statunitensi risulta addestrata su dati provenienti da soli tre Stati (California, Massachusetts e New York), escludendo completamente trentaquattro Stati e includendone solo parzialmente altri tredici. Tale configurazione solleva seri interrogativi sull'affidabilità di questi strumenti nel garantire diagnosi eque su una popolazione eterogenea, caratterizzata da differenze etniche, ambientali e socioeconomiche[24]. Una volta predisposto il *dataset*, le correlazioni tra i dati vengono elaborate autonomamente dal sistema di intelligenza artificiale attraverso processi che, allo stato attuale, come già detto, risultano spesso opachi e difficilmente interpretabili anche dagli stessi sviluppatori[25]. Ciò non significa, tuttavia, che il controllo umano debba venire meno, al contrario, il ruolo dell'uomo si rivela essenziale proprio nelle fasi in cui l'intervento dell'intelligenza biologica è ancora possibile e doveroso: in primo luogo, nella selezione e validazione dei dati utilizzati per l'addestramento del sistema; in secondo luogo, nella valutazione finale degli esiti prodotti dall'algoritmo, al fine di verificare se le decisioni generate in modo automatico e repentino siano coerenti e ragionevolmente comparabili con quelle che sarebbero state assunte da un professionista umano qualificato. Con riferimento ai pregiudizi legati alla progettazione dei dispositivi medici, appare significativo il caso dei saturimetri, strumenti essenziali per la misurazione dell'ossigenazione del sangue, il cui funzionamento si basa sull'emissione di fasci di luce; al riguardo è stato dimostrato che il colore della pelle può influenzare i risultati delle misurazioni, generando un pregiudizio sanitario nei confronti delle persone con pelle scura. Tale criticità è stata rilevata nel 2021 dal *National Health Service* (NHS) britannico e dalla *Medicines and Healthcare products Regulatory Agency* (MHRA), nel pieno della seconda ondata della pandemia da Covid-19, i quali hanno evidenziato come, nei pazienti con pelle scura, i saturimetri tendessero a sovrastimare i livelli di ossigenazione del sangue, con il rischio di non individuare tempestivamente condizioni di insufficienza respiratoria grave[26]. In

situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti».

[24] P. Cozzi, *Nuove riflessioni critiche sul rischio di discriminazione algoritmica in ambito sanitario*, in *Tech4Futures*, 7 gennaio 2025.

[25] D. Morondo Taramundi, *Le sfide della discriminazione algoritmica*, in *Genius*, 2022, 7, il quale parla di «pregiudizi digitali autonomi», in quanto generati da sistemi di machine learning basati su correlazioni costruite automaticamente e non sempre comprensibili neppure agli stessi sviluppatori, circostanza che rende tali *biads* particolarmente difficili da individuare e correggere.

[26] P. Cozzi, *Nuove riflessioni critiche sul rischio di discriminazione algoritmica in ambito sanitario*, in *Tech4Futures*, 7 gennaio 2025.

riferimento, invece, al rischio rappresentato dall'impiego di dati incompleti, occorre valutare criticamente gli strumenti utilizzati per la diagnosi del tumore al seno per il quale vengono considerati *data set* composti esclusivamente da dati relativi a donne caucasiche che tuttavia hanno una densità mammaria differente rispetto alle donne afro-americane e di conseguenza si può avere un rischio di una minore attendibilità della macchina e una discriminazione nell'accesso alle cure molto importanti per il solo fatto di non aver tenuto in adeguata considerazione l'eterogeneità delle persone che si sottopongono al *test di screening*[27]. Queste vicende dimostrano come l'utilizzo dei sistemi algoritmici in ambito sanitario non può prescindere da un adeguato controllo umano, volto a evitare che la decisione automatizzata si traduca in una compressione ingiustificata del diritto alla salute[28]. Non a caso, l'*AI Act* sottolinea espressamente la necessità della supervisione umana, in linea con il principio della non esclusività della decisione algoritmica. Se il primato della valutazione umana rispetto a quella digitale non è in discussione, ciò su cui occorre investire è piuttosto un'adeguata formazione digitale del personale sanitario, condizione imprescindibile affinché la supervisione non rimanga meramente formale. In assenza di tali competenze, infatti, i rischi connessi all'uso dell'intelligenza artificiale sono destinati a persistere anche in presenza di un controllo umano, poiché l'opacità dei sistemi algoritmici può anche indurre gli operatori sanitari ad affidarsi in modo passivo ai risultati prodotti dalla macchina. A tal proposito, appare opportuno richiamare un recente caso di discriminazione, che evidenzia in modo particolarmente significativo l'importanza della formazione tecnico-digitale del personale sociosanitario, quale fattore determinante per prevenire disuguaglianze nell'accesso ai servizi sanitari. Il riferimento è al sistema, *Quantus Skin*, sviluppato nei Paesi Baschi per la valutazione del rischio di cancro cutaneo e per la gestione delle priorità di accesso alle visite dermatologiche. Il sistema, basato sull'analisi algoritmica di immagini cutanee acquisite dai medici di medicina generale, ha mostrato gravi criticità riconducibili alla scarsa qualità dei dati di *input*, determinata dall'inadeguata capacità tecnica dei professionisti nel produrre immagini clinicamente idonee. Tale carenza formativa, combinata con un affidamento acritico e incondizionato alle decisioni automatizzate[29], ha compromesso l'accuratezza delle valutazioni diagnostiche, con conseguenze particolarmente rilevanti se si considera che il melanoma è una neoplasia che richiede un'elevata tempestività diagnostica[30].

***3. La sicurezza dei dati e il* digital divide.** Si è detto che la soluzione per prevenire le discriminazioni algoritmiche consiste soprattutto nell'avere a disposizione dati completi, affidabili e realmente rappresentativi. Tuttavia, la costruzione di *dataset* affidabili non pone

[27] Un caso riportato da numerosi studi relativi ai rischi connessi all'implementazione di *AI systems for breast cancer screening* è richiamato da C. Menech, *Intelligenza artificiale e autodeterminazione in materia sanitaria*, in *BioLawJornal-Rivista di Biodiritto*, 1, 2022, 186.

[28] Dell'importanza del controllo umano per il superamento delle discriminazioni algoritmiche si occupa P. Zuddas, *Algoritmi e discriminazioni*, in *Consulta Online*, Liber amicorum per Pasquale Costanzo, 2020, 11. Analogamente, l'art. 14, Reg. (UE) n. 2024/1689 riconosce la centralità della supervisione umana quale presidio essenziale di tutela del diritto alla salute.

[29] J.P. Solè, *Il regolamento dell'unione europea sull'intelligenza artificiale, la discrezionalità amministrativa e la riserva di umanità*, in *Rivista Trimestrale di diritto pubblico*, 3, 2024, 833, riporta il caso l'*automation bias*, spiegando che gli esseri umani tendono a fidarsi di ciò che i sistemi utilizzati ci dicono e raramente lo mettono in discussione, il che può portare a scenari estremi come le cosiddette «morti da GPS», ovvero persone perse nel deserto che muoiono a causa delle indicazioni sbagliate del navigatore.

[30] A. Bernardo, M. Alvarez del Vayo, C. Torrecillas, A. Maqueda, *Lunar or cancer? El algoritmo que se equivoca en uno de cada tres melanomas y obvia a los pacientes con la piel oscura*, in *Civio*, 26 giugno 2025, spiegano che il sistema avrebbe ignorato circa un melanoma su tre, soprattutto nei pazienti con pelle scura, producendo evidenti effetti discriminatori nell'accesso alle cure.

soltanto un problema tecnico risolvibile tramite correzioni algoritmiche, ma richiede, inoltre, un'adeguata considerazione della sicurezza dei dati sanitari e un'adeguata alfabetizzazione digitale anche dei pazienti. Questi elementi costituiscono presupposti fondamentali per garantire un funzionamento equo e non discriminatorio del sistema sanitario; diversamente, il rischio è quello di generare ulteriori forme di discriminazione legate a fattori tecnico-sociali, più che agli algoritmici in sé. In altre parole, in assenza di solide garanzie di protezione dei dati e di pazienti sufficientemente consapevoli e formati all'uso degli strumenti digitali, la completezza dei *dataset* potrebbe essere compromessa dal timore di condividere le proprie informazioni personali[31].

La questione assume particolare rilevanza nella società digitale contemporanea, in cui gli individui sono spesso disposti a condividere i propri dati personali in cambio di servizi, sconti o altri benefici; quando però la condivisione riguarda dati sanitari, emergono maggiori resistenze legate alla tutela della privacy. Tali preoccupazioni risultano comprensibili alla luce della natura particolarmente sensibile di queste informazioni, che possono incidere profondamente sulla sfera personale dell'individuo e richiedono pertanto garanzie di protezione più elevate rispetto ad altre categorie di dati.

La complessità aumenta ulteriormente a causa della molteplicità di informazioni presenti nei vari dispositivi, a partire dai sistemi di *m-health*, che consentono di raccogliere enormi quantità di dati, i quali possono venire collegati con altre informazioni per profilare le persone[32], spesso nell'oscurità delle cosiddette «scatole nere»[33].

Un esempio dei rischi connessi alla condivisione dei dati sanitari è rappresentato dal caso *Ascension*, colosso della sanità statunitense, che ha ceduto a Google i dati sanitari di milioni di pazienti per sviluppare un software volto a migliorare la collaborazione in tempo reale tra operatori sanitari e garantire l'efficienza delle cure. Le principali preoccupazioni derivano dall'esperienza di *data mining* di *Google* e dal conseguente rischio che tali informazioni possano essere incrociate con altri dati già in possesso del colosso tecnologico, generando nuovi dati personali di elevato valore economico, in particolare nei settori della ricerca medico-scientifica e delle assicurazioni[34].

Va detto, inoltre, che purtroppo il settore sanitario è oggi tra quelli maggiormente esposti agli attacchi informatici: dal gennaio 2023 si registrano in media 4,3 attacchi informatici al mese ai danni di strutture sanitarie. Di questi, circa la metà ha prodotto incidenti con un impatto effettivo sui servizi erogati, mettendo a rischio sia la continuità delle prestazioni sanitarie sia la *privacy* dei pazienti[35].

In questo senso, non si può non ricordare uno dei più gravi incidenti informatici verificatosi in Italia nel 2021, ovvero l'attacco *ransomware* alla Regione Lazio, reso possibile attraverso le credenziali compromesse di un dipendente in *smart working*. Tale errore ha determinato per qualche ora l'impossibilità di accesso a numerosi servizi sanitari nel pieno della campagna

---

[31] E. Scalson, *Cybersicurezza e dispositivi medici*, in *Biodiritto*, 1, 2024, 187, evidenzia come la mancata fiducia nei sistemi digitali sia alimentata dai rischi connessi alla sicurezza e dalle persistenti minacce di cybersicurezza.

[32] Sui rischi legati all'utilizzo della profilazione a discapito per i diritti fondamentali cfr. A. Gatti, *Profilazione e diritti fondamentali. Modelli a confronto: Europa, Usa, America Latina*, Napoli, 2024, 280- 281.

[33] G. Fioriglio, *La protezione dei dati sanitari nella società algoritmica*, cit., 88.

[34] Non a caso, Google ha recentemente proceduto all'acquisizione di *Fitbit*, società produttrice di dispositivi indossabili, come riportato da P. Licata, *Bufera M HEALTH su Google: raccolti dati sanitari di 50 milioni di persone*, in *Network360*, 13 novembre 2019.

[35] Rapporto *La minaccia cibernetica al settore sanitario. Analisi e raccomandazioni*, realizzato dall'Agenzia per la cybersicurezza nazionale, fotografa la situazione nel periodo gennaio 2023 – settembre 2025, 31 ottobre 2025. I diversi casi di *data breach* hanno dimostrato la vulnerabilità degli enti pubblici che gestiscono dati sensibili e servizi essenziali, evidenziando le gravi conseguenze che tali attacchi possono produrre sia sulla tutela dei dati personali dei pazienti sia sulla continuità dell'erogazione dei servizi sanitari.

vaccinale contro il COVID-19[36].
Nonostante tali rischi, è necessario essere consapevoli che il futuro dell'innovazione in ambito sanitario dipende in larga misura dall'interoperabilità dei dati. A testimonianza di questa esigenza, la rivista medico-scientifica *The Lancet* nel gennaio 2025 ha fatto notare come una delle principali debolezze del sistema sanitario italiano risieda proprio nella frammentarietà dell'infrastruttura dei dati sanitari[37]. Tale criticità non riguarda esclusivamente il contesto italiano, ma interessa anche altri paesi europei[38].
L'Unione europea, consapevole dell'importanza dell'interoperabilità dei dati in uno spazio sicuro, sta tentando di costruire una società fondata sulla disponibilità dei dati e sulla fiducia dei cittadini nell'ambiente digitale[39].
La Strategia europea per i dati, pubblicata dalla Commissione europea il 19 febbraio 2020 risponde proprio a questa esigenza e comprende: il regolamento (UE) n. 2022/868, il Data *Governance Act*, entrato in vigore il 23 giugno 2022, volto a rafforzare la fiducia nella condivisione dei dati; nonché il regolamento (UE) n. 2023/2854, *Data Act*, il quale mira a promuovere una condivisione più efficiente dei dati all'interno dell'Unione. Quest'ultimo regolamento introduce anche meccanismi finalizzati ad aumentare la disponibilità dei dati, favorirne il riutilizzo e superare gli ostacoli tecnici e organizzativi che ne limitano la circolazione, con l'obiettivo di migliorare l'accesso ai servizi sanitari, ridurre il rischio clinico-diagnostico e favorire una maggiore personalizzazione delle cure[40].
A perfezionamento del disegno normativo si pone il regolamento sullo Spazio europeo dei dati sanitari, *European Health Data Space* – EHDS, che mira a creare un sistema comune di condivisione dei dati sanitari fondato sui principi di interoperabilità, sicurezza e tutela dei diritti fondamentali. In considerazione della specifica necessità di una maggiore sicurezza nella condivisione dei dati, si inserisce soprattutto la direttiva (UE) n. 2022/2555, NIS 2, adottata il 14 ottobre 2022, che ha come fine proprio quello di creare un elevato livello di sicurezza delle reti e dei sistemi informativi nell'Unione, rafforzando la cooperazione tra gli Stati membri, in particolare nei settori che erogano servizi essenziali[41].
La direttiva introduce un sistema stringente di segnalazione dei rischi con tempistiche di notifica ben definite. In una società algoritmica caratterizzata da sistemi in continua

[36] Provvedimento del Garante per la protezione dei dati personali n. 195 del 21 marzo 2024, con il quale, all'esito di un'istruttoria volta all'accertamento delle responsabilità, l'Autorità ha irrogato una sanzione amministrativa pecuniaria e le sanzioni accessorie ex art. 52, par. 2, lett. i), e art. 83, Reg. (UE) n. 2016/679, nonché ex art. 166, c. 7, del Codice in materia di protezione dei dati personali.
[37] A. De Vico, *The Lancet e il sistema sanitario italiano*, in *Pandora Rivista*, 30 giugno 2025, chiarisce che la principale criticità riguarda l'assenza di un sistema unificato e centralizzato per la documentazione e la condivisione delle cartelle cliniche elettroniche (*Electronic Health Records* – EHR), dei dati ospedalieri e di quelli provenienti dalla medicina generale. La rivista osserva che «la mancanza di standardizzazione impedisce la creazione di registri nazionali, ostacolando l'efficacia delle cure».
[38] Cfr. Á. Bernardo, M. Álvarez del Vayo, A. Maqueda, C. Torrecillas, T. García, *L'arrivo dell'intelligenza artificiale nella sanità pubblica: opaca, diseguale e con poca supervisione*, in *Civio*, 6 novembre 2025. Uno studio della Commissione europea segnala che in Spagna e in Europa si registra una perdita di efficienza sanitaria dovuta alla mancanza di interoperabilità, standardizzazione e semantica dei dati, nonché a difficoltà nell'accesso, nello scambio e nell'analisi massiva delle informazioni. Il dato è ripreso da *Informe C. Inteligencia artificial y salud: potencial y desafíos*, 14 novembre 2022.
[39] E. Sorrentino, A.F. Spagnolo, *Gestione e conservazione dei dati sanitari. Il vulnus normativo che impatta sulla sicurezza e data protection*, in *Federalismi.it*, 29, 2024, 142.
[40] Per approfondimenti, cfr. S. Torreggiani, *Il Data Act: una versione europea del data nationalism?*, in *Rivista italiana di informatica e diritto*, 2, 2023, 138-139.
[41] Quest'ultimo aspetto rappresenta una novità rispetto alla NIS 1, che non teneva adeguatamente conto dell'ambito di applicazione della direttiva, in particolare con riferimento a settori che oggi vengono qualificati dalla nuova disciplina come «particolarmente critici». In tale prospettiva, i soggetti che erogano servizi sanitari sono da considerare essenziali, in ragione della natura fondamentale delle prestazioni rese alla collettività.

evoluzione e da flussi di dati spesso difficilmente controllabili, è fondamentale avere un'infrastruttura capace non solo di rispondere ai singoli incidenti, ma di affrontare anche eventi imprevisti attraverso un modello cooperativo. La sfida principale consiste nel bilanciare l'esigenza di garantire la sicurezza delle infrastrutture critiche con la flessibilità, necessaria per adattarsi alle diverse realtà operative e ai rischi specifici di ciascun settore[42]. In altre parole occorre riadattare i principi di *by design* e *by default*[43] a sistemi in continua evoluzione, che trasferiscono dati continuamente e in modo incontrollabile[44] per questa ragione forse oltre a migliorare la resilienza informatica occorre parallelamente affrontare il problema dell'alfabetizzazione digitale perché come si è avuto modo di leggere dal Rapporto *Clusit* sulla *cybersecurity* in Italia e nel mondo e avuto modo di comprendere grazie all'esempio dell'attacco *hacker* alla Regione Lazio, uno dei più grandi rischi per la cybersicurezza è rappresentato dall'errore umano[45] dovuto spesso dall'inconsapevolezza dei rischi legate alle proprie azioni.

4. Riflessioni conclusive. Dalle considerazioni svolte emerge come l'impiego dell'intelligenza artificiale in ambito sanitario, pur offrendo significative opportunità di miglioramento dell'assistenza e dell'efficienza dei servizi, sollevi questioni particolarmente delicate in relazione alla tutela dei diritti fondamentali e, soprattutto, al rispetto dell'autonomia decisionale del paziente. In questo contesto, il consenso informato conserva un ruolo centrale nel rapporto di cura e richiede che il ricorso a sistemi algoritmici non comporti un arretramento della capacità umana di comprendere, valutare e controllare le decisioni cliniche.

L'effettiva integrazione dell'intelligenza artificiale nella pratica sanitaria presuppone, pertanto, che il professionista mantenga un ruolo attivo e consapevole, capace di orientarsi criticamente tra raccomandazioni algoritmiche e valutazioni cliniche, in un modello di cura che vede il paziente sempre più coinvolto e protagonista delle scelte che riguardano la propria salute.

In tale prospettiva, il Programma Europa Digitale si configura come uno strumento complementare rispetto al quadro normativo europeo in materia di protezione dei dati e cybersicurezza. Esso contribuisce non soltanto a rafforzare le capacità tecnologiche degli Stati membri, ma anche a promuovere le competenze necessarie affinché l'innovazione digitale possa svilupparsi in modo responsabile, interoperabile e rispettoso dei principi di inclusione e non discriminazione[46].

Accanto ai principi di *privacy by design* e *privacy by default*, potrebbe quindi trovare spazio quello che si potrebbe definire, in termini descrittivi, un principio di *by education*, fondato sulla centralità della formazione e dell'*empowerment* digitale degli individui. Tale esigenza appare particolarmente rilevante nel settore sanitario, dove il dato personale non rappresenta più soltanto un bene da proteggere, ma costituisce sempre più una risorsa essenziale per

[42] M. Empler, C. Lisi, R. Madaio, *La cybersicurezza tra legislazione nazionale ed europea*, in M.E. Bucalo, M. Caporale, A. Sterpa (a cura di), *Diritto pubblico di Internet*, Napoli, 2024, 317.

[43] I principi di *privacy by design* e *privacy by default* sono disciplinati dall'art. 25, cc. 1 e 2, del Reg. (UE) 2016/679. Per *privacy by design* si intende l'integrazione della protezione dei dati sin dalla fase di progettazione di un sistema o servizio, mentre per *privacy by default* si intendono le impostazioni predefinite dei servizi o prodotti che devono garantire il massimo livello di protezione dei dati personali

[44] G. Fioriglio, op. cit., *88*.

[45] *Rapporto Clusit sulla cybersecurity in Italia e nel mondo, Security Summit 2025*; M. Empler, C. Lisi, R. Madaio, *La cybersicurezza tra legislazione nazionale ed europea*, cit., 305.

[46] Il reg. (UE) 2021/694 istituisce il programma *Europa digitale*. Cfr. anche la Comunicazione della Commissione europea, COM (2021) 118, la quale pone l'obiettivo di garantire competenze digitali all'80% della popolazione entro il 2030.

l'erogazione, la personalizzazione e il miglioramento dei servizi. Proprio per questo, è fondamentale che gli interessati sviluppino una crescente consapevolezza delle modalità di raccolta, utilizzo e condivisione dei propri dati, così da poter esercitare in modo effettivo e informato i propri diritti[47].

Abstract. Il presente contributo intende indagare l'evoluzione del rapporto di cura, concentrando inizialmente l'attenzione sul mutato ruolo del paziente e poi sul tema della fiducia nel rapporto di cura, muovendo dal presupposto che, così come i medici, anche le macchine possono commettere errori. Da ultimo, si intende riflettere sul fatto che gli errori di discriminazione dipendono dalla qualità dei dati e che, per disporre di dati affidabili e completi sotto il profilo qualitativo, è necessario rafforzare i principi di *by design* e *by default*. Tuttavia, appare opportuno andare oltre, promuovendo la creazione di un sistema resiliente non solo dal punto di vista della sicurezza e della cybersicurezza, ma anche sotto il profilo sociale e culturale. Solo in questo modo sarà possibile mantenere la fiducia in un sistema sanitario fondato sul principio di equità.

Abstract. This contribution aims to investigate the evolution of the care relationship, initially focusing on the changing role of the patient and then on the issue of trust within the care relationship, starting from the premise that, just like doctors, machines can also make mistakes. Finally, this contribution reflects on the fact that discrimination errors depend on data quality and that, in order to ensure qualitatively reliable and complete data, it is necessary to strengthen the principles of by design and by default. However, it also appears necessary to go further by promoting the development of a resilient system not only from the perspective of safety and cybersecurity, but also from social and cultural perspectives. Only in this way can trust be maintained in a healthcare system founded on the principle of equity.

Parole chiave. Intelligenza artificiale in sanità – Autodeterminazione del paziente – Sanità mobile – Equità sanitaria – *Privacy* e sicurezza dei dati – Interoperabilità dei dati sanitari – Formazione digitale.

Key words. Artificial Intelligence in Healthcare – Self-Determination – Mobile Health (s) – Health Equity – Data Privacy and Security – Health Data Interoperability-Digital Training.

[47] V. Molaschi, *Algoritmi e discriminazione*, in *Fundamental Rights*, 2, 2022, 38, introduce il concetto di *by education*, evidenziando la necessità che la formazione dei programmatori sia rafforzata, in quanto soggetti chiamati a sviluppare sistemi che possono generare o subire dinamiche discriminatorie, e che devono possedere le competenze necessarie per prevenirle. L'Autore sottolinea in tal senso che «ciò rende tanto più irrinunciabile un'adeguata educazione».