GIANLUIGI FIORIGLIO

VULNERABILITÀ AUMENTATA

Diritto, cura e algoritmi nell'era della salute digitale

Prassi sociale e teoria giuridica
Collana diretta da Thomas Casadei e Gianfrancesco Zanetti
21

Mucchi Editore

Prassi sociale e teoria giuridica

Collana diretta da Thomas Casadei e Gianfrancesco Zanetti

21

Il dibattito giusfilosofico contemporaneo non è più facilmente ricostruibile a partire da opposizioni chiare e distinte: distinzioni e impianti categoriali di una tradizione rassicurante sono oggi messi radicalmente in questione da nuovi approcci metodologici, da innovazioni tecnologiche e da eventi storici imprevisti, nonché da molteplici questioni sociali e inedite sensibilità morali; contributi giusfilosofici interessanti vengono del resto a volte prodotti nell'ambito di riflessioni ufficialmente afferenti a discipline contigue ma diverse.

Può allora diventare importante ascoltare questo dibattito senza pregiudizi, senza preclusioni dottrinali o ideologiche, mantenendo il rigore della ricerca e la fondamentale *accountability* dell'indagine sul campo.

Questa collana persegue l'intento di sviluppare un'attenzione specifica verso quegli "esiti della ricerca" che si generano a ridosso dei cambiamenti in corso, nella consapevolezza che la riflessione teorica non vive sigillata fuori dalle pratiche sociali, o dall'impegno civile che spesso la motiva.

Prassi sociale e teoria giuridica

Collana diretta da Thomas Casadei e Gianfrancesco Zanetti

issn 2612-002X

I volumi pubblicati nella collana sono stati oggetto di procedura di doppio referaggio cieco (*double blind peer review*), secondo un procedimento concordato dai Direttori della collana con l'Editore, che ne conserva la relativa documentazione.

GIANLUIGI FIORIGLIO

VULNERABILITÀ AUMENTATA

Diritto, cura e algoritmi nell'era della salute digitale

Mucchi Editore

Volume pubblicato nell'ambito del progetto FACILITATE – "Framework for Clinical Trial Participants' Data Reutilization for a Fully Transparent and Ethical Ecosystem", con il contributo dei fondi "Innovative Medicines Initiative 2 Joint Undertaking", "European Union (EU)", "Horizon 2020" and "EFPIA" grant agreement N. 101034366 – FACILITATE – H2020-JTI-IMI2-2020-23-two-stage H2020 IMI2 JU MGA, coordinato dal Prof. Luca Pani e dalla Prof.ssa Johanna Blom (Università di Modena e Reggio Emilia).

isbn 9791281716698

Via Jugoslavia, 14 - 41122 Modena
info@mucchieditore.it www.mucchieditore.it
facebook.com/mucchieditore X.com/mucchieditore instagram.com/mucchi_editore

Tipografia, progetto grafico e pubblicazione digitale STEM Mucchi (MO)

Pubblicato nel mese di novembre del 2025
Versione pdf open access al sito www.mucchieditore.it

A Simone

Indice

Introduzione

Questo volume nasce dalla riflessione critica sull'evoluzione dell'informatica medica in una società dell'informazione divenuta, a tutti gli effetti, società algoritmica con un conseguente ampliamento dell'indagine alla salute digitale nella sua interezza. La tecnica non svolge un mero ruolo strumentale nella pratica della cura e nella promozione del benessere: riconfigura spazi, tempi e priorità dell'agire clinico, organizzativo e quotidiano; rende il dato la trama ordinaria delle attività professionali e dell'autodeterminazione; trasferisce su architetture e modelli scelte che solo in apparenza rimangono neutre. In questo continuo mutamento, il diritto e l'etica non sono un freno; costituiscono la condizione per orientare la tecnica, e la ricerca scientifica, in una direzione che mai perda di vista il rispetto dei diritti alla vita, alla salute e all'autodeterminazione.

Il filo conduttore è la nozione di "vulnerabilità aumentata". L'aggettivo non rinvia a una misura, ma a un modo: lo strato informazionale si fonde stabilmente con la pratica della salute digitale fino a codeterminarne profili soggettivi e oggettivi. Ne derivano esposizioni nuove o amplificate (spaziali e temporali, inferenziali e istituzionali, asimmetriche) cui si sommano le dimensioni computazionale e interazionale: modelli che apprendono, si degradano o non si trasferiscono tra contesti; interfacce che orientano le scelte con regimi informativi e procedure di conferma. L'"aumento" discende dall'ibridazione diffusa nell'ambito della salute digitale: cartelle cliniche elettroniche e fascicoli, telemedicina e *mobile health*, robotica e impianti bionici, medicina personalizzata e di precisione, sistemi di raccomandazione e contenuti generati dall'IA. La vulnerabilità aumentata diviene un criterio di giudizio: indica quando l'apporto digitale riduce l'errore, rende contestabili gli esiti, distribuisce equamente benefici e oneri; e quando, invece, produce oggettificazione (il "doppio informazionale" che rischia di sopravanzare la persona "reale"), eterodirezione (standard che si irrigidiscono in gabbie) e asimmetrie (di informazione, potere e responsabilità).

La tesi del volume è che a questa condizione mista sia possibile guardare nella prospettiva di un'architettura di garanzie che accompagni l'intero ciclo di vita dei sistemi e dei servizi, rendendo intelligibili, motivabili, controllabili e contestabili i passaggi nei quali dati e modelli inci-

dono su salute e autodeterminazione. Si deve rifuggire, dunque, da una logica che riduce la conformità a mera sequenza di adempimenti sovente formali per giungere a una responsabilizzazione sostanziale, che si traduce in spiegabilità effettiva, tracciabilità dei ragionamenti rilevanti, possibilità concreta di deviazione motivata rispetto a protocolli e linee guida, strumenti di tutela efficaci e praticabili nel punto in cui la decisione incide. Al centro deve essere posta la persona-in-relazione, non il solo "interessato" o altra categoria risultante da profilazioni (normative o di mercato): la protezione dei dati è una garanzia accanto a qualità, sicurezza e correttezza metodologica, è un mezzo e non un fine.

Su questo sfondo, i capitoli che seguono ripercorrono criticamente il tragitto che conduce dall'informatica medica alla salute digitale e ne analizzano i profili giuridici ed etici. Nel secondo capitolo, la medicina algoritmica è letta come risorsa da orientare, non come sostituto del giudizio professionale: l'efficienza predittiva non colma l'obbligo di motivazione e la spiegabilità deve essere effettiva. La protezione dei dati recupera la sua funzione primaria di tutela della persona, senza scivolare nel riduzionismo "dataista" né nel paternalismo documentale; la correttezza della produzione e della comunicazione della conoscenza nell'ecosistema digitale è osservata là dove algoritmi di ranking e di raccomandazione selezionano ciò che emerge come "vero" e "rilevante", con ricadute sull'autodeterminazione informativa e sulla fiducia. La regolazione tecnico-scientifica (linee guida, protocolli, PDTA) non deve degenerare in derive difensive: sostiene il monitoraggio e il miglioramento quando consente deviazioni motivate, sottoposte a controllo. In questa ricostruzione, diviene cruciale la garanzia di cibersicurezza, che consente il corretto funzionamento dell'intero ecosistema digitale e protegge effettivamente persone e gruppi sociali. Nel terzo capitolo, sono discusse le applicazioni e le pratiche della salute digitale così da mettere alla prova questa impostazione in ambiti paradigmatici: sistemi informativi sanitari ed *Electronic Health Records*, telemedicina *e m-health*, robotica e tecnologie assistive, medicina personalizzata e di precisione. Il quarto capitolo è focalizzato sulla delicata tematica della restituzione o ritorno dei dati dei partecipanti alle sperimentazioni cliniche (e ai pazienti), sulla base del progetto FACILITATE, evidenziando come esso sia una pratica abilitante di governo effettivo in cui la persona torna a essere un'interlocutrice lungo tutto il processo:

accesso, portabilità, comunicazione di risultati individuali clinicamente validati e comprensibili, riusi tracciati e giustificati.

Le conclusioni articolano le tensioni che attraversano la salute digitale – tra potenza inferenziale e dovere di motivazione, tra apertura alla ricerca e protezione della persona, tra standardizzazione e personalizzazione proporzionata, tra sicurezza tecnica e sicurezza della cura – e le ricompongono in un'architettura di garanzie e responsabilità capace di tenere insieme conoscenza, giustizia e tutela della persona-in-relazione. L'asse proposto non è un bilanciamento contabile, ma il passaggio dalla conformità documentale alla responsabilizzazione sostanziale: spiegabilità diffusa e proporzionata al rischio; tracciabilità dei passaggi decisionali; possibilità effettiva di deviazione motivata da protocolli e linee guida con controllo e rimedi nel punto in cui gli esiti incidono; vigilanza successiva all'implementazione per intercettare scostamenti, pregiudizi e impatti differenziati. In questo quadro, la protezione dei dati è garanzia abilitante congiunta a qualità, sicurezza e correttezza metodologica; le responsabilità sono ibride e riconoscibili; il *nudging* è ammissibile solo se preserva scelte ragionevoli e contestabili, altrimenti degenera in paternalismo algoritmico. Una politica della fiducia si misura sulle ragioni pubblicamente rese e sull'equità degli esiti per persone e comunità. Così ancorati, dato e modello tornano a essere mezzi: il "doppio informazionale" è trattenuto nel suo statuto strumentale e la vulnerabilità aumentata, lungi dall'essere un esito inevitabile, diventa compito istituzionale condiviso.

Il presente volume nasce nell'ambito delle mie ricerche presso il CRID – Centro di Ricerca Interdipartimentale su Discriminazioni e vulnerabilità dell'Università di Modena e Reggio Emilia, diretto dal Prof. Thomas Casadei e da lui fondato con il Prof. Gianfrancesco Zanetti: ad entrambi vanno la mia stima e la mia riconoscenza, anche per avermi accolto nella Scuola modenese.

È altresì il frutto di un percorso di ricerca pluriennale e interdisciplinare maturato all'interno del progetto FACILITATE, coordinato dal Prof. Luca Pani e dalla Prof.ssa Johanna Maria Catharina Blom (Università di Modena e Reggio Emilia): doveroso è dunque il ringraziamento a entrambi, nonché al Prof. Fabio Tascedda e ai Professori che mi hanno guidato in un lungo percorso di ricerca che ha intrecciato profili giusfilosofici e bioetici (con la guida della Prof.ssa Teresa Serra, sin dal 2001);

informatico-medici (grazie al dialogo con il Prof. Peter Szolovits, a metà degli anni duemila); teorico-giuridici (mediante lo scambio con il Prof. Fulco Lanchester).

Rivolgo, infine, un ringraziamento speciale agli amici e colleghi Prof.ssa Anna Di Giandomenico e Prof. Giuseppe Contissa nonché al Dott. Casimiro Coniglione.

Last but not least, l'opera si inserisce in un percorso professionale e di ricerca che ha avuto sempre il sostegno della mia famiglia: mia moglie Daniela, i miei figli Alessandro e Simone, i miei genitori Giuseppina e Pasquale, e mio fratello Antonio.

L'Autore dichiara che i temi di ricerca approfonditi nel presente contributo sono stati oggetto di finanziamento nell'ambito della *Innovative Medicines Initiative Joint Undertaking* (IMI-JU), ai sensi dell'accordo di sovvenzione n. 101034366 (FACILITATE), i cui fondi risultano costituiti da un contributo finanziario dell'Unione europea (IMI) nonché da contributi in natura da parte delle imprese aderenti a EFPIA. L'Autore non ha percepito alcuna remunerazione economica a titolo personale per la stesura del presente volume. Tutte le affermazioni ivi espresse sono esclusivamente riconducibili all'Autore.

I. Dall'informatica medica alla salute digitale: concetti, percorsi, metodi

I.1. Introduzione

Il concetto di salute ha progressivamente superato la riduzione alla mera assenza di malattia ed è oggi inteso come condizione dinamica e relazionale di benessere fisico, mentale e sociale, sensibile alle differenze individuali e ai contesti di vita[1]. In questo processo evolutivo, dalla seconda metà del Novecento una nuova disciplina si è affiancata alla medicina "tradizionale": è l'informatica medica, che, a partire dalle sue prime formalizzazioni nella seconda metà del Novecento, non si è limitata allo studio di teorie, strumenti e applicazioni per lo svolgimento di (comunque fondamentali) funzioni documentali o amministrative, con la creazione dei primi sistemi informativi sanitari: è infatti giunta a dar vita a uno specifico filone di ricerca nell'ambito dell'Intelligenza Artificiale (IA), che ha portato – sin dai primi anni Settanta del secolo scorso – alla realizzazione dei primi sistemi di supporto alle decisioni. Questo percorso ha reso possibile l'avvento della *digital health*, che non è un settore applicativo isolato, ma un vero e proprio paradigma capace di integrare dati, modelli e decisioni in ecosistemi (in senso lato) relativi alla salute potenzialmente interoperabili.

Le questioni giuridiche, informatiche e sociali – oltre, ovviamente, a quelle connesse a ciascun ambito specialistico della salute – sono numerose e in continua evoluzione, come può intuirsi dalla ricostruzione qui effettuata nei suoi tratti essenziali. Esse non sono avulse da quelle che investono la società nel suo complesso, sia per il campo di applicazione ("salute") sia per gli strumenti informatici adoperati (sia "tradizionali" e "intelligenti" sia professionali e non, che interagiscono con dispositivi medici e/o con farmaci).

Per analizzare la predetta transizione e riflettere sul suo impatto sulla persona e sull'ordinamento giuridico appare necessario effettuare una ricostruzione storico-concettuale dell'ambito applicativo dell'informatica

[1] Basti pensare, in tal senso, al Preambolo alla costituzione dell'Organizzazione Mondiale della Sanità, adottata dalla Conferenza Internazionale sulla Sanità, 19-22 giugno 1946.

medica e delle questioni giuridiche ed etiche che sono sorte, discutendo criticamente l'evoluzione dalla salute "tradizionale" a quella "digitale" dal punto di vista teorico-applicativo: sistemi informativi sanitari ed *Electronic Health Records* (EHR), telemedicina, *mobile health* e dispositivi indossabili, robotica e potenziamento umano, medicina personalizzata e di precisione.

Il solo studio dei profili applicativi, però, non consente di delineare, per quanto possibile, un quadro generale e di comprendere il ruolo e le trasformazioni della sanità digitale in una società che è sia "dell'informazione" sia "algoritmica"[2]: dati, di qualsiasi tipologia e in qualsiasi formato, vengono elaborati in modo sempre più automatizzato e "intelligente", con organizzazione dei processi decisionali, e delega totale o parziale del loro svolgimento, a software che – nell'esecuzione di algoritmi più o meno complessi e interconnessi – elaborano le informazioni, giungendo anche ad apprendere dalle stesse grazie agli algoritmi di *machine learning* (apprendimento automatico) che vengono implementati.

Di qui la preliminare discussione circa i profili generali e trasversali che caratterizzano maggiormente la salute digitale nella prospettiva della vulnerabilità. Tali profili possono essere individuati, ai fini del presente volume: (i) nell'IA e nella medicina algoritmica (per il suo impatto sulla conoscenza e sulla sua applicazione da parte degli agenti umani e artificiali); (ii) nella privacy e nella protezione dei dati personali (che contribuiscono a tutelare la libertà e la dignità della persona nonché ad arginare impostazioni riduzionistiche); (iii) nella conoscenza e nella comunicazione delle informazioni relative alla salute e nella fornitura dei servizi online (che si intersecano con i primi due profili e che impattano sull'autodeterminazione); (iv) stru-

[2] Sulla Società algoritmica cfr., fra gli altri, J. Balkin, *The Three Laws of Robotics in the Age of Big Data*, in «Ohio State Law Journal», Vol. 78, 5, 2017, pp. 1217-1241; F. Pasquale, *Towards a Fourth Law of Robotics: Preserving Attribution, Responsability and Explanaibility in an Algorithmic Society*, in «Ohio State Law Journal», Vol. 78, 2017, pp. 1243-1255; G. Gorgoni, *Stay Human. The quest for Responsability in the Algorithmic Sociey*, in «Journal of Ethics and Legal Technologies», 2, 2020, pp. 31-47; W. Barfield (ed.), *The Cambridge Handbook of the Law of Algorithmics*, Cambridge, 2020; M. Schuilenburg, R. Peeters (ed.), *The Algorithmic Society. Technology, Power and Knowledge*, London, 2021; H.W. Micklitz, O. Pollicino, A. Simoncini, G. Sartor, G. De Gregorio (eds.), *Constitutional Challenges in the Algorithmic Society*, Cambridge, 2021; G. Fioriglio, *La Società algoritmica fra opacità e spiegabilità: profili informatico-giuridici,* in «Ars interpretandi», 1, 2021, pp. 53-67; G. Todaro, *L'evoluzione delle fonti del diritto nella «società algoritmica»,* in «Cassazione penale», 64, 4, 2024, pp. 2011-2036; P. Sansò, *Opacità algoritmica e sovranità epistemica nel contesto del capitalismo delle piattaforme*, in «I-Lex», 2, 2025, pp. 36-49.

menti di regolazione tecnico-scientifica della cura, come protocolli, linee guida e PDTA (percorsi diagnostico-terapeutici-assistenziali)(che orientano la governance e costituiscono strumenti di valutazione della diligenza); (v) dataismo e Big Data (che impattano sulla costruzione dell'identità e dell'ecosistema digitale, con rischi di riduzionismo etico e giuridico).

Il quadro è, dunque, particolarmente articolato, ma è possibile individuare un tratto comune sia nell'ambito della sanità digitale sia fra questa e la società nel suo complesso: la datificazione[3]. Essa trasforma corpo e comportamento in flussi informativi potenzialmente continui. Le conseguenze sono assai numerose e significative, nel bene e nel male: aumentate possibilità di prevenzione, diagnosi precoce e personalizzazione della cura; nuovi ambiti di governo tecnocratico nella regolazione tecnico-scientifica; nuove o potenziate asimmetrie informazionali; la riduzione di persone e gruppi sociali a dati.

Sullo sfondo si colloca la questione che costituisce il principale oggetto di studio del presente volume: la "vulnerabilità aumentata". Per essa può intendersi la condizione relazionale e situata in cui, nella società dell'informazione e algoritmica e nel più ampio ecosistema della salute digitale, artefatti, modelli e infrastrutture della cura producono o intensificano figure di vulnerabilità situate riferibili a soggetti o sistemi, determinando eccedenze di esposizione al pregiudizio, compressioni ingiustificate dell'autodeterminazione o deficit di prevenzione, governo e rimedi. L'aggettivo "aumentata" non va inteso in senso quantitativo: rinvia al manifestarsi nel caso concreto di segni convergenti che un giudizio ragionevole, intersoggettivamente controllabile e aperto alla confutazione riconosce come effetti di pratiche di visibilità e di ascolto e di assetti

[3] Sulla datificazione cfr., fra gli altri: T. Numerico, *Intelligenza artificiale e algoritmi: datificazione, politica, epistemologia*, in «Consecutio Rerum», 6, 2019, pp. 241-271; M. Martoni, *Datificazione dei nativi digitali. Una prima ricognizione e alcune brevi note sull'educazione alla cittadinanza digitale*, in «Federalismi.it», 1, 2020, pp. 119-136; U. Pagallo, *La grande trasformazione. Datificazione della società, tutela dell'ambiente e rischi e opportunità dell'innovazione tecnologica*, in M. Durante, U. Pagallo (a cura di), *La politica dei dati. Il governo delle nuove tecnologie tra diritto, economia e società*, Mimesis, Milano-Udine, 2022, pp. 123-140; M. Ruckenstein, N. Dow Schüll, *Tha Datafication of Health*, in «Annual Review of Anthropology», 46, 2017, pp. 261-278; D. Ruggiu, *Spazio economico, tecnologie digitali e decostruzione dello spazio normativo del soggetto*, in «Ars interpretandi», 2, 2024, pp. 61-78; C. Sarra, *Dignità umana nell'era dell'intelligenza artificiale e della datificazione*, Kront, Roma, 2025.

socio-tecnici e istituzionali incompatibili con una cura giusta. La ricorrenza di tale condizione attiva doveri di protezione rafforzata, diligenza qualificata, precauzione, informazione effettiva e comprensibile, supervisione umana effettiva e un onere di motivazione rafforzata e di rendicontazione in capo a progettisti, fornitori e utilizzatori delle tecnologie.

Per poter proficuamente discutere quanto qui succintamente esposto, appare necessario: (i) ricostruire criticamente l'evoluzione dell'informatica medica, definendola e delineandone l'ambito applicativo; (ii) individuarne le principali questioni giuridiche ed etiche; (iii) comprendere come l'informatica giuridica possa contribuire al suo ulteriore sviluppo; (iv) presentare la nozione di vulnerabilità aumentata.

I.2. **Informatica medica: ambito applicativo e definizioni**

Com'è noto, l'informatica ha rivoluzionato la società nel volgere di pochi decenni con una rapidità e una pervasività inimmaginabili. I primi computer digitali programmabili risalgono agli anni Quaranta dello scorso secolo e divengono poi di massa negli anni Ottanta; la creazione del World Wide Web (da non confondersi con quella di ARPANET, sul finire degli anni Sessanta) è di fine anni Ottanta – inizio anni Novanta, mentre la diffusione degli smartphone accelera in modo inarrestabile a partire dagli anni Duemila. In un periodo storicamente breve si è dunque realizzata un'interconnessione pressoché permanente di dispositivi non solo informatici (e dei loro utilizzatori): smartphone, computer, televisori, automobili, elettrodomestici, ecc.[4].

Nessun ambito della conoscenza e dell'esperienza è stato "risparmiato" dalla rivoluzione digitale, seppur con tempi, modalità e cicliche fasi di entusiasmo e disillusione. Emblematica, sotto questo profilo, è l'IA: dagli slanci degli anni Sessanta (giungendo a teorizzare "medici", "avvocati", "giudici" elettronici) alle critiche e ridimensionamenti degli anni Ottanta, fino alle odierne applicazioni diffuse e alla retorica del "prodotto intelligente". In non pochi casi, peraltro, l'utente interagisce con terminali – talora molto sofisticati – che fungono da interfaccia verso un'IA distribu-

[4] Per una ricostruzione di tale evoluzione cfr. M.F. Collen, C.A. Kulikowski, *The Development of Digital Computers*, in M.F. Collen, M.J. Ball (eds.), *The History of Medical Informatics in the United States*, Springer, New York, 2015, pp. 3-73.

ita, connessa a servizi di *cloud computing* necessari per fruire integralmente delle funzionalità[5].

L'ambito sanitario è paradigmatico della differente velocità di adozione: qui la digitalizzazione procede più lentamente rispetto ad altri settori (per esempio la comunicazione), in ragione della particolare delicatezza degli interessi coinvolti. In gioco vi sono diritti fondamentali come vita e salute – presupposto di altri diritti ed emblematici della vulnerabilità umana[6] – nonché interessi economici significativi che coinvolgono una pluralità di attori. Ne discende, tra l'altro, l'esigenza di procedure rigorose di valutazione per i dispositivi medici, ivi incluso il software (*software as a medical device* e software *embedded*)[7].

Nonostante tali cautele, la medicina è sempre più informatizzata e le prospettive che si delineano sono non soltanto promettenti ma, talora, prossime alla "fantascienza" soprattutto nelle prime fasi della loro introduzione (si pensi alla medicina di precisione[8]). Ciò è dovuto tanto al progresso delle tecnologie digitali quanto, soprattutto, agli studi di informatica medica avviati sul finire degli anni Quaranta[9], con l'impiego dei calcolatori in ambito sanitario e, parallelamente, con la riflessione sistematica sulle applicazioni dell'informatica alla medicina. Non a caso, già negli anni Sessanta la letteratura francese impiega i termini *informatique de médecine* e *informatique médicale*; dagli anni Settanta negli Stati Uniti si diffonde *medical informatics*[10].

Bisogna tuttavia chiedersi cosa intendere per "informatica medica". Ancorché le definizioni siano numerose, è utile richiamarne alcune per estrarne tratti comuni, utili a impostare lo studio dei profili etici e giuridici.

In tal senso, è doveroso partire da un pioniere della disciplina, Morris F. Collen, il quale l'ha definita nel 1977 come l'applicazione dei computer e delle tecnologie dell'informazione e della comunicazione a tutti i settori della medicina (pratica medica, formazione, ricerca[11]): definizione

[5] Sull'IA si rinvia al capitolo 2, paragrafo 2.

[6] Sulla vulnerabilità v. *infra*, par. 6.

[7] Sui dispositivi medici v. *infra*, cap. 3.

[8] Cfr. cap. 3, par. 5.

[9] Cfr., per tutti e per una amplissima bibliografia, M.F. Collen, E.H. Shortliffe, *The Creation of a New Discipline*, in M.F. Collen, M.J. Ball (eds.), cit., pp. 75-120.

[10] *Ibidem.*

[11] In tal senso M.F. Collen, *Preliminary announcement for the third world conference on medical informatics*, Medinfo 80, 1977.

ampia, centrata sul versante tecnico-informatico e, com'è fisiologico in una simile fase, meno esplicita sui profili etico-giuridici.

Lo stesso può sostanzialmente dirsi per una successiva proposta formulata da Robert A. Greenes ed Elliot R. Siegel all'esito di uno studio collaborativo fra la National Library of Medicine (NLM) statunitense e l'American College of Medical Informatics (ACMI) finalizzato all'analisi della letteratura scientifica dell'epoca. Greenes e Siegel hanno rilevato come l'Informatica medica, che parte dalle scienze di base (incluse linguistica, matematica, ingegneria elettronica, psicologia), fosse generalmente vista come composta da diverse discipline, fra cui le più importanti sono l'informatica, la scienza delle decisioni, la statistica, la biblioteconomia, l'epidemiologia e, più in generale, la scienza medica. Essa era già allora adoperata in ambito clinico, amministrativo, infermieristico, educativo, nel campo della medicina preventiva e, più in generale, nel sistema sanitario pubblico, per fornire supporto alle decisioni, gestire i database e la conoscenza, trattare delle immagini, effettuare simulazioni, elaborare il linguaggio naturale[12]. Di qui la loro proposta di definizione

Sulla base di tali considerazioni, gli studiosi appena menzionati hanno proposto la seguente definizione di Informatica medica: «il campo che si occupa dei compiti cognitivi nonché del trattamento e della gestione delle informazioni in medicina, assistenza sanitaria e ricerca biomedica, e dell'applicazione a tali compiti della scienza e tecnologia dell'informazione»[13]. Non vi è dunque menzione dei profili etico-giuridici, se non in via implicita per quanto riguarda gli aspetti connessi agli ambiti sopra riportati (con particolare riferimento all'organizzazione del sistema sanitario); non era questo l'oggetto del loro studio, ma anche in questo caso può osservarsi come la letteratura scientifica non si soffermi, se non in pochi casi[14], sulle problematiche etiche e giuridiche che scaturiscono dall'avvento di questa nuova disciplina.

[12] R.A. Greenes, E.R. Siegel, *Characterization of an emerging field: approaches to defining the literature and disciplinary boundaries of medical informatics*, in *Proceedings of the Annual Symposium on Computer Applications in Medical Care*, 1987, p. 413.

[13] Ivi, p. 414.

[14] Cfr. F.T. de Dombal, *Ethical considerations concerning computers in medicine in the 1980s*, in «Journal of Medical Ethics», 13, 4, 1987, pp. 179-184; R.A. Miller, K.F. Schaffner, A. Meisel, *Ethical and Legal Issues Related to the Use of Computer Programs in Clinical Medicine*, in «Annals of Internal Medicine», 102, 1985, pp. 529-536; P. Szolo-

Nel medesimo periodo, tuttavia, può osservarsi un progressivo ampliamento degli orizzonti, dal momento che si faceva sempre più riferimento non tanto e non solo al dispositivo (il computer) e a ciò che il dispositivo tratta (l'informazione), ma a tutte le sue applicazioni alla scienza medica, alla ricerca, all'insegnamento e alla pratica; inoltre, se da un lato si avverte l'esigenza di delinearne più precisamente l'ambito (ad es., infermieristico – *Nursing Informatics*, clinico – *Clinical Informatics*, odontoiatrico – *Dental Informatics*, ecc.)[15], dall'altro alcuni studiosi si interrogano più compiutamente sui profili etici e giuridici[16], per quanto il fulcro della disciplina venga pur sempre rinvenuto nelle c.d. "scienze dure".

Nel senso appena esposto basti richiamare la definizione di Shortliffe e Blois, secondo cui l'Informatica medica è il settore scientifico che si occupa dell'informazione biomedica, dei dati e della loro conservazione, del loro recupero e utilizzo ottimale per la risoluzione di problemi e i processi decisionali. Tocca, dunque, tutti i campi di base e applicativi della scienza biomedica; è strettamente connessa alle moderne tecnologie dell'informazione, in particolare nelle aree dell'informatica e della comunicazione[17].

In questa definizione si può notare l'accento sul profilo biomedico: non a caso, si è sempre più spesso fatto ricorso a "informatica biomedica" più che a "informatica medica". La stessa "American Medical Informatics Association" (AMIA) ha preso posizione sul punto nel 2012, affermando di adottare una prospettiva più limitata del termine "informatica medica" (che continua però a essere adoperato nella denominazione dell'associazione medesima) e, nello specifico, di adoperarlo per riferirsi a quelle componenti di ricerca e pratica nella informatica clinica che si focalizzano sulle patologie e in cui i medici hanno un ruolo predominante.

vits, S.G. Pauker, *Computers and clinical decision making: whether, how much, and for whom?*, in «Proceedings of the IEEE», 67, 1979, pp. 1224-1226.

[15] M.F. Collen, E.H. Shortliffe, op. cit., p. 81. Sul punto v. *infra*.

[16] Su questi profili cfr. K.W. Goodman (Ed.), *Etica, informatica e medicina. L'informatica e la trasformazione dell'assistenza sanitaria* (1998), tr. it., Il Pensiero Scientifico, Roma, 1999, nonché J.D. Bronzino, V.H. Smith, M.L. Wade, *Medical Technology and Society: An Interdisciplinary Perspective*, MIT Press, Cambridge-London, 1990, e T. Forester, P. Morrison, *Computer Ethics. Cautionary Tales and Ethical Dilemmas in Computing*, MIT Press, Cambridge-London, 1994.

[17] E.H. Shortliffe, M.S. Blois, *The computer meets medicine: Emergence of a discipline*, in E.H. Shortliffe, J.J. Cimino (eds.), *Biomedical Informatics. Computer Applications in Health Care and Biomedicine*, Springer, New York, 4th ed., 2014, p. 24.

Pertanto, l'AMIA, in un proprio importante *white paper*, ha dichiarato che avrebbe adoperato il termine "informatica medica" quale nozione parallela ad altri sottosettori dell'informatica clinica (come l'Informatica infermieristica o quella Odontoiatrica). AMIA, dunque, si riferisce alla Informatica biomedica (*Biomedical Informatics*, BMI) quale ambito interdisciplinare che studia gli usi effettivi di informazioni biomediche e conoscenza per la ricerca scientifica, la risoluzione di problemi e i processi decisionali, guidati dagli sforzi per migliorare la salute umana[18].

La dottrina statunitense, così, ha progressivamente "ridimensionato" l'ambito dell'Informatica medica, la cui evoluzione l'ha portata a divenire una branca dell'Informatica biomedica[19], mentre in ambito europeo può tuttora notarsi un diffuso utilizzo di "Informatica medica" anche in seno alla "European Federation for Medical Informatics" (EFMI)[20]. Del resto, come si è visto, il termine "Informatica medica" è stato utilizzato originariamente proprio in Europa.

Indipendentemente dalle oscillazioni terminologiche, il nucleo concettuale rimane l'informazione (per lo più relativa al paziente), in tutta la sua ampiezza: da quella amministrativa alle informazioni su condizioni, trattamenti, esiti. Il trattamento informatico dell'informazione produce benefici evidenti – efficienza organizzativa, riusabilità e integrazione dei dati – ma porta con sé nuovi doveri di diligenza (qualità, sicurezza, tracciabilità) e responsabilità diffuse lungo la filiera tecnica e sociale.

Non è dunque un caso che già nel 2006 il Comitato Nazionale per la Bioetica (CNB) abbia sottolineato che l'informatica medica riguarda tutti: cittadini, pazienti, amministratori sanitari, personale sanitario, ricercatori biomedici, docenti e discenti dei corsi di formazione. Gli obiettivi principali dell'informatica medica consistono nella partecipazione a programmi di "tutela della salute e di cura della malattia", "gestione dei sistemi sanitari", "facilitazione della ricerca biomedica"; secondo il CNB, sotto il profilo etico, quest'area culturale e operativa deve essere caratterizzata dall'uso eticamente corretto dell'informazione e ripropone la definizione finalizzata a tale ultimo aspetto fornita dal Gruppo di lavoro informatico dell'Uni-

[18] C.A. Kulikowski *et al.*, *AMIA Board White Paper: definition of biomedical informatics and specification of core competencies for graduate education in the discipline*, in «Journal of American Medical Informatics Association», 19, 2012, pp. 932-933.

[19] In questo senso altresì M.F. Collen, R.A. Greenes, *Medical Informatics: Past and Future*, in M.F. Collen, M.J. Ball (eds.), cit., p. 747.

[20] Il sito web della EFMI è raggiungibile all'URL <https://www.efmi.org>.

versità di Manchester: «l'informatica medica comporta un uso responsabile dell'informazione a sostegno della cura della salute»[21]. Secondo il CNB, tale definizione – «al di là delle ricorrenti discussioni sull'autonomia epistemologica e disciplinare dell'informatica e di quella medica in particolare – interessa il medico come ogni cittadino ed ogni paziente, poiché sottolinea un uso responsabile e finalizzato dell'informatica, come insieme di metodologie, di algoritmi e di strumenti che trattano dati e informazioni a sostegno di quei particolari modelli della relazionalità fra gli uomini costituiti dalla salute, dalla malattia e dall'organizzazione sanitaria»[22].

Negli ultimi due decenni, infine, il lessico politico-istituzionale ha ampliato l'ambito della "tradizionale" informatica medica: da *e-health* e *m-health* alla più comprensiva *digital health*. Prima di approfondire questo profilo, bisogna premettere che tale evoluzione terminologica e semantica non dismette la centralità dell'informazione: al contrario, la colloca in ecosistemi digitali interoperabili, nei quali l'uso primario e secondario dei dati[23] diventa fattore abilitante di prevenzione, cura e ricerca. Del resto, già negli anni Settanta si era notato che il termine "health" avesse il pregio di porre l'attenzione sulla tutela della salute e sulla protezione dalle malattie più che sulla cura delle patologie[24], anche se tale visione è contestata da chi ritiene che in tal caso si andrebbero ad escluderne le applicazioni alla biologia[25].

Si è dunque diffuso progressivamente, da parte di legislatori e *policymakers*, l'uso del termine "e-health" per contraddistinguere il fenomeno consistente nella creazione e nell'applicazione delle moderne tecnologie informatiche al sistema sanitario complessivamente inteso[26]. Anche in

[21] Comitato Nazionale per la Bioetica, *Etica, salute e nuove tecnologie dell'informazione*, Roma, 2006, pp. 10-11.

[22] Ivi, p. 11.

[23] Su tali profili v. *infra*, cap. 4.

[24] L. Breslow, *Health care versus medical care: implications for data handling*, in M. Laudet (ed.), *Proceedings of an international symposium*, Taylor and Francis, London, 1977, p. 69-75, riportato da M.F. Collen, E.H. Shortliffe, *The Creation of a New* Discipline, cit., p. 86.

[25] E.H. Shortliffe, M.S. Blois, *The computer meets medicine: Emergence of a discipline*, op. cit., p. 23.

[26] D. Silber, *The Case for eHealth*, EIPA, Maastricht, 2003, p. 3. Ad esempio, già all'inizio degli anni Duemila l'allora Commissione delle Comunità europee aveva stabilito che l'*e-health* costituisse una priorità in ambito comunitario, per quanto ostacoli di natura tecnica, organizzativa e giuridica dovessero essere superati per poterne sfruttare i vantaggi. Cfr., in particolare, Commissione delle Comunità Europee, *eEurope 2005: una società dell'informazione*

questo caso, l'informazione ne è il fulcro, in quanto il suo presupposto è, ovviamente, la disponibilità dei dati sanitari in forma digitale.

Premessa la definizione di e-health quale utilizzo delle tecnologie dell'informazione e della comunicazione per supportare l'ambito sanitario e quelli connessi, nonché di "mobile health" (*m-health*)[27] come utilizzo delle tecnologie mobili wireless per il medesimo ambito, l'Organizzazione Mondiale della Sanità così definisce la "Digital health": «*a broad umbrella term encompassing eHealth (which includes mHealth), as well as emerging areas, such as the use of advanced computing sciences in 'big data', genomics and artificial intelligence*»[28].

In sintesi: l'informatica medica è la scienza interdisciplinare che studia e realizza l'applicazione dell'informatica ai molteplici ambiti della salute, avendo per oggetto primario l'informazione biomedica nelle sue fasi di raccolta, trasformazione e uso. L'informatica è il fulcro, ma l'interdisciplinarità è costitutiva: medicina e infermieristica, biologia e statistica, scienza giuridica e bioetica – quest'ultime trasversali – plasmano architetture, processi e pratiche (si pensi, ad esempio, all'impatto della disciplina europea in materia di protezione dei dati personali sulla progettazione dei sistemi informativi sanitari).

Le applicazioni comprendono, a titolo esemplificativo, sistemi informativi sanitari, cartelle cliniche elettroniche, fascicolo sanitario elettronico, biologia computazionale, bioinformatica, diagnostica per immagini, telemedicina, m-health, robotica, medicina di precisione, protocolli di interoperabilità, sorveglianza epidemiologica e sistemi di supporto alle decisioni cliniche. L'elenco potrebbe proseguire; è tuttavia sufficiente a mostrare l'impatto sistemico dell'informatica medica e la verosimile intensificazione di interventi regolatori orientati alle applicazioni e ai casi d'uso più che alla disciplina in quanto tale.

Una regolazione adeguata resta un obiettivo non semplice: occorre calibrare i regimi di responsabilità per prodotti e servizi della sanità digi-

per tutti, COM (2002) 263; Idem, *Sanità elettronica – migliorare l'assistenza sanitaria dei cittadini europei: piano d'azione per uno spazio europeo della sanità elettronica*, COM (2004) 356.

[27] Sulla *m-health* v. *infra*, cap. 3, par. 3.

[28] World Health Organization, *Recommendations on digital interventions for health system strengthening*, Geneva, 2019, p. ix. La definizione citata nel testo era stata già adoperata nell'ambito della stessa OMS (cfr., ad es., World Health Organization, *mHealth: use of appropriate digital technologies for public health: report by the Director-general*, n. A71/20, Geneva, 2018).

tale, tenendo presenti le specificità del settore; e, sul piano etico-giuridico, garantire che l'intero *démos* – senza discriminazioni – possa effettivamente fruire dei servizi digitali, evitando nuove forme di divario digitale in tale ambito, con ricadute diseguali su diritti come la salute e l'accesso alle cure. Già oggi, l'implementazione di sistemi informativi interconnessi consente una più rapida disponibilità dei dati clinici con evidenti benefici – si pensi ai casi di urgenza[29] – purché sia rispettata la stringente normativa sulla protezione dei dati e siano adottate adeguate misure di sicurezza.

Ad ogni buon conto, le tecnologie attuali consentono di andare oltre la gestione efficiente dei flussi informativi: abilitano sistemi di supporto decisionale e, in alcuni casi, sistemi che eseguono compiti complessi con gradi variabili di autonomia. Software sempre più sofisticati sono integrati in dispositivi medici, abilitandone funzioni critiche. Ne consegue che chiunque – pazienti, operatori e operatrici sanitari, strutture sanitarie, aziende – interagisce, talvolta inconsapevolmente, con soluzioni anche estremamente evolute e "intelligenti".

Le questioni giuridiche che ne derivano sono di ordine diverso e richiedono un approccio informatico-giuridico capace di orientare lo sviluppo in conformità a principi e regole non "bloccanti", ma volti a una innovazione sostenibile e responsabile.

I.3. Salute digitale e informatica medica: questioni giuridiche

Lo studio dei profili giuridici dell'informatica medica e della salute digitale non si esaurisce in una mera mappatura delle ricadute applicative o di diritto positivo. Difatti, a duplice livello teorico e pratico, tali tecnologie intersecano, e contribuiscono a plasmare, categorie e principi degli ordinamenti: persona e dignità, salute e cura, autodeterminazione e consenso, responsabilizzazione (*accountability*) e responsabilità, eguaglianza e non-discriminazione, rischio e sicurezza, automazione e disumanizzazione. Ne discende l'esigenza di connettere stabilmente architetture dei dati e governance, standard e interoperabilità, cibersicurezza e gestione del rischio, organizzazione dei processi clinico-assistenziali e sistemi di responsabilità e rimedi giuridici. Sullo sfondo, il "dato" funge insieme da filo condutto-

[29] Ad esempio, in seguito ad eventi traumatici che impongono interventi di pronto soccorso nel cui ambito può essere vitale conoscere eventuali allergie a determinati farmaci.

re e terreno di contesa: tra datificazione, quale elemento della cura digitale, e riduzionismo "dataista", che rischia di ridurre la persona all'«interessato-dato»[30]. In questa cornice, il concetto di vulnerabilità aumentata offre il criterio di giudizio per distinguere gli impieghi che accrescono dignità e autodeterminazione da quelli che, al contrario, generano una maggiore esposizione al danno o compressioni ingiustificate della libertà personale.

La salute digitale non aggiunge semplicemente strumenti alla medicina: riconfigura i presupposti giuridici della cura (intesa non solo come cura delle malattie, ma anche come "cura" di sé stessi e/o degli altri). Mutano l'oggetto delle regole e le forme con cui gli ordinamenti articolano la protezione della persona in tale ecosistema informazionale della cura. In questo quadro, le coppie concettuali richiamate (persona e dignità; salute e cura; autodeterminazione e consenso; responsabilizzazione e responsabilità; eguaglianza e non-discriminazione; rischio e sicurezza; automazione e disumanizzazione) costituiscono l'orizzonte categoriale e valoriale entro cui le scelte architetturali, organizzative e decisionali devono essere compiute. Senza questa "progettazione giuridica delle tutele", la datificazione scivola verso un riduzionismo che accresce la vulnerabilità: espone maggiormente al danno, impoverisce l'autonomia effettiva, rende opachi responsabilità e rimedi.

Pertanto, l'indagine sui profili applicativi e sulle relative questioni giuridiche, deve utilmente essere preceduta da alcune riflessioni di carattere più teorico-generale in ordine alle predette coppie concettuali, partendo da persona e dignità: la digitalizzazione della cura "converte", infatti, il paziente da analogico a digitale, ossia in dati (cartelle elettroniche, segnali di vari sensori, predizioni, classificazioni, ecc.), con il rischio di far coincidere la soggettività con il suo profilo "computabile": ma la persona è più della somma dei suoi dati e la dignità opera come principio di limitazione del potere tecnico-giuridico. Si è appena scritto "tecnico-giuridico", e non a caso: il profilo tecnico è connaturato alle operazioni di trattamento dei dati, mentre quello giuridico detta le condizioni di liceità dei mezzi e dei fini (basti pensare alla raccolta di dati per il monitoraggio della spesa farmaceutica), in una dimensione complessa idonea a incidere concretamente su salute e cura, le quali dipendono sempre più – sin dalla loro programmazione per giungere alla pratica clinica e alla ricerca – dalla valutazione di dati.

[30] V. *infra*, cap. 2, parr. 4 e 7.

La tecnica informatica pervade, del resto, la medicina del XXI secolo in tutti i suoi ambiti (amministrativo, clinico, di ricerca, di formazione, di sanità pubblica e di prevenzione) e ciò a tutti i livelli, dai singoli professionisti e strutture sanitarie agli enti locali e allo Stato nonché, per taluni profili, anche a livello sovranazionale (a titolo esemplificativo, per il monitoraggio della spesa sanitaria, l'analisi del livello delle prestazioni, la sorveglianza epidemiologica, ecc.).

La salute e la cura, però, non sono facilmente riducibili a numeri (come la somma delle prestazioni, la tempistica di erogazione, ecc.), ancorché fondamentali. La cura, infatti, non è mera computazione, ma può intendersi come pratica deliberativa che integra, in particolare, informazione, giudizio clinico, autodeterminazione, responsabilizzazione e responsabilità, portando alla tutela della salute in modo condiviso e non imposto. I confini sono sovente sfumati e gli equilibri difficili da raggiungere e sempre potenzialmente precari, ma raggiungibili: basti pensare alla corretta distinzione fra uso primario per la cura e usi secondari per ricerca, governo del sistema o valutazione delle tecnologie; lungi dall'essere un tecnicismo, è un presidio che impedisce all'ottimizzazione di erodere la logica della cura, purché gli usi secondari siano effettivamente ammessi bilanciando tutti gli interessi in gioco[31].

Proprio l'autodeterminazione è, del resto, cruciale, ma non si esaurisce nella "retorica del consenso": non consiste nel prestarlo, più o meno liberamente (in ragione dell'asimmetria informativa, dello stato di vulnerabilità, ecc.), bensì nel decidere liberamente riguardo alla propria vita, al proprio corpo e ai propri dati, senza imposizioni esterne; un diritto di capacità e di libertà di scelta consapevole, nel rispetto della dignità umana e della libertà individuale. Nell'ambito della salute, è ben noto che non si debba confondere fra il consenso informato e quello al trattamento dei dati personali; il primo riguarda la relazione terapeutica, il secondo la liceità del trattamento medesimo (e non è sempre la più idonea in caso di prestazione sanitaria necessaria o di svolgimento di attività di ricerca che non mettono a rischio i diritti e le libertà degli interessati). L'autodeterminazione, nell'ambito della salute digitale, è però influenzata da altri fattori, a partire dalla comunicazione in tale settore (non solo in relazione alla cura delle patologie, ma anche per ciò che concerne lo stile di vita)[32].

[31] V. *infra*, cap. 4, par. 2.
[32] V. *infra*, cap. 2, par. 5.

Emerge, dunque, una nuova dimensione della responsabilizzazione (*accountability*) e della responsabilità: a quella "tradizionale" dei soggetti che operano professionalmente (basti pensare al titolare del trattamento di dati personali) si aggiunge, infatti, quella dei pazienti e comunque di tutti i destinatari di prodotti e servizi nell'ambito della salute (intesa in senso lato), chiamati a essere attori e attrici responsabili nella gestione dei propri dati e della propria salute digitale, in un ambito che ne vede una molteplicità: Stati e amministrazioni centrali e locali, strutture sanitarie, operatori e operatrici sanitari, aziende farmaceutiche, produttori di dispositivi medici o comunque rilevanti per la salute, fornitori di servizi connessi (dall'*hosting* all'elaborazione dei dati), farmacie e parafarmacie, centri fitness, e così via. Del resto, se la salute non è solo l'assenza di patologie, bensì una condizione dinamica e complessiva di benessere fisico, psichico e sociale, allora entra in gioco, per l'appunto, un numero rilevante di soggetti, mentre il soggetto che entra in contatto con essi (paziente, assistito, interessato, cliente, consumatore) progressivamente si responsabilizza, o dovrebbe farlo, nella prospettiva dell'autodeterminazione.

In capo ai soggetti sopra citati si configurano responsabilità di diversa entità e rilevanza giuridica che toccano questioni di particolare rilevanza ai fini del presente volume: l'eguaglianza e la non discriminazione, il rischio e la sicurezza, l'automazione e la disumanizzazione[33].

Più specificamente, l'eguaglianza e la non discriminazione toccano i profili dell'accesso alle cure, del loro livello della loro disponibilità, il tutto sulla base della gestione della spesa sanitaria. Ogni scelta è idonea a incidere, anche in modo determinante, sul diritto alla vita e alla salute dei consociati. Sono decisioni anche politiche e amministrative che hanno un impatto su come l'ordinamento giuridico li tutela concretamente: dalla chiusura di strutture sanitarie alla scelta di non rendere mutuabili determinati farmaci; ogni scelta conta e non è neutrale. In tale quadro, non è solo la medicina "tradizionale" a essere algoritmica: lo è anche il monitoraggio e il controllo della spesa sanitaria e farmaceutica, che richiede l'effettuazione di complesse elaborazioni statistiche la cui esattez-

[33] Si consideri che l'eventuale eliminazione del rapporto umano avrebbe una conseguenza sovente ignorata: «la cura dell'altro, il fisicamente e manualmente prendersi cura, può comportare un benessere riflesso sull'operatore. E chi conosce questo benessere, quando lo percepisce, ne riconosce il tocco» (G. Zanetti, *Filosofia della vulnerabilità. Percezione, discriminazione, diritto*, Carocci, Roma, 2019, p. 139).

za è fondamentale per contenere la spesa pubblica e meglio gestire i relativi fondi per aumentare il livello di tutela del diritto alla vita e alla salute. Anche in questo caso, un equilibrio assai difficile da raggiungere.

Vi è di più. Devono essere valutati rischi e sicurezza non solo per ciò che concerne i profili medici, ma anche in relazione ai sistemi informatici. Di qui la sempre crescente attenzione verso la cibersicurezza a diversi livelli, come di seguito esposto (in particolare, in riferimento alla privacy e alla protezione dei dati personali, all'IA, ai sistemi informativi sanitari, alla telemedicina e alla *m-health*).

Il quadro qui tratteggiato nei suoi elementi essenziali mostra già inequivocabilmente il ruolo centrale dell'automazione, cui conseguono – intuitivamente – dubbi in ordine alla disumanizzazione della salute digitale, fra protocolli e app, fra IA e monitoraggio della spesa sanitaria, fra limitazioni alla ricerca per le restrizioni agli usi secondari e libera disponibilità di prodotti insicuri (o comunque rivolti al pubblico dei consumatori) che trattano comunque dati relativi alla salute. Vi è il rischio, concreto, che l'essere umano sia sempre più una somma dei propri dati anziché una persona: i principi fondamentali di tutela della libertà e della dignità umana non vengono cancellati, ma devono essere continuamente riaffermati affinché la salute digitale metta il dato, e non la persona, al centro.

Alle vulnerabilità "tradizionali" (e alcune sono connaturate all'essere paziente, assistito, interessato, cliente, consumatore), difatti, rischiano di sommarsi quelle "digitali" – a maggior ragione considerando che molte posizioni giuridiche soggettive appaiono configurarsi come diritti sociali. A tal proposito, è bene ricordare che le problematiche relative ai diritti sociali toccano tre aspetti principali: la relazione fra diritti di libertà (intesi come diritti fondamentali) e i diritti sociali (da riconoscersi – questione controversa – come diritti fondamentali?), il costo dei diritti e in particolare di quelli sociali; la questione della giustiziabilità (ossia della effettiva realizzazione pratica) dei diritti sociali[34]. Inoltre, grazie all'apporto dello Stato, i diritti sociali sono funzionali ad assicurare la libertà, la socializzazione e l'integrazione dell'individuo nella società; appaiono caratterizzati sia da un aspetto prestazionale che da un'aspirazione egualitaria, nel senso della neutralizzazione di specifiche diseguaglianze.

[34] Th. Casadei, *I diritti sociali. Un percorso filosofico-giuridico*, Firenze University Press, Firenze, 2012, pp. 28-29. Sulla questione dei diritti sociali si veda anche S. Zullo, *La dimensione normativa dei diritti sociali: aspetti filosofico-giuridici*, Giappichelli, Torino, 2012.

A tale giustificazione assiologica della categoria generale dei diritti sociali si accompagna poi l'integrazione del riferimento all'interesse sottostante a ciascun diritto sociale (così il diritto alla salute protegge in via diretta l'interesse all'integrità psico-fisica, per cui la protezione quale diritto sociale fa sì che il relativo titolare abbia diritto a ricevere quelle prestazioni che consentano la tutela del predetto interesse anche qualora dovesse trovarsi in una situazione di fatto che glielo impedisce)[35].

Affinché i diritti, sociali e non, possano essere realmente esercitati, e per limitare la vulnerabilità digitale, bisogna però predisporre un "ambiente operativo" idoneo allo sviluppo di una informatica medica rispettosa dei principi e della legislazione di ciascuno Stato in cui "opera". Affinché ciò sia possibile, diviene dunque necessario rispettare determinati requisiti: libertà della ricerca scientifica; libertà della iniziativa economica privata; giustiziabilità effettiva dei diritti fondamentali e sociali; disponibilità di infrastrutture informatiche essenziali e adeguato livello di alfabetizzazione informatica[36]; predisposizione di un adeguato *framework* giuridico relativo al trattamento delle informazioni sanitarie.

Sullo sfondo, nell'odierna Società algoritmica, si pongono però attori particolarmente forti in grado di far sentire la propria voce (prestatori di servizi e fornitori di dispositivi medici) cui si contrappone la moltitudine più o meno disorganizzata di pazienti, interessati, assistiti, clienti. È qui che ciascuno Stato dovrebbe intervenire adeguatamente: ma, al contempo, è lo Stato che fornisce servizi di assistenza sanitaria, per cui si

[35] In tal senso, G. Pino, *Diritti sociali. Per una critica di alcuni luoghi comuni*, in «Ragion pratica», 2016, 2, p. 499.

[36] Ciascuno Stato deve prefiggersi concretamente (ossia andando oltre i proclami solenni) l'obiettivo di eliminare sempre più il divario digitale (o *digital divide*). Con tale termine si indica il divario che separa chi ha accesso alle moderne tecnologie e chi ne è privo. Questo fenomeno assume diverse varianti, per cui si può avere accesso ai computer, ma essere svantaggiati nell'accesso ad Internet per velocità, disponibilità o costo della connessione, oppure si può essere costretti ad utilizzare strumenti ormai obsoleti, e così via. Sul *digital divide* cfr., fra gli altri: D. van Dijk, *The Digital Divide*, Polity Press, Cambridge-Medford, 2020; P. Norris, *Digital Divide. Civic Engagement, Information Poverty, and the Internet Worldwide*, Cambridge University Press, New York, 2002; G. Saraceni, *Digital divide and fundamental rights*, in «Humanities and Rights Global Network Journal», 1, 2020, pp. 66-91; L. Sartori, *Il divario digitale. Internet e le nuove disuguaglianze sociali*, Il Mulino, Bologna, 2006; , S. Vantin, *I divari digitali nell'epoca della rete globale*, in Th. Casadei, S. Pietropaoli (a cura di), *Diritto e tecnologie informatiche*, Wolters Kluwer, Milano, pp. 295-310.

pone insieme come soggetto che regolamenta parzialmente questo settore e come cliente dei fornitori di dispositivi medici e dei prestatori di servizi.

Com'è noto, poi, molti prodotti e servizi sono forniti su scala globale o comunque da soggetti operanti su tale scala, fermo restando che in ciascuno Stato vigono regole specifiche che regolamentano questo settore (cui si aggiungono però servizi trasversali: basti pensare al servizio di posta elettronica). Ciò comporta che, come avviene in molti ambiti, determinate regolamentazioni vengano emanate a livello sovranazionale o internazionale, accompagnandosi però alla combinazione fra *lex informatica* e *lex mercatoria* prodotta dai colossi della Rete. Una Rete, dunque, in cui i poteri privati tendono addirittura a imporsi su quelli pubblici.

Inoltre, si verifica un rimescolamento della gerarchia delle fonti del diritto a tutto favore del contratto e degli usi e a tutto sfavore della legge. Si riscontra un vero e proprio prosciugamento dei poteri "territoriali" dello Stato nonché un sostanzioso adeguamento delle categorie giuridiche alle esigenze mercatorie. Da un lato, ciò è dovuto alle dimensioni e alle interdipendenze planetarie dei mercati economici e finanziari, alla diffusione dei mezzi di comunicazione e all'invasività dell'informazione automatizzata; dall'altro, si verifica un rimescolamento della gerarchia delle fonti del diritto a tutto favore del contratto e degli usi e a tutto sfavore della legge[37].

I.4. Salute digitale e informatica medica: questioni etiche

L'informatica medica e, più in generale, le tecnologie dell'informazione e della comunicazione non costituiscono una sfera "neutrale": cresce la consapevolezza delle implicazioni attuali e potenziali, anche dannose, per il singolo e per la collettività[38]. Del resto, la tecnologia non è «né buona, né cattiva e neppure neutrale»; offre sì opportunità e libera da vincoli materiali e cognitivi, ma può tradursi in minaccia e in forma di potere capace di manipolare, sorvegliare e opprimere[39].

Questi rischi sono accentuati dal fatto che scelte e azioni sono sempre più spesso compiute in una relazione di dipendenza dalla macchina:

[37] F. Riccobono, *I diritti e lo Stato*, Giappichelli, Torino, 2004.

[38] L. Palazzani, *Tecnologie dell'informazione e intelligenza artificiale. Sfide etiche al diritto*, Studium, Roma, 2020, p. 7.

[39] A.C. Amato Mangiameli, Tecno-*diritto e* tecno-*regolazione. Spunti di riflessione*, in «Rivista di filosofia del diritto», speciale, 2017, p. 88.

non più mero strumento rispetto a un fine, ma – nell'esperienza diffusa – interlocutore, facilitatore e, talora, consigliere, che sembra comprendere esigenze e orientare decisioni[40]. Tale dinamica favorisce fenomeni di deresponsabilizzazione: si rinuncia a interrogarsi sulla liceità dei mezzi o dei fini, si confondono fini e mezzi[41], e il mezzo – soprattutto quando è algoritmico – tende a oscurare il fine tanto da dettarlo, alimentando bias dell'automazione e nuove asimmetrie di potere informazionale.

La prospettiva sulla tecnica non è univoca. Come evidenzia Laura Palazzani, infatti, vi è una contrapposizione fra il «tecnoscientismo tecnofilo e ottimista» e l'«anti-tecnoscientismo tecnofobo e pessimista». Se nell'ambito del primo qualsiasi sviluppo della tecnologia viene visto e analizzato come un beneficio per gli esseri umani e l'umanità, in quello del secondo ci si sofferma sempre sulle perplessità e sulle minacce per i singoli e per la società contemporanea e futura; si evidenzia, però, la necessità di cercare una riflessione critica, equilibrata, saggia e prudente. Essa deve, al contempo, garantire il progresso e l'utilizzo delle tecnologie dell'informazione e della comunicazione, promuovendo (e non ostacolando) lo sviluppo dell'identità personale e delle relazioni interpersonali, nel rispetto costante dei valori e dei diritti umani fondamentali (con particolare riferimento a dignità, autonomia, privacy, responsabilità e giustizia)[42].

È in questa cornice che l'informatica medica – e, più ampiamente, la salute digitale – deve essere letta: né feticcio da idolatrare, né minaccia da respingere, ma campo nel quale la razionalità misura e governa poteri, rischi e benefici.

Una simile riflessione è necessaria sia in prospettiva teorica, e dunque soprattutto nell'ottica della bioetica, del biodiritto[43] e, più in generale, della filosofia del diritto (e quindi anche in una loro prospettiva anche pratica),

[40] S. Salardi, M. Saporiti, *Perché l'IA non deve diventare Persona. Una Critica all'ineluttabile 'Divenire antropomorfico' delle Macchine*, in Id., *Le tecnologie 'morali' emergenti e le sfide etico-giuridiche delle nuove soggettività*, Giappichelli, Torino, 2020, p. 52.

[41] T. Serra, *L'uomo programmato*, Giappichelli, Torino, 2003, p. 97.

[42] L. Palazzani, *Tecnologie dell'informazione e intelligenza artificiale. Sfide etiche al diritto*, cit., pp. 7-8.

[43] Proprio il biodiritto, tra l'altro, si caratterizza per essere delimitato da una serie di elementi incidenti su di esso: sub-politica, prassi, mercato, scienza e mercato, scienza e potere, mercato e potere, mentre «la preservazione di uno spazio etico non dipende dalla consapevolezza della sua necessità, ormai acquisita a livello internazionale, ma dall'effettività degli strumenti a disposizione per poterlo garantire» (S. Amato, *Caratteri del biodiritto*, in «Rivista di filosofia del diritto», 1, 2013, p. 45).

sia in una chiave *eminentemente* pratica, come ben evidenziato da Kenneth Goodman, Reid Cushman e Randolph Miller un decennio fa. Secondo questi studiosi, bisogna andare ben oltre a quella che è ritenuta la principale sfida etica su cui focalizzare l'attenzione: la confidenzialità dei dati sanitari di ciascun paziente. Essa è sicuramente fondamentale, ma l'informatica medica è costellata di questioni etiche, che includono la selezione e l'uso appropriato degli strumenti informatici nel contesto clinico (determinando quali siano i soggetti autorizzati ad adoperarli), le obbligazioni di sviluppatori, manutentori e fornitori, l'utilizzo dei computer per il tracciamento degli studi clinici; inoltre, l'informatica genera molte problematiche giuridiche che ne impongono la regolamentazione. Piuttosto, la considerazione delle questioni etiche dell'Informatica medica consiste nella esplorazione del complesso crocevia fra ambiti diversi (in particolare: prestazione dell'assistenza sanitaria, e sua amministrazione; informatica applicata) ed etica (di cui è un vasto ambito di indagine). Negli anni si è fortunatamente sviluppato un crescente interesse nella bioetica e nell'etica del computer, con lo sviluppo di principi etici e linee guida che, essendo finalizzati a orientare i processi decisionali nell'informatica medica, hanno una evidente utilità pratica[44].

Le questioni etiche rimangono dunque centrali per ciò che concerne lo sviluppo e l'utilizzo delle nuove tecnologie nel settore sanitario, con particolare ma non esclusivo riferimento all'informatica medica.

Da questa prospettiva discende un'esigenza di ampiezza definitoria. È opportuno adottare una nozione ampia di informatica medica, capace di dialogare con l'odierna *digital health*: le questioni non riguardano più soltanto il sistema sanitario in senso stretto, ma l'intero ecosistema della salute, in cui operano soggetti pubblici e privati, piattaforme, produttori di dispositivi, fornitori di servizi digitali e comunità di ricerca.

Particolarmente preziosa appare proprio «la riflessione sui principi che guidano l'ambito *eHealth* [, che] ha l'obiettivo di ampliare anche gli sviluppi della sanità elettronica. Infatti, dimostrare che essa può avere un ruolo nei processi decisionali – personali e terapeutici – e che può rappresentare un supporto pratico nella realizzazione dell'*empowerment* del paziente, spinge l'etica a realizzarsi come garanzia di questi aspetti e conferma il connubio

[44] K.W. Goodman, R. Cushman, R.A. Miller, *Ethics in Biomedical and Health Informatics: Users, Standards, and Outcomes*, E.H. Shortliffe, J.J. Cimino (eds.), *Biomedical Informatics. Computer Applications in Health Care and Biomedicine*, Springer, New York, 4th ed., 2014, p. 330.

positivo tra etica e tecnologia, nonché lo sforzo della prima di essere al passo con essa»[45], fermo restando che, più in generale, bisogna sempre garantire il rispetto della dignità umana – che è tuttavia difficilmente configurabile nell'era delle tecnoscienze, in cui diventa oltremodo difficoltoso comprendere «dove fissare il limite, una volta che la vita organica viene vincolata alla tecnologia ed è dunque virtualmente senza un confine predeterminabile ricadendo sotto la gerarchia del progresso tecnoscientifico»[46].

Talvolta ciò comporta la nascita di nuove forme di normatività nei settori dominati dalla scienza e dalla tecnologia, in risposta alla crisi di un diritto cui si chiede di regolare processi e prodotti ancora ignoti – da un lato, promuovendo ricerca e sviluppo in questi ambiti estremamente innovativi; dall'altro, di garantire condizioni di sicurezza per la società. Ai limiti strutturali degli strumenti di *hard law* (e, in particolare, la rigidità e la lunghezza delle procedure) si cerca talvolta di porre rimedio mediante il ricorso a nuove forme di normatività, fra cui l'etica nella sua forma istituzionalizzata, anche grazie al ruolo sempre più centrale che viene assunto da, o che viene fatto assumere a, realtà che pure sarebbero solo consultive come lo European Group on Ethics in Science and New Technologies (EGE). L'etica, così, diviene centrale anche quale «tessuto connettivo *soft* in un rarefatto arcipelago di norme *hard*»[47] e ciò anche in soccorso di ordinamenti giuridici in crisi dinanzi all'incedere vorticoso dei progressi scientifici che rende quanto mai arduo effettuare valutazioni *ex ante* sui medesimi e sugli effetti e le modificazioni che producono nella società.

Allo stesso tempo, il diritto ha conosciuto importanti aggiornamenti: il quadro europeo sulla protezione dei dati ha consolidato il principio di responsabilizzazione e di *privacy by design*; si sono affermati regimi più

[45] L. De Panfilis, S. Zullo, *Aspetti etici delle applicazioni* eHealth, in C. Faralli, R. Brighi, M. Martoni (a cura di), *Strumenti, diritti, regole e nuove relazioni di cura. Il Paziente europeo protagonista nell'eHealth*, Giappichelli, Torino, 2015, pp. 66-67.

[46] U. Pomarici, *Il prisma umano della dignità nell'era delle tecnoscienze. Spunti per una discussione*, in «Rivista di Filosofia del diritto», 2015, speciale, p. 152.

[47] M. Tallacchini, *Scienza e diritto. Prospettive di co-produzione*, in «Rivista di Filosofia del diritto», 2, 2012, pp. 328-330. Inoltre, «L'etica/*soft law* ufficiale, che ripropone l'*ethos* (giuridico) della scienza, è ormai in concorrenza a livello globale con nuove norme e principi privatamente elaborati. Il carattere *soft* di questo nuovo "diritto" è "nelle cose" prima che nello statuto dei provvedimenti non-vincolanti: le "norme" consigliate dalle istituzioni devono competere e sopravvivere in una complessità in cui gli attori sociali coinvolti hanno sempre più la possibilità di invocare (e di rivendicare contro le autorità ufficiali) il "diritto di scelta" dei propri percorsi normativi» (ivi, pp. 331-332).

esigenti per qualità, sicurezza e trasparenza dei sistemi algoritmici impiegati in sanità; si è avviata la costruzione di uno spazio europeo dei dati sanitari per l'uso primario e secondario dell'informazione clinica. Questi sviluppi – che saranno esaminati nei capitoli seguenti – non esauriscono il compito dell'etica; anzi, ne esplicitano la funzione critica e di garanzia.

In conclusione, etica e diritto si presentano come complementari nell'orientare l'innovazione sanitaria in senso umano-centrico e giusto. La loro trasversalità è strutturale: non vi è ambito dell'informatica medica o della salute digitale che non richieda uno sguardo critico, equilibrato, prudente. Solo così la tecnica può essere ricondotta entro un'architettura di garanzie che riconosca la dignità della persona come fine e come limite invalicabile, preservi il diritto all'autodeterminazione informativa, contrasti le disuguaglianze e renda pubblicamente giustificabile l'uso di dati, modelli e decisioni nei processi di cura.

I.5. Sviluppi tecnologici e giuridici: verso una informatica medico-giuridica?

Gli sviluppi dell'applicazione dell'informatica all'ambito sanitario – e, più in generale, alla salute nel suo complesso – stanno segnando una fase ulteriore della trasformazione digitale, che va oltre l'impianto tradizionale centrato su operatori professionalmente dedicati alla prestazione di servizi sanitari in senso stretto (strutture, professionisti, produttori di dispositivi).

Oggi attori tipici della Società dell'informazione concorrono in modo determinante a definire i confini della pratica e dell'immaginario della cura: gli smartphone e gli ecosistemi di dispositivi indossabili hanno normalizzato la raccolta continua di dati fisiologici e comportamentali: tali dati sono elaborati localmente e in ambienti di calcolo remoto, spesso combinati con informazioni contestuali – per esempio la geolocalizzazione o i log dei servizi digitali – e rielaborati in metriche che possono incidere sulle scelte individuali e sull'organizzazione dell'assistenza. La tensione che ne deriva è nota: da un lato, crescono i rischi per la privacy e la protezione dei dati (specie a fronte di inferenze sulla salute a partire da dati apparentemente "non sanitari"); dall'altro, la disponibilità di flussi informativi ad alta frequenza ha mostrato, anche durante la pandemia da Covid-19, la propria utilità per la sanità pubblica, la sorveglianza epidemiologica e l'al-

locazione tempestiva delle risorse, pur entro limiti metodologici ed esigenze di legittimazione sociale che non possono essere sottovalutati.

Questo intreccio rende sempre più arduo delimitare i confini tra attività sanitarie in senso stretto e pratiche digitali a scopo generale. La stessa nozione di "informatica medica" si apre verso una salute digitale che comprende piattaforme, app destinate al consumatore, ambienti domestici connessi e servizi online, nei quali la distinzione tra paziente, utente e consumatore tende a sfumare. Il diritto non può intervenire soltanto *ex post* per riparare gli effetti indesiderati di questa riconfigurazione: la sua funzione è anche quella di orientare lo sviluppo *ex ante*, rendendo esplicite le condizioni di liceità e legittimità delle pratiche digitali che interagiscono con la salute e orientandole finalisticamente verso la tutela della vita, della salute, della libertà e della dignità delle persone (e dei gruppi sociali). In assenza di tale orientamento, l'applicazione di discipline generali del digitale all'ambito della salute rischia di produrre vuoti regolativi o, per converso, sovra-estensioni che non colgono le specificità della cura, aggravando l'incertezza degli operatori e la vulnerabilità degli interessati.

Un rapido sguardo ai profili tecnologici conferma quanto esposto. L'interconnessione capillare di oggetti e ambienti (*Internet of Things*), l'uso pervasivo di tecniche di apprendimento automatico (oggi anche in forme generative e in combinazione con basi di conoscenza di ampia portata e in costante aggiornamento), le applicazioni di realtà aumentata e virtuale nella formazione e nella riabilitazione, la diffusione di gemelli digitali (modelli computazionali dei pazienti) e stampa tridimensionale la personalizzazione e per la pianificazione degli interventi, la robotica, compongono un quadro nel quale la produzione, l'integrazione e l'uso dei dati diventano il fulcro di una medicina sempre più predittiva e personalizzata. Ciascuno di essi solleva questioni giuridiche specifiche che non si riducono (pur includendola sempre) alla sola protezione dei dati; toccano questioni fondamentali fra cui devono qui menzionarsi la qualità e integrità dell'informazione clinica, la trasparenza e la spiegabilità dell'aiuto "algoritmico" alle decisioni, la responsabilità civile, la cibersicurezza, la proprietà intellettuale (che riguarda non solo i programmi per elaboratore, ma anche modelli e dataset), la correttezza delle pratiche di mercato e la concorrenza nei contesti incentrati sulle piattaforme, l'accessibilità e la non discriminazione che consentono di raggiungere l'eguaglianza nell'accesso ai servizi digitali relativi alla salute e dunque di tutelarne i relativi diritti, da quello – per l'appunto – alla salute per giungere sino all'autodeterminazione informativa.

Da qui la centralità, non meramente strumentale, del diritto. Non esiste un "diritto dell'informatica medica" monolitico: a seconda delle fattispecie, si intrecciano diritto costituzionale (dignità, autodeterminazione, salute), diritto privato (contratti, responsabilità, consumatori), diritto commerciale e antitrust (profili societari, Big Tech), diritto del lavoro (trattamenti di dati sul luogo di lavoro), proprietà intellettuale e diritto d'autore (software, hardware, segreti industriali), diritto amministrativo (acquisizione di tecnologie, trasparenza e controllo), oltre alle discipline orizzontali del digitale e ai regimi settoriali della sanità. Questo policentrismo, lungi dall'essere un difetto, è un tratto strutturale: la sanità digitale non è un settore isolato, ma un crocevia nel quale si incontrano – e talora collidono – logiche e valori differenti.

Proprio per questa ragione è utile rivendicare uno sguardo unitario che eviti sia l'astrazione generalissima sia la chiusura settoriale. Come osserva Ugo Pagallo, l'informatica giuridica può orientare lo studio e la pratica delle tecnologie dell'informazione offrendo un principio di coesione nell'atomizzazione dei campi del diritto positivo[48]. Applicata al dominio qui in esame, essa consente di chiarire categorie (soggetti, ruoli, poteri, doveri), di precisare regole (condizioni, limiti, garanzie) e di conformare processi (progettazione, adozione, uso, controllo) in modo coerente con la specificità della cura. In questo senso, il riferimento a una possibile "informatica medico-giuridica" è una suggestione evocativa finalizzata a esprimere l'esigenza di fornire coerenza sistematica a un campo nel quale l'innovazione tecnica e l'innovazione normativa procedono insieme e in cui la constatazione della vulnerabilità dinamica della persona chiede, oggi più che mai, una razionalità pubblica capace di legare efficienza e garanzia.

La trasformazione digitale della salute esige un diritto più strutturato: un'architettura di garanzie e condizioni di liceità, non una mera reazione sanzionatoria *ex post*. In questa prospettiva, l'informatica medica e la salute digitale non sono esiti necessari della tecnica, bensì costruzioni sociali e normative: flussi di dati, interfacce e processi decisionali incorporano scelte di valore e assetti di potere che il diritto deve rendere intelligibili, motivabili, controllabili e contestabili entro regimi di responsabilità effettiva. Solo così l'innovazione evita di alimentare nuove asimmetrie e dipendenze e promuove capacità e autonomia di persone e comunità.

[48] U. Pagallo, *Prolegomeni d'informatica giuridica*, Cedam, Padova, 2003, p. 1.

I.6. Vulnerabilità aumentata

In linea generale, «la vulnerabilità è un tratto costitutivo della condizione umana ed è possibile attivare uno sguardo "dal basso", *ex parte populi*, verso le istituzioni e nei riguardi delle situazioni materiali dei soggetti stessi»[49] – del resto, «il rischio della vulnerabilità è uguale per tutti»[50] e la vulnerabilità può essere considerata una condizione ontologica[51], in quanto universale e costante, dell'essere umano che si manifesta in modi diversi e con intensità variabile[52]. Essa può assumere diversi significati, come «la suscettibilità di subire danni causati da fenomeni naturali o da attività umane» o «una *particolare* suscettibilità, da parte di un soggetto e/o di più soggetti, di subire determinati danni per effetto di determinate azioni o determinati fenomeni naturali»; è un «termine usato in diversi campi dell'esperienza, dotato di innegabile ricchezza semantica. È concetto indeterminato, propriamente vago, dal momento che molteplici sono le condizioni e incerti sono i confini della sua area di applicazione» e «consente di dar conto della precarietà, della fragilità, dell'insicurezza, delle minacce, dei rischi, che caratterizzano l'epoca contemporanea e che incidono sulla vita degli individui»[53].

[49] Th. Casadei, *Soggetti in contesto: vulnerabilità e diritti umani*, in Id. (a cura di), *Diritti umani e soggetti vulnerabili, Violazioni, trasformazioni, aporie*, Giappichelli, Torino, 2012, p. 91.

[50] P. Pettit, *Il repubblicanesimo*, Feltrinelli, Milano, (1977) 2000, p. 152.

[51] «Adottare una connotazione ontologica della vulnerabilità non implica […] necessariamente ritenere che le sue cause della stessa siano riconducibili esclusivamente a variabili endogene alla persona. Essa mi pare, invece, pienamente compatibile con l'individuazione di variabili anche esogene, legate ai modelli di organizzazione sociale, politica, economica, culturale ed al processo di riconoscimento che è, in varie forme, alla base della relazione sociale, nonché dell'identità personale. L'essere umano è ontologicamente vulnerabile non solo e non tanto in conseguenza di elementi relativi a caratteristiche personali, quanto piuttosto in conseguenza del suo collocarsi, con tali specifiche caratteristiche, in un contesto relazionale, risultato di assetti istituzionali, processi di riconoscimento e rapporti di forza» (E. Pariotti, *Vulnerabilità, approccio intersezionale e linguaggio dei diritti*, in «GenIUS», 2, 2023, p. 39).

[52] M.A. Fineman, *The Vulnerable Subject: Anchoring Equality in the Human Condition*, in «Yale Journal of Law and Feminism», 2008, p. 1.

[53] B. Pastore, *Semantica della vulnerabilità, soggetto, cultura giuridica*, Giappichelli, Torino, 2021, pp. 1-3.

Si è osservato che, negli ultimi decenni, il concetto di vulnerabilità (che può essere individuale, di gruppo[54] e di comunità[55]) è stato sviluppato in tre direzioni principali: «all'interno di analisi sul concetto di dipendenza e sull'etica della cura; nella riflessione bioetica; in una prospettiva ontologica, di riflessione sulla condizione umana e sulla corporeità», ed è certo «consistente l'analisi della vulnerabilità come chiave interpretativa di problemi di giustizia distributiva», ancorché per lo più in modo trasversale rispetto ai tre precedenti[56]. Soprattutto, «la teoria della vulnerabilità riabilita la natura relazionale dell'uomo e spesso riscatta i rapporti di cura e di dipendenza reciproca dall'irrilevanza in cui la scienza giuridica li ha collocati per millenni»[57].

Tanto premesso, nel presente volume, alla vulnerabilità si guarda nella prospettiva della salute digitale che costituisce oramai un elemento inscindibile della società contemporanea, che è sia dell'informazione (sotto diversi aspetti) sia algoritmica (sotto altri).

[54] Proprio la protezione dei gruppi vulnerabili e dei suoi componenti è vista come una componente essenziale e centrale del Diritto internazionale dei diritti umani (cfr. I. Nifosi-Sutton, *The Protection of Vulnerable Groups under International Human Rights Law*, Routledge, New York-London, 2017, p. 267).

[55] Nell'ambito della ricerca medica che coinvolge partecipanti umani, è particolarmente significativa la Dichiarazione di Helsinki, in relazione alla «vulnerabilità individuale, di gruppo e di comunità»: «19. Alcuni individui, gruppi e comunità si trovano in una situazione di maggiore vulnerabilità come partecipanti alla ricerca a causa di fattori che possono essere permanenti o contestuali e dinamici, e sono quindi a maggior rischio di subire abusi o danni. Quando tali individui, gruppi e comunità hanno particolari bisogni di salute, la loro esclusione dalla ricerca medica può potenzialmente perpetuare o esacerbare le loro diseguaglianze. Pertanto, i danni determinati dalla loro esclusione devono essere considerati e soppesati rispetto ai danni determinati dalla loro inclusione. Per essere inclusi in modo equo e responsabile nella ricerca, dovrebbero ricevere supporto e protezioni specificamente predisposti per loro. 20. La ricerca medica con individui, gruppi o comunità in situazioni di particolare vulnerabilità è giustificata solo se essa risponde alle loro esigenze e priorità sanitarie, e l'individuo, il gruppo o la comunità può trarre beneficio dalle conoscenze, dalle pratiche o dagli interventi che ne derivano. I ricercatori dovrebbero includere coloro che si trovano in situazioni di particolare vulnerabilità solo quando la ricerca non può essere condotta in un gruppo o comunità meno vulnerabile, o quando escluderli potrebbe perpetuare o esacerbare le loro diseguaglianze» (World Medical Association, *Dichiarazione di Helsinki. Principi etici per la ricerca medica che coinvolge partecipanti umani*, 1964-2024).

[56] F. Macioce, *La vulnerabilità di gruppo. Funzione e limiti di un concetto controverso*, Giappichelli, Torino, 2021, p. 2.

[57] L. Corso, *Vulnerabilità e concetto di diritto*, in Id., G. Talamo (a cura di), *Vulnerabilità di fronte alle istituzioni e vulnerabilità delle istituzioni*, Giappichelli, Torino, 2019, p. 12.

La salute e la cura digitali non sostituiscono l'esperienza materiale: la ampliano e, al contempo, ne riconfigurano tempi, luoghi e priorità, dando vita a una "realtà aumentata" in cui gli elementi digitali si fondono con quelli materiali e con le pratiche quotidiane, mediante servizi, dispositivi e documentazioni quali piattaforme, sensori, algoritmi, protocolli: l'esperienza digitale si innerva su quella materiale in modo inscindibile, orientando le condotte dei vari soggetti in gioco. In questa fusione, ciò che viene reso misurabile tende a diventare governabile; ciò che resta ai margini della rappresentazione perde visibilità pratica (con il rischio di giungere a vulnerabilità invisibili[58]). Lungi dall'essere un semplice supporto, l'infrastruttura digitale complessivamente intesa introduce una grammatica dell'attenzione che struttura il campo di ciò che è visto, discusso, valutato e, in ultima analisi, deciso.

La conseguenza è duplice. Da un lato, la fusione digitale può affinare l'attenzione professionale, favorire la distribuzione delle competenze, aumentare la tempestività e la coerenza delle decisioni lungo percorsi che attraversano luoghi e tempi non più vincolati alla presenza fisica. Dall'altro lato, la stessa dinamica espone a una «vulnerabilità aumentata»[59] e, in linea più generale, bisogna considerare che la vulnerabilità, nella sua forma relazionale[60], assume un significato politico, giuridico[61] e sociale[62].

[58] Esistono «modalità di percezione che generano vulnerabilità tanto più severe e drastiche quanto più non sono individuabili come tali» (G. Zanetti, *Filosofia della vulnerabilità*, op. cit., p. 15).

[59] Si consideri che «partire da condizioni di vulnerabilità, dalle ferite e dalle offese subite, attraverso la contestazione dei paradigmi di valore e delle istituzioni della società che generano e perpetuano forme di discriminazione, subordinazione, oppressione, si avanzano visioni alternative basare su specifici bisogni e improntare alla realizzazione di ideali di emancipazione» (Th. Casadei, *La vulnerabilità in prospettiva critica*, in O. Giolo, B. Pastore (a cura di), *Vulnerabilità. Analisi multidisciplinare di un concetto*, Carocci, Roma, 2018, p. 88).

[60] In riferimento alla cura, essere in una situazione in cui se ne ha necessità significa trovarsi in una condizione di una certa vulnerabilità (J. Tronto, *Moral Boundaries. A Political Argument for an Ethic of Care*, Routledge, New York-London, 1993, p. 134).

[61] Su cui, oltretutto, possono incidere anche prassi diverse delle autorità amministrative in diversi settori, solo raramente oggetto di riflessione giusfilosfica, con lesione dell'eguaglianza formale degli individui – con un potenziale ruolo cruciale delle cliniche legali «nell'illuminare il lato oscuro del diritto» (A. Schiavello, *Vulnerabilità, concetto di diritto e approccio clinico-legale*, in «Etica & Politica», 3, 2019, p. 275).

[62] Teresa Serra pone il quesito se sia «sufficiente ripensare una nuova idea di politica o di giustizia sulla base del principio di vulnerabilità o, piuttosto, accettare che sia un monito contro le ambizioni di potere dell'uomo, nell'impossibilità di raggiungere una sua opera-

Tale aumento non è meramente quantitativo, ma soprattutto qualitativo: si amplia perché si moltiplicano i punti in cui l'immateriale si fonde con il materiale e la rappresentazione digitale incide sulla vita concreta. Quando i modelli non tematizzano esplicitamente un elemento, quel tratto non viene misurato né reso visibile nei criteri di rilevanza e nelle procedure decisionali; ne restano esclusi il confronto e la giustificazione, e scivola fuori dall'orizzonte pratico dell'azione, producendo vulnerabilità invisibili (ad esempio, un telemonitoraggio dello scompenso cardiaco che registra passi e frequenza cardiaca ma non l'aggravarsi della dispnea). Quando la distanza tra rappresentazioni e persone si allarga per deriva del modello, predittori scarsamente informativi o metriche poco trasparenti, il giudizio tende a polarizzarsi sul punteggio: si rafforza l'*automation bias* oppure, per reazione, prende corpo un rifiuto difensivo della mediazione digitale (il clinico che segue il rischio stimato contro evidenze cliniche; il paziente che abbandona l'app dopo falsi allarmi). Infine, quando il potere decisionale viene riallocato lungo la filiera tecnico-organizzativa, protocolli, parametri predefiniti e interfacce delimitano *ex ante* lo spazio delle scelte, assottigliando lo spazio del giudizio professionale argomentato e dell'autogoverno degli interessati. Ne risulta una sequenza ordinata: dal difetto di rappresentazione al bias decisionale fino alla compressione della responsabilità, con un incremento della vulnerabilità di natura strutturale, non meramente quantitativa. Sul piano giuridico, tale sequenza incide su motivazione, trasparenza e contestabilità delle decisioni, e quindi sull'*accountability* degli attori coinvolti.

tività sociale. Ancora, una volta riconosciuto che tutti gli esseri umani sono liberi e uguali, e che tutti gli esseri viventi, tra cui la stessa natura, abbisognano della cura di tutti, non è possibile trovare principi più radicali per organizzare la società su base paritaria. Ma il problema non sono certamente i principi, o gli ideali, bensì il fatto che i principi sono ben lontani dal poter essere realizzabili dal momento che non esiste una loro corrispondenza in un costume generalizzato in una comunità universale di valori. Il tema della cura può sembrare utopistico, e talvolta mistificatorio, se non viene tradotto nella possibilità di trovare punti di incontro sulle prassi concrete: un accordo sui valori minimi come il rispetto della dignità, del corpo, della persona che il diritto deve tutelare. La reciprocità dell'etica della cura evidenzia aspetti fondamentali che caratterizzano la relazione umana nei termini concreti della quotidianità, che è estremamente complessa, anche sul piano del rapporto interindividuale. In essa l'altro non è sempre un soggetto, portatore di una alterità in termini positivi. Può essere e spesso è anche considerato e trattato come un oggetto di cui ci si può appropriare, perché privo di coscienza, o che si può dominare perché privo di volontà» (T. Serra, *Vulnerabilità ed etica della cura*, in A. Di Giandomenico (a cura di), *ETSI DEUS NON DARETUR…Scritti in memoria di Serenella Armellini*, Giappichelli, Torino, 2023, pp. 460-461).

La metafora è utile: la realtà virtuale evoca ambienti chiusi, regolati da protocolli interni, e ambienti separati; la realtà aumentata, invece, descrive la condizione mista della salute digitale. Il corpo resta biologico e situato, ma la sua intelligibilità pratica dipende da strati digitali che orientano l'azione. La promessa di "oggettività" dei dati deve perciò essere letta criticamente, in quanto le metriche non sono neutrali e derivano da scelte. La neutralità apparente dei sistemi e dei servizi (soprattutto se "intelligenti") si traduce facilmente in scelte normative implicite: che cosa misurare, con quali soglie, per quali finalità.

In senso proprio, vulnerabilità aumentata[63] designa l'allargamento della superficie di esposizione prodotto dalla fusione tra strati informativi e dispositivi in riferimento a spazialità, temporalità, inferenzialità, istituzionalità, asimmetricità.

È spaziale, perché sensori, applicazioni e interfacce rendono pervasiva la raccolta e l'uso dei dati con irrilevanza del luogo tradizionale di erogazione: la decisione clinica può maturare in contesti atipici e disseminati, con effetti sulla qualità del setting e sulla responsabilità dei soggetti coinvolti. È temporale, perché persistenza, accumulazione e riuso dei dati generano identità digitali che superano il momento clinico, con traiettorie di rischio e di opportunità che accompagnano le persone nel tempo. È inferenziale, perché catene di elaborazione costruite su pochi segnali consentono deduzioni sensibili sullo stato di salute e sui comportamenti: ne derivano benefici predittivi ma anche rischi di errore sistematico e di ingiustizia, quando gli esiti si distribuiscono in modo non equo. È istituzionale, perché la dipendenza da infrastrutture, standard e fornitori (pubblici e privati, nazionali e transnazionali) incide su qualità e sicurezza, interoperabilità e portabilità, continuità operativa e resilienza, trasparenza e verificabilità, vigilanza e accreditamento, responsabilità professionale, di struttura e di prodotto, oltre che sui diritti degli interessati e sull'effettività dei rimedi. È asimmetrica, perché chi progetta, addestra o governa i sistemi non coincide con chi subisce o beneficia degli esiti, e gli squilibri

[63] Fermo restando che l'utilizzo del paradigma della vulnerabilità debba essere attentamente monitorato sul piano teorico-pratico del diritto affinché non si passi dal modello degli Stati costituzionali di diritto (basato sulla tutela dei diritti fondamentali e sul principio di uguaglianza) a una tutela paternalistica e selettiva "dei più vulnerabili", riportando in auge retoriche e modelli di intervento ritenuti superati (L. Re, *Introduzione. La vulnerabilità fra etica, politica, diritto*, in, M.G. Bernardini, B. Casalini, O. Giolo, L. Re (a cura di), *Vulnerabilità: etica, politica, diritto*, IF Press, Roma, 2018, p. 25).

informazionali e negoziali possono ampliarsi (del resto, tali soggetti perseguono finalità diverse: chi li fornisce persegue normalmente un fine di profitto; chi li utilizza mira al miglioramento del proprio stato di salute).

A queste linee si aggiungono due dimensioni trasversali che pervadono l'intero volume. La prima è computazionale: la qualità delle decisioni dipende questioni tecniche che raramente sono visibili agli utilizzatori ma che condizionano accuratezza, equità e affidabilità. La seconda è interazionale: interfacce, scelte informative, predefiniti e procedure di conferma orientano i comportamenti, con possibile compressione dell'autodeterminazione informativa e decisionale quando il margine critico si riduce a mera ratifica.

In questo quadro, il diritto non agisce come impedimento allo sviluppo della salute digitale[64], bensì quale garanzia di sua conformità all'ordinamento giuridico, affinché l'incremento informativo (nativo digitale o digitalizzato) tenda al miglioramento della salute intesa in senso ampio, come condizione dinamica di benessere fisico, psichico e sociale, attenta alle differenze personali e ai contesti. La razionalità giuridica offre linguaggi e strumenti per rendere esplicite le scelte implicite, sottoporle a controllo pubblico e privato, distribuire responsabilità e assicurare tutele effettive.

Da qui discendono quattro condizioni interconnesse. Anzitutto, criteri di visibilità e priorità che siano pubblici, motivati e sindacabili: occorre poter comprendere perché certe misure contino più di altre e con quali conseguenze. In secondo luogo, idoneità comprovata e adeguatezza al contesto d'uso: non basta che una tecnologia "funzioni" astrattamente, deve funzionare per le persone "reali" che la utilizzano, direttamente o indirettamente. In terzo luogo, rispetto dei principi di necessità e proporzionalità dell'apporto digitale nei percorsi di promozione della salute, del benessere e della cura: un maggior numero di dati o un potenziamento dell'automazione sono necessariamente "migliori". Infine, assetti chiari di responsabilità e tutele effettive, con canali di contestazione, verifica e stru-

[64] Del resto, il valore dei diritti riguarda, «sul piano assiologico-normativo, il valore ultimo della dignità, che implica a sua volta il dovere etico di prendersi cura, oltre che di se stessi, anche degli altri, nonché, sul piano strettamente giuridico, la messa in atto di tecniche che consentano ai soggetti più deboli di essere posti in condizione di poter esercitare concretamente i loro diritti». Questo approccio si mostra «al passo con la vita, nel suo andamento irregolare, multiforme e incerto: non la allontana da sé, ma cerca di penetrarvi. Ciò che è reso possibile […] solo con uno sguardo "dal basso" alla realtà e al mondo del diritto e delle istituzioni» (Th. Casadei, *Soggetti in contesto: vulnerabilità e diritti umani*, op. cit., p. 115).

menti di tutela che operino *ex ante* ed *ex post*, così da prevenire, o intervenire sulle, fattispecie di "vulnerabilità aumentate".

La trattazione che segue sviluppa questa tesi in modo progressivo e coerente con l'impianto del volume: il secondo capitolo elabora i profili teorici e i principi giuridici ed etici trasversali della salute digitale, il terzo ne discute pratiche e applicazioni, mostrando come le scelte teoriche si traducano in forme di organizzazione e di decisione, il quarto, sulla base del progetto FACILITATE, approfondisce, nell'ambito della ricerca e delle sperimentazioni cliniche, la tematica della restituzione dei dati ai pazienti e ai partecipanti. Il quinto capitolo conclude la trattazione discutendo la salute digitale nella prospettiva della vulnerabilità aumentata, con le conseguenti riflessioni sulle possibili sfide e prospettive. Più ampiamente, se la dimensione digitale incide sul reale, "aumentandolo", al diritto spetta il compito di contribuire alla protezione e al miglioramento della salute e la cura orientando le nuove tecnologie, il cui incedere è inarrestabile ma governabile, in una prospettiva che, lungi dal moltiplicare gli adempimenti, renda intelligibili le scelte, riequilibrando oneri e benefici, garantendo la contestabilità degli esiti e responsabilizzando (in modo verificabile) la promessa di benessere che accompagna ogni tecnologia quando entra, davvero, nella vita delle persone, dei gruppi e delle comunità.

II. Profili giuridici ed etici della salute digitale

II.1. Introduzione

La trattazione della salute digitale prendendo la vulnerabilità (aumentata) come filo conduttore richiede una riflessione critica in merito ai suoi profili giuridici ed etici così che tale prospettiva teorica, di carattere più generale, costituisca il fondamento di quella pratica, con precipuo riferimento alle sue applicazioni. In assenza di una simile analisi, la mera discussione delle applicazioni della salute digitale finirebbe per essere meramente descrittiva e si perderebbe il nesso tra fini, mezzi e responsabilità, indispensabile per coglierne l'incidenza su vita, salute e autodeterminazione delle persone e delle comunità nonché per comprendere come la vulnerabilità assuma la connotazione di "aumentata", caratterizzata dalla commistione – profonda, pervasiva e indistinguibile – fra reale e virtuale, digitale e materiale, identità personale e plurime identità digitali. Il tutto rifuggendo dai riduzionismi che la tecnica tende a far nascere o a potenziare, con particolare riferimento al dataismo che discende da una progressiva oggettificazione della persona e da una sua profilazione già a livello normativo, con una sua frammentazione (paziente, interessato, operatore sanitario od operatrice sanitaria, consumatore, utente, e così via[1]) che tende a far perdere la sua caratteristica primaria: l'essere una "persona" che vive in una comunità (magari globale).

In un ambito tecnologico che è costantemente "nuovo" perché gli artefatti mutano costantemente e si evolvono è necessario guardare ad essi, e più in generale all'evoluzione scientifica e tecnologica, anche in una prospettiva maggiormente abilitante, traendo spunto da quanto affermato in merito all'intelligenza collettiva e all'intelligenza artificiale (IA): «Il tempo presente ci impone […] di chiederci se l'intelligenza collettiva cui partecipiamo non includa anche gli agenti non umani capaci di (elaborare) pensiero e linguaggio. La stessa domanda, invero, giusta

[1] Sul punto, bisogna anche considerare l'oppressione derivante dall'appartenenza identitaria: essa «non sta nella vittimizzazione diretta che si ha nel singolo caso, ma nella consapevolezza di tutti gli appartenenti al gruppo di essere esposti a questo rischio proprio in ragione di un'appartenenza identitaria che è (anche solo agli occhi degli altri) collettiva» (Th. Casadei, *Diritto e (dis)parità. Dalla discriminazione di genere alla democrazia paritaria*, Aracne, Roma, 2017, p. 60).

la lezione ermeneutica, viene formulata a partire da un orizzonte in cui i nostri processi cognitivi e decisionali sono già ampiamente ibridati grazie alla quotidiana interazione con quei sistemi. Ebbene, i sistemi avanzati di IA basati su modelli di linguaggio di ultima generazione non possono forse considerarsi parti di una nuova intelligenza collettiva»[2].

Per ciò che concerne la prospettiva teorica e metodologica del presente volume, può qui evidenziarsi che il riferimento alla vulnerabilità aumentata consente di comprendere che nell'ambiente digitale si accentuano le asimmetrie informative tra i vari soggetti (assistito/azienda sanitaria, cliente/azienda farmaceutica, medico/paziente, utente/provider, e così via) e si consolidano dipendenze da infrastrutture, standard e soggetti di diversa tipologia anche su scala globale in un ambiente "misto": ciberspazio, mercato, sanità.

La persona viene gravata di oneri cognitivi e organizzativi nella prospettiva di una sua responsabilizzazione che, ove non correttamente orientata, diviene una deresponsabilizzazione di determinati soggetti che, non a caso, sono proprio quelli che possono avvantaggiarsi dello squilibrio: prestatori di servizi, fornitori di prodotti, strutture sanitarie e professionisti.

L'ambito del giuridico è qui fondamentale: contratti caratterizzati da una profonda vessatorietà (degli «scambi senza accordo»[3]) che regolamentano il rapporto fra utenti e prestatori, clienti e produttori, assistiti e strutture sanitarie e professionisti. I contratti («termini e condizioni», comuni nelle prime due ipotesi[4]) e gli strumenti fondamentali, come il consenso informato – fondamentale per l'esercizio del diritto all'autode-

[2] A. Punzi, *"Accolse l'uomo come opera di natura indefinita". Note su esperienza giuridica e nuovo ordine delle intelligenze*, in «Rivista di filosofia del diritto», 1, 2025, p. 26).

[3] N. Irti, *Scambi senza accordo*, in «Rivista trimestrale di diritto e procedura civile», 1998, pp. 347-364.

[4] In una prospettiva in cui vari soggetti privati che detengono un potere sempre più forte e pervasivo portano all'estremo il rifiuto della regola statale e operano una minuziosa (auto-)regolamentazione di settore, portando agli scambi senza accordo in cui l'unica scelta è, per la parte debole, accettare o meno di concludere un contratto, e, in presenza di fenomeni patologici, trovarsi a essere un novello Davide contro Golia in cui le regole dello scontro vengono per lo più redatte (e addirittura applicate) dal Golia di turno (sia consentito rinviare, sul punto, a G. Fioriglio, *Riflessioni sul "feticismo della legge" nella società contemporanea*, in A. Di Giandomenico (a cura di) *ETSI DEUS NON DARETUR… Scritti in memoria di Serenella Armellini*, Giappichelli, Torino, 2023, pp. 295-311).

terminazione – si tramutano in "armi" contrattuali di deresponsabilizzazione. E ciò potenzialmente sfruttando una situazione di vulnerabilità che tocca non solo chi è affetto da una patologia ma anche chi vuole migliorare il proprio stato di salute sfruttando app, prodotti e informazioni reperibili online anche tramite servizi di IA.

Del resto, la salute digitale costituisce anche un "mercato" di valore ingente, poiché incide su diritti fondamentali della persona: la vita e la salute. Non è tuttavia la rilevanza economica a fondare le scelte; è la tutela di tali diritti, nell'attuale contesto di vulnerabilità aumentata, che impone un criterio ordinatore capace di distinguere quando l'apporto digitale amplia le capacità effettive della persona, consentendole di autodeterminarsi effettivamente, e quando, al contrario, le comprime, riducendo la persona a una componente di un processo di cura o di raggiungimento di un preteso benessere psico-fisico eterodiretto, in cui la cura viene ridotta all'esecuzione di una sequenza di adempimenti e la ricerca del benessere dipende da esigenze di mercato (nella specie, fornitura di servizi e prodotti). Tale criterio deve misurarsi con le asimmetrie informative e con le dipendenze infrastrutturali che, lungo l'intera filiera, spostano oneri e responsabilità (cognitivi, organizzativi e di rischio) dal sistema alla persona.

La protezione della salute digitale richiede un'architettura normativa di garanzie sostanziali che non può essere costituita da un'elencazione di adempimenti tecnici e amministrativi, né può farsi riferimento alla protezione della persona dando eccessiva centralità al diritto alla privacy e alla protezione dei dati personali per evitare derive di burocratizzazione. La tutela si costruisce nell'intersezione tra protezione dei dati, sicurezza dei sistemi e dei dispositivi, qualità e spiegabilità dei processi algoritmici, interoperabilità e continuità dei percorsi clinico-amministrativi, valutazione clinica e accountability degli attori, riequilibrio dei rapporti contrattuali e riduzione del divario digitale. Le scelte tecniche e organizzative devono restare motivabili, documentate e rivedibili lungo l'intero ciclo di vita dei sistemi, ancorate a una gestione del rischio trasparente e a basi documentali adeguate; non può inoltre prescindersi dalla predisposizione di strumenti di tutela agili, rapidi ed efficaci.

Tre questioni, in controluce, attraversano l'intero volume. La prima concerne il rapporto tra correlazione e spiegazione: l'efficienza predittiva non sostituisce l'obbligo di motivazione; la spiegabilità consiste nell'effettiva possibilità di ricostruire, e conseguentemente poter sindacare, gli

iter che portano a determinate scelte e a determinati output, così da rendere possibili giustificazione e controllo. La seconda riguarda il ruolo della persona nei flussi informativi: il dato è traccia biografica e relazionale, non risorsa neutra; preservarne il contesto significa evitare che standard e monitoraggi degenerino in normalizzazione o sorveglianza, e che la personalizzazione introduca nuove diseguaglianze e riduca la persona alla somma dei suoi dati finalisticamente orientata (per costruire l'identità di assistito, consumatore, paziente, utente, e così via). La terza attiene all'equilibrio fra regola e applicazione al caso concreto: le architetture tecnico-scientifiche della cura – linee guida, protocolli, e così via – sostengono un monitoraggio per supportare le decisioni a diversi livelli (dalle politiche sanitarie alla cura del singolo paziente); diventano derive difensive quando sostituiscono il ragionamento clinico e cancellano la "deviazione motivata" talora necessaria nel caso concreto.

Sullo sfondo si pongono la cibersicurezza e, soprattutto, la sottrazione della persona da logiche di sua oggettificazione per esigenze di mercato o efficienza tecnica o amministrativa. Più specificatamente, se la tecnologia connota l'ambito digitale della salute, è ovvio che tutelare la sicurezza e il corretto funzionamento della prima è necessario per proteggere la seconda. Basti pensare, in modo paradigmatico, a un attacco ransomware andato a buon fine, che può bloccare l'operatività di una struttura, e a bias di un sistema di IA utilizzato nell'ambito della salute che possono discriminare individui e gruppi, ledendone i diritti fondamentali.

Il capitolo sviluppa queste linee senza separarle. Così, l'analisi critica dell'IA permette di sorreggere la pretesa a un suo sviluppo e a un suo utilizzo quale strumento, trasparente, di ausilio alle decisioni umane, evitando rischi di deumanizzazione soprattutto in riferimento al rapporto medico/paziente ma anche pericoli di algoritmizzazione della salute con evidente impatto sull'autodeterminazione, che diventerebbe eterodeterminazione.

L'IA, però, si basa sui dati e, più in generale, la salute digitale e l'informatica medica sono comunque incentrate sul dato. Ne conseguono la centralità e la trasversalità della privacy e della protezione dei dati personali, di cui si propone un ritorno alla loro funzione originaria ed essenziale di tutela della persona: in Warren e Brandeis dall'assalto dei mass media, oggi dall'assalto delle tecnologie, ma anche da una prospettiva monodimensionale che converte la persona in interessato, sovente sen-

za un adeguato bilanciamento di tale diritto con altri (in primis, il diritto alla salute).

Queste tematiche, a loro volta, si intrecciano con le questioni inerenti alla produzione e alla circolazione della conoscenza nel ciberspazio, prodotta da agenti artificiali e umani con logiche differenti, e dunque sempre più mediata non solo dai tradizionali provider, ma anche da sistemi "intelligenti". Di qui, dunque, la successiva trattazione del dataismo sia per ciò che concerne la persona nel ciberspazio e nell'ecosistema della salute digitale sia nella regolazione tecnico-scientifica e nei processi di cura oltre che di mercato: questo ecosistema è, tuttavia, assai fragile e vede una molteplicità di agenti artificiali e umani al suo interno, per cui la sua sopravvivenza dipende anche dalla garanzia di cibersicurezza.

II.2. Intelligenza artificiale e salute algoritmica

L'intelligenza artificiale (sovente abbreviata in IA), o *artificial intelligence* (AI) è divenuta sempre più popolare negli ultimi anni. Essa ha come scopo lo studio e la comprensione dell'intelligenza; «è usualmente definita come la scienza intesa a sviluppare modelli computazionali del comportamento intelligente, e quindi a far sì che gli elaboratori possano eseguire compiti che richiederebbero intelligenza da parte dell'uomo»[5].

Il suo progresso è stato notevolissimo in un arco di tempo relativamente ristretto: è infatti nel 1956 che John McCarthy – un pioniere di questo ambito – ha coniato proprio il termine "intelligenza artificiale" in occasione della proposta di una ricerca compiuta da più studiosi di diversi settori[6].

[5] G. Sartor, *Intelligenza artificiale e diritto. Un'introduzione*, Giuffrè, Milano, 1996, p. 9.

[6] «Lo studio dovrà procedere sulla base dell'ipotesi secondo cui ogni aspetto dell'apprendimento, o qualunque altra caratteristica dell'intelligenza, può essere in linea di principio descritto con tale precisione da poter essere simulato da una macchina. Si tenterà di comprendere come rendere le macchine capaci di usare il linguaggio, formare astrazioni e concetti, risolvere tipi di problemi oggi riservati all'essere umano e migliorare se stesse. Riteniamo che un progresso significativo possa essere raggiunto in uno o più di questi ambiti se un gruppo accuratamente selezionato di scienziati vi lavorerà insieme per un'estate» (J. McCarthy, M.L. Minsky, N. Rochester, C.E. Shannon, *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence* (August 31,

Ai suoi primordi vi erano notevoli interessi e speranze circa la realizzazione di soluzioni che potessero consentire addirittura di sostituire l'uomo nelle professioni intellettuali anziché, "semplicemente", di coadiuvarlo. Così, negli anni Sessanta si discuteva e ci si augurava che fosse possibile creare medici e giudici computerizzati capaci sia di effettuare le medesime mansioni di un essere umano, o comunque rimpiazzarne gran parte delle funzioni[7], sia di non commetterne i tipici errori. Quest'ultimo profilo, poi, era ed è particolarmente sentito, dal momento che le conseguenze di tali sbagli possono essere gravi ed irreparabili soprattutto in ambito sanitario[8]. Sul punto bisogna però considerare che, invero, è più probabile una riduzione degli errori che una loro eliminazione, in quanto i sistemi informatici possono presentare malfunzionamenti di diversa natura che spaziano dall'hardware al software; ciò anche quando vengono compiute rigorose procedure di test e di collaudo in ragione della loro crescente complessità nonché della sempre più marcata esigenza di interoperabilità e quindi di acquisire una molteplicità di input, seppur strutturati e standardizzati, da fonti diverse (e ferma restando l'obbligatorietà di procedure e sistemi di *disaster recovery* e *business continuity*). Non vi sono dubbi, comunque, circa i benefici che le nuove tecnologie possono apportare anche sotto questo profilo, purché vengano sempre fornite le adeguate garanzie di buon funzionamento dei sistemi adottati e adoperati.

Nel tempo, le definizioni di intelligenza artificiale sono andate suddividendosi in quattro categorie principali: sistemi che pensano come gli esseri umani; sistemi che agiscono come gli esseri umani; sistemi che pensano razionalmente; sistemi che agiscono razionalmente[9].

1955), oggi riportato nelle sue parti principali in «AI Magazine», 27, 4, 2006, p. 12). Cfr. anche J. McCarthy, P. Hayes, *Some philosophical problems from the standpoint of artificial intelligence*, in «Machine Intelligence», 4, 1969, pp. 463-502; A.M. Turing, *Computing Machinery and Intelligence*, in «Mind», 4, 1950, pp. 433-460; P.H. Winston, *Artificial Intelligence*, Addison Wesley, Boston (MA), 1992.

[7] In tal senso W.B. Schwartz, *Medicine and the computer: the promise and problem of change*, in «The New England Journal of Medicine», 283, 1970, pp. 1257-1264.

[8] Si pensi, a titolo esemplificativo, che da uno studio condotto negli Stati Uniti diversi anni fa è emerso che ogni anno circa 98.000 decessi avvenuti nelle strutture sanitarie statunitensi fossero imputabili ad errori umani (L.T. Kohn, J.M. Corrigan, M.S. Donaldson (eds.), *To Err is Human: Building a Safer Health System*, National Academy Press, Washington, DC, 2000).

[9] S.J. Russell, P. Norvig, *Artificial Intelligence. A Modern Approach*, 4th Edition, Pearson, Hoboken (NJ), 2020, versione ebook.

Oggi, in una prospettiva tecnica, tende a distinguersi fra IA "ristretta" o "debole", "generale" o "forte", e "Superintelligenza artificiale". Più specificatamente, nel caso della IA "ristretta" (*Artificial Narrow Intelligence* - ANI), le competenze e capacità sono limitate e finalizzate alla esecuzione di compiti specifici. È, al momento, l'unica tipologia di IA realizzata con successo, mediante sistemi che – per quanto possano sembrare "intelligenti" – sono molto più limitati degli esseri umani, anche se in ipotesi possono essere più efficienti degli stessi nella esecuzione di compiti specifici (come una calcolatrice può essere più efficiente di un essere umano, in fin dei conti). Nell'IA "generale" (*Artificial General Intelligence* - AGI) o "forte", invece, le capacità cognitive e prestazionali sono paragonabili a quelle di un essere umano. I sistemi di IA "forte", dunque, possono pensare, capire e agire al pari degli esseri umani. Non sono stati ancora realizzati. Infine, i sistemi di "Superintelligenza artificiale" (*Artificial Superintelligence* - ASI) hanno capacità cognitive e operative sono superiori a quelle umane. Non sono stati ancora realizzati, e ciò appare ovvio, dal momento che non esistono, allo stato attuale, sistemi di IA "forte"[10].

All'IA e ai relativi sistemi bisogna guardare avendo ben presente un altro concetto cruciale: quello di agente, ossia un'entità che percepisce il suo ambiente attraverso sensori e agisce in esso mediante attuatori[11]. Vi sono diverse definizioni di agente e appare qui opportuno riprendere quella "debole" di Wooldridge e Jennings, secondo cui può sostenersi che un agente debba avere le seguenti proprietà: (a) autonomia (possibilità di operare senza il diretto intervento umano ed esercizio di un certo grado di controllo sulle proprie azioni e sul suo stadio interno), (b) abi-

[10] Si è altresì distinto fra IA "forte" e "debole" in altra prospettiva, ossia della possibilità che una macchina possa o meno avere una vera e propria coscienza. Tuttavia, «la coscienza è un qualche cosa che è qualitativamente diverso dal cervello e che si colloca fuori dal corpo. Non è dunque solo un problema di quantità di calcolo ma un problema di qualità di processo» (G. Taddei Elmi, *Informatica giuridica. Presupposti, storia, disciplina, insegnamento, esiti*, in Id. [a cura di], *Informatica giuridica*, Simone, Napoli, 2016, p. 38). Pertanto, «le macchine anche molto evolute e molto intelligenti sembrano non superare la dicotomia cosa-persona e la soglia minima di soggettività. Restano, oggi, al livello del valore» (ivi, p. 39), anche se bisogna considerare che «Diventano sempre più labili le linee di demarcazione tra naturale e artificiale, soggetto e oggetto, organico e inorganico, vita e morte» (S. Amato, *Biodiritto 4.0. Intelligenza artificiale e nuove tecnologie*, Giappichelli, Torino, 2020, p. 7).

[11] S.J. Russell, P. Norvig, *Artificial Intelligence*, op. cit..

lità sociale (capacità di comunicare con altri agenti e con esseri umani), (c) reattività (percezione dell'ambiente e capacità di reagire in un ragionevole periodo di tempo), (d) proattività (capacità di agire per il raggiungimento di un risultato e di prendere l'iniziativa)[12].

Quanto appena affermato consente di comprendere un'ulteriore classificazione: quella fra sistema intelligente monolitico e multi-agente. Nel primo opera un solo agente, nel secondo due o più (anche una molteplicità, per cui può essere estremamente complesso).

Può altresì distinguersi fra agenti che hanno componenti materiali, come i robot[13], e quelli composti esclusivamente da software (come, per l'appunto, gli agenti software). I secondi sono dunque eseguiti da sistemi informatici di diversa tipologia, per cui pur essendo immateriali necessitano di componenti materiali (ad esempio un server). Ad ogni buon conto, anche gli automi richiedono del software per poter funzionare. Ovviamente ciò non significa che l'immaterialità delle percezioni e delle azioni degli agenti software renda quest'ultime irrilevanti per il diritto, in quanto esse sono assolutamente reali e potenzialmente produttive di effetti giuridici: basti pensare al caso dei contratti conclusi via Internet, in cui è ipotizzabile che una parte contratti con un agente software senza rendersene conto.

Già queste prime considerazioni mostrano come gli agenti intelligenti impongano una riflessione continuativa e complessa, che deve essere affrontata a livello generale prima di affrontare il dominio specifico dell'informatica medica e della salute digitale. È continuativa poiché si evolvono costantemente ed è complessa per sua natura in quanto il loro studio si pone al crocevia fra l'informatica, la filosofia, l'etica e il diritto, ponendo così talune questioni cruciali in una prospettiva sia teorica sia pratica.

Innanzi tutto, tra gli agenti intelligenti si stabiliscono relazioni semi-giuridiche[14] e le loro azioni comportano conseguenze particolarmente delicate per la Società dell'informazione[15] che contribuiscono a

[12] M. Wooldridge, N.R. Jennings, *Intelligent agents: theory and practice*, in «The Knowledge Engineering Review», 10, 2, 1995, p. 116.

[13] Sulla robotica (e sul potenziamento) v. *infra*, cap. 3, par. 3.3.

[14] C. Faralli, *La filosofia del diritto contemporanea*, Laterza, Roma-Bari, 2012, p. 81.

[15] Ciò avviene «perché il tramite della comprensione tra l'uomo e la macchina è un significato oggettivato, una struttura formale: *una forma, non una volontà,* una particolare informazione, ed in questa forma *adeontica* è necessario chiedersi che cosa vi sia di giuridico, oppure che cosa diventi un diritto distaccato dalla volontà diretta all'altrui compor-

far evolvere in Società algoritmica; bisogna quindi chiedersi preliminarmente se sia possibile o meno conferire soggettività giuridica agli agenti medesimi e, anche in caso di risposta negativa, è necessario comprendere se siano sostenibili la sussistenza e la rilevanza di stati cognitivi in capo ad essi, nonché cosa comporti la considerazione della prevedibilità o dell'imprevedibilità delle loro condotte.

Non v'è dubbio che, indipendentemente dalla prospettiva adottata, il primo scoglio sia comprendere in quali casi ci si trovi dinanzi a un sistema intelligente così da delineare una potenziale risposta del diritto alle problematiche che derivano dal loro utilizzo e che dovrebbero essere oltretutto equilibrate dai benefici che arrecano, ma senza che ciò comporti un contrasto con l'utilità sociale (per riprendere l'espressione dell'art. 41, comma 1, Cost.).

Sul punto, la risposta può essere fornita facendo ricorso alla definizione, prima menzionata, di Wooldridge e Jennings, valutando così, in ciascun caso concreto se il sistema di riferimento rispetti i requisiti ivi delineati[16] e possa dunque essere ritenuto "intelligente", fermo restando che ciò che accade nell'ambito di tali sistemi non sia ontologicamente paragonabile a ciò che accade nella mente umana: non è una inafferrabilità metafisica, bensì un prodotto artificiale del connubio fra tecnica e diritto.

Allo stato, non pare né opportuno né sostenibile attribuire una vera e propria soggettività giuridica agli agenti software e ai robot, cui dovrebbe poi conseguire il riconoscimento di diritti di varia tipologia e che potrebbe altresì portare a una deresponsabilizzazione dei loro utilizzatori o comunque di chi fruisce degli effetti positivi delle relative azioni, aprendo la strada alla creazione di veri e propri "capri espiatori digitali". Come sostiene Paolo Moro, del resto, attualmente gli automi non sono in grado di riprodurre o formalizzare quello specifico procedimento mentale, ossia l'intuizione intellettuale, che identifica la capacità del pensiero umano di cogliere una cosa; in altri termini, di vederla come qualcosa di intero pur

tamento» (F. Romeo, *Il dato digitale e la natura delle cose*, in A. Ballarini (a cura di), *Diritto interessi ermeneutica*, Giappichelli, Torino, 2012, pp. 102-103).

[16] Questa nozione è infatti generale, ma allo stesso tempo chiara e specifica nei suoi elementi essenziali che colgono proprio le principali peculiarità di questi agenti e, loro tramite, dei sistemi in cui essi sono adoperati. Appare inoltre comprensibile anche per chi non è dotato di particolari competenze informatiche, anche se poi la sua applicazione ai casi concreti richiede l'apporto di persone dotate di competenze specialistiche.

prescindendo da un procedimento logico di tipo dimostrativo. Questa abilità è ben nota sin dalla filosofia classica, come dimostra quanto affermato da Aristotele nella *Metafisica* (XII, 9, 1075a), ma è frutto di un'attività non discorsiva bensì intuitiva ed essendo priva di procedimento logico non è formalizzabile e quindi non pare essere riproducibile da un elaboratore elettronico. A quest'ultimo, inoltre, manca la comprensione del ragionamento meccanico che svolge. Emerge, qui, tutta la distanza fra sintassi e semantica. In ultima istanza, vi è il problema dell'attuale impossibilità, per il robot, di riprodurre l'attività della coscienza che rappresenta criticamente sé stessa: l'attività dell'autentica filosofia è proprio caratterizzata da essa, che si pone alla radice di qualsiasi pensiero[17].

È tuttavia opportuno tenere viva la discussione su questa tematica, poiché permette di costruire progressivamente i fondamenti teorici che consentono di definire quegli strumenti concettuali necessari per affrontare adeguatamente le sfide che la società tecnologica costantemente pone, quanto meno dal punto di vista etico[18].

Nonostante non sembri possibile attribuire personalità giuridica agli agenti intelligenti, è invece ipotizzabile, ancorché difficilmente praticabile, l'individuazione in essi di capacità cognitive così da prenderne in considerazione elementi soggettivi attribuiti in via immediata agli stessi e in via mediata al loro utilizzatore o a chi ne ha un controllo esclusivo o comunque determinante nella effettuazione di una determinata condotta. Tale questione appare rilevante dal momento che le conseguenze giuridiche di una condotta derivano spesso dalla sussistenza dell'elemento soggettivo del dolo o della colpa[19], ma si pone il problema di una società tecnologica

[17] P. Moro, *Libertà del* robot*? Sull'etica delle macchine intelligenti*, in R. Brighi, S. Zullo (a cura di), *Filosofia del diritto e nuove tecnologie. Prospettive di ricerca tra teoria e pratica*, Aracne, Roma, 2015, pp. 530-532

[18] Sul punto appare opportuno menzionare l'opera di Luciano Floridi, con particolare riferimento ai suoi scritti: *Infosfera. Etica e filosofia nell'età dell'informazione*, tr. it., Giappichelli, Torino, 2009; *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, tr. it., Raffaello Cortina, Milano, 2017; *Pensare l'infosfera. La filosofia come design concettuale*, tr. it., Raffaello Cortina, Milano, 2020 (versione ridotta, comprendente l'introduzione, i primi quattro capitoli e la postfazione, di *The Logic of Information. A Theory of Philosophy as Conceptual Design*, Oxford University Press, Oxford, 2019).

[19] Francesco Romeo evidenzia che vengono spesso negate capacità cognitive ai robot o agli agenti software utilizzando un criterio che più rigoroso di quello adoperato per valutare quelle umane. Nondimeno, la scienza non ha ancora compreso pienamente in base a quali regole le persone reagiscono agli stimoli, fra cui quelli linguistici, mentre le regole

sempre più caratterizzata da una esplosione di entità che, pur non essendo dei soggetti di diritto, la plasmano eseguendo autonomamente una molteplicità di algoritmi e prendendo decisioni in applicazione di direttive comunque previste, anche molto remotamente, dall'uomo.

In breve: agiscono come soggetti e non come oggetti o come cose, ma rientrano nella categoria dei secondi e non dei primi (anche qualora siano immateriali, come gli agenti software).

Bisogna dunque comprendere come regolamentare le "condotte" di tali entità e i relativi effetti: in tal senso, appare opportuno attribuire maggiori obblighi in capo al loro utilizzatore, indipendentemente dalla possibilità di prevedere o meno le azioni degli agenti intelligenti. L'imprevedibilità[20], infatti, potrebbe essere invocata da fornitori di prodotti e servizi intelligenti quale circostanza per esimersi da responsabilità, soprattutto in sistemi e in ambienti in cui questi interagiscono con agenti umani che intervengono parallelamente a quelli software, per modificarne od orientarne il funzionamento (o perché ci si trova in ambienti 'misti'), anche se la finalità principale dell'utilizzo di un sistema intelligente dovrebbe essere proprio quella di evitare l'intervento umano o comunque di limitarlo il più possibile. Insorge comunque il problema della stratificazione di apporti paralleli e magari contemporanei in sistemi e ambiti assai articolati e in continua modificazione, cui si aggiunge il possibile cambiamento della base di conoscenza di ciascun agente (grazie alle tecniche di apprendimento automatico o ad aggiornamenti manuali).

secondo cui i programmi rispondono a chi interagisce con loro possono ritenersi conosciute o conoscibili. Eppure, la maggior parte delle opinioni negative riposa su questa differenza e presunzione, per cui anche sotto questo profilo sarebbe necessaria una riflessione più incisiva (F. Romeo, *Il dato digitale e la natura delle cose*, cit., p. 96). Una simile impostazione "restrittiva" trova la sua ragion d'essere nella delicatezza della problematica, anche per le conseguenze a cascata che si avrebbero su ciascun ordinamento giuridico: basti pensare alla già citata del riconoscimento della titolarità di una serie di diritti in capo ad essi.

[20] Può distinguersi fra imprevedibilità teorica e pratica. La prima discende dalla considerazione che la combinazione della complessità degli agenti software e degli ambienti rende molto difficile, se non impossibile, una previsione accurata del loro comportamento. La seconda è dovuta al fatto che dedicare le proprie energie all'esatta previsione del comportamento dell'agente sarebbe in contraddizione con il fine di delegare ad esso i compiti cognitivi connessi all'attività svolta (G. Sartor, *Gli agenti software e la disciplina giuridica degli strumenti cognitivi*, in «Il diritto dell'informazione e dell'informatica», 1, 2003, p. 62).

Sul punto, è interessante notare come già i sistemi attuali siano oramai caratterizzati da modalità sempre più evolute di apprendimento automatico, che consentono di "imparare facendo" e di modificare la propria condotta dinanzi a fattispecie analoghe o addirittura uguali proprio grazie all'esperienza accumulata. Bisogna però considerare che un sistema risponde pur sempre a delle regole stabilite da chi ne ha il controllo: a differenza dell'essere umano, non ha il libero arbitrio, che potrà al limite essere "emulato" grazie a sofisticati algoritmi, ma che tale rimarrà: pertanto, le scelte saranno comunque riferibili a chi ne ha strutturato la logica, implementandola poi nei software eseguiti dagli agenti medesimi, o comunque a chi ha la titolarità dei diritti sul sistema medesimo (che poi, in caso di illeciti contrattuali o aquiliani di terze parti, potrà rivalersi sulle medesime).

Un quadro, dunque, che già appare estremamente complesso in linea generale e che lo è ancor di più in riferimento all'ambito sanitario, che per sua natura coinvolge diritti fondamentali che costituiscono oltretutto un presupposto per l'esercizio di altri diritti (non solo, ovviamente, il diritto alla vita e alla salute, ma anche il diritto alla privacy e alla protezione dei dati personali, ad esempio).

La ricerca in questo settore è sostanzialmente parallela a quella, più in generale, sulla IA, ivi incluse le illusioni e le disillusioni cui ha poi fatto seguito una vera e propria esplosione. Più specificatamente, gli studi sull'applicazione dell'IA alla medicina sono stati avviati già all'inizio degli anni Settanta[21], ma senza giungere nel breve termine allo sviluppo di applicazioni realmente utili e intelligenti, il che aveva fatto sorgere numerosi dubbi proprio su tali studi prima che, sul medio e lungo termine, la situazione si ribaltasse: il che è, oggi, un fatto notorio.

Rimane però attuale quanto già sostenuto sul finire degli anni Ottanta, per cui nonostante la progressiva informatizzazione della società e dei settori sanitari e giuridici, dottori e giudici non sono stati (ancora) sostituiti da sistemi informatici o da automi come si sarebbe prospettato in un racconto di fantascienza[22], ancorché i passi in avanti siano oramai

[21] Cfr. P. Szolovits (ed.), *Artificial Intelligence in Medicine*, Westview Press, Boulder, 1982.

[22] W.B. Schwartz, R.S. Patil, P. Szolovits, *Artificial Intelligence in Medicine. Where Do We Stand?*, in «The New England Journal of Medicine», 316, 1987, p. 685. Negli anni si è riacceso il dibattito sulla giustizia algoritmica, in merito a cui cfr. A. Garapon, J.

numerosi. La dottrina si è così interrogata sulle cause di questa mancata rivoluzione, ripercorrendo altresì le esperienze svolte in modo da apprendere dagli errori del passato e non riproporli nello sviluppo delle nuove applicazioni. Invero, tali ipotesi appaiono avveniristiche anche in relazione allo stato attuale della tecnologia: più che attraverso una rivoluzione, pare che l'informatizzazione possa e debba avvenire seguendo più fasi[23], che possono anche essere estremamente brevi.

Difatti, la prassi medica e non (basti pensare ai dispositivi indossabili e al loro impatto sull'ambito della salute) mostra come le applicazioni dell'intelligenza artificiale trovino un'applicazione sempre più vasta, giungendo addirittura all'utilizzo di robot operanti in domini specializzati[24], nell'ambito, però, di un generale senso di deresponsabilizzazione alimentato dalla semplice possibilità tecnica di "realizzare qualcosa", soprattutto in ordine alla valutazione della liceità, e talvolta della opportunità, dell'obiettivo prescelto[25].

Oggi, poi, da un lato pare riemergere quel medesimo timore circa la presumibile eccessiva intelligenza dei sistemi informatici[26], dopo che per

Lassègue, *Justice digitale: révolution graphique et rupture anthropologique***,** Presses Universitaires de France, Paris, 2018.

[23] T. Bodenheimer, K. Grumbach, *Electronic Technology. A Spark to Revitalize Primary Care?*, in «Journal of the American Medical Association», 2, 2003, p. 263.

[24] A titolo esemplificativo, può qui citarsi il robot chirurgico "da Vinci" (sul punto cfr., in particolare, il paragrafo 4.2, "The Artificial Doctor", in U. Pagallo, *The Laws of Robots. Crimes, Contracts, and Torts*, Springer, Dordrecht, 2013, p. 88 e ss.).

[25] In questo senso T. Serra, *L'uomo programmato*, cit., pp. 97-98. Del resto, «le macchine e le tecnologie che in esse trovano applicazione non stanno soltanto mantenendo le loro promesse, ma sono andate ben oltre quanto si potesse ragionevolmente immaginare. Sta comunque all'Uomo mantenere la parola data ai propri simili, perché la contropartita del macchinico non diventi un alibi per sfruttare l'umano. Questo è forse l'unico modo in cui l'Intelligenza Artificiale potrà dirsi, senza eccessivi timori, meritevole della nostra *fiducia*» (M. Saporiti, *Questioni di "intelligenza politica". Prospettive europee in materia di Intelligenza Artificiale e di proceduralità algoritmica*, in «Notizie di Politeia», 143, 2021, p. 99).

[26] Ad esempio, in riferimento all'applicazione automatica del diritto, al centro delle discussioni dei giuristi e degli informatici non si poneva tanto l'impossibilità pratica quanto la sua stratta non desiderabilità. Così, Spiros Simitis non dubitava della possibilità di giungere ad un'applicazione automatica del diritto o, comunque, di un'analisi delle future decisioni dei giudici sulla base della giurisprudenza preesistente, ma piuttosto della sua intrinseca necessità, poiché potrebbe irrigidire l'attività giudiziaria sostanziandosi in un controllo sulla medesima per verificare se i giudici si siano attenuti o meno alle norme vigenti e ai precedenti giurisprudenziali (S. Simitis, *Crisi dell'informazione giuridica ed elaborazione elettronica dei dati*, tr. it., Giuffrè, Milano, 1977, p. 110).

diverso tempo ci si era concentrati sulla loro mancanza di intelligenza, e dall'altro, in linea generale, permangono le paure di un loro potenziale utilizzo per fini illeciti. Ovviamente ciò comporterà una sempre maggior attenzione verso la definizione del concetto di intelligenza, poiché da esso discendono numerose altre considerazioni, pur se nella difficoltà – o nella impossibilità – di trovare una risposta univoca, il che non potrà che giovare alla discussione in materia.

Si delinea, così, l'orizzonte di una «medicina algoritmica»[27], che vede dunque un ulteriore attore (per quanto *sui generis*) emergere nel, e progressivamente pervadere il, complesso mondo della salute: l'algoritmo.

Sul punto è doveroso premettere che «un elaboratore elettronico può svolgere solo compiti che siano riducibili a un algoritmo: un algoritmo è una sequenza di prescrizioni o "istruzioni" che indica in modo preciso e non ambiguo i passi da compiere per risolvere correttamente, a partire da determinate informazioni, un certo tipo di problema (se una soluzione esiste), in un tempo finito»[28].

Così, vi sono algoritmi capaci di apprendere regole decisionali da dati nonché di migliorare le loro prestazioni in modo automatico sulla base dell'esperienza accumulata e i sistemi complessi che vengono realizzati possono prendere decisioni anche in situazioni di incertezza, effettuando delle scelte alla luce di molteplici fattori che però vengono, almeno in linea generale, predeterminati algoritmicamente.

La comune esperienza, però, mostra come talora la crescente complessità dei sistemi informatici venga utilizzata dai loro produttori o dai prestatori dei servizi resi a mezzo degli stessi quale elemento che li porta a considerarli "altri" rispetto a loro, salvo poi trarne i rilevanti benefici patrimoniali che ne conseguono. Ciò assume particolare rilevanza in caso di decisioni erronee, o comunque di errori del sistema automatico.

Non v'è dubbio che in ambito sanitario le conseguenze di uno o più errori possono essere addirittura catastrofiche, come nel caso di un

[27] Cfr. altresì il capitolo 3, par. 3.5, sulla medicina personalizzata e sulla medicina di precisione.

[28] G. Sartor, *Le applicazioni giuridiche dell'intelligenza artificiale. La rappresentazione della conoscenza*, Giuffrè, Milano, 1990, p. 5. Per una disamina critica su algoritmi e diritto si vedano, tra gli altri, A. Avitabile, *Il diritto davanti all'algoritmo*, in «Rivisita italiana per le scienze giuridiche», 8, 2017, pp. 313-325; M. Faioli, *Mansioni e macchina intelligente*, Giappichelli, Torino, 2019; N. Lettieri, *Antigone e gli algoritmi. Appunti per un approccio giusfilosofico*, Mucchi, Modena, 2020.

macchinario di radioterapia (il "Therac 25") i cui difetti nel software di gestione provocarono, a metà degli anni Ottanta, gravi lesioni e in alcuni casi addirittura la morte di diversi pazienti[29]. Oltretutto, tanto più un programma informatico è complesso quanto più alte sono le possibilità che esso contenga degli errori che possano provocarne malfunzionamenti o addirittura blocchi, per quanto la situazione sia comunque abbastanza confortante.

Pertanto, oggi, le procedure di test e di monitoraggio sono sempre più accurate e inoltre, nonostante l'informatizzazione delle strutture sanitarie sia sempre più diffusa e pervasiva, non si sono verificati eventi particolarmente catastrofici. Ovviamente ciò non significa che non si siano verificati incidenti, malfunzionamenti od errori, bensì evidenzia come le problematiche sinora riscontrate non abbiano impedito il progresso tecnologico in materia, come dimostrano, ad esempio, gli avanzamenti nell'ambito della chirurgia robotica. Inoltre, da tempo i sistemi esperti[30] possono essere utilizzati in ambito medico per la diagnosi, la prognosi, la terapia (e già negli anni Settanta il sistema esperto denominato MYCIN aveva dato ottimi risultati, seppur non perfetti[31]).

Successivamente, però, sistemi simili non hanno trovato utilizzi efficaci nella pratica medica per diversi fattori, di cui alcuni di carattere etico e giuridico inerenti già al fatto stesso di affidare, in tutto o in parte, decisioni sulla diagnosi, la prognosi o la terapia di una persona umana ad una macchina. Ovviamente tale problema risulta amplificato qualora la macchina effettui la c.d. "chiusura del *loop*", ossia sia in grado di prendersi cura del paziente sotto tutti i punti di vista.

Altri problemi sono stati rinvenuti, anche più in generale, nella incapacità dei sistemi esperti "tradizionali" di fornire consistentemente riposte complete e relative ai casi concreti nonché nella difficoltà dell'ampliamento e dell'aggiornamento della loro base di conoscenza, adoperata dal motore inferenziale per rispondere ai quesiti. I già citati metodi di

[29] Cfr. N. Leveson, C.S. Turner, *An Investigation of the Therac-25 Accidents*, in «IEEE Computer», 7, 1993, pp. 18-41.

[30] I sistemi esperti sono dei sistemi informatici basati su un modello del comportamento intelligente, in grado di effettuare attività che richiedono particolari competenze o cognizioni (G. Sartor, *Intelligenza artificiale e diritto. Un'introduzione*, cit., p. 22).

[31] V.L. Yu *et al.*, *An Evaluation of MYCIN's ADVICE*, in B.G. Buchanan, E.H. Shortliffe (eds.), *Rule-Based Expert Systems: The MYCIN Experiments of the Stanford Heuristic Programming Project*, Addison Wesley, Reading (MA), 1984, pp. 589-596.

apprendimento automatico hanno permesso di fare un salto di qualità, poiché grazie ad essi alla macchina viene fornito un metodo di apprendimento che viene applicato dalla stessa ai dati cui ha accesso[32].

In tutti i casi, comunque, si pongono delicate questioni in ordine all'imputazione della responsabilità per eventuali difetti presenti in tali sistemi cui conseguano eventi dannosi anche qualora siano utilizzati sotto la supervisione di personale esperto (tanto che ancor oggi in dottrina si evidenzia la necessità di non ridurre in nessun caso la figura del professionista sanitario a mero esecutore o intermediario di eventuali sistemi di supporto alle decisioni in ambito clinico, pur se avanzatissimi)[33], e in tal senso è anche la recente l. 132/2025 che armonizza l'ordinamento giuridico italiano al Regolamento (UE) 2024/1689 (il c.d. AI Act). Più specificatamente, i commi 5 e 6 dell'art. 7 dispongono, rispettivamente, che «i sistemi di intelligenza artificiale in ambito sanitario costituiscono un supporto nei processi di prevenzione, diagnosi, cura e scelta terapeutica, lasciando impregiudicata la decisione, che è sempre rimessa agli esercenti la professione medica» e che «i sistemi di intelligenza artificiale utilizzati in ambito sanitario e i relativi dati impiegati devono essere affidabili, periodicamente verificati e aggiornati al fine di minimizzare il rischio di errori e migliorare la sicurezza dei pazienti», andando nella medesima direzione indicata nel 2020 dal Comitato Nazionale per la Bioetica e dal Comitato Nazionale per la Biosicurezza, le Biotecnologie e le Scienze della Vita[34].

Qualora in futuro dovessero comunque essere sviluppati e adoperati sistemi che chiudono il *loop*, ove ciò dovesse essere consentito dalla normativa vigente, sarà necessario evitare che si verifichino una sperso-

[32] G. Sartor, *Introduzione al focus su "L'intelligenza artificiale e il diritto"*, in «Rivista di filosofia del diritto», 1, 2020, pp. 66.

[33] In tal senso F. Lagioia, G. Contissa, *The strange case of Dr. Watson: liability implications of AI evidence-based decision support systems in health care*, in «European Journal of Legal Studies», 2, 2020.

[34] «L'IA va considerata esclusivamente come un aiuto nelle decisioni del medico, che rimangono controllate e supervisionate dall'uomo. Resta compito del medico, in ogni caso prendere la decisione finale, in quanto la macchina fornisce solo ed esclusivamente un supporto di raccolta e analisi dei dati, di natura consultiva. Un sistema di "assistenza cognitiva automatizzata" nella attività diagnostica e terapeutica non è un "sistema decisionale autonomo". Esso effettua la raccolta di dati clinici e documentali, li confronta con statistiche relative a pazienti simili, accelerando il processo di analisi del medico» (Comitato Nazionale per la Bioetica-Comitato Nazionale per la Biosicurezza le Biotecnologie e le Scienze della Vita, *Intelligenza artificiale e medicina: aspetti etici*, Roma, 2020, p. 10).

nalizzazione e una "disumanizzazione" della medicina, dal momento che il rapporto umano che si stabilisce fra medico e paziente può assumere un'importanza fondamentale per quest'ultimo e il rapporto medico elettronico-paziente ne costituirebbe un surrogato fortemente impoverito in quanto privo di ogni traccia di umanità e di coscienza, anche ove "imitata" e appresa (grazie alle tecniche di *machine learning*) dalle macchine.

Si è del resto osservato che l'assunto dell'IA è un'epistemologia riduzionista per cui l'intelligenza umana può essere ridotta ad algoritmi, quali serie finite di elementi matematici (algoritmi), in una prospettiva che dimentica considerare che l'essere umano e le sue azioni derivano da una complessità di fattori e non quale mero risultato di una determinazione causale dovuta a stimolazioni biochimiche o neurofisiologiche, o dovuta a condizioni socio-ambientali esterne. Tali fattori includono la libertà personale, la consapevolezza di sé e l'intenzionalità, oltre che la razionalità e il calcolo. Un sistema di questo tipo dovrebbe dunque essere definito «sistema di cognizione calcolante artificiale», dotata di «autonomia operativa» mediante algoritmi predittivi, meramente funzionale relativamente allo svolgimento di compiti in aree predeterminate, dotato di tecnologie più o meno avanzate grazie alle quali ha un'autonomia più o meno ampia[35].

Dinanzi a sfere notoriamente e intuitivamente tanto complesse e variegate, e non sempre algoritmizzabili, appare dunque chiaro il ruolo ancillare della "medicina algoritmica" (e della "salute algoritmica", come risultato delle elaborazioni e delle "azioni" dell'IA sul corpo elettronico), che può essere di supporto a quella tradizionale, senza poterla però sostituire in tutti quei casi in cui entrano in gioco le relazioni interpersonali. Nello stesso senso anche quanto autorevolmente affermato dal Comitato Nazionale per la Bioetica e dal Comitato Nazionale per la Biosicurezza, le Biotecnologie e le Scienze della Vita, secondo cui pare auspicabile l'uso di macchine intelligenti e robot in medicina, qualora più efficienti, precisi, rapidi e meno costosi, per la sostituzione dell'uomo nello svolgimento di attività ripetitive, noiose, pericolose, umilianti o faticose, automatizzando le attività burocratiche, di mera routine, o che espongono i profes-

[35] L. Palazzani, *Tecnologie dell'informazione e intelligenza artificiale. Sfide etiche al diritto*, cit., p. 54.

sionisti a pericoli evitabili: ciò consentirà un'aumentata disponibilità di tempo da dedicare ai pazienti oltre alla riduzione dei rischi[36].

In ogni caso, la diffusione di strumenti informatici intelligenti nell'ambito della sanità mostra la necessità di costruire un *framework* legale ponendo dei limiti chiari e invalicabili, così da garantire effettivamente la dignità umana pur promuovendo lo sviluppo di nuove tecnologie che potrebbero avere un impatto benefico sui diritti alla vita e alla salute, e in generale sul benessere psico-fisico delle persone. Questa esigenza è oramai fortemente avvertita già in relazione all'IA *tout court*[37], anche se la risposta dei vari legislatori rimane tuttora inadeguata e tardiva.

In tale quadro, complesso e in divenire anche per ciò che concerne i profili applicativi, si colloca proprio il regolamento (UE) n. 2024/1689 (AI Act), che appare tuttavia essere una normativa estremamente farraginosa. Non è questa la sede per una sua approfondita disamina[38], ma può qui evidenziarsi che il legislatore europeo ha scelto di disciplinare l'IA nella prospettiva dei suoi prodotti, ossia dei «sistemi di IA»[39] – sistemi

[36] Comitato Nazionale per la Bioetica-Comitato Nazionale per la Biosicurezza le Biotecnologie e le Scienze della Vita, *Intelligenza artificiale e medicina: aspetti etici*, cit., pp. 9-10.

[37] Del resto, per affrontare il "livello 4.0" della realtà attuale («le cui direttrici di sviluppo sono dettate dall'interazione tra uomo e macchina (interfacce, realtà aumentata) e dall'uso e dall'analisi dei dati (big data, open data, Internet of Things, machine-to-machine, cloud computing, machine learning) bisogna che etica e diritto muovano dalla fondamentale distinzione tra scienza e pseudo-scienza, tra fatti e opinioni, e al contempo diano ampio spazio a quella ricerca di base che ha quale primo obiettivo l'avanzamento della conoscenza e la comprensione teorica delle diverse variabili in un determinato processo. Una ricerca, questa, che fornisce le fondamenta per ulteriori ricerche e che di solito non ha un particolare scopo pratico, sebbene i suoi risultati possano avere e abbiano delle ricadute applicative» (A.C. Amato Mangiameli, *Algoritmi e big data. Dalla carta sulla robotica*, in «Rivista di filosofia del diritto», 1, 2019, pp. 122-123).

[38] La letteratura in materia è oramai molto ampia. Cfr., fra gli altri: F. Donati, G. Finocchiaro, O. Paolucci, O. Pollicino (a cura di), *La disciplina dell'intelligenza artificiale*, Giuffrè, Milano, 2025; M. Iaselli (a cura di), *AI Act. Principi, regole ed applicazioni pratiche del Reg. UE 1689/2024*, Maggioli, Santarcangelo di Romagna, 2024; M. Punzi, *L'Artificial Intelligence Act dell'Unione Europea*, in «Rassegna dell'Arma dei Carabinieri», 2, 2024, pp. 79-89; G. Taddei Elmi, A. Contaldo (a cura di), *Intelligenza artificiae. AI Act, Regolamento (UE) 1689/2024: il nuovo scenario giuridico europeo*, Pacini, Pisa, 2024.

[39] Ai sensi dell'art. 3(1), è «un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali».

informatici, ancorché caratterizzati dalla peculiarità di essere "intelligenti". I sistemi vengono distinti e disciplinati in base al rischio che pongono: inaccettabile, alto, limitato e minimo. I primi sono vietati, i secondi sono sottoposti a determinate regole che divengono assai meno stringente per i terzi; i quarti non sono sottoposti a regole ulteriori, fatta salva l'adesione volontaria a codici di condotta. I sistemi di IA che costituiscono componente di sicurezza di un dispositivo medico o di un dispositivo medico-diagnostico in vitro, oppure che sono essi stessi il prodotto, sono considerati "ad alto rischio".

A valle di tale inquadramento, e in particolare per i sistemi "ad alto rischio" impiegati nella salute, si impone un corollario etico-giuridico di particolare rilevanza: la spiegabilità degli output e dei processi decisionali[40], quale condizione di legittimità delle decisioni e di corretta imputazione della responsabilità. La possibilità di conoscere i relativi ragionamenti svolti sino ad oggi è stata negata o sostanzialmente celata dall'oscurità e dall'opacità[41] dei codici informatici eseguiti dalle «scatole nere»[42] che pervadono la Società algoritmica, nonostante talune aperture sul punto grazie alla normativa in materia di protezione dei dati personali[43]. Più specificatamente, il requisito della, e la pretesa alla, spiegabilità, è relativo a qualsiasi sistema informatico intelligente e diviene tanto più importante quanto più esso costituisca una infrastruttura essenziale (ad esempio perché permette di reperire informazioni, in particolare ma non esclusivamente sanitarie) o comunque fornisce servizi essenziali o molto importanti per la Società dell'informazione o algoritmica[44], sia per evita-

[40] Il dibattito è oramai crescente. Cfr., fra gli altri, L. Floridi *et al.*, *AI4People – An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations*, in «Minds and Machines», 28, 2018, pp. 689-707 (in una prospettiva più generale su un *framework* etico per la Società dell'informazione, nel cui ambito assume rilievo esplicito la spiegabilità); U. Pagallo, *Algoritmi e conoscibilità*, in «Rivista di Filosofia del diritto», 1, 2020, pp. 93-106; M. Palmirani, Big data *e conoscenza*, in «Rivista di Filosofia del diritto», 1, 2020, pp. 73-91.

[41] Sulla opacità dei sistemi informatici sia consentito rinviare a G. Fioriglio, *Opacità dei sistemi intelligenti e sicurezza informatica: un difficile equilibrio fra regolazione e tecno-regolazione*, in «Rivista elettronica di Diritto, Economia, Management», 3, 2016.

[42] Cfr. F. Pasquale, *The Black Box Society. The Secret Algorithms That Control Money and Information*, Harvard University Press, Cambridge-London, 2015.

[43] V. *infra*, par. 3.

[44] Si pensi, in particolare, al settore dei motori di ricerca web (sempre più importante anche per il reperimento di informazioni aventi rilevanza per l'ambito della salute

re decisioni arbitrarie sia per una corretta e precisa imputazione e graduazione della responsabilità. Esso, inoltre, non può che essere obbligatorio nell'ambito della salute, ove è necessario che qualsiasi decisione e qualsiasi attività possa essere spiegata e giustificata[45].

II.3. Privacy, protezione dei dati personali, consenso

Il diritto alla privacy e alla protezione dei dati personali si caratterizza per la sua trasversalità e per la sua centralità nel settore della salute in generale e nell'informatica medica in particolare, poiché la quasi totalità dei rispettivi profili teorico-pratici ne richiede una considerazione e una esigenza di tutela più o meno marcate a seconda dei casi (che, a sua volta, richiede una riflessione circa la confidenzialità dei dati e la sicurezza dei sistemi).

È bene premettere che di questo diritto si individuano tradizionalmente un ambito negativo (e passivo) e uno positivo (e attivo), seguendo l'evoluzione concettuale e fattuale in materia (la sua nozione è, del resto, «specificamente flessibile, reattiva e sensibile ai cambiamenti»[46]): il primo è caratterizzato dalla pretesa di non subire ingerenze nella propria sfera privata, di "essere lasciati soli" secondo l'originaria concettualizzazione di Samuel D. Warren e Louis D. Brandeis[47], mentre il secondo dalla facoltà di controllare i propri dati personali, di potersi autodeterminare.

[su cui v. *infra*, par. 2.5]), che oggi sono stati affiancati proprio da servizi "intelligenti" come ChatGPT cui rivolgersi per avere risposte senza cercare sul web. Sul punto sia consentito rinviare a G. Fioriglio, *La "dittatura" dell'algoritmo: motori di ricerca web e neutralità della indicizzazione. Profili informatico-giuridici*, in «Bocconi Legal Papers», 5, 2015, pp. 113-139.

[45] Ciò appare ancor più evidente ove si consideri che «l'assistenza medica comporta anche grandi interessi economici, pertanto l'IA può essere orientata, attraverso la costruzione degli algoritmi, ad influenzare in vari modi le decisioni del medico ad esempio facilitando le prescrizioni attraverso un aumento o una diminuzione dei valori di normalità per una serie di parametri funzionali o biochimici» (Comitato Nazionale per la Bioetica-Comitato Nazionale per la Biosicurezza le Biotecnologie e le Scienze della Vita, *Intelligenza artificiale e medicina: aspetti etici*, cit., p. 12).

[46] V. Colomba, G. Zanetti, *Aspetti problematici della nozione di privacy da un punto di vista filosofico-giuridico*, in «Teoria e critica della regolazione sociale», 1, 2017, p. 29.

[47] S.D. Warren, L.D. Brandeis, *The right to privacy*, in «Harvard Law Review», 4, 1890, pp. 193-220. Cfr. S. Scoglio, *Privacy: diritto, filosofia, storia*, Editori Riuniti, Roma, 1994.

Il tutto è stato perfettamente evidenziato da Stefano Rodotà, che ha individuato, da un lato, le specifiche tendenze evolutive consistenti nel «diritto di mantenere il controllo sulle proprie informazioni» e nel «diritto all'autodeterminazione informativa»; dall'altro, i passaggi fondamentali «dalla privacy alla non discriminazione» e «dalla segretezza al controllo»[48]. Inizialmente, infatti, la privacy «è stata costruita come un dispositivo "escludente", come uno strumento per allontanare lo sguardo indesiderato. Ma l'analisi delle sue definizioni mostra anche le sue progressive trasformazioni, che hanno fatto emergere un diritto sempre più finalizzato a rendere possibile la libera costruzione della personalità, l'autonomo strutturarsi dell'identità, la proiezione nella sfera privata dei principi fondamentali della democrazia»[49], fermo restando che, negli ordinamenti continentali, il diritto alla riservatezza è normalmente considerato un diritto fondamentale e inviolabile[50].

Ciò nonostante, esso è costantemente violato e in pericolo nella Società dell'informazione e nella Società algoritmica: del resto, basti pensare che, in un'epoca estremamente meno tecnologica e informatizzata di quella contemporanea, già la creazione di elaboratori elettronici più sofisticati e di banche dati contenenti dati personali aveva spinto diversi legislatori, sin dagli anni Settanta, a disciplinare questo ambito a causa dei potenziali rischi per le libertà e i diritti delle persone fisiche le cui informazioni personali venivano trattate (e non a caso si parlava di "privacy informatica").

Questi rischi, oggi, sono ben maggiori in una società che è addirittura pervasa dall'informatica e ciò vale, a maggior ragione, per lo specifico dominio della salute, in cui vengono comunemente trattate informazioni particolarmente delicate che spaziano da quelle idonee a rivelare determinate patologie a quelle genetiche. Il loro trattamento è tuttavia necessario ed è sempre più digitale; è bene precisare che una originaria problematica etico-giuridica, che può dirsi oggi superata, consisteva nella discussione cir-

[48] Sul punto, anche per i relativi approfondimenti, cfr. S. Rodotà, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in «Rivista critica del diritto privato», 1997, p. 589.

[49] S. Rodotà, *Il diritto di avere diritti*, Laterza, Roma-Bari, 2012, p. 320.

[50] Per una lettura dell'evoluzione del diritto alla riservatezza anche alla luce dell'avvento della rivoluzione informatica, nonché per una discussione dell'impatto dell'informatica medica su tale diritto, sia consentito rinviare a G. Fioriglio, *Il diritto alla privacy. Nuove frontiere nell'era di Internet*, Bononia University Press, Bologna, 2008.

ca la possibilità stessa della informatizzazione dei dati sanitari per una serie di motivazioni, fra cui il risparmio di costi e la maggiore efficienza[51], cui si contrapponevano i timori circa potenziali utilizzi illeciti dei dati sanitari (ma come si è giustamente rilevato a suo tempo, la tutela dei dati personali non dovrebbe essere realizzata impedendo o limitando l'utilizzo dell'ICT nel settore sanitario, ma piuttosto nello sviluppo di tecnologie che consentano la protezione delle informazioni in un ambiente informatico[52]).

La rivoluzione informatica è oggi inarrestabile, per cui può darsi per acquisito che tale processo sia irreversibile, ma ciò non significa che il diritto e l'etica debbano disinteressarne e divenire ancillari rispetto all'evoluzione tecnologica: vale, piuttosto, il contrario. Essi devono perimetrare l'ambito delle nuove tecnologie e farle evolvere nel rispetto dei diritti fondamentali e inviolabili della persona, fra cui il diritto alla privacy e alla protezione dei dati personali (il cui rispetto consente, fra le altre cose, di proteggere la dignità umana). Ciò appare particolarmente importante per l'informatica medica, dal momento che essa si basa su un concetto-chiave: l'informazione, la cui confidenzialità deve essere sempre assicurata.

Per poter oggi compiutamente discutere tali profili è tuttavia necessario approfondire gli aspetti principali della normativa vigente in ambito europeo, che rileva anche sul piano teorico: offre coppie concettuali teorico-pratiche (persona/dignità; autodeterminazione/relazione; rischio/garanzia; responsabilizzazione/dimostrabilità) e principi di valutazione (necessità, proporzionalità, limitazione della finalità, minimizzazione) fondamentali anche per lo svolgimento di una riflessione che non può del tutto prescindere dal diritto positivo per non essere avulsa dalla realtà

[51] Con ovvi benefici: ad esempio, poter accedere in tempi rapidi alla storia clinica di una persona in caso di bisogno, come in caso di emergenza, può essere cruciale per salvarne la vita o comunque preservarne o ristabilire l'integrità psico-fisica. Eppure, anche in tempi recenti, addirittura ottenere la copia delle proprie cartelle cliniche e delle informazioni sanitarie poteva richiedere un processo lungo e costoso in una nazione all'avanguardia come gli Stati Uniti, dove all'elevata informatizzazione delle strutture sanitarie ed all'esplicita previsione del diritto soggettivo ad ottenere una copia dei propri dati sanitari faceva da contraltare la realtà di procedure che potevano richiedere lungo tempo per essere espletate o la fornitura di documentazione in formato cartaceo e non informatico. Sul punto sia consentito rinviare a: G. Fioriglio, P. Szolovits, *Copy Fees and Patients' Rights to Obtain a Copy of Their Medical Records: From Law to Reality*, in «Proceedings of American Medical Informatics Association Annual Symposium», 2005, pp. 251-255.

[52] National Research Council, *For the Record. Protecting Electronic Health Information*, National Academy Press, Washington, DC, 1997, p. 161.

in cui viene svolta. Oltretutto, lo studio di tale normativa offre utili spunti di critica al data-centrismo e al dataismo, mettendo la persona al centro – ancorché talune letture restrittive della normativa medesima portino all'effetto contrario, dando maggiore centralità all'interessato più che alla persona stessa, come di seguito discusso[53], con il rischio che un'eccessiva protezione dei dati personali porti alla datificazione del soggetto identificato dagli stessi costruendone un "corpo elettronico" che il diritto positivo rischia di proteggere seguendo una logica paternalistica che mina la possibilità effettiva di autodeterminazione senza riuscire a garantire un controllo effettivo sui propri dati personali. Ma, nel bene e nel male, la società contemporanea è plasmata anche da tale normativa, che delinea e disciplina il perimetro entro cui tutti i soggetti, pubblici e privati possono trattare i dati personali, in un percorso che ha visto il principale punto di partenza nella Direttiva 95/46/CE per giungere poi al Regolamento (UE) n. 2016/679 (Regolamento Generale sulla Protezione dei Dati, RGPD, o GDPR, *General Data Protection Regulation*[54]).

Il GDPR ha un ambito di applicazione molto ampio[55] e si basa su alcuni principi fondamentali: primariamente, la responsabilizzazione (*accountability)* e la *privacy by design* e *by default*. Prima di approfondirli, e per poterla compiutamente comprendere, è necessario effettuare alcuni cenni a determinati concetti fondamentali, a partire dal "trattamento": qualsiasi operazione o insieme di operazioni svolte sui dati personali[56], a

[53] V. *infra*, par. 7. Per una discussione in tal senso, sia consentito rinviare a G. Fioriglio, *Trattamento dei dati sanitari e ricerca medica: profili informatico-giuridici e istituzionali nel contesto europeo*, in «Jura Gentium», 2, 2025.

[54] Ogni Stato membro si è dotato di propria normativa di armonizzazione (nel caso dell'Italia, mediante numerose modifiche al D.lgs. 196/2003, ossia al "Codice in materia di protezione dei dati personali").

[55] Il GDPR si applica, infatti, quando viene svolto un trattamento di dati personali non solo da un titolare che abbia uno stabilimento all'interno dell'Unione europea, ma anche qualora il titolare non abbia ubicato detto stabilimento all'interno dell'Unione medesima e ciò nonostante offra prodotti o servizi (anche gratuitamente) a interessati ubicati nell'UE o comunque ove monitori il loro comportamento. Ciò consente sia di evitare l'elusione della normativa (mediante l'ubicazione degli stabilimenti al di fuori dell'Unione europea) sia di renderla comunque applicabile anche qualora non vi sia un intento elusivo ma si operi legittimamente e in buona fede anche nell'Unione europea da uno Stato terzo.

[56] Art. 4(2) GDPR: «qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati per-

loro volta definiti come «qualsiasi informazione riguardante una persona fisica identificata o identificabile ("interessato")». Queste informazioni, come autorevolmente scritto da Rodotà, costituiscono complessivamente il già citato «corpo elettronico» che va al di là del corpo e della sua fisicità[57].

Il GDPR, inoltre, tipizza alcune figure, di cui alcune già presenti nella disciplina previgente: in particolare, il titolare, il responsabile e l'interessato, cui si è aggiunto il Responsabile della protezione dei dati (RPD, meglio noto con l'acronimo inglese DPO, ossia "Data Protection Officer"[58] – è un consulente, esperto e qualificato, che affianca il titolare nella gestione delle questioni connesse al trattamento dei dati personali e che lo aiuta a rispettare la normativa vigente). Più specificatamente, il titolare è «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali[59]» (art. 4(7) GDPR). Deve avere un quadro chiaro e inequivocabile dei trattamenti effettuati e deve utilizzare tutti gli strumenti previsti dal GDPR per proteggere adeguatamente i diritti degli interessati, mettendo inoltre in atto misure tecniche e organizzative adeguate a ciascun trattamento specifico, garantendone sempre una sicurezza adeguata al relativo rischio. Possono esservi più titolari (contitolari o titolari autonomi, a seconda dei casi). Il responsabile è invece la «persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati per conto del titolare del trattamento» (art. 4(8) GDPR), mentre l'interessato è la persona fisica cui si riferiscono i dati personali. Sono inoltre previsti altri soggetti, come il

sonali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione».

[57] S. Rodotà, *Il diritto di avere diritti*, op. cit., p. 270.

[58] Sul DPO cfr. fra gli altri: R. Acciai, S. Angeletti (a cura di), *Il DPO protagonista dell'innovazione. Il responsabile della protezione dei dati tra competenze e certificazioni*, Aracne, Roma, 2019; A. Losacco, *Il responsabile della protezione dei dati (RPD): equivalente italiano del data protection officer (DPO)*, Jovene, Napoli, 2018.

[59] Ancora, «quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri» (art. 4(7) GDPR).

«destinatario»[60] e il «terzo»[61]. Devono inoltre menzionarsi gli «autorizzati», ossia le persone che compiono materialmente le operazioni di trattamento (sotto la direzione e la supervisione del titolare o del responsabile), e i «soggetti designati»[62].

Per quanto di rispettiva competenza, il titolare e il responsabile del trattamento devono rispettare il principio di *accountability* (responsabilizzazione), consistente nell'obbligo di adottare comportamenti proattivi e idonei a dimostrare di aver concretamente messo in atto misure tecniche e organizzative adeguate per garantire il rispetto di quanto previsto dal GDPR, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, riesaminando e aggiornando le suddette misure qualora ciò si renda necessario.

Inoltre, in ossequio al principio della *privacy by design* ("Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita", art. 25 GDPR), il titolare deve mettere in atto misure tecniche e organizzative adeguate (ad esempio, la pseudonimizzazione) finalizzate ad attuare in modo efficace i principi di protezione dei dati (ad esempio, la minimizzazione) e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del GDPR e tutelare i diritti degli interessati (sia in fase di progettazione sia lungo l'intero ciclo di vita del trattamento); ancora, nel rispetto del principio della *privacy by default*, il titolare deve attuare misure tecniche e organizzative adeguate affinché siano trattati, per impostazione predefinita (*by default*), solo i dati personali necessari per ogni specifica finalità del trattamento (in particolare in riferimen-

[60] «La persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi» (art. 4 (9) GDPR).

[61] «La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile» (art. 4(10) GDPR).

[62] «Il titolare o il responsabile del trattamento possono prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità» (art. 2-*quaterdecies*, comma 1, d.lgs. 196/2003). Ai sensi del successivo comma 2, «Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta».

to a quantità dei dati raccolti, estensione del trattamento, periodo di conservazione e accessibilità).

Un quadro qui appena tratteggiato, dunque, ma da cui già emerge come l'intento del legislatore europeo sia quello di obbligare qualsiasi soggetto che operi professionalmente (e che dunque tratta informazioni personali) a inserire a pieno titolo la protezione dei dati nell'ambito dei propri processi, il che ha implicazioni notevoli anche in relazione alla loro sicurezza e alla loro integrità, con la necessità di adottare tutte le cautele possibili per evitare trattamenti illeciti o comunque errati perché basati su dati inesatti.

Quanto sin qui tratteggiato costituisce la cornice entro cui si colloca il trattamento dei dati relativi alla salute, che sono ben distinti dai dati personali comuni. Per essi si intendono, infatti, «i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute» (art. 4(15) GDPR); in essi «dovrebbero rientrare tutti i dati riguardanti lo stato di salute dell'interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso» (cons. 35 GDPR)[63]. Questa tipologia di dati rientra fra le "categorie particolari" di cui all'art. 9 GDPR, che ne dispone, al par. 1, il divieto di trattamento a meno che non ricorra uno dei casi di cui al par. 2, fra i quali assumono particolare rilevanza ai fini del presente contributo soprattutto le finalità di ricerca scientifica o statistica (lett. j), che

[63] Ancora, «questi comprendono informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria o della relativa prestazione di cui alla direttiva 2011/24/UE del Parlamento europeo e del Consiglio; un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco a fini sanitari; le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici; e qualsiasi informazione riguardante, ad esempio, una malattia, una disabilità, il rischio di malattie, l'anamnesi medica, i trattamenti clinici o lo stato fisiologico o biomedico dell'interessato, indipendentemente dalla fonte, quale, ad esempio, un medico o altro operatore sanitario, un ospedale, un dispositivo medico o un test diagnostico in vitro» (cons. 35 GDPR). Sui dati sanitari e sul loro trattamento, cfr., oltre ai contributi citati nel prosieguo, G. Fioriglio, *La protezione dei dati sanitari nella Società algoritmica. Profili informatico-giuridici*, in «Journal of Ethical and Legal Technologies», 2, 2021, pp. 79-102.

si intersecano, però, con il consenso (lett. a)[64] e con l'interesse pubblico nel settore della sanità pubblica (lett. i)[65].

Per le "finalità di cura" si può invece fare riferimento alla lett. h), che ammette il trattamento dei dati relativi alla salute qualora sia necessario, fra l'altro, per finalità di medicina preventiva o del lavoro, diagnosi, assistenza o terapia sanitaria o sociale, o gestione dei sistemi e servizi sanitari o sociali su base normativa o contrattuale, purché, come previsto dal par. 3, i dati siano trattati da, o sotto la responsabilità di, soggetto all'obbligo di segretezza. Con provvedimento del 7 marzo 2019, il Garante per la protezione dei dati personali ha precisato che il consenso non deve essere richiesto per i trattamenti necessari al perseguimento delle finalità di cura (ossia essenziali per il raggiungimento di una o più finalità determinate ed esplicitamente connesse alla cura della salute); per i trattamenti attinenti solo in senso lato alla cura si deve invece individuare una diversa base giuridica (consenso o altro presupposto di liceità)[66].

[64] Sul consenso cfr. Comitato Europeo sulla Protezione dei Dati, *Linee guida 5/2020 sul consenso ai sensi del regolamento (UE 2016/679)*, 4 maggio 2020.

[65] Si consideri che l'art. 2-*ter* d.lgs. 196/2003 dispone che, fermi restando gli obblighi del GDPR e del medesimo d.lgs 196/2003, il trattamento dei dati personali da parte di una pubblica amministrazione «è anche consentito se necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri ad esse attribuiti». L'art. 2-*sexies* d.lgs. 196/2003 effettua, al comma 2, una elencazione di trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri in diverse materie. Nell'ambito della salute rilevano i seguenti trattamenti: «attività socio-assistenziali a tutela dei minori e soggetti bisognosi, non autosufficienti e incapaci»; «attività amministrative e certificatorie correlate a quelle di diagnosi, assistenza o terapia sanitaria o sociale, ivi incluse quelle correlate ai trapianti d'organo e di tessuti nonché alle trasfusioni di sangue umano»; «compiti del servizio sanitario nazionale e dei soggetti operanti in ambito sanitario, nonché compiti di igiene e sicurezza sui luoghi di lavoro e sicurezza e salute della popolazione, protezione civile, salvaguardia della vita e incolumità fisica»; «programmazione, gestione, controllo e valutazione dell'assistenza sanitaria, ivi incluse l'instaurazione, la gestione, la pianificazione e il controllo dei rapporti tra l'amministrazione ed i soggetti accreditati o convenzionati con il servizio sanitario nazionale»; «vigilanza sulle sperimentazioni, farmacovigilanza, autorizzazione all'immissione in commercio e all'importazione di medicinali e di altri prodotti di rilevanza sanitaria»; «tutela sociale della maternità ed interruzione volontaria della gravidanza, dipendenze, assistenza, integrazione sociale e diritti dei disabili»; «trattamenti effettuati […] per fini di ricerca scientifica».

[66] Garante per la protezione dei dati personali, *Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario*, 7 marzo 2019, provv. n. 55/2019 (doc. web n. 9091942).

Così, in linea di principio e in riferimento al trattamento di dati relativi alla salute, è proprio il consenso (esplicito e manifestato per iscritto) a essere normalmente considerato come la base giuridica di riferimento per finalità di ricerca scientifica o statistica[67], che può essere anche a fasi progressive[68], e fermo restando che un trattamento per finalità di ricerca deve essere «interpretato in senso lato»[69]. Intuitivamente, però, la raccolta del consenso potrebbe limitarne o impedirne lo svolgimento, perché non potrebbero essere effettuati trattamenti in assenza del consenso medesimo.

È dunque necessario trovare un equilibrio fra la protezione dei dati personali e la ricerca scientifica; per poterne discutere, è necessario ricordare che, in linea generale ai sensi dell'art. 5, par. 1, lett. b), GDPR, i dati personali devono essere raccolti per finalità determinate, esplicite e legittime (uso primario), ma possono essere ulteriormente trattati, tra l'altro,

[67] Tuttavia, «in molti casi non è possibile individuare pienamente la finalità del trattamento dei dati personali a fini di ricerca scientifica al momento della raccolta dei dati. Pertanto, dovrebbe essere consentito agli interessati di prestare il proprio consenso a taluni settori della ricerca scientifica laddove vi sia rispetto delle norme deontologiche riconosciute per la ricerca scientifica. Gli interessati dovrebbero avere la possibilità di prestare il proprio consenso soltanto a determinati settori di ricerca o parti di progetti di ricerca nella misura consentita dalla finalità prevista» (cons. n. 33 GDPR).

[68] Cfr. il parere del 30 giugno 2022 del Garante della protezione dei dati personali su un'istanza di consultazione preventiva (doc. web n. 9791886). Sul punto, il Comitato Europeo sulla Protezione dei Dati aveva affermato che qualora sia possibile specificare pienamente le finalità della ricerca, grava sul titolare del trattamento l'obbligo di cercare altri modi per ottenere un consenso valido; ad esempio, si può offrire agli interessati la possibilità di acconsentire a una finalità di ricerca in termini più generali e a fasi specifiche di un progetto di ricerca già conosciute o pianificate, ottenendo poi, nel corso della ricerca, il consenso per le fasi successive del progetto prima dell'inizio della fase corrispondente. Rimane fermo l'obbligo di conformità alle norme deontologiche applicabili alla ricerca scientifica (*Linee guida 5/2020*, cit., p. 34).

[69] Esso dovrebbe «includere ad esempio sviluppo tecnologico e dimostrazione, ricerca fondamentale, ricerca applicata e ricerca finanziata da privati, oltre a tenere conto dell'obiettivo dell'Unione di istituire uno spazio europeo della ricerca ai sensi dell'articolo 179, paragrafo 1, TFUE. Le finalità di ricerca scientifica dovrebbero altresì includere gli studi svolti nell'interesse pubblico nel settore della sanità pubblica. Per rispondere alle specificità del trattamento dei dati personali per finalità di ricerca scientifica dovrebbero applicarsi condizioni specifiche, in particolare per quanto riguarda la pubblicazione o la diffusione in altra forma di dati personali nel contesto delle finalità di ricerca scientifica. Se il risultato della ricerca scientifica, in particolare nel contesto sanitario, costituisce motivo per ulteriori misure nell'interesse dell'interessato, le norme generali del […] GDPR dovrebbero applicarsi in vista di tali misure» (cons. 159 GDPR).

a fini di ricerca scientifica o statistici conformemente all'art. 89, par. 1, GDPR (uso secondario); sul punto è altresì doveroso menzionare la normativa sullo Spazio europeo dei dati sanitari (EHDS, *European Health Data Space*) di cui al Regolamento (UE) 2025/327, che va a fornire le definizioni di uso e secondario[70] dei dati sanitari elettronici[71] rilevanti ai fini della normativa medesima.

[70] Uso primario e secondario sono definiti anche dalla normativa europea sullo Spazio europeo dei dati sanitari. Più specificatamente, ai sensi dell'art. 2, par. 1, lett. d), Reg. (UE) 2025/327, per "uso primario" si intende «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». L'"uso secondario" è invece il trattamento dei dati sanitari elettronici per finalità diverse da quelle iniziali per le quali i dati medesimi sono stati raccolti o prodotti (lett. e); tali finalità sono elencate nell'art. 53 e consistono in: pubblico interesse nell'ambito della sanità pubblica o della medicina del lavoro (lett. a), definizione delle politiche e attività regolamentari a sostegno di enti pubblici o istituzioni, organi e organismi dell'UE (lett. b), statistiche (lett. c) o insegnamento o formazione (lett. d) nel settore sanitario o dell'assistenza, ricerca scientifica (lett. e) miglioramento dell'assistenza, ottimizzazione delle cure ed erogazione di assistenza sulla base dei dati sanitari elettronici di altre persone fisiche (lett. f).

[71] Le categorie minime sono elencate all'art. 53, par. 1, Reg. (UE) 2025/327: «a) dati sanitari elettronici provenienti da cartelle cliniche elettroniche; b) dati su fattori con un'incidenza sulla salute, compresi i determinanti socioeconomici, ambientali e comportamentali della salute; c) dati aggregati sulle esigenze di assistenza sanitaria, sulle risorse assegnate all'assistenza sanitaria, sulla prestazione di assistenza sanitaria e sul suo accesso, sulla spesa per l'assistenza sanitaria e sul suo finanziamento; d) dati sugli agenti patogeni che incidono sulla salute umana; e) dati amministrativi relativi all'assistenza sanitaria, anche relativamente alle dispensazioni, alle domande di rimborso e ai rimborsi; f) dati genetici, epigenomici e genomici umani; g) altri dati molecolari umani, quali quelli provenienti dalla proteomica, dalla trascrittomica, dalla metabolomica, dalla lipidomica e altri dati omici; h) dati sanitari elettronici personali generati automaticamente mediante dispositivi medici; i) dati provenienti dalle applicazioni per il benessere; j) dati relativi allo status e alla specializzazione e all'istituzione dei professionisti sanitari coinvolti nella cura di una persona fisica; k) dati provenienti da registri dei dati sanitari basati sulla popolazione, come i registri di sanità pubblica; l) dati provenienti da registri medici e da registri della mortalità; m) dati provenienti da sperimentazioni cliniche, studi clinici, indagini cliniche e studi delle prestazioni soggetti […] alla normativa europea]; n) altri dati sanitari provenienti da dispositivi medici; o) dati provenienti da registri di medicinali e dispositivi medici; p) dati provenienti da coorti di ricerca, questionari e indagini in materia di salute, dopo la prima pubblicazione dei risultati; q) dati sanitari provenienti da biobanche e banche dati associate». Ciascuno Stato membro può intervenire sia per stabilire catego-

Vi è di più: bisogna infatti menzionare anche l'art. 110 d.lgs. 196/2003[72] (come novellato dal d.l. 19/2024 conv. con l. 56/2024)[73], che consente di prescindere dal consenso per il trattamento dei dati relativi alla salute a fini di ricerca scientifica in campo medico, biomedico o epidemiologico qualora la ricerca sia effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea (in conformità all'art. 9, par. 2, lett. j) GDPR, ivi inclusi gli studi che rientrano nel programma di ricerca sanitaria di cui all'art. 12-*bis* d.lgs. 502/1992, previa effettuazione e pubblica diffusione di una valutazione d'impatto. Il consenso, inoltre, non è necessario se informare gli interessati risulti impossibile, implichi uno sforzo sproporzionato o rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca. Il titolare del trattamento può, in questi casi, effettuare il trattamento, previa adozione di misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato e previo parere favorevole del comitato etico competente.

Tali trattamenti devono però rispettare le garanzie di cui alle "Regole deontologiche per trattamenti a fini statistici o di ricerca scientifica ai sensi degli artt. 2-*quater* e 106 d.lgs. 196/2003 (del. 298/2024)" emanate dal Garante per la protezione dei dati personali, con cui l'Autorità medesima ha individuato motivi etici e di impossibilità organizzativa. I primi sono relativi all'ignoranza della propria condizione da parte dell'interessato, cui potrebbe nuocere (materialmente o psicologicamente) la rivelazione di notizie circa la conduzione dello studio. I secondi, che per il Garante devono essere residuali, concernono sia lo sforzo sproporzionato (dovuto alla numerosità del campione) sia l'impossibilità di contattare gli interessati (perché deceduti o non contattabili).

rie aggiuntive di dati sia introdurre misure più rigorose e garanzie supplementari (art. 53, par. 2 e par. 4, Reg. (UE) 2025/327).

[72] Si è rilevato che sia l'art. 110 sia l'art. 110-*bis* d.lgs. 196/2003 introducono due nuovi basi giuridiche, senza però disciplinare delle vere e proprie attività di ricerca scientifica, e ciò sulla base dell'art. 9, par. 4, GDPR, ai sensi del quale ciascuno Stato «può mantenere o introdurre ulteriori condizioni, comprese limitazioni, con riguardo al trattamento di dati genetici, dati biometrici o dati relativi alla salute» (M. Liotta, op. cit., pp. 366-367).

[73] Prima di tale modifica, era necessario sottoporre il programma di ricerca anche a consultazione preventiva al Garante per la protezione dei dati personali oltre che al Comitato etico territorialmente competente.

Nei predetti casi, oltre (i) all'adozione di misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato nonché (ii) all'acquisizione del parere favorevole del comitato etico territorialmente competente, (iii) il titolare del trattamento deve motivare e documentare la sussistenza dei motivi di cui sopra. Il Garante dispone altresì che, ove vengano trattati dati di soggetti deceduti o non contattabili, debba essere svolta e pubblicata una valutazione d'impatto (*ex* art. 35 GDPR), dandone comunicazione al Garante medesimo[74].

Da quanto esposto, emerge, dunque, un ruolo molto importante per il consenso quale base giuridica di riferimento per il trattamento di dati relativi alla salute, anche se le progressive aperture del legislatore consentono di superarne un'eccessiva rigidità che andrebbe a limitare notevolmente la ricerca scientifica e statistica, con evidenti conseguenze negative. La chiave non è nella radicalizzazione del consenso o, all'opposto, nella sua eliminazione: è nel bilanciamento fra i vari interessi in gioco, da valutare caso per caso – il che pare anche conforme, in linea generale, al principio di *accountability*.

È d'uopo precisare, però, che non si deve confondere fra il consenso informato e il consenso al trattamento di dati personali.

Il primo implica una relazione simmetrica in cui operano due centri di valutazione e di decisione: l'esercente la professione sanitaria (che individua le strategie terapeutiche proponibili in una determinata situazione clinica), da un lato, e la persona assistita (cui si riconosce la dignità di soggetto in grado di autodeterminarsi e dunque il diritto di decidere circa gli interventi diagnostici e terapeutici da effettuarsi sulla sua perso-

[74] Per completezza, si deve altresì menzionare l'art. 110-*bis* d.lgs. 196/2003 che disciplina il trattamento ulteriore da parte di terzi dei dati personali a fini di ricerca scientifica o a fini statistici in assenza di consenso degli interessati. Più specificatamente, il legislatore ha disposto che il trattamento ulteriore di dati personali (comuni e sensibili) a fini di ricerca scientifica o a fini statistici da parte di soggetti terzi che svolgano principalmente tali attività possa essere effettuato solo previa autorizzazione del Garante qualora, a causa di particolari ragioni, informare gli interessati risulta impossibile o implica uno sforzo sproporzionato, oppure rischia di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità della ricerca. In tali ipotesi devono essere adottate misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, il tutto in conformità all'art. 89 GDPR. Per ulteriori approfondimenti sia consentito rinviare a G. Fioriglio, *Trattamento dei dati sanitari e ricerca medica: profili informatico-giuridici e istituzionali nel contesto europeo*, op. cit.

na, così come proposti dal medico)[75], anche se «pecca di soverchia astrattezza postulare una parità negoziale fra sanitari e pazienti»[76].

Una simile relazione si ha nel secondo, in cui viene effettuata una richiesta di prestazione del consenso dal titolare, o comunque per suo conto, nei confronti dell'interessato, cui si riconosce il diritto di poter negare il consenso al trattamento (nei casi in cui ciò sia possibile e dunque quando il consenso costituisce idonea base giuridica, e fermi restando i casi di opposizione al trattamento).

In entrambi i casi, però, il consenso diviene sempre più "informatico" e ciò costituisce un ulteriore aspetto di criticità che emerge di pari passo alle nuove evoluzioni nell'ambito della salute.

In tal senso, «il consenso 'informatico' dovrà essere (a differenza delle applicazioni consuete nell'area biomedica) ampio, flessibile, dinamico (con caratteristiche ben diverse dal consenso informato 'classico', usato nella biomedicina, ossia ristretto e specifico, rigido e dettagliato, statico). Il consenso informatico diviene una sorta di 'presa di coscienza' della raccolta dei dati, dell'impossibilità (o comunque difficoltà) dell'anonimato, della non precisa determinazione a priori delle modalità d'uso, delle incertezze sui luoghi e sui tempi della conservazione dei dati, dell'impossibilità di garantire sicurezza e confidenzialità sempre e in ogni circostanza. Una presa d'atto che serve a rendere consapevole l'utente digitale, generatore di dati nella rete, dei rischi della "dazione" e condivisione dei dati, in specie in ambito sanitario»[77].

Sembra così delinearsi una commistione fra due profili separati, che però ora diventano strettamente collegati nella prospettiva di una medicina "digitale" in cui il contatto fra l'operatore sanitario (in particolare, medici e infermieri) e il paziente potrebbe essere mediato dalle nuove tecnologie in un numero crescente di casi, anche perché il consenso allo svolgimento di determinate prestazioni sanitarie (preventive o terapeutiche) e quello al trattamento dei dati personali possono intrinsecamente

[75] P. Borsellino, *Bioetica tra "morali" e diritto*, nuova ed., Raffaello Cortina, Milano, 2018, p. 153.

[76] A. Di Giandomenico, *il consenso informato: questioni di frontiera*, in P. Savarese, G. Sorgi (a cura di), *Filosofia, politica e diritto: questioni di frontiera. Scritti in onore di Teresa Serra*, FrancoAngeli, Milano, 2018, p. 78.

[77] L. Palazzani, *Tecnologie dell'informazione e intelligenza artificiale. Sfide etiche al diritto*, cit., p. 31.

legarsi qualora il buon esito delle prime dipenda, in tutto o in parte, da un'ampia possibilità di accesso alla storia clinica del paziente, possibilmente mediante informazioni rispettose degli standard di comunicazione che consentano un dialogo fra i professionisti, le strutture sanitarie, i pazienti e i sistemi informatici da loro utilizzati.

Sullo sfondo si colloca altresì il tema della profilazione algoritmica degli utenti dei sistemi informatici, mediante la quale si costruiscono identità digitali – anche in ambito sanitario – per finalità eterogenee, dalla personalizzazione dei servizi al targeting pubblicitario, talora in conformità e talora in frizione con il quadro normativo vigente. Si tratta di un profilo particolarmente delicato, sia per il possibile disallineamento tra identità digitale e identità personale, sia per il rischio di una riduzione della persona a mero consumatore di prodotti e servizi della Società dell'informazione.

Alla luce della breve ricognizione svolta, il diritto non appare come mera istanza limitativa, bensì come fattore abilitante e dispositivo di controllo dello sviluppo tecnologico in ambito biomedico: esso ne orienta la traiettoria a presidio della dignità della persona, della riservatezza e della protezione dei dati personali.

II.4. Conoscenza, comunicazione, prodotti e servizi online nell'ambito della salute digitale

Nella Società dell'informazione e algoritmica, la salute digitale impone una riflessione sui profili etici, sociali e giuridici dei passaggi che trasformano dati in conoscenza e conoscenza in comunicazione, coinvolgendo prodotti e servizi online (piattaforme, applicazioni, dispositivi): dalla produzione e validazione alla mediazione algoritmica e fino alla comunicazione pubblica, attraverso canali digitali e tradizionali, a fini clinici, di prevenzione, di sanità pubblica e di promozione del benessere (*well-being*).

Tradizionalmente, la conoscenza nell'ambito della salute si forma attraverso processi cumulativi di osservazione, sperimentazione e validazione, nel rispetto di metodologie rigorose e con il coinvolgimento di strutture istituzionali di controllo (come università, enti di ricerca, ministeri competenti, comitati etici, agenzie regolatorie e autorità sanitarie

regionali e locali). Di base, si regge su un modello epistemologico lineare: i dati empirici sono raccolti, interpretati e verificati secondo protocolli condivisi e standard riconosciuti, nel rispetto dei principi etici e del quadro normativo, con valutazione dei comitati etici e, ove previsto, documentazione in registri pubblici. Gli esiti di tali processi sono quindi sistematizzati e tradotti in sapere per la salute digitale – evidenze, raccomandazioni, linee guida e strumenti operativi – destinati a orientare non solo la pratica della cura, ma anche la prevenzione, l'organizzazione dei servizi e la promozione del benessere individuale e collettivo. La conoscenza così prodotta (in contesti accreditati e sottoposta a revisione paritaria) è dunque essenziale per l'evoluzione della società e per la tutela della vita e della salute, individuale e collettiva; la sua affidabilità discende tanto dalla correttezza metodologica quanto dalla responsabilità, individuale e collettiva, degli attori coinvolti.

Tuttavia, nell'ecosistema digitale, alle predette forme tradizionali si affiancano modalità eterogenee e più fluide che ne modificano struttura e attori, includendo anche soggetti che non operano professionalmente nell'ambito della salute (o che operano in assenza di idonee e certificate competenze e cognizioni). Piattaforme, siti web e forum di discussione, motori di ricerca, sistemi di IA, social network e sistemi di raccolta automatizzata dei dati sanitari (dai dispositivi indossabili ai registri elettronici) generano flussi informativi continui e non sempre pienamente controllabili, entro cui la distinzione tra dato grezzo, informazione e conoscenza tende a sfumare, cui si aggiunge la problematica della disinformazione digitale, ampliata – in particolare – proprio dai social network, i quali possono amplificare sia le informazioni accurate sia quelle non accurate[78]. La costruzione della conoscenza non avviene più soltanto "a valle" della validazione formale, ma anche "a monte", attraverso algoritmi di classificazione, sistemi di raccomandazione e modelli predittivi o generativi che selezionano, interpretano e sintetizzano i dati in modo automatizzato.

In particolare, l'IA introduce nuovi agenti epistemici. I sistemi analitici o predittivi intervengono nei processi inferenziali, coadiuvando – o

[78] J.C. Blom, V. Rivi, F. Tascedda, L. Pani, *Building trust in clinical research: a systems approach to ethical engagement and sustainable outcomes*, in «Frontiers in Pharmacology», 2025, doi 10.3389/fphar.2025.1570899, p. 8. Cfr. altresì S. Kanchan, A. Gaidhane, *Social Media Role and Its Impact on Public Health: A Narrative Review*, in «Cureus», 15, 1, 2023, doi:10.7759/cureus.33737.

talora sostituendo – la valutazione umana nella produzione di evidenze. Vi è di più. L'IA generativa opera in una fase ulteriore, in quanto non si limita a estrarre correlazioni, ma produce nuova conoscenza nell'ambito della salute, anche potenzialmente errata in assenza di validazione scientifica e presidio umano. Ne deriva un mutamento non solo tecnologico, ma anche metodologico, sociale e istituzionale, con ricadute ontologiche sul modo in cui si configura il "soggetto della conoscenza": dalla persona e dalla comunità scientifica si passa a reti ibride in cui le componenti computazionali svolgono un ruolo costitutivo.

L'ambito soggettivo si amplia notevolmente a livello sia quantitativo (nuovi soggetti) sia qualitativo (*emporwement* e responsabilizzazione): sviluppatori di modelli, fornitori e curatori di dati, gestori di piattaforme e infrastrutture, *content creator* e *influencer* (professionisti sanitari e non), creatori di prodotti che trattano dati relativi alla salute, fornitori di servizi (come le app per la salute e il benessere), professionisti che impiegano gli output e, non da ultimi, utenti-pazienti che, tramite interazioni e dati generati in prima persona, alimentano e orientano sistemi di IA, social network, forum e siti web, nonché le strategie comunicative di tutto il "mercato" della salute. La conoscenza diviene così il risultato di una cooperazione distribuita e algoritmica, in cui si intrecciano interessi economici, poteri informazionali e requisiti di trasparenza, affidabilità e *accountability* lungo l'intera filiera.

Le criticità sono numerose, così come le difficoltà di governare adeguatamente i flussi informativi trovando un equilibrio fra libertà della ricerca scientifica, di manifestazione del pensiero e di iniziativa economica privata, da un lato, e tutela della vita, della salute e dell'autodeterminazione, dall'altro[79].

[79] I rischi della disinformazione sono assai gravi nell'ambito della medicina, che deve confrontarsi con la diffusione di notizie fase, inaccurate o incomplete: cfr. W.S. Chou, A. Oh, W.M.P. Klein, *Addressing health-related misinformation on social media*, in «JAMA», 320, 23, 2018, pp. 2417-2418. Si consideri, infatti, che anche sperimentazioni scientificamente solide e condotte nel rispetto dei principi etici possono incontrare una diffusa resistenza pubblica. Per affrontare tale fenomeno, i ricercatori clinici devono non solo praticare una scienza rigorosa, ma anche investire in strategie di comunicazione digitale trasparenti, culturalmente pertinenti e capaci di rispondere alla disinformazione online. La collaborazione con leader d'opinione nelle comunità, con le associazioni di pazienti e i loro rappresentanti, nonché con comunicatori della salute digitale, può contribuire a colmare il divario tra scienza e percezione pubblica (J.C. Blom, V. Rivi, F. Tascedda,

Emblematico, del resto, è il divario tra la rigorosa regolamentazione dei dispositivi medici e la zona grigia nella quale operano dispositivi e servizi rivolti direttamente agli utenti (al contempo utenti e consumatori, e sovente in condizione di vulnerabilità anche nel caso in cui non siano "pazienti") che possono incidere sulla loro salute: rientrano in tale area, ad esempio, i dispositivi indossabili e, più in generale, i servizi informativi sanitari online che hanno impatti, anche indiretti, in fase preventiva o terapeutica. Il discrimine tra dispositivi medici (inclusi i software) e le applicazioni rilevanti per la salute e il benessere risiede nella finalità dichiarata e nelle rivendicazioni funzionali (*intended purpose*): da essa discendono gli obblighi in tema di sicurezza, performance e sorveglianza.

Ciò pone delicate questioni bioetico-giuridiche, che impongono garanzie sulla qualità delle informazioni e interventi strutturali di alfabetizzazione digitale e sanitaria, affinché gli utenti sappiano riconoscere fonti autorevoli e valutare l'affidabilità dei contenuti[80].

Non sono, tuttavia, problematiche semplici da risolvere. Alle maggiori possibilità di acquisire informazioni (generali o specifiche per ciascun utente qualora venga richiesto un consulto medico online), e dunque al potenziale beneficio per il diritto all'autodeterminazione informativa (che per essere realmente esercitato richiede però, quanto meno, senso critico e possibilità di comprendere le informazioni ricevute, presupponendo che siano corrette e correttamente esposte), fanno da contraltare alcune questioni che hanno rilevanza bioetico-giuridica, nel cui ambito assumono una particolare importanza quelle relative all'affidabilità delle fonti, al possesso di adeguate cognizioni teorico-pratiche in chi ne fruisce e agli effetti dei consulti a carattere sanitario online.

Tanto premesso, si possono ora analizzare compiutamente le questioni appena menzionate, partendo dalla prima citata, l'affidabilità delle fonti, e ponendosi nella prospettiva del recettore delle informazioni, siano esse sollecitate o meno. L'affidabilità dovrebbe essere valutata tenendo conto di diversi criteri: autorevolezza del soggetto erogatore; trasparenza autoriale; metodo e verificabilità (citazioni e aggiornamenti); gestione dei

L. Pani, *Building trust in clinical research: a systems approach to ethical engagement and sustainable outcomes*, op. cit., p. 8).

[80] Comitato Nazionale per la Bioetica, *Etica, salute e nuove tecnologie dell'informazione*, op. cit., p. 30.

conflitti di interesse; tracciabilità delle trasformazioni algoritmiche; netta separazione tra informazione e pubblicità.

Sono da intendersi sollecitate ove fornite su sua richiesta, come nel caso della richiesta di un consulto medico online, mentre non lo sono, o al più possono esserlo indirettamente, qualora gli siano proposte dai servizi automatici che elaborano le sue richieste o all'esito di attività promozionali e pubblicitarie, come comunemente avviene nella prestazione dei servizi di social network o di motori di ricerca, nel primo caso, e in seguito alla ricezione di newsletter o messaggi promozionali, nel secondo. Va distinto l'insieme delle prestazioni sanitarie digitalmente mediate (teleconsulto, teleassistenza, telemonitoraggio, telerefertazione e operazioni/tele-programmazione su dispositivi medici connessi) dalla comunicazione informativa generalista, cui si applicano (quanto meno in linea di principio) doveri di trasparenza e corrette prassi editoriali.

Così, l'acquisizione delle informazioni può avvenire mediante un intermediario qualificato che comunica direttamente con esso (come il proprio medico di medicina generale, un medico specialista, un infermiere) oppure in via indiretta tramite altre fonti (ad esempio, mass media tradizionali e non). Nel primo caso l'informazione assume un'importanza fondamentale nell'ambito del rapporto fra il professionista e il paziente, poiché solo in seguito ad una corretta e completa informativa resa dal personale sanitario al destinatario delle cure (preventive o terapeutiche) appare possibile prestare un consenso consapevole all'effettuazione di trattamenti sanitari, siano essi relativi a patologie vere e proprie o a indicazioni per il benessere e la tutela della salute. In ogni caso, però, informazioni corrette e affidabili sono fondamentali per costruire un ciberspazio in cui si tenda alla verità e non alla "post-verità", nel rispetto del pluralismo degli Stati costituzionali e dei principi e dei valori su cui questi si fondano.

Com'è noto, il lessema "post-verità" è stato adoperato negli ultimi anni per esprimere ciò che è relativo a, o che denota, circostanze in cui gli appelli all'emotività e le convinzioni personali influenzano maggiormente l'opinione pubblica rispetto ai fatti obiettivi[81]: si può sostenere che la

[81] Questa la definizione degli *Oxford Dictionaries* (<https://en.oxforddictionaries.com/word-of-the-year/word-of-the-year-2016>). Come sostenuto da Paolo Savarese, tale definizione non deve essere intesa in modo rigoroso: per esserlo dovrebbe precisare il senso dei suoi termini, che sono invece chiari solo in apparenza; sono infatti densi di storia nonché di trabocchetti ed equivoci sul piano teoretico. Pertanto, tale formula non

post-verità sia altro dalla verità (è il suo opposto e il suo rifiuto)[82] e che sia inconciliabile con la democrazia e con il pluralismo che costituisce un valore-chiave di ciascuno Stato costituzionale[83]. Del resto, si verifica «una profonda trasformazione dell'ambiente entro cui si esperisce uno dei diritti fondamentali della cultura giuridica e politica liberale e democratica, la libertà di espressione: il rapporto tra la notizia e il suo accreditamento presso il pubblico è mutato, e questo cambiamento ha offerto un protagonismo del tutto nuovo alla questione del "falso", e quindi della verità, nella comunicazione e nel sistema dell'informazione»[84].

In linea generale, così, nel ciberspazio la post-verità può trovare terreno fertile grazie a diversi fattori, con conseguenze estremamente delicate nell'ambito della salute digitale. Un fattore comune a molte esperienze in tal senso può essere individuato nel fine di lucro, anche qualora la disinformazione che stravolge il concetto stesso di verità non sia direttamente finalizzata a ottenere vantaggi patrimoniali bensì, ad esempio, a diffondere e difendere una propria ideologia o una propria convinzione su un argomento, convinzione che si ritiene giusta. Bisogna infatti considerare che nella memorizzazione e nella diffusione delle informazioni un ruolo fondamentale è rivestito non solo da chi le produce, ma altresì (e spesso in modo preponderante) dai prestatori dei servizi informatici

descrive accuratamente né fa intendere il fenomeno che segnala, ma è importante in quanto fornisce una rilevazione circostanziata di una direzione di fondo della nostra cultura, per quanto tale indicatore sia privo di consistenza epistemica e comunque situato dichiaratamente sull'asse *doxatico* (P. Savarese, *Dalla bugia alla menzogna: la posterità e l'impossibilità del diritto*, in «Nomos», 2, 2018, p. 3, <https://www.nomos-leattualitaneldiritto.it/nomos/paolo-savarese-postverita-e-impossibilita-del-diritto/>). Cfr. altresì A. Schiavello, *Postdiritto: una breve guida per i perplessi*, in «Rivista di filosofia del diritto», 2, 2023, pp. 261-280.

[82] Sul rapporto fra diritto e verità cfr. in particolare: P. Häberle, *Diritto e verità*, tr. it., Einaudi, Torino, 2000; M. La Torre, *La verità del diritto senza verità*, in «Sociologia del diritto», 1, 2013, pp. 187-199; F. Mancuso, *Le 'verità' del diritto. Pluralismo dei valori e legittimità*, Giappichelli, Torino, 2013; A. Pintore, *Il diritto senza verità*, Giappichelli, Torino, 1996, D. Patterson, *Diritto e verità*, tr. it., Giuffrè, Milano, 2010.

[83] Sul punto sia consentito rinviare a G. Fioriglio, *Contro la post-verità: il pluralismo assiologico quale limite del potere e garanzia della giustizia nello Stato costituzionale*, in «Nomos», 3, 2016, <https://www.nomos-leattualitaneldiritto.it/nomos/gianluigi-fioriglio-contro-la-postverita-il-pluralismo-assiologico-quale-limite-del-potere-e-garanzia-della-giustizia-nello-stato-costituzionale/>.

[84] Th. Casadei, *L'irruzione della post-verità*, in «Governare la paura», 2019, pp. 4-5, <https://governarelapaura.unibo.it/article/view/9411>.

della Società dell'informazione e algoritmica, come sistemi di IA, social network, *hosting provider,* motori di ricerca e piattaforme per la distribuzione di app (come Apple App Store e Google Play Store), la cui finalità è quella di raggiungere il maggior numero possibile di persone così da poter fornire servizi accessori da "monetizzare" (sovente si tratta di spazi di pubblicità personalizzata da vendere agli inserzionisti).

Questi poteri privati controllano dunque il flusso delle informazioni. Già vent'anni fa, del resto, Yochai Benkler aveva evidenziato come solo (relativamente) pochi siti fossero enormemente visitati, mentre la maggior parte passava (e passa) inosservata[85]; oggi come allora, pochi soggetti si pongono quali intermediari fra chi produce informazioni e chi accede alle medesime, controllando più o meno attivamente il flusso delle informazioni che viaggiano in Rete (basti pensare al dominio sugli algoritmi che permettono di suggerire determinati contenuti, ad esempio in riferimento ai social network o agli spazi dedicati alle notizie correlate, o per ciò che concerne l'ordine di elencazione nelle pagine dei risultati dei motori di ricerca, ossia al *ranking* nelle SERP – *Search Engine Results Page*, o di suggerimenti circa eventuali app da installare, o, in misura ancora maggiore, con l'IA generativa). Rileva inoltre il design delle interfacce (incluse pratiche persuasive e *dark patterns*), capace di orientare scelte sanitarie e di benessere, con ricadute sull'autodeterminazione.

Un quadro generale, dunque, che mostra alcuni chiaroscuri: alle aumentate possibilità di manifestare il proprio pensiero e di informarsi online si accompagna la difficoltà di individuare le fonti affidabili a cui rivolgersi, che però non sono sempre facili da riconoscere e da distinguere da quelle inaffidabili[86].

Una difficoltà più generale, del resto, emerge ove si consideri che «la scienza non riesce più a proporsi come sapere oggettivo, capace di fondare

[85] Y. Benkler, *The Wealth of Networks. How Social Production Tranforms Markets and Freedom*, Yale University Press, New Haven-London, 2006, *passim*.

[86] In taluni casi, poi, si fa ricorso a metodologie, tecniche e tecnologie di costruzione della post-verità idonee a essere sfruttate per creare ed alimentare la paura, soprattutto ove l'agente sia in grado non solo di adoperare in modo abile le tecnologie dell'informazione e della comunicazione ma anche di volgere a proprio vantaggio i margini derivanti dal diritto alla libera manifestazione del proprio pensiero (in argomento sia consentito rinviare a G. Fioriglio, *Post-verità, paura e controllo dell'informazione: quale ruolo per il diritto?*, in *Governare la paura*, 2019, pp. 105-124; <https://governarelapaura.unibo.it/article/view/9416>).

basi comuni, di per sé condivisibili. In taluni campi i dati scientifici sembrano non risolutivi e sono soggetti a interpretazioni che conducono a risultati e valutazioni molto distanti» e anche nel momento in cui diventano oggetto di regolazione giuridica «non perdono di 'valenza divisiva'»[87].

Le fonti inaffidabili, però, danneggiano le prime, ingenerando – o contribuendo a ingenerare – in alcune persone un senso di sfiducia, con la potenziale conseguenza di orientarne il comportamento verso un rifiuto di informazioni (e servizi) online anche quando questi sarebbero utili per finalità di prevenzione epidemiologica, come nel caso della emergenza dovuta al Covid-19 (sia le piattaforme tradizionali generaliste, come i social network, sia le app di tracciamento sviluppate *ad hoc* possono infatti fornire un contributo per prevenire, studiare e debellare le epidemie e le pandemie – o, al contrario, essere di ostacolo[88].

Ad ogni buon conto, oramai da tempo si moltiplicano i canali informatici per la diffusione di informazioni sulla salute, il dibattito pubblico, l'automonitoraggio, ecc.[89], che consentono anche una interazione più o meno forte con i propri utenti: fra essi si possono qui ricordare i siti web, i social network, le app e le loro piattaforme di distribuzione, i servizi di messaggistica, i sistemi di IA. Inoltre, la loro diffusione appare sempre

[87] B. Pastore, *Tecnologie emergenti, incertezze della scienza, regolamentazione giuridica*, in «Teoria e critica della regolazione sociale», 2, 2018, p. 98.

[88] La bibliografia in materia è oramai sterminata: fra gli altri, cfr. P. Borsellino, *Covid-19: Quali criteri per l'accesso alle cure e la limitazione terapeutica in tempo di emergenza sanitaria?*, in «Notizie di Politeia», 2020, pp. 5-25; L. D'Avack, *CoViD-19: criteri etici*, in «BioLaw Journal. Rivista di BioDiritto», 1S, 2020, pp. 371-378; F. De Vanna, *Il diritto "imprevedibile": notazioni sulla teoria della necessità a partire dall'emergenza Covid-19*, in «Nomos», 2, 2020, (<https://www.nomos-leattualitaneldiritto.it/nomos/francesco-de-vanna-il-diritto-imprevedibile-notazioni-sulla-teoria-della-necessita-a-partire-dallemergenza-covid-19>); L. Palazzani, *La pandemia CoViD-19 e il dilemma per l'etica quando le risorse sono limitate: chi curare?*, in «BioLaw Journal. Rivista di BioDiritto», 1S, 2020, pp. 359-370; N. Miniscalco, *La sorveglianza attiva per contrastare la diffusione dell'epidemia di Covid-19: strumento di controllo o di garanzia per i cittadini?*, in «Osservatorio costituzionale», 3, 2020, pp. 95-115; P. Zuddas, *Covid-19 e* digital divide: *tecnologie digitali e diritti sociali alla prova dell'emergenza sanitaria*, in «Osservatorio costituzionale», 3, 2020, pp. 285-307. Per ulteriori riferimenti si rinvia alla bibliografia tematica sul Covid-19 a cura di F. De Vanna resa disponibile sul sito del CRID – Centro di Ricerca Interdipartimentale su Discriminazioni e vulnerabilità dell'Università di Modena e Reggio Emilia al seguente URL: <http://www.crid.unimore.it/site/home/archivio-in-primo-piano/articolo1065055035.html>.

[89] Sul punto v. anche *infra*, capitolo 3, par. 3.4.

più capillare e pervasiva, agevolata dal sempre maggior utilizzo di dispositivi indossabili per l'acquisizione e il monitoraggio di dati relativi alla salute, cui si è già accennato. Ciò comporta che le informazioni a carattere sanitario vengono trattate in misura crescente anche da soggetti non operanti in tale settore o comunque al di fuori delle strutture sanitarie, mentre va a dematerializzarsi il rapporto con il paziente non solo quando esso coinvolge medici, infermieri e strutture sanitarie, ma anche altri soggetti (ad esempio, come le farmacie, che operano sempre più spesso online nel rispetto della rigorosa normativa in materia)[90].

Si può dunque ravvisare l'importanza di riflettere sulla fondamentale importanza del requisito dell'affidabilità della fonte che fornisce comunicazioni e servizi online nell'ambito della salute, indipendentemente dal fatto che siano meramente informativi (come nel caso dei siti e dei post sui social network che si occupano di queste tematiche) o costituiscano veri e propri canali di fornitura di servizi di consulenza e di prodotti. Questa riflessione è, del resto, fondamentale per consentire di tracciare nuovi percorsi teorico-pratici in prospettiva informatico-giuridica, poiché, come rilevato in dottrina, «dall'analisi dello stato dell'arte in definitiva si può concludere che strumenti di filtro, codici e griglie di valutazione adottati ex-post non hanno portato ai risultati sperati, anche per la velocità e l'eterogeneità dei dati prodotti dai servizi informatici»[91].

Necessario, dunque, promuovere il senso critico e la cittadinanza attiva, che si concretizza – a livello statuale – soprattutto garantendo un'istruzione e una formazione incentrata anche su questi profili, anche se, come evidenziato da Martha C. Nussbaum, gli Stati, attratti dalla logica del profitto, tendono ad accantonare quei saperi indispensabili a man-

[90] Per ciò che concerne l'ordinamento giuridico italiano, il d.lgs. 19 febbraio 2014, n. 17 (Attuazione della direttiva 2011/62/UE, che modifica la direttiva 2001/83/CE, recante un codice comunitario relativo ai medicinali per uso umano, al fine di impedire l'ingresso di medicinali falsificati nella catena di fornitura legale), ha aperto la strada alla vendita online di farmaci senza obbligo di prescrizione medica (SOP). La vendita online è però consentita unicamente alle farmacie e agli esercizi commerciali autorizzati alla vendita di medicinali e operanti 'fisicamente' sul territorio: dunque non è attualmente possibile che un esercizio venda farmaci esclusivamente online.

[91] R. Brighi, *Il valore informativo dei dati in rete: il problema della* veridicità. *Analisi e soluzioni informatico-giuridiche*, in C. Faralli, R. Brighi, M. Martoni (a cura di), *Strumenti, diritti, regole e nuove relazioni di cura. Il Paziente europeo protagonista nell'eHealth*, cit., p. 27.

tenere viva la democrazia, cui consegue la "produzione" non di cittadini e cittadine a pieno titolo in grado di pensare autonomamente, bensì di docili macchine che non hanno senso critico anche nei confronti della tradizione e che non comprendono cosa significano le sofferenze e le esigenze altrui. Ciò si concretizza in un investimento sul profitto a breve termine garantito dai saperi tecnico-scientifici più idonei per il perseguimento di questa finalità, ridimensionando sia gli studi umanistici ed artistici sia l'aspetto creativo, inventivo e di pensiero critico e rigoroso della scienza e della scienza sociale[92], mentre sarebbe necessario puntare su un modello di insegnamento legato alla tradizione filosofica occidentale di teoria pedagogica (grazie agli insegnamenti di illustri studiosi come Jean-Jacques Rousseau e John Dewey) per abituare la mente a diventare attiva, competente e responsabilmente critica verso le complessità del mondo[93].

Quanto appena argomentato, inoltre, è strettamente connesso alla seconda questione posta in apertura del presente paragrafo: la riflessione circa la predisposizione di strumenti informatico-giuridici finalizzati a garantire che chi fruisce di informazioni, prodotti e servizi informatici nell'ambito della salute sia posto in condizione di possedere adeguate cognizioni teorico-pratiche.

Bisogna però tener presente che l'intermediazione degli strumenti informatici comporta comunque una tendenza verso la disumanizzazione, eliminando l'elemento della corporeità sino a poco tempo fa del tutto metabolizzato e nel volgere di pochi anni affiancato, e talvolta superato, dalla immaterialità delle nuove tecnologie (problema, dunque, che si ripropone e che si riverbera sul rapporto fra il professionista sanitario e la persona assistita), soprattutto nella prospettiva dell'IA: i relativi sistemi, infatti, tendono a dialogare in modo "umanizzato" con chi interagisce. Ma rimangono sistemi informatici che eseguono software basato su com-

[92] M.C. Nussbaum, *Non per profitto. Perché le democrazie hanno bisogno della cultura umanistica*, tr. it., Il Mulino, Bologna, 2013, pp. 21-22. La formazione, comunque, prepara le persone al lavoro e a una vita degna di essere vissuta (ivi, p. 28). Fra i numerosi studi in materia, si può qui ricordare, sull'individualità e sullo sviluppo di sé, K.A. Appiah, *The Ethics of Identity*, Princeton University Press, Princeton, 2005.

[93] M.C. Nussbaum, *Non per profitto*, op. cit., p. 31 ss. Sul ritorno di Dewey nella discussione contemporanea in tema di formazione democratica e funzioni del diritto si veda C. Crocetta, *A partire da Dewey: didattica del diritto e cittadinanza democratica,* in *Teoria e critica della regolazione sociale*, 2020: <https://www.mimesisjournals.com/ojs/index.php/tcrs/article/view/284>.

plessi algoritmi, sovente assai efficienti. In tale quadro, il rischio di vulnerabilità aumentata impone presìdi di ri-personalizzazione del dato e di *accountability* lungo l'intera filiera informativa e comunicativa.

L'evoluzione della produzione della conoscenza e della sua comunicazione ha un rilevante impatto sulla vulnerabilità a più livelli, soprattutto in riferimento ai rischi dell'IA ove la stessa non venga governata rettamente (ossia nel rispetto dei principi e dei valori di ciascun ordinamento giuridico, con particolare riferimento alla tutela della vita, della salute e della dignità umana): non solo utenti e pazienti, ma anche operatori e operatrici sanitari, che rischiano di essere delegittimati in una società in cui i flussi informativi, e la percezione della conoscenza nell'ambito della salute, sono controllati anche da *influencer,* mass media generalisti, i gestori di piattaforme e di sistemi di IA, fornitori di prodotti e servizi, ciascuno in ambiti più o meno vasti.

II.5. Dataismo, Big Data e regolazione tecnico-scientifica della salute e della cura: tra responsabilizzazione e derive difensive

Nella società algoritmica si tende a rendere tutto computabile[94], incluse le persone, che vengono categorizzate a seconda della finalità perseguita dal titolare (legittimo o meno) di un trattamento consistente, sostanzialmente, nella profilazione[95]. La persona diviene un "interessa-

[94] Non a caso, gli elaboratori elettronici sono costruiti proprio per "computare". Sul punto cfr. altresì l'inquadramento generale in Th. Casadei, S. Pietropaoli, *Intelligenza artificiale: l'ultima sfida per il diritto?*, in Id. (a cura di) *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, Wolters Kluwer, Milano, 2024, pp. 257-272, nonché, per una prospettiva umanistica e giuridica, C. Coniglione, *Le criticità del diritto computazionale e della giustizia predittiva. Le* humanities *come "nuova" modalità di approccio al diritto contemporaneo?*, in «Heliopolis», 1, 2025, pp. 67-79; J. Mazzuca, *L'intelligenza artitificiale. Luci e ombre del ragionamento algoritmico*, in «Ragion pratica», 1, 2024, pp. 241-264.

[95] Per essa si intende «qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica» (art. 4(4) GDPR). Come si è evidenziato, «l'essere umano è, oggi, *in competizione* con le macchine che trattano i suoi dati. Macchine che riescono a recuperare informazio-

to", figura che certamente non la esaurisce nella sua pienezza: eppure la misura informazionale della vita non deve oscurarne la dimensione personale, relazionale e comunitaria, che è il vero riferimento delle garanzie. Del resto, in una prospettiva più ampia, il ruolo che deve svolgere il diritto non è «quello di garantire il diritto di ciascuno ad essere solo, ingabbiato in se stesso, bensì di promuovere l'essere con gli altri per ritrovare se stessi. L'uomo non è proprietario di un sé inteso come uno spazio da difendere, ma è un pellegrino il cui cammino incrocia gli altri e per tratti più o meno lunghi prosegue con loro. Il suo bene è spesso anche il bene dell'altro e comunque, che lo voglia o meno, può essere raggiunto solo se l'altro è accanto con lui»[96].

Per ciò che concerne l'ambito della salute, la centralità delle relative informazioni non può rovesciarsi in primato del dato sulla salute, il che può realizzarsi, in particolare, perché (i) un errato bilanciamento fra riservatezza e salute sacrifica indebitamente la prima; (ii) la datificazione comporta scelte dovute a distorsioni nell'elaborazione dei dati (scelte individuali, nell'esercizio del diritto all'autodeterminazione, o pubbliche, per ciò che concerne le politiche in tale ambito, intese in senso lato).

Il rischio di un nuovo riduzionismo – il «dataismo»[97] – è evidente. Ogni dato è una riduzione del reale: selezione, astrazione, decontestualizzazione seguita da ricontestualizzazione. Il reale non si lascia ricondurre alla somma delle sue parti; come i dati sono una riduzione della realtà, anche il loro uso rischia di essere una rappresentazione riduttiva del reale (in quanto il reale non può essere considerato quale mera somma delle sue parti)[98] e sono quindi necessari interpretazione, controllo del

ni, e a elaborare dati, che sono in grado di disegnare, attorno all'individuo, un profilo (o "corpo elettronico", come scriverebbe Stefano Rodotà) ancora più preciso di come l'essere umano conosca se stesso, e capace persino di prevedere e, perché no, di orientare i comportamenti» (G. Ziccardi, *Diritti digitali. Informatica giuridica per le nuove professioni*, Raffaello Cortina, Milano, 2022, p. 69).

[96] A. Punzi, *L'umanesimo digitale: verso un nuovo principio di responsabilità?*, in «Democrazia e diritti sociali», 1, 2023, p. 28.

[97] «Dataism betrays a belief in the objectivity of quantification and in the potential of tracking all kinds of human behavior and sociality through online data» (J. Van Dijck, *Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology*, in «Surveillance & Society», 12, 2, 2014, p. 201).

[98] L. Palazzani, *Tecnologie dell'informazione e intelligenza artificiale. Sfide etiche al diritto*, Studium, Roma, 2020, pp. 28-29.

contesto e verifica delle assunzioni[99]. Difatti, il dato non è autoevidente: richiede un impianto metodologico di interpretazione, giustificazione e controllo, onde impedire che la mera correlazione prenda il posto della spiegazione. Nondimeno, nell'uso applicativo, il dato è sovente orientato a ricondurre la persona entro categorie predeterminate (consumatore, paziente, utente, studente, lavoratore, elettore, contribuente, assicurato, assistito, fino al "profilo di rischio") con effetti di semplificazione identitaria e di eterodirezione delle scelte e di governo dei comportamenti. Inoltre, lo stesso «concetto di interiorità della persona si trasforma gradatamente in un'appendice impersonale della complessa dimensione dell'esteriorità (social networks, influencers, immagini, big data, motori di ricerca, app, etc…) che altro non è se non la costellazione dei dati della nuova economia informazionale»[100].

L'emersione del dataismo si intreccia con l'evoluzione della società dell'informazione e algoritmica: l'incremento delle capacità di calcolo, da un lato, e di archiviazione e di volume, velocità e varietà delle tracce digitali, dall'altro, ha reso effettuabili trattamenti ed elaborazioni prima impossibili. Da una enorme e crescente mole di dati possono trarsi inferenze probabilistiche e correlazioni inattese, ma bisogna garantire adeguatezza, rappresentatività e correttezza dei dati nonché delle relative elaborazioni, che dovrebbero essere trasparenti e spiegabili, quanto meno in linea di principio[101].

[99] Th. Casadei, *I divari digitali di genere: frontiera del "costittuzionalismo digitale"?*, in «Diritto e questioni pubbliche», 2025, *Special Issue* (maggio), p. 7.

[100] L. Avitabile, *Il diritto davanti all'algoritmo*, in «Rivista italiana per le scienze giuridiche», 8, 2017, p. 315).

[101] Più specificatamente: volume (grandi quantità), velocità (incremento esponenziale della velocità di generazione dei dati sino alla loro acquisizione ed elaborazione in tempo reale), varietà (diverse tipologie da diverse fonti, per cui si ha una forte eterogeneità). Vi sono ulteriori specificazioni, precisazioni e discussioni circa tali caratteristiche, ma ai fini del presente volume è sufficiente fare riferimento a quanto sopra richiamato. Per un approfondimento cfr., fra gli altri e in aggiunta agli altri testi citati, Comitato Nazionale per la Bioetica, *Tecnologie dell'informazione e della comunicazione e* big data*: profili bioetici*, Roma, 2016; F. Faini, *Big data, algoritmi e diritti*, in «DPCE online», 3, 2019, pp. 1869-1882; F. Faini, Data society: *governo dei dati e tutela dei diritti nell'era digitale*, Giuffrè, Milano, 2019; S. Pietropaoli, *Habeas data. I diritti umani alla prova dei* big data, in S. Faro, T.E. Frosini, G. Peruginelli (a cura di), *Dati e algoritmi. Diritto e diritti nella società digitale*, Il Mulino, Bologna, 2020, pp. 97-111. cfr. altresì C. Maioli, E. Sánchez Jordán, *Big Data e capacità informativa per l'autodeterminazione del paziente*, in C. Faralli, R. bri-

Il riferimento quantitativo ("big") non deve però trarre in inganno, nel senso che esso è il viatico per un miglioramento qualitativo: grazie alla *Data analytics* è infatti possibile estrarre correlazioni probabilistiche inattese dalle grandi masse di dati[102]. Determinate operazioni possono essere svolte solo mediante queste analisi su larga scala, con effetti su mercati, aziende, relazioni fra cittadini e pubblica amministrazioni, e così via[103]. Ad esempio, è possibile analizzare le dinamiche dei mercati e prevedere l'evoluzione di domanda e offerta, stabilendo così i prezzi di prodotti e servizi o quali categorie di consumatori potrebbero comprare un determinato bene in un certo arco temporale. Nell'ambito della salute possono essere estremamente preziosi in ambito epidemiologico, nelle attività di sorveglianza di sanità pubblica, nelle analisi dell'appropriatezza prescrittiva e dell'aderenza terapeutica, nel monitoraggio della spesa sanitaria, nello svolgimento di attività mirate di prevenzione, nel supporto alle decisioni cliniche, nella medicina di precisione e così via.

Tuttavia, «i dati non sono oggettivi e i modelli statistici rappresentano la realtà modificandola, e cioè orientando i comportamenti»[104]; i Big Data non sono neutri: la loro lettura e i modelli adoperati per la rappresentazione modificano la realtà che pretendono di descrivere, orientando aspettative e comportamenti; inoltre, la provenienza e la qualità dei dati, anche in termini di esattezza, sono fondamentali, poiché eventuali errori sui dati comportano, a cascata, errori nelle operazioni successivamente svolte. Ciò a maggior ragione in sanità, dove l'errore informativo può compromettere non solo la correttezza di un trattamento, ma l'autode-

ghi, M. Martoni (a cura di), *Strumenti, diritti, regole e nuove relazioni di cura. Il Paziente europeo protagonista nell'eHealth*, Giappichelli, Torino, 2015, pp. 155-176.

[102] G. Sartor, *L'informatica giuridica e le tecnologie dell'informazione. Corso d'informatica giuridica*, Giappichelli, Torino, 2016, p. 188. Ovviamente ciò comporta un vantaggio competitivo enorme per le grandi aziende che detengono una posizione monopolistica o dominante in determinati settori, come Google fra i prestatori del servizio di motore di ricerca, Facebook fra le reti sociali, Amazon fra le piattaforme di e-commerce. Ciò comporta un rafforzamento del loro potere verso i soggetti pubblici, che sono costretti a rivolgersi a questi poteri privati per acquisire informazioni necessarie allo sviluppo delle proprie politiche (ivi, p. 189).

[103] V. Mayer-Schönberger, K. Cukier, *Big Data: A Revolution That Will Transform How We Live, Work and Think*, John Murray, London, 2013, p. 10.

[104] A.C. Amato Mangiameli, *Algoritmi e big data. Dalla carta sulla robotica*, in «Rivista di filosofia del diritto», 1, 2019, p. 111. Su questi aspetti cfr. N. Lettieri, *Antigone e gli algoritmi*, cit.

terminazione informativa del paziente (si pensi alla raccolta del consenso in ambiente digitale)[105]. Qui la "cura del dato" è cura della persona che richiede necessariamente qualità, contestualizzazione, rispetto di principi etici e giuridici. Del resto, da tempo si è posto in evidenza come, in ragione della particolarità dei dati trattati, l'uso eticamente corretto dell'informazione assuma un'importanza fondamentale in ambito bioetico soprattutto con riferimento ai sistemi informatici[106], atteso che alcuni difetti presenti in tali sistemi possono comportare la fornitura di informazioni inesatte potenzialmente idonee a ledere il diritto all'autodeterminazione informativa[107] oltre che il diritto alla vita e alla salute, a seconda dei casi.

Sullo sfondo opera la profilazione automatizzata: come anticipato, si costruiscono plurime identità digitali (del consumatore, del paziente, dell'atleta, e così via) che non coincidono con la persona[108]. Interfacce conversazionali "umanizzate" attenuano la percezione della loro artificialità e interagiscono con persone, non con profili (anche se per tali sistemi, la persona viene ridotta a "profilo"). La cosiddetta gratuità dei servizi si traduce in corrispettivi non economici ma informativi (previa prestazione di numerosi consensi, magari inconsapevoli, con attenti tracciamenti delle condotte e imponenti raccolte di dati da archiviarsi ed elaborarsi)[109]. L'identità digitale, così, non è solo rappresentazione: divie-

[105] In una prospettiva informatico-giuridica si è osservato come sia difficoltoso assicurarsi della qualità dei dati che sono posti online e ciò si riverbera sull'affidabilità stessa delle elaborazioni compiute dai sistemi di *Big Data Analytics*, rischiando di vanificarne l'apporto anche in quei casi in cui sarebbe estremamente utile – ad esempio, in relazione alle emergenze epidemiologiche (cfr. R. Brighi, *The Quality and Veracity of Digital Data on Health: from Electronic Health Records to Big Data*, in «Revista de Bioética y Derecho», 42, 2018, pp. 163-179).

[106] In tal senso Comitato Nazionale per la Bioetica, *Etica, salute e nuove tecnologie dell'informazione*, Roma, 2006, p. 11.

[107] Un esempio appare emblematico: a causa di un errore software presente in un sistema utilizzato presso il dipartimento di immunologia dell'ospedale di Sheffield, a numerose donne era stato erroneamente diagnosticato di avere un basso rischio di dare alla luce bambini affetti da sindrome di Down (J.K. Gable, *An Overview of the Legal Liabilities Facing Manufacturers of Medical Information Systems*, in «Quinnipiac Health Law Journal», 5, 2001, p. 129).

[108] Su identità e IA cfr. M.N. Campagnoli, M. Farina, *Identità digitale e intelligenza artificiale: tra regolazioni, poteri asimmetrici e sfide per il futuro*, in «Journal of Ethical and Legal Tecnologies» 7, 1, 2025, pp. 81-115.

[109] Cfr., in particolare, G. Cerrina Feroni (a cura di), *Commerciabilità dei dati personali. Profili economici, giuridici, etici della monetizzazione*, Il Mulino, Bologna, 2024.

ne anche leva di governo dei comportamenti. Ciò vale anche quando la personalizzazione sembra "benigna" grazie alla sua utilità pratica: l'architettura dell'informazione influenza scelte e aspettative, per cui la neutralità dei contesti digitali è più presunta che reale.

Nell'ambito della salute, l'incidenza su diritti fondamentali (vita, salute, autodeterminazione) è diretta e particolarmente forte. Dispositivi indossabili, registri sanitari elettronici e fascicoli sanitari, congiunti a pratiche di medicina di precisione e a servizi di varia tipologia (da quelli per il fitness a quelli propriamente medici), prefigurano forme embrionali di rappresentazione digitale del paziente o comunque della persona, funzionali alla personalizzazione delle cure e, più ampiamente, della salute, fino a forme prototipali di «gemello digitale» non solo in ambito clinico, ma bisogna tener presente la necessità di evitare la degenerazione verso la «tirannia dei dati», ossia nella direzione di «comportamenti oppressivi di controllo e monitoraggio delle persone, oltre i limiti dettati dalle esigenze di salute individuale e pubblica»[110].

L'asse si sposta dalla spiegazione causale all'inferenza modellistica: un salto metodologico che chiede prudenza argomentativa e responsabilità istituzionale. Il potere effettivo di governare i riusi dei dati, infatti, tende ad assottigliarsi proprio quando la distanza tra chi fornisce i dati e chi decide sui modelli aumenta. Vi è dunque una duplice distanza: tra dati e persona, e tra persona e decisioni che i dati concorrono a orientare in modo più o meno determinante. Colmarla è compito non solo tecnico, ma giuridico-istituzionale, ed è necessario valutare con attenzione quando l'elaborazione dei dati consente di far avanzare la ricerca e la conoscenza scientifica, o quanto risponde a mere esigenze di mercato, così da poter adottare politiche più o meno restrittive a seconda dei casi.

Rendere effettivo il diritto alla protezione dei dati richiede allora un cambio di baricentro: dal solo "interessato" alla persona in relazione, situata in comunità e istituzioni, bilanciando protezione dei dati e ricerca.

Per la ricerca medica ciò non significa rinunciare alla conoscenza, ma condizionarne la legittimità: proporzionalità dei trattamenti, giustificazione degli accessi, controllo dei riusi. La prospettiva personalistica e relazionale consente di evitare tanto il culto del dato quanto la sua demonizza-

[110] S. Salardi, *Intelligenza artificiale e semantica del cambiamento: una lettura critica*, op. cit., p. 119.

zione. Bisogna dunque chiedersi quale conoscenza serve davvero la persona e la collettività, a quali condizioni, con quali controlli e quali strumenti di tutela. Al contempo, è necessario interrogarsi su quali interpretazioni o strumenti non portino alcun vantaggio alla persona (interessato) mentre, al contempo, diminuiscono la concreta possibilità di fare ricerca (e dunque di tutelare, in modo diffuso, il diritto alla vita e alla salute).

La normativa europea in materia di protezione dei dati personali ha certamente contribuito a sedimentare una cultura di tutela; ciononostante, nel quotidiano delle organizzazioni si sono prodotti talora irrigidimenti: quando il formalismo documentale sostituisce il giudizio sostanziale, gli adempimenti si moltiplicano senza migliorare le garanzie o senza tutelare effettivamente la libertà e la dignità degli interessati. Si giunge, così, a una dicotomia: responsabilizzazione e derive difensive. La prima richiede motivazioni, metriche spiegabili, revisione critica periodica; le seconde si riconoscono dall'ipertrofia di burocrazia e attestazioni, dove la forma prevale sulla sostanza. Questa dialettica si manifesta, in concreto, nella trama degli strumenti di regolazione tecnico-scientifica della cura (prescindendo, dunque, dall'ambito del benessere per quanto riguarda le considerazioni che seguono).

In tale prospettiva, tale regolazione (assunta in senso ampio) include non solo linee guida, protocolli e PDTA (percorsi diagnostico terapeutico assistenziali), ma anche procedure organizzative e cliniche, manuali per la qualità e l'accreditamento, procedure operative standard, sistemi di classificazione e codifica, regole di rimborso e criteri di appropriatezza, indicatori, programmi di vigilanza (come la farmacovigilanza), strumenti di supporto decisionale, soglie di allerta e triage, specifiche di interoperabilità e sicurezza, politiche per la telemedicina, capitolati di acquisto e requisiti di gara, nonché esiti di valutazione delle tecnologie sanitarie. Tali dispositivi non sono neutri: traducono evidenze e valori in architetture operative, allocano oneri di diligenza e delimitano gli spazi dell'appropriatezza.

Il rischio di un'adesione meramente difensiva riguarda l'intero insieme di questi dispositivi. Operano, in particolare, tre spinte strutturali: (i) l'asimmetria dei costi dell'errore in contesti di controllo *ex post*, che incentiva strategie di minimizzazione della varianza decisionale (è più facile contestare l'inosservanza formale che valutare una deviazione motivata); (ii) la trasformazione di strumenti conoscitivi in vincoli com-

portamentali attraverso sistemi di accreditamento, indicatori di processo e requisiti di rimborso, con l'effetto che la misura, assunta come obiettivo, perde capacità informativa e finisce per eterodirigere la prassi; (iii) la pressione organizzativa (tempi, carichi, frammentazione delle responsabilità, rischio di contenzioso) che privilegia la conformità meramente formale e affievolisce la responsabilità sostanziale (che richiede valutazione nel merito). Gli esiti sono ricorrenti: incremento degli oneri documentali, ridondanza delle liste di controllo e standardizzazione ingiustificata, anche quando un caso concreto richiederebbe deviazioni motivate.

L'alternativa è una responsabilizzazione sostanziale che coinvolge: (i) la diligenza come giustificazione in concreto delle decisioni e facoltà di deviazione motivata rispetto agli schemi; (ii) il monitoraggio come ciclo di verifica con effetti reali sull'agire (revisione periodica delle metriche, controllo indipendente, correzione degli esiti); (iii) l'appropriatezza come criterio di personalizzazione proporzionata, non come pretesto uniformante. In tale logica, l'onere primario non è l'accrescimento della produzione documentale e della burocrazia, ma la giustificabilità pubblica e controllabile delle decisioni: esplicitazione dei presupposti, tracciabilità dei criteri, giustificabilità pubblica delle scelte e predisposizione di strumenti di tutela effettivi, tenendo sempre conto del fatto che, affinché ciò possa realizzarsi, è necessario stabilire dei tetti massimi al rapporto numerico fra operatori sanitari e pazienti (per l'ambito clinico), affinché sia possibile riservare un periodo di tempo adeguato a ciascuna persona (prima di essere "assistiti" si è "persone").

Nell'ambito della ricerca, è necessario invece soffermarsi su due profili prima di effettuare una riflessione conclusiva sull'impatto del dataismo.

In primo luogo, la distinzione tra anonimizzazione e pseudonimizzazione va letta in concreto, "per chi" e "con quali mezzi ragionevoli": l'identificabilità deve essere valutata in funzione del contesto, delle tecniche disponibili, dei costi e dei tempi prevedibili, oltre che delle misure effettivamente adottate. Dati ragionevolmente anonimi per determinati soggetti possono essere impiegati lecitamente a fini di studio senza pregiudizio per la persona. Questo criterio consente un bilanciamento proporzionato da svolgersi caso per caso, portando a risultati più solidi per i singoli, minori ostacoli ingiustificati per gli operatori e, soprattutto, una miglior tutela della salute pubblica. Bisogna dunque chiedersi chi possa realmen-

te re-identificare, con quali strumenti e con quali costi, non in via astratta bensì in riferimento a ciascun caso concreto[111].

In secondo luogo, la scelta della base giuridica deve evitare scorciatoie speculari: l'estensione indiscriminata del consenso come chiave universale e la compressione di basi legali specifiche per la ricerca conducono, entrambe, a esiti inefficienti e iniqui. Se le misure sono adeguate (inclusa una pseudonimizzazione robusta) e rendono non ragionevolmente identificabili i soggetti per chi tratta, un vincolo impeditivo che arresti studi socialmente utili sarebbe ingiustificato e iniquo. La risposta non è solo tecnica, in quanto entrano in gioco intervengono la valutazione dei profili etici (con l'importante ruolo dei Comitati etici territoriali), la responsabilità del titolare, il sindacato degli organi competenti. L'interesse dell'interessato è a non essere danneggiato; l'interesse della persona è che la ricerca possa procedere.

L'orizzonte è quello di una responsabilizzazione diffusa, verificabile e svolta su basi concrete, considerando che, nel governo della salute e del-

[111] Questa interpretazione è conforme al considerando n. 26 GDPR, che fa riferimento ai mezzi di cui il titolare o un terzo possa ragionevolmente avvalersi per identificare una persona fisica. Particolarmente rilevante è, sul punto, la posizione della Corte di Giustizia dell'Unione europea: «non si deve ritenere che i dati pseudonimizzati costituiscano, in ogni caso e per qualsiasi persona, dati personali […] in quanto la pseudonimizzazione può, a seconda delle circostanze del caso di specie, effettivamente impedire a persone diverse dal titolare del trattamento di identificare l'interessato in modo tale che, per esse, quest'ultimo non sia o non sia più identificabile» (Corte di giustizia, 4 settembre 2025, causa C-413/23 P, Garante europeo della protezione dei dati contro Comitato di risoluzione unico). La Corte è stata chiamata a decidere sull'annullamento della sentenza del Tribunale dell'UE del 26 aprile 2023 (CRU/GEPD, T-557/20), in cui il Tribunale aveva già correttamente evidenziato come i dati pseudonimizzati non debbano sempre essere considerati dati personali in quanto tale nozione è relativa e varia in considerazione del soggetto che potrebbe identificare o re-identificare gli interessati). Ciò che la Corte afferma è del tutto condivisibile e ribadisce che la qualificazione giuridica del dato richiede un accertamento puntuale e contestuale della ragionevole probabilità di reidentificazione riferibile a soggetti determinati, valutando il contesto d'uso, i mezzi tecnici disponibili (e prevedibili), i costi e i tempi, nonché le misure tecniche e organizzative effettivamente implementate. In tale prospettiva, l'impiego di basi di dati ragionevolmente anonimizzate risulta giuridicamente giustificato e scientificamente produttivo, poiché consente un bilanciamento proporzionato tra tutela dei dati e avanzamento della ricerca, con benefici per tutti i portatori di interesse: per gli individui, che accedono a risultati scientifici più avanzati; per gli operatori, che non sono frenati da assetti eccessivamente protezionistici; per gli Stati, che possono meglio garantire diritti e salute dei consociati, riducendo potenzialmente i costi dell'assistenza e innalzandone la qualità.

la cura, responsabilizzare non significa moltiplicare adempimenti, bensì ancorare l'azione a criteri sostanziali di giustificazione pubblica orientati agli esiti di salute individuali e collettivi.

La diligenza non coincide con l'adesione letterale a schemi predeterminati: esige la possibilità di una deviazione motivata quando il caso concreto lo richiede, ma anche quando la prospettiva si allarga alla prevenzione, alla promozione della salute e alla comunicazione del rischio, dove scelte proporzionate devono essere rese trasparenti nelle loro assunzioni e nelle alternative considerate.

Il monitoraggio non è la mera contabilizzazione di indicatori: è un ciclo di apprendimento che collega metriche, verifica indipendente e correzione degli esiti, evitando che l'indicatore – divenuto obiettivo – perda capacità informativa; in sanità pubblica ciò si traduce nella capacità di leggere gli esiti nelle popolazioni, di intercettare diseguaglianze e di verificare se gli interventi digitali producano benefici distribuiti in modo equo. L'appropriatezza non è uniformazione: è personalizzazione proporzionata che modula protocolli e linee guida alla luce della persona e del contesto, ma che, nella dimensione della salute, include anche la ragionevolezza degli interventi preventivi e la coerenza tra mezzi impiegati e benefici attesi per la comunità.

Possono tuttavia registrarsi fenomeni degenerativi e, nella specie, si produce una deriva difensiva quando i tre assi si irrigidiscono; la diligenza si riduce a formalismo (cieca adesione), il monitoraggio a mero conteggio di indicatori, l'appropriatezza a conformismo protocollare. Ciò vale sia a livello di pratica clinica sia di più ampie e generali politiche nell'ambito della salute, dove piani e programmi possono scivolare verso una compliance formalistica che occulta la valutazione nel merito. L'asimmetria dei costi dell'errore e la prevalenza di controlli *ex post* alimentano tale esito: è più semplice sanzionare l'inosservanza formale che valutare una deviazione argomentata o un adattamento di policy fondato su evidenze emergenti.

In controtendenza, la centralità del giudizio professionale controllabile va salvaguardata mediante condizioni abilitanti reali – tempi effettivi, carichi sostenibili, lavoro d'équipe ove necessario – senza le quali la valutazione resta meramente formale. I dati, in questa cornice, sono mezzi e non fini: servono a giustificare scelte cliniche e di salute pubblica, non a surrogarne il ragionamento. L'epistemica dell'azione in sanità richiede

trasparenza delle assunzioni, controllo del contesto e rigore esplicativo; le correlazioni orientano, non sostituiscono la spiegazione, e l'utilità va verificata rispetto agli esiti rilevanti per le persone e per le comunità. Ne discende la centralità non dell'accumulo documentale, bensì della forza argomentativa delle decisioni: verificabilità, coerenza con gli esiti e capacità di rendere ragione tanto delle conformità quanto delle eccezioni, con attenzione all'equità nella distribuzione di benefici e oneri.

Così intesa, la responsabilizzazione contrappone la persona alla ricerca, la privacy alla salute e alla cura: ordina strumenti, dati e procedure attorno alla persona in relazione e alla comunità, privilegiando giustificazioni pubbliche, controlli effettivi e rimedi praticabili rispetto al mero adempimento. In equilibrio tra diligenza motivata, monitoraggio che apprende e appropriatezza proporzionata, la regolazione tecnico-scientifica della salute e della cura evita la burocrazia difensiva e sostiene decisioni migliori, orientate alla dignità della persona e all'equità degli esiti di salute.

II.6. Sicurezza e cibersicurezza

La riflessione sui profili etici e giuridici della salute digitale impone di affrontare un'ulteriore questione trasversale, che esige un approccio interdisciplinare: la sicurezza e la cibersicurezza. Com'è noto, la nozione di "sicurezza" è ampia; per essa può intendersi, in termini generali, una funzione di garanzia: lo stato e la pratica istituzionale di protezione, orientata alla tutela della persona, dei diritti e delle funzioni essenziali (nella salute e nel benessere), che organizza il governo del rischio mediante l'identificazione e la riduzione delle vulnerabilità, la prevenzione, la rilevazione, la resistenza e il recupero, secondo i principi di necessità e proporzionalità e attraverso doveri positivi di protezione e responsabilizzazione, evitando derive securitarie.

La cibersicurezza ne è una specificazione settoriale e può intendersi come «l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche» (art. 2, par. 1, Reg. (UE) 2019/881, c.d. Cyberse-

curity Act)[112]. Al suo interno, la sicurezza dei sistemi e dei modelli di IA costituisce una specificazione ulteriore.

Nella prospettiva della vulnerabilità aumentata, la sicurezza delle reti e dei sistemi (cibersicurezza) e della persona nell'interazione con artefatti digitali compongono un'unica architettura delle garanzie, orientata alla tutela della dignità, della salute e del benessere. Questa architettura, lungo l'intero ciclo di vita tecnologico, determina doveri di protezione, criteri di prevenzione, controllo e rimedio, nonché regole di responsabilità secondo i principi di proporzionalità e necessità.

Entrambe sono oggi centrali: la cibersicurezza, poiché reti e sistemi informativi costituiscono infrastrutture essenziali da cui dipende – con intensità variabile a seconda dei contesti – l'operatività di soggetti pubblici e privati; la sicurezza, in senso lato, perché la pervasività del digitale impone la protezione di beni, persone e diritti in molteplici settori e a tutti i livelli. Con precipuo riferimento ai sistemi di IA, è opportuno distinguere sin d'ora tra sicurezza "interna" (robustezza, affidabilità, resilienza ad attacchi e malfunzionamenti) e sicurezza "esterna" o sistemica (impatti su reti, servizi, organizzazioni e persone, inclusi i rischi sistemici e di filiera), valutando tanto i rischi intrinseci ai modelli quanto quelli che la loro integrazione introduce nell'ambiente.

La cibersicurezza non è, però, una questione meramente "tecnico-ingegneristica"[113], ancorché si basi su tre principi chiave, riassunti nella c.d. triade CIA: *confidentiality* (confidenzialità o riservatezza), *integrity* (integrità), *availability* (disponibilità)[114]; essa è ormai fondamentale per la dife-

[112] Per «minaccia informatica», «qualsiasi circostanza, evento o azione che potrebbe danneggiare, perturbare o avere un impatto negativo di altro tipo» sui predetti sistemi e soggetti (art. 2, par. 8, Reg. (UE) 2019/881). La «minaccia informatica significativa» è quella che, in base alle caratteristiche tecniche, si presume possa avere un grave impatto sui sistemi informatici e di rete di un'entità o sugli utenti dei relativi servizi, causando perdite materiali o immateriali considerevoli (art. 6, n. 11, Dir. (UE) 2022/2555 – NIS2).

[113] R. Brighi, *Cybersecurity. Scenari tecnologici e regolamentazione di un'area in espansione*, in Th. Casadei, S. Pietropaoli (a cura di), *Diritto e tecnologie informatiche*, cit., p. 77.

[114] La confidenzialità si riferisce al rispetto delle restrizioni circa l'accesso e la divulgazione delle informazioni in tutto il loro ciclo di vita, mentre l'integrità indica la protezione delle informazioni da modifiche o cancellazioni non autorizzate nonché la garanzia di non ripudiabilità e di autenticità dei dati stessi. Infine, la disponibilità concerne l'accesso tempestivo e affidabile alle informazioni, oltre alla loro fruibilità in modo continuativo ed efficiente. Come affermato da ENISA, «la cibersicurezza copre tutti gli aspetti della

sa degli Stati e degli ordinamenti democratici ed è un prerequisito per lo stesso funzionamento della società contemporanea e per la tutela dei diritti e delle libertà delle persone fisiche e, per quanto applicabile, giuridiche. Non a caso, il legislatore europeo ha progressivamente intensificato gli sforzi regolatori in materia e il quadro regolatorio è oramai complesso e stratificato[115]: anche sin troppo, rendendo difficile orientarsi in esso, e ciò vale sia per i giuristi sia per tutti gli operatori dei vari settori coinvolti, con normative assai minuziose che, nell'estrema complessità, rendono difficile e costosa una conformità effettiva anche solo per comprendere quali siano effettivamente gli obblighi che ne scaturiscono. Sarebbe forse più opportuno riflettere sull'adozione di una prospettiva diversa, sì basata sul rischio e sull'*accountability*, ma, al contempo, prevedendo un numero relativamente ristretto di obblighi chiari e ben distinti in base a criteri certi e univoci.

Tanto premesso, prima di discuterne brevemente i profili più rilevanti per la sanità digitale e l'informatica medica, appare opportuno menzionare brevemente le principali minacce informatiche relative ai sistemi "tradizionali" e a quelli di IA, che permettono di cogliere ulteriori aspetti della vulnerabilità aumentata. È un ambito ampio e, partendo dai sistemi informatici tradizionali (ossia escludendo i sistemi di IA), ai fini della presente trattazione appare opportuno partire da una mappatura sintetica delle principali minacce informatiche[116]: (i) *ransomware*[117];

prevenzione, previsione, tolleranza, rilevamento, mitigazione, rimozione, analisi e investigazione degli incidenti informatici. Considerando i diversi tipi di componenti del cyberspazio, la cybersicurezza dovrebbe includere i seguenti attributi: disponibilità, affidabilità, sicurezza, riservatezza, integrità, manutenibilità (per sistemi tangibili, informazioni e reti); robustezza, sopravvivenza, resilienza (per supportare la dinamicità del cyberspazio); responsabilità, autenticità e non ripudio (per garantire la sicurezza delle informazioni)» (ENISA, *ENISA overview of cybersecurity and related terminology*, Heraklion, 2017, p. 6).

[115] Oltre al GDPR (e al connubio inscindibile fra privacy e sicurezza), possono qui citarsi: il "*Cybersecurity Act*" (Reg. (UE) 2019/881, regolamento sulla cibersicurezza), il "*Cyber Resilience Act*" (Reg. (UE) 2024/2487, regolamento sulla ciberresilienza), la direttiva NIS2 (Dir. (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione europea, recepita in Italia con il d.lgs. 138/2024), il regolamento DORA (Reg. (UE) 2022/2554 relativo alla resilienza operativa digitale per il settore finanziario).

[116] La mappatura fa riferimento a quanto osservato da ENISA, *ENISA threat landscape 2024*, Attiki-Heraklion-Brussels, 2024, pp. 7-8.

[117] Attacchi in cui un soggetto ottiene l'accesso non autorizzato a risorse informative e ne impedisce l'uso legittimo (tipicamente mediante cifratura o blocco operativo), pretendendo un riscatto per il ripristino. La pressione estorsiva è spesso aumentata dalla

(ii) *malware*[118]; (iii) ingegneria sociale[119]; (iv) violazioni dei dati (personali e non)[120]; (v) negazione del servizio (*Denial of Service*, DoS; se distribuita, DDoS)[121]; (vi) manipolazione delle informazioni[122]. In tutti que-

minaccia di pubblicare o distruggere i dati sottratti, così da massimizzare il danno reputazionale, interrompere l'operatività o ottenere altri vantaggi.

[118] Software malevolo concepito per eseguire processi non autorizzati idonei a ledere riservatezza, integrità o disponibilità. Rientrano in questa classe, tra gli altri, i virus che si replicano all'esecuzione agganciandosi a file legittimi, i *trojan* (cavalli di Troia) che si presentano come leciti occultando funzioni dannose, i *worm* che si propagano autonomamente in rete, gli *spyware* che sorvegliano l'attività dell'utente e i *rootkit* che si nascondono nel sistema per conferire privilegi elevati all'attaccante. Il *ransomware* ne è una sottospecie con finalità estorsive.

[119] Insieme di tecniche che sfruttano il fattore umano per ottenere informazioni o accessi o per indurre condotte pregiudizievoli. Ne sono espressione, in particolare, le comunicazioni che imitano fonti affidabili per carpire credenziali (come il *phishing*), i messaggi via SMS (*smishing*) o telefonate (*vishing*), la compromissione di siti abitualmente frequentati (*watering hole*), l'uso di "esche" che spingono a compiere azioni rischiose (*baiting*), la costruzione di scenari o identità fittizie (*pretexting*), la promessa di vantaggi in cambio di accessi o dati (*quid pro quo*), l'adescamento relazionale (*honeytrap*) e i falsi avvisi di sicurezza che inducono ad installare programmi dannosi o inutili (*scareware*). Queste tecniche non operano solo nella fase di ingresso: possono essere impiegate anche per consolidare il controllo, alimentare frodi (ad esempio, compromissione dell'e-mail aziendale), sostituirsi alla vittima o estorcere ulteriori pagamenti.

[120] Nel GDPR (art. 4 (12)) la violazione dei dati personali è così definita: «la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati». Le minacce ai dati assumono, sul piano tecnico, due configurazioni principali. Si parla di violazione dei dati (*data breach*) quando vi è un'azione intenzionale volta a ottenere accesso non autorizzato e a sottrarre o divulgare informazioni sensibili, riservate o protette. Si parla invece di fuga di dati (*data leak*) quando l'esposizione è non intenzionale e dipende da errori, configurazioni errate o vulnerabilità non presidiate.

[121] Gli attacchi di negazione del servizio ne minano la disponibilità: l'utente legittimo non riesce ad accedere a risorse o servizi perché si saturano, deliberatamente, componenti applicativi o di rete. La saturazione può avvenire per invio massivo di richieste oltre la capacità di risposta (*flooding*) o mediante tecniche di amplificazione che moltiplicano il traffico verso il bersaglio, anche orchestrando molteplici sorgenti coordinate: in tal caso si parla di DDoS. L'impatto è spesso dimostrativo o circoscritto nel tempo, ma può divenire significativo quando colpisce funzioni critiche o quando si combina con richieste estorsive o altre azioni sinergiche.

[122] Per manipolazione delle informazioni si intendono pratiche intenzionali e coordinate che alterano contesti informativi con l'obiettivo di orientare percezioni e decisioni collettive, incidendo su valori, procedure e processi, in particolare politici e istituzionali. Possono essere poste in essere da attori statali o non statali, anche attraverso reti

sti casi può registrarsi un tratto comune: lo sfruttamento delle vulnerabilità – tecniche, organizzative e umane – che, nell'ecosistema della salute digitale, si traducono in rischi non solo per sistemi e dati, ma anche per la persona, la sua dignità e il suo benessere.

Tali minacce non sono nuove, ancorché da un punto di vista tecnico si evolvano costantemente, e sono idonee a colpire anche i sistemi di IA, che sono a loro volta esposti a minacce ulteriori. L'IA, inoltre, è "a doppio uso": può potenziare tanto l'offesa quanto la difesa. È una risorsa, anche assai preziosa, nel contrasto alle minacce informatiche e al rafforzamento dei relativi strumenti (si pensi al rilevamento delle minacce, *threat detection*, e alla risposta agli incidenti, *incident response*, adoperando tecniche di apprendimento automatico, ossia *machine learning* e *deep learning*[123]); è tuttavia una minaccia quando viene utilizzata per scopi illegali, in quanto consente di incrementare significativamente le potenzialità offensive degli attaccanti.

Prendendo come riferimento gli attacchi informatici, anche per la loro significatività, si possono qui menzionare: (i) *Data poisoning* (avvelenamento dei dati di addestramento)[124]; (ii) *Adversarial attacks* (attacchi antagonisti)[125]; (iii) *Model extraction* (estrazione del modello) e *Model*

di agenti interne ed esterne a un territorio; spesso non violano formalmente la legge, ma agiscono sull'asimmetria informativa e sulla visibilità dei messaggi – tra media tradizionali e piattaforme digitali – per produrre effetti reali su comportamenti e scelte.

[123] Una metodologia evoluta di apprendimento automatico impiegata per estrarre conoscenze in modo autonomo da ampi volumi di dati.

[124] Si effettua attraverso l'introduzione di informazioni volutamente errate o manipolate nei dataset di training così da alterare le prestazioni e il comportamento del modello di IA, e dunque del sistema, compromettendone accuratezza e affidabilità del sistema (può infatti provocare regressione, errori di classificazione, ecc.) e dunque potenzialmente rendendolo inutilizzabile.

[125] Sono finalizzati a ingannare il modello mediante input (anche grafici, come le immagini) non percettibili dagli operatori umani, così che il sistema di IA fornisca risposte errate o effettui condotte inattese (minando ad esempio il funzionamento di sistemi di visione artificiale, di riconoscimento vocale o di elaborazione del linguaggio naturale). Di particolare interesse sono gli attacchi antagonisti di tipo *concept drift*: in linea generale, il *concept drift* si ha quando un modello predittivo perde progressivamente accuratezza a causa della modifica dei dati col passare del tempo, rendendo necessario aggiornare il modello o adottare strategie per mantenerne la capacità predittiva. In una prospettiva malevola, invece, si può manipolare in modo graduale (*incremental drift*), improvviso (*sudden drift*) o ricorrente (*recurring* drift) il flusso di dati. In tal modo il sistema, rispettivamente, non

inversion (inversione del modello)[126] (iv) *Membership inference*[127] (inferenza sull'appartenenza). Per completezza, si consideri che i bias e le discriminazioni sono ancor più pericolosi delle minacce informatiche, in quanto i modelli di IA possono replicare e amplificare forme di discriminazione nel caso in cui i dati di addestramento non siano rappresentativi o siano espressione di pregiudizi, mettendo dunque a rischio diritti fondamentali e non.

Il quadro qui tratteggiato è particolarmente rilevante anche nell'ambito della salute digitale, considerando che essa è caratterizzata da strumenti sia informatici sia di IA e che la loro cibersicurezza diviene un presupposto fondamentale per il suo corretto funzionamento. Con precipuo riferimento ai sistemi di IA, in un'epoca in cui anche l'operato degli esseri umani dipende da tali sistemi, l'aumento delle "allucinazioni" (ossia di risposte errate, ma presentate come corrette) può avere conseguenze assai gravi; non può negarsi che molti facciano affidamento su di essi, dando magari per scontata la correttezza delle risposte ricevute o delle decisioni prese. Che ciò avvenga per negligenza, imperizia, imprudenza, poco conta: comunque avviene e bisogna tenerne conto. È fondamentale, dunque, educare all'uso delle tecnologie e dei sistemi di IA.

Vi è di più. Nelle more, come si è autorevolmente affermato, si deve evitare una eccessiva dipendenza dall'IA in relazione alla cibersicurezza, bilanciandola con fattori individuali e sociali[128]. Si deve tuttavia prendere in considerazione la questione della dipendenza dalle norme tecniche, che, come dimostra a titolo esemplificativo l'IA Act, vanno sostanzialmente a regolare il vasto ambito – tecnicamente ed eticamente complesso – delle tecnologie digitali più innovative. Pertanto, il loro contenuto dovrà necessariamente comprendere valutazioni delicate su valori e diritti fondamentali dell'UE, impattando pesantemente sulla vita degli individui, mentre la normazione tecnica armonizzata acquisi-

riuscirà a riconoscere le istanze sospette, reagire con tassi di errore elevati, o non reagire efficacemente dinanzi a *pattern* "vecchi" se è stato tarato su quelli nuovi.

[126] Sono attacchi finalizzati a ricostruire la logica interna del sistema e/o estrarre i dati di addestramento interagendo con il medesimo (ad esempio attraverso le API).

[127] Consente di determinare se un dato sia stato incluso nel dataset di addestramento, con potenziale impatto sulla privacy e sulla protezione dei dati personali.

[128] L. Floridi, *The Ethics of Artificial Intelligence*, cit., p. 139. Cfr. altresì, fra gli altri, M. Taddeo, T. McCutcheon, L. Floridi, *Trusting artificial intelligence in cybersecurity is a double-edged sword*, in «Nature Machine intelligence», 1, 2019, pp. 557-60.

sce nuove dimensioni, giungendo al piano politico, economico, geopolitico, giuridico ed etico[129].

È anche importante adottare un approccio ragionato e concreto alla tematica della sicurezza e della cibersicurezza dei sistemi di IA. È necessario svolgere valutazioni specifiche su ciascun sistema di IA, che di per sé potrebbe presentare rischi elevati *ex lege*, ma, al contempo, essere ipoteticamente esposto a minori rischi per ciò che concerne le sue caratteristiche tecniche e di utilizzo. A titolo esemplificativo, potrebbe infatti essere adoperato in locale da operatori qualificati in ambiente anche materialmente protetto, risultando difficilmente attaccabile dall'esterno. Questo esempio evidenzia altresì quanto sia difficoltoso il compito del legislatore, mentre quanto discusso sinora mostra l'imprescindibilità di un approccio non meramente multidisciplinare, bensì interdisciplinare per regolamentare, governare e orientare efficacemente l'IA. Difatti, le diverse discipline coinvolte devono necessariamente dialogare e confrontarsi tra loro, scambiando concetti, metodologie e prospettive teoriche e applicative, giungendo a una "contaminazione di saperi" che rappresenta la condizione necessaria per raggiungere un fondamentale obiettivo comune: regolare efficacemente l'IA, senza tuttavia ostacolarne lo sviluppo. È oramai cruciale orientare in modo effettivo l'IA affinché rappresenti uno strumento per il progresso e il benessere della società nel suo complesso, e non per favorire la concentrazione delle risorse e dei benefici economici nelle mani di pochi attori oligopolistici in grado anche di manipolare l'informazione e i mercati, controllando, in ultima analisi e in misura più o meno intensa, addirittura la politica interna ed esterna degli Stati e, per ciò che concerne l'ambito di indagine del presente volume, la salute di individui e comunità, in modo più o meno indiretto.

La sicurezza, inoltre, ha struttura intrinsecamente relazionale: la vulnerabilità di un nodo sanitario – struttura ospedaliera, fornitore, professionista – si riverbera sulla rete di cui è parte. Ne deriva che la distribuzione degli oneri di prevenzione, controllo e rimedio non può essere affidata a mere economie di scala o a clausole di stile; occorrono criteri di equità distributiva che impediscano di scaricare il rischio sui soggetti più esposti e rendano esigibili i doveri di diligenza e correttezza lungo l'intera

[129] In tal senso A. Volpato, *Il ruolo delle norme armonizzate nell'attuazione del regolamento sull'intelligenza artificiale*, in «Quaderni AISDUE», 2, 2024, p. 17.

filiera tecnologica e organizzativa. La sicurezza, così intesa, crea e consolida la fiducia negli strumenti digitali e in ciò che viene svolto tramite essi.

Infine, bisogna guardare alla sicurezza nella prospettiva della tutela della persona (e delle comunità), nel senso che anche la normazione tecnica deve tradurre operativamente scelte etiche e giuridiche che devono restare contestabili e rivedibili. Più in generale, la cibersicurezza nell'ambito della salute svolge una funzione di protezione dell'ecosistema, riduce la vulnerabilità senza violare la dignità e rende possibile l'innovazione e il progresso della ricerca scientifica tutelando i vari diritti coinvolti. È un costo: ma vale la pena sostenerlo.

III. Applicazioni e pratiche della salute e della cura digitale

III.1. Introduzione

Come la Società algoritmica contribuisce a plasmare la società nel suo complesso, incidendo sull'esistenza dei suoi consociati attraverso strumenti divenuti d'uso quotidiano e parte della loro quotidianità[1], così il mondo della salute digitale non si esaurisce nella mera integrazione di strumenti e servizi nelle strutture tradizionali di cura e nel dominio del benessere: concorre, in modo talora determinante, a modellare vita, salute e autodeterminazione. Ne sono paradigmatici i sistemi informativi sanitari (oramai necessari per il corretto funzionamento organizzativo e clinico) e le app e i dispositivi mobili che orientano le condotte degli utilizzatori in vista del miglioramento del benessere psico-fisico.

Applicando il criterio ordinatore delineato nel capitolo precedente, si può dunque guardare alle applicazioni e alle pratiche della salute e della cura digitale per stabilire quando l'apporto del digitale accresce le capacità effettive della persona (comprendere, scegliere, prendersi cura di sé) e quando, invece, diventa fine a sé o mezzo per tutelare interessi di terzi (di burocrazia, di medicina difensiva o di profitto), relegando in secondo piano la persona. Ciò non nega la legittimità di tali interessi; afferma, però, la loro subordinazione alla tutela dei diritti fondamentali. È legittimo ed etico documentare le scelte compiute o raccogliere il consenso informato; non lo è sovraccaricare il paziente di oneri informativi sproporzionati che non aumentano comprensione né qualità della presa in carico. Parimenti, è legittimo ed etico immettere sul mercato un dispositivo per il monitoraggio individuale che supporti programmi di allenamento; non lo è farlo in assenza di valida base clinica e informativa, con metriche opache o funzioni di profilazione invasive, con impostazioni predefinite intrusive o con prassi che trasferiscono sulla persona rischi e responsabilità impropri, normalizzando una sorveglianza continuativa priva di proporzione.

[1] Ma ciò pone il rischio di un intorbidimento cerebrale che può discendere da un'eccessiva delega alla macchina, in relazione a cui gli unici rimedi a disposizione degli esseri umani sono costituiti da riflessività e vigilanza (L. Corso, *Breve tassonomia dei rapporti fra Intelligenza Artificiale, etica e diritto. Tre questioni*, in «AI Law», 2, 2025, p. 222).

Questi divari e questi contrasti devono essere letti nella prospettiva della vulnerabilità aumentata: non come rifiuto della tecnica, ma come rischio di oggettificazione e di eterodeterminazione che si sostituiscono alla persona quale soggetto al centro della salute digitale e alla sua autodeterminazione.

Di qui la necessità di approfondire criticamente quelle applicazioni e quelle pratiche ritenute maggiormente idonee a incidere, in prospettiva sia attuale sia futura, sul complesso e fragile ecosistema della salute digitale.

In tal senso, appare opportuno partire dai sistemi informativi sanitari e dalle cartelle sanitarie elettroniche, che non sono il frutto di mere scelte tecniche od organizzative, o del passaggio dal cartaceo al digitale (che è, comunque, non semplice e richiede il ripensamento di tutti i processi organizzativi). L'infrastruttura informatica nel suo complesso diviene essenziale e travalica l'ambito della singola struttura sanitaria: essa diventa la trama che rende possibile la continuità della presa in carico; da essa dipendono, in concreto, i tempi e la qualità delle decisioni cliniche e organizzative e, non di rado, si ridisegna la distribuzione di oneri e poteri lungo filiere che superano il perimetro del singolo ente. L'interoperabilità non coincide con la conversione dei formati: senza un linguaggio clinicamente condiviso e senza regole semantiche stabili, il dato si decontestualizza, alimenta errori sistematici e indebolisce l'affidabilità delle inferenze. Identificazione univoca del paziente, accessi tracciati, disponibilità e integrità delle registrazioni sono condizioni giuridiche della tutela, non meri profili tecnici: l'opacità mina la sicurezza delle cure e rende le scelte incontestabili. Dove questi presidi – inclusa una cibersicurezza commisurata al rischio – sono effettivi, la vulnerabilità si riduce; dove prevalgono frammentazione e oscurità, cresce l'esposizione informativa e si assottigliano i margini di tutela della salute.

Vi è di più. La telemedicina e la *mobile health* (*m-health*) trasformano la cura sul piano spaziale e temporale, ma anche la più ampia "ricerca del benessere". Il monitoraggio continuo reso possibile da sensori e applicazioni può colmare i vuoti tra prestazioni, sostenere l'aderenza e prevenire o anticipare criticità; a condizione, però, che resti ancorato a finalità determinate, a misure proporzionate e a finestre temporali definite, con canali e tempi di ricontatto esplicitati e responsabilità chiare. In assenza di tali condizioni, la quotidianità rischia di convertirsi in sorveglianza e medicalizzazione non orientate alla tutela della vita e della salute o al leci-

to miglioramento del benessere, ma funzionali a esigenze di burocrazia, di medicina difensiva o di profitto.

Lo scenario diviene ancor più complesso e delicato nei contesti della robotica e delle tecnologie assistive, nei quali sistemi materiali guidati da software complessi operano sul corpo del paziente, pur se manovrati da personale formato e competente. In prospettiva, l'innesto diretto di componenti sul corpo, superando il mero ripristino funzionale e spingendosi verso il potenziamento, riapre questioni bioetiche (liceità dei mezzi e dei fini) e giuridiche (limiti agli atti di disposizione del proprio corpo), con il rischio di trasformazioni irreversibili, e fermo restando che già per ciò che concerne il profilo del ripristino funzionale (o dell'abilitazione nel caso di disabilità presenti sin dalla nascita)[2] si pongono ovvie questioni di eguaglianza sostanziale che investono, più in generale, le politiche sanitarie di ciascun ordinamento giuridico e il relativo servizio sanitario.

La tecnologia e la ricerca, dunque, assumono una centralità crescente fino a prospettive oggi consolidate come la medicina personalizzata e di precisione. Essa muove dall'individuale (raccolta di dati clinici e omici, tracce digitali, contesto), li elabora al livello generale (modellizzazione, stratificazione del rischio, validazioni e controllo di bias), per poi ritornare all'individuale (decisione sul singolo caso). Proprio questo passaggio dall'individuale al generale per tornare all'individuale è il suo punto di forza e, insieme, la sua vulnerabilità: ciò che è assente nei dati di partenza tende a mancare nelle generalizzazioni e, di riflesso, nelle decisioni; la calibrazione per sottogruppi, la verifica della generalizzabilità, la tracciabilità delle assunzioni e la spiegabilità proporzionata all'uso clinico diventano, quindi, condizioni di giustificazione. Le relazioni causali consentono motivazioni trasparenti; le correlazioni su basi dati ampie ed eterogenee richiedono un lavoro aggiuntivo di intelligibilità nella pratica e di umanizzazione del rap-

[2] È d'uopo precisare che «è sbagliato distinguere fra persone disabili e non disabili come se si trattasse di due liste dicotomicamente escludentisi. Nella vita si può, purtroppo, diventare disabili anche solo temporaneamente. […] Periodi di disabilità rientrano, infatti, nelle probabilità statistiche di una vita umana di lunghezza ed evoluzione differente, ma l'invecchiamento comporta in ogni caso, quando si valica la soglia che definisce un "grande anziano" elementi di disabilità. Disabilità è il nome di una condizione, non di una categoria di persone, e la possibilità di diventare disabile fa parte integrante della condizione umana in generale» (G. Zanetti, *Filosofia della vulnerabilità. Percezione, discriminazione, diritto*, Carocci, Roma, 2019, p. 138).

porto medico-paziente, per evitare nuove diseguaglianze dovute a squilibri informativi e a forme di riduzionismo.

Quanto sin qui esposto permette di cogliere il filo conduttore del capitolo, consistente nella riflessione critica, per ciascuna pratica paradigmatica, sulle conseguenze della vulnerabilità aumentata. In altri termini, è necessario interrogarsi sui profili teorico-pratici dell'innovazione, per comprendere quando tuteli la vita, la salute e l'autodeterminazione della persona e quando, invece, le leda, creando nuove forme di vulnerabilità o potenziando quelle preesistenti.

Esperienze come FACILITATE, trattato nel capitolo successivo, indicano che questa direzione è praticabile: il ritorno dei dati ai partecipanti come cerniera tra produzione di conoscenza e percorsi di cura; il riuso inteso come uso regolato e tracciabile, valutato alla luce dei suoi effetti concreti; la persona come interlocutrice reale, e non come "mera" assistita o "interessato" ai sensi del GDPR, lungo l'intero processo. Non si tratta di aggiungere adempimenti, ma di riallineare regole, prassi e tecniche all'architettura della salute e della cura, perché la società algoritmica non cristallizzi profili, bensì sostenga vita, salute e autodeterminazione.

III.2. Sistemi informativi sanitari ed *Electronic Health Records*

I sistemi informativi sanitari sono oggi molto diffusi e possono essere utilizzati per lo svolgimento di molteplici funzioni sia di carattere medico che amministrativo. In particolare, rendono possibili la creazione e l'aggiornamento di database dei pazienti, ivi comprese le loro cartelle cliniche, nonché l'ordinaria gestione amministrativa della struttura sanitaria che ne fa uso, con funzionalità per lo svolgimento delle attività cliniche, della ricerca scientifica, della didattica, e così via[3]. Nella Socie-

[3] Sui sistemi informativi sanitari cfr., fra gli altri, B. Blobel, *Analysis, design and implementation of secure and interoperable information systems*, IOS Press, Amsterdam, 2002; P. Cristiani, F. Pinciroli, M. Stefanelli (a cura di), *I sistemi informativi sanitari*, Patron, Bologna, 1996; T. Lippeveld, R. Sauerborn, C. Bodart (eds.), *Design and implementation of health information systems*, World Health Organization, Geneva, 2000; J.A. Magnuson, B.E. Dixon (eds.), *Public Health Informatics and Information Systems*, 3rd Edition, Springer, Cham, 2020; A. Rosotti, *Informatica Medica. Sistemi Informativi Sanitari e Reti di Telemedicina*, McGraw Hill, Milano, II ed., 2021.

tà dell'informazione e algoritmica, tali sistemi non sono meri archivi: strutturano i processi della salute e della cura, connettono attori e contesti (ospedalieri, territoriali, domiciliari, emergenza-urgenza, farmacie, servizi sociali), integrano prevenzione, diagnosi, terapia e riabilitazione, e sostengono la continuità assistenziale lungo l'intero percorso di vita.

Grazie ad un sistema ben realizzato risulta possibile migliorare l'assistenza sanitaria, poiché i dati relativi alle condizioni di salute dei pazienti possono venire consultati e trasferiti in tempi assai rapidi, agevolandone quindi la cognizione ed evitando che vengano duplicati qualora si faccia uso di un database unico. In tal modo, quindi, non è necessario immettere più volte le medesime informazioni relative a una stessa persona, con un evidente risparmio di tempo da parte del personale (e dunque con costi minori). Affinché ciò sia possibile devono tuttavia essere utilizzati standard che assicurino l'interoperabilità di sistemi diversi. Oltre all'interoperabilità "tecnica" è cruciale anche quella "semantica": i sistemi devono accordarsi non solo sul formato dei dati, ma sul loro significato clinico, altrimenti si moltiplicano fraintendimenti e si riduce la qualità decisionale.

Del resto, l'interconnessione delle diverse strutture sanitarie, anche a livello sovranazionale, assume sempre maggiore importanza nella società contemporanea, ove alla mobilità delle persone consegue la necessità di poterne reperire i dati sanitari in caso di necessità in qualsiasi posto esse vengano a trovarsi. Il tema investe l'intero *continuum* della salute e della cura – dalla prevenzione alla presa in carico, dalla gestione delle cronicità alla riabilitazione e all'assistenza di lungo periodo – nei contesti ospedalieri, territoriali e domiciliari, come pure nelle situazioni di mobilità transfrontaliera e nelle emergenze collettive: l'accesso tempestivo e proporzionato alle informazioni clinicamente rilevanti incide sugli esiti, sull'appropriatezza e sull'equità degli interventi.

Nella creazione dei moderni sistemi informativi sanitari si intrecciano sia esigenze tecniche che il dovere di rispettare alcune norme giuridiche preesistenti: standardizzazione anche per consentire l'interoperabilità di sistemi di varia tipologia; sicurezza dei dati contenuti nel sistema, nel rispetto delle normative sulla protezione dei dati personali, anche in virtù della sempre maggior diffusione di tecnologie di *cloud computing* e di dispositivi portatili (come i *tablet*); riduzione dei costi, che dovrebbe conseguirsi dall'utilizzo di un sistema ben realizzato; trattamento automatizzato dei dati, in modo da renderli facilmente accessibili ed utiliz-

zabili; usabilità, affinché questi sistemi siano degli strumenti che agevolino lo svolgimento delle attività in ambito sanitario[4] anziché rallentarle o renderle più onerose[5]. Contano i fattori umani: interfacce intellegibili, carico cognitivo contenuto, segnalazioni proporzionate (per evitare "stanchezza da allerta"), formazione continua che accompagni l'adozione e ne sostenga la maturità d'uso nel tempo.

I creatori di sistemi informativi sanitari, pertanto, devono far sì che le informazioni contenute nei relativi database siano accessibili, facilmente e senza ritardo, solo da soggetti legittimati[6] quando ciò è necessario: equilibrare queste esigenze non è, tuttavia, un compito facile. L'accesso deve essere proporzionato alle funzioni, tracciabile e giustificabile; affidabilità, tempi di risposta e continuità operativa sono dimensioni della qualità della cura e della salute non meno della correttezza dei contenuti.

Tali profili si intrecciano con quelli etici non solo in ordine al diritto alla riservatezza individuale e collettiva, ma anche, in linea più generale, con i principi di rispetto della dignità della persona, anche perché questi sistemi possono contenere l'intera storia clinica di ciascun paziente e dunque dati di estrema delicatezza. La "cura del dato" è parte della cura della persona: qualità, contestualizzazione e proporzione non sono artifizi retorici, ma condizioni di affidabilità e di giustizia.

[4] Le applicazioni pratiche, però, vanificano talvolta gli sforzi teorici. Emblematico in tal senso è uno studio commissionato dalla American Medical Association, in cui sono stati presentati e discussi diversi fattori critici evidenziati da numerosi medici statunitensi: scarsa usabilità delle cartelle cliniche elettroniche, lenta e onerosa immissione delle informazioni nei sistemi, interferenza col rapporto diretto col paziente, impossibilità di scambiare informazioni sanitarie fra diversi sistemi e peggioramento della documentazione clinica (M.W. Friedberg *et al.*, *Factors Affecting Physician Professional Satisfaction and Their Implications for Patient Care, Health Systems, and Health Policy*, RAND Health, Santa Monica, 2013, p. 33).

[5] Uno studio, ad esempio, ha mostrato – seppur sulla base di un campione limitato – che gli operatori sanitari adibiti al pronto soccorso impiegano il 44% del proprio tempo per l'inserimento di dati a fronte del 28% per il contatto con il paziente; inoltre, con una media di due pazienti e mezzo l'ora, effettuano ben quattromila click per ciascun turno di dieci ore (R.G. Hill, L.M. Sears, S.W. Melanson, *4000 Clicks: a productivity analysis of electronic medical records in a community hospital ED*, in «American Journal of Emergency Medicine», 31, 2013, pp. 1591-1594).

[6] Cfr. A. Lioy, *Riservatezza e sicurezza nei sistemi informativi sanitari*, in P. Cristiani, F. Pinciroli, M. Stefanelli (a cura di), cit., pp. 143-155.

Da un lato, proprio il non utilizzarli sarebbe suscettibile di cagionare danni assai gravi, potendo incidere negativamente sulla protezione del diritto alla salute degli assistiti, che potrebbe essere garantito più efficacemente, ad esempio, mediante l'effettivo utilizzo di sistemi informativi sanitari che consentano un rapido accesso ad informazioni sanitarie già acquisite nelle ipotesi di emergenza (ad esempio, per prestare le cure necessarie in seguito ad eventi traumatici) poiché diviene possibile offrire in tempi celeri cure adeguate al soggetto che ne necessita. Un impiego consapevole riduce errori terapeutici, evita duplicazioni inutili di esami, sostiene decisioni che devono essere prese in tempi ristretti (ictus, trauma, sepsi) e migliora l'aderenza ai percorsi di cura.

Dall'altro, utilizzarli comporta dei rischi, soprattutto in tema di sicurezza nella duplice prospettive dei loro utilizzatori e dei sistemi in sé e per sé.

In relazione alla prima, sovente il problema principale da affrontare non è la garanzia della sicurezza intrinseca di un sistema informativo, ma piuttosto la condotta dei suoi utilizzatori, i quali dovrebbero ricevere un'adeguata formazione per evitare che si verifichino casi di ingegneria sociale[7] e comunque per maneggiare con la dovuta cura gli strumenti informatici. Vi è così una vulnerabilità "interna", relativa a condotte colpose o dolose dei soggetti legittimati all'accesso, che può altresì concretizzarsi in seguito allo smarrimento di dispositivi mobili (come tablet, computer portatili, smartphone, periferiche di memorizzazione) per lo svolgimento di attività professionale e di ricerca al di fuori del luogo di lavoro, con eventuale acquisizione degli stessi da parte di terzi non autorizzati ove non siano state adottate misure adeguate come la cifratura delle memorie di massa, il che comporta una violazione di dati personali (*data breach*)[8]. La sicurezza, in definitiva e come si è già osservato, dipende non solo da fattori tecnici, ma anche umani e di cultura organizzativa, poiché si fonda sulla sedimentazione di prassi corrette, sulla responsabilizzazione diffusa,

[7] Ossia «l'uso del proprio ascendente e delle capacità di persuasione per ingannare gli altri, convincendoli che l'ingegnere sociale sia quello che non è oppure manovrandoli. Di conseguenza l'ingegnere sociale può usare la gente per strapparle informazioni con o senza l'ausilio di strumenti tecnologici» (K.D. Mitnick, *L'arte dell'inganno. I consigli dell'hacker più famoso del mondo*, tr. it., Feltrinelli, Milano, 2003, p. 10).

[8] Ossia «la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati» (art. 4(12) GDPR).

sulla verifica periodica mediante esercitazioni e su una consapevolezza dei rischi che travalica il perimetro fisico dell'ente o del soggetto riferimento.

Con riferimento alla seconda, è ben noto che ciascun sistema informatico possa contenere delle falle di sicurezza che consentono a utenti malintenzionati un accesso abusivo svolto a qualsiasi fine (come il danneggiamento, l'acquisizione illecita di dati, una semplice bravata)[9] e tale eventualità può realizzarsi con maggiore probabilità sfruttando proprio l'interconnessione dei database nel ciberspazio, essendo esposti in Rete[10]. Oltre alla perdita di riservatezza, rilevano gli impatti sulla continuità operativa: interruzioni o degradazioni delle infrastrutture informative compromettono la tempestiva disponibilità dei dati e dei supporti decisionali, determinano dilazioni nei percorsi assistenziali e, nei contesti in cui il tempo è un fattore cruciale, possono incidere negativamente sugli esiti.

Le problematiche sin qui citate non hanno, com'è noto, arrestato lo sviluppo e la diffusione dei sistemi informativi sanitari; né potrebbe essere altrimenti. Resta però decisivo orientare tale sviluppo in modo che sicurezza, libertà e dignità della persona costituiscano vincoli di progetto e non meri corollari, agevolando il lavoro dei professionisti e sostenendo esiti di salute verificabili nel tempo. L'obiettivo non è l'automazione come fine in sé, bensì l'elevazione della qualità dell'azione clinica e organizzativa: i sistemi devono agire come infrastrutture abilitanti che semplificano i processi essenziali, riducono gli oneri impropri e restituiscono tempo clinico al giudizio professionale e alla relazione di cura.

In questa prospettiva, alle cornici regolative e organizzative vanno affiancate condizioni abilitanti sostanziali: standard aperti e profili di scambio realmente interoperabili, interfacce intellegibili e carico cognitivo contenuto, segnalazioni proporzionate e non intrusive, percorsi formativi che accompagnino l'intero ciclo di vita del sistema e si modulino sulle

[9] Cfr. Gruppo di lavoro Articolo 29, *Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche (CCE)*, 00323/07EN, WP 131, 15 febbraio 2007, p. 20 (pare opportuno osservare che pareri, linee guida e opinioni di autorità di controllo, comitati e altri soggetti devono oggi essere sempre interpretati alla luce del GDPR, ove antecedenti al medesimo). Su questi aspetti si veda, da ultimo, la sezione monografica "Vulnerabilità e nuove tecnologie" pubblicata su «Notizie di Politeia», 136, 2019, a cura di C. Faralli (con scritti di R. Brighi, M. Palmirani e M. Martoni, F. Di Tano, M. Martoni, A. Verza, S. Vida, M.L. Rizzo, M.C. Mazzotti, S. Pelotti, S. Zullo).

[10] National Research Council, *For the Record. Protecting Electronic Health Information*, National Academy Press, Washington, DC, 1997, p. 165.

diverse professionalità. Affidabilità, prontezza e continuità operativa sono dimensioni della qualità della cura non meno della correttezza dei contenuti informativi. Non si tratta di un quadro astratto: il banco di prova è la cartella clinica elettronica e, più in generale, il Fascicolo Sanitario Elettronico (FSE), dove i principi quali l'interoperabilità, l'usabilità e la continuità operativa non restano meri enunciati, ma trovano attuazione concreta.

Con l'espressione cartella clinica elettronica si designa, in termini generali, la documentazione sanitaria in forma digitale che rende prontamente disponibili i dati sullo stato di salute di una persona ai fini della cura e di attività strettamente connesse. Nel lessico corrente, la "cartella" centrata su una singola organizzazione offre una vista parziale; il "fascicolo" orientato alla rete della salute abilita la condivisione lungo percorsi che attraversano contesti ospedalieri, territoriali e domiciliari. Sempre più spesso, si affianca la dimensione personale: raccolte gestite dall'interessato che integrano referti e misurazioni prodotte nel quotidiano. Si aprono qui opportunità di continuità e partecipazione, ma anche nuovi oneri di alfabetizzazione e di validazione dei contenuti.

In linea generale, la cartella clinica rappresenta un insieme di documenti nei quali viene registrato un complesso eterogeneo di informazioni prevalentemente sanitarie, ma anche anagrafiche, sociali, ambientali e giuridiche relative a un paziente determinato. Essa è redatta al fine di dedurre diagnosi e terapia, di predisporre gli opportuni interventi medici nonché di usufruire del suo contenuto per indagini di natura scientifica, statistica o medico-legale[11].

Le CCE costituiscono una delle più importanti innovazioni che l'informatica può portare alla medicina, poiché grazie ad esse è possibile avere un quadro completo delle informazioni sanitarie relative ad una persona (una sorta di «sportello unico»[12]). In linea di principio un EHR

[11] V. Milana, *La cartella clinica*, in F. Buzzi, P. Danesino (a cura di), *Gli esercenti le professioni sanitarie nel recente riassetto formativo. Interazioni e responsabilità nell'attuale cornice normativa delle aziende sanitarie. Pavia, 26-27 settembre 2002*, Giuffrè, Milano, 2003, p. 215.

[12] Si realizza, infatti, una sorta di "sportello unico" di cui beneficiano aree quali l'accesso ai dati personali e alle informazioni sanitarie, l'accesso ai servizi per i pazienti e, più in generale, la comunicazione interattiva, con benefici per la continuità dei rapporti di cura, la fruibilità di raccolte di informazioni di supporto, la comunicazione educativa e le raccomandazioni sanitarie personalizzate (in tal senso C. Maioli, E. Sánchez Jordán, *Big Data e capacità informativa per l'autodeterminazione del paziente*, in C. Faralli, R. Bri-

(*Electronic Health Record*) dovrebbe infatti racchiudere tutti i dati inerenti a un individuo, acquisiti in qualsiasi momento della sua vita. Appare chiaro che, in tal modo, non solo non potranno aversi lacune derivanti dalla perdita di talune informazioni o, al contrario, loro duplicazioni, ma inoltre esse potrebbero essere utilizzate rapidamente anche in caso di emergenza. Questa funzione di integrazione informativa è effettiva solo se i dati sono accurati, aggiornati e leggibili nei punti in cui servono; in difetto, la ricchezza si trasforma in "rumore" informativo.

Appare inoltre basilare garantire l'affidabilità dell'identificazione dei pazienti: si pensi, infatti, alle conseguenze negative che potrebbero derivare da una errata identificazione, per cui ad un individuo potrebbe essere, in ipotesi, attribuito l'EHR di un altro[13]. Inoltre, è indispensabile che le tecnologie di riconoscimento di una persona siano assolutamente certe affinché sia impossibile la verificazione di furti di identità[14]. L'identificazione, tuttavia, è anche processo che comporta pratiche operative, controlli incrociati e coerenza dei dati attraverso i diversi contesti.

Purtroppo, però, sorgono anche numerosi problemi sia di carattere bioetico-giuridico che informatico, anche connesse a un cattivo uso delle nuove tecnologie[15]. Bisogna infatti considerare che un EHR può potenzialmente contenere una mole anche assai ingente di dati sensibili, per cui le questioni connesse alla sicurezza delle trasmissioni elettroniche appaiono assai delicate. Non meno rilevante è la qualità del dato: completezza, accuratezza e tempestività sono presupposti di decisioni affidabili tanto quanto la confidenzialità.

Inoltre, si deve sottolineare il problema della mancanza di standard comuni che consentano a tutte le periferiche e a tutti i dispositivi di dialogare proficuamente, anche se esso potrebbe essere risolto mediante l'a-

ghi, M. Martoni (a cura di), *Strumenti, diritti, regole e nuove relazioni di cura. Il Paziente europeo protagonista nell'eHealth*, Giappichelli, Torino, 2015, p. 162).

[13] In simili ipotesi potrebbero verificarsi addirittura lesioni mortali, come nel caso in cui un paziente sia allergico a determinati farmaci che gli potrebbero essere somministrati qualora ciò non sia riportato nell'EHR scambiato.

[14] Gruppo di lavoro Articolo 29, *Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche (CCE)*, cit., p. 14.

[15] Ad esempio, per la 'tentazione' di copiare e incollare dati relativi ad altri pazienti per risparmiare tempo (M.L. Balestra, *Electronic Health Records: Patient Care and Ethical and Legal Implications for Nurse Practitioners*, in «The Journal for Nurse Practitioners», 2, 2017, p. 108).

dozione di standard come l'HL7 ("Health Level 7"), sviluppato da un'organizzazione senza scopo di lucro[16]. La generalizzata accettazione di uno standard appare fondamentale per garantire una reale interoperabilità fra sistemi diversi e, dunque, garantire CCE realmente adatte alle esigenze di una società sempre più globalizzata. Negli ultimi anni si sono affermati profili di scambio più flessibili, orientati a risorse e interfacce applicative, che favoriscono l'integrazione selettiva dei dati clinici e il loro impiego nei servizi di supporto alle decisioni.

Si consideri, poi, che EHR correttamente implementati possono migliorare la riservatezza e la sicurezza dei dati relativi allo stato di salute, poiché è possibile adottare tecnologie e procedure per impedire accessi non autorizzati oppure scoraggiare potenziali abusi. In tal modo è possibile utilizzare tecnologie di autenticazione e controllo degli accessi, anche mediante sistemi misti (ad esempio, basati su *physical tokens* e dati biometrici[17]), al fine di garantire l'accesso solo a soggetti legittimati a farlo. Inoltre, grazie a file di *log* è possibile tenere traccia degli eventuali accessi alle informazioni in modo da individuare eventuali abusi e, inoltre, la trasmissione degli EHR può avvenire cifrando le informazioni allo scopo di garantire la segretezza e la sicurezza delle comunicazioni[18]. La trasparenza degli accessi – preferibilmente visibile anche all'interessato – rafforza la fiducia e funge da deterrente agli usi impropri.

Appare chiaro, dunque, che la garanzia della confidenzialità dei dati appaia un presupposto primario per la creazione di sistemi nei quali possano venire realmente utilizzate le CCE in tutto il loro potenziale: nell'ipotesi

[16] <Http://www.hl7.org>.

[17] La biometria è la scienza che studia l'autenticazione e l'identificazione degli esseri umani mediante l'analisi delle loro caratteristiche fisiche (impronte digitali, iride, ecc.) o comportamentali (firma, andatura, ecc.). I dispositivi biometrici consentono, dunque, di autenticare e/o identificare un individuo attraverso sue caratteristiche uniche, talora mediante l'analisi combinata di più tecnologie di autenticazione e/o di identificazione. La progressiva diffusione di tali dispositivi, dovuta anche a sempre più sentite esigenze di sicurezza, solleva notevoli problematiche etiche e giuridiche in tema di tutela della riservatezza individuale nonché della libertà e della dignità di un uomo il cui corpo viene ridotto a mero strumento di autenticazione o di identificazione e che diviene, così, un semplice ammasso di informazioni che possono essere trattate mediante gli strumenti informatici (cfr. Comitato Nazionale per la Bioetica, *L'identificazione del corpo umano: profili bioetici della biometria*, Roma, 2010).

[18] National Research Council, *For the Record. Protecting Electronic Health Information*, cit., pp. 161-162.

di sussistenza di diffusi dubbi circa la riservatezza delle informazioni idonee a rivelare lo stato di salute o la vita sessuale non potrebbe certo raggiungersi un consenso sufficiente a rendere effettiva questa nuova evoluzione delle strutture sanitarie di qualsiasi tipologia, per quanto il processo di informatizzazione sia oramai inarrestabile: basti pensare, in tal senso, alla già citata esperienza italiana del Fascicolo Sanitario Elettronico e, più in generale, alla progressiva digitalizzazione delle strutture sanitarie. La fiducia è cruciale: senza fiducia i sistemi esistono, ma non funzionano.

Pertanto, oggi vi è una mole enorme di EHR che costituisce una ingente base di dati che potrebbe essere utilizzata potenzialmente anche per finalità di ricerca[19] qualora si dovesse riuscire a trovare un equilibrio fra la tutela di un diritto fondamentale come quello alla privacy e le esigenze della ricerca scientifica, così da portare, in ultima analisi, a una maggiore protezione del diritto alla vita e alla salute; ciò, tuttavia, è estremamente difficoltoso[20]. L'uso secondario dei dati esige qualità dei dati e della documentazione, riduzione ragionevole del rischio di reidentificazione e finalità determinate, chiare e verificabili, così da contemperare equamente riservatezza e ricerca giungendo a proteggere, anche in prospettiva futura, la persona e le comunità mediante un progresso scientifico non ostracizzato bensì responsabilizzato.

Ai requisiti già delineati per i sistemi informativi sanitari, cui si rinvia, si aggiunge dunque un requisito raccomandato: la previsione di integrare e rendere automatica l'anonimizzazione dei dati contenuti nei sistemi nazionali di EHR per la sola finalità di ricerca scientifica, nell'ottica di una maggior protezione del diritto alla salute (intesa in senso conforme al considerando n. 26 GDPR, che, come già esposto, fa riferimento ai mezzi di cui il titolare o un terzo possa ragionevolmente avvalersi per identificare una persona fisica). L'automazione può essere utile, ma non sostituisce il giudizio: non esiste anonimizzazione "assoluta"; occorre una valutazione in concreto del rischio residuo e della proporzionalità, con presìdi

[19] Cfr., fra gli altri, C. Xiao, E. Choi, J. Sun, *Opportunities and challenges in developing deep learning models using electronic health records data: a systematic review*, in «Journal of the American Medical Informatics Association», 10, 2018, pp. 1419-1428.

[20] La letteratura scientifica evidenzia ancor oggi quanto sia complesso raggiungere un equilibrio fra la tutela della privacy e la gestione delle informazioni per finalità di ricerca in ambito clinico (M.R. Cowie *et al.*, *Electronic health records to facilitate clinical research*, in «Clinical Research in Cardiology», 106, 2017, p. 6).

organizzativi e tecnici adeguati al contesto e con verifiche indipendenti, affinché la correlazione non prenda il posto della spiegazione e l'ottimizzazione non oscuri la giustificazione.

III.3. Telemedicina, *mobile health (mHealth)* e dispositivi indossabili

La telemedicina può essere definita come «l'integrazione, monitoraggio e gestione dei pazienti, nonché l'educazione dei pazienti e del personale, usando sistemi che consentano un pronto accesso alla consulenza di esperti ed alle informazioni del paziente, indipendentemente da dove il paziente o le informazioni risiedano»[21].

Si distingue correntemente fra teleconsulto, televisita, telemonitoraggio, teleassistenza e teleriabilitazione; sono, dunque, modalità che riorganizzano tempi e luoghi della cura senza uno snaturamento dell'atto professionale. Se collocati e adoperati entro percorsi chiari, trasparenti nelle responsabilità e nei canali, tutti questi strumenti digitali sono idonei a non sopprimere, bensì a potenziare la relazione, in quanto viene resa praticabile in altra forma e potenzialmente più continuativa, venendo meno taluni ostacoli intrinseci alla materialità: basti pensare a tempistiche e spostamenti, che riconfigurano la temporalità e la spazialità.

Giovamenti possano aversi in merito all'esercizio delle attività cliniche, assistenziali e didattiche, grazie anche alle facilitate possibilità di connessione offerte dalla capillare diffusione di Internet e di dispositivi informatici, grazie a cui si possono trasmettere e condividere informazioni sanitarie di qualsiasi tipo ed a velocità sempre maggiori. Sul piano clinico, il passaggio dal contatto episodico all'osservazione continuativa nel tempo introduce parametri digitali acquisiti costantemente da sensori (ad es. variabilità della frequenza cardiaca, glicemia, profili sonno-veglia, ecc.), che richiedono validazione analitica e clinica e interpretazione nel caso concreto, evitando sovradiagnosi e automatismi di medicalizzazione.

[21] Questa definizione, del 1990, è del gruppo di lavoro creato dalla Commissione Europea su «Advanced Informatics in Medicine». Sulla telemedicina cfr., fra gli altri, C. Botrugno, *Telemedicina e trasformazione dei sistemi sanitari. Un'indagine di bioetica*, Aracne, Roma, 2018.

Grazie al progresso delle tecnologie, inoltre, sono oggi disponibili app e sensori anche integrati in dispositivi indossabili di uso comune, come si è già osservato, che possono diventare strumenti preziosi nell'ambito della telemedicina. Così, è possibile monitorare costantemente lo stato di salute di un paziente, svolgere esercizi di fisioterapia mediante applicazioni di realtà virtuale e aumentata, coadiuvare nel controllo del rispetto delle terapie farmacologiche, ecc. Inoltre, l'ingente mole di dati che vengono raccolti può essere elaborata mediante tecniche di *Big Data analytics* i cui risultati possono essere potenzialmente preziosissimi[22]; ma tali dati sono anche estremamene potenti e delicati in virtù della loro natura reticolare, continuamente aggiornata, dinamica e pervasiva (il che può portare a una evoluzione dal *nudge* al c.d. *hypernudge*)[23], oltre che operante su scala globale[24].

La loro utilità non è tuttavia scontata. Un parametro digitale diventa una risorsa per la salute digitale solo quando poggia su misurazioni affidabili, metriche leggibili e pertinenti, e su un controllo nel tempo; diversamente genera rumore, spinge verso sovradiagnosi e medicalizzazione, e impoverisce il giudizio clinico attraverso il pregiudizio di automazione. La questione è, insieme, tecnica, giuridica ed etica: ciò che non è spiegabile e tracciabile non è realmente contestabile, e ciò che non è validato nel contesto non può assurgere a standard di diligenza. Vi è di più. Questo profilo ha un impatto sull'umanizzazione della cura, dal momento che l'osservazione continuativa può restituire la singolarità della persona, ma la "conversione" dalla persona ai dati (come se fosse, metaforicamente, la conversione da un formato informatico all'altro: ma, nel caso di specie, si passa dall'umano al digitale), pur necessari, rischia di trasformarla in standardizzazione e distanza qualora questi strumenti e informazioni digitali siano privi di una supervisione umana effettiva (caso per caso).

Lo scenario, però, è ancor più complesso di quanto sembri, poiché a tali dispositivi e servizi resi in modo professionale se ne affiancano di altri

[22] Cfr. I. Glenn Cohen, H. Fernandez Lynch, E. Vayena, U. Gasser (eds.), *Big Data, Health Law, and Bioethics*, Cambridge University Press, Cambridge, 2018.

[23] Cfr. K. Yeung, *'Hypernudge': Big Data as a mode of regulation by design*, in «Information, Communication & Society», 20, 2017, pp. 118-136. Per alcuni riferimenti alla *nudge theory* v. infra, par. 5.

[24] Il che pone la questione dei confini e dei limiti del diritto: cfr., su tale tematica generale, G. Zanetti, *Confini e elimiti del diritto*, Editoriale Scientifica, Napoli, 2020.

nell'ambito della c.d. *Mobile Health* (*mHealth* o *m-health*)[25], che può definirsi come «l'insieme di tecnologie "mobili", ossia l'uso di comunicazione wireless (cellulari e smartphone, tablet, dispositivi digitali, con o senza sensori indossabili), applicate in ambito medico-sanitario o in ambiti correlati alla salute»[26] e, ovviamente, in costante evoluzione[27]. Essa non aggiunge semplicemente un canale, ma innesta componenti della vita quotidiana nei percorsi di prevenzione, diagnosi, cura e riabilitazione anche mediante i dispositivi di uso comune. Questo innesto è giuridicamente ed eticamente legittimo solo se le finalità sono determinate e giustificate, le basi giuridiche chiare, i limiti dell'osservazione proporzionati e temporalmente definiti, le responsabilità individuate lungo l'intero ciclo di vita, e la persona è messa nelle condizioni di comprendere e scegliere (informazione adeguata e consenso effettivamente informato e libero). Diversamente, l'integrazione dei dispositivi mobili nell'ambito della salute rischia di portare a pratiche di sorveglianza pubblica e privata (soprattutto in riferimento alla zona grigio di alcuni dispositivi e servizi di cui si dirà nel prosieguo) nonché di medicalizzazione, accrescendo la vulnerabilità anziché ridurla.

Esse possono comportare nuove opportunità per la salute, in quanto idonee a promuovere uno stile salutare di vita, facilitare e velocizzare la comunicazione medico/paziente, personalizzare i trattamenti, incrementare l'autonomia e la sicurezza del paziente che può essere controllato e localizzato a distanza, migliorare l'efficienza del sistema sanitario (attraverso la riduzione dei costi di assistenza e ospedalizzazione, la telemedicina, la comunicazione di informazioni), contribuire alla ricerca (acquisendo dati soprattutto per ricerche epidemiologiche, studi della correlazione tra determinate condizioni mediche e ambientali, ecc.), ampliare l'accesso alle cure raggiungendo utenti che altrimenti non avrebbero avuto assistenza medica, stimolare il trasferimento di ricerca, la produzione e l'innovazione, condividere casi clinici e richiedere secondi pareri in tempo reale[28].

[25] Per una panoramica internazionale cfr. K. Kodama, S. Sengoku (eds.), *Mobile Health (mHealth). Rethinking Innovation Management to Harmonize AI and Social Design*, Springer, Singapore, 2022.

[26] Comitato Nazionale per la Bioetica, *"Mobile-health" e applicazioni per la salute: aspetti bioetici*, Roma, 2015, p. 5.

[27] Cfr. J. Portz, S. Moore, S. Bull, *Evolutionary Trends in the Adoption, Adaptation, and Abandonment of Mobile Health Technologies: Viewpoint Based on 25 Years of Research*, in «Journal of Medical Internet Research», 26, 2024, doi:10.2196/62790.

[28] Ivi, p. 7.

Le stesse funzioni possono alimentare forme di vulnerabilità aumentata quando la vita quotidiana viene riscritta come sequenza "numerica", con conseguenti dipendenza dal dato e ipervigilanza sanitaria, estensione della sorveglianza informale negli ambienti familiari e processi di stigmatizzazione algoritmica che irrigidiscono le opzioni di cura e di vita. Di qui la potenziale compressione degli ambiti di autonomia individuale, con una relazione che rischia di poggiare eccessivamente su profili numerici e non dialogici, che sulle prime devono basarsi senza essere pretermessi. Per questo i servizi non devono essere disegnati assumendo gli effetti deteriori come inevitabili, ma per prevenirli: misurare solo ciò che è clinicamente necessario e per il tempo strettamente utile; rendere comprensibili e controllabili le inferenze; assicurare governo umano effettivo e facoltà di revoca; limitare la circolazione dei profili al caso d'uso pertinente. Solo in queste condizioni l'integrazione digitale sostiene la persona senza trasformarla in oggetto di monitoraggio e senza far degenerare l'umanizzazione in standardizzazione.

Tali nuovi strumenti devono, del resto, essere finalizzati a migliorare l'interazione fra i soggetti coinvolti affiancandosi, e non sostituendosi, alla relazionalità così come tradizionalmente intesa[29]. L'alleanza terapeutica resta, comunque, il necessario presupposto perché sposta il baricentro dal dispositivo alla relazione: chiarire scopi e rischi, insieme a canali e tempi di ricontatto, definisce *ex ante* pertinenza, proporzionalità e durata dell'osservazione, delimita responsabilità e condizioni di intervento, impedisce che la gestione clinica venga assorbita dall'apparato tecnico. Ricondurre ogni rilevazione digitale alla biografia clinica della persona evita decontestualizzazioni, riduce il rischio di equivalenze errate tra variazioni individuali e patologia, preserva il giudizio professionale da automatismi, con conseguenze in ambito giuridico e organizzativo: ciò che è spiegato e tracciato è valutabile e sindacabile; ciò che è necessario e proporzionato è legittimo; ciò che ha tempi e canali definiti assicura continuità di presa in carico senza scivolare in sorveglianza. In breve, il dato digitale integra la relazione soltanto quando è reso intelligibile, governabile e responsabile.

[29] Per una recente mappatura e discussione critica, che parte dalle questioni di privacy, governance e proprietà del dato cfr. I. Glenn Cohen, D.B. Kramer, J. Adler-Milstein, C. Shachar, *Digital Health Care outside of Traditional Clinical Settings. Ethical, legal and regulatory challenges and opportunities*, Cambridge University Press, Cambridge, 2024.

La telemedicina, poi, appare particolarmente utile qualora sia necessario monitorare le condizioni di salute di persone che si trovano in isolamento domiciliare, così da ridurre il carico di lavoro delle strutture sanitarie garantendo, al tempo stesso, il loro diritto alla salute dal momento che si potrebbe intervenire solo in caso di bisogno, evitando un inutile dispendio di risorse[30]. Oltre le contingenze emergenziali, essa concorre alla continuità dell'assistenziale territoriale e si è giunti, nel 2025, alla Piattaforma Nazionale di Telemedicina, sviluppata dall'Agenzia Nazionale per i Servizi Sanitari Regionali (AGENAS) in qualità di Agenzia Nazionale per la Sanità Digitale. L'infrastruttura nazionale è gestita centralmente proprio dall'AGENAS, mentre ogni Regione e Provincia autonoma implementa la propria infrastruttura regionale per erogare servizi di televisita, teleconsulto, teleassistenza e telemonitoraggio.

Il quadro qui appena tratteggiato mostra, dunque, una serie di benefici che la telemedicina può apportare, nonché, intuitivamente, una sua sempre maggiore diffusione di pari passo all'evoluzione tecnologica grazie ad app, professionali e non, nell'ambito della salute che vengono sviluppate e rese disponibili e che riescono a sfruttare le potenzialità dei dispositivi di comunicazione wireless che vengono adoperati. Tale sviluppo richiede una corretta qualificazione giuridica del software, che può in determinati casi, essere considerato dispositivo medico ai sensi del Reg. (UE) 2017/745[31]. Il considerando 19 del medesimo regolamento precisa

[30] «Le forme della prestazione sanitaria a distanza inducono specie nel medio-lungo periodo la riorganizzazione del sistema sanitario, concorrendo a ridefinirne la struttura nel senso di portare il centro di gravità dell'assistenza dall'ospedale al territorio. In questo senso, la telemedicina, concretizzazione ed espressione dell'amministrazione digitale nel campo sanitario, concorre a perseguire, in chiave di "sussidiarietà", l'obiettivo di lasciare il paziente «a casa» quando la prestazione sanitaria non debba essere in base al principio di adeguatezza essere attratta via via al livello superiore ovvero al presidio medico o all'ospedale» (A. Mazza Laboccetta, *Telemedicina: sfide, problemi, opportunità*, in «Federalismi.it», 22, 2023, p. 182).

[31] Il software è espressamente riportato nella definizione di cui all'art. 2(1) Reg. (UE) 2017/745: «"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 informa-

che «il software specificamente destinato dal fabbricante a essere impiegato per una o più delle destinazioni d'uso mediche indicate nella definizione di dispositivo medico si considera un dispositivo medico, mentre il software destinato a finalità generali, anche se utilizzato in un contesto sanitario, o il software per fini associati allo stile di vita e al benessere non è un dispositivo medico. La qualifica di software, sia come dispositivo sia come accessorio, è indipendente dall'ubicazione del software o dal tipo di interconnessione tra il software e un dispositivo».

Non tutte le app e i dispositivi che rilevano per l'ambito della salute, però, sono dispositivi medici: ciò comporta che non sono sottoposte a una disciplina tanto stringente e che sono dunque idonee a risultare più facilmente dannose.

La loro aumentata disponibilità, inoltre, può contribuire alla nascita di forme ossessive di salutismo individualistico e di medicalizzazione, facendo così emergere una nuova forma di vulnerabilità dell'era tecnologica. È la tendenza al "*Quantified self*" a registrare ogni azione (*self-tracking, self-monitoring*), quantificare e comparare i dati, per poi condividerli su internet. Il metodo scientifico quantitativo viene applicato alla vita quotidiana, per controllare se stessi e il mondo esterno (espressione del-

zioni 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». L'art. 17, rubricato "Sistemi elettronici programmabili – dispositivi contenenti sistemi elettronici programmabili e software che costituiscono dispositivi a sé stanti", dispone che «17.1. I dispositivi contenenti sistemi elettronici programmabili, compresi i software, o i software che costituiscono dispositivi a sé stanti, sono progettati in modo tale da garantire la riproducibilità, l'affidabilità e le prestazioni in linea con la destinazione d'uso per essi prevista. In caso di condizione di primo guasto sono previsti mezzi adeguati per eliminare o ridurre, per quanto possibile, i rischi che ne derivano o il peggioramento delle prestazioni. 17.2. Per i dispositivi contenenti un software o per i software che costituiscono dispositivi a sé stanti, il software è sviluppato e fabbricato conformemente allo stato dell'arte, tenendo conto dei principi del ciclo di vita dello sviluppo, della gestione del rischio, compresa la sicurezza delle informazioni, della verifica e della convalida. 17.3. I software di cui al presente punto destinati a essere usati in combinazione con piattaforme di calcolo mobili sono progettati e fabbricati tenendo conto delle peculiarità della piattaforma mobile (ad esempio dimensioni e grado di contrasto dello schermo) e di fattori esterni connessi al loro uso (variazioni ambientali relative al livello di luce o di rumore). 17.4. I fabbricanti indicano requisiti minimi in materia di hardware, caratteristiche delle reti informatiche e misure di sicurezza informatica, compresa la protezione contro l'accesso non autorizzato, necessari per far funzionare il software come previsto».

la volontà di auto-controllo sul proprio corpo e sulla propria psiche), rischiando di dimenticare la dimensione qualitativa della persona umana e, con una ossessiva concentrazione su di se, a ritenere irrilevante il mondo esterno, a ridurre la salute ad una dimensione numerica, nel contesto di una visione riduzionistica antropologica. «La quantificazione si inserisce nella ricerca di conformarsi ad uno standard 'normale' definito dagli sviluppatori sulla base di parametri statistici sociali: la standardizzazione porta alla creazione di 'norme di comportamento' che tendono ad imporsi (peraltro, spesso in modo arbitrario o meramente statistico), diminuendo la sfera personale di libertà»[32].

In primo luogo, dunque, si pone il problema della determinazione dei criteri per distinguere fra applicazioni *m-health* rientranti o meno fra i dispositivi medici, dal momento che – come evidenzia il Comitato Nazionale per la Bioetica – diversi soggetti tendono ad aggirare la normativa in materia presentando i propri prodotti e servizi come semplici modalità di controllo del benessere nonostante siano, in sostanza, dei veri e propri dispositivi medici, per cui è possibile riscontrare un'ambiguità nell'offerta di applicazioni sulla salute, che da un lato consentono ai produttori di tenersi a distanza dalle applicazioni medicali in senso stretto ma che dall'altro si pongono come vicine alla salute, distribuendo applicazioni sempre più connesse alla salute che non vengono però qualificate come mediche[33].

Poiché il funzionamento di questi strumenti implica il trattamento di grandi quantità di dati, destinati ad alimentare aggregazioni su larga scala, la questione non è confinata alle strutture sanitarie e ai professionisti operanti in questo ambito, giungendo invece all'ambito del consumo di massa. Così, smartphone, fitness band, smartwatch, app di benessere, assistenti vocali e piattaforme domestiche tracciano, memorizzano, inviano ed elaborano dati relativi a routine, movimenti, sonno, voce, parametri ambientali e psico-fisici (saturazione, battito cardiaco, ecc.): materiali che, anche quando nascono come dati non direttamente relativi alla salute e per finalità tradizionalmente "mediche", riconfigurano la linea

[32] L. Palazzani, *Dalla bio-etica alla tecno-etica: nuove sfide al diritto*, Giappichelli, Torino, 2017, p. 370.

[33] Comitato Nazionale per la Bioetica, *"Mobile-health" e applicazioni per la salute: aspetti bioetici*, p. 9. Utili spunti possono rinvenirsi nella Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR del Medical Device Coordination Group.

di confine non appena consentono di inferire stati o rischi di salute. È in questo passaggio che la circolazione informativa cessa di essere neutra: le stesse infrastrutture che promettono continuità di servizio e personalizzazione ampliano i poteri di collegamento e ri-contestualizzazione, spingendo verso usi ulteriori (commerciali, assicurativi, organizzativi) che incidono sulla persona e sul modo in cui la sua vita viene descritta e trattata, e, dunque, anche sulla sua autodeterminazione, che diviene eterdoterminazione in modo più o meno marcato.

Si è giustamente posto in evidenza, del resto, il rischio – soprattutto nel rapporto fra medico e paziente – che si faccia ricorso al digitale sostituendo anziché integrando il rapporto interpersonale reale. Così, il professionista potrebbe essere tentato di adoperare le nuove tecnologie per risparmiare tempo, diminuendo però la propria attenzione verso il paziente. A sua volta, quest'ultimo tende sempre più a rivolgersi alle risorse online senza consultare il medico, alimentando la tendenza all'autoreferenzialità medica (il c.d. *self-patient*) sia per la diagnosi (auto-diagnosi) sia per la terapia (auto-medicazione): il tutto mettendo a rischio la propria salute, in assenza di indicazioni, consulenze e controlli. In tutta evidenza, una medicina digitale è idonea a guardare al rapporto fra medico e paziente nella prospettiva di un contratto fra un consumatore, da un lato, e un prestatore di servizi, dall'altro. Per evitare o ridurre questo rischio sarebbe necessario che l'utilizzo delle nuove tecnologie avvenisse dopo che si sia stabilita l'alleanza terapeutica fra il medico e il paziente, con la costituzione di un *rapporto di fiducia*: in tal modo si potrebbero aumentare la collaborazione, la partecipazione e l'interazione con il medico[34].

In conclusione, telemedicina e *mobile health* comportano un ripensamento della spazialità, della materialità e della temporalità della salute. Si pongono, dunque, diverse questioni etiche e giuridiche che, come si è visto, sono idonee a incidere sull'autodeterminazione individuale e sul rapporto fra chi opera professionalmente nell'ambito sanitario e i pazienti, nonché fra i produttori e i fornitori di dispositivi e servizi che toccano l'ambito della salute e del benessere. Se rettamente orientata, in prospettiva antropocentrica e non tecnocentrica né profittocentrica, l'innovazione integra, e non sostituisce, la relazione; riduce, e non accresce, la vulne-

[34] L. Palazzani, *Tecnologie dell'informazione e intelligenza artificiale. Sfide etiche al diritto*, cit., pp. 11-12.

rabilità aumentata; e distribuisce i benefici senza generare nuove esclusioni. Solo così la tecnologia entra stabilmente, come risorsa rispettosa della dignità e dell'autodeterminazione della persona, nei percorsi di prevenzione, cura e riabilitazione, nella promozione del benessere e nell'organizzazione dei servizi di salute.

III.4. Robotica, potenziamento umano e tecnologie assistive

Come facilmente desumibile dalla sua denominazione, la robotica è un ambito disciplinare avente ad oggetto lo studio per lo sviluppo e la realizzazione di robot, che possono trovare applicazione in una molteplicità di settori, che spaziano da quello manifatturiero a quello medico[35]. Nell'ambito della salute digitale, la rilevanza dei sistemi robotici non è meramente strumentale: è organizzativa e relazionale, poiché la loro introduzione ridisegna la distribuzione di compiti e responsabilità, il governo dei dati e la qualità della relazione di cura, introducendo, di fatto, un ulteriore "soggetto" tecnico-organizzativo nel circuito decisionale e informativo.

Fra gli ambiti principali di ricerca, che appaiono di interesse per il presente volume, vi è ovviamente quello dell'evoluzione della loro IA, che si connette parzialmente a quanto si è già osservato nel capitolo precedente. Essa è, ovviamente, strettamente legata ai progressi effettuati in ordine alla loro tecnologia costruttiva, dal momento che lo svolgimento di compiti materiali che richiedono intelligenza presuppone, al contempo, che i robot medesimi abbiano un hardware che consenta di eseguire il software (basti pensare ai sensori con cui il robot percepisce l'ambiente e agli attuatori con cui opera). Nel dominio sanitario e, più in generale,

[35] Sugli aspetti informatico-giuridici della robotica cfr., fra gli altri, U. Pagallo, *The Laws of Robots. Crimes, Contracts, and Torts*, Springer, Dordrecht, 2013; sui suoi profili etici e sociali cfr. S. Salardi, *Robótica e inteligencia artificial: retos para el Derecho*, in «Derechos y libertades», 42, 2020, pp. 203-232; P. Lin, K. Abney, G.A. Bekey (eds.), *Robot Ethics. The Ethical and Social Implications of Robotics*, MIT Press, Cambridge-London, 2014. Più in particolare, sull'autonomia cfr. G. Sartor, A. Omicini, *The Autonomy of Technological Systems and Responsibilities for their Use*, in N. Bhuta, S. Beck, R. Geiss, C. Kress, H.Y. Liu (eds.), *Autonomous Weapons Systems: Law, Ethics, Policy*, Cambridge University Press, Cambridge, 2016, pp. 39-74; sulla responsabilità in chiave comparatistica cfr. G. Guerra, *La sicurezza degli artefatti robotici in prospettiva comparatistica. Dal cambiamento tecnologico all'adattamento giuridico*, Il Mulino, Bologna, 2018.

della salute digitale, l'integrazione tra componenti fisiche e logiche incide direttamente su sicurezza, qualificazione giuridica e tracciabilità delle decisioni clinicamente rilevanti, soprattutto quando moduli algoritmici sostengono o indirizzano atti diagnostici e terapeutici. Il quadro europeo (Reg. (UE) 2017/745 sui dispositivi medici, Reg. (UE) 2017/746 sui dispositivi medico-diagnostici in vitro, Reg. (UE) 2023/1230 sulle macchine. Reg. (UE) 2024/1689 sull'intelligenza artificiale, Reg. (UE) 2024/2847 sui requisiti orizzontali di cibersicurezza per prodotti con elementi digitali – *Cyber Resilience Act*), Reg. (UE) 2019/881 – *Cybersecurity Act*), Dir. (UE) 2022/2555 – NIS2), va letto unitariamente: non per moltiplicare adempimenti, ma per ridurre vulnerabilità sistemiche della cura (opacità delle inferenze, integrazioni difettose, aggiornamenti non sicuri) e assicurare controllo e responsabilità lungo l'intero ciclo di vita.

I progressi richiamati hanno già tradotto in soluzioni operative scenari un tempo affidati alla fantascienza, avvicinando utopie e distopie alla pratica; i processi di elaborazione concettuale, valutazione etica e regolazione procedono tuttavia più lentamente dell'evoluzione tecnico-scientifica[36], con effetti di disallineamento nella governance. Ne discendono questioni tecniche, etiche e giuridiche che si possono utilmente discutere nella prospettiva della vulnerabilità aumentata: corporea (rischi da malfunzionamento o uso improprio), informativa (trattamenti e inferenze su dati sanitari), relazionale (sostituzione o compressione dell'interazione clinica), organizzativa e scientifica (dipendenze tecnologiche, erosione delle competenze, pregiudizi di automazione).

Già la Risoluzione del Parlamento europeo del 16 febbraio 2017 sulle norme di diritto civile della robotica, seguita da quella del 12 febbraio 2019 su una politica industriale europea in materia di intelligenza artificiale e robotica, aveva colto la portata di questa trasformazione, sollecitando un bilanciamento tra innovazione e responsabilità.

Quei testi, però, sono anteriori alla piena applicazione del Reg. (UE) 2017/745 sui dispositivi medici e del Reg. (UE) 2017/746 sui dispositivi diagnostici in vitro, all'adozione del Reg. (UE) 2024/1689 sull'intelligenza artificiale, al riassetto della sicurezza dei prodotti (Reg. (UE) 2023/1230 sulle macchine e Regolamento (UE) 2023/988 sulla sicurez-

[36] European Group on Ethics in Science and New technologies, *Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems*, Brussels, 2018, p. 11.

za generale dei prodotti) e al rafforzamento della resilienza digitale (Reg. (UE) 2019/881 – sulla cibersicurezza, Dir. (UE) 2022/2555 – NIS2, Regolamento (UE) 2024/2847 - ciberresilienza). Ne risulta, ad oggi, non un quadro unico e compiuto, bensì un'architettura in costruzione: alcuni pilastri sono operativi, altri si applicano per gradi, altri ancora richiedono atti attuativi e implementazione nazionale. In questo contesto, formazione continua del personale, autonomia supervisionata dei sistemi e tracciabilità delle decisioni sono cruciali in regimi vincolanti che attraversano progettazione, gestione del rischio, sorveglianza post-implementazione e segnalazione di incidenti e vulnerabilità. È su questo terreno che la promessa di efficienza e sicurezza può essere tradotta in pratiche che riducano, e non amplifichino, le forme di vulnerabilità aumentata.

È interessante notare, inoltre, come si sia progressivamente posta una particolare attenzione circa la formazione del personale sanitario nell'utilizzo dei robot, in modo che, da un lato, chi si trova a operare con essi li padroneggi quali strumenti e che, dall'altro, rifugga dalla tentazione di affidarsi ai medesimi minando il rapporto personale che si instaura e che deve instaurarsi con ciascun paziente. La prevenzione del pregiudizio di automazione è componente essenziale dell'alleanza terapeutica: le automazioni della macchina non surrogano il ragionamento clinico, che rimane situato e motivato. Il riconoscimento dei robot quali dispositivi medici comporta obblighi di valutazione clinica e di sorveglianza post-commercializzazione, con responsabilità ripartite tra fabbricanti e operatori economici, strutture e professionisti.

Un quadro, dunque, che seppur qui appena tratteggiato, consente di intravedere, o quanto meno di ipotizzare, i possibili sviluppi futuri, quando probabilmente agli avanzamenti tecnologici si accompagnerà la predisposizione di normative sempre più specifiche per regolamentare compiutamente la robotica e le sue applicazioni. Più che "nuove" regole, emerge l'esigenza di integrazione coerente di quelle esistenti: dispositivi, sicurezza dei prodotti con elementi digitali, cibersicurezza in sanità, responsabilità professionale e organizzativa.

Non si deve limitare l'analisi ai robot destinati a sostituire o coadiuvare la persona, poiché vi sono ambiti di ricerca volti a riparare, sostenere o potenziare funzioni corporee e cognitive. In questo quadro si collocano le tecnologie assistive: esoscheletri, sistemi di mobilità, comunicazione aumentativa e alternativa, interfacce uomo-macchina e interfacce cervello-

computer con finalità terapeutiche o riabilitative. La valutazione non è soltanto tecnica: è anche giuridica ed etica e riguarda accessibilità e usabilità, l'impatto sull'autonomia personale, inclusione e non discriminazione.

Così, la bionica è la scienza che studia sistemi elettronici capaci di simulare il comportamento di organismi viventi o loro parti. In medicina, indica la sostituzione od il miglioramento di organi od altre parti del corpo umano effettuati mediante l'inserimento, nel corpo stesso, di componenti elettronici e/o meccanici. A differenza delle protesi, gli impianti bionici possono consentire non solo il recupero delle funzioni svolte da un determinato organo, ma addirittura l'acquisizione e l'utilizzo di funzioni ulteriori o di caratteristiche superiori. Sul piano giuridico ed etico assume rilevanza la distinzione tra interventi di ripristino funzionale e interventi potenziativi: i primi si giustificano entro la logica della cura; i secondi richiedono cautele rafforzate in termini di proporzionalità, sicurezza, equità di accesso e non discriminazione, per evitare derive perfezionistiche e nuove forme di esclusione, con oneri di giustificazione e controllo adeguati[37].

Nei prossimi anni, la disponibilità degli impianti bionici, presumibilmente assai costosi, porrà questione etiche e giuridiche relative non solo alle tradizionali normative sui dispositivi medici, ma anche, presumibilmente, in ordine all'accesso generalizzato a simili cure – senza discriminazioni – ove siano terapeutiche e finalizzate a ripristinare funzionalità proprie dell'essere umano. Il profilo distributivo non è ancillare: in una prospettiva di giustizia distributiva ed eguaglianza sostanziale, l'innova-

[37] Come si è evidenziato, «Si è soliti affermare che l'era digitale e postmoderna in cui ci troviamo immersi presenta un volto bifronte come quello del dio Giano. Indubbiamente, viviamo in un'epoca paradossale dal momento che, da una parte, il transumanesimo ci prospetta un futuro carico di speranze sulla base di uno sviluppo illimitato, in termini etici e giuridici, della biomedicina e dell'ingegneria genetica nel quale, secondo le sue previsioni, si potrà sradicare la quasi totalità delle malattie che affliggono l'umanità, e ritardare se non addirittura arrestare la sua senescenza; d'altra parte, questo approccio scientista difeso dal progetto transumanista attraverso l'utilizzo illimitato delle tecnologie NBIC, della robotica e dell'intelligenza artificiale, presuppone – come ha evidenziato il filosofo morale francese Luc Ferry – il passaggio da un paradigma medico tradizionale, quello del modello terapeutico, che presenta come finalità principale quella di "rimediare", curare le malattie e le patologie, a un modello "superiore", orientato al miglioramento e al "perfezionamento" dell'essere umano» (F.H. Llano Alonso, *Transumanesimo, vulnerabilità e dignità umana: il giurista di fronte alle sfide della rivoluzione tecnologica 4.0*, in «Ordines», 2, 2021, p. 108).

zione sanitaria esige un onere di giustificazione pubblica delle scelte allocative. Ne seguono regimi di rimborso trasparenti, criteri di priorità espliciti e verificabili e impegno strutturale nella ricerca su popolazioni sottorappresentate, affinché l'evoluzione tecnologica ulteriore diseguaglianza, ma in effettivo ampliamento delle opportunità di cura.

Lo specifico ambito del "potenziamento umano" ("*human enhancement*" o "*enhancement*") è, invece, diverso ed è relativo alle «diverse possibilità, dischiuse dalla biomedicina contemporanea, di intervenire per via farmacochimica o elettro-meccanica sul corpo o sulla mente di individui sani allo scopo di aumentare e migliorare caratteristiche o funzioni psicofisiche esistenti, ovvero di implementarne di nuove, eventualmente anche trasmissibili ai discendenti»[38]. La discussione incrocia dignità, identità personale, eguaglianza e responsabilità: la regolazione non può fermarsi a dichiarazioni di principio, ma deve misurarsi con i casi d'uso, assicurare controlli indipendenti e fissare limiti sostanziali all'eterodirezione del corpo. In questa prospettiva, è necessario guardare all'impiego concreto: i sistemi che incidono sulla persona devono rendere ragione delle inferenze in modo comprensibile e controllabile; l'intervento tecnico è legittimo se necessario e proporzionato, accompagnato da supervisione umana effettiva, tracciabilità delle decisioni e reali strumenti di tutela. La promozione dell'innovazione non può tradursi in esclusioni di fatto: occorrono condizioni eque di accesso e informazione adeguata, mentre restano precluse forme di direzione del corpo estranee alla cura. Solo così l'innovazione si salda con la tutela dell'autonomia relazionale e non accresce la vulnerabilità (anche di persone e comunità escluse dal "potenziamento").

Inoltre, fermo restando il presupposto del ripudio della guerra, si porrà il problema dell'applicazione delle predette tecnologie in ambito bellico, che potrebbe portare a interventi (irreversibili o meno) di *enhancement* sui militari, con potenziale progettazione e manipolazione di esseri umani come armi vere e proprie anche mediante protesi e supporti informatici: sarà necessario rispettare i principi di dignità, integrità, non

[38] F.G. Pizzetti, *Potenziamento umano e principio lavorista. Spunti di riflessione*, in «Rivista di filosofia del diritto», 2, 2018, p. 261.

maleficenza, autonomia e uguaglianza[39], anche considerando che queste tecnologie potrebbero stravolgere la stessa natura umana[40].

Le questioni connesse alla robotica e al potenziamento umano sono ampie e delicate. Bisogna necessariamente adottare una prospettiva antropocentrica per tutelare la vita, la salute, l'integrità e la libertà personale anche quale autodeterminazione, con l'obiettivo, pratico prima che teorico, di governare il rischio senza accrescere le vulnerabilità, e ciò vale nella clinica, nella prevenzione e nella riabilitazione, nell'organizzazione dei servizi, nella ricerca e nei mercati della salute digitale. Ragionare in senso contrario equivarrebbe a rendere la tecnica gerarchicamente sovraordinata all'umano. In questa prospettiva, il criterio non è l'adesione ai requisiti della tecnica in quanto tali, ma la capacità delle soluzioni di rendere possibile l'autonomia della persona, di giustificare e rendere controllabili le inferenze, di assicurare supervisione umana effettiva, tracciabilità e reali possibilità di contestazione e tutela giuridica (anche amministrativa), e di distribuire i benefici nel rispetto del principio di eguaglianza sostanziale. Solo così l'innovazione può essere un fattore di promozione e di protezione della salute digitale senza degenerare in retoriche salvifiche e senza portare a nuove diseguaglianze – anzi, contribuendo a ridurre i divari già in essere.

III.5. Medicina personalizzata e medicina di precisione

La medicina personalizzata o di precisione è una evoluzione della medicina moderna che sovverte un paradigma classico: all'approccio basato sull'applicazione sostanzialmente uniforme sulla popolazione (all'esito di trials clinici) se ne sostituisce uno in cui ci si prefigge di individuare il nesso tra le caratteristiche biologiche dei pazienti, le diagnosi

[39] Cfr. Comitato Nazionale per la Bioetica, *Diritti umani, etica medica e tecnologie di potenziamento (enhancement) in ambito militare*, Roma, 2013, *passim*.

[40] In argomento cfr. altresì S. Amato, *Neuroscienze e utilizzazione militare delle tecniche di potenziamento umano*, in «Etica & politica», 2, 2014, pp. 182-198; S. Fuselli, *Diritto, neuroscienze, filosofia*, FrancoAngeli, Milano, 2014; S. Fuselli, Metaverso e neurotecnologie: una ricognizione, in «Journal of Ethics and Legal Technologies», 5, 2, 2023, pp. 6-28; L. Palazzani, *Il potenziamento umano. Tecnoscienza, etica e diritto*, Giappichelli, Torino, 2015; S. Salardi, *When the 'Age of Science and Technology' meets the 'Age of Rights'. 'Moral' Bioenhancement as a Case Study*, in A. D'Aloia, M.C. Errigo (eds.), *Neuroscience and Law: Complicated Crossings and New Perspectives*, Springer, Cham, 2020, pp. 239-255.

e le opzioni terapeutiche; essa, dunque, si propone pertanto di "cucire" trattamenti terapeutici su misura per ciascun paziente[41], con un approccio "sartoriale". Si verifica, così, una integrazione dell'*evidence-based medicine* con livelli di stratificazione molecolare, clinica e digitale, spostando il baricentro dalla "media" statistica al "profilo" individuale e alla sua tracciabilità lungo i percorsi di cura.

Le tecnologie e le tecniche coinvolte sono eterogenee (ad esempio: genomica, nanotecnologie, neurotecnologie e analisi dei big data). Rilevano inoltre i biomarcatori digitali ricavati da misure comportamentali, fisiologiche e ambientali, spesso ottenute in modo attivo o passivo tramite smartphone, dispositivi indossabili e sensori ambientali; nonché le cosiddette "-omiche" (trascrittomica, proteomica, metabolomica, microbiomica ed epigenomica). Assumono rilievo anche i *Real world data* e la conseguente generazione di *Real world evidence*, così come l'impiego di tecniche di apprendimento automatico, deep learning incluso, per compiti di classificazione, predizione di esiti, stratificazione del rischio e *clustering*.

Una definizione molto ampia, dunque, nel cui ambito si può distinguere fra *Explicit Personalized Medicine* (EPM) e *Implicit Personalized Medicine* (IPM).

La prima identifica e spiega in modo relativamente semplice ed esplicito relazioni biologiche tra le caratteristiche misurabili di un singolo paziente e i probabili esiti medici, così da rendere comprensibile il perché un determinato trattamento sia personalizzato in modo specifico per quella persona. La seconda (detta anche *black box medicine*) si ha quando l'individuazione delle suddette relazioni e l'elaborazione di un approccio terapeutico richiedono il ricorso ad un complesso di dati molto ampio (i Big Data assumono dunque notevole importanza), che consente numerose predizioni senza però che venga spiegato esplicitamente come si sia pervenuti a tali connessioni (e quest'ultime non sono in gene-

[41] PCAST (President's Council of Advisors on Science and Technology), *Priorities for Personalized Medicine. Report of the President's Council of Advisors on Science and Technology*, Washington D.C., 2008, p. 1. A livello europeo manca, ad oggi, una definizione ufficiale di medicina di precisione/personalizzata. Si potrebbe tuttavia adottare la definizione proposta nella Staff Working Document della Commissione Europea secondo cui questa consisterebbe in un modello che usa la profilazione molecolare per 'cucire' la strategia terapeutica corretta per una data persona nel momento corretto, e/o per determinare la predisposizione a patologie, e/o per rilasciare una prevenzione tempestiva e mirata (EC Commission SWD (2013) 436 final, p. 5).

re confermabili attraverso trials clinici)[42]. Nella pratica, gli approcci predittivi basati su apprendimento statistico e automatico si fondano su correlazioni ad alta dimensionalità con gradi variabili di intelligibilità; le tecniche di spiegabilità offrono ragioni operative, ma non equivalgono a una spiegazione causale-meccanicistica tipica della medicina "tradizionale" e richiedono validazione esterna e prospettica, verifica della generalizzabilità e della calibrazione, nonché monitoraggio continuo post-implementazione (deriva dei dati e dei modelli, bias, impatti clinici).

Se, da un lato, il rovesciamento dell'approccio terapeutico comporta benefici in ordine alla possibile massimizzazione degli effetti terapeutici prescrivendo la dose esatta di farmaci che servono in un caso specifico (riducendo così i rischi conseguenti all'iper-dosaggio), emergono numerose criticità etico-giuridiche fra cui assumono un rilievo centrale la protezione dei dati personali (e la dicotomia fra trasparenza e segretezza), il determinismo genetico, la qualità delle evidenze prodotte in contesti non sperimentali, la frammentazione del rapporto fra soggetto e paziente, le nuove forme di disuguaglianza e discriminazione nell'accesso alle cure[43]. È opportuno soffermarsi brevemente su ciascuna di esse.

Più specificatamente, lo sviluppo della medicina di precisione richiede, necessariamente, di acquisire un elevato numero di dati personali al fine di tracciare un profilo il più possibile "specifico" e dunque elaborare modelli terapeutici e/o di prevenzione tagliati su misura per ciascuna persona., che nel caso della IPM va a correlarsi con le elaborazioni svolte sui Big Data. Ne derivano tensioni strutturali con i principi di minimizzazione, limitazione della finalità e proporzionalità del trattamento; strumenti come il consenso dinamico, le valutazioni di impatto e la data governance interistituzionale diventano condizioni di legittimità e affidabilità. Ovviamente ciò comporta il necessario ricorso alle già menzionate "scatole nere", ponendo in primissimo piano la problematicità della dicotomia fra trasparenza e segretezza.

La prima consiste nella trasparenza delle persone e dei loro profili digitali, costruiti grazie alla raccolta di una grande varietà di loro dati

[42] N. Price, *Black-Box Medicine*, in «Harvard Journal of Law & Technology», 2, 2015, pp. 427-430.

[43] Sul punto cfr. altresì l'opinion n. 29, del 13 ottobre 2015, dello European Group on Ethics in Science and New Technologies (*The ethical implications of new health technologies and citizen participation*).

personali e frammentati nei server che elaborano i *Big Data*[44], per cui il controllo su di essi passa, sostanzialmente e contrariamente alla *ratio* della normativa vigente, ai titolari del trattamento. Questa asimmetria informativa produce una vulnerabilità cognitiva del paziente, che può essere mitigata solo con diritti effettivi di accesso, portabilità e contestazione, oltre che con registri di tracciabilità degli utilizzi.

La seconda è invece segretezza dei dati e, soprattutto, degli algoritmi e dei codici informatici che li eseguono, nonché della sorte delle informazioni medesime (che vengono decontestualizzate, ricontestualizzate ed elaborate all'infinito)[45]. La protezione del segreto commerciale non può tuttavia essere opposta agli obblighi di trasparenza e controllo propri della vigilanza clinica e regolatoria; l'operatore deve assicurare accessi controllati a soggetti competenti e terze parti indipendenti, mettere a disposizione documentazione tecnica idonea alla verifica e mantiene un sistema di tracciabilità delle decisioni clinicamente rilevanti.

In particolare, non è dato sapere quali e quante informazioni siano effettivamente acquisite ed elaborate, anche grazie alla protezione fornita proprio dagli ordinamenti giuridici: i codici informatici e gli algoritmi sono protetti dalla normativa in materia di diritto d'autore e proprietà intellettuale (o comunque quali segreti industriali)[46]. Proprio la segretezza può costituire lo schermo dietro cui celare eventuali violazioni di sicurezza che potrebbero non essere comunicate dai detentori delle predette informazioni ai relativi interessati (nonostante i relativi obblighi previsti, ad esempio, dal GDPR[47]), i quali magari non sarebbero in

[44] Sul punto cfr. altresì il cap. 2, par. 2.4.

[45] Del resto, come si è già esposto, viviamo in una società delle scatole nere (F. Pasquale, *The Black Box Society. The Secret Algorithms That Control Money and Information*, Harvard University Press, Cambridge-London, 2015), in cui i flussi informativi viaggiano sovente all'insaputa dei loro utilizzatori (e dei loro "interessati") e i sistemi intelligenti sono caratterizzati da una loro opacità intrinseca (G. Fioriglio, *Opacità dei sistemi intelligenti e sicurezza informatica: un difficile equilibrio fra regolazione e tecno-regolazione*, in «Rivista elettronica di Diritto, Economia, Management», 3, 2016).

[46] Oltretutto, gli interessati possono godere di una tutela molto debole in caso di errori, malfunzionamenti e trattamenti illeciti (R.A. Ford, N. Price, *Privacy and Accountability in Black-Box Medicine*, in «Michigan Telecommunications and Technology Law Review», 1, 2016, pp. 26-29).

[47] Ai sensi dell'art. 33, comma 1, GDPR, il titolare deve notificare la violazione dei dati personali all'autorità di controllo competente senza ingiustificato ritardo e comunque entro settantadue ore dal momento in cui ne è venuto a conoscenza, salvo che sia

grado di apprezzarne la gravità, essendo comunque ignari della quantità di dati in possesso dei primi[48]. Si pone, inoltre, il problema dell'ulteriore trattamento dei dati per finalità diverse da quelle originarie, talora mediante inferenze inattese, che impone, tra l'altro, l'effettiva osservanza del principio di limitazione delle finalità e controlli stringenti sui trasferimenti verso paesi terzi.

Proprio la particolarità, la qualità e la quantità delle informazioni, oltretutto, risultano in costante crescita, come risulta chiaramente tratteggiando in modo unitario un quadro che comprenda, al contempo, la genetica, la genomica e l'informatica. In tal senso, all'incremento delle conoscenze genetiche si accompagnano la diffusione di test genetici economici e di facile esecuzione nonché elaborazioni informatiche sempre più sofisticate. La disponibilità del sequenziamento su larga scala e dei test diretti al consumatore accresce il quantitativo di dati che si pongono al confine tra dato relativo alla salute e non, rendendo centrale la corretta qualificazione sia dei dati sia del trattamento (anche ai fini dell'art. 9 GDPR, essendo dati appartenenti a categorie particolari, e della esatta determinazione delle finalità) e la qualità e comprensibilità dell'informativa resa agli interessati (di cui agli artt. 13 e 14 GDPR).

Si aprono, così, nuove possibilità diagnostiche con il rischio di rivitalizzare la tendenza, che sarebbe di per sé superata, al determinismo genetico[49], sulla base della errata convinzione per cui la conoscenza genetica possa consentire di raggiungere una conoscenza piena e profonda della persona, come avviene per talune ricerche il cui scopo è individuare quei processi fisiologici da cui potrebbero scaturire la depressione, la bulimia, l'anoressia, ecc.; eppure, come sovente si afferma in ambito bioetico e filosofico, la persona non può essere ridotta alla mera somma dei geni (così come, in relazione al dataismo, non può essere ridotta alla somma dei dati: diverse prospettive riduzionistiche, dunque) e ciò che è anche il frutto di complesse interrelazioni con gli altri e con l'ambiente che la circondano.

improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

[48] In sostanza, a Davide (l'interessato) si contrappongono tanti Golia (titolari), che controllano le scatole nere. Ma come può ciascun Davide resistere all'assalto di tanti Golia? Restano così del tutto aperti, e all'apparenza irrisolti, i nodi problematici nel caso di utilizzo di tali scatole nere nell'ambito della medicina di precisione.

[49] Cfr., fra gli altri, S. Salardi, *Test genetici tra determinismo e libertà*, Giappichelli, Torino, 2010.

Sul piano teorico-giuridico, ciò richiama un'antropologia relazionale della cura e impone cautele contro forme di essenzialismo biologico (e di determinismo genetico) nelle decisioni cliniche e amministrative.

I rischi, però, sono ancora maggiori ove si considerino, in aggiunta, le potenziali conseguenze negative di trattamenti svolti in modo incontrollato su larga scala in un ambito tanto scivoloso, poiché potrebbero far emergere nuove forme di disuguaglianza e discriminazione sotto diversi profili. La composizione dei dati condiziona prestazioni ed effetti: campioni sbilanciati o con copertura incompleta generano errori sistematici e differenze di accuratezza e calibrazione tra sottogruppi, con rischio di discriminazione indiretta a danno dei gruppi sottorappresentati.

In relazione all'accesso alle cure bisogna infatti considerare che, dal momento che la medicina di precisione, e soprattutto la IPM, necessita di elaborare un notevole numero di dati al fine svolgere una personalizzazione accurata, le persone affette da patologie rare potrebbero essere discriminate, in violazione del principio di uguaglianza sostanziale. Difatti, gli studi potrebbero essere disincentivati a causa del basso numero di persone affette, in quanto gli strumenti terapeutici di precisione necessitano di un corposo quantitativo di dati e, comunque, vi sarebbero pochi 'consumatori' dei farmaci eventualmente prodotti (incidendo sul c.d. fenomeno dei farmaci orfani). La composizione dei dati impatta sulle prestazioni e sull'equità dei modelli, dal momento che squilibri di campionamento o coperture incomplete producono differenze di accuratezza e di calibrazione tra sottogruppi, con evidente rischio di discriminazione indiretta. Sul punto, non rileva unicamente la numerosità relativa, in quanto bisogna altresì tener conto della qualità e della coerenza delle misurazioni, della validità delle diagnosi e degli esiti di riferimento, dell'eterogeneità di protocolli e fonti, della rarità di taluni fenotipi e delle intersezioni tra caratteristiche. Ne discendono obblighi di diversa tipologia, ossia equità nell'arruolamento e nel campionamento, armonizzazione delle misurazioni, verifiche di accuratezza e calibrazione per sottogruppo, validazioni esterne e prospettiche, nonché monitoraggio post-implementazione con documentazione dei correttivi.

Inoltre, i portatori di patologie disabilitanti, anche se ad insorgenza futura, potrebbero essere discriminati in quanto potrebbero costituire un costo per la società e per eventuali datori di lavoro, nonostante gli ovvi effetti benefici sulla prevenzione delle malattie. Ulteriori criticità riguar-

dano l'assicurabilità e l'occupabilità, atteso che la profilazione predittiva può ledere la dignità e l'eguaglianza sostanziale. Di qui la necessità di stabilire divieti d'uso improprio e di svolgere controlli effettivi, *ex ante* ed *ex post*, sui modelli, sui dati e sulle decisioni.

Più in generale, il connubio fra i progressi della medicina e quelli dell'informatica può costituire, in una visione caratterizzata da una distopia di possibile realizzazione, una formidabile spinta verso modelli di società salutistiche e medicalizzate, in cui, come già evidenziato da Michel Foucault, si pone il rischio della diffusione di modi subdoli di "normalizzazione" da parte dello Stato che, attraverso l'incremento di forme di "medicalizzazione", finisce per esercitare un controllo pervasivo sul corpo delle persone, cercando di orientarle verso modelli ritenuti ideali in termini di benessere[50], il che può essere tuttavia ottenuto anche mediante il modello di paternalismo libertario della *Nudge theory*, con un approccio funzionale all'orientamento dei cittadini verso comportamenti e scelte ritenute desiderabili da parte dello Stato[51] (che, nelle intenzioni dei fautori di tale teoria, preserva comunque la libertà di scelta non ponendo limiti all'esercizio della libertà da parte degli individui: ma la «coniugazione arditamente proposta fra paternalismo ed approccio libertario» è un «autentico ossimoro, di difficile conciliazione»[52]). Una

[50] M. Foucault, *The Birth of Clinic. An Archaeology of Medical Perception*, Routledge, London, 1976, pp. 38-39.

[51] «Private and public choice architects are not merely trying to track or to implement people's anticipated choices. Rather, they are self-consciously attempting to move people in directions that will make their lives better. They nudge. A nudge, as we will use the term, is any aspect of the choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives» (R.H. Thaler, C.R. Sunstein, *Nudge: Improving Decisions about Health, Wealth, and Happiness*, Yale University Press, New Haven, 2008, p. 6. Per una discussione critica: M. Galletti, S. Vida, *Libertà vigilata: una critica del paternalismo libertario***,** IF Press, Roma, 2018).

[52] «È noto, infatti, come nel liberalismo si dia spazio al paternalismo, laddove sono riconosciute condizioni di diminuita capacità di deliberazione (tipicamente i minori e gli adulti, quando presentano limiti cognitivi dovuti a patologie sopraggiunte o esistenti sin dall'infanzia). Non altrettanto può essere postulato, tuttavia, in una prospettiva libertaria ove è riconosciuta primazia assoluta alla volontà deliberata dell'individuo, prescindendo da valutazioni inerenti alla presenza o meno di condizionamenti che possano pregiudicare il processo di formazione della volontà e, soprattutto, nella disposizione dei propri beni. Thaler e Sunstein risolvono in maniera abbastanza semplicistica questa apparente contraddizione fra "orientamento" delle scelte e approccio libertario, annotando come nella costruzione del framing delle scelte non sia omessa alcuna delle opzioni possibili, ma ne

governance inadeguata della medicina di precisione è idonea a trasformare la prevenzione in prescrizione sociale, imponendo oneri di conformità aggiuntivi a carico di ciascuna persona e ledendo potenzialmente il diritto all'autodeterminazione.

Il tutto si inserisce nell'ambito di una modificazione della stessa relazione fra medico e paziente, che passa dal modello contrattualistico (in cui vi è una base consensuale: medico e paziente condividono responsabilità) a una relazione in cui l'asse della responsabilità si sposta sul paziente, il quale diventa il primo responsabile del mantenimento della propria condizione di salute, dopo essere stato edotto circa le fragilità e i rischi di un corpo analizzato addirittura sino alla sua struttura genetica[53]. Bisogna però tener presente che una responsabilizzazione non correttamente governata trasferisce sul paziente oneri decisionali non proporzionati, generati da informazioni complesse e incerte e normalmente di difficile comprensione per i "non addetti ai lavori"; occorre un'alleanza terapeutica che assicuri una ripartizione proporzionata di oneri informativi e responsabilità decisionali.

Un quadro, dunque, da cui risulta evidente come, ancora una volta, le tecnologie informatiche aumentino considerevolmente le possibilità di raccolta ed elaborazione dei dati sanitari, che possono essere poi blindati e celati agli sguardi altrui grazie all'utilizzo delle scatole nere. La risposta del diritto appare contrastante, alla luce della necessità di trovare un difficile equilibrio fra l'esigenza di proteggere la proprietà industriale e intellettuale nonché l'iniziativa economica privata con potenziali benefici anche in relazione al diritto alla vita e alla salute, da un lato, e quella di tutelare il diritto alla protezione dei dati personali e di promuovere l'eguaglianza sostanziale con conseguenze positive per il diritto alla dignità umana

viene alterato l'ordine di presentazione: una soluzione, appunto, che appare estremamente semplicistica che ha dato luogo ad una serie di osservazioni critiche, focalizzantesi sulla natura subdolamente manipolativa di tale tecnica. Tutto ciò senza considerare l'ulteriore profilo di problematicità, che trova origine nella sua applicazione ad individui adulti e non già minorenni e/o maggiorenni in condizioni di limitate capacità cognitive: quale grado di ammissibilità può essere riconosciuto a questo approccio, espressamente declinato come libertario?» (A. Di Giandomenico, *Nuove forme di promozionalità? La* Nudge Theory, in Id. (a cura di), *ETSI DEUS NON DARETUR…Scritti in memoria di Serenella Armellini*, Giappichelli, Torino, 2023, pp. 247-248).

[53] European Group on Ethics in Science and New technologies, *The ethical implications of new health technologies and citizen participation*, Brussels, 2015, pp. 34-35.

e all'autodeterminazione informativa, dall'altro. In tale precario equilibrio si colloca il *framework* normativo europeo relativo all'uso primario e secondario dei dati sanitari, più volte menzionato nel presente volume.

In una prospettiva etica è necessario raggiungere, però, un equilibrio, in quanto i potenziali benefici della medicina di precisione sono tali e tanti da renderne sicuramente necessario, più che opportuno, uno sviluppo – che deve però essere rispettoso dei principi e dei valori degli ordinamenti costituzionali alla luce delle criticità sopra evidenziate, per evitare nuove vulnerabilità o comunque non potenziare quelle già esistenti. Ridurre la vulnerabilità aumentata richiede, tuttavia, un governo dell'intero ciclo di vita (modelli documentati e verificabili, con tracciabilità; spiegazioni proporzionate e operativamente utili in ambito clinico); sorveglianza post-implementazione con possibilità effettive di contestazione e di tutela giuridica (con procedure parallele a quelle giudiziarie); valutazioni documentate di accuratezza e calibrazione per sottogruppo e del profilo di equità degli esiti; informazioni comprensibili e completa per garantire che il consenso sia effettivamente informato e libero). È opportuno prevedere un divieto dell'impiego clinico di sistemi predittivi opachi: un principio di "spiegabilità per impostazione predefinita" che, quale pretesa fondamentale di una società dell'informazione rispettosa della dignità umana, esiga ragioni intellegibili e controllabili delle inferenze ed eviti nuovi *arcana imperii*.

In conclusione, la medicina di precisione è sostenibile quando resta ancorata a criteri di validità, affidabilità e riproducibilità, giustifica le inferenze, assicura equa ripartizione di rischi e benefici e preserva l'autonomia relazionale della persona nella cura.

IV. Sperimentazioni cliniche e ritorno dei dati ai partecipanti: riflessioni a partire dal progetto FACILITATE

IV.1. Introduzione: il progetto FACILITATE

FACILITATE (Framework for Clinical Trial Participants' Data Reutilization for a Fully Transparent and Ethical Ecosystem) è un progetto quadriennale promosso nell'ambito dell'Innovative Medicines Initiative (IMI) (nell'ambito del programma Horizon 2020 e con il supporto della European Federation of Pharmaceutical Industries and Associations – EFPIA)[1].

Il suo obiettivo è la ricerca di un equilibrio fra i vari diritti e interessi in gioco nell'ambito delle sperimentazioni cliniche[2]. Già in linea generale può ritenersi che la condivisione dei dati della ricerca clinica risponda a ragioni scientifiche, economiche ed etiche: consente il confronto e la combinazione di risultati, facilita le metanalisi, rende riesaminabili le conclusioni e apre alla verifica di nuove ipotesi, accrescendo la validità complessiva delle evidenze. Sul piano economico, valorizza l'investimento originario ed evita duplicazioni, ragione del sostegno di istituzioni pubbliche e grandi finanziatori. Eticamente, onora la generosità dei partecipanti e corrobora l'idea che, se l'accesso alla salute è un dirit-

[1] Sito web FACILITATE Project: <https://facilitate-project.eu>. Il consorzio riunisce ventinove soggetti tra associazioni di pazienti, strutture ospedaliere, università, esperti/e di sperimentazione clinica e membri dell'EFPIA; il coordinamento è affidato all'Università di Modena e Reggio Emilia (Prof. Luca Pani e Prof.ssa Johanna Maria Catharina Blom) e a Sanofi, in una logica di collaborazione pubblico-privato che valorizza competenze eterogenee e complementari.

[2] Si è giustamente rilevato che, più in generale, i risultati di tali sperimentazioni possano essere considerati un "bene pubblico", dal momento che se il finanziamento delle sperimentazioni cliniche sui nuovi farmaci fosse assunto come responsabilità pubblica a livello globale, ne deriverebbero benefici ulteriori: la condivisione dei dati secondo canoni di accesso aperto comprimerebbe i costi delle indagini ridondanti nel sistema sanitario globale; e, invece di accrescere i prezzi nei Paesi in via di sviluppo tramite un preteso diritto di proprietà intellettuale sui dati di prova, un meccanismo di finanziamento internazionale fondato su contributi equi ai costi complessivi abbasserebbe i costi di offerta, rendendo più accessibili, ovunque, sia i medicinali brevettati sia quelli non brevettati (J.H. Reichman, *Rethinking the Role of Clinical Trial Data in International Intellectual Property Law: the Case for a Public Goods Approach*, in «Marquette Intellectual Property Law Review», 13, 1, 2009, p. 68).

to fondamentale, anche l'accesso a dati idonei a migliorarla meriti tutela e promozione[3].

FACILITATE, in particolare, ha l'obiettivo di dare centralità proprio alla persona che partecipa alla sperimentazione (non necessariamente una persona malata), perseguendo la costruzione di un processo realmente innovativo di condivisione e riutilizzo dei dati sanitari, incardinato in un quadro etico approvato e pienamente conforme alle normative europee e nazionali vigenti.

L'impostazione di FACILITATE comporta la co-progettazione dell'ecosistema della sperimentazione clinica insieme ai loro rappresentanti e a partire dai loro punti di vista, raccolti lungo l'intero sviluppo del processo, in una prospettiva di cambiamento culturale dal paradigma paternalistico del «sappiamo noi che cosa è meglio per i pazienti"» al principio del «costruiamo insieme il sistema»[4].

In altri termini, FACILITATE intende delineare un'architettura di governance del dato che, fin dalla progettazione, integri criteri di liceità, correttezza e trasparenza, secondo un'impostazione coerente con i principi del diritto dell'Unione e con le discipline interne.

Il progetto mira a consentire ai partecipanti agli studi clinici di accedere ai propri dati sanitari personali, dove possibile, raccolti nel corso delle sperimentazioni e di farne uso, così da agevolare l'effettuazione di decisioni rilevanti in modo condiviso con i professionisti sanitari coinvolti nella loro cura, nonché di istituire un processo che permetta il riutilizzo di tali dati anche in future attività di ricerca.

Del resto, a livello più ampio e generale, il paziente diviene progressivamente sempre più centrale anche nella prassi clinica e nella riflessione bioetica, in cui – nella direzione dell'assistenza sanitaria giustificabile – si richiede che «il ragionamento pratico sottostante al *decision-making* nel rapporto medico-paziente sia reso trasparente a tutte le parti interessate e la decisione sia basata su un approccio sistematico e olistico. Così si

[3] C. Ohmann *et al.*, *Sharing and reuse of individual participant data from clinical trials: principles and recommendations*, in «BMJ Open», 2017, 7:e018647 (doi:10.1136/bmjopen-2017-018647), p. 2.

[4] C. Staunton, J.M.C. Blom, D. Mascalzoni, on behalf of the IMI FACILITATE Consortium. *Ethical framework for FACILITATE: a foundation for the return of clinical trial data to participants*, in *Frontiers in Medicine,* 11, 2024, <https://www.frontiersin.org/journals/medicine/articles/10.3389/fmed.2024.1408600/full> p. 2.

è passati da un criterio di tipo vitalistico/paternalistico, dove il "meglio" veniva definito sulla base di aspetti puramente biologici della cura e dove la decisione, perlopiù in carico al professionista sanitario, era poco incline a considerare i bisogni psico-sociali e i valori del paziente ad un approccio il più possibile condiviso con quest'ultimo, dove la comunicazione con il medico e il rispetto dell'autonomia del paziente vengono a collocarsi al centro della relazione di cura»[5].

L'idea alla base di FACILITATE è, dunque, che i dati degli studi clinici relativi ai pazienti possano essere resi disponibili per confronti incrociati con altri archivi: oggi, infatti, i dati clinici sono frammentati e conservati in archivi separati, non potendo essere normalmente utilizzati al di fuori specifiche sperimentazioni. La maggiore trasparenza e apertura, inoltre, può ridurre la portata di determinate vulnerabilità[6].

La ricerca è pertanto finalizzata a raggiungere un obiettivo assai ambizioso: garantire che l'intero processo – dalla raccolta dei dati fino alla loro distruzione o anonimizzazione, dalla condivisione al riutilizzo – sia conforme ai requisiti giuridici ed etici, da un lato, e sia allineato non solo agli interessi e alle volontà dei partecipanti allo studio, ma anche a quelli delle strutture sanitarie, del mondo accademico e dell'industria, dall'altro[7].

[5] S. Zullo, *L'impatto della medicina algoritmica sul* shared decision making, in «Notizie di Politeia», 143, 2021, p. 152.

[6] Si pensi alla vulnerabilità delle donne (e, analogamente, delle persone anziane e dei membri di minoranze etniche nelle rappresentazioni cliniche) che dipende non solo dalle condizioni in cui si trova in un determinato momento della vita, «ma anche dal fatto che il sistema della ricerca clinica e farmacologica tende strutturalmente ad una sorta di auto-rappresentazione delle donne per ragioni molteplici, alcune delle quali riconducibili a meccanismi sistemici di oppressione; tale contesto produce una maggiore esposizione a rischi – che vanno da una maggiore incidenza di reazioni avverse ai farmaci, a un rischio di *overmedication* legato a dosaggi non tarati sul corpo femminile, all'uso di modelli di consenso informato pensati per il c.d. individuo universale-neutro-maschile, ad altro ancora – che prescindono dalla vulnerabilità di ciascun soggetto, e che tuttavia producono una condizione di svantaggio per tutte le donne (nella duplice veste di pazienti e di partecipanti a sperimentazioni)» (F. Macioce, *La vulnerabilità di gruppo. Funzioni e limiti di un concetto controverso*, Giappichelli, Torino, 2021, p. 63).

[7] C. Staunton, J.M.C. Blom, D. Mascalzoni, on behalf of the IMI FACILITATE Consortium. *Ethical framework for FACILITATE: a foundation for the return of clinical trial data to participants*, op. cit., pp. 2-3.

IV.2. La restituzione o ritorno dei dati ai partecipanti nelle sperimentazioni cliniche

La comprensione sia dell'obiettivo sia dell'importanza degli esiti di FACILITATE richiede la previa trattazione di taluni concetti fondamentali, con particolare riferimento alla "restituzione" (o "ritorno") dei dati ai pazienti[8] e al relativo *framework* legislativo[9]. Per essa si intende l'insieme

[8] Di particolare interesse è la proposta dei seguenti principi per la condivisione dei dati delle sperimentazioni cliniche: (1) La messa a disposizione dei dati individuali dei partecipanti dovrebbe essere promossa, incentivata e adeguatamente sostenuta fino a divenire prassi ordinaria della ricerca clinica. I piani di condivisione vanno descritti in via prospettica ed entrare nello sviluppo dello studio sin dalle fasi iniziali. (2) La condivisione dei dati individuali dei partecipanti si fonda sul consenso esplicito e ampio dei soggetti arruolati (o, ove del caso, dei loro rappresentanti legali) alla condivisione e al riuso dei dati per fini scientifici. (3) I dati individuali resi disponibili per la condivisione devono essere predisposti allo scopo, con de-identificazione degli insiemi di dati per minimizzare il rischio di re-identificazione; le fasi di de-identificazione adottate devono essere documentate. (4) Per promuovere l'interoperabilità e preservare il significato ai fini dell'interpretazione e dell'analisi, i dati condivisi dovrebbero, per quanto possibile, essere strutturati, descritti e formattati secondo standard ampiamente riconosciuti per dati e metadati. (5) L'accesso ai dati individuali e ai documenti della sperimentazione deve essere il più aperto possibile e solo nella misura strettamente necessaria limitato, al fine di tutelare la riservatezza dei partecipanti e ridurre il rischio di uso improprio. (6) Nel contesto di accesso gestito, qualunque cittadino o gruppo che formuli una domanda scientificamente fondata e disponga della competenza per rispondervi dovrebbe poter richiedere l'accesso ai dati e ai documenti di studio. (7) Il trattamento delle richieste di accesso ai dati deve essere esplicito, riproducibile e trasparente e, per quanto possibile, ridurre l'onere burocratico per tutte le parti coinvolte. (8) Oltre agli insiemi di dati individuali, dovrebbero essere condivisi anche altri oggetti informativi della sperimentazione (ad es. protocolli, rapporti di studio clinico, piani di analisi statistica, moduli di consenso informato in bianco) per consentire una piena comprensione dei dati. (9) Dati e documenti resi disponibili alla condivisione dovrebbero essere trasferiti a un archivio dati idoneo, così da garantirne la corretta preparazione, la disponibilità di lungo periodo, la conservazione sicura e una governance rigorosa. (10) Qualsiasi insieme di dati o documento reso disponibile alla condivisione dovrebbe essere accompagnato da metadati di individuazione concisi, pubblicamente disponibili e strutturati in modo coerente, che descrivano non solo l'oggetto informativo ma anche le modalità di accesso, al fine di massimizzarne la reperibilità sia per le persone sia per i sistemi informatici (C. Ohmann et al., *Sharing and reuse of individual participant data from clinical trials: principles and recommendations*, op. cit., p. 5).

[9] Di particolare rilevanza è, a tal proposito, il *White paper* di FACILITATE di recente pubblicazione: C. Staunton et al., *The return of Individual Participant Data in clinical trial research: a FACILITATE White Paper*, FACILITATE Consortium, 2025.

dei flussi informativi in uscita dal progetto verso i partecipanti, su tre piani distinti: (i) la comunicazione di risultati individuali clinicamente validati e proporzionati (ivi inclusi eventuali reperti incidentali); (ii) la messa a disposizione di risultati aggregati in linguaggio accessibile (*lay summary*), oggetto di specifico obbligo di trasparenza nelle sperimentazioni cliniche tramite il Clinical Trials Information System (CTIS); (iii) l'abilitazione o il rafforzamento dell'accesso e della portabilità dei dati personali nei limiti della normativa vigente in materia di protezione dei dati.

Si consideri, tuttavia, che l'obbligo relativo alla sintesi per i non addetti ai lavori non coincide con la restituzione di dati o risultati individuali, né la implica automaticamente: si tratta di un obbligo di trasparenza pubblica che opera *erga omnes* e non assicura, di per sé, l'individualizzazione informativa necessaria alla presa di decisione del singolo partecipante.

Ben altro rilievo assume la restituzione di esiti individuali, che richiede autonoma giustificazione clinica ed etica, cautele proporzionate e un'organizzazione dedicata; è un'attività onerosa, ma potenzialmente decisiva per porre realmente il partecipante (o paziente, a seconda dei casi) al centro. Si devono restituire ai partecipanti e ai pazienti esclusivamente informazioni clinicamente validate, azionabili e intellegibili per quella persona, evitando tanto il "minimalismo informativo" quanto l'ipertrofia documentale. La proporzionalità opera come criterio di bilanciamento tra utilità clinica, onere cognitivo e rischio di fraintendimento: non tutto ciò che è tecnicamente ottenibile è, per ciò solo, giuridicamente o eticamente dovuto. Deve essere (i) "clinicamente validato" poiché i risultati devono essere corroborati da evidenze appropriate e da un percorso metodologico trasparente; (ii) "azionabile", perché la conoscenza deve essere idonea a orientare decisioni cliniche sensate per quella persona e in quel contesto (diagnosi, terapia, follow-up); (iii) "intellegibile", ossia resa comprensibile grazie all'utilizzo di un linguaggio chiaro, dall'esplicitazione dell'incertezza e, ove opportuno, da una stratificazione progressiva dell'informazione.

Pertanto, in linea di principio sono da intendersi esclusi dall'obbligo di "ritorno" i semplici segnali preliminari, i dati grezzi e le ipotesi non corroborate, per evitare di trasferire un onere improprio di interpretazione sul partecipante o paziente; vi rientrano, invece, i risultati aggregati in linguaggio accessibile e quelli individuali ove affidabili e proporzionati nelle potenziali conseguenze, inclusi eventuali reperti incidentali qualora

sussista una tempestività clinicamente rilevante. Ovviamente i dati devono essere "restituiti" con una tempistica ragionevole e con una mediazione professionale, e, in ogni caso, in modo coerente con il consenso prestato.

Ne consegue che, da un lato, può evitarsi il minimalismo che elide l'autodeterminazione e mina la fiducia; dall'altro, si evita quell'ipertrofia documentale che, per finalità difensive, cela la responsabilità all'interno di copiosa produzione documentale per perseguire invece una trasparenza sostanziale, verificabile *ex post* mediante verifiche di comprensione, tracciabilità decisionale e audit dell'azionabilità dichiarata. Infine, non devono essere possibili discriminazioni e deve essere garantita l'eguaglianza sostanziale: la restituzione deve essere accessibile anche a chi presenta bassa alfabetizzazione sanitaria o digitale, rispettare i principi di protezione dei dati (necessità, minimizzazione, sicurezza) e armonizzarsi con gli strumenti di accesso e portabilità previsti dall'ordinamento.

In altri termini, la restituzione di risultati individuali clinicamente validi e utili e di risultati aggregati comprensibili consente, tra l'altro, di ridurre l'asimmetria informativa che grava sui partecipanti, spesso in posizione di vulnerabilità. Ciò non deve ridursi a un ulteriore adempimento burocratico (ad es., mera consegna di copiosa documentazione), bensì tradursi in risultati effettivamente individualizzati, spiegati in modo compiuto a ciascun partecipante, cui guardare innanzitutto come persona e non come "partecipante" o "interessato". Pertanto, il dato diviene abilitante e consente a questi di potersi realmente autodeterminare.

Tali obiettivi e considerazioni si innestano sul quadro normativo delle sperimentazioni cliniche. Esse sono disciplinate primariamente dal Reg. (UE) n. 2014/536, che ha abrogato la direttiva 2001/20/CE. Il Regolamento si applica alle sperimentazioni cliniche di medicinali per uso umano condotte nell'Unione europea e non si applica agli studi non interventistici. Proprio talune definizioni di cui al Reg. (UE) n. 536/2014 consentono di esporre taluni concetti fondamentali, precisando sin d'ora che una sperimentazione clinica deve essere progettata per generare dati affidabili e robusti; inoltre, può essere condotta solo se vengono tutelati, con prevalenza su tutti gli altri interessi, i diritti, la sicurezza, la dignità e il benessere dei soggetti (art. 3 Reg. (UE) n. 536/2014).

Bisogna però distinguere fra studio clinico e sperimentazione clinica. Più specificatamente, per studio clinico deve intendersi «qualsiasi indagine effettuata in relazione a soggetti umani volta a: a) scoprire o

verificare gli effetti clinici, farmacologici o altri effetti farmacodinamici di uno o più medicinali; b) identificare eventuali reazioni avverse di uno o più medicinali; oppure c) studiare l'assorbimento, la distribuzione, il metabolismo e l'eliminazione di uno o più medicinali, al fine di accertare la sicurezza e/o l'efficacia di tali medicinali» (art. 2, par. 2(2)).

La sperimentazione clinica è invece «uno studio clinico che soddisfa una delle seguenti condizioni: a) l'assegnazione del soggetto a una determinata strategia terapeutica è decisa anticipatamente e non rientra nella normale pratica clinica dello Stato membro interessato; b) la decisione di prescrivere i medicinali sperimentali e la decisione di includere il soggetto nello studio clinico sono prese nello stesso momento; o c) sono applicate ai soggetti procedure diagnostiche o di monitoraggio aggiuntive rispetto alla normale pratica clinica» (art. 2, par. 2(2))[10], mentre gli studi diversi dalle sperimentazioni cliniche sono definiti "studi non interventistici".

Intuitivamente, l'effettuazione di una sperimentazione clinica implica il trattamento di dati relativi alla salute, ossia di dati appartenenti a categorie particolari ex art. 9 Reg. (UE) n. 2016/679, il cui trattamento è quindi vietato (art. 9, par. 1), a meno che non ricorrano le eccezioni di cui al par. 2. Ne consegue che, oltre al consenso informato[11], è dunque necessario acquisire il consenso al trattamento dei dati personali per ciò che consente l'uso primario dei medesimi.

Si pone, tuttavia, il problema dell'uso secondario, di cui già si è detto. Sul punto assume rilevanza l'art. 28, par. 2, Reg. (UE) n. 536/2014,

[10] Per completezza, si riporta altresì la definizione di «sperimentazione clinica a basso livello di intervento»: «una sperimentazione clinica che soddisfa tutte le seguenti condizioni: a) i medicinali sperimentali, ad esclusione dei placebo, sono autorizzati; b) in base al protocollo della sperimentazione clinica, i) i medicinali sperimentali sono utilizzati in conformità alle condizioni dell'autorizzazione all'immissione in commercio; o ii) l'impiego di medicinali sperimentali è basato su elementi di evidenza scientifica e supportato da pubblicazioni scientifiche sulla sicurezza e l'efficacia di tali medicinali sperimentali in uno qualsiasi degli Stati membri interessati; e c) le procedure diagnostiche o di monitoraggio aggiuntive pongono solo rischi o oneri aggiuntivi minimi per la sicurezza dei soggetti rispetto alla normale pratica clinica in qualsiasi Stato membro interessato» (art. 2, par., 2(3)).

[11] «L'espressione libera e volontaria di un soggetto della propria disponibilità a partecipare a una determinata sperimentazione clinica, dopo essere stato informato di tutti gli aspetti della sperimentazione clinica rilevanti per la decisione del soggetto di partecipare oppure, nel caso dei minori e dei soggetti incapaci, l'autorizzazione o l'accordo dei rispettivi rappresentanti legalmente designati a includerli nella sperimentazione clinica» (art. 2, par. 2(21) Reg. (UE) n. 536/2014).

ai sensi del quale, fatta salva la vigente normativa in materia di protezione dei dati personali, il promotore può, all'atto della raccolta del consenso informato alla partecipazione alla sperimentazione clinica, chiedere al soggetto (o al suo rappresentante legale) anche il consenso all'uso (secondario) dei dati per fini di ricerca scientifica al di fuori di quanto previsto nel protocollo. Ovviamente tale consenso è revocabile in qualsiasi momento.

Da quanto sin qui succintamente esposto può intuirsi come due diverse discipline vadano a intersecarsi: la normativa sulla protezione dei dati personali, da un lato, e quella sulle sperimentazioni cliniche, dall'altro. Per poter effettuare una sperimentazione clinica è infatti necessario effettuare trattamenti di dati comuni e, soprattutto, di dati relativi alla salute, con tutto ciò che ne consegue in ordine alle relative condizioni di liceità: com'è noto, il consenso – manifestato per iscritto – è la base giuridica di riferimento, dunque la regola in relazione a cui interpretare e applicare le eccezioni previste dal legislatore[12]. E proprio il consenso, pur essendo una base giuridica fondamentale per garantire il controllo degli interessati sui dati personali che li riguardano, può diventare un ostacolo all'effettuazione di trattamenti ulteriori, giungendo a compromettere, potenzialmente, gli obiettivi della ricerca medica di cui possono giovarsi individui e gruppi.

Si impone, pertanto, un processo di bilanciamento particolarmente delicato, nel quale convergono e talora confliggono interessi diversi, tutti meritevoli di tutela. Un equilibrio, per quanto intrinsecamente instabile, può nondimeno essere raggiunto solo a seguito di una considerazione complessiva di tali interessi, senza mai oltrepassare il presidio irrinunciabile rappresentato dalla dignità della persona.

La riflessione deve inoltre tenere conto che i dati trattati nell'ambito della sperimentazione possono conservare un rilievo significativo per i partecipanti anche dopo la conclusione del protocollo, soprattutto qualora emergano ulteriori informazioni pertinenti al loro stato di salute attuale o futuro.

[12] «È necessario che nelle procedure per l'acquisizione del consenso alla partecipazione ad una sperimentazione siano non soltanto fornite le informazioni rilevanti, ma vengano considerate anche le percezioni soggettive e le aspettative, e il ruolo delle istituzioni alle quali si fa riferimento e che promuovono la ricerca; soprattutto, è necessario che siano tenuti in considerazione i bisogni specifici (di tipo informativo, ma anche di tipo sociale e relazionale) che i gruppi vulnerabili manifestano, e che non si riducono ai molti, e variabili, interessi individuali» (F. Macioce, *La vulnerabilità di gruppo. Funzione e limiti di un concetto controverso*, Giappichelli, Torino, 2021, p. 150).

Per di più, tali dati potrebbero essere utilizzati per evitare l'esecuzione di ulteriori accertamenti e indagini cliniche, con conseguente riduzione dei costi e ottimizzazione dell'impiego delle risorse del servizio sanitario (o, in difetto di copertura, dei privati), e risultano idonei a sostenere decisioni sanitarie più consapevoli da parte dei partecipanti che possono così autodeterminarsi. I benefici per la salute sono evidenti: le informazioni in questione possono incidere sul percorso terapeutico individuale, consentendo ai partecipanti di autodeterminarsi in modo più pieno attraverso scelte realmente informate.

La restituzione, o ritorno, dei dati si confronta con una pluralità di criticità, prevalentemente di ordine giuridico, che si riflettono poi sul piano operativo. La letteratura segnala, infatti, che la comunicazione sistematica dei dati ai partecipanti è evenienza rara, e lo è ancor di più una volta conclusa la sperimentazione. Le cause sono eterogenee. Tra queste, l'incertezza circa l'individuazione del soggetto effettivamente responsabile della restituzione. Si consideri, inoltre, che le imprese farmaceutiche non possono contattare direttamente i partecipanti e che una restituzione dei dati su orizzonti temporali medio-lunghi comporta oneri gestionali e finanziari che gravano direttamente sulle strutture sanitarie. A ciò si aggiunge l'assenza di veri e propri standard condivisi sia per la restituzione sicura dei dati, sia per la pubblicazione dei risultati aggregati delle sperimentazioni. Resta, nondimeno, fermo quanto già osservato: la restituzione dei dati ai singoli partecipanti sarebbe, in linea di principio, particolarmente utile e significativa.

Per contro, la fisiologica tensione tra sperimentazioni cliniche e protezione dei dati personali non implica affatto che si debbano sacrificare l'efficacia e le potenzialità delle prime in nome della privacy, né, in senso inverso, che possa essere compresso un diritto ormai fondamentale quale la protezione dei dati personali. Occorre invece perseguire un punto di equilibrio, nella consapevolezza che esso sarà verosimilmente instabile e richiederà un periodico riesame e riassetto. Di ciò, in particolare, si è occupato il già menzionato Comitato Europeo sulla Protezione dei Dati con il suo parere 3/2019, secondo cui «tutti i trattamenti correlati a uno specifico protocollo di sperimentazione clinica durante l'intero ciclo di vita della sperimentazione, dal suo avvio alla cancellazione una volta scaduto il periodo di archiviazione, vadano intesi come uso primario dei dati della sperimentazione clinica», distinguendo fra i trattamenti corre-

lati a finalità di affidabilità e sicurezza e quelli correlati esclusivamente ad attività di ricerca[13].

La base giuridica dei primi è individuata nell'art. 9, par. 2, lett. i) («il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali […] la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale»)[14].

Il Comitato ritiene, poi, che i secondi possano «rientrare fra quelli per cui l'interessato ha prestato un consenso esplicito (art. 6, par. 1, lett. a) in combinato disposto con l'art. 9, par. 2, lett. a)), tra i trattamenti necessari per l'esecuzione di un compito di interesse pubblico (art. 6, par. 1, lett. e)), o tra i trattamenti necessari per il perseguimento del legittimo interesse del titolare del trattamento (art. 6, par. 1, lett. f), in combinato disposto con l'art. 9, par. 2, lett. i) o j)», GDPR[15].

Ancora più sensibile si rivela, tuttavia, la questione del riuso dei dati raccolti nell'ambito della sperimentazione clinica per finalità scientifiche ulteriori, vale a dire al di fuori del perimetro e delle previsioni del protocollo originario. Sul punto, il Comitato afferma, significativamente, che «qualora i dati siano successivamente trattati a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, tale trattamento non è a priori considerato incompatibile con la finalità iniziale, purché ciò avvenga in conformità delle disposizioni» dell'art. 89 GDPR, fermi restando gli obblighi previsti dalla vigente normativa in materia di protezione dei dati (con particolare riferimento alla correttezza del trattamento, la liceità, la necessità e la proporzionalità del trattamento, la qualità dei dati)[16].

Il quadro rimane ancora complesso e numerosi dubbi interpretativi impediscono attualmente di realizzare il pieno potenziale di eventuali aumentate possibilità di trattamento dei dati relativi alla salute nell'am-

[13] Comitato Europeo sulla Protezione dei Dati, *Parere 3/2019 relativo alle domande e risposte sull'interazione tra il regolamento sulla sperimentazione clinica e il regolamento generale sulla protezione dei dati (articolo 70, paragrafo 1, lettera b))*, pp. 4-5.

[14] Ivi, p. 5.

[15] Ivi, p. 6.

[16] Ivi, p. 9.

bito delle sperimentazioni cliniche, ovviamente nel rispetto dei diritti e delle libertà degli interessati, anche al fine di tutelarne maggiormente il diritto alla salute sia per la probabile maggiore efficacia dei percorsi terapeutici sia per gli intuitivi risparmi economici per l'assistenza sanitaria.

Trovare un equilibrio non è, tuttavia, un compito agevole.

Come ben evidenziato in dottrina, è opportuno potenziare il ruolo del paziente, che possa diventare parte attiva nella definizione delle strategie e nella progettazione degli studi clinici, assumendo nuovi diritti e correlate responsabilità nell'ambito delle sperimentazioni e dello sviluppo dei farmaci. La ricerca clinica può così avere l'obiettivo di costruire una vera e propria alleanza sociale, che coinvolga tutti i portatori di interesse (pazienti, professionisti sanitari, autorità regolatorie e aziende farmaceutiche) per giungere a prendere decisioni condivise: un processo collaborativo, dunque, che dovrebbe consentire di tener conto sia delle migliori evidenze disponibili sia delle preferenze e dei valori del paziente (senza dimenticare che proprio quest'ultimo si trova in una situazione di vulnerabilità, transitoria o permanente a seconda dei casi: preziosi, in tal senso, i contributi della dottrina)[17].

IV.3. Il framework di FACILITATE

Nell'ambito del progetto FACILITATE è stato sviluppato un framework etico; ancorché non ancora definitivo dal momento che il progetto è attualmente in corso (con conclusione nel 2026), permette di trarre utili spunti di riflessione in merito all'oggetto dell'indagine del presente volume. Più specificatamente, esso concepito come guida operativa per industria, accademia e altri *stakeholders* chiamati a muoversi nel terreno, spesso intricato, della restituzione dei dati.

Nell'ambito del Reg. (UE) 536/2014, esso è finalizzato assicurare una gestione eticamente corretta della restituzione dei dati individuali, definendo principi e procedure in grado di orientare le scelte e di ren-

[17] J.M.C. Blom, V. Rivi, F. Tascedda, L. Pani, *The nexus of social alliances and diverse moral domains: a bedrock for participatory clinical research*, in *Frontiers in Medicine*, 10 2023, (<https://www.frontiersin.org/journals/medicine/articles/10.3389/fmed.2023.1250247/full>).

derle giustificabili e controllabili. Il quadro distingue principi sostanziali e principi procedurali, non in rapporto gerarchico ma in un equilibrio da perseguire caso per caso; la bozza indica inoltre le modalità pratiche con cui tradurre tali principi e mantenerne il bilanciamento.

I principi sostanziali sono così individuati: (i) *Diritti e rispetto della persona e della collettività*. Le persone hanno diritto a decisioni autonome e informate, inclusa la scelta se ricevere o meno i dati della sperimentazione. La restituzione deve rispettare il diritto a essere informati, il diritto di accedere o di non accedere ai propri dati e le preferenze espresse dal partecipante. La restituzione non deve dipendere dal completamento della sperimentazione. (ii) *Beneficenza e non-maleficenza*. La restituzione dei dati deve essere guidata dal miglior interesse del partecipante e avvenire in modo da massimizzare i benefici e minimizzare i rischi per la persona coinvolta. (iii) *Riservatezza e confidenzialità*. La restituzione deve rispettare la riservatezza del soggetto e la confidenzialità dei suoi dati. Ogni eventuale limitazione di tali diritti deve essere necessaria, limitata, proporzionata, soggetta a responsabilità e trasparente, con adeguate misure a tutela continua della riservatezza e della confidenzialità. (iv) *Autonomia*. Principio fondamentale che afferma il diritto della persona a decisioni informate sulla propria partecipazione e sulla restituzione dei dati della sperimentazione. (v) *Utilità*. I dati restituiti devono avere valore per il partecipante, inteso in termini soggettivi (ad es. valore azionabile per le proprie scelte di salute), e non meramente oggettivi. (vi) *Potenziamento decisionale*. I partecipanti devono essere messi in condizione di assumere decisioni informate sulla propria salute. Sia i dati individuali restituiti sia il processo di restituzione (inclusa l'individuazione di chi effettua la restituzione) devono abilitare tale potenziamento. (vii) *Valore pubblico*. Scopo primario della ricerca clinica è la produzione di conoscenza generalizzabile a beneficio dei pazienti e della salute pubblica. Ogni restituzione, e la relativa tempistica, va bilanciata con l'integrità scientifica della sperimentazione. (viii) *Custodia dei dati*. Per restituire dati affidabili e di qualità è essenziale il controllo sul processo che ha generato i risultati. La tracciabilità dei processi assicura accuratezza e pertinenza dei dati restituiti al corretto partecipante. (ix) *Giustizia*. La restituzione deve avvenire in modo lecito, corretto ed equo. (x) *Trasparenza*. Il processo di restituzione va descritto in modo chiaro al momento del consenso informato: quali dati saranno restituiti, quando e come. Devono essere altresì chiare le moda-

lità da seguire qualora il partecipante modifichi le proprie preferenze. (xi) *Responsabilità*. Deve essere definito in modo univoco chi è responsabile di garantire la restituzione dei dati ai partecipanti[18].

La proposta integra principi chiave e oramai tradizionali della bioetica (beneficenza, non-maleficenza, giustizia) con categorie più recenti, tra cui potenziamento decisionale e utilità. In relazione al primo, la persona deve essere realmente autonoma nel prendere le proprie decisioni e ciò richiede strumenti, risorse, informazione e accompagnamento adeguati. In tal modo, pratiche e politiche non solo preservano la scelta individuale, ma abilitano una partecipazione piena e consapevole sulle decisioni che incidono sulla vita e sulla salute. Per ciò che concerne il secondo, i dati restituiti devono avere un valore concreto e azionabile per il partecipante, in un quadro di integrazione e coordinamento, e non di conflitto, con il diritto di accesso di cui all'art. 15 del GDPR (che rimane incondizionato)[19]; bisogna guardare al principio di utilità in prospettiva proattiva, guidando la restituzione anche quando il partecipante non

[18] Cfr. FACILITATE Consortium, *Deliverable 3.4 Ethical standards and guidelines No.* 2, 2024, pp. 5-6.

[19] Ai sensi dell'art. 15 GDPR, «1. L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni: a) le finalità del trattamento; b) le categorie di dati personali in questione; c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali; d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento; f) il diritto di proporre reclamo a un'autorità di controllo; g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine; h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato. 2. Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento. 3. Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento. In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune. 4. Il diritto di ottenere una copia di cui al paragrafo 3 non deve ledere i diritti e le libertà altrui».

sia in grado di formulare richieste puntuali o di anticipare la rilevanza clinica delle informazioni. Ai principi etici sopra menzionati, il *framework* etico di FACILITATE affianca principi e linee guida per l'attuazione: chiarificazione di ruoli e responsabilità lungo l'intero percorso decisionale; informazione chiara, continua e comprensibile ai partecipanti; pianificazione, già prevista nel protocollo, di se e come restituire dati individuali durante la sperimentazione e dopo la sua conclusione; previsione di ricontatto in presenza di informazioni potenzialmente rilevanti per la salute; riconoscimento dei diritti di accesso ai risultati delle indagini cui il partecipante abbia acconsentito. Dati urgenti e azionabili devono essere restituiti nel corso dello studio e ciò vale anche qualora la restituzione dei dati individuali comporti lo smascheramento involontario del partecipante e possa pregiudicare l'integrità complessiva della sperimentazione nel rispetto della disciplina sulle sperimentazioni cliniche; per informazioni non urgenti ma azionabili la restituzione è tendenzialmente dovuta, salvo esigenze di tutela dell'integrità scientifica. Al termine dello studio, la restituzione deve essere completa, con cautele adeguate per i dati sensibili e con l'indicazione del soggetto responsabile e delle modalità (lettera, portale dedicato, tramite il medico curante o un membro del team di ricerca, ecc.). È, inoltre, previsto il ritorno dei risultati generali in forme accessibili (incontri, seminari online, pubblicazione su siti dedicati), garantendo che tutti sappiano dove e come reperirli e possano porre domande. A sostegno di tali processi, è in sviluppo uno strumento digitale di informazione e decisione[20].

IV.4. Ricerca e protezione dei dati personali: dal soggetto all'oggetto

Una tendenza, propria della Società dell'informazione e algoritmica, lega la ricerca nell'ambito della salute (incluso lo svolgimento delle sperimentazioni cliniche) e la protezione dei dati attraverso la progressiva conversione della persona nel suo «doppio informazionale»[21]. Sul pia-

[20] Cfr. C. Staunton, J.M.C. Blom, D. Mascalzoni, on behalf of the IMI FACILITATE Consortium. *Ethical framework for FACILITATE: a foundation for the return of clinical trial data to participants*, op. cit., pp. 5-6.

[21] Per doppio informazionale si intende la rappresentazione algoritmica, costruita e situata, di un soggetto a fini decisionali. Si distingue dal c.d. gemello digitale che è,

no della normatività ciò espone al rischio, paradossale, di ridurre la tutela della persona a quella dell'"interessato" inteso nella sola accezione delle disposizioni in materia di protezione dei dati personali e, dunque, di confondere il soggetto della tutela (la persona) con il suo oggetto (i dati).

Questa impostazione difensiva non è neutra: la scomposizione della persona nelle sue componenti identificative la oggettifica come "interessato", singolarmente individuato, ma privo di relazione. Si perdono di vista, così, i beni giuridici che il diritto della ricerca e della protezione dei dati dovrebbero servire (la vita, la salute, l'autodeterminazione) in una prospettiva paternalistica e non di effettivo *empowerment*. È, questo, un punto cruciale: la ricerca scientifica, specie in ambito sanitario, non è l'antagonista di tali beni; al contrario, quando è ben governata, ne è uno strumento privilegiato. Essa consente di prevenire, diagnosticare e curare, di ridurre incertezze e diseguaglianze, di restituire al paziente informazioni comprensibili e quindi poteri di scelta. Essa, inoltre, contribuisce al benessere individuale e collettivo non solo per la via terapeutica, ma anche incidendo sugli stili di vita (basti pensare all'alimentazione e alla promozione di pratiche salutari) rendendo più razionali e trasparenti le decisioni senza trasformarle in imposizioni. Pertanto, una protezione dei dati che finisca per ostacolare in via di principio la ricerca tradisce sé stessa, perché sottrae alla persona delle opportunità di tutela effettiva.

In questa prospettiva, la compatibilità delle finalità di cui all'art. 5, par. 1, lett. b), GDPR, letta insieme alle garanzie per la ricerca scientifica di cui all'art. 89, non si configura come clausola eccezionale o di mera tolleranza: essa costituisce la cerniera argomentativa che consente di giustificare la transizione dalla continuità d'uso al riuso (legittimo) dei dati, mostrando che cosa si conserva, che cosa muta e per quali ragioni: non legittima semplificazioni e impone, invece, un preciso onere di motivazione circa la coerenza tra l'impianto originario e le nuove utilizzazioni, i limiti introdotti e le misure idonee a prevenire effetti lesivi. Non bisogna ovviamente confondere fra pseudonimizzazione e anonimizzazione: occorre valutare con estrema attenzione la residua possibilità di re-identificazione; inoltre, la qualità dei dati, la ricostruibilità della loro provenienza e delle trasformazioni cui sono stati sottoposti, nonché la traccia-

invece (per quanto riguarda il contesto del presente volume), il modello computazionale di una persona (paziente), sincronizzato con i relativi flussi di dati e idoneo a effettuare simulazioni predittive e a supportare il controllo a ciclo chiuso (*closed loop*).

bilità delle versioni, sono condizioni di correttezza metodologica e di affidabilità dei risultati, non meri adempimenti formali.

Nella prassi contemporanea, il consenso tende a ridursi a un adempimento burocratico: modulistica standardizzata, informative ridondanti, caselle da spuntare. Di qui la necessità di ripristinarne l'importante funzione di strumento attraverso cui l'ordinamento riconosce e tutela l'autodeterminazione della persona nella relazione di cura e di ricerca. Perché tale funzione non venga assolta solo sul piano meramente formale, il consenso deve poggiare su un'informazione comprensibile, su tempi e modalità ragionevoli di decisione, su effettivi spazi di interlocuzione e di ripensamento; soprattutto, deve avere ad oggetto ciò che si intende fare e le ragioni per cui lo si fa, non formule generiche né clausole di stile.

Quando, tuttavia, la finalità perseguita è di interesse pubblico e sono approntate idonee garanzie sostanziali, l'ordinamento ammette che la base giuridica non sia il consenso, ma la funzione collettiva della ricerca (artt. 6 e 9 GDPR, in combinato disposto con l'art. 89). Non costituisce, per ciò solo, una lesione della libertà e dei diritti della persona (nel suo ruolo di interessato): al contrario, si evita che essa risulti, in concreto, compressa da oneri informativi e decisionali sproporzionati, con l'esito paradossale di un paternalismo mascherato da autodeterminazione.

In tali ipotesi, il rispetto dei diritti della persona si misura non dalla quantità di firme raccolte, ma dalla qualità delle ragioni pubblicamente rese, dalla proporzionalità delle misure e dalla trasparenza delle pratiche (inclusa la restituzione dei risultati) attraverso cui la ricerca si fa strumento effettivo di tutela della vita, della salute e dell'autodeterminazione.

In tale quadro, trasparenza e restituzione assumono un rilievo primario. La prima non si realizza in una copiosa produzione documentale, ma è comunicazione delle finalità, dei metodi, dei criteri di selezione e di qualità dei dati, dei limiti e delle cautele; è la capacità di spiegare, a chi partecipa e alla comunità, come si è cercato di ridurre i rischi e perché le scelte compiute sono ragionevoli (anche mediante messa a disposizione della valutazione di impatto[22]). La restituzione, a sua volta, non

[22] La valutazione d'impatto sulla protezione dei dati è un documento cruciale per esporre le scelte compiute, che vengono argomentate: è lo spazio in cui si esplicitano la coerenza tra uso primario e riuso, la proporzionalità delle misure, le ragioni della disclosure e dell'eventuale anonimizzazione, e si rende conto del modo in cui la ricerca – in concreto – tutela la persona e non soltanto i suoi dati.

è concessione discrezionale, ma elemento costitutivo del patto di ricerca: i risultati aggregati vanno resi disponibili in modo chiaro; i risultati individuali, quando clinicamente validati e proporzionati, devono essere restituiti per consentire decisioni più consapevoli. In questo senso, comunicazione e restituzione riconducono l'"interessato" alla persona e dunque soggetto i cui diritti alla vita, alla salute e all'autodeterminazione devono essere tutelati.

Fondamentale, del resto, è la questione della fiducia, che rappresenta il collante fra i vari soggetti coinvolti. Difatti, fiducia e affidabilità sono essenziali per il successo della ricerca clinica, poiché incidono sul coinvolgimento dei partecipanti, sull'integrità dei dati e sugli esiti complessivi degli studi. Tali qualità scaturiscono da interazioni complesse tra i vari *stakeholders*: promotori, partecipanti, clinici, ricercatori e autorità regolatorie[23]. La fiducia, però, non è un punto di arrivo statico, bensì un principio dinamico e in evoluzione plasmato proprio dai soggetti sopracitati. Tuttavia, la fiducia nella ricerca clinica si confronta con minacce nuove e in evoluzione: fra esse, è primario lo scetticismo del pubblico causato anche dalla disinformazione digitale amplificata dai social media. Per contrastarla, le strategie future devono andare oltre la mera conformità etica, includendo alfabetizzazione digitale, comunicazione trasparente e partenariati con voci comunitarie affidabili. Tali sforzi sono cruciali per garantire che la ricerca non sia soltanto eticamente solida, ma anche socialmente intelligibile e contestualmente pertinente. Inoltre, la costruzione della fiducia non segue un modello unico: le sperimentazioni interventistiche richiedono una fiducia immediata e a elevata posta in gioco, in ragione dei rischi intrinseci; gli studi osservazionali, invece, sollevano preoccupazioni di lungo periodo sull'uso e sulla rappresentazione dei dati[24].

Anche nelle prospettive sopra evidenziate, e in conclusione, può dunque argomentarsi che la distinzione tra uso primario e uso secondario non debba essere letta come frattura, bensì come passaggio che esige motivazione: quando la finalità rimane coerente, le cautele sono reali e la persona è messa in condizione di conoscere e, per quanto possibile, di scegliere, il riuso non indebolisce la protezione; la rafforza, perché amplia

[23] J.C. Blom, V. Rivi, F. Tascedda, L. Pani, *Building trust in clinical research: a systems approach to ethical engagement and sustainable outcomes*, in «Frontiers in Pharmacology», 2025, doi 10.3389/fphar.2025.1570899, p. 2.

[24] Ivi, p. 8.

le possibilità di prevenire, diagnosticare e curare, e dunque di dare concreta attuazione ai beni giuridici posti a fondamento dell'ordinamento (artt. 2 e 32 Cost.). In questo orizzonte, ricerca e protezione dei dati possono essere contemperate, governandone la conflittualità e mutandola in interazione, così che diventino strumenti convergenti per proteggere la ricerca da tendenze fortemente paternalistiche la persona dai riduzionismi e, in particolare, dal dataismo, evitando che il "doppio informazionale" si sostituisca alla persona "reale" e, al contrario, mettendolo al servizio della sua libertà.

V. Conclusioni: salute digitale e vulnerabilità aumentata. Sfide e prospettive

V.1. Vulnerabilità aumentata e salute digitale

Il percorso argomentativo del presente volume consente di precisare in che senso la vulnerabilità sia "aumentata". L'aggettivo non allude a un mero incremento quantitativo, ma al fatto che lo strato informazionale si integra stabilmente nelle pratiche della cura e della salute digitale sino a co-determinarne contesti, tempi e priorità: come nella realtà aumentata, ciò che si aggiunge non si sovrappone, ma si fonde con la realtà e, per il tramite di tale mediazione percettiva, orienta la condotta.

Ne discende che le coordinate dell'esperienza sanitaria e del benessere digitale mutano il proprio statuto: sul piano spaziale, poiché la presa in carico e l'autogestione si estendono oltre i luoghi tradizionali, penetrando nei contesti ordinari di vita e moltiplicando i punti di esposizione e le dipendenze da infrastrutture digitali e organizzative; sul piano temporale, perché flussi continui e capacità predittive anticipano decisioni e proiettano sul presente vincoli e opportunità del domani; sul piano inferenziale, poiché i modelli, con le soglie e i criteri che li governano, non si limitano a descrivere, ma orientano le decisioni. In questo senso, la vulnerabilità "aumentata" è emblematica nel rappresentare la fusione operativa tra dato, modello e vita "reale", che coinvolge tanto i percorsi di cura quanto le pratiche di benessere mediate da strumenti informatici e reti telematiche.

Di qui la necessità, più volte esposta, di recuperare il concetto ontologico di persona in luogo della frammentazione nei profili che gli ambiti del giuridico e dell'economico, della normatività e del mercato, tendono a costruire: non solo interessato, utente, consumatore, cliente, e così via, ma soprattutto persona in relazione con gli altri. È essa, e non il suo "doppio informazionale", la misura di scopi, limiti e responsabilità.

L'autodeterminazione non si esaurisce nella formale prestazione di consensi sovente privi di reale significato in quanto parte di quel costante sovraccarico informativo che è una delle cifre della società contemporanea. È da intendersi, piuttosto, come pratica relazionale che richiede informazione comprensibile, tempi congrui, possibilità di ripensamento e di interlocuzione; le interfacce e i "gemelli digitali" la abilitano quando rendono visibili presupposti e costi delle scelte, la mortificano quando trasformano

la decisione in esecuzione di itinerari precostituiti. La deviazione motivata dal caso standard non è un cedimento allo specialismo, ma la sede in cui il giudizio professionale resta controllabile e applicato in modo ragionato alla persona, che torna a essere centrale nell'ambito della salute e della cura.

Da quanto esposto discendono talune implicazioni normative. Se la decisione è ibrida, ibrida è anche la responsabilità: vanno rese riconoscibili le assunzioni dei modelli, giustificate le soglie che li governano, conservata la possibilità di contestazione e di strumenti effettivi di tutela nel punto in cui gli esiti incidono. La protezione dei dati, in questa luce, non è fine a sé stessa: è garanzia abilitante insieme a qualità, sicurezza e correttezza metodologica, perché mantiene aperta la relazione tra la vita e la sua rappresentazione, impedendo che la seconda si sostituisca alla prima. Così intesa, essa sostiene una ricerca trasparente, controllabile e capace di restituzione accrescendo le possibilità di tutela della vita, della salute e dell'autodeterminazione.

In conclusione, l'analogia con la realtà aumentata non è un espediente retorico: chiarisce che l'"aumento" esige ragioni più stringenti e responsabilità più visibili, ma la stessa valutazione dell'*accountability* deve essere svolta in una prospettiva ampia, che valuti le attività di ricerca anche per i benefici che possono portare alla collettività bilanciando opportunamente i diritti e gli interessi delle persone coinvolte. È solo ancorando i dispositivi informazionali alla priorità della persona in relazione che la vulnerabilità, pur accresciuta dall'ibridazione digitale, può essere governata e non subìta.

V.2. Salute e benessere digitali: fra evoluzione, *nudging* e paternalismo algoritmico

La crescente ibridazione di pratiche e dispositivi rende sempre più evanescente il confine tra salute e benessere, come si è visto. Si consideri, infatti, che vi sono artefatti (come sensori, piattaforme di monitoraggio, sistemi di raccomandazione) impiegati sia nei percorsi di prevenzione, diagnosi, terapia e *follow-up* sia nelle pratiche quotidiane di automonitoraggio e promozione della salute; eppure, la continuità tecnica non si traduce automaticamente in continuità di garanzie, poiché basi giuridiche, responsabilità e strumenti di tutela variano in ragione delle finalità e del contesto d'uso. Alla massima tutela che l'ordinamento prescrive per i dispositivi medici e per l'utilizzo in ambito clinico (da parte di pazienti sotto controllo medico, professionisti e strutture) si affianca la criticità

della "zona grigia" degli artefatti che, pur non qualificandosi come dispositivi medici, incidono sulla salute digitale.

Com'è noto, il mercato tende a spingere verso forme che trasferiscono sulla persona il peso di decisioni preconfigurate (anche dinamicamente grazie alle continuative elaborazioni dei sistemi di IA): la spinta gentile scivola in eterodirezione, mentre l'intensificazione della misurazione e il rinvio a sistemi opachi accrescono dipendenze infrastrutturali e asimmetrie di comprensione difficilmente emendabili *ex post*. È in questo slittamento che la vulnerabilità è "aumentata": il dato non si limita a descrivere, ma incide, in modo anche determinante, sulle scelte, con effetti che superano il perimetro clinico e investono il quotidiano del benessere digitale.

Tuttavia, il *nudging* – già di per sé problematico[1] – è compatibile con un'etica della salute digitale quando preserva scelte ragionevoli e contestabili; non lo è quando l'architettura dei sistemi, giungendo anche a schemi manipolativi, indirizza preferenze in modo poco trasparente o non realmente esigibile. In tali contesti, soglie e indicatori sostituiscono biografie singolari con profili astratti e spostano la responsabilità dalla progettazione all'adesione (per lo più passiva) dell'utente. La promessa di *empowerment* si consuma nell'onere cognitivo di interpretare metriche opache: la persona viene ricondotta alla figura dell'"interessato" nella prospettiva del dataismo più che alla persona in relazione che, insieme a professionisti e istituzioni (e sovente nell'ambito del "mercato" della salute digitale), si autodetermina.

La progressiva degenerazione verso il paternalismo algoritmico è, dunque, concreta. Per combattere tale fenomeno, non v'è dubbio che sia necessario recuperare la centralità della persona in relazione, privilegiando gli aspetti sostanziali su quelli formali in merito a (i) finalità, (ii) idoneità e adeguatezza al contesto d'uso, (iii) necessità e proporzionalità, (iv) responsabilità e responsabilizzazione.

Più specificatamente, l'esposizione delle finalità dei trattamenti, lungi dal ridursi a una copiosa produzione documentale e a una granularità anche eccessiva dei consensi, esige la dichiarazione intelligibile di scopi, vincoli e priorità delle tecnologie, rendendo visibili i bilanciamenti che esse incorporano. L'idoneità e l'adeguatezza al contesto d'uso esigono

[1] Vi sono problemi epistemici, etici e pratici: «Il problema etico scaturisce da quello epistemico: se il *nudger* non conosce i veri interessi degli individui finirà per imporre interessi eteronomi che confliggono con l'autonomia e il diritto delle persone (liberale ed epistemicamente connotato) di autodeterminarsi compiendo scelte nel proprio interesse» (M. Galletti, S. Vida, *Libertà vigilata. Una critica del paternalismo libertario*, IF Press, Roma, 2018, p. 306).

che l'impiego del digitale sia motivato da un beneficio concreto e verificabile (clinico, organizzativo o di benessere) e non da mere enunciazioni di principio sull'innovazione o su asseriti benefici. I principi di necessità e proporzionalità escludono raccolte e trattamenti ridondanti, soprattutto quando i dati sono suscettibili di reimpieghi, anche indiretti, in ambiti sanitari. Infine, responsabilità definite e tutele effettive richiedono che spiegazioni, tracciabilità delle scelte e strumenti di tutela siano disponibili in relazione al punto in cui la decisione produce effetti, e che una vigilanza successiva all'implementazione intercetti tempestivamente scostamenti, pregiudizi algoritmici e impatti differenziati su gruppi e sottogruppi, predisponendo adeguati meccanismi di correzione.

Questa deriva, peraltro, non si esaurisce nell'ambito, ancorché trasversale e dunque necessariamente rilevante, della protezione dei dati. Il paternalismo algoritmico incide sulla qualità e sulla sicurezza delle cure e degli interventi nell'ambito del benessere, sull'appropriatezza clinica e organizzativa, sull'equità nell'accesso e nella distribuzione delle opportunità, sulla dignità e sull'eguaglianza con rischi di discriminazione diretta e indiretta; riguarda il rapporto fra standard e deviazione motivata, l'allocazione delle responsabilità lungo la filiera tecnico-organizzativa e la correttezza, anche sostanziale, delle procedure (spiegazioni comprensibili, strumenti di tutela e possibilità di contestazione, tempi e luoghi della decisione). Metriche e soglie operano come dispositivi normativi: definiscono che cosa conta e che cosa viene escluso, possono normalizzare corpi e condotte, medicalizzare il quotidiano e trasferire oneri cognitivi senza adeguata giustificazione. La questione investe, dunque, l'intero campo della bioetica della salute digitale (beneficenza, non maleficenza, autonomia, giustizia) e la trama costituzionale dei diritti fondamentali (basti pensare agli artt. 2, 3, 32 Cost.).

Questa impostazione consente, pertanto, di orientare l'innovazione senza frenarla. Restituisce al giudizio professionale controllabile il suo ruolo; chiarisce quando un artefatto ricade nell'orbita della cura (con gli obblighi che ne derivano) e quando resta nel perimetro del benessere, impedendo che la qualificazione in termini di "benessere", magari svolta per mere finalità promozionali e di marketing, diventi scorciatoia regolativa. Soprattutto, consolida una politica della fiducia che non si misura sulla quantità della produzione documentale, ma sulla qualità delle ragioni pubblicamente rese e sull'equità degli esiti per persone e comunità. In tal modo, dato e modello tornano a essere mezzi al servizio della persona, nella clinica e nella quotidianità, e non di terzi o, addirittura, essi stessi il fine.

V.3. Sfide e prospettive

Quanto esposto converge su tensioni che non richiedono un bilanciamento contabile dei valori, ma un assetto di garanzie e responsabilità capace di tenere insieme conoscenza, giustizia e tutela della persona in relazione nell'intero perimetro della salute digitale. Esse si dispiegano lungo quattro assi: capacità inferenziale e dovere di motivazione; apertura alla ricerca e protezione della persona; standardizzazione e personalizzazione proporzionata; sicurezza tecnica e sicurezza della cura e della salute digitale. È opportuno soffermarsi, sia pur sinteticamente, su ciascuno.

Una prima tensione oppone potenza inferenziale e dovere di motivazione. Quanto più i sistemi accrescono la capacità predittiva, tanto più l'ordinamento esige una spiegabilità proporzionata all'impatto: non si tratta di un accesso indiscriminato al codice sorgente (oltretutto di difficile realizzazione concreta anche in relazione al codice effettivamente eseguito da un sistema), ma ragioni operative verificabili, tracciabilità dei passaggi significativi, strumenti effettivi di tutela quando l'esito incide sui percorsi di salute e cura digitale. In difetto di tale architettura argomentativa e di responsabilità, l'errore può essere caratterizzato da scalabilità, invisibilità e/o irreparabilità, mentre la vulnerabilità diviene sistemica.

Una seconda tensione concerne il rapporto fra ricerca e protezione della persona. L'esperienza della restituzione dei dati e del riuso ragionevolmente regolato mostra che interessi individuali e collettivi possono essere ricomposti entro architetture di garanzia che rendano intelligibili, motivabili, controllabili e contestabili finalità, misure di minimizzazione e di riduzione del rischio di reidentificazione, permettendo di delineare catene di trattamento e responsabilità; e ciò anche quando i dati provengono da app, piattaforme e dispositivi di *m-health* o da servizi e prodotti non qualificati come dispositivi medici. Un obiettivo fondamentale, dunque, consiste nel non radicalizzare il conflitto fra consenso e interesse pubblico per dare invece realizzazione concreta alla responsabilizzazione, grazie alla già argomentata combinazione fra obblighi informativi e di valutazione di ciascun caso concreto (con particolare riferimento alla ragionevolezza dei rischi di re-identificazione).

Una terza tensione riguarda standardizzazione e personalizzazione proporzionata. Gli strumenti di regolazione tecnico-scientifica sono essenziali per diversi fini, dal controllo della spesa sanitaria e farmaceutica alla presunzione, in linea generale, della diligenza di una determinata

condotta professionale; diventano difensivi quando la deviazione motivata viene sostanzialmente esclusa e il giudizio professionale controllabile viene posto ai margini. Ciò vale tanto nei *setting* clinici quanto nei programmi e nelle pratiche di benessere digitale, dove la computazione generalizzata rischia di imporre degli standard di fatto. La via d'uscita non è l'arbitrio, ma un approccio ragionato e ragionevole al monitoraggio, con verifiche indipendenti e revisioni periodiche, tenendo conto dell'ambito sociale (persone e comunità) e delle relative diseguaglianze di accesso, consentendo deviazioni motivate, tracciabili e reversibili.

Infine, la tensione tra sicurezza tecnica e sicurezza della cura impone di guardare alla protezione della cibersicurezza come obiettivo fondamentale per la sopravvivenza stessa dell'ecosistema digitale. Continuità operativa, resilienza delle piattaforme, integrità e disponibilità di dati e modelli, interoperabilità semantica e chiara ripartizione dei rischi non sono oneri accessori, ma sono condizioni per il funzionamento di tale ecosistema. La cibersicurezza, in questo senso, è "cura della cura" (e, più ampiamente, della salute digitale): preserva la memoria informazionale e clinica, rende effettiva la trasparenza delle responsabilità operative e mantiene accessibili e funzionanti gli strumenti di tutela.

Quelle qui elencate sono, insieme, sfide e prospettive. Solo un diritto rigoroso e un'etica della salute digitale, operanti lungo l'intero ciclo di vita dei sistemi (sin dalla progettazione) possono trasformare le promesse della tecnica in capacità effettive di persone e comunità. Ciò implica una spiegabilità diffusa e proporzionata al rischio; la centralità della persona-in-relazione nel governo dei dati e dei modelli anche in contesti extraclinici; un investimento stabile in capitale professionale e nel tempo di cura; una fiducia radicata in pratiche controllabili e pubblicamente verificabili; la conformità non come elencazione di adempimenti, bensì quale responsabilità argomentata delle scelte ed equità misurabile dei loro esiti. Così la vulnerabilità è detta "aumentata" non in senso quantitativo, ma perché la dimensione digitale si innerva in quella materiale, riplasma tempi, luoghi e priorità dell'azione e genera forme di esposizione più intense o inedite. Sullo sfondo, il "doppio informazionale" resta nello statuto che gli compete: rappresentazione operativa a fini di cura e di governo, senza assurgere a surrogato della persona né criterio ultimo e autosufficiente della decisione.

Bibliografia

Acciai, R., Angeletti, S. (a cura di), *Il DPO protagonista dell'innovazione. Il responsabile della protezione dei dati tra competenze e certificazioni*, Aracne, Roma, 2019.

Amato Mangiameli, A.C., *Algoritmi e big data. Dalla carta sulla robotica*, in «Rivista di filosofia del diritto», 1, 2019, pp. 107-124.

Amato Mangiameli, A.C., Tecno-*diritto e* tecno-*regolazione. Spunti di riflessione*, in «Rivista di fiosofia del diritto», speciale, 2017, pp. 87-112.

Amato, S., *Caratteri del biodiritto*, in «Rivista di filosofia del diritto», 1, 2013, pp. 31-50.

Id., *Neuroscienze e utilizzazione militare delle tecniche di potenziamento umano*, in «Etica & politica», 2, 2014, pp. 182-198.

Id., *Biodiritto 4.0. Intelligenza artificiale e nuove tecnologie*, Giappichelli, Torino, 2020.

Appiah, K.A., *The Ethics of Identity*, Princeton University Press, Princeton, 2005.

Balestra, M.L., *Electronic Health Records: Patient Care and Ethical and Legal Implications for Nurse Practitioners*, in «The Journal for Nurse Practitioners», 2, 2017, pp. 105-111.

Barfield, W. (ed.), *The Cambridge Handbook of the Law of Algorithmics*, Cambridge, 2020.

Balkin, J., *The Three Laws of Robotics in the Age of Big Data*, in «Ohio State Law Journal», Vol. 78, 5, 2017, pp. 1217-1241.

Benkler, Y., *The Wealth of Networks. How Social Production Tranforms Markets and Freedom*, Yale University Press, New Haven-London, 2006.

Bhuta, N., Beck, S., Geiss, R., Kress, C., Liu, H.Y. (eds.), *Autonomous Weapons Systems: Law, Ethics, Policy*, Cambridge University Press, Cambridge, 2016.

Blobel, B., *Analysis, design and implementation of secure and interoperable information systems*, IOS Press, Amsterdam, 2002.

Blom, J.C., Rivi, V., Tascedda, F., Pani, L. *Building trust in clinical research: a systems approach to ethical engagement and sustainable outcomes*, in «Frontiers in Pharmacology», 2025, doi 10.3389/fphar.2025.1570899, pp. 1-10.

Bodenheimer, T., Grumbach, K., *Electronic Technology. A Spark to Revitalize Primary Care?*, in «Journal of the American Medical Association», 2, 2003, pp. 259-264.

Borsellino, P., *Covid-19: Quali criteri per l'accesso alle cure e la limitazione terapeutica in tempo di emergenza sanitaria?*, in «Notizie di Politeia», 2020, pp. 5-25.

Id., *Bioetica tra "morali" e diritto*, nuova ed., Raffaello Cortina, Milano, 2018

Botrugno, C., *Telemedicina e trasformazione dei sistemi sanitari. Un'indagine di bioetica*, Aracne, Roma, 2018.

Breslow, L., *Health care versus medical care: implications for data handling*, in M. Laudet (ed.), *Proceedings of an international symposium*, Taylor and Francis, London, 1977, p. 69-75.

Brighi, R., *Il valore informativo dei dati in rete: il problema della* veridicità. *Analisi e soluzioni informatico-giuridiche*, in C. Faralli, R. Brighi, M. Martoni (a cura di), *Strumenti, diritti, regole e nuove relazioni di cura. Il Paziente europeo protagonista nell'eHealth*, Giappichelli, Torino, 2015, pp. 21-42.

Ead., *The Quality and Veracity of Digital Data on Health: from Electronic Health Records to Big Data*, in «Revista de Bioética y Derecho», 42, 2018, pp. 163-179.

Bronzino, J.D., Smith, V.H., Wade, M.L., *Medical Technology and Society: An Interdisciplinary Perspective*, MIT Press, Cambridge-London, 1990.

Buzzi, F., Danesino, P. (a cura di), *Gli esercenti le professioni sanitarie nel recente riassetto formativo. Interazioni e responsabilità nell'attuale cornice normativa delle aziende sanitarie. Pavia, 26-27 settembre 2002*, Giuffrè, Milano, 2003.

Campagnoli, M.N., Farina, M., *Identità digitale e intelligenza artificiale: tra regolazioni, poteri asimmetrici e sfide per il futuro*, in «Journal of Ethical and Legal Tecnologies», 1, 2025, pp. 81-115.

Casadei, Th., Pietropaoli, S., *Intelligenza artificiale: l'ultima sfida per il diritto?*, in Id. (a cura di) *Diritto e tecnologie informatiche. Questioni di informatica giuridica, prospettive istituzionali e sfide sociali*, Wolters Kluwer, Milano, 2024, pp. 257-272.

Casadei, Th., *I diritti sociali. Un percorso filosofico-giuridico*, Firenze University Press, Firenze, 2012.

Id., *Soggetti in contesto: vulnerabilità e diritti umani*, in Id. (a cura di), *Diritti umani e soggetti vulnerabili, Violazioni, trasformazioni, aporie*, Giappichelli, Torino, 2012, pp. 91-116.

Id., *Diritto e (dis)parità. Dalla discriminazione di genere alla democrazia paritaria*, Aracne, Roma, 2017.

Id., *La vulnerabilità in prospettiva critica*, in O. Giolo, B. Pastore (a cura di), *Vulnerabilità. Analisi multidisciplinare di un concetto*, Carocci, Roma, 2018, pp. 73-99.

Id., *L'irruzione della post-verità*, in «Governare la paura», 2019, pp. 4-5, <https://governarelapaura.unibo.it/article/view/9411>.

Id., *I divari digitali di genere: frontiera del "costittuzionalismo digitale"?*, in «Diritto e questioni pubbliche», 2025, *Special Issue* (maggio), pp. 7-24.

Cerrina Feroni, G. (a cura di), *Commerciabilità dei dati personali. Profili economici, giuridici, etici della monetizzazione*, Il Mulino, Bologna, 2024.

Chou, W.S., Oh, A., Klein, W.M.P., *Addressing health-related misinformation on social media*, in «JAMA», 320, 23, 2018, pp. 2417-2418.

Collen, M.F., Kulikowski, C.A., *The Development of Digital Computers*, in M.F. Collen, M.J. Ball (eds.), *The History of Medical Informatics in the United States*, Springer, New York, 2015, pp. 3-73.

Collen, M.F., Shortliffe, E.H., *The Creation of a New Discipline*, in M.F. Collen, M.J. Ball (eds.), cit., pp. 75-120.

Collen, M.F., *Preliminary announcement for the third world conference on medical informatics*, Medinfo 80, 1977.

Colomba, V., Zanetti, G., *Aspetti problematici della nozione di privacy da un punto di vista filosofico-giuridico*, in «Teoria e critica della regolazione sociale», 1, 2017, pp. 27-40.

Comitato Europeo sulla Protezione dei Dati, *Linee guida 5/2020 sul consenso ai sensi del regolamento (UE 2016/679)*, 4 maggio 2020.

Id., *Parere 3/2019 relativo alle domande e risposte sull'interazione tra il regolamento sulla sperimentazione clinica e il regolamento generale sulla protezione dei dati*.

Comitato Nazionale per la Bioetica, *Etica, salute e nuove tecnologie dell'informazione*, Roma, 2006.

Id., *L'identificazione del corpo umano: profili bioetici della biometria*, Roma, 2010.

Id., *Diritti umani, etica medica e tecnologie di potenziamento (enhancement) in ambito militare*, Roma, 2013.

Id., *"Mobile-health" e applicazioni per la salute: aspetti bioetici*, Roma, 2015, p. 5.

Id., *Tecnologie dell'informazione e della comunicazione e* big data*: profili bioetici*, Roma, 2016.

Comitato Nazionale per la Bioetica-Comitato Nazionale per la Biosicurezza le Biotecnologie e le Scienze della Vita, *Intelligenza artificiale e medicina: aspetti etici*, Roma, 2020.

Commissione delle Comunità Europee, *eEurope 2005: una società dell'informazione per tutti*, COM (2002).

Id., *Sanità elettronica – migliorare l'assistenza sanitaria dei cittadini europei: piano d'azione per uno spazio europeo della sanità elettronica*, COM (2004).

Coniglione, C., *Le criticità del diritto computazionale e della giustizia predittiva. Le* humanities *come "nuova" modalità di approccio al diritto contemporaneo?*, in «Heliopolis», 1, 2025, pp. 67-79.

Corso, L., *Vulnerabilità e concetto di diritto*, in Id., G. Talamo (a cura di), *Vulnerabilità di fronte alle istituzioni e vulnerabilità delle istituzioni*, Giappichelli, Torino, 2019, pp. 3-14.

Id., *Breve tassonomia dei rapporti fra Intelligenza Artificiale, etica e diritto. Tre questioni*, in «AI Law», 2, 2025, pp. 204-222.

Cowie, M.R. *et al.*, *Electronic health records to facilitate clinical research*, in «Clinical Research in Cardiology», 106, 2017, pp. 1-9.

Cristiani, P., Pinciroli, F., Stefanelli, M. (a cura di), *I sistemi informativi sanitari*, Patron, Bologna, 1996.

Crocetta, C., *A partire da* Dewey*: didattica del diritto e cittadinanza democratica,* in *Teoria e critica della regolazione sociale*, 2020, <https://www.mimesisjournals.com/ojs/index.php/tcrs/article/view/284>.

D'Aloia, A., Errigo, M.C. (eds.), *Neuroscience and Law: Complicated Crossings and New Perspectives*, Springer, Cham, 2020.

D'Avack, L., *CoViD-19: criteri etici*, in «BioLaw Journal. Rivista di BioDiritto», 1S, 2020, pp. 371-378.

de Dombal, F.T., *Ethical considerations concerning computers in medicine in the 1980s*, in «Journal of Medical Ethics», 13, 4, 1987, pp. 179-184; R.A. Miller, K.F. Schaffner, A. Meisel, *Ethical and Legal Issues Related to the Use of Computer Programs in Clinical Medicine*, in «Annals of Internal Medicine», 102, 1985, pp. 529-536.

De Panfilis, L., Zullo, S., *Aspetti etici delle applicazioni* eHealth, in C. Faralli, R. Brighi, M. Martoni (a cura di), *Strumenti, diritti, regole e nuove relazioni di cura. Il Paziente europeo protagonista nell'eHealth*, Giappichelli, Torino, 2015, pp. 55-67.

De Vanna, F., *Il diritto "imprevedibile": notazioni sulla teoria della necessità a partire dall'emergenza Covid-19*, in «Nomos», 2020, 2 (<https://www.nomos-leattualitaneldiritto.it/nomos/francesco-de-vanna-il-diritto-imprevedibile-notazioni-sulla-teoria-della-necessita-a-partire-dallemergenza-covid-19>).

Di Giandomenico, A., *il consenso informato: questioni di frontiera*, in P. Savarese, G. Sorgi (a cura di), *Filosofia, politica e diritto: questioni di frontiera. Scritti in onore di Teresa Serra*, FrancoAngeli, Milano, 2018, p. 71-79.

Donati, F., Finocchiaro, G., Paolucci, F., Pollicino, O. (a cura di), *La disciplina dell'intelligenza artificiale*, Giuffrè, Milano, 2025.

ENISA, *ENISA overview of cybersecurity and related terminology*, Heraklion, 2017.

Id., *ENISA threat landscape 2024*, Attiki-Heraklion-Brussels, 2024.

European Group on Ethics in Science and New technologies, *The ethical implications of new health technologies and citizen participation*, Brussels, 2015.

Id., *Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems*, Brussels, 2018.

Faini, F., *Big data, algoritmi e diritti*, in «DPCE online», 3, 2019, pp. 1869-1882.

Ead., Data society: *governo dei dati e tutela dei diritti nell'era digitale*, Giuffrè, Milano, 2019.

Faioli, M., *Mansioni e macchina intelligente*, Giappichelli, Torino, 2019.

Faralli, C., *La filosofia del diritto contemporanea*, Laterza, Roma-Bari, 2012.

Fineman, M.A., *The Vulnerable Subject: Anchoring Equality in the Human Condition*, in «Yale Journal of Law and Feminism», 2008, pp. 1-23.

Fioriglio, G., Szolovits, P., *Copy Fees and Patients' Rights to Obtain a Copy of Their Medical Records: From Law to Reality*, in *Proceedings of American Medical Informatics Association Annual Symposium*, 2005, pp. 251-255.

Fioriglio, G., *Il diritto alla privacy. Nuove frontiere nell'era di Internet*, Bononia University Press, Bologna, 2008.

Id., *La "dittatura" dell'algoritmo: motori di ricerca web e neutralità della indicizzazione. Profili informatico-giuridici*, in «Bocconi Legal Papers», 5, 2015, pp. 113-139.

Id., *Contro la post-verità: il pluralismo assiologico quale limite del potere e garanzia della giustizia nello Stato costituzionale*, in «Nomos», 2016, 3, <https://www.nomos-

leattualitaneldiritto.it/nomos/gianluigi-fioriglio-contro-la-postverita-il-pluralismo-assiologico-quale-limite-del-potere-e-garanzia-della-giustizia-nello-stato-costituzionale/>.

Id., *Opacità dei sistemi intelligenti e sicurezza informatica: un difficile equilibrio fra regolazione e tecno-regolazione*, in «Rivista elettronica di Diritto, Economia, Management», 3, 2016.

Id., *Post-verità, paura e controllo dell'informazione: quale ruolo per il diritto?*, in *Governare la paura*, 2019, pp. 105-124; <https://governarelapaura.unibo.it/article/view/9416>).

Id., *La protezione dei dati sanitari nella Società algoritmica. Profili informatico-giuridici*, in «Journal of Ethical and Legal Technologies», 2, 2021, pp. 79-102.

Id., *La Società algoritmica fra opacità e spiegabilità: profili informatico-giuridici,* in «Ars interpretandi», 1, 2021, pp. 53-67.

Id., *Riflessioni sul "feticismo della legge" nella società contemporanea*, in A. Di Giandomenico (a cura di) *ETSI DEUS NON DARETUR… Scritti in memoria di Serenella Armellini*, Giappichelli, Torino, 2023, pp. 295-311.

Id., *Trattamento dei dati sanitari e ricerca medica: profili informatico-giuridici e istituzionali nel contesto europeo*, in «Jura Gentium», 2, 2025.

Floridi, L, *Infosfera. Etica e filosofia nell'età dell'informazione*, tr. it., Giappichelli, Torino, 2009.

Id., *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, tr. it., Raffaello Cortina, Milano, 2017.

Id., *Pensare l'infosfera. La filosofia come design concettuale*, tr. it., Raffaello Cortina, Milano, 2020 (versione ridotta, comprendente l'introduzione, i primi quattro capitoli e la postfazione, di *The Logic of Information. A Theory of Philosophy as Conceptual Design*, Oxford University Press, Oxford, 2019).

Floridi, L. *et al.*, *AI4People – An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations*, in *Minds and Machines*, 2018, 28, pp. 689-707.

Ford, R.A., Price, N., *Privacy and Accountability in Black-Box Medicine*, in «Michigan Telecommunications and Technology Law Review», 1, 2016, pp. 26-29.

Forester, T., Morrison, P., *Computer Ethics. Cautionary Tales and Ethical Dilemmas in Computing*, MIT Press, Cambridge-London, 1994.

Foucault, M., *The Birth of Clinic. An Archaeology of Medical Perception*, Routledge, London, 1976.

Friedberg, M.W., *et al.*, *Factors Affecting Physician Professional Satisfaction and Their Implications for Patient Care, Health Systems, and Health Policy*, RAND Health, Santa Monica, 2013.

Fuselli, S., *Diritto, neuroscienze, filosofia*, FrancoAngeli, Milano, 2014;

Id., *Metaverso e neurotecnologie: una ricognizione*, in «Journal of Ethics and Legal Technologies», 5, 2, 2023, pp. 6-28;

Gable, J.K., *An Overview of the Legal Liabilities Facing Manufacturers of Medical Information Systems*, in «Quinnipiac Health Law Journal», 5, 2001, pp. 127-147.

Galletti, M., Vida, S., *Libertà vigilata. Una critica del paternalismo libertario*, IF Press, Roma, 2018.

Garante per la protezione dei dati personali, *Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario*, 7 marzo 2019, provv. n. 55/2019 (doc. web n. 9091942).

Garapon, A., Lassègue, J., *Justice digitale: révolution graphique et rupture anthropologique*, Presses Universitaires de France, Paris, 2018.

Giandomenico, A. (a cura di), *ETSI DEUS NON DARETUR… Scritti in memoria di Serenella Armellini*, Giappichelli, Torino, 2023.

Glenn Cohen, I., Fernandez Lynch, H., Vayena, E., Gasser, U. (eds.), *Big Data, Health Law, and Bioethics*, Cambridge University Press, Cambridge, 2018.

Glenn Cohen, I., Kramer, D.B., Adler-Milstein, J., Shachar, C., *Digital Health Care outside of Traditional Clinical Settings. Ethical, legal and regulatory challenges and opportunities*, Cambridge University Press, Cambridge, 2024.

Goodman, K.W., Cushman, R., Miller, R.A, *Ethics in Biomedical and Health Informatics: Users, Standards, and Outcomes*, in E.H. Shortliffe, J.J. Cimino (eds.), *Biomedical Informatics. Computer Applications in Health Care and Biomedicine*, Springer, New York, 4th ed., 2014, p. 330.

Goodman, K.W. (a cura di), *Etica, informatica e medicina. L'informatica e la trasformazione dell'assistenza sanitaria* (1998), tr. it., Il Pensiero Scientifico, Roma, 1999.

Gorgoni, G., *Stay Human. The quest for Responsability in the Algorithmic Sociey*, in «Journal of Ethics and Legal Technologies», 2, 2020, pp. 31-47.

Greenes, R.A., Siegel, E.R., *Characterization of an emerging field: approaches to defining the literature and disciplinary boundaries of medical informatics*, in *Proceedings of the Annual Symposium on Computer Applications in Medical Care*, 1987, p. 413.

Gruppo di lavoro Articolo 29, *Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche (CCE)*, 00323/07EN, WP 131, 15 febbraio 2007.

Guerra, G., *La sicurezza degli artefatti robotici in prospettiva comparatistica. Dal cambiamento tecnologico all'adattamento giuridico*, Il Mulino, Bologna, 2018.

Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR del Medical Device Coordination Group.

Häberle, P., *Diritto e verità*, tr. it., Einaudi, Torino, 2000.

Hill, R.G., Lears, L.W., Melanson, S.W., *4000 Clicks: a productivity analysis of electronic medical records in a community hospital ED*, in «American Journal of Emergency Medicine», 31, 2013, pp. 1591-1594.

Hill, R.G., Sears, L.M., Melanson, S.W., *4000 Clicks: a productivity analysis of electronic medical records in a community hospital ED*, in «American Journal of Emergency Medicine», 31, 2013, pp. 1591-1594.

Iaselli, M. (a cura di), *AI Act. Principi, regole ed applicazioni pratiche del Reg. UE 1689/2024*, Maggioli, Santarcangelo di Romagna, 2024.

Irti, N., *Scambi senza accordo*, in «Rivista trimestrale di diritto e procedura civile», 1998, pp. 347-364.

Kanchan, S., Gaidhane, A., *Social Media Role and Its Impact on Public Health: A Narrative Review*, in «Cureus», 15, 1. 2023, doi:10.7759/cureus.33737, pp. 1-10.

Kodama K, Sengoku, S. (eds.), *Mobile Health (mHealth). Rethinking Innovation Management to Harmonize AI and Social Design*, Springer, Singapore, 2022.

Kohn, L.T., Corrigan, J.M., Donaldson, M.S., (eds,), *To Err is Human: Building a Safer Health System*, National Academy Press, Washington, DC, 2000.

Kulikowski, C.A., *et al.*, *AMIA Board White Paper: definition of biomedical informatics and specification of core competencies for graduate education in the discipline*, in Journal of American Medical Informatics Association, 19, 2012, pp. 932-933.

La Torre, M., *La verità del diritto senza verità*, in «Sociologia del diritto», 1, 2013, pp. 187-199.

Lagioia, F., Contissa, G., *The strange case of Dr. Watson: liability implications of AI evidence-based decision support systems in health care*, in «European Journal of Legal Studies», 2, 2020, pp. 245-289.

Lettieri, N., *Antigone e gli algoritmi. Appunti per un approccio giusfilosofico*, Mucchi, Modena, 2020.

Leveson, N., Turner, C.S., *An Investigation of the Therac-25 Accidents*, *IEEE Computer*, 1993, 7, pp. 18-41.

Lin, P., Abney, K., Bekey, G.A. (eds.), *Robot Ethics. The Ethical and Social Implications of Robotics*, MIT Press, Cambridge-London, 2014.

Lioy, A., *Riservatezza e sicurezza nei sistemi informativi sanitari*, in P. Cristiani, F. Pinciroli, M. Stefanelli (a cura di), Patron, Bologna, 1996, pp. 143-155.

Lippeveld, T., Sauerborn, R., Bodart, C. (eds), *Design and implementation of health information systems*, World Health Organization, Geneva, 2000.

Llano Alonso, F.H., *Transumanesimo, vulnerabilità e dignità umana: il giurista di fronte alle sfide della rivoluzione tecnologica 4*.0, in «Ordines», 2, 2021, pp. 106-122.

Losacco, A., *Il responsabile della protezione dei dati (RPD): equivalente italiano del data protection officer (DPO)*, Jovene, Napoli, 2018.

Macioce, F., *La vulnerabilità di gruppo. Funzione e limiti di un concetto controverso*, Giappichelli, Torino, 2021

Magnuson, J.A., B.E. Dixon, B.E. (eds.), *Public Health Informatics and Information Systems*, 3rd Edition, Springer, Cham, 2020.

Maioli, C., Sánchez Jordán, E., *Big Data e capacità informativa per l'autodeterminazione del paziente*, in C. Faralli, R. Brighi, M. Martoni (a cura di), *Strumenti, diritti, regole e nuove relazioni di cura. Il Paziente europeo protagonista nell'eHealth*, Giappichelli, Torino, 2015, pp. 155-176.

Mancuso, F., *Le 'verità' del diritto. Pluralismo dei valori e legittimità*, Giappichelli, Torino, 2013.

Martoni, M., *Datificazione dei nativi digitali. Una prima ricognizione e alcune brevi note sull'educazione alla cittadinanza digitale*, in «Federalismi.it», 1, 2020, pp. 119-136.

Mayer-Schönberger, V., Cukier, K., *Big Data: A Revolution That Will Transform How We Live, Work and Think*, John Murray, London, 2013.

Mazza Laboccetta, A., *Telemedicina: sfide, problemi, opportunità*, in «Federalismi.it», 22, 2023, pp. 135-182.

Mazzuca, J., *L'intelligenza artificiale. Luci e ombre del ragionamento algoritmico*, in «Ragion pratica», 2024, 1, pp. 241-264.

McCarthy, J., Hayes, P., *Some philosophical problems from the standpoint of artificial intelligence*, in «Machine Intelligence», 4, 1969, pp. 463-502.

McCarthy, J., Minsky, M.L., Rochester, N., Shannon, C.E. *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence*, in *AI Magazine*, 27, 4, 2006, pp. 1-13.

Micklitz, H.W., Pollicino, O., Simoncini, A., Sartor G., De Gregorio, G (eds.), *Constitutional Challenges in the Algorithmic Society*, Cambridge, 2021.

Milana, V., *La cartella clinica*, in F. Buzzi, Danesino (a cura di), *Gli esercenti le professioni sanitarie nel recente riassetto formativo. Interazioni e responsabilità nell'attuale cornice normativa delle aziende sanitarie. Pavia, 26-27 settembre 2002*, Giuffrè, Milano, 2003, pp. 215-218.

Miniscalco, N., *La sorveglianza attiva per contrastare la diffusione dell'epidemia di Covid-19: strumento di controllo o di garanzia per i cittadini?*, in *Osservatorio costituzionale*, 3, 2020, pp. 95-115.

Mitnick, K.D., *L'arte dell'inganno. I consigli dell'hacker più famoso del mondo*, tr. it., Feltrinelli, Milano, 2003.

Moro, P., *Libertà del* robot*? Sull'etica delle macchine intelligenti*, in R. Brighi, S. Zullo (a cura di), *Filosofia del diritto e nuove tecnologie. Prospettive di ricerca tra teoria e pratica*, Aracne, Roma, 2015, pp. 525-544.

National Research Council, *For the Record. Protecting Electronic Health Information*, National Academy Press, Washington, DC, 1997.

Nifosi-Sutton, I., *The Protection of Vulnerable Groups under International Human Rights Law*, Routledge, New York-London, 2017.

Norris, P., *Digital Divide. Civic Engagement, Information Poverty, and the Internet Worldwide*, New York, Cambridge University Press, 2002.

Numerico, T., *Intelligenza artificiale e algoritmi: datificazione, politica, epistemologia*, in «Consecutio Rerum», 2019, 6, pp. 241-271.

Nussbaum, N.C., *Non per profitto. Perché le democrazie hanno bisogno della cultura umanistica*, tr. it., Il Mulino, Bologna, 2013.

Ohmann, C. *et al.*, *Sharing and reuse of individual participant data from clinical trials: principles and recommendations*, in «BMJ Open», 2017, (doi:10.1136/bmjopen-2017-018647).

Pagallo, U., *Prolegomeni d'informatica giuridica*, Cedam, Padova, 2003.
Id., *The Laws of Robots. Crimes, Contracts, and Torts*, Springer, Dordrecht, 2013.
Id., *Algoritmi e conoscibilità*, in «Rivista di Filosofia del diritto», 1, 2020, pp. 93-106.
Id., *La grande trasformazione. Datificazione della società, tutela dell'ambiente e rischi e opportunità dell'innovazione tecnologica*, in M. Durante, U. Pagallo (a cura di), *La politica dei dati. Il governo delle nuove tecnologie tra diritto, economia e società*, Mimesis, Milano-Udine, 2022, pp. 123-140.
Palazzani, L., *Il potenziamento umano. Tecnoscienza, etica e diritto*, Giappichelli, Torino, 2015.
Ead., *La pandemia CoViD-19 e il dilemma per l'etica quando le risorse sono limitate: chi curare?*, in «BioLaw Journal. Rivista di BioDiritto», 1S, 2020, pp. 359-370.
Ead., *Tecnologie dell'informazione e intelligenza artificiale. Sfide etiche al diritto*, Studium, Roma, 2020.
Palmirani, M. Big data *e conoscenza*, in «Rivista di Filosofia del diritto», 1, 2020, pp. 73-91.
Pariotti, E., *Vulnerabilità, approccio intersezionale e linguaggio dei diritti*, in «GenIUS», 2, 2023, pp. 35-42.
Pasquale, F., *The Black Box Society. The Secret Algorithms That Control Money and Information*, Harvard University Press, Cambridge-London, 2015.
Id., *Towards a Fourth Law of Robotics: Preserving Attribution, Responsability and Explanaibility in an Algorithmic Society*, in «Ohio State Law Journal», Vol. 78, 2017, pp. 1243-1255.
Pastore, B., *Tecnologie emergenti, incertezze della scienza, regolamentazione giuridica*, in «Teoria e critica della regolazione sociale», 2, 2018, pp. 98-112.
Id., *Semantica della vulnerabilità, soggetto, cultura giuridica*, Giappichelli, Torino, 2021.
Patterson, D., *Diritto e verità*, tr. it., Giuffrè, Milano, 2010.
PCAST (President's Council of Advisors on Science and Technology), *Priorities for Personalized Medicine. Report of the President's Council of Advisors on Science and Technology*, Washington D.C., 2008.
Pettit, P., *Il repubblicanesimo*, Feltrinelli, Milano, (1977) 2000.
Pietropaoli, S., *Habeas data. I diritti umani alla prova dei* big data, in S. Faro, T.E. Frosini, G. Peruginelli (a cura di), *Dati e algoritmi. Diritto e diritti nella società digitale*, Il Mulino, Bologna, 2020, pp. 97-111
Pino, G., *Diritti sociali. Per una critica di alcuni luoghi comuni*, in «Ragion pratica», 2016, pp. 495-518.
Pintore, A., *Il diritto senza verità*, Giappichelli, Torino, 1996.
Pizzetti, F.G., *Potenziamento umano e principio lavorista. Spunti di riflessione*, in «Rivista di filosofia del diritto», 2, 2018, pp. 261-272.
Pomarici, U., *Il prisma umano della dignità nell'era delle tecnoscienze. Spunti per una discussione*, in «Rivista di Filosofia del diritto», 2015, speciale, pp. 141-169.
Portz, J., Moore, S., Bull, S., *Evolutionary Trends in the Adoption, Adaptation, and Abandonment of Mobile Health Technologies: Viewpoint Based on*

25 Years of Research, in «Journal of Medical Internet Research», 26, 2024, doi:10.2196/62790.

Price, N., *Black-Box Medicine*, in «Harvard Journal of Law & Technology», 2, 2015, pp. 427-430.

Punzi, A., *L'umanesimo digitale: verso un nuovo principio di responsabilità?*, in «Democrazia e diritti sociali», 1, 2023, pp. 23-32.

Id., *L'Artificial Intelligence Act dell'Unione Europea*, in *Rassegna dell'Arma dei Carabinieri*, 2024, 2, pp. 79-89; G. Taddei Elmi, A. Contaldo (a cura di), *Intelligenza artificiale. AI Act, Regolamento (UE) 1689/2024: il nuovo scenario giuridico europeo*, Pacini, Pisa, 2024.

Id., *Accolse l'uomo come opera di natura indefinita". Note su esperienza giuridica e nuovo ordine delle intelligenze*, in «Rivista di filosofia del diritto», 1, 2025, pp. 21-32.

Re, L., *Introduzione. La vulnerabilità fra etica, politica, diritto*, in, M.G. Bernardini, B. Casalini, O. Giolo, L. Re (a cura di), *Vulnerabilità: etica, politica, diritto*, IF Press, Roma, 2018, pp. 7-26.

Reichman, J.H., *Rethinking the Role of Clinical Trial Data in International Intellectual Property Law: the Case for a Public Goods Approach*, in «Marquette Intellectual Property Law Review», 13, 1, 2009, pp. 1-68.

Riccobono, F., *I diritti e lo Stato*, Giappichelli, Torino, 2004.

Rodotà, S., *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in «Rivista critica del diritto privato», 1997, pp. 583-609.

Id., *Il diritto di avere diritti*, Laterza, Roma-Bari, 2012.

Romeo, F., *Il dato digitale e la natura delle cose*, in A. Ballarini (a cura di), *Diritto interessi ermeneutica*, Giappichelli, Torino, 2012, pp. 87-124.

Rosotti, A., *Informatica Medica. Sistemi Informativi Sanitari e Reti di Telemedicina*, McGraw Hill, Milano, II ed., 2021.

Ruckenstein M., Dow Schüll N., *Tha Datafication of Health*, in «Annual Review of Anthropology», 46, 2017, pp. 261-278.

Ruggiu, D., *Spazio economico, tecnologie digitali e decostruzione dello spazio normativo del soggetto*, in «Ars interpretandi», 2, 2024, pp. 61-78.

Russell, J., Norvig, P., *Artificial Intelligence. A Modern Approach*, 4th Edition, Pearson, Hoboken (NJ), 2020.

Salardi, S., Saporiti, M., *Perché l'IA non deve diventare Persona. Una Critica all'ineluttabile 'Divenire antropomorfico' delle Macchine*, in Id., *Le tecnologie 'morali' emergenti e le sfide etico-giuridiche delle nuove soggettività*, Giappichelli, Torino, 2020, pp. 52-74.

Salardi, S., *Test genetici tra determinismo e libertà*, Giappichelli, Torino, 2010.

Ead., *Robótica e inteligencia artificial: retos para el Derecho*, in «Derechos y libertades», 42, 2020, pp. 203-232.

Ead., *When the 'Age of Science and Technology' meets the 'Age of Rights'. 'Moral' Bioenhancement as a Case Study*, in A. D'Aloia, M.C. Errigo (eds.), *Neuroscience*

and Law: Complicated Crossings and New Perspectives, Springer, Cham, 2020, pp. 239-255.

Sansò, P., *Opacità algoritmica e sovranità epistemica nel contesto del capitalismo delle piattaforme*, in «I-Lex», 2, 2025, pp. 36-49.

Saporiti, M., *Questioni di "intelligenza politica". Prospettive europee in materia di Intelligenza Artificiale e di proceduralità algoritmica*, in «Notizie di Politeia», 143, 2021, pp. 87-103.

Saraceni, G., *Digital divide and fundamental rights*, in «Humanities and Rights Global Network Journal», 1, 2020, pp. 66-91.

Sarra, C., *Dignità umana nell'era dell'intelligenza artificiale e della datificazione*, Kront, Roma, 2025.

Sartor, G., Omicini, A., *The Autonomy of Technological Systems and Responsibilities for their Use*, in N. Bhuta, S. Beck, R. Geiss, C. Kress, H.Y. Liu (eds.), *Autonomous Weapons Systems: Law, Ethics, Policy*, Cambridge University Press, Cambridge, 2016, pp. 39-74.

Sartor, G., *Le applicazioni giuridiche dell'intelligenza artificiale. La rappresentazione della conoscenza*, Giuffrè, Milano, 1990.

Id., *Intelligenza artificiale e diritto. Un'introduzione*, Giuffrè, Milano, 1996.

Id., *Gli agenti software e la disciplina giuridica degli strumenti cognitivi*, in «Il diritto dell'informazione e dell'informatica», 1, 2003, pp. 57-87.

Id., *L'informatica giuridica e le tecnologie dell'informazione. Corso d'informatica giuridica*, Giappichelli, Torino, 2016.

Id., *Introduzione al focus su "L'intelligenza artificiale e il diritto"*, in «Rivista di filosofia del diritto», 1, 2020, pp. 65-72.

Sartori, L., *Il divario digitale. Internet e le nuove disuguaglianze sociali*, Il Mulino, Bologna, 2006.

Savarese, P., *Dalla bugia alla menzogna: la posterità e l'impossibilità del diritto*, in «Nomos», 2, 2018, <https://www.nomos-leattualitaneldiritto.it/nomos/paolo-savarese-postverita-e-impossibilita-del-diritto/>).

Schiavello, A., *Vulnerabilità, concetto di diritto e approccio clinico-legale*, in «Etica & Politica», 3, 2019, pp. 255-277.

Id., *Postdiritto: una breve guida per i perplessi*, in «Rivista di filosofia del diritto», 2, 2023, pp. 261-280.

Schuilenburg, M., Peeters P. (eds.), *The Algorithmic Society*. *Technology, Power and Knowledge*, London, 2021.

Schwartz, W.B., Patil, R.S., Szolovits, P, *Artificial Intelligence in Medicine. Where Do We Stand?*, in «The New England Journal of Medicine», 316, 1987, pp. 685-688.

Schwartz, W.B., *Medicine and the computer: the promise and problem of change*, in «The New England Journal of Medicine», 283, 1970, pp. 1257-1264.

Scoglio, S., *Privacy: diritto, filosofia, storia*, Editori Riuniti, Roma, 1994.

Serra, T., *L'uomo programmato*, Giappichelli, Torino, 2003.

Ead., *Vulnerabilità ed etica della cura*, in A. Di Giandomenico (a cura di), *ETSI DEUS NON DARETUR… Scritti in memoria di Serenella Armellini*, Giappichelli, Torino, 2023, pp. 459-466.

Shortliffe, E.H., Blois, M.S., *The computer meets medicine: Emergence of a discipline*, in E.H. Shortliffe, J.J. Cimino (eds.), *Biomedical Informatics. Computer Applications in Health Care and Biomedicine*, Springer, New York, 4th ed., 2014, pp. 3-45.

Silber, D., *The Case for eHealth*, EIPA, Maastricht, 2003.

Simitis, S., *Crisi dell'informazione giuridica ed elaborazione elettronica dei dati*, tr. it., Giuffrè, Milano, 1977.

Staunton, C., Blom, J.M.C., Mascalzoni, D., on behalf of the IMI FACILITATE Consortium. *Ethical framework for FACILITATE: a foundation for the return of clinical trial data to participants*, in «Frontiers in Medicine», 2024, 11, <https://www.frontiersin.org/journals/medicine/articles/10.3389/fmed.2024.1408600/full>.

Staunton, C., *et al.*, *The return of Individual Participant Data in clinical trial research: a FACILITATE White Paper*, FACILITATE Consortium, 2025.

Szolovits, P., Pauker, S.G., *Computers and clinical decision making: whether, how much, and for whom?*, in «Proceedings of the IEEE», 67, 1979, pp. 1224-1226.

Szolovits, P. (ed.), *Artificial Intelligence in Medicine*, Westview Press, Boulder, 1982.

Taddei Elmi, G., *Informatica giuridica. Presupposti, storia, disciplina, insegnamento, esiti*, in Id. (a cura di), *Informatica giuridica*, Simone, Napoli, 2016.

Taddeo, M., McCutcheon, T., Floridi, L., *Trusting artificial intelligence in cybersecurity is a double-edged sword*, in «Nature Machine intelligence», 2019, 1, pp. 557-60.

Tallacchini, M., *Scienza e diritto. Prospettive di co-produzione*, in «Rivista di Filosofia del diritto», 2, 2012, pp. 316-336.

Thaler, R.H., Sunstein, C.R., *Nudge: Improving Decisions about Health, Wealth, and Happiness*, Yale University Press, New Haven, 2008.

Todaro, G., *L'evoluzione delle fonti del diritto nella «società algoritmica»,* in «Cassazione penale», 64, 4, 2024, pp. 2011-2036.

Tronto, J., *Moral Boundaries. A Political Argument for an Ethic of Care*, Routledge, New York-London, 1993

Turing, A.M., *Computing Machinery and Intelligence*, in «Mind», 4, 1950, pp. 433-460.

Van Dijck, J., *Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology*, in «Surveillance & Society», 12, 2, 2014, pp. 197-208.

van Dijk, D., *The Digital Divide*, Polity Press, Cambridge-Medford, 2020.

Vantin, S., *I divari digitali nell'epoca della rete globale*, in Th. Casadei, S. Pietropaoli (a cura di), *Diritto e tecnologie informatiche*, Wolters Kluwer, Milano, pp. 295-310.

Volpato, A., *Il ruolo delle norme armonizzate nell'attuazione del regolamento sull'intelligenza artificiale*, in «Quaderni AISDUE», 2, 2024, pp 1-18.

Warren, S.D., Brandeis, L.D., *The right to privacy*, in «Harvard Law Review», 1890, 4, pp. 193-220.

Winston, P.H., *Artificial Intelligence*, Addison Wesley, Boston (MA), 1992.
Wooldridge, M, Jennings, N.R, *Intelligent agents: theory and practice*, in «The Knowledge Engineering Review», 10, 2, 1995, pp. 115-152.
World Health Organization, *Recommendations on digital interventions for health system strengthening*, Geneva, 2019.
World Medical Association, *Dichiarazione di Helsinki. Principi etici per la ricerca medica che coinvolge partecipanti umani*, 1964-2024.

Xiao, C., Choi, E., Sun, J., *Opportunities and challenges in developing deep learning models using electronic health records data: a systematic review*, in «Journal of the American Medical Informatics Association», 10, 2018, pp. 1419-1428.
Yeung, K., *'Hypernudge': Big Data as a mode of regulation by design*, in «Information, Communication & Society», 20, 2017, pp. 118-136.
Yu, V.L. *et al.*, *An Evaluation of MYCIN's ADVICE*, in B.G. Buchanan, E.H. Shortliffe (eds.), *Rule-Based Expert Systems: The MYCIN Experiments of the Stanford Heuristic Programming Project*, Addison Wesley, Reading (MA), 1984, pp. 589-596.

Zanetti, G., *Confini e limiti del diritto*, Editoriale Scientifica, Napoli, 2020.
Id., *Filosofia della vulnerabilità. Percezione, discriminazione, diritto*, Carocci, Roma, 2019.
Ziccardi, G., *Diritti digitali. Informatica giuridica per le nuove professioni*, Raffaello Cortina, Milano, 2022.
Zuddas, P., *Covid-19 e* digital divide: *tecnologie digitali e diritti sociali alla prova dell'emergenza sanitaria*, in «Osservatorio costituzionale», 3, 2020, pp. 285-307.
Zullo, S., *La dimensione normativa dei diritti sociali: aspetti filosofico-giuridici*, Giappichelli, Torino, 2012.
Ead., *L'impatto della medicina algoritmica sul* shared decision making, in «Notizie di Politeia», 143, 2021, pp. 151-155.

Collana **Prassi sociale e teoria giuridica**
diretta da *Thomas Casadei* e *Gianfrancesco Zanetti*

1. Serena Vantin, *Gli eguali e i diversi. Diritto,* manners *e ordine politico in Edmund Burke*, 2018
2. Francesco De Vanna, *Il ruolo dei principî nelle teorie neocostituzionaliste. Un percorso interpretativo*, 2019
3. Leonardo Marchettoni, Ius*,* potestas *e* ratio *in Guglielmo di Ockham*, 2019
4. Alessandro Di Rosa, Hate speech *e discriminazione. Un'analisi performativa tra diritti umani e teorie della libertà*, 2020
5. Gianluigi Fioriglio, *Informatica medica e diritto. Un'introduzione*, 2020
6. Francesco De Vanna (a cura di), *Misure di sicurezza e vulnerabilità: la "detenzione" in casa di lavoro*, 2020
7. Nicola Lettieri, *Antigone e gli algoritmi. Appunti per un approccio giusfilosofico*, 2020
8. Carlo Adolfo Porro, Pierluigi Faloni (a cura di), *Emergenza Covid-19: impatto e prospettive*, 2021
9. Annamaria Loche, La liberté ou la mort. *Il progetto politico e giuridico di Olympe de Gouges*, 2021
10. Rosaria Pirosa, *Dal diritto alla salute all'*healthism*. Una ricognizione giusfilosofica*, 2021
11. Barbara Giovanna Bello, *Verso una* Critical Youth Theory. *Giovani, diritto e pratiche sociali*, 2021
12. Mattia Volpi, *Il suddito democratico*. *Libertà e uguaglianza nel pensiero giuridico-politico di Tocqueville*, 2021
13. Charles Péguy, *La crisi dell'insegnamento e il diritto all'istruzione. Tre saggi*, a cura di Vincenzo Pacillo, 2022
14. Giacomo Pisani, *Piattaforme digitali e autodeterminazione. Relazioni sociali, lavoro e diritti al tempo della "governamentalità algoritmica"*, 2023
15. Claudia Atzeni, *Liberalismo autoritario. La crisi dell'Unione europea a partire dalle riflessioni di Hermann Heller*, 2023
16. Giulio Di Donato, *Il pensiero giuridico dei presocratici.* Nómos *e* phýsis, 2024
17. Federico Oliveri, Machina mundi. *Per una regolazione democratica dei poteri digitali*, 2025

18. Vincenzo Rapone, *Sul "diritto sociale", tra fatto e valore. Un percorso tra filosofia, scienze sociali e dimensione normativa*, 2025
19. Barbara G. Bello, Thomas Casadei (a cura di), *"Minori Stranieri Non Accompagnati" ed esercizio dei diritti. Sicurezza, consapevolezza, uso delle tecnologie*, 2025
20. Claudia Severi, *Visioni di giustizia. Clima, cibo, ambienti digitali*, 2025
21. Gianluigi Fioriglio, *Vulnerabilità aumentata, Diritto, cura e algoritmi nell'era della salute digitale*, 2025

Il volume propone un'indagine in chiave giusfilosofica della salute digitale nella cosiddetta "società algoritmica".
Il filo conduttore è quello della "vulnerabilità aumentata", idonea a qualificare la fusione fra immateriale e corporeo: l'esperienza digitale si innerva infatti, inscindibilmente, su quella materiale.
Dopo aver discusso i principali profili giuridici ed etici della salute digitale (dall'intelligenza artificiale alla privacy, dal dataismo alla cibersicurezza), ne vengono analizzate pratiche e applicazioni particolarmente significative (sistemi informativi sanitari, telemedicina e *mobile health*, robotica, medicina personalizzata e di precisione); quindi, anche alla luce del Progetto FACILITATE, viene approfondita la questione della restituzione dei dati ai partecipanti alle sperimentazioni cliniche.

Gianluigi Fioriglio è professore associato di Filosofia del Diritto presso il Dip. di Giurisprudenza dell'Università di Modena e Reggio Emilia - Unimore, ove insegna "Informatica giuridica" e "Sociologia del diritto ed elementi di Informatica giuridica" e, presso l'Accademia Militare di Modena, "Filosofia del diritto" e "Sociologia giuridica".
Coordinatore dell'Officina informatica "Diritto Etica e Tecnologie" del CRID - Centro di Ricerca Interdipartimentale su Discriminazioni e vulnerabilità, è componente del Comitato Etico di Ateneo per la Ricerca e WP leader e membro dello Steering Committee del Progetto FACILITATE (<https://facilitate-project.eu/>).
È stato, fra l'altro, *Visiting Scientist* presso il Massachusetts Institute of Technology (Computer Science and Artificial Intelligente Laboratory - Clinical Decision Making Group) e *Max Weber Fellow* presso lo European University Institute.

isbn 9791281716698

€ 18,00 i.c.