

LA PREVENZIONE NELL'ERA DIGITALE: INTELLIGENZA ARTIFICIALE, TELEMEDICINA E LA SICUREZZA DEI DATI DEL PAZIENTE

a cura di Stefano Manzini



QUADERNI DI DIRITTO
DELLE ATTIVITÀ MOTORIE E SPORTIVE

Collana diretta da Carlo Bottari

I volumi della Collana “Quaderni di Diritto delle attività motorie e sportive”

1. Nicola Cavallaro, *La cessione dei diritti economici dei calciatori* (2021)
2. Francesco Pegreffi, Giovanni Paruto (a cura di), *Stili di vita e nuove tecnologie* (2022)
3. Luigi Melica, *Sport e “diritti” in Italia e nel mondo* (2022)
4. Carlo Bottari, Alceste Santuari (a cura di), *Le associazioni sportive dilettantistiche: riforme e profili gestionali* (2022)
5. Francesco Pegreffi (a cura di), *Giulio Faldini pioniere dell'ortopedia moderna tra Italia e Perù* (2022)
6. Giovanni Paruto, Francesco Pegreffi (a cura di), *La telemedicina nell'assistenza terapeutica e in particolare oncologica* (2022)
7. Carlo Bottari (a cura di), *Curare o prendersi cura? Etica ed emergenza pandemica* (2023)
8. Alessandro Bortolotti (a cura di), *Il management sportivo umanistico* (2023)
9. Giovanni Paruto, Daniele Verri (a cura di), *Sport e inclusione nel sitting volley* (2023)
10. Chiara Pazzaglia, Francesco Pegreffi (a cura di), *Mi prendo cura di lei. Contrasto e prevenzione al gioco d'azzardo femminile* (2023)
11. Luca Dimasi, Silvia Marzot (a cura di), *Welfare State: scenari futuri e criticità irrisolte delle politiche sociali e socio-sanitarie in Italia* (2024)
12. Antonio Alfonso Pisani, *Telemedicina: quadro normativo, tutele e diritti, sistema delle responsabilità* (2024)
13. Gary Louis Pietrantonio, *Assetti amministrativi, organizzativi e contabili del calcio professionistico* (2024)
14. Renato Nicolai, Luca Zambelli (a cura di), *La disciplina del Basket tra tutele e mercato* (2025) - Sport: 1 Pallacanestro
15. Federico Laus (a cura di), *La sicurezza alimentare tra procedimento, azioni strategiche e sistema di controlli. Food safety: procedures, strategic actions and control system* (2025)
16. Francesco Pegreffi, Maria Paola Hachfeld (a cura di), *Ci vediamo in campo. Manuale introduttivo al gioco del basket in carrozzina* (2025)
17. Carlo Zoli (a cura di), *Il mondo del tennis tra sport e diritto* (2025) - Sport: 2 Tennis
18. Simone Perillo, Tommaso Di Paolo (a cura di), *Il cavallo atleta: tutele e prospettive* (2025) - Sport: 3 Sport Equestri
19. Luca Zambelli, Angelo Francini (a cura di), *Diritti, gestione e sostenibilità dell'impiantistica sportiva* (2025)

COMITATO SCIENTIFICO

Carlo Bottari
Roberto Cippitani
Paco D'Onofrio

Massimiliano Iovino
Luigi Melica
Alessandro Pajno

Carlo Rasia
Elena Zucconi Galli Fonseca

LA PREVENZIONE NELL'ERA DIGITALE: INTELLIGENZA ARTIFICIALE, TELEMEDICINA E LA SICUREZZA DEI DATI DEL PAZIENTE

a cura di Stefano Manzini

Con contributi di

Carlo Bottari, Davide Carmelo Calderone, Luca Dimasi,
Paco D'Onofrio, Angelo Francini, Lorenzo Gasparini,
Federico Laus, Stefano Manzini, Antonio Alfonso Pisani

Bologna
University Press



Il volume è stato pubblicato con il contributo dell'Alma Mater Studiorum - Università di Bologna e di Cyske: Cybersecurity & Safety, Bologna.

Fondazione Bologna University Press
Via Saragozza 10 – 40123 Bologna
tel. (+39) 051 232 882

www.buponline.com
email: info@buponline.com

© 2025 Bologna University Press

Quest'opera è pubblicata sotto licenza CC-BY 4.0

ISBN: 979-12-5477-649-0
ISBN online: 979-12-5477-650-6
DOI: 10.30682/9791254776346

In copertina: elaborazione grafica da www.dreamstime.com.

Impaginazione: DoppioClickArt (San Lazzaro di Savena - BO)

Prima edizione: settembre 2025

SOMMARIO

Prefazione	7
Carlo Bottari	
Il dato sanitario come elemento fondante dell'intelligenza artificiale al servizio del paziente e della ricerca	9
Paco D'Onofrio	
L'implementazione di soluzioni evolute nell'erogazione dei servizi sanitari tra opportunità di crescita e rafforzamento della cybersicurezza	21
Stefano Manzini	
Come l'intelligenza artificiale impatta nelle soluzioni e integrazioni della telemedicina	29
Antonio Alfonso Pisani	
Approccio al rischio dell'AI Act e rivoluzione del settore delle cure preventive	45
Lorenzo Gasparini	
La complessa normazione della sperimentazione tra dati sanitari, ricerca scientifica e intelligenza artificiale	59
Federico Laus	
Il Nuovo Regolamento europeo sull'intelligenza artificiale: nuove prospettive	69
Luca Dimasi	
Le possibili applicazioni (e benefici) dell'utilizzo dell'IA nel mondo sportivo	81
Davide Carmelo Calderone, Angelo Francini	
Notizie sugli autori	96

PREFAZIONE

Carlo Bottari

Tematica di grande impatto e di cruciale importanza per lo sviluppo del nostro sistema sanitario, quella della raccolta, catalogazione, archiviazione e utilizzazione del dato sanitario mantiene ancora più che mai la sua attualità e necessità di attento e qualificato approfondimento.

La non più rinviabile digitalizzazione dell'organizzazione delle strutture interessate, che gode, fra l'altro, di specifico finanziamento nell'ambito del PNRR, ormai di prossima scadenza, deve tenere conto di tutte le gravose problematiche legate alla tutela della riservatezza.

L'Unione europea, pur attirandosi pesanti e non richieste critiche da parte di autorità extracomunitarie, ha provveduto ad avviare discipline di settore sempre più puntuali che richiedono, peraltro, condivisione e coordinamento tanto a livello europeo quanto, soprattutto, a livello nazionale. Sembra, purtroppo, irrealistico che limitrofe strutture sanitarie all'interno della medesima azienda ospedaliera non riescano a scambiarsi i dati e che ancora oggi occorra adibire personale per il trasferimento "manuale" di predetti dati!

Ma oltre alle precedenti tematiche, che nel presente volume trovano qualificate trattazioni per molti versi originali e propositive, emergono per la loro rilevanza quelle legate alla commercializzazione costituendo il motore principale indispensabile alla utilizzazione delle nuove tecnologie.

L'intelligenza artificiale si alimenta di dati, le nuove applicazioni e i nuovi algoritmi ne richiedono in sempre maggiori quantità: per adesso. Ma il passo è breve per introdurre onerosi e opportuni sistemi di selezione, scorporamento, aggregazione che incideranno certamente sul mercato determinandone la qualità e la domanda.

Come verrà condizionata la sperimentazione medica e bioetica? Quali nuove professionalità, che oggi ancora non conosciamo, emergeranno e diverranno maggiormente attrattive tanto da indirizzare corsi di laurea e formazioni di tipo strettamente tecnico?

Si tratta di interrogativi che, probabilmente, avremmo dovuto porci già anni fa ma siamo ancora in tempo per recuperare.

Con questo innovativo studio si apre un percorso che andrà costantemente alimentato sotto la regia di mani più che esperte con le quali ci onoriamo di collaborare confidando nell'apprezzamento degli addetti ai lavori, di giovani e capaci studiosi, di quanti ritengono che delle nuove tecnologie non si possa farne a meno, in una cornice di attenta e condivisa riflessione.

IL DATO SANITARIO COME ELEMENTO FONDANTE DELL'INTELLIGENZA ARTIFICIALE AL SERVIZIO DEL PAZIENTE E DELLA RICERCA

Paco D'Onofrio

I. BLOCKCHAIN, TELEMEDICINA E GARANZIE COSTITUZIONALI NELLA GESTIONE DEI DATI SANITARI: MODELLI INNOVATIVI E CRITICITÀ GIURIDICHE

L'irruzione della tecnologia blockchain nell'ambito sanitario non costituisce un mero passo avanti sul piano tecnico-informatico, bensì segna un vero spartiacque concettuale ed operativo nella configurazione giuridica della gestione dei dati sanitari e, più in generale, nei modelli di erogazione delle prestazioni assistenziali¹. L'interazione sempre più stretta tra sanità digitale, intelligenza artificiale e architetture distribuite chiama oggi il diritto a confrontarsi con una dimensione inedita, nella quale le tradizionali categorie dogmatiche risultano messe alla prova da esigenze di efficienza, sicurezza e rispetto delle libertà fondamentali². Si assiste così ad una tensione, tanto feconda quanto problematica, fra l'innovazione tecnologica e il presidio dei diritti, fra l'urgenza della semplificazione operativa e la complessità della tutela giuridica, in un equilibrio che, *ictu oculi*, appare ancora instabile. In questo contesto, blockchain e telemedicina si impongono non solo come strumenti tecnici, ma come autentici dispositivi regolativi, capaci di ridefinire le responsabilità giuridiche, le relazioni istituzionali e le forme normative attraverso cui si struttura il governo del dato sanitario³.

La blockchain, nella sua essenza di registro distribuito e immutabile, si configura quale infrastruttura decentralizzata per l'archiviazione e la gestione dell'informazione,

¹ E. CATELANI, *Nuove tecnologie a tutela del diritto della salute: potenzialità e limiti dell'uso della Blockchain*, in *Federalismi.it*, 2022; E. SIGNORINI, F. ZAMBARDINO, *La blockchain e la telemedicina: quali opzioni per la sicurezza e l'integrità dei dati sanitari*, in *Federalismi.it*, 27, 2024, p. 205 ss.

² F. APERIO BELLA, *L'accesso alle tecnologie innovative nel settore salute tra universalità e limiti organizzativi (con una postilla sull'emergenza sanitaria)*, in *Persona e Amministrazione*, 2020, p. 220.

³ G. CHIARINI, *Telemedicina, attenzione ai profili di responsabilità*, 2024, in *www.sanita24.ilsole24ore.com*; M. FACCIOLO, *La responsabilità sanitaria in telemedicina*, 2021, in *Resp. Civ. Prev.*, pp. 740-755.

nella quale ogni nodo della rete detiene copia integrale delle transazioni e partecipa alla loro validazione tramite meccanismi di consenso condiviso. Tale architettura, per sua natura, si oppone strutturalmente ad ogni tentativo di manipolazione arbitraria, garantendo integrità, trasparenza e tracciabilità dell'informazione. Tali caratteristiche assumono un rilievo dirimente nel settore sanitario, connotato da un'elevatissima sensibilità dei dati trattati e da una fitta rete di relazioni tra pazienti, operatori sanitari, enti pubblici e soggetti privati. In siffatto ambito, l'innovazione in parola assurge a strumento fiduciario, in grado di assicurare la verificabilità e la sicurezza degli scambi informativi, nel rispetto del principio di *accountability* che rappresenta uno dei pilastri del trattamento, legittimo, dei dati.

Il connubio tra blockchain e telemedicina produce effetti dirompenti sul piano sistemico, amplificando la portata trasformativa delle tecnologie digitali. La telemedicina, quale forma di assistenza erogata a distanza, si pone al crocevia tra accessibilità, sostenibilità ed innovazione, sfidando i modelli tradizionali di presa in carico del paziente. L'integrazione tra questi strumenti consente la costruzione di un ecosistema sanitario connesso, ove la raccolta, l'elaborazione e la condivisione dei dati diventano processi continui e dinamici, idonei a promuovere una medicina predittiva e personalizzata. In tal modo, si afferma una nuova centralità del paziente, che da oggetto di cura si trasforma in soggetto attivo del proprio percorso terapeutico, secondo una logica che potrebbe dirsi, *rectius*, partecipativa. L'impiego di apparecchi *wearable*, sensori biometrici, piattaforme di telemonitoraggio, intelligenze artificiali clinicamente addestrate e dispositivi ingeribili marca, in questo senso, un punto di svolta nell'architettura della relazione di cura.

In tale quadro, la blockchain assume una funzione strutturante nella protezione dell'informazione, assicurando la tracciabilità delle transazioni, la protezione contro accessi non autorizzati e la possibilità di ricostruzione dell'intera filiera informativa⁴. Il modello peer-to-peer, privo di un'autorità centrale, riduce la vulnerabilità tipica dei sistemi accentrati, notoriamente esposti a cyberattacchi e disservizi. Ogni blocco della catena contiene il riferimento al precedente, in un *continuum* che rende impossibili modifiche retroattive, garantendo un controllo diffuso, secondo una logica di sorveglianza orizzontale. Il dato, così strutturato, assume valore probatorio potenzial-

⁴ F. FAINI, *Blockchain e diritto. La "catena del valore" tra documenti informatici, smart contracts e data protection*, in *Responsabilità civile e previdenza*, 2020, I, pp. 297-316; ID., *Il diritto nella tecnica: tecnologie emergenti e nuove forme di regolazione*, in *federalismi.it*, 2020, XVI, pp. 79-117; ID., *Data society. Governo dei dati e tutela dei diritti nell'era digitale*, Milano, 2019; B. CAPIELLO, G. CARULLO, *Blockchain, Law and Governance*, Cham, 2020; R. BRUSCHI, *Le applicazioni delle nuove tecnologie: criptovalute, blockchain e smart contract*, in *Il Diritto industriale*, 2020, II, pp. 162-164; M. CASTELLANI, P. POMI, C. TIBERTI, A. TURATO, *Blockchain. Guida pratica tecnico giuridica all'uso*, Firenze, 2019; R. BASHIR, *Mastering Blockchain. Distributed ledger technology, decentralization, and smart contracts explained*, Birmingham, 2018; M. FINK, *Blockchains and Data Protection in the European Union*, in *European Data Protection Law Review*, 2018, IV, pp. 17-35.

mente rilevante, in linea con la tendenza giurisprudenziale a valorizzare le tecnologie come strumenti di tracciabilità giuridicamente rilevante.

Tra le applicazioni più promettenti vi è certamente quella relativa alla gestione del consenso informato. In un ecosistema sanitario fondato sulla centralità del dato, è imprescindibile garantire modalità di acquisizione del consenso che siano trasparenti, verificabili e reversibili. La blockchain consente di registrare il consenso dell'interessato in forma immutabile, conferendogli un valore giuridico (quindi, in prospettiva, anche processuale) rafforzato, capace di soddisfare al contempo le esigenze di prova e di autodeterminazione informativa. L'interessato può, in ogni momento, conoscere chi ha avuto accesso ai suoi dati, in quale circostanza e per quali finalità, nel rispetto del principio di trasparenza, che *ex lege* ispira l'intero assetto normativo del GDPR. Si realizza così una sintesi equilibrata fra efficienza e garanzia, fra fluidità operativa e protezione dei diritti.

Tuttavia, una tale applicazione in ambito sanitario solleva interrogativi complessi di compatibilità normativa, specie in relazione ai principi posti dal Regolamento (UE) 2016/679. L'immutabilità del registro, elemento costitutivo della blockchain, mal si concilia con i diritti alla rettifica ed alla cancellazione dei dati personali, previsti *in primis* dagli artt. 16 e 17 del GDPR. Analoga problematicità emerge sul fronte dell'individuazione del titolare del trattamento, reso opaco dalla struttura distribuita del sistema. Ciò impone un ripensamento dell'intero paradigma regolativo, alla luce di una ricostruzione sistematica che, senza abdicare ai principi fondanti dell'ordinamento europeo, sia in grado di integrare le nuove tecnologie nel tessuto giuridico esistente.

Al contempo, l'interazione tra blockchain, intelligenza artificiale e telemedicina impone una riflessione rinnovata sulla responsabilità sanitaria. In un ambiente in cui le decisioni cliniche sono supportate da strumenti algoritmici e l'informazione è condivisa in modalità decentralizzata, occorre ridefinire i confini della colpa medica, degli obblighi informativi e delle garanzie assicurative. L'uso integrato di dati eterogenei – genetici, comportamentali, ambientali – apre scenari diagnostici inediti, ma espone anche a nuove forme di discriminazione, che vanno arginate con strumenti normativi ispirati al principio di precauzione. Non si tratta di erigere nuove barriere, ma di governare la complessità secondo una logica di equilibrio dinamico tra tutela ed innovazione.

In tale orizzonte, il Fascicolo Sanitario Elettronico (FSE) rappresenta il primo banco di prova dell'incontro tra innovazione digitale e garanzie giuridiche⁵. Esso condensa le tensioni tra interoperabilità e sicurezza, tra centralità della persona e uniformità dei protocolli, tra apertura dei dati e riservatezza. L'implementazione della blockchain potrebbe favorire la nascita di un'infrastruttura unitaria, interoperabile e trasparente, in cui le informazioni siano consultabili in tempo reale da soggetti

⁵ M. FARINA, *Blockchain e tutela della salute: verso la riorganizzazione dei sistemi sanitari?* in *Federalismi.it*, 2020, p. 173.

autorizzati, nel rispetto del principio di minimizzazione e con idonei meccanismi di controllo da parte dell'interessato. Si tratta di un'evoluzione non solo tecnologica, ma eminentemente giuridica, che richiama l'esigenza di un governo pubblico della trasformazione digitale.

Non va sottaciuto, peraltro, che l'adozione di soluzioni come la telemedicina e, ancor più, della blockchain, implica un radicale mutamento culturale e organizzativo. La *digital literacy*, vale a dire la competenza digitale degli utenti, si configura come prerequisito indefettibile per un accesso equo e consapevole alle cure. Occorre, *in re ipsa*, accompagnare tale transizione con percorsi formativi rivolti tanto ai cittadini quanto agli operatori sanitari, chiamati ad acquisire nuove abilità tecniche, deontologiche e giuridiche. L'assenza di tali strumenti rischierebbe di generare nuove forme di esclusione e disuguaglianza, in contraddizione con il mandato inclusivo proprio della sanità pubblica.

Un segnale in tale direzione proviene dal legislatore nazionale, che con la legge n. 33/2023 e il d.lgs. n. 29/2024 ha inteso rafforzare il ruolo della telemedicina e dell'assistenza digitale domiciliare, anche mediante il sostegno offerto dal Piano Nazionale di Ripresa e Resilienza (PNRR). In particolare, è stato previsto che l'accesso ai servizi digitali avvenga previa valutazione dell'eleggibilità clinica, tecnologica e sociale dell'assistito, secondo criteri fissati da AGENAS. Si tratta di un primo tentativo, certo ancora perfettibile, di coniugare l'innovazione tecnologica con l'imperativo costituzionale dell'uguaglianza sostanziale.

Non meno rilevante è il contributo che la blockchain può offrire sul versante della tracciabilità dei farmaci e del contrasto alle frodi assicurative. La possibilità di attestare l'autenticità, la provenienza e la correttezza prescrittiva dei medicinali consente, *a fortiori*, di tutelare il paziente e razionalizzare la spesa sanitaria. L'utilizzo di *smart contracts* e algoritmi predittivi può semplificare la gestione dei sinistri e dei rimborsi, a condizione che vengano predisposti presidi efficaci di trasparenza, controllo e attribuzione della responsabilità⁶.

In definitiva, il nesso tra blockchain, telemedicina e trattamento dei dati sanitari interpella il diritto nella sua capacità di governare la modernità. Da un lato, s'impone la necessità di predisporre regole chiare e coerenti, che prevengano abusi e rafforzino la fiducia dei cittadini; dall'altro, si apre la possibilità di utilizzare le tecnologie per dare attuazione concreta ai principi costituzionali di solidarietà, efficienza e inclusione. *Tertium non datur*: il diritto, in una prospettiva normativa fluida deve porsi come garante dell'innovazione, o finirà fatalmente per esserne un ostacolo, potendo contribuire a costruire un sistema sanitario orientato alla persona e capace di reggere la complessità del tempo presente. La blockchain, in quest'ottica, non è più solo uno strumento tecnico,

⁶ M. GIULIANO, *La blockchain e gli smart contracts nell'innovazione del diritto nel terzo millennio*, in *Dir. Inform.*, 2018, p. 996.

ma diventa lo spazio in cui il diritto è chiamato a reinventare sé stesso, coniugando la dignità della persona e l'efficienza dei processi in un nuovo patto giuridico sulla salute.

2. IL GOVERNO NORMATIVO DEI DATI SANITARI TRA CONSERVAZIONE E SICUREZZA

La gestione e la conservazione dei dati sanitari rappresentano, nell'attuale ecosistema digitale, una delle sfide più complesse e controverse del diritto pubblico dell'innovazione. Essi si collocano al crocevia tra l'istanza di efficienza ed accessibilità dei servizi sanitari, da un lato, e la necessità di salvaguardare la riservatezza, l'integrità e la disponibilità di informazioni ad alta densità sensibile, dall'altro. Il tessuto normativo vigente, nondimeno, appare talvolta inadeguato a sostenere la portata di tale complessità: come ha rilevato una parte della dottrina, permane un *vulnus* regolativo, tanto nell'ordinamento nazionale quanto in quello sovranazionale, che genera effetti distorsivi sulla sicurezza dei dati, sulla loro conservazione prolungata e sul pieno rispetto dei diritti dell'interessato⁷. L'assenza di una cornice normativa organica rischia di compromettere l'attuazione del principio di *accountability*, esponendo il sistema sanitario ad un'instabilità strutturale che, *rebus sic stantibus*, può minare la legittimazione stessa del processo di digitalizzazione.

I dati sanitari, come noto, rientrano tra le informazioni qualificabili *ex lege* come “*particolari*”, ai sensi dell'art. 9 del Regolamento (UE) 2016/679 (GDPR), e la loro gestione impone l'adozione di tutele rafforzate in ogni fase del trattamento. La definizione offerta dall'art. 4, par. 15, del medesimo Regolamento, che include qualsiasi informazione relativa alla salute fisica o mentale della persona, estende l'oggetto della protezione ben oltre i dati clinici in senso stretto, includendo anche elementi potenzialmente idonei a rivelare indirettamente lo stato di salute. In un contesto in cui la medicina evolve verso modelli predittivi e personalizzati, e in cui le distinzioni tra dato, informazione e conoscenza tendono a sfumare, diventa dirimente assicurare che le modalità di conservazione siano non solo conformi alle più aggiornate tecnologie, ma anche rispondenti ai principi generali dell'ordinamento, primi fra tutti quelli di liceità, minimizzazione, integrità e correttezza⁸.

Una delle criticità maggiormente evidenziate in sede scientifica riguarda l'assenza di criteri chiari ed uniformi per la conservazione a lungo termine dei dati digitali in ambito sanitario. Tale carenza finisce con l'indebolire il valore giuridico delle in-

⁷ E. SORRENTINO, *Gestione e conservazione dei dati sanitari. Il vulnus normativo che impatta su sicurezza e data protection*, in *Federalismi.it*, 29, 2024, p. 137 ss.

⁸ F. DI CIOMMO, *Il trattamento dei dati sanitari tra interessi individuali e collettivi*, in *Danno e resp.*, 2002, 2, 121; S. MELCHIONNA, F. CECAMORE, *Le nuove frontiere della sanità e della ricerca scientifica*, in R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 679/2016 e al d.lgs. 101/2018*, Giuffrè, Milano, 2019, p. 585 e ss.

formazioni e con il compromettere la qualità del percorso assistenziale. Il Fascicolo Sanitario Elettronico (FSE), che dovrebbe costituire il cardine del sistema, appare ancora oggi afflitto da disomogeneità regionali, difficoltà di interoperabilità e carenze nell'indicizzazione univoca dei documenti. Nonostante l'apparato normativo di riferimento, costruito a partire dal d.l. n. 179/2012 e rafforzato dal d.p.c.m. n. 178/2015 e le spinte provenienti dal PNRR, l'implementazione concreta del FSE presenta criticità tali da ostacolare la trasformazione del dato in conoscenza clinicamente utile. Di conseguenza, il diritto del paziente a una cura informata, tempestiva ed efficace rischia di rimanere inattuato.

La mancata definizione di standard condivisi si pone altresì in contrasto con quanto prescritto dall'art. 44, comma 1-*ter*, del Codice dell'Amministrazione Digitale (d.lgs. n. 82/2005), che impone ai sistemi di conservazione dei documenti informatici il rispetto di requisiti di autenticità, leggibilità e affidabilità. Tradurre questi parametri nella realtà del dato sanitario implica un profondo ripensamento delle architetture informative, nonché un investimento strategico nelle competenze archivistiche e nei modelli organizzativi. In assenza di tali condizioni, il rischio è quello di generare una documentazione clinica fragile, esposta a fenomeni di obsolescenza, disallineamento semantico e compromissione del valore medico-legale.

A rendere ancora più articolato il quadro, si aggiunge la problematica dell'uso secondario dei dati sanitari, vale a dire il loro trattamento per finalità ulteriori rispetto a quelle originarie. Tra le più ricorrenti vi sono la ricerca biomedica, la programmazione sanitaria, le statistiche pubbliche, fino alla messa a punto di modelli predittivi. Tuttavia, l'ampiezza degli interessi pubblici in gioco non può legittimare deroghe indiscriminate ai diritti dell'interessato: si impone *ex necessitate* un bilanciamento ponderato tra la valorizzazione del patrimonio informativo e la protezione della sfera personale. Il Regolamento europeo sullo Spazio dei Dati Sanitari (EHDS) tenta di individuare una sintesi, prevedendo il riutilizzo di dati anonimizzati o pseudonimizzati, pur restando pendenti numerose criticità, in particolare sul fronte della trasparenza, del consenso e della valutazione d'impatto. Il parere congiunto dell'EDPB e del GEPD ha opportunamente richiamato la necessità di salvaguardare l'equilibrio fra finalità collettive e diritti individuali, ribadendo che l'innovazione normativa non può prescindere dal rigoroso rispetto del GDPR.

Un passaggio fondamentale verso un sistema più coerente è rappresentato dall'applicazione dei principi FAIR (*Findable, Accessible, Interoperable, Reusable*), già noti nel campo della ricerca scientifica. Questi principi mirano a strutturare il dato in modo che esso sia realmente fruibile, condivisibile e riutilizzabile, anche in contesti eterogenei. Tuttavia, *non omittendum*, la loro trasposizione nel settore sanitario richiede un'opera di adattamento profondo, che tenga conto della natura particolare del dato clinico e dei rischi di re-identificazione. Occorre quindi integrare i principi FAIR con una cornice normativa ispirata alla precauzione, ancorata ai valori costituzionali di dignità e autodeterminazione.

Il Garante per la protezione dei dati personali, nel valutare l'impianto normativo dell'Ecosistema Dati Sanitari (EDS), ha formulato osservazioni puntuali e severe, evidenziando profili di carenza sostanziale e procedurale. In particolare, l'Autorità ha sottolineato il pericolo di una concentrazione eccessiva delle informazioni cliniche, con il rischio di accessi impropri, utilizzi distorti e perdita del controllo da parte del titolare del dato. La duplicazione dei dati già presenti nel FSE, in assenza di una base giuridica chiara e di una valutazione d'impatto *ex art. 35 GDPR*, rafforza le perplessità circa la legittimità dell'intervento. Il Garante, tuttavia, non assume una posizione di "opposizione tecnologica", bensì svolge un ruolo di presidio critico, volto a garantire che l'innovazione si sviluppi nel rispetto dell'architettura dei diritti.

In un simile contesto, il principio di *privacy by design and by default*, previsto all'art. 25 GDPR, si conferma come uno strumento imprescindibile⁹. Esso impone che ogni progetto informatico incorpori *ab origine* le garanzie necessarie alla protezione del dato. Nella pratica della sanità digitale, ciò significa disegnare sistemi che proteggano automaticamente l'informazione sensibile, anche a costo di sacrificare, in via temporanea, alcuni margini di efficienza. La sostenibilità giuridica del sistema non può essere disgiunta dalla sua legittimità democratica: una sanità digitale priva di presidi normativi efficaci tradirebbe il patto fiduciario che deve legare cittadino ed istituzioni.

Non si tratta, pertanto, di una questione meramente tecnica. La riflessione giuridica è chiamata a compiere un salto di scala, elaborando una teoria costituzionale dell'informazione sanitaria, che ne riconosca la natura non neutrale. Il dato clinico, in quanto riflesso della persona, ha una valenza ontologica e simbolica ulteriore: custodirlo significa proteggere la memoria biografica, l'identità e la dignità del soggetto. In questa prospettiva, il legislatore non può limitarsi a regolare procedure, ma deve farsi promotore di una cultura pubblica della protezione dei dati, ispirata all'etica della cura ed alla responsabilità collettiva.

Il prefato argomento merita, infine, una puntualizzazione terminologica tutt'altro che irrilevante: la distinzione tra *data retention* e *data preservation*, spesso utilizzate in modo intercambiabile, in realtà risponde a logiche giuridiche differenti. La *retention* implica una conservazione a tempo determinato, funzionale alla finalità del trattamento; la *preservation*, invece, mira ad una custodia di lungo periodo, motivata da esigenze di interesse pubblico, quali la continuità terapeutica, la documentazione medico-legale o la ricerca. *In claris non fit interpretatio*: in ambito sanitario la necessità di garantire la permanenza del dato nel tempo deve accompagnarsi a misure di protezione rafforzata, ad una chiara individuazione delle finalità e ad una valutazione rigorosa della proporzionalità degli strumenti adottati.

In conclusione, il tema della conservazione dei dati sanitari rivela tutta la tensione tra diritto e tecnica, tra innovazione e tutela. Il vuoto normativo cui si è fatto

⁹ S. CALZOLAIO, *Privacy by design. Principi, dinamiche, ambizioni del nuovo Reg. UE 2016/679*, in *Federalismi.it*, 24, 2017, pp. 1-21.

riferimento non è solo una lacuna regolativa, ma il sintomo di un'incapacità più profonda di governare il cambiamento secondo principi di razionalità giuridica e rispetto della persona. Superarlo implica un'azione coordinata, multidisciplinare e costituzionalmente orientata, capace di fondare un nuovo modello di *governance* dei dati, rispettoso delle garanzie e aperto all'innovazione. La salute digitale deve diventare lo spazio in cui dignità, trasparenza e cura si saldano in un orizzonte condiviso, senza che tuttavia lo scenario di incertezza porti ad una rigidità burocratizzazione in chiave irragionevolmente prudente, con il rischio che la mancata circolazione dei dati rallenti la ricerca scientifica e vulneri il prezioso sostegno del *machine learning*¹⁰.

3. OLTRE LA PROTEZIONE: DATI SANITARI, MERCATI INFORMATIZIONALI E SFIDE GIURIDICHE DELLA MONETIZZAZIONE

Dunque, nel panorama della società digitale, i dati personali ed in particolar modo quelli sanitari assumono una centralità strategica che travalica la dimensione protettiva per accedere a quella propriamente economica e conoscitiva. Essi si impongono non solo come oggetto di tutela costituzionale, ma altresì come asset informativo capace di alimentare modelli di sviluppo scientifico, progresso biotecnologico ed innovazione terapeutica. La possibilità di impiegare e valorizzare, anche economicamente, tali dati, se adeguatamente anonimizzati, non si presenta più come un tabù etico o giuridico, bensì come un imperativo di sistema, volto a coniugare il progresso della medicina con l'efficienza e l'equità dei servizi sanitari pubblici¹¹. L'impiego di tecnologie emergenti, come l'intelligenza artificiale e il *machine learning*, rappresenta, in tale prospettiva, non un fine, ma un mezzo di razionalizzazione virtuosa, che trova nei dati la linfa vitale della sua operatività.

Il dato sanitario cessa, dunque, di essere concepito esclusivamente quale elemento soggettivamente "intangibile" e si configura piuttosto come risorsa comune, da valo-

¹⁰ F. PIRAINO, *I "diritti dell'interessato" nel Regolamento generale sulla protezione dei dati personali*, in *Giur. it.*, 2019, XII, 2777; R. PANETTA (a cura di), *Circolazione e protezione dei dati personali, tra libertà e regole di mercato. Commentario al Reg. UE n. 2016/679 (GDPR) e al novellato D.lgs. n. 196/2003*, Milano, 2019; F. SENIGAGLIA, *Reg. UE 2016/679 e il diritto all'oblio nella comunicazione telematica. Identità, informazione e trasparenza nell'ordine della dignità personale*, in *Leggi Civ. Comm.*, 2017, p. 1023 ss.; R. TORINO, *Il diritto di opposizione al trattamento dei dati personali e il diritto a non essere sottoposti a decisioni basate su trattamenti automatizzati e alla profilazione nel Regolamento (UE) 2016/679*, in *Cittadinanza eur.*, 2018, p. 45 ss.; P. PERLINGIERI, *Privacy digitale e protezione dei dati personali*, cit., pp. 483-484; ID., *Principio personalista, dignità umana e rapporti civili*, in *Annali della SISDIC*, 2020, p. 1 ss.; E. TOSI (a cura di), *Privacy digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice privacy*, Milano, 2019.

¹¹ L.M. LUCARELLI TONINI, *La monetizzazione dei dati personali: applicazione e rischi relativi al trattamento dei dati inerenti la salute*, in *Dirittifondamentali.it*, n. 2, 2022.

rizzare secondo logiche di utilità collettiva. La sua circolazione in forma anonimizzata, lungi dal porsi in antitesi con la protezione dei diritti fondamentali, appare oggi funzionale alla creazione di una medicina predittiva, personalizzata e proattiva. La cessione regolata e trasparente di tali informazioni, in forma aggregata, contribuisce allo sviluppo di algoritmi diagnostici e modelli decisionali che innalzano il livello qualitativo dell'intervento clinico e favoriscono l'allocazione efficiente delle risorse.

Tale mutamento di paradigma impone, *de iure condendo*, una revisione dell'inquadramento giuridico dei dati sanitari anonimizzati, che non può più essere rigidamente ancorato all'alveo dei diritti soggettivi, ma deve orientarsi verso la sfera degli interessi legittimi. Tale riconfigurazione, lungi dal depotenziare le garanzie dell'individuo, consente un bilanciamento più equilibrato tra tutela personale e finalità di ricerca, rendendo possibile un utilizzo dei dati coerente con i principi di proporzionalità e ragionevolezza. In ciò risiede la premessa per un nuovo patto tra diritto e scienza, capace di sostenere l'innovazione senza arretramenti sul fronte delle garanzie.

La disciplina europea, pur nata all'insegna della protezione individuale, non preclude la valorizzazione dei dati sanitari a fini scientifici e commerciali, purché tale impiego avvenga nel rispetto delle condizioni previste. L'uso secondario dei dati anonimizzati, se diretto a finalità di ricerca, innovazione terapeutica o pianificazione pubblica, è ritenuto compatibile con l'etica medica e con l'impianto regolativo del GDPR. Il requisito dell'anonimizzazione effettiva, in tale ambito, rappresenta condizione dirimente, pena la trasformazione di uno strumento di progresso in un potenziale strumento di sorveglianza.

Le imprese private e le piattaforme tecnologiche non devono, dunque, essere demonizzate, piuttosto riconosciute come attori essenziali di un ecosistema complesso, nel quale pubblico e privato collaborano alla produzione di valore scientifico. Il loro apporto è determinante per integrare, standardizzare e armonizzare dati sanitari provenienti da fonti eterogenee, rendendoli disponibili per l'elaborazione algoritmica e la sperimentazione clinica. È *in re ipsa* che tale cooperazione impone l'adozione di presidi regolatori solidi, che garantiscano trasparenza, *accountability* e tracciabilità dell'intero processo di trattamento.

La disponibilità crescente di dati anonimizzati consente, inoltre, di perseguire obiettivi di sostenibilità economica del sistema sanitario, attraverso una programmazione fondata su evidenze reali ed una gestione oculata delle risorse. La possibilità di anticipare bisogni clinici, evitare sprechi e migliorare l'efficacia degli interventi è strettamente legata alla qualità e quantità dei dati disponibili, ed alla loro corretta utilizzazione. In tal senso, la valorizzazione del dato diventa leva di razionalizzazione e giustizia allocativa.

Secondo le stime più recenti, il mercato dei dati sanitari è destinato a raggiungere valori significativi nei prossimi anni, con un impatto crescente sul PIL delle economie avanzate. In tale contesto, l'Italia, forte di un sistema sanitario universalistico e di

un vasto patrimonio informativo, può aspirare ad un ruolo da protagonista. Per farlo, tuttavia, è necessario uno sforzo di coordinamento istituzionale, capace di promuovere sinergie tra ricerca pubblica e iniziativa privata, nonché di attrarre investimenti eticamente sostenibili in settori strategici della medicina del futuro.

Tale evoluzione richiede, fatalmente un aggiornamento del quadro giuridico, non solo in termini di adeguamento normativo, ma anche sul piano concettuale. Occorre abbandonare l'approccio difensivo, incentrato su logiche meramente limitative, per adottare una visione proattiva che riconosca esplicitamente il valore economico-sociale del dato. In questo contesto, la transizione da una titolarità soggettiva assoluta verso un interesse legittimo a contenuto collettivo si presenta come una soluzione giuridicamente fondata e moralmente doverosa.

L'analisi delle dinamiche di mercato mostra un'espansione costante del settore della sanità digitale, sostenuta da normative europee come l'EHDS e da iniziative nazionali tese ad incentivare la valorizzazione del dato. Questo scenario di grande fermento espone però a rischi tangibili: tra essi, la gestione opaca del consenso, la perdita di controllo da parte dell'interessato, la profilazione algoritmica e l'utilizzo non autorizzato delle informazioni per finalità diverse da quelle originarie. Si tratta di *pericula in mora*, che impongono l'adozione di misure rigorose di vigilanza, informazione e controllo.

Il mercato si articola in filiere complesse: assicurazioni, industria farmaceutica, ricerca clinica e *health tech* rappresentano ambiti ad altissima intensità informativa, e in particolare, il comparto assicurativo evidenzia una crescente domanda di dati per la personalizzazione delle polizze, tramite algoritmi capaci di calcolare il rischio individuale sulla base di parametri biometrici e comportamentali tipizzati¹². Pur se funzionale ad una maggiore equità, tale pratica espone, altresì, ad evidenti rischi di discriminazione sanitaria e selezione avversa, soprattutto nei confronti dei soggetti fragili. Si pone quindi l'esigenza di un presidio regolativo che impedisca derive escludenti e garantisca il rispetto del principio di uguaglianza sostanziale.

Analogamente, il settore farmaceutico e biotecnologico fa sempre più affidamento su database clinici anonimizzati, indispensabili per velocizzare sperimentazioni e approvazioni. La riduzione dei costi e dei tempi di accesso al mercato è, in questo caso, il riflesso di una nuova metodologia, *data-driven* e flessibile. Tuttavia, qualora l'anonimizzazione risulti imperfetta o le finalità dichiarate vengano aggirate, si rischia una sostanziale elusione dei diritti dell'interessato. Il principio di finalità, sancito dal GDPR, deve essere il *punctum pruriens* di ogni valutazione giuridica sull'uso dei dati sanitari in ambito industriale.

L'impiego a fini statistici e scientifici, pur promosso dalle politiche europee, solleva questioni di controllo democratico e trasparenza. La progressiva centralizzazione

¹² E. BATTELLI, *Big data e algoritmi predittivi nel settore assicurativo: vantaggi e rischi*, in *Il Corriere giuridico*, 12, 2019, p. 1517 ss.

dei dati, se non adeguatamente presidiata, può trasformarsi in uno strumento opaco di concentrazione informativa, sottraendo al cittadino il potere effettivo di disporre del proprio patrimonio digitale. Il rischio di una deriva panottica, seppur latente, impone l'adozione di misure di controllo multilivello, ispirate a principi di legalità, proporzionalità e partecipazione informata.

In tale quadro, il diritto è chiamato a svolgere una funzione regolativa di alto profilo, che superi l'ottica emergenziale e si traduca in un disegno normativo compiuto. Il GDPR, pur rappresentando un riferimento imprescindibile, non basta più: occorrono discipline settoriali specifiche, capaci di delineare confini netti tra uso legittimo e abuso, nonché di costruire un nuovo equilibrio tra interesse generale alla salute pubblica e tutela dei diritti individuali. Il rapporto tra pubblico e privato deve essere ridefinito in chiave cooperativa, ma senza rinunciare a un presidio pubblico forte e autorevole.

Un modello virtuoso passa, inevitabilmente, attraverso la responsabilità sociale d'impresa. Le imprese devono farsi carico di un'etica della trasparenza, dell'equità algoritmica e della tracciabilità. Il principio di *accountability*, inteso come dovere di rendicontazione sostanziale, deve diventare l'asse portante di ogni intervento normativo e operativo. Strumenti come gli audit indipendenti, le certificazioni di conformità e i codici di condotta assumono, in tale ottica, un ruolo sistemico.

Ultimo, ma non per importanza, è il ruolo della cittadinanza informata. Un'effettiva emancipazione digitale richiede campagne educative, strumenti semplici di gestione del consenso e una nuova cultura della protezione dei dati¹³. Il cittadino deve poter esercitare una signoria informativa effettiva, consapevole e non subordinata a meri formalismi.

In conclusione, il mercato dei dati sanitari costituisce una delle prove più complesse del diritto contemporaneo. Il compito dell'interprete è quello di costruire, passo dopo passo, un ordinamento capace di integrare innovazione e diritti, efficienza e dignità, progresso tecnologico e solidarietà. Solo attraverso una rinnovata architettura regolativa, radicata nella Costituzione ma contemporaneamente aperta al futuro, sarà possibile trasformare il dato sanitario in uno spazio di libertà, conoscenza e giustizia condivisa.

¹³ C. IRTI, *Consenso negoziato e circolazione dei dati personali*, Torino, Giappichelli, 2021, pp. 50-56.

**L'IMPLEMENTAZIONE DI SOLUZIONI EVOLUTE NELL'EROGAZIONE
DEI SERVIZI SANITARI TRA OPPORTUNITÀ DI CRESCITA
E RAFFORZAMENTO DELLA CYBERSICUREZZA**

Stefano Manzini

I. INTRODUZIONE

Lo sviluppo e l'implementazione di soluzioni tecnologiche evolute (con particolare riferimento alla telemedicina e all'intelligenza artificiale) nell'erogazione delle prestazioni di assistenza e cura, da parte di strutture sanitarie pubbliche e private, rappresenta oggi un aspetto importante per l'efficientamento delle risorse e la ricerca di una sempre maggiore qualità e innovazione dei servizi. L'integrazione di tali elementi di modernizzazione nell'erogazione delle prestazioni è sostenuta sotto il profilo economico dal Piano Nazionale di Ripresa e Resilienza, la cui Missione 6 mette a disposizione ingenti risorse da investire per il rafforzamento, la digitalizzazione e l'ammodernamento del Sistema Sanitario¹.

Se è vero che l'adozione di tali strumenti e modalità di prestazione delle attività tecnologicamente avanzate appare sempre più urgente, è altresì chiaro che il percorso di implementazione non può prescindere dalla considerazione dei rischi informatici e delle eventuali carenze di sicurezza per quanto concerne sistemi, applicazioni e dispositivi utilizzati dalle strutture sanitarie, tenuto conto che, in questo contesto, le esigenze di protezione dei dati trattati si fanno più pressanti.

L'impulso a valutare la sicurezza dei sistemi informatici e di rete proviene, oltre che dall'incidenza degli attacchi informatici sul settore sanitario, anche, sotto il profilo normativo, dall'entrata in vigore della Direttiva NIS2 (*Network and Information Security*), nel dicembre del 2022, e dal percorso di attuazione della stessa gradualmente sviluppatosi a partire dal settembre 2024, con l'entrata in vigore del Decreto di recepimento interno della disciplina europea. In tal senso, l'adeguamento (seppure obbligato) alle disposizioni normative rappresenta nondimeno, per gli at-

¹ La Componente 1 ha ad oggetto "Reti di prossimità, strutture e telemedicina per l'assistenza sanitaria territoriale", mentre la Componente 2 attiene all'"Innovazione, ricerca e digitalizzazione del Servizio Sanitario".

tori dell'ambito sanitario, un'opportunità per acquisire consapevolezza e prendere in seria considerazione anche il profilo della sicurezza degli asset e delle risorse, al fine di approntare una solida tutela dei dati.

2. LO SCENARIO NAZIONALE ED EUROPEO IN MATERIA DI *CYBER ATTACKS*

La spinta ad investire risorse nella sicurezza informatica proviene in primo luogo da un'evidenza materiale: le strutture sanitarie, e in particolare quelle ospedaliere, rappresentano uno dei bersagli più esposti agli attaccanti, come dimostrato da diversi report sul tema². È evidente che il settore esercita una particolare attrattiva, stante il carattere sensibile dei dati che vengono trattati nell'esercizio delle attività di cura e assistenza.

Il primo studio condotto da ENISA (*European Union Agency for Cybersecurity*) sullo "stato di salute" del settore sanitario in riferimento alle minacce informatiche, risalente al luglio del 2023, faceva emergere una situazione piuttosto allarmante; tale esito derivava dall'analisi ed elaborazione dei dati relativi agli incidenti occorsi nei confronti degli attori del settore *healthcare* nei due anni precedenti la pubblicazione del documento, essendo altresì vero che il periodo di tempo oggetto della disamina comprendeva lo scoppio della pandemia da Covid-19, durante la quale il settore ha rappresentato un obiettivo preferenziale per gli attaccanti³. Un dato interessante si rileva in relazione alla correlazione elevata tra vulnerabilità di *software* e *hardware* e incidenti subiti: in base ai dati in possesso di ENISA, è possibile attribuire a tali vulnerabilità la causa di una larga parte della totalità di incidenti verificatisi⁴. Per quanto riguarda le tipologie maggiormente diffuse di attacco, dalle informazioni raccolte ed elaborate dall'Agenzia europea risultava che gli attacchi *ransomware* (i quali si caratterizzano per l'acquisizione del controllo su asset o dati, con conseguente estorsione di una somma di denaro a danno del soggetto attaccato, al fine di ripristinare la disponibilità o la riservatezza degli stessi⁵) fossero in aumento – un trend confermato sia per l'anno 2022, sia nel corso del 2023⁶. Infatti, non è difficile comprendere come da un attacco della tipologia sopra descritta possa derivare per l'attaccante un ricavo economico molto elevato, se ed in quanto viene messa in pericolo la riservatezza dei

² Il rapporto tra gli incidenti informatici "totali" e quelli che mirano al settore sanitario è preso in considerazione, ad esempio, dai Rapporti del Clusit: il trend risultante dal Rapporto più aggiornato illustra un andamento non lineare, con un picco di attacchi al settore sanitario nel 2023 e una notevole riduzione per il 2024. Si veda inoltre, il *Threat Landscape* pubblicato da ENISA; l'edizione più recente risale al settembre del 2024.

³ European Union Agency for Cybersecurity, *ENISA Threat Landscape: Health Sector*, p. 3.

⁴ *Ibidem*.

⁵ *Ivi*, p. 13.

⁶ *Ibidem*.

dati sanitari⁷. Com'è ovvio, gli asset maggiormente colpiti dagli attacchi sono stati i dati dei pazienti⁸.

Anche i dati relativi agli eventi di cybersicurezza e agli incidenti informatici in ambito sanitario gestiti dal CSIRT Italia, raccolti ed elaborati a partire dall'anno 2023, fino al marzo del 2025, e diffusi dall'Agenzia per la Cybersicurezza Nazionale nello stesso mese, mostrano uno scenario coerente con quanto già illustrato in precedenza da ENISA⁹, pur con le dovute specificazioni e integrazioni, legate al contesto nazionale. A proposito delle tipologie più diffuse di incidenti informatici, si rileva, a livello nazionale e in riferimento al periodo di tempo specificato, una diminuzione nell'incidenza del *ransomware*, e un incremento delle intrusioni tramite l'utilizzo di credenziali valide¹⁰. Dal report dell'Agenzia emerge inoltre con chiarezza che il settore sanitario presenta evidenti lacune sotto il profilo della sicurezza dei sistemi e delle infrastrutture¹¹. Tale postura in materia di cybersicurezza non solo è correlata e contribuisce ad una maggiore probabilità di successo degli attacchi¹², ma espone i dati e le informazioni relativi ai pazienti a seri rischi per la loro riservatezza¹³, senza considerare gli ulteriori effetti in termini di disservizi e di danno all'immagine per la struttura¹⁴. Le c.d. "vulnerabilità esposte" del settore sono state accorpate dall'Agenzia in tre categorie: dispositivi e servizi esposti incautamente; servizi con vulnerabilità o obsoleti; configurazioni errate o non rispettose delle *best practices*¹⁵. Inoltre, l'Agenzia individua, quali *bad practices* caratterizzanti la maggior parte delle strutture sanitarie:

- la gestione decentralizzata di sistemi digitali;
- l'obsolescenza dei dispositivi;
- la carenza di personale dedicato alla cybersicurezza¹⁶.

Pertanto, l'Agenzia consiglia ed esorta l'adozione di misure di sicurezza (ad esempio *patch management*, redazione e implementazione di un *response plan*) al fine di porre rimedio alle insufficienze rilevate¹⁷.

⁷ *Ivi*, p. 10.

⁸ *Ivi*, pp. 24-25.

⁹ Agenzia per la Cybersicurezza Nazionale, *La minaccia cibernetica al settore sanitario. Analisi e raccomandazioni*, p. 5.

¹⁰ *Ivi*, p. 12.

¹¹ Vedasi in particolare il cap. 2 (pp. 18-20) del documento *La minaccia cibernetica al settore sanitario. Analisi e raccomandazioni*.

¹² Agenzia per la Cybersicurezza Nazionale, *La minaccia cibernetica al settore sanitario. Analisi e raccomandazioni*, p. 5.

¹³ *Ivi*, p. 18.

¹⁴ *Ivi*, p. 12.

¹⁵ *Ivi*, p. 19.

¹⁶ *Ivi*, pp. 21-22.

¹⁷ *Ivi*, p. 25.

3. L'ADEMPIMENTO AGLI OBBLIGHI DELLA DIRETTIVA NIS2

Le strutture sanitarie sono pertanto chiamate ad adottare misure di natura tecnica e organizzativa, volte a potenziare la cybersicurezza dei sistemi informatici e di rete, non solo al fine di eliminare o quantomeno limitare le *chances* di attacco, ma anche per attenersi a quanto disposto dalla Direttiva (UE) 2022/2555, ossia la già citata Direttiva NIS2, il cui scopo è la definizione di un livello comune europeo di cybersicurezza: gli Stati membri sono chiamati a definire strategie nazionali di rafforzamento della sicurezza informatica nazionale e di incremento della cyber-resilienza dei soggetti che operano nei settori individuati come strategici per le attività sociali ed economiche degli Stati stessi.

La Direttiva NIS2, oltre a responsabilizzare la *governance* delle organizzazioni che rientrano nel suo perimetro applicativo¹⁸, prevede l'adempimento da parte delle medesime di una serie piuttosto nutrita di obblighi, tra cui la notifica obbligatoria di un incidente significativo¹⁹ e l'adozione e attuazione di misure di sicurezza adeguate e proporzionate utili a gestire e mitigare il rischio informatico, sulla base di un approccio multi-rischio²⁰. Le misure appena menzionate devono almeno riguardare gli elementi elencati nell'art. 21, par. 2, lett. da a) a j)²¹, i quali sono stati ulteriormente declinati, per le organizzazioni nazionali, in "misure" e "requisiti" dalla Determina-

¹⁸ Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recante modifica del Regolamento (UE) n. 910/2014 e della Direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148, art. 20, rubricato "Governance".

¹⁹ *Ivi*, art. 23, "Obblighi di segnalazione"; art. 25, "Obblighi in materia di notifica di incidente", d.lgs. 4 settembre 2024, n. 138. L'art. 30 della Direttiva NIS2 e l'art. 26 del medesimo Decreto, entrambi rubricati "Notifica volontaria di informazioni pertinenti", riguardano le notifiche volontarie di informazioni, relative a quasi-incidenti e a minacce informatiche.

²⁰ Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022, art. 21, "Misure di gestione dei rischi di cybersicurezza", parr. 1-2.

²¹ In particolare, tali elementi sono:

- a) politiche di analisi dei rischi e di sicurezza dei sistemi informatici;
- b) gestione degli incidenti;
- c) continuità operativa, come la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi;
- d) sicurezza della catena di approvvigionamento, compresi aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi;
- e) sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità;
- f) strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cybersicurezza;
- g) pratiche di igiene informatica di base e formazione in materia di cybersicurezza;
- h) politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura;
- i) sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli attivi;

zione n. 164179/2025, datata 14 aprile 2025, dell'Agenzia per la Cybersicurezza Nazionale.

Il recepimento interno della menzionata normativa è avvenuto ad opera del d.lgs. 4 settembre 2024, n. 138, il quale, per il settore sanitario, dispone che:

- esso è compreso tra i “settori ad alta criticità” di cui all'Allegato I (punto 5) al Decreto; più precisamente, vi rientrano:
 - i prestatori di assistenza sanitaria quali definiti dall'art. 3, lett. g), della Direttiva 2011/24/UE del Parlamento europeo e del Consiglio²²;
 - i laboratori di riferimento dell'UE quali definiti all'art. 15 del Regolamento (UE) 2022/2371 del Parlamento europeo e del Consiglio²³;
 - i soggetti che svolgono attività di ricerca e sviluppo relative ai medicinali quali definiti dall'art. 1, punto 2), della Direttiva 2001/83/CE del Parlamento europeo e del Consiglio²⁴;

j) uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, se del caso.

Essi sono riportati pressoché identici nell'art. 24, “Obblighi in materia di misure di gestione dei rischi per la sicurezza informatica”, comma 2, lett. da a) a l), d.lgs. 4 settembre 2024, n. 138.

²² Direttiva 2011/24/UE del Parlamento europeo e del Consiglio del 9 marzo 2011 concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera. Ai sensi della lettera g) dell'art. 3, “prestatore di assistenza sanitaria” è “una qualsiasi persona fisica o giuridica o qualsiasi altra entità che presti legalmente assistenza sanitaria nel territorio di uno Stato membro”.

²³ Regolamento (UE) 2022/2371 del Parlamento europeo e del Consiglio del 23 novembre 2022 relativo alle gravi minacce per la salute a carattere transfrontaliero e che abroga la decisione n. 1082/2013/UE, art. 15, “Laboratori di riferimento dell'UE”:

“1. Nel settore della sanità pubblica o in settori specifici della sanità pubblica rilevanti per l'attuazione del presente regolamento o dei piani nazionali di prevenzione, di preparazione e di risposta, la Commissione può designare mediante atti di esecuzione laboratori di riferimento dell'UE per fornire sostegno ai laboratori nazionali di riferimento al fine di promuovere le buone pratiche e l'allineamento da parte degli Stati membri su base volontaria in materia di diagnosi, metodi di prova, uso di determinati test per la sorveglianza, la notifica e la segnalazione uniforme delle malattie da parte degli Stati membri.

Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'art. 29, par. 2.

2. I laboratori di riferimento dell'UE sono responsabili di coordinare la rete di laboratori nazionali di riferimento, in particolare nei settori seguenti:

- a) diagnostica di riferimento, compresi i protocolli di prova;
- b) risorse materiali di riferimento;
- c) valutazioni esterne della qualità;
- d) consulenza scientifica e assistenza tecnica;
- e) cooperazione e ricerca;
- f) monitoraggio, notifiche degli allarmi e sostegno alla risposta ai focolai, comprese le malattie trasmissibili emergenti e i batteri e virus patogeni; e
- g) formazione. [...]”.

²⁴ Direttiva 2001/83/CE del Parlamento europeo e del Consiglio del 6 novembre 2001 recante un codice comunitario relativo ai medicinali per uso umano. Ai sensi dell'art. 1, numero 2), un medicinale

- i soggetti che fabbricano prodotti farmaceutici di base e preparati farmaceutici di cui alla sezione C, divisione 21, della NACE Rev. 2²⁵;
- i soggetti che fabbricano dispositivi medici considerati critici durante un'emergenza di sanità pubblica (elenco dei dispositivi critici per l'emergenza di sanità pubblica) di cui all'art. 22 del Regolamento (UE) 2022/123 del Parlamento europeo e del Consiglio²⁶.
- le Aziende Sanitarie Locali rientrano nel perimetro applicativo della normativa²⁷.

In aggiunta a quanto detto, un altro aspetto da considerare nella valutazione e nella gestione del rischio è la sicurezza della *supply chain*. Occorre infatti sottolineare che le eventuali vulnerabilità presenti in capo ai fornitori si possono riverberare sull'erogazione dei servizi da parte degli attori del settore *healthcare*; si ritiene che lo sfruttamento di tali vulnerabilità rimarrà un fenomeno piuttosto rilevante anche in futuro²⁸. Peraltro è la stessa Direttiva (e il Decreto legislativo) a richiedere e imporre ai soggetti interessati di adottare le misure di sicurezza della catena di approvvigionamento, valutando debitamente le vulnerabilità dei fornitori e le pratiche di sicurezza da loro adottate²⁹.

4. CONCLUSIONE

Si deve comprendere che lo scenario è in continua evoluzione, come si evince dal Rapporto Clusit sugli incidenti occorsi nel settore a livello globale, aggiornato con i

è “ogni sostanza o composizione presentata come avente proprietà curative o profilattiche delle malattie umane. Ogni sostanza o composizione da somministrare all'uomo allo scopo di stabilire una diagnosi medica o di ripristinare, correggere o modificare funzioni fisiologiche dell'uomo è altresì considerata medicinale”.

²⁵ La divisione 21 della sezione C della NACE Rev. 2 corrisponde a “Manufacture of basic pharmaceutical products and pharmaceutical preparations”.

²⁶ Regolamento (UE) 2022/123 del Parlamento europeo e del Consiglio del 25 gennaio 2022 relativo a un ruolo rafforzato dell'Agenzia europea per i medicinali nella preparazione alle crisi e nella loro gestione in relazione ai medicinali e ai dispositivi medici, art. 22, “Elenco dei dispositivi medici critici e informazioni da fornire”:

“1. Immediatamente dopo il riconoscimento di un'emergenza di sanità pubblica, l'MDSSG consulta il gruppo di lavoro di cui all'art. 21, par. 5. Immediatamente dopo tale consultazione l'MDSSG adotta un elenco delle categorie dei dispositivi medici critici che considera critici nel corso dell'emergenza di sanità pubblica ('elenco dei dispositivi critici per l'emergenza di sanità pubblica') [...]”.

²⁷ D.lgs. 4 settembre 2024, n. 138, “Recepimento della direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del Regolamento (UE) n. 910/2014 e della Direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148”, Allegato III, comma 1, lett. c), n. 4).

²⁸ European Agency for Cybersecurity, *ENISA Threat Landscape: Health Sector*, p. 3.

²⁹ Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022, art. 21, par. 3; d.lgs. 4 settembre 2024, n. 138, art. 24, comma 3.

dati relativi al primo trimestre del 2025: esso evidenzia, per quanto concerne l'anno 2024 e il primo trimestre del 2025, un “rallentamento nell'aumento”³⁰ di incidenti, e illustra un trend di rapida crescita per gli attacchi DDoS (*Distributed Denial of Service*)³¹ e una leggera mitigazione dell'impatto degli attacchi (da *critical* a *high*), probabilmente dovuta proprio agli effetti più contenuti sortiti da tale tipologia di attacco³².

Per concludere, si può affermare che la cybersicurezza rappresenti non soltanto un obiettivo imposto dalla normativa, ma anche e soprattutto un “fattore abilitante fondamentale per molti settori critici, affinché questi possano attuare con successo la trasformazione digitale e cogliere appieno i vantaggi economici, sociali e sostenibili della digitalizzazione”³³: ciò vale tanto più per il settore sanitario, che ricopre un ruolo di assoluta centralità per la società civile.

L'adozione di risorse e strumenti tecnologici più avanzati nel contesto sanitario non può prescindere dalla necessità di garantire la sicurezza dei dati trattati, quale aspetto fondamentale per lo sviluppo e l'implementazione sicuri nell'erogazione delle prestazioni sanitarie; ad un'attenta e rigorosa valutazione dell'organizzazione e dei rischi che si pongono sotto il profilo informatico devono conseguire l'individuazione e l'attuazione delle misure tecniche ed organizzative reputate adeguate e proporzionate, al fine di fronteggiare i rischi informatici, di garantire la continuità nell'erogazione dei servizi e la massima tutela del dato sanitario.

³⁰ Associazione Italiana per la Sicurezza Informatica, *Rapporto Clusit Healthcare Q1 2025*, p. 6.

³¹ *Ivi*, p. 9.

³² *Ivi*, pp. 12-13.

³³ Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022, Considerando 3.

COME L'INTELLIGENZA ARTIFICIALE IMPATTA NELLE SOLUZIONI E INTEGRAZIONI DELLA TELEMEDICINA

Antonio Alfonso Pisani

I. INTRODUZIONE

Negli ultimi anni, la telemedicina ha smesso di essere un'opzione marginale per trasformarsi in un tassello centrale nel panorama della sanità pubblica, soprattutto in risposta alle sfide poste dalla pandemia di Covid-19¹. In Italia, questa trasformazione ha ricevuto una forte spinta dal Piano Nazionale di Ripresa e Resilienza (PNRR)², che ha destinato risorse significative all'innovazione digitale e all'adozione di strumenti tecnologici nella medicina territoriale. In questo scenario in rapido mutamento, l'intelligenza artificiale (IA) si sta ritagliando un ruolo sempre più strategico. Non è solo uno strumento di supporto, ma un vero e proprio motore di cambiamento nell'organizzazione, nell'erogazione e nel monitoraggio delle cure, in particolare nei contesti della medicina a distanza.

Il potenziale dell'IA nella telemedicina risiede nella sua capacità di analizzare grandi volumi di dati clinici, biometrici e comportamentali in tempo reale, fornendo supporto decisionale personalizzato e tempestivo³. Grazie all'uso di modelli predittivi e algoritmi di apprendimento automatico, è oggi possibile identificare precocemente

¹ Ministero della Salute (2022). *Telemedicina: Linee guida nazionali*. Il testo stabilisce i requisiti organizzativi, tecnologici e professionali per l'erogazione sicura ed efficace delle prestazioni sanitarie a distanza, distinguendo tra diverse tipologie (es. televisita, telemonitoraggio, telecooperazione). Viene sottolineato il ruolo delle Regioni nell'attuazione delle Linee guida, oltre all'importanza dell'integrazione dei servizi di telemedicina nel Fascicolo Sanitario Elettronico. Si evidenzia inoltre i punti critici e le sfide applicative, tra cui privacy, consenso informato e interoperabilità dei sistemi. Le Linee guida rappresentano un passo normativo rilevante verso la strutturazione definitiva della telemedicina nel SSN.

² Presidenza del Consiglio dei Ministri (2021), *Piano Nazionale di Ripresa e Resilienza (PNRR)*, Missione 6: Salute.

³ T. DAVENPORT, R. KALAKOTA, *The potential for AI in healthcare*, in *Future Healthcare Journal*, 6(2), 2019, pp. 94-98.

segnali clinici di rischio, ottimizzare i percorsi di cura e ridurre la pressione sulle strutture sanitarie. L'IA può elaborare input provenienti da dispositivi *wearable*, sensori ambientali, cartelle cliniche elettroniche e sistemi di monitoraggio remoto, trasformandoli in informazioni clinicamente rilevanti e fruibili dal personale sanitario. Questo rappresenta un salto qualitativo nella gestione della cronicità, della fragilità e delle fasi post-ospedaliere, aree dove la telemedicina gioca un ruolo chiave.

Nel contesto del Servizio Sanitario Nazionale (SSN), l'integrazione tra intelligenza artificiale e telemedicina sta aprendo nuove frontiere⁴. Le Regioni stanno sperimentando piattaforme digitali che collegano in modo strutturato medici di medicina generale, specialisti e pazienti, alimentate da dati clinici raccolti in continuo. L'obiettivo è duplice: da un lato migliorare l'accessibilità ai servizi, in particolare nelle aree interne o scarsamente servite; dall'altro aumentare l'efficienza del sistema, evitando prestazioni inutili o ripetitive, e favorendo la personalizzazione dei piani terapeutici. In questo contesto, l'IA agisce come una sorta di "filtro intelligente" che permette di cogliere correlazioni complesse tra variabili cliniche, segnali fisiologici e andamenti storici dei pazienti, restituendo un quadro dinamico e proattivo dello stato di salute.

Tuttavia, perché tutto questo sia realmente efficace, serve una base solida: i dati. I dati clinici, quando raccolti in modo strutturato, sicuro e interoperabile, diventano l'elemento abilitante di qualsiasi applicazione di IA in ambito sanitario. La qualità del dato – in termini di accuratezza, completezza, tempestività – determina direttamente l'affidabilità dell'algoritmo che lo utilizza⁵. Ma non si tratta solo di quantità o formato: è fondamentale garantire che i dati siano trattati nel rispetto della privacy del paziente, della trasparenza dei processi decisionali e del diritto all'autodeterminazione, tutti principi che non possono essere sacrificati sull'altare dell'innovazione.

In particolare, nel campo della telemedicina, i dati elaborati dall'IA possono essere integrati nei sistemi di monitoraggio continuo dei pazienti domiciliari. Ciò consente di attivare alert predittivi su anomalie vitali, segnalare automaticamente deterioramenti clinici, proporre aggiustamenti terapeutici in tempo reale o suggerire

⁴ L'Agenzia per l'Italia Digitale (AgID) ha pubblicato delle *Linee Guida per l'adozione dell'intelligenza artificiale (IA) nel sistema sanitario nazionale*. Queste linee guida mirano a garantire un utilizzo responsabile dell'IA, assicurando trasparenza, sicurezza e tutela dei diritti dei pazienti. Un aspetto chiave delle linee guida è la definizione di ruoli e responsabilità, in particolare la collaborazione tra il Responsabile della Protezione dei Dati (DPO) e il Responsabile della Transizione Digitale (RTD). Questa sinergia è fondamentale per garantire che l'adozione dell'IA sia conforme alle normative sulla privacy e sulla protezione dei dati personali. Le linee guida sottolineano l'importanza di una *governance* chiara e di una valutazione d'impatto sulla protezione dei dati (DPIA) prima dell'implementazione di sistemi di IA. Inoltre, promuovono l'adozione di soluzioni tecnologiche che rispettino i principi di *privacy by design* e *by default*, assicurando che la protezione dei dati sia integrata fin dalla progettazione dei sistemi.

⁵ B.D. MITTELSTADT, P. ALLO, M. TADDEO, S. WACHTER, L. FLORIDI, *The ethics of algorithms: Mapping the debate*, in *Big Data & Society*, 2016.

interventi urgenti da parte degli operatori. Alcuni esempi concreti già attivi in Italia includono i sistemi per la gestione remota di pazienti diabetici, ipertesi o affetti da insufficienza cardiaca, in cui l'IA aiuta a interpretare flussi di dati⁶ provenienti da glucometri, holter, bilance intelligenti o saturimetri connessi. Questo approccio permette di superare il modello reattivo della medicina tradizionale, passando a un modello proattivo, in cui la tecnologia anticipa le criticità e indirizza le risorse sanitarie dove sono davvero necessarie.

Questo contributo si propone quindi di approfondire, in modo critico e documentato, il ruolo dell'intelligenza artificiale nelle nuove architetture della telemedicina italiana, analizzandone vantaggi, limiti e prospettive. I principali obiettivi del lavoro sono:

- analizzare come l'IA venga attualmente utilizzata nei servizi di telemedicina del SSN, sia a livello sperimentale sia operativo, mettendo in luce le soluzioni già adottate e le principali aree applicative;
- esaminare il ruolo centrale dei dati nella costruzione di sistemi di IA efficaci e sicuri, con particolare attenzione alla qualità, sicurezza, interoperabilità e protezione della privacy;
- valutare criticamente le implicazioni etiche dell'uso dell'IA in telemedicina, considerando i temi della trasparenza algoritmica, dell'autonomia decisionale del paziente e del possibile rischio di disuguaglianze sanitarie legate all'accesso tecnologico;
- individuare le sfide organizzative e regolatorie che ostacolano una piena adozione dell'IA nella pratica clinica quotidiana, e proporre alcune direzioni strategiche per il futuro.

In definitiva, il lavoro intende offrire una riflessione informata e orientata all'azione sul modo in cui l'intelligenza artificiale, se ben governata, può rafforzare le potenzialità della telemedicina e contribuire a costruire un modello sanitario più equo, sostenibile e centrato sulla persona.

2. CONTESTO ATTUALE DELLA TELEMEDICINA

La telemedicina oggi non è più soltanto un'opzione tecnologica accessoria, ma una componente strutturale di un sistema sanitario in trasformazione. In un contesto segnato da un progressivo invecchiamento della popolazione, da una crescente pressione sulle strutture ospedaliere e da una domanda sempre più orientata alla personalizzazione delle cure, le soluzioni digitali stanno diventando strumenti fondamentali per ripensare la presa in carico del paziente. In Italia, la transizione verso una sanità

⁶ Commissione Europea, *Il libro bianco sull'intelligenza artificiale. Un approccio europeo all'eccellenza e alla fiducia*, 2020.

più connessa e distribuita ha trovato nel digitale un alleato strategico, non solo per superare i vincoli imposti dalle distanze geografiche, ma anche per riorganizzare l'erogazione delle prestazioni sanitarie in modo più proattivo, continuo e integrato. Se la pandemia ha fatto da catalizzatore, il vero cambio di paradigma si gioca ora sulla capacità del sistema sanitario di capitalizzare sull'esperienza acquisita, investendo in infrastrutture, formazione e interoperabilità. La telemedicina non si limita più a colmare assenze o emergenze: entra nel cuore del modello assistenziale, ridisegnando i confini tra ospedale e territorio, tra medico e paziente, tra cura e prevenzione.

Questa trasformazione, tuttavia, non può essere ridotta a una risposta emergenziale. La telemedicina si sta consolidando come una componente strutturale e strategica della sanità del futuro, grazie anche agli investimenti previsti dal Piano Nazionale di Ripresa e Resilienza (PNRR), in particolare nella Missione 6 – Salute, che mira a potenziare la medicina territoriale attraverso l'innovazione digitale⁷.

Alla base della telemedicina vi è un ecosistema di tecnologie integrate che permettono l'erogazione di prestazioni sanitarie a distanza. I principali strumenti comprendono:

- piattaforme digitali per la gestione dei flussi clinici, accessibili via web o applicazioni mobili, che permettono ai medici di monitorare i pazienti, prescrivere terapie e gestire appuntamenti;
- dispositivi *wearable* (indossabili), come *smartwatch*, sensori di glucosio o saturimetri intelligenti, in grado di raccogliere e trasmettere dati biometrici in tempo reale;
- sistemi di videocomunicazione per consulti a distanza, sia tra medici che con i pazienti;
- intelligenza artificiale e *machine learning*, impiegati per l'elaborazione predittiva dei dati clinici, la triage automatizzata o la personalizzazione dei percorsi terapeutici;
- *cloud computing*, per l'archiviazione e la condivisione sicura dei dati sanitari, con elevati standard di protezione e *compliance* normativa (GDPR);
- interfacce interoperabili con i sistemi informativi regionali e nazionali (come il Fascicolo Sanitario Elettronico), fondamentali per garantire continuità assistenziale e accesso ai dati ovunque.

⁷ Uno dei pilastri della Missione 6 del PNRR è Il d.m. 77/2022 (Decreto ministeriale del 23 maggio 2022) che definisce il nuovo modello organizzativo dell'assistenza territoriale in Italia, nell'ambito della riforma del Servizio Sanitario Nazionale. Introduce strutture come le Case della Comunità, gli Ospedali di Comunità e le Centrali Operative Territoriali, con l'obiettivo di potenziare la sanità di prossimità e ridurre il ricorso agli ospedali. Valorizza il ruolo del medico di medicina generale e dell'infermiere di famiglia, promuovendo un approccio multidisciplinare. Stabilisce standard quantitativi e qualitativi per l'erogazione uniforme dei servizi sanitari e mira a garantire continuità assistenziale, presa in carico e maggiore equità territoriale.

L'utilizzo efficace di queste tecnologie richiede una *governance* centralizzata e competenze digitali diffuse tra i professionisti sanitari. Per questo motivo, una parte significativa delle risorse del PNRR è stata destinata a programmi di formazione e aggiornamento.

L'erogazione di servizi di telemedicina in Italia è oggi normata da specifiche Linee guida emanate dal Ministero della Salute nel 2022, che definiscono il quadro giuridico e operativo per l'utilizzo di questi strumenti. Le linee guida chiariscono che la telemedicina non può essere considerata una prestazione "inferiore" rispetto a quelle tradizionali, ma deve essere garantita nel rispetto di standard clinici, etici e tecnici equivalenti.

Tra i requisiti fondamentali vi sono: la validazione scientifica delle tecnologie e dei protocolli utilizzati, sicurezza e protezione dei dati trattati durante l'erogazione dei servizi, il consenso informato esplicito da parte del paziente, la tracciabilità delle attività svolte e l'interoperabilità tra sistemi regionali e nazionali.

Un aspetto importante riguarda la definizione di modelli tariffari adeguati, ancora in fase di elaborazione, per rendere la telemedicina economicamente sostenibile e integrabile nei Livelli Essenziali di Assistenza (LEA).

2.1. La Piattaforma Nazionale di Telemedicina (PNT)

Uno degli interventi più strategici previsti dal PNRR è la creazione della Piattaforma Nazionale di Telemedicina (PNT), che ha l'obiettivo di superare l'attuale frammentazione delle esperienze regionali e garantire un'infrastruttura unificata, sicura e interoperabile su scala nazionale.

La PNT sarà un nodo centrale di coordinamento, in grado di connettere tra loro le piattaforme regionali esistenti, i medici di medicina generale, i medici specialisti e i pazienti, con l'intento di:

- centralizzare i dati clinici e renderli accessibili a tutti gli attori autorizzati;
- offrire servizi di telemedicina standardizzati, come teleconsulto, televisita, telemonitoraggio e telecooperazione;
- implementare moduli di supporto decisionale basati sull'IA;
- garantire la *compliance* normativa (privacy, sicurezza, interoperabilità).

Il coordinamento tecnico della piattaforma è stato affidato ad AGENAS, in sinergia con il Ministero della Salute e con il supporto tecnico di soggetti tecnologici qualificati. Il primo passo per l'attivazione della PNT è stato l'avvio della gara CONSIP per la realizzazione dell'infrastruttura, a cui seguiranno i test di interoperabilità con le singole regioni.

L'implementazione diffusa della telemedicina promette benefici tangibili su più fronti come l'accessibilità, ovvero la possibilità di ricevere assistenza anche in aree remote, montane o carenti di strutture sanitarie fisiche, riducendo le disuguaglianze

territoriali⁸. Di conseguenza, la continuità assistenziale, e quindi il monitoraggio remoto, che consente una presa in carico più proattiva e tempestiva dei pazienti cronici, riducendo il numero di ricoveri ospedalieri evitabili.

Negli ultimi anni si parla anche di *empowerment* del paziente: che può accedere ai propri dati sanitari, ricevere notifiche e *reminder* terapeutici, partecipare attivamente al percorso di cura.

In ultimo, la raccolta dei dati per la ricerca assume un'importanza cruciale. I *big data* prodotti possono alimentare studi epidemiologici, valutazioni di efficacia clinica e modelli predittivi avanzati⁹.

2.2. Sfide e criticità

Nonostante l'evidente potenziale trasformativo della telemedicina, la sua implementazione su larga scala si scontra con una serie di ostacoli strutturali, normativi e culturali che ne limitano la diffusione e l'efficacia all'interno del Servizio Sanitario Nazionale. Una delle problematiche più urgenti riguarda la scarsa interoperabilità tra le diverse piattaforme regionali. La mancanza di standard tecnici comuni e la prevalenza di soluzioni proprietarie rendono difficile l'integrazione dei dati sanitari, compromettendo la continuità assistenziale, specialmente in contesti di mobilità interregionale del paziente.

A ciò si aggiunge una crescente preoccupazione per la sicurezza informatica. L'aumento della digitalizzazione dei servizi sanitari espone le infrastrutture a rischi significativi di cyberattacchi, con possibili compromissioni della privacy dei dati sensibili. In tale contesto, emerge con forza l'esigenza di rafforzare i protocolli di *cybersecurity*, adottando misure tecniche e organizzative adeguate a garantire integrità, disponibilità e riservatezza delle informazioni trattate¹⁰.

Sul piano giuridico e deontologico, persistono incertezze relative alla responsabilità medico-legale nelle prestazioni rese in modalità telematica. L'assenza di una giurisprudenza consolidata, unitamente alla novità dei modelli organizzativi digitali, impone una riflessione accurata circa la definizione delle responsabilità in caso di eventi avversi, errori diagnostici o malfunzionamenti tecnologici.

Dal punto di vista sociale, la questione del *digital divide* rappresenta un ulteriore elemento critico. Ampie fasce della popolazione, in particolare gli anziani o i cittadini con basso livello di istruzione, incontrano ostacoli nell'accesso e nell'uso delle

⁸ Ministero per l'Innovazione tecnologica e la Transizione digitale. Strategia nazionale per la Digitalizzazione della Sanità 2021-2026, Roma, 2021.

⁹ L. CORRADETTI, *La farmacia dei servizi: un presidio sociosanitario di prossimità in divenire*, in *Federalismi.it*, 2024.

¹⁰ R. BRIGHI, *Cybersecurity e intelligenza artificiale. Un'analisi critica*, in *Biolaw Journal*, 2024.

tecnologie digitali, con il rischio di accentuare le disuguaglianze esistenti¹¹. Inoltre, in alcune aree del territorio nazionale, permangono deficit infrastrutturali che limitano l'accesso alla rete, compromettendo l'efficacia delle soluzioni digitali anche nei casi in cui esse sarebbero potenzialmente utili.

Infine, non va sottovalutata una certa resistenza culturale, soprattutto tra gli operatori sanitari, che talvolta percepiscono la tecnologia come un'interferenza nella relazione medico-paziente, o come un fattore di complicazione delle prassi operative consolidate. In parallelo, la mancanza di un quadro tariffario definito e sostenibile limita la possibilità di inserire stabilmente la telemedicina nei Livelli Essenziali di Assistenza, relegandola spesso a progetti sperimentali o a iniziative circoscritte.

Nel delineare le prospettive future della telemedicina in Italia, appare evidente come la sfida principale non sia più di natura tecnologica, bensì organizzativa e sistemica. Le soluzioni digitali oggi disponibili, infatti, sono sufficientemente mature da consentire l'erogazione di servizi efficienti e sicuri. Tuttavia, la piena realizzazione del potenziale della telemedicina richiede un ripensamento complessivo delle logiche di funzionamento del sistema sanitario, fondato su un approccio integrato, coordinato e centrato sul paziente.

In tal senso, la Piattaforma Nazionale di Telemedicina rappresenta un tassello strategico per superare la frammentazione esistente e garantire un'infrastruttura uniforme, interoperabile e conforme agli standard europei in materia di protezione dei dati. L'obiettivo non è solamente tecnico, ma profondamente politico: costruire una sanità digitale accessibile, equa e sostenibile, in cui la telemedicina non sia una soluzione opzionale o residuale, ma parte integrante dei percorsi assistenziali.

L'integrazione dell'intelligenza artificiale e dei *big data* potrà ulteriormente rafforzare l'efficacia della telemedicina, introducendo modelli predittivi e sistemi di supporto decisionale in grado di anticipare le criticità cliniche, personalizzare le terapie e migliorare la qualità complessiva dell'assistenza. Tuttavia, affinché tali innovazioni producano valore reale, sarà indispensabile garantire un impianto etico solido, basato sulla trasparenza algoritmica, sulla protezione della privacy e sul rispetto dell'autonomia del paziente¹².

In conclusione, il successo della telemedicina nel contesto italiano dipenderà dalla capacità di governare in modo intelligente questa transizione, promuovendo una visione olistica della salute digitale che sappia coniugare innovazione tecnologica, sostenibilità organizzativa e inclusione sociale. Il passaggio da sperimentazione a sistema non sarà immediato, ma costituisce una necessità inderogabile per garantire la resilienza e l'equità del SSN nei decenni a venire.

¹¹ L. FLORIDI, *AI4People. An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations*, in *Minds and Machines*, 2018, 28(4), pp. 689-707.

¹² E. SIGNORINI, F. ZAMBARDINO, *La blockchain e la telemedicina: quali opzioni per la sicurezza e l'integrità dei dati sanitari*, in *Federalismi.it*, 2024.

2.3. Protezione dei dati e *governance* della Piattaforma Nazionale di Telemedicina: il parere del Garante

Nel gennaio 2025, il Garante per la protezione dei dati personali ha espresso un parere favorevole – con alcune osservazioni – sullo schema di decreto che disciplina i trattamenti di dati personali nell’ambito della Piattaforma Nazionale di Telemedicina (PNT), in attuazione degli investimenti previsti dal PNRR. Il documento rappresenta un punto di svolta per la regolamentazione dell’ecosistema digitale sanitario italiano, in particolare per quanto riguarda l’interoperabilità tra sistemi regionali, la protezione della privacy e la trasparenza nei processi di trattamento dei dati sanitari. La piattaforma, articolata in un’Infrastruttura Nazionale (INT) e nelle Infrastrutture Regionali di Telemedicina (IRT), si configura come un sistema integrato, finalizzato a supportare la continuità assistenziale attraverso l’erogazione di prestazioni sanitarie in modalità remota¹³.

Secondo quanto definito nello schema di decreto, l’INT ha la funzione di garantire servizi abilitanti alle IRT, fungendo da nodo centrale per l’interoperabilità tra le regioni e per la standardizzazione dei processi. Tuttavia, per quanto riguarda la protezione dei dati personali, è stato chiarito che la INT non effettuerà direttamente trattamenti di dati sanitari individuali. Al contrario, tale responsabilità è attribuita alle IRT, che rappresentano le articolazioni operative della PNT a livello territoriale e che consentono l’effettiva erogazione dei servizi di telemedicina. In tale contesto, la trasparenza e la sicurezza diventano elementi imprescindibili. Il decreto stabilisce infatti che ogni trattamento debba avvenire nel rispetto dei principi di minimizzazione, esattezza, proporzionalità e finalità, in linea con quanto previsto dal Regolamento (UE) 2016/679.

Il Garante ha sottolineato l’importanza dell’informativa all’interessato, che dovrà essere fornita in modo comprensibile, accessibile e omogeneo su tutto il territorio nazionale. È previsto che tale informativa venga integrata con quella già predisposta per il Fascicolo Sanitario Elettronico (FSE) e per l’Ecosistema Dati Sanitari (EDS), assicurando che il cittadino sia adeguatamente informato sui trattamenti effettuati, sulle finalità e sulle modalità di esercizio dei propri diritti. Il decreto include inoltre precise disposizioni sul periodo di conservazione dei dati, stabilendo, ad esempio, che le informazioni relative all’autenticazione e all’accesso ai servizi di telemedicina siano conservate per un massimo di dodici mesi, mentre i dati elaborati per fini di governo debbano essere cancellati entro ventiquattro ore dalla loro estrazione.

Un’ulteriore evoluzione positiva del testo riguarda il superamento della visione della PNT come banca dati a sé stante. In seguito alle osservazioni del Garante, è stato chiarito che i dati prodotti nell’ambito della telemedicina non saranno duplica-

¹³ Garante per la protezione dei dati personali. Parere n. 2 del 16 gennaio 2025 sul trattamento dei dati nella Piattaforma nazionale di telemedicina, 2025

ti nella INT, ma resteranno centralizzati nell'EDS, da cui potranno essere estratti in forma pseudonimizzata per finalità di governo e monitoraggio, nel rispetto delle garanzie previste. Tale approccio evita inutili duplicazioni, riduce i rischi di incoerenze e rafforza il controllo sul ciclo di vita dei dati.

Particolare attenzione è stata infine riservata alla sicurezza. L'allegato tecnico del decreto dettaglia una serie di misure da adottare, tra cui la cifratura dei dati, l'uso di sistemi SIEM per la gestione degli incidenti di sicurezza, l'adozione di strumenti di monitoraggio avanzato e la registrazione dei log di accesso. La distinzione tra le misure applicabili all'INT e quelle per le IRT riflette la diversa natura dei trattamenti effettuati e rappresenta un esempio di approccio proporzionato al rischio, in linea con il principio di *accountability*.

Nel complesso, il parere del Garante contribuisce a rafforzare l'impianto regolatorio della telemedicina in Italia, garantendo che lo sviluppo tecnologico avvenga nel pieno rispetto dei diritti fondamentali delle persone. La PNT si configura così non solo come un'infrastruttura tecnica, ma come un'architettura giuridica e organizzativa pensata per rendere la sanità digitale un ambiente sicuro, trasparente e al servizio del cittadino. L'equilibrio tra innovazione, *governance* e tutela dei dati rappresenta la condizione necessaria per il successo duraturo di qualunque iniziativa di trasformazione digitale in ambito sanitario.

3. TELEMEDICINA AUMENTATA: IL RUOLO REGOLATO DELL'IA NELLE DECISIONI CLINICHE

L'integrazione dell'intelligenza artificiale (IA) nei sistemi di supporto alle decisioni cliniche rappresenta una delle più promettenti applicazioni della trasformazione digitale in sanità. In particolare, nell'ambito della telemedicina, l'IA consente di estrarre valore clinico da enormi quantità di dati sanitari eterogenei, offrendo ai professionisti strumenti capaci di analizzare, prevedere e suggerire decisioni terapeutiche in modo rapido e personalizzato. La crescente disponibilità di dati elettronici (dalle cartelle cliniche digitali ai flussi generati da dispositivi indossabili) ha creato le premesse per l'evoluzione di modelli computazionali avanzati che, grazie a tecniche di *machine learning* e *deep learning*, possono identificare pattern nascosti, produrre valutazioni predittive e supportare diagnosi e monitoraggi remoti¹⁴.

Nel contesto della telemedicina, questi strumenti sono particolarmente rilevanti. Il medico che gestisce a distanza pazienti cronici o fragili può essere supportato da sistemi di IA in grado di suggerire modifiche al piano terapeutico, attivare *alert* intelli-

¹⁴ A.E. Tozzi, *Il connubio tra telemedicina e intelligenza artificiale per un salto di qualità nelle cure*, *Monitor*, 2021, 46, p. 39 ss.

genti in caso di anomalie vitali, o addirittura anticipare eventi critici grazie all'analisi di dati longitudinali. L'intelligenza artificiale non sostituisce il giudizio clinico, ma ne potenzia l'efficacia, offrendo una sorta di "secondo parere computazionale" che riduce l'incertezza e migliora l'accuratezza delle scelte mediche.

L'efficacia di questi sistemi, tuttavia, è direttamente proporzionale alla qualità, accessibilità e interoperabilità dei dati su cui si fondano. In questo senso, la creazione di un ecosistema europeo in grado di armonizzare l'uso dei dati sanitari rappresenta una sfida fondamentale. A tal fine, l'Unione Europea ha presentato il Regolamento sullo Spazio Europeo dei Dati Sanitari (*European Health Data Space*, EHDS), attualmente in fase avanzata di approvazione¹⁵. L'EHDS mira a garantire un accesso sicuro e standardizzato ai dati sanitari dei cittadini europei, favorendo al tempo stesso la ricerca, l'innovazione e lo sviluppo di nuove tecnologie in ambito sanitario, inclusi gli algoritmi di IA¹⁶.

Uno degli elementi distintivi dell'EHDS è il principio della "doppia finalità" del dato: da un lato, i dati vengono raccolti e trattati per finalità primarie legate alla cura del paziente; dall'altro, possono essere riutilizzati – in forma anonimizzata o pseudonimizzata – per scopi secondari, come la ricerca scientifica, la pianificazione sanitaria e la valutazione delle politiche pubbliche. Questo doppio uso, tuttavia, richiede meccanismi stringenti di *governance*, un *framework* giuridico solido e strumenti tecnologici che garantiscano l'anonimato, la sicurezza e la tracciabilità dei flussi informativi. In tale contesto, l'EHDS introduce la figura degli *Health Data Access Bodies*, enti deputati a gestire le richieste di accesso ai dati per uso secondario e a vigilare sul rispetto delle norme in materia di privacy e sicurezza.

In parallelo, l'Europa ha introdotto un ulteriore strumento normativo cruciale: l'*Artificial Intelligence Act*, il primo regolamento orizzontale sull'intelligenza artificiale, che stabilisce una classificazione dei sistemi di IA in base al livello di rischio che essi comportano. I sistemi di IA destinati all'assistenza sanitaria rientrano generalmente nella categoria "ad alto rischio", e come tali devono rispettare requisiti particolarmente stringenti in termini di trasparenza, tracciabilità, robustezza, e supervisione umana. Questo significa che gli algoritmi utilizzati nei sistemi di supporto alle decisioni mediche dovranno essere sottoposti a rigorose procedure di conformità prima di essere immessi sul mercato o adottati nelle strutture sanitarie.

Il regolamento sull'IA impone, tra l'altro, l'obbligo di documentazione tecnica dettagliata, auditabilità dei processi decisionali automatizzati e la possibilità, per l'u-

¹⁵ La proposta sull'*European Health Data Space* (EHDS) è stata presentata dalla Commissione Europea nel maggio 2022. Dopo negoziati tra Parlamento e Consiglio, è stato raggiunto un accordo provvisorio nel marzo 2024 e il testo definitivo è stato approvato da entrambe le istituzioni nella primavera 2025.

¹⁶ E. SORRENTINO, A.F. SPAGNUOLO, *Gestione e conservazione dei dati sanitari. Il vulnus normativo che impatta su sicurezza e data protection*, in *Federalismi.it*, 2024.

tente umano, di comprendere e contestare le decisioni generate dalla macchina. In altre parole, l'approccio europeo si distingue per una forte enfasi su etica, *accountability* e controllo umano, in netta contrapposizione a modelli più permissivi adottati in altri contesti geopolitici. È evidente che l'applicazione di questo regolamento in sanità comporterà costi aggiuntivi in termini di sviluppo e certificazione dei dispositivi IA, ma al tempo stesso rappresenterà una garanzia per la sicurezza dei pazienti e la fiducia degli operatori.

Non meno importante è il quadro normativo che disciplina i dispositivi medici. Con l'entrata in vigore del Regolamento (UE) 2017/745, noto anche come *Medical Device Regulation* (MDR), è stato introdotto un nuovo sistema di classificazione e certificazione che interessa anche i software basati su IA impiegati per finalità diagnostiche o terapeutiche¹⁷. Il regolamento prevede che qualunque software che svolga una funzione medica specifica (per esempio, un algoritmo che suggerisce un trattamento sulla base di dati clinici) sia considerato a tutti gli effetti un dispositivo medico e debba quindi essere certificato da un organismo notificato. I requisiti includono la validazione clinica, la sorveglianza post-commercializzazione e il monitoraggio continuo delle prestazioni.

In tale contesto, l'EMA (Agenzia Europea per i Medicinali) ha recentemente pubblicato delle linee guida volte a facilitare l'integrazione dell'IA nei processi regolatori relativi ai farmaci e ai dispositivi medici. Le linee guida EMA pongono l'accento su aspetti come la trasparenza algoritmica, la gestione del rischio, la robustezza dei dati di addestramento e la necessità di coinvolgere i pazienti e i professionisti sanitari nella progettazione dei sistemi IA. Viene inoltre ribadita la necessità di considerare l'IA come un elemento del ciclo di vita del prodotto, da monitorare e aggiornare nel tempo, specialmente in presenza di sistemi adattivi (che evolvono in funzione dei dati)¹⁸.

L'applicazione dell'IA in telemedicina, alla luce di questo complesso quadro regolatorio, richiede pertanto un approccio multidisciplinare, in cui ingegneri, clinici, esperti legali e responsabili della protezione dei dati collaborino fin dalle fasi iniziali del processo di sviluppo. La sola validazione tecnica di un algoritmo non è sufficiente¹⁹: occorre dimostrarne l'impatto clinico, la comprensibilità per gli utenti finali, la sicurezza e la conformità etico-giuridica.

¹⁷ Il MDR ha sostituito la precedente direttiva 93/42/CEE, rafforzando i requisiti per la sicurezza, la tracciabilità e la trasparenza dei dispositivi medici. Introduce un sistema di identificazione unica (UDI) e potenzia il ruolo degli organismi notificati. Prevede una vigilanza più rigorosa e maggiori responsabilità per i fabbricanti. L'obiettivo è garantire un elevato livello di protezione della salute per pazienti e utenti.

¹⁸ *Reflection paper on the use of artificial intelligence (AI) in the medicinal product lifecycle*, European Medicines Agency, 2023.

¹⁹ Z. OBERMEYER, E.J. EMANUEL, *Predicting the Future. Big Data, Machine Learning, and Clinical Medicine*, in *New England Journal of Medicine*, 2016, 375 (13).

L'Italia, pur con un certo ritardo rispetto ad altri paesi europei, ha cominciato a strutturare percorsi di validazione per soluzioni IA in ambito sanitario, anche grazie al ruolo dell'Agenzia Italiana del Farmaco (AIFA), dell'Istituto Superiore di Sanità (ISS) e delle collaborazioni con le Regioni più attive sul fronte della sanità digitale. Tuttavia, rimangono aperte molte sfide: la frammentazione normativa tra ambito sanitario e tecnologico, la carenza di personale qualificato nella valutazione dei sistemi IA, e la necessità di infrastrutture dati adeguate, interoperabili e sicure.

Alla luce di quanto esposto, è evidente che i sistemi di supporto alle decisioni cliniche basati su IA possono rappresentare una risorsa strategica per migliorare l'efficacia e l'efficienza della telemedicina. Tuttavia, la loro diffusione su larga scala potrà avvenire solo attraverso un equilibrio tra innovazione e regolamentazione, tra libertà di sviluppo tecnologico e responsabilità nei confronti del paziente. La fiducia, elemento intangibile ma fondamentale, potrà essere costruita solo attraverso trasparenza, controllo pubblico e un'adeguata comunicazione dei benefici e dei limiti delle tecnologie adottate.

4. CASE STUDY E APPLICAZIONI REALI

La telemedicina sta evolvendo da semplice supporto tecnologico a strumento strutturale nei sistemi sanitari globali. Lontano dall'essere un concetto astratto, essa trova concretezza in esperienze operative che rispondono a bisogni reali: dalla gestione delle cronicità all'assistenza in territori isolati, fino all'erogazione di cure in zone di conflitto. Farà seguito un'analisi di alcune delle più rilevanti applicazioni internazionali della telemedicina, con un'attenzione specifica alle soluzioni ad alto impatto sociale e organizzativo. L'obiettivo è mostrare come approcci diversi, in contesti diversi, abbiano saputo integrare efficacemente tecnologia, *governance* e assistenza centrata sulla persona.

4.1. Le cabine di telemedicina H4D: una risposta ai “deserti medici” francesi

In Francia, il fenomeno dei “deserti medici” – aree con grave carenza di medici di base – ha spinto all'adozione di soluzioni innovative. Una di queste è la “Consult Station” sviluppata dalla startup H4D: una cabina di telemedicina dotata di strumenti diagnostici (come stetoscopio, otoscopio, misuratore di pressione) che consente ai pazienti di eseguire autonomamente esami clinici, guidati da un medico in videochiamata.

Queste cabine sono state installate in oltre 100 località, soprattutto in zone rurali, permettendo ai cittadini di accedere a consulti medici senza dover percorrere lunghe distanze. Il successo dell'iniziativa ha portato la SNCF, la compagnia ferrovia-

ria nazionale francese, ad annunciare l'installazione di cabine simili in 300 stazioni ferroviarie entro il 2028, sfruttando la capillarità della rete ferroviaria per migliorare l'accesso alle cure²⁰.

4.2. *Seba Virtual Hospital*: l'ospedale virtuale più grande al mondo

Il *Seba Virtual Hospital* (SVH), operativo dal 2022, rappresenta il più grande ospedale virtuale al mondo e una delle più ambiziose iniziative sanitarie digitali promosse da uno Stato. Il progetto, sviluppato dal Ministero della Salute saudita, è parte integrante della Vision 2030, un piano strategico che mira a diversificare l'economia nazionale, puntando fortemente sulla digitalizzazione del settore sanitario. SVH non è un semplice centro di teleconsulto, ma un'infrastruttura tecnologica avanzata connessa a oltre 200 ospedali su tutto il territorio del Regno, in grado di offrire prestazioni in 44 specialità cliniche, dalla cardiologia alla psichiatria.

La sua peculiarità è l'integrazione tra telemedicina sincrona (videoconsulti in tempo reale) e supporto clinico asincrono (analisi di esami, diagnosi remota, telepatologia), grazie anche all'uso di intelligenza artificiale, robotica e strumenti di realtà aumentata. SVH consente una gestione distribuita delle risorse sanitarie, migliorando l'efficienza del sistema e riducendo le disuguaglianze tra le aree urbane e le regioni più remote. Non si tratta solo di trasferire prestazioni: attraverso la teleformazione e il supporto clinico da remoto, l'ospedale virtuale contribuisce attivamente al rafforzamento delle competenze locali, con un modello di "rete clinica virtuale" che potrebbe diventare riferimento per molti altri paesi²¹.

4.3. *Sehat Kahani*: telemedicina per l'empowerment femminile in Pakistan

In Pakistan, le restrizioni culturali e religiose hanno portato a un paradosso strutturale: nonostante una presenza elevata di donne medico laureate, molte di esse non esercitano la professione a causa delle pressioni sociali e familiari. *Sehat Kahani* nasce nel 2017 proprio per rispondere a questa contraddizione, trasformandola in opportunità. La piattaforma, fondata da due donne medico, ha creato un sistema di cliniche periferiche in zone rurali, gestite in presenza da infermiere locali e collegate virtualmente con dottoresse che operano da casa, in sicurezza e secondo i vincoli culturali vigenti.

²⁰ N. HUET, *Can't find a doctor? This hi-tech telemedicine booth offers a handy, hands-on checkup*, in *Euronews*, 2023, <https://www.euronews.com/health/2023/02/04/cant-find-a-doctor-this-hi-tech-telemedicine-booth-offers-hands-on-checkup-medical-desert>.

²¹ S. NEVILLE, *'Virtual hospitals' deliver home treatment to remote patients*, in *Financial Times*, 2025, <https://www.ft.com/content/104151c3-f808-4c2d-a20a-b1394846772c>.

Il modello ha una duplice valenza: da un lato offre assistenza sanitaria di qualità a comunità isolate e spesso trascurate dal sistema pubblico; dall'altro consente alle donne medico di valorizzare le proprie competenze professionali, contribuendo attivamente al sistema sanitario. Finora *Sehat Kahani* ha fornito oltre un milione di consulti e gestisce oltre 60 unità critiche. Il progetto è sostenuto anche da fondi internazionali per lo sviluppo ed è riconosciuto come *best practice* nei contesti in cui l'accesso alla sanità è ostacolato da fattori culturali, geografici o economici. È un esempio paradigmatico di come la telemedicina possa fungere da leva di inclusione sociale e di equità di genere²².

4.4. *Arian Teleheal*: supporto medico a distanza in zone di guerra

Il progetto *Arian Teleheal* si distingue come una delle più importanti esperienze di medicina umanitaria digitale a livello globale. Fondato dal medico anglo-afghano Waheed Arian, rifugiato e vittima della guerra in Afghanistan, il programma nasce dalla necessità di fornire supporto medico a distanza in contesti estremi come zone di conflitto o aree colpite da disastri umanitari. Attraverso una rete di medici volontari con sede in Europa, negli Stati Uniti e in Canada, Arian Teleheal fornisce teleconsultenze e supporto clinico continuo a operatori sanitari che operano in Afghanistan, Siria, Iraq, Sud Sudan e Uganda.

La logica del progetto non è quella di sostituire l'intervento medico in loco, ma di rafforzare la capacità decisionale dei professionisti locali, spesso costretti a lavorare in condizioni drammatiche, senza strumenti diagnostici adeguati o con livelli di formazione non sufficienti per casi complessi. La piattaforma utilizza strumenti di comunicazione sicura, accessibili anche con banda limitata, e garantisce l'anonimato dei pazienti. Oltre all'impatto clinico immediato – con una percentuale di successo del 88% nei casi critici – *Arian Teleheal* ha anche una funzione educativa, offrendo sessioni di aggiornamento, linee guida e supporto continuo. È un caso esemplare di come la telemedicina, applicata con flessibilità e visione etica, possa salvare vite in scenari inaccessibili per la sanità tradizionale²³.

4.5. *Hospital at Home* (Stati Uniti): la deospedalizzazione digitale

Negli Stati Uniti, il modello “Hospital at Home” si è affermato come una delle innovazioni più rilevanti per la gestione delle acuzie in ambito domiciliare. Il programma dell'NYU Langone Health a Long Island rappresenta un caso avanzato di deospe-

²² *Sehat Kahani, a health story from Pakistan*, in *Country Connector*, 2022, <https://ccpsh.org/blog/sehat-kahani-health-story-pakistan>.

²³ C. GOODYEAR, *The doctor using smartphones to save lives in war zones*, in *University of Cambridge*, 2019, <https://www.cam.ac.uk/this-cambridge-life/waheed-arian>.

dalizzazione supportata da tecnologia digitale. Rivolto a pazienti che necessitano di cure ospedaliere ma non di sorveglianza intensiva, il progetto prevede la somministrazione a domicilio di terapie farmacologiche, ossigenoterapia, radiografie portatili, esami ematici, e monitoraggio costante tramite dispositivi connessi²⁴.

Ogni paziente viene dotato di un kit tecnologico completo e seguito quotidianamente da infermieri e medici, con supporto remoto 24 ore su 24. L'intero percorso è tracciato digitalmente e inserito nella cartella clinica elettronica centralizzata. I risultati sono significativi: riduzione dei costi sanitari, minore rischio di infezioni nosocomiali, maggiore soddisfazione del paziente e dei caregiver. Ma soprattutto, si osserva un miglioramento nell'aderenza terapeutica e nella rapidità del recupero post-acuto. In un contesto sanitario complesso e costoso come quello statunitense, il modello "Hospital at Home" rappresenta una risposta concreta alla necessità di rendere l'assistenza più sostenibile, umana e integrata nel contesto di vita del paziente²⁵.

5. CONCLUSIONI

Nel delineare le prospettive future della telemedicina in Italia, appare evidente come la sfida principale non sia più di natura tecnologica, bensì organizzativa e sistemica. Le soluzioni digitali oggi disponibili, infatti, sono sufficientemente mature da consentire l'erogazione di servizi efficienti e sicuri. Tuttavia, la piena realizzazione del potenziale della telemedicina richiede un ripensamento complessivo delle logiche di funzionamento del sistema sanitario, fondato su un approccio integrato, coordinato e centrato sul paziente.

In tal senso, la Piattaforma Nazionale di Telemedicina rappresenta un tassello strategico per superare la frammentazione esistente e garantire un'infrastruttura uniforme, interoperabile e conforme agli standard europei in materia di protezione dei dati. L'obiettivo non è solamente tecnico, ma profondamente politico: costruire una sanità digitale accessibile, equa e sostenibile, in cui la telemedicina non sia una soluzione opzionale o residuale, ma parte integrante dei percorsi assistenziali.

L'integrazione dell'intelligenza artificiale e dei *big data* potrà ulteriormente rafforzare l'efficacia della telemedicina, introducendo modelli predittivi e sistemi di supporto decisionale in grado di anticipare le criticità cliniche, personalizzare le terapie e migliorare la qualità complessiva dell'assistenza. Tuttavia, affinché tali innovazioni producano valore reale, sarà indispensabile garantire un impianto etico solido, basato

²⁴ J. KELLY, *Groundbreaking program brings hospital-quality care to home*, in *New York Post*, 2024, <https://nypost.com/2024/04/29/health/groundbreaking-program-brings-hospital-quality-care-to-home/>.

²⁵ *Telemedicine Transforms Response to COVID-19 Pandemic in Disease Epicenter*, in *NYU Langone Health*, 2020, <https://nyulangone.org/news/telemedicine-transforms-response-covid-19-pandemic-disease-epicenter>.

sulla trasparenza algoritmica, sulla protezione della privacy e sul rispetto dell'autonomia del paziente.

In conclusione, il successo della telemedicina nel contesto italiano dipenderà dalla capacità di governare in modo intelligente questa transizione, promuovendo una visione olistica della salute digitale che sappia coniugare innovazione tecnologica, sostenibilità organizzativa e inclusione sociale. Il passaggio da sperimentazione a sistema non sarà immediato, ma costituisce una necessità inderogabile per garantire la resilienza e l'equità del SSN nei decenni a venire.

APPROCCIO AL RISCHIO DELL'AI ACT E RIVOLUZIONE DEL SETTORE DELLE CURE PREVENTIVE

Lorenzo Gasparini

L'intelligenza artificiale "IA" sta rapidamente trasformando numerosi settori della ricerca e del sapere; il suo potenziale è particolarmente evidente proprio nel settore sanitario, con un impatto importante nelle cure preventive. Tuttavia, il suo impiego solleva interrogativi di natura etica, sociale e normativa. L'AI Act, Regolamento europeo 1689/2024¹, si propone di fornire un quadro regolatorio completo, adottando un approccio basato sul rischio. Questo modello consente di bilanciare l'innovazione e la tutela dei diritti fondamentali, rappresentando una guida cruciale per la rivoluzione delle cure preventive².

In considerazione dell'impatto significativo che l'IA potrà avere sulla società, e quindi della necessità di creare maggiore fiducia tra i consociati, sarà essenziale che la stessa venga sviluppata conformemente ai valori dell'Unione sanciti dall'art. 2 del trattato sull'Unione europea³ (TUE), ai diritti e alle libertà fondamentali contenuti nei trattati stessi. Al fine di garantire un livello costante ed elevato di tutela degli interessi pubblici in materia di salute, sicurezza e diritti fondamentali, è opportuno stabilire regole comuni per i sistemi di IA, classificando gli stessi sulla base del rischio dai medesimi creato. Si rende pertanto necessario un quadro giuridico europeo che

¹ F.R. PESCE, E. BRAMBILLA, L. MANTOVANI, *L'etica e la governance dell'intelligenza artificiale: prospettive predittive e tutela dei diritti nell'AI Act*, in *Cyberspazio e diritto: rivista internazionale di informatica giuridica*, n. 3, 2024, pp. 409-422.

² L. FERRARA, *Gli strumenti di intelligenza artificiale e le istituzioni museali, tra il piano nazionale per la digitalizzazione del patrimonio culturale e il Regolamento UE 1689/2024. Prime osservazioni*, 2024, (Intervento presentato al convegno Prin 2022 "Intelligenza amministrativa artificiale per l'uguaglianza territoriale" tenutosi a Chieti, Università "G. D'Annunzio" di Chieti e Pescara nel 16 settembre 2024).

³ Art. 2, Trattato dell'Unione Europea: "L'Unione si fonda sui valori del rispetto della dignità umana, della libertà, della democrazia, dell'uguaglianza, dello Stato di diritto e del rispetto dei diritti umani, compresi i diritti delle persone appartenenti a minoranze. Questi valori sono comuni agli Stati membri in una società caratterizzata dal pluralismo, dalla non discriminazione, dalla tolleranza, dalla giustizia, dalla solidarietà e dalla parità tra donne e uomini".

istituisca regole armonizzate in materia di IA per promuovere lo sviluppo, l'uso e l'adozione della stessa nel mercato interno, garantendo allo stesso tempo un elevato livello di protezione degli interessi pubblici, quali la salute, la sicurezza e la protezione dei diritti fondamentali. Per ottenere questo risultato è necessario introdurre delle regole che disciplinino l'immissione sul mercato, la messa in servizio e l'utilizzo dei sistemi di IA, garantendo in tal modo il buon funzionamento del mercato interno e, soprattutto, i diritti fondamentali della collettività.

Con l'intento di perseguire le finalità sopra richiamate⁴, il Regolamento 1689/2024, come accennato, disciplina una classificazione dei sistemi di intelligenza artificiale in base al rischio caratterizzante gli stessi; infatti, tale ultima valutazione presuppone che dall'utilizzo dei sistemi di IA, anche nelle situazioni di corretta adozione degli stessi, possa sempre essere calcolata una probabilità circa la verifica di danni. Sul punto, preme sottolineare come il regolamento sopracitato, in fase di apertura, art. 2, indirizzi le disposizioni ivi contenuti ad una platea molto ampia di operatori del settore, ricomprendendo, a titolo esemplificativo, i fornitori, i *deployer*⁵, gli sviluppatori, i rappresentanti e, in generale, tutti gli interessati che si trovino all'interno del territorio dell'Unione⁶.

Come accennato, il provvedimento adotta un approccio *risk-based*⁷, suddividendo i sistemi di intelligenza artificiale in tre categorie in base al rischio per la sicurezza degli utenti e per il rispetto dei diritti fondamentali dei cittadini, individuando per ciascuna categoria gli obblighi gravanti sui fornitori e sugli utilizzatori "professionali"⁸:

⁴ E. MAESTRI, *Introduzione e note di sintesi al Regolamento (UE) 2024/1689 sull'intelligenza artificiale (testo ufficiale e integrale)*, Napoli, Jovene, 2024, vol. 6, pp. 173-180.

⁵ Con il termine "deployer" si indica una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che utilizza un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale.

⁶ È bene precisare come lo stesso regolamento escluda la relativa applicazione da alcuni ambiti d'interesse, tra i quali i settori che non rientrano nell'ambito di applicazione del diritto dell'Unione e, in ogni caso, non pregiudicano le competenze degli Stati membri in materia di sicurezza nazionale, indipendentemente dal tipo di entità incaricata dagli Stati membri di svolgere compiti in relazione a tali competenze. Non si applica a tutti i sistemi di IA se e nella misura in cui sono immessi sul mercato, messi in servizio o utilizzati con o senza modifiche esclusivamente per scopi militari, di difesa o di sicurezza nazionale, indipendentemente dal tipo di entità che svolge tali attività, ai sistemi di IA che non sono immessi sul mercato o messi in servizio nell'Unione, qualora l'output sia utilizzato nell'Unione esclusivamente per scopi militari, di difesa o di sicurezza nazionale, indipendentemente dal tipo di entità che svolge tali attività. Ancora, il presente regolamento non si applica ai sistemi di IA o modelli di IA, ivi compresi i loro output, specificamente sviluppati e messi in servizio al solo scopo di ricerca e sviluppo scientifici. Per una completa disamina si veda l'art. 2, Regolamento 1689/2024.

⁷ A.M. POP, *Il risk-based approach, la governance e le sanzioni nell'AI Act*, in M.G. PELUSO (a cura di) *Cyberspazio e diritto: rivista internazionale di informatica giuridica*, 2024, pp. 423-435.

⁸ A differenza del testo inizialmente proposto dalla Commissione europea nel 2021, la versione definitiva del Regolamento prevede inoltre delle disposizioni specifiche per i modelli di IA per finalità

- Sistemi di IA che comportano rischi considerati “inaccettabili”
- Sistemi di IA ad alto rischio
- Sistemi di IA a rischio limitato
- Sistemi di IA a rischio minimo

Partendo dalla disamina dei sistemi considerati a rischio inaccettabile, è di primario interesse specificare come il Regolamento 1689/2024 abbia formalmente introdotto un generico divieto di utilizzazione degli stessi; infatti, l'art. 5, rubricato “pratiche di IA vietate”, al comma 1, introduce un vasto elenco di pratiche per le quali l'immissione sul mercato, la messa in servizio o l'uso di un sistema di IA è da considerare tassativamente vietato. Nello specifico, tali limitazioni mirano soprattutto alla tutela e alla protezione di una vasta gamma di diritti fondamentali della persona, quali la tutela della libertà personale di scelta, la tutela di tutti coloro che a causa di vulnerabilità psico-fisiche sono maggiormente raggruppabili dalle statuizioni degli operatori, la protezione dei dati sensibili⁹, nonché la riservatezza¹⁰. Tra le applicazioni ad uso vietato vi sono quindi gli strumenti di polizia predittiva, volti ad “etichettare” un individuo quale socialmente pericoloso¹¹ sulla base di meri comportamenti e precedenti. Sono poi vietati anche i sistemi di riconoscimento delle emozioni, soprattutto nelle scuole o nei luoghi frequentati da un'ampia categoria di persone. Si suole far riferimento a tutte quelle tecnologie che permettono di analizzare il tono della voce, i gesti, nonché le espressioni facciali di una persona per capire il suo umore e le sue abitudini di vita. Infine, ampio spazio è dedicato al tema del riconoscimento biometrico delle persone in ampi spazi pubblici¹².

generali (art. 51 ss.), ossia per quei modelli, addestrati con grandi quantità di dati, che sono in grado di svolgere con competenza molteplici funzioni e che possono essere integrati in un'ampia gamma di dispositivi (art. 3, n. 63).

⁹ E. STRINGHI, *La governance dell'IA: quale spazio per le Autorità di protezione dei dati personali?: prime riflessioni sull'AI Act*, in M.G. PELUSO (a cura di) *Cyberspazio e diritto: rivista internazionale di informatica giuridica*, 2024, pp. 437-453.

¹⁰ L. FERRARA, *Gli strumenti di intelligenza artificiale e le istituzioni museali, tra il piano nazionale per la digitalizzazione del patrimonio culturale e il Regolamento UE 1689/2024. Prime osservazioni*, 2024, (Intervento presentato al convegno Prin 2022 “Intelligenza amministrativa artificiale per l'uguaglianza territoriale” tenutosi a Chieti, Università “G. D'Annunzio” di Chieti e Pescara nel 16 settembre 2024).

¹¹ E. PIETROCARLO, *La predictive policing nel regolamento europeo sull'intelligenza artificiale*, in *La legislazione penale*, 2024, pp. 1-35.

¹² L'art. 5 sopracitato dedica un ampio spazio alla disciplina concernente l'utilizzo dei sistemi biometrici di identificazione delle persone, precisando che il relativo utilizzo, salvo eccezioni, è vietato dal regolamento stesso. Infatti, tali sistemi permettono agli utilizzatori di identificare una persona attraverso l'analisi delle caratteristiche fisiche uniche e intrasferibili, come ad esempio le impronte digitali, l'iride o i lineamenti del viso. L'implementazione di tali strumenti con i sistemi di IA permetterebbe un'identificazione sicuramente più celere e precisa ma, al tempo stesso, un utilizzo improprio dei medesimi rischierebbe di pregiudicare i diritti costituzionalmente garantiti ai cittadini. Il legislatore europeo ne ha quindi fortemente limitato l'utilizzo, confinando gli stessi soprattutto ad

Passando alla disamina della normativa europea in tema di sistemi IA ad alto rischio¹³, preme in apertura sottolineare la generale differenza rispetto agli strumenti sopra analizzati. Infatti, come detto, l'art. 5 del citato regolamento, salvo deroghe tassativamente indicate, tende a vietare l'utilizzo dei suindicati sistemi in settori che potrebbe gravemente pregiudicare i diritti fondamentali della persona. All'opposto, i sistemi di IA ad alto rischio, che parimenti trovano vita in settori di assoluto rilievo per la collettività, quali la tutela della salute, sono pienamente ammessi dalle istituzioni europee, seppur in presenza di una serie molto vasta di presupposti e criteri volti a regolamentarne la produzione, il commercio, la distribuzione e l'utilizzo. Il Regolamento europeo 1689/2024 ha dedicato l'intero capo III alla trattazione dei sistemi IA ad alto rischio, specificando all'art. 6, parr. 1 e 2, i criteri che un'apparecchiatura deve possedere per poter essere inserita all'interno della quivi analizzata categoria: "A prescindere dal fatto che sia immesso sul mercato o messo in servizio indipendentemente dai prodotti di cui alle lettere a) e b), un sistema di IA è considerato ad alto rischio se sono soddisfatte entrambe le condizioni seguenti: a) il sistema di IA è destinato a essere utilizzato come componente di sicurezza di un prodotto, o il sistema di IA è esso stesso un prodotto, disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'allegato I; b) il prodotto, il cui componente di sicurezza a norma della lett. a) è il sistema di IA, o il sistema di IA stesso in quanto prodotto, è soggetto a una valutazione della conformità da parte di terzi ai fini dell'immissione sul mercato o della messa in servizio di tale prodotto ai sensi della normativa di ar-

attività di controllo specifico; "l'uso di sistemi di identificazione biometrica remota 'in tempo reale' in spazi accessibili al pubblico a fini di attività di contrasto a meno che, e nella misura in cui, tale uso sia strettamente necessario per uno degli obiettivi seguenti: i) la ricerca mirata di specifiche vittime di sottrazione, tratta di esseri umani o sfruttamento sessuale di esseri umani, nonché la ricerca di persone scomparse; ii) la prevenzione di una minaccia specifica, sostanziale e imminente per la vita o l'incolumità fisica delle persone fisiche o di una minaccia reale e attuale o reale e prevedibile di un attacco terroristico; iii) la localizzazione o l'identificazione di una persona sospettata di aver commesso un reato, ai fini dello svolgimento di un'indagine penale, o dell'esercizio di un'azione penale o dell'esecuzione di una sanzione penale per i reati di cui all'allegato II, punibile nello Stato membro interessato con una pena o una misura di sicurezza privativa della libertà della durata massima di almeno quattro anni". L'utilizzo dei sistemi IA di identificazione biomedica delle persone in tempo reale è comunque subordinato a molteplici controlli, i quali sono vincolano gli operatori sia in chiave preventiva, mediante la previa verifica dell'autorità giudiziaria o dell'autorità amministrativa preposta, sia dalle autorità di vigilanza: "è subordinato a un'autorizzazione preventiva rilasciata da un'autorità giudiziaria o da un'autorità amministrativa indipendente, la cui decisione è vincolante, dello Stato membro in cui deve avvenire l'uso, rilasciata su richiesta motivata e in conformità delle regole dettagliate del diritto nazionale di cui al par. 5. Tuttavia, in una situazione di urgenza debitamente giustificata, è possibile iniziare a usare il sistema senza autorizzazione a condizione che tale autorizzazione sia richiesta senza indebito ritardo, al più tardi entro 24 ore. Se tale autorizzazione è respinta, l'uso è interrotto con effetto immediato e tutti i dati nonché i risultati e gli output di tale uso sono immediatamente eliminati e cancellati".

¹³ M. AIMO, *Sistemi di gestione algoritmica: la risposta dell'Europa di fronte ad una trasformazione "ad alto rischio"*, in *Il diritto del lavoro nell'era delle transizioni*, Pisa, Pacini Giuridica, 2024, vol. 1, pp. 1-23.

monizzazione dell'Unione elencata nell'allegato I. 2. Oltre ai sistemi di IA ad alto rischio di cui al paragrafo 1, sono considerati ad alto rischio anche i sistemi di IA di cui all'allegato III¹⁴. Per quanto di nostro interesse, l'ambito medico viene direttamente interessato dalla normativa europea attraverso il rinvio operato dal par. 1, lett. a) sopra riportato, in forza del quale un sistema IA viene definito ad alto rischio qualora venga considerato quale prodotto disciplinato dalle plurime normative dell'Unione elencate nell'allegato I¹⁵. Quest'ultimo, quindi, contiene un'ampia elencazione di tutte quelle normative che, disciplinando specifici aspetti e prodotti, sono direttamente interessate dalla classificazione operata dall'art. 6. Nello specifico, l'allegato I al Regolamento europeo, al numero 11, indica quali normative interessate dallo stesso; il Regolamento (UE) 2017/745¹⁶ del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medici, nonché, al seguente numero 12, il Regolamento (UE) 2017/746¹⁷ del Parlamento europeo e del Consiglio, del 5 aprile 2017,

¹⁴ L'allegato III definisce sistemi di IA, quali apparecchiature e strumenti classificabili in base al settore specifico di utilizzo, prescindendo, quindi, dai due requisiti posti dall'art. 6, par. 1. Infatti, trattasi di settori estremamente tecnici, quali, a titolo esemplificativo, l'Istruzione e la formazione professionale; Occupazione, gestione dei lavoratori e accesso al lavoro autonomo; Accesso a servizi privati essenziali e a prestazioni e servizi pubblici essenziali e fruizione degli stessi; Migrazione, asilo e gestione del controllo delle frontiere, nella misura in cui il pertinente diritto dell'Unione o nazionale ne permette l'uso; Amministrazione della giustizia e processi democratici.

¹⁵ Il citato allegato contiene un ampio elenco di normative europee che, a seguito del regolamento 1689/2024, sono direttamente interessate dall'armonizzazione; infatti, con tale termine si suole fare riferimento all'applicazione di nuove specifiche tecniche e puntuali ad una molteplicità di normative già presenti nel comparto europeo. Il regolamento quivi citato, infatti, applica le nuove regole in tema di sistemi IA ad alto rischio a tutti quei sistemi che già erano stati introdotti nel nostro ordinamento in passato, e che ora dovranno necessariamente adeguarsi alle nuove regole applicate.

¹⁶ Il Regolamento n. 745/2024 stabilisce le norme relative all'immissione sul mercato, la messa a disposizione sul mercato o la messa in servizio dei dispositivi medici per uso umano e degli accessori per tali dispositivi nell'Unione. Il presente regolamento si applica inoltre alle indagini cliniche relative a tali dispositivi medici e relativi accessori condotte nell'Unione.

¹⁷ Il presente regolamento si apre con una precisa definizione dei dispositivi medici ivi descritti, la quale si fonda su di un generico rinvio al contenuto del Regolamento 745/2017. Nello specifico, si applicano le seguenti definizioni: "1) 'dispositivo medico': un 'dispositivo medico' quale definito all'articolo 2, punto 1), del Regolamento (UE) 2017/745. 2) 'dispositivo medico-diagnostico in vitro': qualsiasi dispositivo medico composto da un reagente, un prodotto reattivo, un calibratore, un materiale di controllo, un kit, uno strumento, un apparecchio, una parte di attrezzatura, un software o un sistema, utilizzato da solo o in combinazione, destinato dal fabbricante a essere impiegato in vitro per l'esame di campioni provenienti dal corpo umano, inclusi sangue e tessuti donati, unicamente o principalmente al fine di fornire una o più delle seguenti informazioni: a) su un processo o uno stato fisiologico o patologico; b) su una disabilità fisica o intellettuale congenita; c) sulla predisposizione a una condizione clinica o a una malattia; d) per determinare la sicurezza e la compatibilità con potenziali soggetti riceventi; e) f) per prevedere la risposta o le reazioni a un trattamento; per definire o monitorare le misure terapeutiche".

relativo ai dispositivi medico-diagnostici in vitro¹⁸. Il rinvio operato dall'art. 6 dell'IA Act ai qui citati regolamenti, permette, quindi, di considerare ad alto rischio tutti quei dispositivi medici e diagnostici descritti nelle stesse normative, sicché, come anticipato, saranno a questi ultimi applicabili le nuove stringenti regole introdotte dal testo europeo. La normativa sull'intelligenza artificiale si applica a tutti quei dispositivi medici in possesso delle caratteristiche descritte dalle fonti di rinvio; infatti, il Regolamento 745/2017, all'art. 1, definisce i già menzionati dispositivi come tutti quegli strumenti, apparecchi, apparecchiature, software, impianti, reagenti, materiali o altro articolo, destinati dal fabbricante a essere impiegati sull'uomo per una pluralità di attività mediche¹⁹. Questi ultimi, che quindi debbono necessariamente possedere le caratteristiche contenute nelle citate fonti europee, ai quali si applicano altresì tutti i plurimi obblighi ivi contenuti, sono considerati dal Regolamento 1689/2024 ad alto rischio, sicché ad essi si applicherà tutto quell'ampio corpus normativo di obblighi, vincoli, limitazioni e controlli introdotto dall'IA ACT.

Analizzando ora le principali novità applicabili ai sistemi IA ad alto rischio, tra i quali rientrano appieno i dispositivi medici sopra citati, pare imprescindibile porre l'attenzione su alcuni aspetti di centrale importanza; infatti, tali sistemi possono essere legittimamente prodotti, commercializzati e utilizzati solamente se rispettosi di una serie di requisiti. Si pensi all'adozione di un sistema di gestione dei rischi (art. 9), alla necessaria supervisione tecnica (art. 14), senza contare l'ampio corpus di obblighi applicabili ai fornitori e ai *deployer*²⁰.

¹⁸ Il Regolamento n. 746/2017 stabilisce le norme relative all'immissione sul mercato, la messa a disposizione sul mercato o la messa in servizio dei dispositivi medico-diagnostici in vitro per uso umano e degli accessori per tali dispositivi nell'Unione. Esso si applica inoltre agli studi delle prestazioni riguardanti tali dispositivi medico diagnostici in vitro e relativi accessori condotti nell'Unione.

¹⁹ Il testo indica quali finalità degli strumenti medici:

- diagnosi, prevenzione, monitoraggio, previsione, prognosi, trattamento o attenuazione di malattie,
- diagnosi, monitoraggio, trattamento, attenuazione o compensazione di una lesione o di una disabilità,
- studio, sostituzione o modifica dell'anatomia oppure di un processo o stato fisiologico o patologico,
- fornire informazioni attraverso l'esame in vitro di campioni provenienti dal corpo umano, inclusi sangue e tessuti donati,
- nonché;
- dispositivi per il controllo del concepimento o il supporto al concepimento,
- i prodotti specificamente destinati alla pulizia, disinfezione o sterilizzazione dei dispositivi di cui all'articolo 1, par. 4, e di quelli di cui al primo comma del presente punto.

²⁰ Infatti, la sezione 3, dall'art. 16 in poi, contiene un ampio novero di obblighi in capo ai fornitori quali, a titolo esemplificativo, la creazione di un sistema di gestione della qualità che garantisca la conformità degli strumenti al regolamento; un'ampia conservazione dei documenti; un dovere di informazione; generici obblighi di controllo, valutazione del rischio e collaborazione con le autorità preposte.

Come sopra anticipato, i sistemi medici di IA, utilizzati altresì nel comparto delle cure preventive, rientrando nella classificazione quivi analizzata, sono destinatari di tutti questi importanti obblighi e requisiti introdotti dal legislatore europeo con l'intento di proteggere la collettività che ne sarà destinataria.

Analizziamo di seguito alcune delle più rilevanti novità.

L'art. 9 dell'IA ACT introduce il tema della gestione e valutazione dei rischi; come anticipato, i sistemi ad alto rischio si fondano sulla probabilità che dal relativo utilizzo possa derivare un nocumento sia per l'utilizzatore che per il destinatario. Sul punto, il Regolamento 1689/2024 impone l'adozione di un piano di valutazione e gestione del rischio, definendo lo stesso come "un processo iterativo continuo pianificato ed eseguito nel corso dell'intero ciclo di vita di un sistema di IA ad alto rischio, che richiede un riesame e un aggiornamento costanti e sistematici". Non è quindi sufficiente la mera creazione di un documento esplicativo delle buone pratiche di utilizzazione del sistema IA, ma sarà necessario un continuo studio dell'impatto che il sistema potrebbe avere sui più, riesaminando e aggiornando costantemente le pratiche e le tecniche operative. Il processo di valutazione dei rischi comprende plurime fasi; l'identificazione e la valutazione dei rischi noti e prevedibili, una classificazione dei rischi in base al relativo impatto, la predisposizione di tecniche di riduzione o eliminazione degli stessi, nonché una costante documentazione delle attività espletate. Queste procedure valutative sono tuttavia pur sempre limitate a quei rischi che possono essere ragionevolmente contenuti o eliminati; infatti, le prescrizioni contenute nell'art. 9, che quindi condizionano lo sviluppo e il commercio dei sistemi IA, riguardano solamente i rischi ragionevoli e prevedibili, ossia quelli che, seppur derivanti da un utilizzo improprio del sistema, si sarebbero potuti evitare applicando le regole predeterminate²¹. Nello specifico, a chiusa di tale disamina, il par. 5 dell'art. 9 indica come "Le misure di gestione dei rischi di cui al par. 2, lett. d), sono tali che i pertinenti rischi residui associati a ciascun pericolo nonché il rischio residuo complessivo dei sistemi di IA ad alto rischio sono considerati accettabili". Il rinvio al par. 2 permette di collocare tale disposizione entro la valutazione dei rischi derivanti dall'utilizzo proprio del sistema di IA di cui al par. 2, lett. a)²², sicché il rischio resi-

²¹ La valutazione dei rischi non si limita quindi ad un utilizzo improprio dei sistemi tecnologici di IA, ma si estende ad ogni possibile applicazione degli stessi da parte degli operatori sanitari e non. Questo assunto si traduce in un generale obbligo di previsione dei rischi evitabili, siano essi conseguenti agli errori umani impropri, che al regolare utilizzo dei sistemi stessi.

²² Così il par. 2 del Regolamento 1689/2024: "Il sistema di gestione dei rischi è inteso come un processo iterativo continuo pianificato ed eseguito nel corso dell'intero ciclo di vita di un sistema di IA ad alto rischio, che richiede un riesame e un aggiornamento costanti e sistematici. Esso comprende le fasi seguenti: a) identificazione e analisi dei rischi noti e ragionevolmente prevedibili che il sistema di IA ad alto rischio può porre per la salute, la sicurezza e i diritti fondamentali quando il sistema di IA ad alto rischio è utilizzato conformemente alla sua finalità prevista; b) stima e valutazione dei rischi che possono emergere quando il sistema di IA ad alto rischio è usato conformemente alla sua finalità

duale derivante dall'utilizzo corretto dell'apparecchio si considera sempre accettabile e non contenibile.

La gestione del rischio nell'AI Act è quindi essenziale per garantire trasparenza, sicurezza e affidabilità nei sistemi di IA, soprattutto quelli ad alto rischio, vincolando i fornitori, distributori, utilizzatori e le autorità di vigilanza all'adempimento costante delle regole suindicate, permettendo così la tutela dei diritti di tutti i soggetti interessati.

Infine, si ricorda brevemente come i sistemi di intelligenza artificiale ad alto rischio debbano sempre essere sottoposti a rigorose prove di conformità prima della loro immissione nel mercato. Questi test valutano l'affidabilità, la sicurezza, la trasparenza e la protezione dei dati, garantendo che l'IA operi in modo corretto nel rispetto dei diritti fondamentali e delle regole prescritte dallo stesso regolamento. Le verifiche includono analisi dei dati, test di robustezza contro errori e attacchi informatici, nonché simulazioni in scenari reali. Qualora un sistema non dovesse superare le quivi citate prove, lo stesso non potrà essere commercializzato, dovendo attendere il vaglio di conformità²³.

Ancora, un'altra disposizione di particolare interesse, soprattutto in ambito medico, si individua nell'art. 11, rubricato "documentazione tecnica"; infatti, quest'ultimo impone la redazione di una completa relazione inerente al funzionamento del dispositivo prima dell'immissione nel mercato dello stesso, con il conseguente obbligo di aggiornamento continuo in capo agli operatori del settore. La documentazione tecnica ha come obiettivo primario quello di accertare in via preventiva che il sistema di IA ad alto rischio sia conforme ai requisiti di cui alla presente sezione, con l'intento di fornire alle autorità nazionali competenti le informazioni necessarie per valutare la conformità del sistema di IA a tali requisiti. In riferimento al contenuto della citata relazione, la disposizione quivi analizzata rinvia a quanto edotto nell'allegato IV del Regolamento 1689/2024, il quale contiene un ampio elenco di informazio-

prevista e in condizioni di uso improprio ragionevolmente prevedibile; c) valutazione di altri eventuali rischi derivanti dall'analisi dei dati raccolti dal sistema di monitoraggio successivo all'immissione sul mercato di cui all'articolo 72; d) adozione di misure di gestione dei rischi opportune e mirate intese ad affrontare i rischi individuati ai sensi della lett. a)". Ad ogni buon conto pare fondamentale sottolineare come le conoscenze tecniche, l'esperienza, l'istruzione e la formazione dei *deployer*, nonché il contesto presumibile in cui il sistema è destinato ad essere usato, si pongono come presupposto per la valutazione dei rischi, non potendosi quindi pretendere una gestione sproporzionata rispetto ai parametri qui ricordati.

²³ Art. 6: "I sistemi di IA ad alto rischio sono sottoposti a prova al fine di individuare le misure di gestione dei rischi più appropriate e mirate. Le prove garantiscono che i sistemi di IA ad alto rischio funzionino in modo coerente per la finalità prevista e che siano conformi ai requisiti di cui alla presente sezione [...]. Le prove dei sistemi di IA ad alto rischio sono effettuate, a seconda dei casi, in un qualsiasi momento dell'intero processo di sviluppo e, in ogni caso, prima della loro immissione sul mercato o messa in servizio. Le prove sono effettuate sulla base di metriche e soglie probabilistiche definite precedentemente e adeguate alla finalità prevista perseguita dal sistema di IA ad alto rischio".

ni che debbono necessariamente essere contenute nello stesso documento tecnico²⁴. L'obbligo di documentazione tecnica si accompagna altresì al generale vincolo per i costruttori di creare i sistemi IA ad alto rischio nel modo più trasparente possibile, così da permettere ai *deployer* di interpretare correttamente l'output del sistema. L'art. 13, contenente tale indicazione, precisa come i sistemi di IA ad alto rischio debbano essere accompagnati da istruzioni per l'uso, le quali devono necessariamente contenere informazioni concernenti plurimi aspetti, come l'identità e i dati di contatto del fornitore; le caratteristiche, le capacità e i limiti delle prestazioni del sistema di IA ad alto rischio; le eventuali modifiche apportate al sistema di IA e le misure di sorveglianza umana di cui all'art. 14²⁵.

La documentazione tecnica è quindi un requisito essenziale per l'approvazione e il monitoraggio dei sistemi di IA ad alto rischio. Fornitori e sviluppatori dovranno garantire la relativa completezza e chiarezza, aggiornandola costantemente per evitare sanzioni e restrizioni nell'uso del sistema stesso.

Infine, nel trattare le maggiori prescrizioni applicabili ai sistemi IA ad alto rischio, pare necessario soffermarsi sulla sorveglianza umana, la cui disciplina è contenuta nell'art. 14 dell'analizzato regolamento europeo. La citata disposizione introduce un sistema di controllo e sorveglianza particolarmente tecnico, il quale mira a personalizzare le attività di verifica e vigilanza in base al sistema IA commercializzato

²⁴ A titolo esemplificativo, si riportano qui le macrocategorie che contengono le singole previsioni necessarie alla creazione del documento tecnico; Una descrizione generale del sistema di IA comprendente; Una descrizione dettagliata degli elementi del sistema di IA e del processo relativo al suo sviluppo; Informazioni dettagliate sul monitoraggio, sul funzionamento e sul controllo del sistema di IA, in particolare per quanto riguarda: le sue capacità e limitazioni in termini di prestazioni, compresi i gradi di accuratezza relativi a determinate persone o determinati gruppi di persone sui quali il sistema è destinato a essere utilizzato e il livello di accuratezza complessivo atteso in relazione alla finalità prevista del sistema; i prevedibili risultati indesiderati e fonti di rischio per la salute, la sicurezza e i diritti fondamentali, nonché di rischio di discriminazione in considerazione della finalità prevista del sistema di IA; le misure di sorveglianza umana necessarie in conformità dell'articolo 14, comprese le misure tecniche poste in essere per facilitare l'interpretazione degli output dei sistemi di IA da parte dei *deployer*; le specifiche relative ai dati di input, se del caso; Una descrizione dell'adeguatezza delle metriche di prestazione per il sistema di IA specifico; Una descrizione dettagliata del sistema di gestione dei rischi in conformità dell'articolo 9; Una descrizione delle modifiche pertinenti apportate dal fornitore al sistema durante il suo ciclo di vita; Un elenco delle norme armonizzate applicate integralmente o in parte i cui riferimenti sono stati pubblicati nella Gazzetta ufficiale dell'Unione europea; nei casi in cui tali norme armonizzate non sono state applicate, una descrizione dettagliata delle soluzioni adottate per soddisfare i requisiti di cui al capo III, sezione 2, compreso un elenco delle altre norme e specifiche tecniche pertinenti applicate; Una copia della dichiarazione di conformità UE di cui all'articolo 47; Una descrizione dettagliata del sistema predisposto per valutare le prestazioni del sistema di IA nella fase successiva all'immissione sul mercato in conformità dell'articolo 72, compreso il piano di monitoraggio successivo all'immissione sul mercato di cui all'articolo 72, paragrafo 3".

²⁵ Per una completa disamina degli obblighi di trasparenza, si veda il Regolamento 1689/2024 in <https://eur-lex.europa.eu/eli/reg/2024/1689/oj?locale=it>.

e al livello di rischio conseguente al relativo utilizzo. Infatti, come anticipato, la pianificazione del rischio, così come sopra descritto, assume centrale importanza in plurimi aspetti concernenti l'utilizzo dei sistemi di Intelligenza Artificiale, ponendo al centro di quest'ultimo il controllo umano²⁶. La finalità della sorveglianza umana è agilmente rinvenibile nella prevenzione e riduzione dei rischi per la salute²⁷, nell'implementazione della sicurezza e in generale nella tutela dei diritti fondamentali²⁸, sicché la normativa europea tende a vincolare non solo l'utilizzatore dei sistemi ad alto rischio, ma altresì il fornitore degli stessi²⁹. Di particolare importanza appare il disposto di cui al par. 4 del quivi analizzato articolo, il quale impone a tutti gli agenti, *in primis* al fornitore, di creare un sistema di sorveglianza umana che permetta agli utilizzatori di comprendere correttamente le capacità e i limiti pertinenti del sistema di IA, potendo intervenire, correggere o annullare decisioni automatizzate quando necessario³⁰.

²⁶ I sistemi di IA ad alto rischio sono progettati e sviluppati anche con strumenti di interfaccia uomo-macchina adeguati, in modo tale da poter essere efficacemente supervisionati da persone fisiche durante il periodo in cui sono in uso.

²⁷ Come più volte sottolineato nella presente trattazione, i sistemi ad alto rischio sono pienamente utilizzabili nel settore sanitario, sicché il riportato riferimento alla tutela della salute, contenuto nell'art. 14, par. 2, non deve essere inteso in senso alternativo, bensì come rafforzativo di una protezione già insita nel capo del regolamento analizzato.

²⁸ I rischi concernenti un sistema IA sono esaminati e prevenuti sia nelle situazioni di utilizzo conforme alle relative finalità, sia in riferimento ad un possibile utilizzo improprio e non rispettoso delle linee guida e del piano predeterminato.

²⁹ Nello specifico, il par. 3 dell'art. 14 specifica come le misure di sorveglianza umana devono sempre essere strutturate in modo tale da garantire almeno una delle seguenti garanzie: "a) misure individuate e integrate nel sistema di IA ad alto rischio dal fornitore prima della sua immissione sul mercato o messa in servizio, ove tecnicamente possibile; b) misure individuate dal fornitore prima dell'immissione sul mercato o della messa in servizio del sistema di IA ad alto rischio, adatte ad essere attuate dal *deployer*". Come agilmente evincibile dal tenore della disposizione, le misure ivi contenute impongono proprio al fornitore di individuare le misure di sorveglianza utilizzabili dal *deployer* prima di immettere nel mercato il sistema stesso, confermando l'applicazione della normativa a 360 gradi.

³⁰ Gli utilizzatori dei sistemi ad alto rischio devono sempre essere posti nelle condizioni di "a) comprendere correttamente le capacità e i limiti pertinenti del sistema di IA ad alto rischio ed essere in grado di monitorarne debitamente il funzionamento, anche al fine di individuare e affrontare anomalie, disfunzioni e prestazioni inattese; b) restare consapevole della possibile tendenza a fare automaticamente affidamento o a fare eccessivo affidamento sull'output prodotto da un sistema di IA ad alto rischio ('distorsione dell'automazione'), in particolare in relazione ai sistemi di IA ad alto rischio utilizzati per fornire informazioni o raccomandazioni per le decisioni che devono essere prese da persone fisiche; c) interpretare correttamente l'output del sistema di IA ad alto rischio, tenendo conto ad esempio degli strumenti e dei metodi di interpretazione disponibili; d) decidere, in qualsiasi situazione particolare, di non usare il sistema di IA ad alto rischio o altrimenti di ignorare, annullare o ribaltare l'output del sistema di IA ad alto rischio; e) intervenire sul funzionamento del sistema di IA ad alto rischio o interrompere il sistema mediante un pulsante di 'arresto' o una procedura analoga che consenta al sistema di arrestarsi in condizioni di sicurezza".

Gli operatori devono quindi essere adeguatamente formati per comprendere il funzionamento del sistema, valutare criticamente i suoi risultati ed evitare una dipendenza cieca dall'IA. La sorveglianza umana è essenziale in settori particolarmente delicati come la sanità, la giustizia e la sicurezza pubblica, nei quali un possibile errore del sistema automatizzato potrebbe avere conseguenze gravi sui diritti e sulle libertà fondamentali delle persone.

Quanto sopra premesso in tema di sistemi IA ad alto rischio trova piena applicazione, come già debitamente esplicitato, nel settore sanitario³¹.

Con esplicito riferimento alle cure preventive³², si sottolinea come i sistemi di IA stiano trasformando queste ultime in modo radicale, offrendo strumenti innovativi per migliorare la diagnosi precoce, la personalizzazione dei trattamenti e il monitoraggio della salute.

L'apporto di maggior rilievo dell'IA nel settore preventivo si individua certamente nell'ampia attività di studio e ricerca svolta *ex ante*; infatti, l'utilizzo di algoritmi avanzati, attraverso i quali è possibile analizzare una quantità massiva di dati appartenenti a un numero indefinito di soggetti aventi medesime caratteristiche e patologie, permette di rilevare segnali precoci di tumori o malattie cardiovascolari prima che i sintomi diventino evidenti³³. L'utilizzo di questi sistemi permette sia lo studio di grandi quantità di dati sanitari³⁴, con l'obiettivo di individuare e prevenire una patologia in fase di proliferazione, che una generale personalizzazione delle cure erogate ai singoli pazienti.

Grazie all'analisi avanzata dei dati, l'IA può prevedere la predisposizione a determinate patologie, suggerendo strategie personalizzate per uno stile di vita più sano. Algoritmi intelligenti supportano la diagnosi precoce attraverso l'analisi automatizzata di esami medici, aumentando l'accuratezza e riducendo i tempi di rilevamento

³¹ T. CANTELMÌ, L. LODEVOLE, *Nuove prassi e norme per un sistema sanitario "smart": ricadute dell'AI Act sulla relazione di cura*, in *Rivista italiana di informatica e diritto*, 2024, pp. 607-630.

³² Le cure preventive sono interventi medici e pratiche sanitarie volte a prevenire l'insorgenza di malattie o a ridurre il rischio di complicazioni future. Le stesse si dividono in tre macrocategorie. Le cure preventive primarie hanno come obiettivo quello di evitare la manifestazione di una malattia attraverso strumenti quali le vaccinazioni, l'alimentazione sana, l'attività fisica, lo screening e l'uso di dispositivi di sicurezza; le cure preventive secondarie servono a individuare le malattie nelle fasi iniziali, prima che causino sintomi gravi; le cure preventive terziarie puntano a limitare le complicanze di una malattia già diagnosticata, migliorando la qualità di vita.

³³ G. GRECO, *Intelligenza artificiale e cure primarie: tecnologie e sfide*, 2022, in *AGENAS*, <https://www.agenas.gov.it/images/articolo-16.pdf>.

³⁴ I dati sensibili rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. Il medesimo paragrafo introduce un divieto generale di trattamento dei suindicati dati sensibili, prevedendo, al secondo paragrafo, una disciplina di deroga particolarmente ampia che individua soprattutto nelle esigenze sanitarie la propria fonte.

di tumori, malattie cardiache e altre condizioni critiche. Inoltre, i sistemi di monitoraggio basati su IA aiutano i pazienti affetti da patologie croniche a mantenere sotto controllo i loro parametri vitali, prevenendo complicazioni altrimenti non rilevabili. L'uso di chatbot e assistenti virtuali rende più accessibili consigli medici personalizzati, mentre l'IA applicata ai *big data* epidemiologici consente di prevedere e contenere la diffusione di malattie infettive. In questo scenario, la tecnologia sta contribuendo a un modello sanitario sempre più preventivo e predittivo, riducendo costi e migliorando la qualità della vita.

In ambito medico si suole utilizzare due terminologie per affrontare il tema qui-vi analizzato; la medicina personalizzata e d'iniziativa. La prima si definisce come la medicina che adotta un approccio integrato per la prevenzione, diagnosi, cura e monitoraggio di patologie complesse, basandosi sull'analisi dettagliata delle caratteristiche individuali dei pazienti, permettendo quindi di personalizzare le cure in modo capillare³⁵. La medicina d'iniziativa mira invece a prevenire l'insorgenza delle patologie attraverso un sistema di controlli e di monitoraggio, identificando i fattori di rischio e intervenendo prima dell'insorgenza delle malattie³⁶.

Nel settore sanitario, quindi, sono già affermati da molti anni sistemi tecnologici che appaiono oggi imprescindibili; questi ultimi, quali il *machine learning* e il *deep learning*, migliorano la precisione diagnostica e la personalizzazione dei trattamenti. Gli strumenti tecnologici citati necessitano però di un'ampia quantità di dati per poter espletare al meglio le proprie funzioni; infatti, solamente attraverso lo studio di molteplici informazioni e dati, sarà possibile affrontare determinati casi, realizzando un'attività di comparazione e confronto con antecedenti simili.

Nel campo del monitoraggio, l'AI permette di raccogliere dati in tempo reale su molteplici parametri vitali, quali la frequenza cardiaca, la pressione sanguigna e i livelli di ossigeno nel sangue. Il sistema automatizzato analizza i dati alla ricerca di anomalie, riportando agli organi competenti i risultati e le possibili segnalazioni.

Nonostante i benefici sopra richiamati, l'uso dell'IA nel settore delle cure preventive presenta diverse sfide che devono essere gestite con attenzione; infatti, a causa di un utilizzo non consono delle tecnologie qui descritte, possono emergere gravi conseguenze in tema di sicurezza e privacy dei dati personali, aprendo un aspro dibattito sulle implicazioni etiche del relativo utilizzo.

³⁵ Per una maggiore disamina del tema si veda P. CAPPELLETTI, *La Medicina Personalizzata fra ricerca e pratica clinica: il ruolo della Medicina di Laboratorio*, in RIMeL/IJLaM, 2009, pp. 26-32; A. CESARIO, M. D'ORIA, G. SCAMBIA (a cura di), *La medicina personalizzata fra ricerca e cura*, Milano, Franco Angeli, 2020.

³⁶ P. BONANNI *et al.*, *La prevenzione e la medicina di iniziativa*, in *Toscana Medica*, 2010; POLITECNICO DI MILANO, OSSERVATORI DIGITAL INNOVATION, *Life Science: il digitale per accelerare la trasformazione. Convegno di presentazione dei risultati della Ricerca 2024*.

Questi aspetti, come sopra descritto, sono stati parzialmente affrontati dal legislatore europeo, il quale, collocando i sistemi e le apparecchiature mediche all'interno della classificazione dell'IA ad alto rischio, ha inteso vincolare l'utilizzo dei sistemi in sanità a tutte le preclusioni e i controlli già analizzati (si pensi al management del rischio, alla programmazione e previsione dei danni, alla sorveglianza umana, ai plurimi vincoli in tema di produzione e commercializzazione). In questo settore, tuttavia, per poter avere piena contezza delle novità apportate dai sistemi di IA in sanità, sarà necessario attendere la completa attuazione del Regolamento 1689/2024 da parte di tutti gli stati membri; infatti, solamente la piena operatività dei vincoli previsti ai sistemi di IA ad alto rischio permetterà di comprendere appieno le sfide e le rivoluzioni che il sistema delle cure preventive sarà chiamato ad affrontare, in una generale ottica di aggiornamento costante delle apparecchiature atte alla prevenzione e alla diagnosi.

In conclusione, l'approccio basato sul rischio dell'AI Act rappresenta un elemento chiave per bilanciare il potenziale delle nuove tecnologie con la necessità di proteggere i diritti fondamentali. Nel settore delle cure preventive, questa normativa potrebbe favorire una trasformazione epocale, migliorando la qualità della vita e la salute pubblica. Affrontando con attenzione le sfide etiche e normative, l'IA può diventare un alleato prezioso nella costruzione di un sistema sanitario più efficace, equo e sostenibile.

LA COMPLESSA NORMAZIONE DELLA SPERIMENTAZIONE TRA DATI SANITARI, RICERCA SCIENTIFICA E INTELLIGENZA ARTIFICIALE

Federico Laus

1. TELEMEDICINA E DATI SANITARI: ESIGENZE DI RICERCA

L'analisi dell'evoluzione del servizio sanitario in termini di tecnologia a supporto dell'assistenza comprende molteplici profili e richiede specifici approfondimenti a seconda della direzione investigativa assunta. È evidente che il tema, in principio, investe questioni organizzative, infrastrutturali, di pianificazione e programmazione degli investimenti, alle quali il legislatore e l'amministrazione devono affrettarsi a rispondere. Il moderno modello di servizio sanitario non può, infatti, prescindere dal ricorso ad ogni strumento e risorsa che l'evoluzione tecnologica e scientifica ha prodotto, rischiando altrimenti l'obsolescenza, ma occorre che la tecnicizzazione del servizio sia compensata da una infrastruttura di regole e procedure che permettano ai professionisti di raggiungere l'obiettivo, ossia assistere il paziente.

Tra i temi connessi alle criticità attuative della telemedicina, non può negarsi la rilevanza della normativa sulla gestione dei dati sanitari, d.lgs. 196/2003, già modificato dal d.l. 19/2024 e, d'ora innanzi, oggetto di un progressivo aggiornamento ad opera del Regolamento (UE) 2025/327 sullo spazio europeo dei dati sanitari, così come della normativa sulla intelligenza artificiale Regolamento (UE) 2024/1689, nella prospettiva di una più diffusa adozione nell'assistenza sanitaria.

Indubbiamente la maggiore difficoltà che incontra l'evoluzione del servizio sanitario è rappresentata dall'incalzante successione di normative e dal dialogo che si genera tra ricerca e assistenza, utilizzo dei dati sanitari e implementazione di nuove tecnologie. Il rapporto tra ricerca scientifica, sperimentazione normativa e intelligenza artificiale incide sulla telemedicina, quale insieme di prestazioni che possono essere offerte solo dopo una adeguata maturazione normativa e scientifica.

La ricerca scientifica rappresenta il motore del servizio sanitario e non potrebbe essere altrimenti. Tuttavia, occorre che la normativa che ad essa è rivolta sia efficace.

Partendo dalla normativa italiana che, in parte, ha anticipato la normativa europea, reagendo alle esigenze della ricerca, il d.lgs. 196/2003 ha dedicato alla ricerca scientifica alcune specifiche deroghe alle regole altrimenti applicabili al trattamento dei dati sanitari. Significativo è che l'ultimo rilevante aggiornamento della normativa italiana sia intervenuto con il citato d.l. 19/2024, recante ulteriori disposizioni urgenti per l'attuazione del Piano nazionale di Ripresa e Resilienza.

Disciplinato tra l'altro dall'art. 2-*septies* d.lgs. 196/2003 e dall'art. 9 Regolamento (UE) 2016/679 (c.d. GDPR), riassuntivamente il trattamento dei dati genetici e relativi alla salute è ammissibile ove sia prestato l'esplicito consenso da parte del soggetto interessato, ove sussistano motivi di interesse pubblico rilevante o sussistano ragioni di interesse pubblico nel settore della sanità pubblica, nonché per finalità di cura (precisamente ove sussistano finalità di medicina preventiva, diagnosi, assistenza o terapia sanitaria o sociale, oltre che amministrative e di gestione con riguardo ai servizi sanitari o sociali), oltre che ove si perseguano fini di ricerca scientifica. Il tutto, ferma l'osservanza di misure di garanzia, quali misure di sicurezza (tecniche di cifratura e di pseudonimizzazione) e misure di minimizzazione.

Se da un lato il trattamento dei dati sanitari per finalità di cura, inteso anche come uso primario dei dati, parrebbe non destare perplessità, l'utilizzo della telemedicina e delle nuove tecnologie ha imposto specifici chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario ad opera del Garante per la protezione dei dati sanitari. Nello specifico, con il provvedimento n. 55 del 7 marzo 2019 l'Autorità garante ha precisato che i trattamenti di cura che non richiedono il consenso sono quelli "necessari" al perseguimento delle specifiche "finalità di cura" previste dalla norma, cioè quelli essenziali per il raggiungimento di una o più finalità determinate ed esplicitamente connesse alla cura della salute. Gli eventuali trattamenti attinenti solo in senso lato alla cura, ma non strettamente necessari, richiedono, quindi, anche se effettuati da professionisti della sanità, una distinta base giuridica da individuarsi, eventualmente, nel consenso dell'interessato o in un altro presupposto di liceità.

Con riferimento ai trattamenti in ambito sanitario che non rientrano nelle ipotesi di cura e, quindi, che richiedono il consenso esplicito dell'interessato, sono stati individuati, per quanto di nostro interesse, i trattamenti connessi all'utilizzo di App mediche, attraverso le quali autonomi titolari raccolgono dati, anche sanitari, dell'interessato, per finalità diverse dalla telemedicina oppure quando, indipendentemente dalla finalità dell'applicazione, ai dati dell'interessato possano avere accesso soggetti diversi dai professionisti sanitari o altri soggetti tenuti al segreto professionale.

Quanto all'utilizzo dei dati sanitari in ricerca, nell'ambito del c.d. uso secondario dei dati, la normativa italiana, ai sensi dell'art. 110 del codice privacy, ha anticipato parzialmente il favore derogatorio riconosciuto alla ricerca scientifica dal Regolamento (UE) 2025/327, che tuttavia vedrà attuazione solo tra il 2027 e il 2031. Nel

2024 (d.l. 19/2924) viene prevista l'eliminazione della consultazione preventiva del Garante, ferma la possibilità per il Garante di fissare garanzie con regole deontologiche. Già dal 2018, in forza della modifica recata dal d.lgs. 101/2018, il consenso dell'interessato per il trattamento dei dati relativi alla salute, a fini di ricerca scientifica in campo medico, biomedico o epidemiologico, non è più necessario quando la ricerca è effettuata in base a disposizioni di legge o di regolamento o al diritto dell'Unione europea o quando la ricerca rientra in un programma di ricerca biomedica o sanitaria, ferma resta la elaborazione e pubblicazione di una valutazione d'impatto ai sensi degli artt. 35 e 36 del GDPR. Inoltre, il consenso non risulta necessario se 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 (ad esempio, in caso di interessati deceduti o nel caso non ci siano informazioni sufficienti per il contatto oppure per motivi etici).

In tali casi, il titolare del trattamento deve adottare misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, e il programma di ricerca deve essere oggetto di motivato parere favorevole del competente comitato etico a livello territoriale. Tuttavia, dal 2018 fino alla più recente modifica, occorre, inoltre, la previa consultazione del Garante, quale obbligo per il titolare del trattamento di richiedere un'autorizzazione preliminare speciale, caso per caso, al Garante. Come immaginabile, tale previsione ha avuto un impatto insostenibile per la ricerca, non potendo più basarsi su autorizzazioni generali (adottabili nella diversa previsione ante 2018), ma dovendo chiedere autorizzazioni *ad hoc*. Se da un lato il Garante aveva frequentemente risposto positivamente alle richieste di autorizzazioni, l'iter della ricerca era certamente complicato in termini di tempi e burocrazie, limitando l'operatività dei ricercatori nella realizzazione tempestiva e competitiva dei progetti.

Per contro, le privilegiati autorizzazioni generali, invece, garantivano un minor sforzo procedimentale per il Garante, un risparmio di tempo per il titolare del trattamento (ossia per l'istituto di ricerca), nonché la prevedibilità del risultato di tutela, prevedendo apparati omogenei di regole e misure di sicurezza, nonché profili di responsabilità al quale adeguare le strutture degli enti di ricerca.

Come anticipato, con l'ultima modifica del 2024, pur confermando le deroghe al consenso, viene eliminata l'obbligo della autorizzazione preventiva del Garante, pur restando l'onere consultivo del comitato di bioetica. Viene invece prevista la facoltà in capo al Garante di individuare le garanzie nell'ambito delle regole deontologiche, pur non costituendo un ritorno al regime delle autorizzazioni generali, in quanto non costituiscono precondizioni al trattamento¹.

¹ Sul punto, per maggiori e più approfondite considerazioni, L. BOLOGNINI, S. ZIPPONI (a cura di), *Privacy e diritto dei dati sanitari*, Milano, Giuffrè, 2024, in particolare da pp. 207 a 236.

L'attuale versione dell'art. 110 parrebbe idonea a consentire una maggiore efficacia e rapidità nella predisposizione di progetti di ricerca, necessari per giungere allo sviluppo delle nuove tecnologie in ambito sanitario.

In tale contesto normativo italiano, si inserisce il recentissimo Regolamento (UE) 2025/327 sullo spazio europeo dei dati sanitari. Le nuove tecnologie in sanità sono avide di dati sanitari, la cui circolazione ed il cui utilizzo rappresentano il presupposto indefettibile della efficacia stessa della tecnologia. Il maggiore ostacolo all'utilizzo dei dati sanitari elettronici, inteso tanto come uso primario quanto come uso secondario², è rappresentato indubbiamente dalla disomogeneità di attuazione e interpretazione dell'RGPD da parte degli Stati membri, ove autorità nazionali hanno fornito linee più o meno restrittive all'utilizzo dei dati stessi.

La precedente (anche se attualmente ancora in parte vigente dato il rinvio dell'entrata in vigore di numerosi articoli della novella) regolamentazione dell'accesso ai dati sanitari, oltre a produrre ostacoli alla cura, impedisce alle persone fisiche di beneficiare di cure innovative. Peraltro, tale situazione non consente ai responsabili delle politiche di reagire in modo efficace a una crisi sanitaria, a causa degli ostacoli che impediscono l'accesso a ricercatori, innovatori, regolatori e responsabili delle politiche ai necessari dati sanitari elettronici³. Inoltre, a causa delle differenti norme

² Al riguardo si ricorda che il Regolamento (UE) 2025/327 all'art. 2, comma 2, individuando le definizioni utili alla lettura del regolamento definisce alla lettera d), l'uso primario, come il trattamento dei dati sanitari elettronici per la prestazione di assistenza sanitaria al fine di valutare, mantenere o ripristinare lo stato di salute della persona fisica cui si riferiscono tali dati, comprese la prescrizione, la dispensazione e la fornitura di medicinali e dispositivi medici, nonché per i pertinenti servizi sociali, amministrativi o di rimborso. Diversamente, l'uso secondario viene definito alla lettera f), come il trattamento dei dati sanitari elettronici per le finalità indicate al capo IV del presente regolamento, che sono diverse dalle finalità iniziali per le quali tali dati sono stati raccolti o prodotti.

³ Anche ogni innovativo percorso di cura appare condizionato enormemente dalla disciplina di accesso ai dati. Si pensi ai provvedimenti del Garante per la privacy (n. 415, 416, 417 del 15 dicembre 2022), poi annullati, con cui aveva sanzionato tre Asl friulane, responsabili di aver classificato gli assistiti in relazione al rischio di avere o meno complicità in caso di infezione da Covid-19, mediante algoritmi ed impiegando dati sanitari, senza previo consenso allo specifico trattamento. Le Asl avevano elaborato i dati presenti nelle banche dati aziendali allo scopo di attivare nei confronti degli assistiti opportuni interventi di medicina di iniziativa e individuare per tempo i percorsi diagnostici e terapeutici più idonei. Nel corso dell'istruttoria dell'Autorità, che si era mossa dopo la segnalazione di un medico, è infatti emerso che i dati degli assistiti erano stati trattati in assenza di una idonea base normativa, senza fornire agli interessati tutte le informazioni necessarie (in particolare sulle modalità e finalità del trattamento) e senza aver effettuato preliminarmente la valutazione d'impatto prevista dal Regolamento UE in materia di protezione dati. L'Autorità ha ribadito che la profilazione dell'utente del servizio sanitario, sia regionale o nazionale, determinando un trattamento automatizzato di dati personali volto ad analizzare e prevedere l'evoluzione della situazione sanitaria del singolo assistito e l'eventuale correlazione con altri elementi di rischio clinico, può essere effettuata solo in presenza di un idoneo presupposto normativo, nel rispetto di requisiti specifici e garanzie adeguate per i diritti e le libertà degli interessati, mancanti nel caso di specie. Accertate dunque le violazioni e valutato che nel caso specifico le operazioni, attraverso l'uso di algoritmi, avevano riguardato dati sulla salute di un ingente numero di assistiti, il Garante aveva ordinato a ognuna

e dell'interoperabilità limitata, i fabbricanti di prodotti di sanità digitale e i prestatori di servizi di sanità digitale che operano in uno Stato membro, incontrano ostacoli e costi aggiuntivi nell'accedere a un altro Stato membro.

Con riguardo alla telemedicina, il Regolamento (UE) 2025/327 ricorda, al Considerando n. 28, che la telemedicina sta diventando uno strumento sempre più importante in grado di fornire ai pazienti l'accesso all'assistenza e fare fronte alle disuguaglianze e che ha il potenziale di ridurre le disuguaglianze sanitarie e rafforzare la libera circolazione dei cittadini dell'Unione a livello transfrontaliero. Ad esempio, gli strumenti digitali e altri strumenti tecnologici possono agevolare la fornitura dell'assistenza nelle regioni remote. Quando i servizi digitali accompagnano l'erogazione fisica di un servizio di assistenza sanitaria, il servizio digitale dovrebbe essere considerato parte integrante dell'intera prestazione di assistenza.

Orbene, se ai sensi dell'art. 168 del trattato sul funzionamento dell'Unione europea (TFUE), gli Stati membri sono responsabili della loro politica sanitaria, in particolare dell'organizzazione e dell'erogazione dei servizi sanitari e dell'assistenza medica, secondo il legislatore europeo le diverse politiche in materia di assistenza sanitaria non dovrebbero tuttavia costituire un ostacolo alla libera circolazione dei dati sanitari elettronici nell'ambito dell'assistenza sanitaria transfrontaliera, ad esempio in relazione alla telemedicina ed ai servizi farmaceutici online.

La realizzazione dello spazio europeo dei dati sanitari richiede un accesso sicuro ai dati sanitari elettronici, anche in situazioni transfrontaliere, mediante servizi di accesso ai dati sanitari elettronici e servizi di telemedicina che dovrebbero consentire alle persone fisiche di esercitare i propri diritti indipendentemente dal loro Stato membro di affiliazione e dovrebbero pertanto supportare l'identificazione delle persone fisiche mediante qualsiasi mezzo di identificazione elettronica.

La creazione della nuova infrastruttura di sanità digitale transfrontaliera, quale la piattaforma centrale di interoperabilità per la sanità digitale LaMiaSalute@UE (MyHealth@EU), dovrebbe favorire e agevolare lo scambio di dati sanitari elettronici personali tra i punti di contatto nazionali per la sanità digitale degli Stati membri e consentire agli Stati membri di erogare servizi supplementari in grado di agevolare la telemedicina, la sanità mobile, l'accesso da parte delle persone fisiche alle traduzioni esistenti dei loro dati sanitari e lo scambio o la verifica di certificati sanitari, nonché servizi a sostegno della sanità pubblica e della vigilanza della sanità pubblica o di sistemi, servizi e applicazioni interoperabili di sanità digitale, al fine di conseguire un elevato livello di fiducia e sicurezza, migliorare la continuità dell'assistenza e garantire l'accesso a un'assistenza sanitaria sicura e di elevata qualità.

Occorrerà attendere la definizione, con atti di esecuzione da parte della Commissione, degli aspetti tecnici di detti servizi supplementari.

delle tre Aziende di pagare la sanzione di 55.000 euro e di procedere alla cancellazione dei dati elaborati;
<https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9845339>.

2. SPERIMENTAZIONE E INTELLIGENZA ARTIFICIALE

Per sostenere il processo di innovazione, il Regolamento (all'art. 19) chiede agli Stati membri a designare autorità di sanità digitale competenti per la pianificazione e l'attuazione di norme per l'accesso ai dati sanitari elettronici e per la loro trasmissione, nonché per l'applicazione dei diritti delle persone fisiche e dei professionisti sanitari, sotto forma di autorità separate o come parte di autorità già esistenti.

Legandoci al tema qui introdotto, nello svolgimento dei loro compiti, le autorità di sanità digitale dovrebbero cooperare con il comitato europeo per l'intelligenza artificiale istituito dal Regolamento (UE) 2024/1689. Ciò anche in considerazione del fatto (particolarmente rilevante per l'evoluzione del servizio sanitario digitale) che l'attività di *training* di sistemi di intelligenza artificiale e algoritmi quali finalità lecite di uso secondario. Difatti, se la fornitura dei dati dovrebbe favorire attività correlate alla ricerca scientifica, in tale nozione di ricerca scientifica il regolamento ricomprende lo sviluppo tecnologico e la dimostrazione, la ricerca fondamentale, la ricerca applicata e la ricerca finanziata da soggetti privati. Le attività correlate alla ricerca scientifica comprendono le attività di innovazione quali l'addestramento di algoritmi di intelligenza artificiale che potrebbero essere utilizzati nell'assistenza sanitaria o nella cura delle persone fisiche, nonché la valutazione e l'ulteriore sviluppo di algoritmi e prodotti esistenti a tali fini.

Pur considerata l'inevitabile interazione tra normative diverse, il Regolamento (UE) 2025/327 lascia impregiudicati i Regolamenti (UE) 2017/745, (UE) 2017/746 e (UE) 2024/1689 per quanto riguarda la sicurezza dei dispositivi medici, dei dispositivi medico-diagnostici in vitro e dei sistemi di intelligenza artificiale (IA) che interagiscono con i sistemi di cartelle cliniche elettroniche.

In particolare, il Regolamento (UE) 2024/1689 che stabilisce regole armonizzate sull'intelligenza artificiale (AI Act), ha prestato particolare attenzione alla regolazione giuridica della sperimentazione e della immissione nel mercato dei prodotti tecnologicamente avanzati.

Il Regolamento (UE) 2024/1689 mira a incoraggiare lo sviluppo e l'adozione di sistemi di intelligenza artificiale (IA) sicuri e affidabili in tutto il mercato unico dell'Unione europea (Unione) sia nel settore pubblico che in quello privato, garantendo al contempo la salute e la sicurezza dei cittadini dell'Unione e il rispetto dei diritti fondamentali

È emersa, infatti, una chiara esigenza di gestione del rischio⁴, che il regolamento approccia tanto in termini di regolazione del mercato quanto di monitoraggio, attività affidate principalmente alle amministrazioni pubbliche nazionali.

⁴ Al proposito L. FLORIDI, *Soft Ethics and the Governance of the Digital*, in *Philosophy & Technology*, n. 31, 2018, p. 1 ss., ha rilevato che “the real challenge is no longer digital innovation, but the governance

La mutevolezza della tecnologia, centrale in un sistema di *machine learning*, fa sì che l'incertezza del rischio sia esponenziale, e impone, come misura di salvaguardia, la sorveglianza umana dalla fase di progettazione e durante tutto il ciclo di vita dei prodotti e dei sistemi di IA.

Su queste premesse, il regolamento predilige un approccio alla gestione del rischio debole⁵, nel senso di un approccio normativo orizzontale all'IA, equilibrato e proporzionato, che si limiti ai requisiti minimi necessari per affrontare i rischi e i problemi ad essa collegati, senza limitare od ostacolare indebitamente lo sviluppo tecnologico o altrimenti aumentare in modo sproporzionato il costo dell'immissione sul mercato di soluzioni di IA⁶.

Il regolamento stabilisce norme basate sul rischio per quanto riguarda l'immissione sul mercato, la messa in servizio e l'utilizzo di taluni sistemi IA; il divieto di determinate pratiche di IA; i requisiti e gli obblighi relativi ai sistemi di IA ad alto rischio; la trasparenza per taluni sistemi di IA; la trasparenza e la gestione dei rischi per i modelli di IA per finalità generali (modelli IA potenti che supportano i sistemi IA in grado di svolgere una vasta gamma di compiti); il monitoraggio del mercato, la vigilanza del mercato, la governance e l'esecuzione; il sostegno all'innovazione, concentrandosi sulle piccole e medie imprese (PMI) e sulle *start-up*.

Il Regolamento definisce l'utilizzo dell'IA come ad alto rischio, a causa del potenziale impatto sui diritti fondamentali, la sicurezza e il benessere, comprendendo, ad esempio, il complesso dei servizi essenziali, intesi quali sistemi di IA utilizzati dalle autorità pubbliche per valutare l'ammissibilità alle prestazioni e ai servizi di assistenza pubblica (compresi i servizi di assistenza sanitaria), il merito di credito, la valutazione del rischio di assicurazione e la priorità delle risposte di emergenza. Come noto, i sistemi di IA ad alto rischio devono essere immessi sul mercato dell'Unione, messi in servizio o utilizzati solo se soddisfano determinati requisiti obbligatori. In generale, per quanto ci interessa, il Regolamento ha inteso limitare i sistemi di IA identificati come ad alto rischio a quelli che hanno un impatto nocivo significativo sulla salute, la

of the digital" (p. 2), intendendosi riferire "not just to digital governance but also to digital ethics and digital regulation, i.e. to the whole normative map" (p. 4).

⁵ Il riferimento è a R.B. STEWART, *Environmental regulatory decision making under uncertainty*, in T. SWANSON (a cura di), *An Introduction to the Law and Economics of Environmental Policy: Issues in Institutional Design*, Emerald Group Publishing Limited, Bingley, 2002, p. 71 ss., ove l'autore distingue gli approcci alla gestione precauzionale del rischio incerto in debole e forte, sostenendo, in conclusione (pp. 124-126), l'opportunità della regolamentazione preventiva piuttosto che della proibizione o forte limitazione dell'attività "rischiosa".

⁶ L. TORCHIA, *Lo Stato digitale. Una introduzione*, Il Mulino, Bologna, 2023, p. 85 discute di un "equilibrio fra la stabilità e la flessibilità dell'assetto regolatorio, per evitare sia di dettare regole troppo vacue, sia di irrigidire eccessivamente un settore caratterizzato quasi per definizione dalla capacità innovativa".

sicurezza e i diritti fondamentali delle persone nell'Unione, e tale limitazione dovrebbe ridurre al minimo eventuali potenziali restrizioni al commercio internazionale.

Per tale ragione, individuando una soluzione idonea a non condizionare eccessivamente il mercato, allo sviluppo e all'uso di sistemi di IA ad alto rischio si applica innanzitutto misure di maggiore trasparenza. Si prevede, inoltre, che prima che un sistema di IA ad alto rischio sia utilizzato da entità che forniscono servizi pubblici, deve esserne valutato l'impatto sui diritti fondamentali e che i sistemi di IA ad alto rischio e le entità che li usano devono essere registrati in una banca dati dell'Unione.

In merito alla sanità digitale, rilevante è osservare come il considerando 47 ritenga che i sistemi di IA potrebbero avere un impatto negativo sulla salute e sulla sicurezza delle persone, in particolare quando tali sistemi sono impiegati come componenti di sicurezza dei prodotti. Coerentemente con gli obiettivi della normativa di armonizzazione dell'Unione di agevolare la libera circolazione dei prodotti nel mercato interno e di garantire che solo prodotti sicuri e comunque conformi possano essere immessi sul mercato, è importante che i rischi per la sicurezza che un prodotto nel suo insieme può generare a causa dei suoi componenti digitali, compresi i sistemi di IA, siano debitamente prevenuti e attenuati.

Ad esempio, – osserva il legislatore europeo – i robot sempre più autonomi, sia nel contesto della produzione sia in quello della cura e dell'assistenza alle persone, dovrebbero essere in misura di operare e svolgere le loro funzioni in condizioni di sicurezza in ambienti complessi. Analogamente, nel settore sanitario, in cui la posta in gioco per la vita e la salute è particolarmente elevata, è opportuno che i sistemi diagnostici e i sistemi di sostegno delle decisioni dell'uomo, sempre più sofisticati, siano affidabili e accurati.

Pur riconoscendo la sensibilità degli interessi coinvolti, il legislatore non ha in alcun modo inteso ostacolare il progresso tecnologico neppure nel settore sanitario.

Anzi, aprendo la strada al regolamento sulla spazio europeo dei dati già trattato, il considerando 68 dispone che, ai fini dello sviluppo e della valutazione di sistemi di IA ad alto rischio, è opportuno concedere ad alcuni soggetti, come fornitori, organismi notificati e altre entità pertinenti, quali i poli europei dell'innovazione digitale, gli impianti di prova e sperimentazione e i ricercatori, l'accesso a set di dati di elevata qualità e la possibilità di utilizzarli nell'ambito dei settori di attività di tali attori soggetti al presente regolamento. Gli spazi comuni europei di dati istituiti dalla Commissione e l'agevolazione della condivisione dei dati tra imprese e con i governi, nell'interesse pubblico, saranno fondamentali per fornire un accesso affidabile, responsabile e non discriminatorio a dati di elevata qualità a fini di addestramento, convalida e prova dei sistemi di IA. Ad esempio, per quanto riguarda la salute, lo spazio europeo di dati sanitari agevolerà l'accesso non discriminatorio ai dati sanitari e l'addestramento di algoritmi di IA a partire da tali set di dati in modo sicuro, tempestivo, trasparente, affidabile e tale da tutelare la vita privata, nonché con un'adeguata

governance istituzionale. Le autorità competenti interessate, comprese quelle settoriali, che forniscono o sostengono l'accesso ai dati, possono anche sostenere la fornitura di dati di alta qualità a fini di addestramento, convalida e prova dei sistemi di IA.

In tal senso, il Regolamento sull'intelligenza artificiale, all'interno del capo dedicato alle misure a sostegno dell'innovazione e dopo aver introdotto l'obbligo per gli stati membri di prevedere spazi di sperimentazione normativa⁷ per l'IA (entro agosto 2026), con l'art. 59 è intervenuto sull'ulteriore trattamento dei dati personali per lo sviluppo nello spazio di sperimentazione normativa per l'IA di determinati sistemi di IA nell'interesse pubblico.

Ha così sancito che, nello spazio di sperimentazione normativa per l'IA, i dati personali legalmente raccolti per altre finalità possono essere trattati unicamente ai fini dello sviluppo, dell'addestramento e delle prove di determinati sistemi di IA nello spazio di sperimentazione quando i sistemi di IA sono sviluppati per salvaguardare un interesse pubblico rilevante da parte di un'autorità pubblica o di un'altra persona fisica o giuridica e, tra gli altri, nel settore della sanità pubblica, compresi l'individuazione, la diagnosi, la prevenzione, il controllo e il trattamento delle malattie e il miglioramento dei sistemi sanitari.

Premesse tali caratteristiche dello scenario normativo in tema di IA, ecco, dunque, che emerge un intreccio di norme tutte finalizzate, secondo la tendenza che può osservarsi, a garantire l'avanzamento della tecnologia e limitare al necessario gli ostacoli al progresso scientifico. Rispetto a tali sviluppi è estremamente attuale interrogarsi sull'adeguatezza di principi, istituti, organico e strumenti degli apparati pubblici.

⁷ Intendendosi, per spazio di sperimentazione normativa per l'IA, un quadro controllato istituito da un'autorità competente che offre ai fornitori o potenziali fornitori di sistemi di IA la possibilità di sviluppare, addestrare, convalidare e provare, se del caso in condizioni reali, un sistema di IA innovativo, conformemente a un piano dello spazio di sperimentazione per un periodo di tempo limitato sotto supervisione regolamentare.

IL NUOVO REGOLAMENTO EUROPEO SULL'INTELLIGENZA ARTIFICIALE: NUOVE PROSPETTIVE

Luca Dimasi

Non dobbiamo dimenticare [...] che nessuna innovazione è neutrale. La tecnologia nasce per uno scopo e, nel suo impatto con la società umana, rappresenta sempre una forma di ordine nelle relazioni sociali e una disposizione di potere, che abilita qualcuno a compiere azioni e impedisce ad altri di compierne altre. Questa costitutiva dimensione di potere della tecnologia include sempre, in una maniera più o meno esplicita, la visione del mondo di chi l'ha realizzata. Questo vale anche per i programmi di intelligenza artificiale. Affinché questi ultimi siano strumenti per la costruzione del bene e di un domani migliore, debbono essere sempre ordinati al bene di ogni essere umano. Devono avere un'ispirazione etica.

Papa Francesco, discorso pronunciato dal Santo Padre al G7

1 INTRODUZIONE: CRASH DI SISTEMA

Don DeLillo, nel suo romanzo intitolato *Rumore Bianco*, scriveva: “Questa è la ragione d'essere della tecnologia. Da una parte produce fame di immortalità. Dall'altra minaccia l'estinzione universale. La tecnologia è lussuria estrapolata dalla natura”.

Parafrasando queste parole, si potrebbe dire che il dato ineludibile del momento storico che stiamo attraversando è che le macchine ci stanno conducendo verso una visione del mondo a venire destinata a cambiare per sempre il destino dell'umanità.

Nell'idea di robot intelligenti c'è, infatti, qualcosa che ci affascina e al tempo stesso ci terrorizza, alimentando le nostre febbrili visioni di onnipotenza così come la paura, che da esse si genera, di giungere al punto di non ritorno in cui, come affermato da Steve Wozniak, il cofondatore di Apple, saranno gli umani a diventare gli animali domestici di robot super-intelligenti¹.

Nonostante sia molto difficile fare previsioni su un futuro in cui si aggireranno in mezzo a noi macchine sempre più intelligenti, non si può negare che stia diventando una presa di coscienza comune che, in assenza di misure precauzionali estremamente rigorose e complesse, un'Intelligenza Artificiale (da ora in avanti, IA) addestrata anche allo scopo più banale, può presentare serissimi rischi. “La macchina”, scrive Stephen Omohundro nello studio intitolato *The Basic AI Drivers*, “farà

¹ Cfr. M. O'CONNELL, *Essere una macchina*, Milano, Adelphi, 2017.

di tutto [, infatti,] per non farsi spegnere, cercherà di accedere ad altre macchine e di replicarsi, tentando al contempo di procurarsi risorse senza riguardo per la sicurezza di nessuno. Questi comportamenti potenzialmente pericolosi non saranno programmati, bensì dovuti alla natura intrinseca dei sistemi orientati”².

Da questo punto di vista, per gli sviluppatori dell’IA la sfida consisterà, quindi, nel progettare la tecnologia in modo che si comporti come noi desideriamo, e che non si opponga al suo spegnimento. Ecco perché l’espressione “valori umani” ricorre molto spesso nelle discussioni sull’IA, anche se ogni volta risulta molto difficile dare una definizione significativa e precisa di che cosa debba intendersi esattamente con tale espressione. Ad esempio, potremmo immaginare di attribuire il massimo valore alla sicurezza della nostra famiglia e inserire nel robot un imperativo per cui esso non dovrà mai esporre i bambini al benché minimo rischio. È questo, in fondo, il principio che ha ispirato la prima delle tre leggi della robotica elaborate da Isaac Asimov: “Un robot non può recare danno a un essere umano né permettere che, a causa del suo mancato intervento, un essere umano venga danneggiato”.

Eppure, nei fatti, diversamente da quel possiamo pensare – fa notare Mark O’Connell – “non siamo poi così ciecamente orientati a evitare che i nostri figli non subiscano danni. Un’automobile a guida autonoma che osservi con assoluto rigore questa legge, ad esempio, potrebbe considerare il notevole rischio di incidenti lungo il tragitto, e rifiutarsi di portare i nostri figli a vedere l’ultimo film di animazione digitale, che parla delle avventure di un bambino con il suo amico robot”³.

Ecco allora che, invece di inscrivere nel codice sorgente della macchina valori e criteri di scelta impliciti, la soluzione alternativa – proposta anche da Stuart Russell, docente di Informatica all’Università di Berkeley⁴ – potrebbe essere quella di programmarla in modo che impari osservando il comportamento umano. Del resto, anche noi interiorizziamo i nostri sistemi di valori proprio attraverso questo meccanismo, che, così come osservato dallo stesso Russell è, dopotutto, un “fatto biologico [e lo] dimostra ad esempio la nostra avversione al dolore. In parte è un fatto esplicito, nel senso che sono gli altri a insegnarci che non si ruba. Soprattutto, però, osserviamo il comportamento delle persone e ne desumiamo i valori a cui si ispira. Ecco cosa dovrebbero imparare a fare le macchine”.

Non è difficile intuire, da queste brevi premesse, che il problema della regolazione dell’IA è tutt’altro che semplice, dal momento che le questioni che essa pone sono di tal rilevanza da mettere in crisi la capacità del diritto stesso di creare fiducia e sicurezza nel rapporto tra uomo e tecnologia.

² S. OMOHUNDRO, *The Basic AI Drives*, in P. WANG, B. GOERTZEL, S. FRANKLIN, *Artificial General Intelligence 2008: Proceedings of the First AGI Conference*, Amsterdam, IOS Press, 2008.

³ M. O’CONNELL, *Essere una macchina*, cit.

⁴ Stuart Russell è coautore con Peter Norvig, direttore della ricerca di Google, di *Intelligenza artificiale: Un approccio moderno*, il testo base più diffuso nei corsi universitari di informatica sull’IA.

La necessità, per il Legislatore, di confrontarsi con il fenomeno in parola è parsa procedere di pari passo con l'utilizzo sempre più massivo degli strumenti di IA (prima a supporto, e poi) a sostituzione del tradizionale individuo "organico" nel compimento di scelte riferibili agli ambiti più disparati: dalla concessione del credito nel perimetro dell'*agere* bancario⁵ all'amministrazione di sistemi di *trading* ad alta frequenza di strumenti finanziari⁶, dalle scelte in merito alle strategie di *marketing* più adeguate a raggiungere un determinato mercato *target* fino ad ipotizzare una sorta di "delega in bianco" ai sistemi automatizzati di decisione in merito alla gestione di un contratto tra le parti, attraverso una costante azione di definizione, integrazione, e perfino *enforcement*, di quello che, certamente con un discreto senso dell'umorismo, è stato definito un vero e proprio *smart contract*⁷.

Ma non solo. Dall'agire privato a quello pubblico il passo è stato, per il vero, piuttosto breve, essendosi manifestata da tempo la possibilità di utilizzare algoritmi decisionali anche per lo svolgimento di compiti connessi con l'attività della pubblica amministrazione, con il conseguente emergere di ampie riserve – risolte, poi, in senso affermativo – circa la compatibilità di tale processo con il dettato dell'art. 97 Cost. In particolare, è stato sostenuto che "l'assenza di intervento umano in un'attività di mera classificazione automatica di istanze numerose, secondo regole predeterminate (che sono, queste sì, elaborate dall'uomo), e l'affidamento di tale attività a un efficiente elaboratore elettronico appaiono come doverose declinazioni dell'art. 97 Cost. coerenti con l'attuale evoluzione tecnologica"⁸, a condizione, però, che il *software* di elaborazione risponda a principi di piena conoscibilità e imputabilità della decisione⁹.

È, dunque, in questo contesto di costante e apparentemente inarrestabile decodificazione del reale in termini logico-matematici, che si fa strada il *periculum*, insito nella quarta rivoluzione industriale, della rimozione dell'uomo dal centro del ragionamento logico, perché "nella nuova dimensione il potere non è conferito dai dati, ma dalla capacità di elaborarli, e si declina in termini di potere computazionale (quello che aumenta, come insegna la prima legge di Moore, ogni due per tre con

⁵ M. HURLEY, J. ADEBAYO, *Credit Scoring in the Era of Big Data*, in *Yale Journal of Law and Technology*, vol. 18, n. 1, 2017.

⁶ M. WOODWARD, *The Need for Speed: regulatory Approaches to High-Frequency Trading in the United States and the European Union*, in *Vanderbilt Journal of Transnational Law*, vol. 50, n. 5, 2017.

⁷ Cfr. R. PARDOLESI, A. DAVOLA, *Algorithmic legal decision making: la fine del mondo (del diritto) o il paese delle meraviglie?*, in *Questione Giustizia*, 1, 2020. Sul tema dello *smart contract*, v. R. PARDOLESI, A. DAVOLA, "Smart Contract". *Lusinghe ed equivoci dell'innovazione purchasea*, in F. CAPRIGLIONE (a cura di), *Liber Amicorum Guido Alpa*, Padova-Milano, Cedam, 2019.

⁸ S. CRISCI, *Evoluzione tecnologica e trasparenza nei procedimenti "algoritmici"*, in *Dir. internet*, 2019, commento a Cons. Stato, sez. VI, n. 2270/19.

⁹ Cfr. R. PARDOLESI, A. DAVOLA, *Algorithmic legal decision making: la fine del mondo (del diritto) o il paese delle meraviglie?*, cit.

vertiginosa progressione geometrica, facendo apparire banalmente semplice quel che eravamo abituati a concepire come intrattabile)”¹⁰.

Ecco perché, in una proiezione storica delle future prospettive della regolamentazione dei sistemi di IA, la riflessione non può che partire, tornando all’osservazione iniziale, dalla conclamata esigenza di assicurare una perdurante centralità del controllo umano, foriera di una nuova concezione di “umanesimo digitale” capace di coniugare, come meglio si dirà nel prosieguo del presente lavoro, una rinnovata spinta antropocentrica con il ruolo che si ritiene le macchine possano effettivamente rivestire all’interno del dispiegarsi del tessuto sociale.

“Qui si assume stia” – secondo quanto giustamente affermato da Pardolesi e Davola – “la vera linea di confine, da cui discende il consolante monito [...] circa l’ineludibile necessità, proprio per far spazio alle magnifiche sorti e progressive, di una saggia supervisione sul funzionamento dei meccanismi algoritmici, che sottende una magica cifra cooperativa di ‘tecnica al servizio di...’”¹¹.

2. IL DIRITTO CHE VERRÀ: TENTATIVI DI FUTURO DA ARMONIZZARE

Di fronte alle importanti sfide che caratterizzano il rapporto tra l’uomo e la macchina, il modello su cui si basa il (futuro) Regolamento europeo in materia di IA¹² è quello incentrato sul rischio e sulla sua gestione (secondo un processo interattivo continuo eseguito nel corso dell’intero ciclo di vita di un sistema di IA¹³), unitamente a un meccanismo di responsabilizzazione lungo la catena di valore tra fornitori, distributori, importatori, operatori o altri terzi¹⁴.

Il *risk approach*, nella prospettiva europea, consente – sulla scorta di quando già affermato nella Risoluzione 2015/2103¹⁵ – di non ostacolare l’innovazione tecnologica ricorrendo a restrizioni eccessive, ma di governarla sulla base di obblighi e responsabilità proporzionati al grado di rischio introdotto dal sistema utilizzato.

¹⁰ *Ibidem*. Per un maggior approfondimento sul tema, v. M. DURANTE, *Potere computazionale. L'impatto delle ICT sul diritto, società sapere*, Milano, Maltemi, 2019; J. NIEVA-FENOLL, *Intelligenza artificiale e processo*, Torino, Giappichelli, 2019.

¹¹ *Ibidem*.

¹² Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024.

¹³ Art. 9.

¹⁴ Art. 25.

¹⁵ Risoluzione del Parlamento europeo del 16 febbraio 2017 recante raccomandazioni alla Commissione concernente norme di diritto civile sulla robotica. In essa si legge, infatti, che “gli esseri umani [...] si trova[no] ora sulla soglia di un’era nella quale robot, bot, androidi e altre manifestazioni dell’intelligenza artificiale sembrano sul punto di avviare una nuova rivoluzione industriale, suscettibile di toccare tutti gli strati sociali, rendendo imprescindibile che la legislazione ne consideri le implicazioni e le conseguenze legali ed etiche, senza ostacolare l’innovazione” [punto B] dell’Introduzione.

L'obiettivo è quello di delineare un quadro normativo flessibile (si potrebbe dire *by design*), in grado di adattarsi dinamicamente all'evoluzione tecnologica e all'emergere di nuove situazioni da cui potrebbe derivare un *vulnus* ai diritti fondamentali e ai valori dell'Unione.

In particolare, l'atto europeo cerca di trovare un punto di equilibrio tra quattro distinte esigenze:

1. fare in modo che l'IA immessa sul mercato sia sicura per la tenuta dei valori e dei diritti fondamentali;
2. dotare il sistema di una chiara *governance* delle istituzioni europee e nazionali per garantire la *compliance*;
3. favorire gli investimenti nell'innovazione tecnologica assicurando la certezza del diritto;
4. sviluppare il mercato unico europeo¹⁶.

Tale Regolamento, in quanto strumento di *hard law*, rappresenta un *unicum* rispetto alla tendenza, quasi generale di tutti gli altri Stati, di prediligere un'altra tipologia di approccio (di *soft law*), forse per la paura che un eccesso di regolazione possa determinare il soffocamento di un settore ritenuto cruciale, dato il suo pressoché sconfinato potenziale applicativo¹⁷.

Nonostante ciò, com'è stato sottolineato in occasione del primo *AI Safety Summit*¹⁸, la necessità di un'azione internazionale quanto più congiunta, condivisa ed uniforme si pone come obiettivo fondamentale non solo “per aumentare l'accesso all'intelligenza artificiale in modo che le economie in via di sviluppo possano beneficiare del suo enorme potenziale”¹⁹, bensì anche per garantire il suo monitoraggio e mitigare i danni futuri.

I sistemi di IA stanno raggiungendo, infatti, livelli di autonomia via via più avanzati, al punto che le macchine sono in grado oggi, se opportunamente istruite, di imparare ed elaborare soluzioni in maniera (quasi) del tutto autonoma (*machine learning* e *deep learning*)²⁰.

¹⁶ Cfr. M. TUOZZO, *Note intorno al (futuro) Artificial Intelligence Act. Prospettive costituzionali e sfide dell'immigrazione nell'ecosistema digitale*, in *Diritto Pubblico Europeo*, n. 1, 2024.

¹⁷ Cfr. M. GRANIERI, *Una sinopsi comparativa e una prospettiva critica sui tentativi di regolazione dell'intelligenza artificiale*, in *Comp. dir. civ.*, 2, 23.

¹⁸ All'evento, svoltosi nei giorni 1 e 2 novembre 2023, hanno preso parte i governi di 28 paesi, tra cui Stati Uniti, UE e Cina. La sede dell'incontro è stato Bletchley Park, che durante la Seconda guerra mondiale era stato un centro di decrittazione, in cui veniva scardinata la famigerata macchina elettromeccanica tedesca di crittazione chiamata “Enigma”.

¹⁹ Intervento del Segretario generale dell'ONU Antonio Guterres al *World Economic Forum* di Davos (Svizzera) nel gennaio 2024.

²⁰ Sul punto, v. P. BENANTI, *Le macchine sapienti. Intelligenze artificiali e decisioni umane*, Torino, Marietti, 2018.

Ciò ha finito, inevitabilmente, con lo scardinare le tradizionali categorie giuridiche finora utilizzate per offrire copertura giuridica alle continue sfide poste dalla c.d. rivoluzione digitale.

Pur ammettendo di poter condividere la ricostruzione favorevole all'utilizzo dei costrutti giuridici esistenti – facendo tesoro, in pratica, del complesso di disposizioni codicistiche contenute negli artt. 2049-2054 c.c. domestico, ravvisando, come la migliore dottrina non ha mancato di fare, quale elemento fondativo della nascente responsabilità robotica quello della responsabilità “oggettiva” –, non si può non osservare, infatti, come l'avvento (ormai prossimo) di robot dotati di una propria coscienza (in grado, perciò, di agire non secondo schemi prestabiliti, ma con la possibilità di adeguarsi autonomamente alle diverse circostanze), unito alla peculiarità rappresentata dalla circostanza che l'elemento “pensante” di un sistema di IA non è materialmente connesso alla realtà fisica, sia causa di profonda incertezza, posto che occorre introdurre nel novero degli elementi caratterizzanti il sistema delle responsabilità civili anche il concetto di algoritmo, talvolta addirittura governato da remoto, ed elaborato da un soggetto che può (ma non è detto sia) essere coincidente con il produttore del sistema²¹.

Se poi si considera che tale algoritmo viene a sua volta implementato in un *software*, che viene poi caricato all'interno di una componente *hardware*, va da sé che il novero dei soggetti rispetto ai quali si potrebbe sviluppare un rapporto conflittuale si amplia notevolmente, apparendo logico domandarsi quale soluzione potrebbe essere prospettata nel caso in cui il sistema causi un danno ad un soggetto parte contrattuale o terzo. In altre parole, il creatore dell'algoritmo può essere considerato responsabile solo da un punto di vista contrattuale con la società che crea il *software* e lo vende o implementa a sua volta nel robot²²?

Naturalmente, quelle appena presentate sono (per ora) solo delle suggestioni, ma lo sviluppo dell'IA ha dimostrato, in questi ultimi anni, di essere spesso imprevedibile, per cui è bene – quantunque il momento in cui sarà davvero necessario riconoscere anche ai sistemi intelligenti una vera e propria personalità giuridica, con conseguente attribuzione agli stessi di una responsabilità patrimoniale per i danni che saranno in grado di compiere, sembra essere ancora molto lontano – non farsi trovare del tutto impreparati, anche perché potrebbero essere le stesse macchine a domandare il riconoscimento dello *status* di persona.

²¹ Cfr. S. ACETO DI CAPRIGLIA, *Intelligenza artificiale: una sfida globale tra rischi, prospettive e responsabilità. Le soluzioni assunte dai governi unionale, statunitense e sinico. Uno studio comparato*, in *Federalismi.it*, n. 9, 24.

²² A. CANTALDO, F. CAMPARA, *Intelligenza artificiale e diritto. Dai sistemi esperti “classici” ai sistemi esperti “evoluti”*, in G. TADDEI ELMI, A. CANTALDO, *Intelligenza artificiale. Algoritmi giuridici, ius condendum o “fantadiritto”?*, Pisa, Pacini Giuridica, 2020.

Come non rammentare, a tal proposito, l'accorato appello che Andrew Martin, intelligenza artificiale antropomorfa interpretata da Robin Williams, ebbe a rivolgere al "Congresso mondiale": "Come robot avrei potuto vivere per sempre, ma dico a tutti voi, oggi, che preferisco morire come uomo, che vivere per tutta l'eternità come macchina. [Vorrei] essere riconosciuto per chi sono e per ciò che sono. Niente di più, niente di meno. Non per la gloria, per l'approvazione, ma per la semplice verità di questo riconoscimento. È stato l'elemento propulsivo di tutta la mia esistenza e devo riuscire ad ottenerlo, se voglio vivere o morire con dignità".

Sempre in un'ottica futuristica, si dovrà anche fare i conti con la possibilità che la figura corporea (non necessariamente antropomorfa) e la parte cosciente siano tra loro slegate, sicché l'essere "persona" (intesa come "figura umana") potrebbe non essere più considerato condizione indefettibile per il riconoscimento di taluni diritti e doveri²³.

Verrà un tempo, infatti, in cui non solo l'emulazione integrale del cervello umano diventerà realtà e la vita biologica verrà totalmente assorbita dalla tecnologia, bensì sarà possibile realizzare il trasferimento della coscienza umana su di un supporto di tipo elettronico.

Ma senza arrivare a tanto, è sufficiente guardare alla situazione attuale, per rendersi conto che il potenziamento delle capacità umane, tramite l'ibridazione sempre più stretta tra l'uomo e la macchina (si pensi, ad esempio, alla messa a punto di esoscheletri robotici, di impianti cocleari o retinali o ancora alla stimolazione cerebrale), lungi dall'essere un lontano miraggio, rappresenta oggi una concreta possibilità.

Tutto ciò concorre a definire una nuova dimensione dell'umano, quella appunto del "post-umano". Questo congedo dell'umano dall'umano (nelle definizioni più recenti, "post-umano" è inteso, in particolare, nel senso di "meglio dell'umano") rappresenterebbe, quindi, il futuro prossimo dell'uomo, lasciando aperti, però, una serie di interrogativi, a partire dai limiti morali di uno "sfruttamento grettamente egoistico"²⁴ delle nuove opportunità offerte dalle nuove tecnologie.

Senza considerare il fatto che anche la prospettiva stessa del "post-umano" dovrà fare i conti, come già osservava acutamente Stefano Rodotà, con il crescente affermarsi dell'autonomia quale "carattere delle cose", sicché nell'era – che lo stesso Rodotà ha definito "del capitalismo 'automatico'"²⁵ – anche l'autonomia della persona rischia di venire progressivamente eclissata.

²³ Cfr. S. ACETO DI CAPRIGLIA, *Intelligenza artificiale: una sfida globale tra rischi, prospettive e responsabilità. Le soluzioni assunte dai governi unionale, statunitense e sinico. Uno studio comparato*, cit.

²⁴ N. WIENER, *The human use of human beings*, Boston, Houghton Mifflin, 1950.

²⁵ S. RODOTÀ, *Dall'umano al postumano*, discorso pronunciato in occasione dell'inaugurazione dell'anno accademico 2015 presso l'Università di Perugia, che è possibile consultare al seguente link: <https://www.umbriaon.it/2015/wp-content/uploads/2015/04/Stefano-Rodotà.pdf>.

Questa sarà la “sfida definitiva”²⁶ di un conflitto tra uomo e macchina; ed è in questo intreccio tra presente e futuro che si colloca la faticosa definizione di un contesto di regole che abbiano quale finalità, oltre a quella di prevenire i rischi che le nuove tecnologie inevitabilmente portano con sé, di assicurare un “uso umano degli esseri umani”²⁷.

La tecnica, come noto, è nata dall’esigenza di salvaguardare la vita umana (che poi si è evoluta nella ricerca anche del suo miglioramento), ma non possiamo riporre su di essa tutte le nostre speranze di salvezza o almeno non fino al punto da essere disposti a pagare un prezzo molto alto, come quello della definitiva rinuncia alla nostra umanità.

Se vogliamo davvero salvare l’umano, è necessario, perciò, fare in modo che questi non perda la propria identità. Tuttavia, “il problema cruciale non è [tanto] quello del rapporto tra naturale e artificiale, ma quello della distinzione tra uomo e ambiente, tra uomo e mondo dell’uomo”²⁸.

Detto in altri termini, la custodia dell’identità umana, a differenza di quella delle altre specie viventi, non è una questione solamente biologica, ma rappresenta, *in primis*, un fatto culturale. Di fatti, a ben vedere – e lo sottolinea molto bene Francesco Viola – è proprio “l’incompletezza biologica dell’essere umano [a] implic[are] che l’aspetto culturale sia parte costitutiva dell’identità umana”.

Ciò implica, essendo appunto l’uomo, per definizione, un “animale sociale”, che appartiene alla sua stessa natura “la caratteristica di formulare giudizi di valore, di partecipare ad orizzonti di valore che sono in qualche modo comuni all’interno di specifici contesti culturali, di sentirsi obbligato a rispettare i valori e a proporseli come fini dell’azione”²⁹.

Se ciò è vero (ed è vero), non sarà difficile comprendere come la tendenza della tecnica alla ricerca – costi quel che costi – di un esasperato perfezionismo biologico non potrà che condurci ad un progressivo e pericoloso affrancamento dell’umano dai condizionamenti che sono propri della cultura, riducendone financo a distruggerla la composita varietà delle sue forme³⁰.

Il primo corollario di tutto questo discorso è, insomma, questo: la condizione umana è precaria. La seconda ricaduta è anch’essa alquanto evidente (o, perlomeno,

²⁶ *Ibidem*.

²⁷ *L’uso umano degli esseri umani* è il titolo dell’opera, edita nel 1950, di N. Wiener, unanimemente considerato il padre della cibernetica, contenente le riflessioni dell’autore sulle conseguenze delle conquiste della tecnica sull’organizzazione sociale.

²⁸ F. VIOLA, *Umano e post-umano: la questione dell’identità*, in F. Russo (a cura di), *Natura cultura libertà*, Roma, Armando, 2010.

²⁹ *Ibidem*.

³⁰ Sul punto, v. J. BALLESTEROS, *Biotechnología, biolítica, posthumanismo*, in J. BALLESTEROS, E. FERNÁNDEZ (a cura di), *Biotechnología y Posthumanismo*, Cizur Menor, 2007.

dovrebbe esserlo): l'umanità non è garantita dalla genetica ed essere umani è più che sopravvivere come organismi biologici.

Ecco perché, scrive sempre Viola, “i sostenitori del totale riduzionismo della cultura ai processi biologici e neurologici dovrebbero, ben più degli altri, difendere la tesi della protezione della *specie umana così com'essa s'è spontaneamente formata e farsi guardinghi di fronte ad un uso trasformativo delle biotecnologie*, se ritengono che l'umanità sia un valore. Infatti, se viene meno l'umano, non potrà più esserci l'umanità. Non dico che non ci sarebbe più cultura, ma certamente non più cultura ‘umana’ con tutto ciò che essa implica, compreso anche il nostro modo di concepire la scienza e il carattere multiforme del bene”³¹.

Quel che allora resta da capire è come la nostra condizione umana di esseri culturali possa contribuire ad orientare le scelte – sulla questione dei valori, delle norme, della morale e dell'ideologia – che di qui al prossimo futuro il legislatore europeo (e con esso i legislatori del mondo) dovranno compiere di fronte alle sfide sempre più importanti che il progresso tecnologico inevitabilmente porta con sé.

In questo senso, la scelta di fondo cui si ispira l'attuale AI Act europeo rappresenta un primo importante punto fermo nell'approccio alle tecnologie intelligenti. L'idea di una IA che sia “*human centric*” pone, infatti, le basi concrete per raggiungere e mantenere un opportuno equilibrio tra la lecita spinta all'innovazione tecnologica e l'altrettanta legittima volontà di assicurare la maggiore tutela possibile ai diritti fondamentali degli individui, cosicché l'IA possa essere sviluppata e utilizzata in maniera responsabile, sicura, etica e legale. Tale quadro normativo non solo pone l'accento sulla necessità di un costante controllo umano per prevenire, o quantomeno mitigare, i rischi associati all'uso dell'IA, ma introduce anche un modello di responsabilità che spinge verso una maggiore trasparenza e *accountability* degli sviluppatori e degli utilizzatori di queste tecnologie³².

Certamente, com'è stato da più parti osservato, il sistema di norme introdotte dal Regolamento europeo, benché particolarmente esteso e caratterizzato da un alto tasso di burocratizzazione, non è, per il vero, particolarmente dettagliato, essendo per lo più composto da regole “orizzontali” che considerano, ma già lo abbiamo detto, solo la classificazione dei rischi dei sistemi, omettendo di dettare specifiche discipline nei settori più sensibili di maggiore applicazione dell'IA, come la medicina, la comunicazione, i trasporti ecc.

D'altro canto, allo stato attuale, appare irrealistico immaginare che possano essere introdotte regole universali, mancando all'appello, anche a causa dei numerosi conflitti in atto, alcune grandi potenze come la Russia, la Cina e l'India e gli altri

³¹ F. VIOLA, *Umano e post-umano: la questione dell'identità*, cit.

³² Cfr. F. CABITZA, S. STEFANELLI, *Sorveglianza umana dell'IA: cos'è e perché è centrale nell'AI Act*, in *Agenda Digitale*, 21 marzo 2024, consultabile al seguente link: <https://www.agendadigitale.eu/cultura-digitale/sorveglianza-umana-dellai-cose-e-perche-e-centrale-nellai-act/>.

paesi che compongono il gruppo dei BRICS³³. Auspicabilmente, però, occorrerebbe tentare di individuare, se non una disciplina dettagliata, quantomeno le linee direttrici e i principi generali giuridici, prima ancora che etici, per questa nuova forma di globalizzazione che avrà il nome di IA.

3. SULLA FINE E SUGLI INIZI: ABBOZZANDO UNA CONCLUSIONE

“I dati, il codice, le comunicazioni. Nei secoli dei secoli, amen”. È questa l’invocazione che nel film *TechnoCalyps*, girato nel 2006, un giovane coi capelli chiari e gli occhiali, completamente vestito di nero, pronuncia prima di rivolgere una benedizione esoterica ai quattro punti cardinali, in corrispondenza di ciascuno dei quali pronuncia il nome di un profeta del computer: Alan Turing, John Neumann, Charles Babbage e Ada Lovelace. Quel ragazzo, che conclude il rito restando immobile con le braccia spalancate come in croce, è Anders Sandberg ed è un ricercatore, futurista e transumanista svedese.

Quei gesti e quelle parole fanno riflettere. Non sono pochi, infatti, coloro che già oggi pensano che nel prossimo futuro l’IA possa assumere il ruolo di divinità onnipotente, a cui dedicare spazi fisici (chiese o templi, come ogni culto che si rispetti) per interagire con essa³⁴. Ciò a ribadire, come si accennava all’inizio, che siamo ormai arrivati alla soglia della massima evoluzione dell’era del digitale, ma che proprio per questo occorre fare attenzione che qualcosa non finisca irreversibilmente collo sfuggirci di mano.

L’interrogativo di fondo resta sempre lo stesso ed è stato recentemente riproposto anche da Elon Musk che, in occasione della conferenza tecnologica *VivaTech* tenutasi nel 2024 a Parigi, ha concluso il suo intervento invitando gli interlocutori a riflettere

³³ Si tratta di un acronimo, utilizzato in economia internazionale, che individua cinque paesi (Brasile, Russia, India, Cina e Sudafrica) accomunati da alcune caratteristiche simili, tra le quali: la condizione di economie in via di sviluppo, una popolazione numerosa, un vasto territorio, abbondanti risorse naturali strategiche e sono stati caratterizzati, nell’ultimo decennio, da una forte crescita del PIL e della quota nel commercio mondiale. Fu l’analista Jim O’Neill, a fine 2001, a identificare questo nuovo aggregato geoeconomico sulla base di dette comuni caratteristiche.

³⁴ Si pensi, ad esempio, al collettivo *Theta Noir*, fondato nel 2020 da artisti fermamente convinti che prima o poi una macchina si mostrerà benevola nei confronti dell’umanità, ponendo fine alle disuguaglianze che la devastano e aiutandola a costruire un domani migliore. C’è, poi, la c.d. *Turing Church*, che fa capo a un gruppo di ricercatori all’intersezione tra scienza e religione, spiritualità e tecnologia, ingegneria e fantascienza, mente e materia. E prima ancora era nata *The way of the future*, ma chiesa (ormai defunta) fondata nel 2017 dall’ex ingegnere Uber Anthony Levandowski, con l’obiettivo di promuovere la realizzazione, l’accettazione e l’adorazione di una Divinità basata sull’intelligenza artificiale sviluppata attraverso *hardware* e *software*. Come non menzionare, infine, anche il *New Order Technoism*, un collettivo nato nel 2020 con lo scopo di promuovere un mondo tecnologico etico. I suoi seguaci pare stiano lavorando alla costruzione di una superintelligenza automatica chiamata DOOM (*Divine Omniscient Omnifluent Machina*).

proprio su questa domanda: l'IA ci porterà davvero in un'era di libertà o ci costringerà piuttosto a cercare un nuovo significato della nostra esistenza?

Anche il fondatore di Facebook e CEO di Meta Mark Zuckerberg teme un futuro in cui ci inginocchieremo davanti a un essere onnisciente e onnipotente, di cui testimonieremo, pur non potendo vederlo, i miracoli: una conoscenza superiore dalle capacità quasi infinite.

Più ottimista è, invece, la posizione di Bill Gates che, nonostante tutto, continua a vedere nell'IA una forza positiva, soprattutto se utilizzata per migliorare le condizioni di vita o fornire supporto in ambito sanitario.

Certo è che l'idea di una divinità artificiale non è solo una provocazione filosofica, ma ci invita a ragionare seriamente di problemi regolatori, posto che la sperimentazione delle tecnologie di IA in ambienti reali se, da un lato, ha dimostrato tutto il suo potenziale, dall'altro, ha messo in luce anche tutta la difficoltà, data dalla mancanza di un esaustivo compendio di norme che consentano l'integrazione di macchine intelligenti nella realtà (o meglio la loro partecipazione alle azioni e ai contesti sociali reali), con tutte le conseguente in termini di accettazione delle tecnologie di IA e di sperimentazione non solo delle stesse, ma anche delle regole, speciali e derogatorie rispetto a quelle ordinarie, nel loro effettivo funzionamento³⁵.

Da questo punto di vista, l'approccio migliore, al fine di individuare quali potrebbero essere le migliori soluzioni regolatorie da adottare eventualmente a livello generale, pare certamente essere quello ispirato al c.d. "federalismo sperimentale", fondato sull'idea che favorire la differenziazione e la competizione tra i sistemi giuridici può stimolare l'innovazione e la sperimentazione nella ricerca di strumenti normativi d'avanguardia.

In Europa, questo sta già accadendo con la disciplina in materia di dati personali. Il Regolamento (UE) 2016/679 fa proprio, infatti, un meccanismo di delega di poteri agli Stati membri con riferimento alle esenzioni per il trattamento di dati personali ad uso scientifico, storico, statistico ecc., per la valutazione dell'impatto tecnologico e la legittimazione ad agire collettiva. Anche se ciò potrebbe, invero, aprire la strada a possibili problemi di coordinamento tra i vari Stati membri, ciò nondimeno "il fenomeno della sperimentazione locale rende bene l'idea della necessità di spostare anche sul livello territoriale la ricerca di soluzioni volte a verificare l'impatto delle tecnologie robotiche e dell'IA sulle regole giuridiche esistenti nonché in termini di accettabilità delle conseguenze sociali dalle stesse prodotte"³⁶.

In questo senso, si potrebbe immaginare, come già suggerito da Elettra Stradella, di realizzare nello spazio giuridico europeo uno strumento simile alla cooperazione

³⁵ Cfr. E. STRADELLA, *La regolazione della Robotica e dell'Intelligenza artificiale, il dibattito, le proposte, le prospettive, Alcuni spunti di riflessione*, in *Rivista di Diritto dei Media*, 1, 19.

³⁶ *Ibidem*.

rafforzata, attraverso il quale ciascuno Stato sarebbe chiamato a dare il proprio contributo nell'introduzione di sperimentazioni normative sulla robotica e l'IA, per poi verificare, all'esito di un periodo di monitoraggio e di verifica, quali siano state le soluzioni migliori (comprese le *best practices* sia di regolazione che di *self regulation*) che meritano di essere tradotte in termini estesi, vuoi attraverso fonti di *soft law* vuoi di regolazione diretta.

I temi di frontiera rispetto ai quali le Istituzioni europee – e, insieme con esse, il resto del mondo – saranno presto chiamate concentrare i propri sforzi regolari sono del resto molteplici, a cominciare dalle neurotecnologie e dalle loro ricadute sulla sfera dei diritti fondamentali e, segnatamente, sulla “privacy mentale” dei soggetti, con la conseguente necessità di espansione della cornice dei diritti umani nella categoria dei “neurodiritti”³⁷.

Molto importante è anche la centralissima questione della soggettività giuridica e dei diritti ascrivibili alle “*non-human entities with artificial intelligence*”; questione rispetto alla quale uno dei nodi di più difficile soluzione è dato certamente dall'opportunità di estendere o meno ai robot il principio di dignità³⁸.

Insomma, la strada da percorrere è ancora molto lunga ed è difficile prevedere quale sarà l'esito finale del suo percorso.

Una cosa, però, è certa: anche in un tempo in cui la tecnologia finisce con l'allontanare sempre di più l'uomo da sé stesso, poiché esso varca i limiti che sono propri della sua natura, passando da una sfera che non è più naturale, nel regno dell'ibrido e dell'artificiale³⁹, non dobbiamo cadere nella tentazione di pensare che l'uomo sia ormai divenuto un qualcosa di antiquato.

A tal proposito, le riflessioni proposte da Byung-Chul Han sembrano restituirci quella giusta dose di autostima di cui, in quanto umani, abbiamo bisogno arrivati a conclusione di questa breve passeggiata giuridica: “L'intelligenza artificiale impara dal passato, ma il futuro che essa calcola non è futuro vero e proprio. L'intelligenza artificiale è cieca dinanzi agli eventi. Il pensiero dispone invece di un proprio carattere di evento, in quanto lancia nel mondo qualcosa di completamente *Altro*. All'intelligenza artificiale manca proprio la negatività della rottura capace di fare decollare il Nuovo enfaticamente inteso. Essa si limita a perpetuare l'Uguale. Intelligenza significa *scegliere tra* (inter-legere): essa compie solo una scelta tra opzioni *precostituite*, alla fine tra *uno* e *zero*. Non si spinge oltre il precostituito per arrivare, così, all'*ignoto*”⁴⁰.

³⁷ Sul punto, v. M. IENCA, *Tra cervelli e macchine: riflessioni su neurotecnologie e su neurodiritti*, in *notizie di POLITEIA*, 35, 19.

³⁸ Per un maggior approfondimento sul tema, v. F.G. PIZZETTI, *The Robot Sophia as a “New Citizen” of Saudi Arabia: what about granting legal personhood, “citizenship” and eventually dignity to non-human entities with artificial intelligence?*, in *notizie di POLITEIA*, n. 35, 19.

³⁹ Cfr. G. ANDERS, *L'uomo è antiquato?*, Torino, Bollati Boringhieri, 2007.

⁴⁰ BYUNG-CHUL HAN, *Le non cose. Come abbiamo smesso di vivere il reale*, Torino, Einaudi, 2023.

LE POSSIBILI APPLICAZIONI (E BENEFICI) DELL'UTILIZZO DELL'IA NEL MONDO SPORTIVO *

Davide Carmelo Calderone, Angelo Francini

I. OSSERVAZIONI INTRODUTTIVE: SOCIETÀ, SPORT E TRASFORMAZIONE DIGITALE

Nell'immaginario collettivo, molto spesso, almeno in prima battuta e, in particolare, da parte dei tifosi, lo sport è associato alla singola competizione, al singolo incontro, come una partita di basket o di calcio, una gara automobilistica o motociclistica, mentre, sempre di più, gli eventi sportivi, oltre ad essere occasioni di intrattenimento, sono prima di tutto il risultato di una vera e propria industria che occupa un posto considerevole nell'economia, sia italiana che europea¹.

L'organizzazione di eventi sportivi, infatti, è uno dei molteplici ambiti che costituiscono l'industria sportiva, che si contraddistingue per eterogeneità, comprendendo tanto la produzione di abbigliamento, attrezzature e veicoli, con particolare riguardo alla ricerca, finalizzata a potenziare le prestazioni degli sportivi professionisti ma che può dare impulso anche a tutti i relativi comparti, quanto l'organizzazione e gestione dei servizi connessi alla fruizione (trasporti, *hospitality*, ristorazione, *shopping*) e il settore dei media e delle scommesse².

L'importanza economica dell'industria sportiva deriva anche dalle c.d. esternalità positive che conseguono dalla pratica sportiva, in particolare da quella non agonistica, in termini sia di miglioramento della salute collettiva, con notevoli risparmi per i sistemi sanitari nazionali delle spese per la cura di alcune patologie (infarto e disturbi

* Sebbene il lavoro sia il risultato di una riflessione comune, i parr. 1 e 2 sono da attribuire ad Angelo Francini e i parr. 3, 4, 5, 6 e 7 a Davide Carmelo Calderone.

¹ Per una visione critica del rapporto intercorrente tra industria e sport, il rinvio è a H. GAMMELSÆTER, *Sport is not industry: bringing sport back to sport management*, in *European Sport Management Quarterly*, vol. 21, n. 2, 2021.

² S. BASTIANON, *Lo Sport in Europa tra regole di concorrenza e politica industriale*, in *Eurojus*, numero speciale 3 aprile 2023, p. 130.

coronarici, cancro al seno, tumore del colon-retto, diabete di tipo 2, ecc.)³, che di coesione sociale⁴.

Il rilievo economico dell'industria sportiva si è ancor più incrementato con lo sviluppo del comparto degli sport elettronici (c.d. video giochi competitivi)⁵, in conseguenza dell'ampia diffusione della digitalizzazione che, in modo fortemente accelerato, sta coinvolgendo e modificando, più o meno profondamente, tutti i settori economici e tutte le attività della vita quotidiana, incidendo sulle relazioni dei singoli e dei gruppi tra loro e con i soggetti pubblici⁶.

³ Per tutti, il rimando è a C. BOTTARI, *L'assetto costituzionale delle competenze in materia*, in C. BOTTARI, P. D'ONOFRIO, F. FRANCESCHETTI, F. LAUS, R. NICOLAI, G. PARUTO, *Diritto, organizzazione e gestione dello Sport e delle attività motorie*, Bologna, Bologna University Press, 2021, p. 30. Sul tema anche Rapporto Sport 2023 redatto da Istituto per il Credito Sportivo e Sport e Salute, p. 41.

⁴ Sul punto, il rimando è alla Missione 5, componente 2, investimento 3.1, del PNRR italiano cui sono assegnati 700 milioni di euro con lo scopo di puntare “sugli impianti sportivi e la realizzazione di parchi urbani attrezzati, al fine di favorire l'inclusione e l'integrazione sociale, soprattutto nelle zone più degradate e con particolare attenzione alle persone svantaggiate”. Sempre in tema, si rimanda al Punto 37 dell'Agenda 2030 in cui si afferma come “Anche lo sport è un attore importante per lo sviluppo sostenibile. Riconosciamo il crescente contributo dello sport per la realizzazione dello sviluppo e della pace attraverso la promozione di tolleranza e rispetto e attraverso i contributi per l'emancipazione delle donne e dei giovani, degli individui e delle comunità, così come per gli obiettivi in materia di inclusione sociale, educazione e sanità”.

⁵ Il valore economico del mercato degli sport elettronici, a livello mondiale, è stimato per il 2024 in oltre 218 miliardi di dollari, con un bacino di circa 3 miliardi di utenti/appassionati (per il 55% nell'area Asia/Pacifico). Il rimando è, ancora, a S. BASTIANON, *Lo Sport in Europa tra regole di concorrenza e politica industriale*, in *Eurojus*, n.s., 3 aprile 2023, p. 131.

⁶ Vastissima la dottrina in materia; *ex multis*, M.A. STEFANELLI, *Online Dispute Resolution. Regolamentazione europea ed evoluzione normativa*, in M. BERTOLISSI, M. LAMANDINI, R. NANIA (a cura di), *La tutela giurisdizionale effettiva dei diritti. Sfide e prospettive in materia economico-finanziaria nell'ordinamento italiano*, Torino, Giappichelli, 2024; B. BERTARINI, *European Union Digital Single Market. Legal Framework and Challenges*, Milano, Giappichelli, 2023; P. D'ONOFRIO, *La blockchain nell'azione pubblica e privata di governo*, in *Il lavoro nelle pubbliche amministrazioni*, 2, 2022; C. BOTTARI (a cura di), *La salute del futuro. Prospettive e nuove sfide del diritto sanitario*, Bologna, Bononia University Press, 2020; F.A. BELLA, *Tecnologie innovative nel settore salute tra scarsità delle risorse e differenziazione: alla ricerca di un equilibrio difficile*, in *Federalismi*, 2, 2020; G. ALPA (a cura di), *Diritto e intelligenza artificiale*, Pacini Giuridica, Pisa, 2020; B. BERTARINI, *Il quadro giuridico per il mercato unico digitale*, in *Percorsi Costituzionali*, n. 1, 2018; D. CROCCO, G. NEGRI, *La digitalizzazione della società moderna: incidenze e refluente della tecnologia digitale sulle istituzioni pubbliche e il diritto nell'esperienza italiana*, Napoli, 2016; P. DEGLI ESPOSTI, *Essere prosumer nella società digitale: produzione e consumo tra atomi e bit*, Milano, 2015; K. KELLY, *New Rules for the New Economy*, London, 1999; P.A. MERCIER, F. PLASSARD, V. SCARDIGLI, *La società digitale: le nuove tecnologie nella vita quotidiana*, Venezia, 1984.

La cosiddetta crescita digitale della società⁷ e delle imprese⁸, comprese quelle sportive⁹, assegna alle tecnologie dell'informazione e della comunicazione un ruolo centrale, di vero fondamento dei sistemi economici innovativi moderni, per la loro capacità di estrapolare, raccogliere, conservare ed analizzare enormi volumi di dati, garantendo così “la produzione in tempo reale di informazioni idonee ad attribuire un vantaggio competitivo agli interpreti della moderna economia della conoscenza”¹⁰.

In un ampio numero di mercati e comparti, grazie all'utilizzo dei *big data*¹¹, è possibile acquisire informazioni, conoscere caratteristiche di beni e servizi e elaborare

⁷ Report OECD, *How's Life in the Digital Age?: opportunities and risks of the Digital Transformation for people's Well-being*, 2019.

⁸ In tema si vedano l'analisi dell'OECD, *Productivity Growth in the Digital Age*, febbraio 2019, nello specifico, p. 4, e il paper di S. SOBRE, P. GAL, G. NICOLETTI, TIMILLOTIS, *Digital Dividend: Policies to Harness the Productivity Potential of Digital Technologies*, OECD Economic Policy Paper, n. 26, p. 9, che sottolinea come “there is broad consensus that digital technologies can yield positive effects on productivity at the firm and industry level. 3 However, productivity gains from digital adoption are not automatic. They depend crucially on firms' organisational capital and management skills, as well as on their ability to deploy complementary investments and innovations to improve business processes and automate certain routine tasks. In addition, productivity gains can take time to materialise”.

⁹ V. COZZOLI, *Introduzione al Focus su “Imprese e Società sportive”*, in *Il Nuovo Diritto delle Società*, 10, 2024, p. 1645.

¹⁰ A. GIANNACCARI, *La storia dei Big Data, tra riflessioni teoriche e primi casi applicativi*, in *Mercato Concorrenza Regole*, 2, 2017, p. 308.

¹¹ Comunicazione della Commissione del 26 luglio 2023, *Verso uno spazio comune europeo di dati per il turismo: promuovere la condivisione dei dati e l'innovazione in tutto l'ecosistema del turismo*, che richiama come “La strategia europea per i dati ha introdotto spazi comuni europei di dati in campi e settori economici strategici e di interesse pubblico come sviluppi politici essenziali per dare al settore pubblico e privato gli strumenti per sfruttare il valore dei dati a beneficio dell'economia e della società europee”; Comunicazione della Commissione del 25 aprile 2018, *Comunicazione “Verso uno spazio comune europeo dei dati”*, che specifica come “L'innovazione guidata dai dati è un motore essenziale per la crescita e l'occupazione, in grado di accrescere la competitività europea sul mercato globale” e la Comunicazione della Commissione del 2 luglio 2014, *Verso una florida economia basata sui dati*, che aggiunge come l'economia digitale si basi su un vero e proprio bene, caratterizzato da un proprio valore, i cosiddetti *Big Data*, ovvero “grandi quantità di dati di tipo diverso prodotti a grande velocità da numerosi tipi di fonti. La gestione di questi dataset ad elevata variabilità e in tempo reale impone il ricorso a nuovi strumenti e metodi, quali ad esempio potenti processori, software e algoritmi”. Dati in grado di generare un vero e proprio *business* per le società che li detengono mirando, come afferma B. RABAI, *I “Big Data” nell'ecosistema digitale: tra libertà economiche e tutela dei diritti fondamentali*, in *Amministrare*, 3, 2017, p. 408, a “raccogliere e processare informazioni per rivenderle successivamente a terzi, che, a loro volta, ne usufruiscono al fine di consolidare la propria posizione nei mercati di riferimento (attraverso offerte mirate e personalizzate) oppure al fine di acquisire significativi vantaggi competitivi in fette di mercato ancora poco conosciute”. Secondo il Consiglio d'Europa, *Guidelines on the Protection of individuals with regard to the processing of personal data in a world of Big Data*, del 23 gennaio 2017, l'espressione “usually identifies extremely large data sets that may be analysed computationally to extract inferences about data patterns, trends, and correlations”, che richiama altresì la definizione offerta dall'*International Telecommunication Union*, per cui i *Big Data* costituiscono “a

risultati “senza l'intervento umano, tali decisioni sono infatti assunte direttamente da algoritmi e altre forme di intelligenza artificiale”¹² (IA) e proprio l'intelligenza artificiale¹³, consentendo di “trattare grandi quantità di dati in tempo reale” favorisce l'incremento della “produttività in molti settori, ad esempio, la sanità, l'energia, l'agricoltura, l'istruzione e la protezione ambientale”¹⁴, a motivo anche della propria peculiare capacità di *self learning*, e cioè “di essere in grado di evolversi nel tempo sulla base della esperienza acquisita, attraverso l'analisi di dati omogenei e la loro conseguente razionalizzazione e clusterizzazione”¹⁵.

La transizione digitale coinvolge anche l'intero settore sportivo, a partire dalla *performance* dell'atleta, professionista o dilettante, tramite le c.d. *wearable technology*, e dalla relazione con i tifosi e i sostenitori, per mezzo dei canali social o della commercializzazione di innovativi “gadget”, anche i c.d. *Non Fungible Tokens* (o NFT), fino all'assetto

paradigm for enabling the collection, storage, management, analysis and visualization, potentially under real-time constraints, of extensive datasets with heterogeneous characteristics” (ITU 2015. Recommendation Y3600, *Big data. Cloud computing based requirements and capabilities*).

¹² L. CALZOLARI, *La collusione fra algoritmi nell'era dei “big data”: l'imputabilità alle imprese delle “intese 4.0” ai sensi dell'art. 101 TFUE*, in *Rivista di diritto dei media*, 3, 2018, p. 220. In tema, il rinvio è anche a L. AMMANNATI, *Verso un diritto delle piattaforme digitali*, in *Federalismi*, 7, 2019, p. 6, ove si richiama che “l'enorme massa di dati raccolti e disponibili per essere organizzati e utilizzati consente, [...] una segmentazione granulare degli utenti dei servizi e un crescente perfezionamento della profilazione che, a seconda dei mercati, può avere effetti negativi incrementando i profili di rischio come nel caso del mercato assicurativo retail o può avere effetti discriminatori derivanti da politiche di prezzo”.

¹³ In tema di intelligenza artificiale, F. DONATI, *Intelligenza artificiale e giustizia*, in *Rivista AIC*, n. 1, 2020, p. 415; ove l'A. riporta come in via introduttiva “non esiste una definizione generalmente condivisa di IA. Ai nostri fini possiamo definire l'IA come la tecnologia che permette ad un computer di analizzare grandi quantità di dati e, sulla base della conoscenza e dell'esperienza acquisita, adottare comportamenti intelligenti o proporre decisioni. Si tratta, in altri termini, di una tecnologia che permette ad una macchina di svolgere funzioni tradizionalmente riconosciute dalla sola capacità umana”. Vastissima la dottrina in tema, il rinvio è a: G. SALANITRO (a cura di), *Scenari dell'intelligenza artificiale. Uomo e algoritmo nelle scienze sociali*, Pisa, Pacini Giuridica, 2024; F. LAUS, *Organizzazione amministrativa e gestione del rischio nei sistemi di intelligenza artificiale*, in *Inteligencia artificial y administraciones públicas: una triple visión en clave comparada*, Madrid, Iustel, 2024; G. FINOCCHIARO, *Intelligenza artificiale, quali regole?*, Bologna, Il Mulino, 2023; V. FALCE (a cura di), *Strategia dei dati e intelligenza artificiale. Verso un nuovo ordine giuridico del mercato*, Torino, Giappichelli, 2023; G. LEMME, *La transizione giuridica. La crisi del diritto di fronte alla sfida tecnologica*, Torino, Giappichelli, 2023; T.E. FROSINI, *L'orizzonte giuridico dell'intelligenza artificiale*, in *BioLaw Journal*, 1, 2022; G. SARTOR, *L'intelligenza artificiale e il diritto*, Torino, Giappichelli, 2022; R. GIORDANO, A. PANZAVOLTA, A. POLICE, S. PREZIOSI, M. PROTO (a cura di), *Il diritto nell'era digitale. Persona, Mercato, Amministrazione, Giustizia*, Milano, 2022; B. VITIELLO, *L'utilizzo dei dati relativi alla salute*, in C. BOTTARI (a cura di) *La salute del futuro. Prospettive e nuove sfide del diritto sanitario*, Bologna, Bononia University Press, 2020.

¹⁴ Commissione europea, COM (2019) 22, 30 gennaio 2019, *Documento di riflessione Verso un'Europa sostenibile entro il 2030*, p. 29.

¹⁵ M.G. ORTOLANI, *La giustizia predittiva nell'ordinamento giuridico italiano e nei principali ordinamenti di common Law*, in *Annali della Facoltà Giuridica dell'Università di Camerino*, 12, 2023, p. 2.

e all'organizzazione delle società sportive, incluse le modalità di finanziamento con l'offerta di *tokens* o *crypto-assets*, ascrivibili all'ambito delle *Initial Coins Offerings* (o ICOs)¹⁶, “in un contesto in cui il *broadcasting* e le sponsorizzazioni assumeranno via via un peso economico crescente sui ricavi delle società e degli atleti professionisti”¹⁷.

Grazie all'*internet of things*¹⁸ e alle metodologie AI di *machine learning*¹⁹, le attività e i risultati conseguiti dagli atleti vengono convertiti in dati con lo scopo primario di migliorare le prestazioni individuali, registrando ogni informazione relativa ad una specifica azione o mossa, così da focalizzare i punti di forza e di debolezza, dando attuazione pure in ambito sportivo a “quel processo di datizzazione del reale – per cui ogni attività può essere trasformata in un dato –, che consente di rileggere la stessa natura umana, anche dal punto di vista ontologico, non più solo nella sua materialità, ma anche (e principalmente) come produttrice di dati”²⁰.

¹⁶ In tema, il rimando, su tutti, è a M.T. PARACAMPO (a cura di), *FinTech: introduzione ai profili giuridici di un mercato unico tecnologico dei servizi finanziari*, Torino, 2021. Per l'uso degli NFT nel mondo sportivo, M. GALASSO, M.B. SCANNAPIECO, *NFT e Sport. Prospettive applicative ed ostacoli da superare*, in *Il Nuovo Diritto delle Società*, 11, 2022; M. GIULIANO, *I nuovi beni digitali nel quadro normativo europeo*, in *Il Nuovo Diritto delle Società*, 11, 2022; S. RIBERTI, *L'impatto degli NFT nel mondo dello sport: sfide “metagiuridiche”*, in *Il Nuovo Diritto delle Società*, 11, 2022; S. SICILIA, *eSports, Fan Token e NFTV*, in *Il Nuovo Diritto delle Società*, 11, 2022; V. ZAMBRANO (a cura di), *Sport e rivoluzione digitale. Analisi e riflessioni*, Milano, Cedam, 2022.

¹⁷ F. ZATTI, *Sport e trasformazione digitale: questioni giuridiche aperte*, in *Il Nuovo Diritto delle Società*, 9, 2023, p. 1369.

¹⁸ Sul ruolo dell'*Internet of things*, vasta è la dottrina giuridica, *ex multis*, C. CAMARDI, G. NOTO LA DIEGA, *Internet of things and the law*, in *Jus civile*, 4, 2023; M.W. MONTEROSSO, *La circolazione dei dati generati dai prodotti connessi a Internet: luci e ombre del Regolamento europeo sui dati*, in *AIDA*, 1, 2023; G. SAJEVA, *Owning lands, seas, and the internet of things. From the tragedies of the commons to the tragedies of the anti-commons. Introduction*, in *Ragion pratica*, 59, 2022; G.N. LA DIEGA, *I beni comuni nell'età della rimaterializzazione. Internet delle Cose fra apertura e resistenza collettiva*, in *Ragion pratica*, 59, 2022; A. AMBROSINO, “Internet of Things” al servizio della salute e della sicurezza dei lavoratori, in *Diritto della Sicurezza sul Lavoro*, 2, 2022; M. MOLÈ, *The Internet of Things and Artificial Intelligence as Workplace Supervisors: Explaining and Understanding the New Surveillance to Employees Beyond Art. 8 ECHR*, in *Italian Labour Law e-Journal*, 2, 2022; M. RABITTI, *Internet of Things. Intelligenza artificiale e danno: l'incerta attribuzione delle responsabilità*, in L. AMMANNATI, A. CANEPA (a cura di), *Tech Law. Il diritto di fronte alle nuove tecnologie*, Napoli, 2021; G. PEROTTO, *La standardizzazione europea nel settore dell'ICT nell'era dell'“Internet of Things”: qualificazione giuridica e controllo di validità degli standard tecnici armonizzati*, in *Il diritto dell'economia*, 3, 2020; E. PEZZOLI, “Internet of Things”, tecnologia “blockchain” e diritti IP, in *Il Diritto industriale*, 2, 2020.

¹⁹ Si tratta di sistemi nei quali lo sviluppo del “ragionamento” algoritmico diventa, a un certo punto, incomprensibile o comunque non del tutto intellegibile. Questo accade perché la correlazione tra i dati, che consente di estrarre la “regola” su cui si basa la decisione, viene sviluppata dalla macchina, rendendo tale correlazione difficile da comprendere o addirittura sconosciuta, anche a chi ha programmato l'algoritmo e creato il relativo software.

²⁰ F. MATTASSOGLIO, *Sport e innovazione digitale: un cambio di prospettiva non solo giuridico*, in *Il Nuovo Diritto delle Società*, 9, 2023, p. 1327.

2. LA CENTRALITÀ DELLA REGOLAZIONE GIURIDICA NELL'ERA DELLA DIGITALIZZAZIONE: L'AI ACT EUROPEO

L'estesa diffusione della digitalizzazione e del progresso tecnologico e il valore strategico che rivestono ne impongono una regolazione giuridica efficace²¹, così da sfruttarne appieno le opportunità insite, dal momento che “il diritto già da tempo è entrato nella società tecnologica”, potendosi infatti “riformulare l'antico brocardo latino *ubi societas technologica, ibi ius*”²², nella convinzione che “l'era digitale apre a prospettive incredibili e impone a ciascuno di noi di rivedere in radice i propri strumenti di analisi, rimuovendo consolidati paradigmi e superando radicati precetti”²³.

Soprattutto a livello europeo²⁴, è già emersa l'esigenza della definizione di un adeguato contesto normativo, atto a valorizzarne le potenzialità ed i benefici ma pure a fronteggiarne i rischi²⁵ in quanto le enormi potenzialità dell'intelligenza artificiale di tipo generativo, qual è quella della piattaforma di ChatGPT, della società OpenAI, in grado di creare o generare una nuova informazione, di qualsiasi tipologia, utilizzando come base i dati con cui viene alimentata, e la possibilità concreta di arrivare alla profilazione degli individui, grazie alla raccolta di un numero elevatissimo di informazioni in tempi strettissimi, richiedono tanto il coordinamento con la disciplina relativa alla riservatezza, per le implicazioni in tema di tutela dei dati personali, quanto l'adozione di sistemi atti a garantire la correttezza delle informazioni elaborate²⁶.

Non sempre, infatti gli atleti sono “adeguatamente informati sul tipo di aggregazione e rielaborazione dei loro dati, né tantomeno sull'utilizzo che si intende fare sia

²¹ In tema, B. BERTARINI, *La regolamentazione giuridica europea della digitalizzazione quale strumento di crescita economica e sociale*, in S. DOMINELLI, G.L. GRECO (a cura di), *I mercati dei servizi fra regolazione e governance*, Torino, Giappichelli, 2019; M. CLARICH, *Istituzioni, nuove tecnologie, sviluppo economico*, in *Diritto pubblico*, 1, 2017, p. 86, in cui l'A. evidenzia come “uno dei principi fondamentali della nuova regolazione delle autorità indipendenti è quello della neutralità tecnologica. I regolatori non devono, per quanto possibile, privilegiare tecnologie già esistenti delle quali sono in possesso soltanto alcune imprese e categorie di esse. Devono, invece, fissare regole tecnologicamente neutrali in modo da non creare distorsioni nella concorrenza e da non disincentivare il progresso tecnologico”.

²² T.E. FROSINI, *L'orizzonte giuridico dell'intelligenza artificiale*, in *BioLaw Journal, Rivista di BioDiritto*, n. 1, 2022, p. 159.

²³ N. LIPARI, *Diritto, algoritmo, predittività*, in *Rivista trimestrale di Diritto processuale civile*, 3, 2023, p. 730. Sul punto anche M.A. STEFANELLI, *Mercato, consumatori digitali, giustizia predittiva. Le recenti proposte di revisione della normativa europea in materia di soluzione alternativa delle controversie*, in *Percorsi costituzionali*, 2, 2023; F. ROMEO, *Un percorso di machine learning al concetto di diritto*, in *Rivista di filosofia del diritto*, 1, 2020.

²⁴ F. MATTASSOGLIO, *Sport e innovazione digitale: un cambio di prospettiva non solo giuridico*, cit., p. 1325.

²⁵ *Ivi*, p. 1326.

²⁶ Vastissima in tema la dottrina giuridica. Per tutti, F. BRAVO (a cura di), *Dati personali. Protezione, libera circolazione e governance*, vol. 1, *Principi*, Pisa, Pacini Giuridica, 2023.

del dato originale sia del nuovo dato generato. Le società sportive utilizzano i dati rielaborati con finalità economico commerciali al fine della valorizzazione dell'atleta sul mercato, senza che l'atleta ne sia consapevole²⁷.

Già diversi studi sottolineano come talvolta le analisi scaturenti da sistemi di elaborazione automatica si fondino su dati errati o diano esiti scorretti²⁸, oltre che talora discriminatori²⁹, e quanto sia estremamente difficoltoso verificare i risultati e individuare le correlate responsabilità³⁰.

La regolazione si pone, dunque, come condizione fondamentale affinché l'AI espliciti appieno le sue potenzialità, attenuandone i rischi³¹, tanto che si sta sviluppando un nuovo filone di ricerca incentrato su un uso etico dell'IA³², e può contribuire a circoscrivere i dubbi e i timori degli esperti ma pure la diffidenza dell'opinione pubblica.

²⁷ M.L. GUARDAMAGNA, *Machine learning e sport: i problemi legati al trattamento dei dati personali*, in *Il Nuovo Diritto delle Società*, 11, 2022, p. 2087.

²⁸ D.K. CITRON, *Technological Due Process*, in *Wash. Law Review*, 2008, p. 1249 ss.

²⁹ *Ex Multis*, L. AMMANNATI, G.L. GRECO, *Il credit scoring "intelligente": esperienze, rischi e nuove regole*, in *Rivista di Diritto bancario*, 3, 2023; M. RABITTI, *Credit scoring via machine learning e prestito responsabile*, in *Rivista di Diritto bancario*, 1, 2023, p. 184 ss. in cui l'A. specifica come "I bias hanno prodotto, ad esempio, discriminazioni di Gender denunciate nel rapporto *Women World Banking*; discriminazioni per ragioni di razza, religione, orientamenti sessuali ecc. In diversa (ma non meno preoccupante) prospettiva, basti pensare che uno studio recente americano dà conto del fatto, metagiuridico, che vi sono stati algoritmi che hanno tracciato l'attività dei richiedenti credito sui social e hanno rilevato stati di ansia e difficoltà di gestione della propria attività quotidiana, facendo da ciò conseguire una valutazione negativa sulla capacità di adempimento delle obbligazioni contrattuali e di rimborso del finanziamento da parte dei richiedenti. Negli Stati Uniti, il ricorso a *Soft Data* ha portato ad attribuire rilievo anche alle geolocalizzazioni dell'utente, ai contatti social, alle abitudini d'acquisto e di investimento, ma anche ai dati personali, quali quelli sanitari, dando luogo a un acceso dibattito sul rischio di discriminazione, oltre che al rischio di violazione del diritto alla protezione dei propri dati personali. Sebbene in Europa non sia espressamente previsto il diritto a non essere discriminati, questo profilo sta oggi assumendo crescente importanza proprio in considerazione dell'impatto delle nuove tecnologie sui diritti delle persone, in termini di nuove vulnerabilità".

³⁰ F. MATTASSOGLIO, *Sport e innovazione digitale: un cambio di prospettiva non solo giuridico*, in *Il Nuovo Diritto delle Società*, 9, 2023, p. 1328 e J. BURRELL, *How the machine "thinks": Understanding opacity in machine learning algorithms*, in *Big Data & Society*, January-June 2016, pp. 1-12.

³¹ F. MATTASSOGLIO, *Sport e innovazione digitale: un cambio di prospettiva non solo giuridico*, in *Il Nuovo Diritto delle Società*, 9, 2023, p. 1329. In tema di regolazione, più ampiamente, il rimando è per F. PASQUALE, *Le nuove leggi della robotica. Difendere la competenza umana nell'era dell'intelligenza artificiale*, Roma, Luiss University Press, 2021.

³² Sui rischi che possono essere causati dall'utilizzo dell'AI, si veda, in particolare, il nuovo filone di ricerca sulla sua etica, tra cui si deve citare L. FLORIDI, J. COWLS, T.C. KING, M. TADDEO, *How to Design AI for Social Good: Seven Essential Factors*, in *Science and Engineering Ethics*, 26 (3), 2020, p. 1771 ss., in <https://doi.org/10.1007/s11948-020-00213-5>; L. FLORIDI, M. TADDEO, *What Is Data Ethics?*, in *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 2016, 374 (2083): 20160360, in <https://doi.org/10.1098/rsta.2016.0360>.

Il regolamento europeo sull'intelligenza artificiale, adottato dal Consiglio il 21 maggio 2024 ed entrato in vigore il 1° agosto 2024, la cui composizione era stata avviata nella primavera del 2021, mira a promuovere "l'innovazione e l'occupazione [...] rendendo l'Unione un leader nell'adozione di un'IA affidabile"³³ che sia "strumento per le persone, con il fine ultimo di migliorare il benessere degli esseri umani"³⁴.

Scopo del regolamento è "migliorare il funzionamento del mercato interno istituendo un quadro giuridico uniforme in particolare per quanto riguarda lo sviluppo, l'immissione sul mercato, la messa in servizio e l'uso di sistemi di intelligenza artificiale (sistemi di IA) nell'Unione, in conformità dei valori dell'Unione," promuovendo "la diffusione di un'intelligenza artificiale (IA) antropocentrica e affidabile, garantendo nel contempo un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea ('Carta'), compresi la democrazia, lo Stato di diritto e la protezione dell'ambiente, proteggere contro gli effetti nocivi dei sistemi di IA nell'Unione, nonché [...] l'innovazione"³⁵, in modo da poter facilitare gli investimenti e l'innovazione, secondo un approccio proporzionato e basato sul rischio³⁶.

Indicando il rischio ne "la combinazione della probabilità del verificarsi di un danno e la gravità del danno stesso"³⁷; il regolamento assegna particolare rilievo alla qualificazione dei sistemi di AI in base al livello di rischio che possono comportare, suddividendoli in quattro diverse categorie: sistemi che presentano un rischio inaccettabile, che sono vietati; quelli che comportano un rischio elevato, che dovrebbero essere oggetto di attenta regolazione; quelli che presentano un rischio limitato e, infine, quelli a rischio basso o minimo.

In particolare, nelle pratiche vietate dovrebbero essere incluse tutte le casistiche in cui l'uso dell'AI è considerato inaccettabile perché in contrasto con i valori dell'Unio-

³³ Considerando (2) del Regolamento (UE) 2024/1689 del Parlamento Europeo e del Consiglio del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale.

³⁴ Considerando (6) del Regolamento (UE) 2024/1689 del Parlamento Europeo e del Consiglio del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale.

³⁵ Considerando (1) del Regolamento (UE) 2024/1689 del Parlamento Europeo e del Consiglio del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale.

³⁶ G. NATALE, *Intelligenza artificiale, neuroscienze, algoritmi*, Pisa, Pacini Giuridica, 2024, p. 289. In tema, L. FLORIDI, *Soft Ethics and the Governance of the Digital*, in *Philosophy & Technology*, 31, 2018, p. 1 ss., ove l'A. afferma come "the real challenge is no longer digital innovation, but the governance of the digital" (p. 2), riferendosi "not just to digital governance but also to digital ethics and digital regulation, i.e. to the whole normative map" (p. 4). Per la gestione del rischio in genere e nel settore sanitario, il rinvio è a F. LAUS, *L'amministrazione del rischio. Tra regolazione e procedimento, principio di precauzione e approccio multidimensionale*, Milano, Cedam-Wolters Kluwer, 2023.

³⁷ Art. 3, par. 1, punto 2 del Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale.

ne, quali sono i casi di violazione dei diritti fondamentali. I divieti riguardano anche l'utilizzo di metodologie con un potenziale significativo di manipolazione delle persone per mezzo di tecniche subliminali al di là della loro coscienza o di sfruttamento della vulnerabilità di specifici gruppi.

Le ingenti quantità di dati raccolte per mezzo delle nuove tecnologie consentono, tra l'altro, di disporre di informazioni preziose per attuare azioni di tutela della salute, *in primis* dell'atleta, facilitando l'individuazione delle cause degli infortuni e la definizione delle connesse azioni preventive e di recupero, ma anche dell'intera collettività, che può indubbiamente trarre beneficio dai risultati ottenuti.

3. L'IA NELLO SPORT, CONTESTO STORICO E STATO DELL'ARTE

L'utilizzo dell'intelligenza artificiale nel mondo dello sport si è sviluppato molto nel corso degli anni. In una prima fase, l'utilizzo dell'Intelligenza Artificiale era principalmente incentrato sul miglioramento della *performance* individuale degli atleti e sulle tattiche e strategie di gioco della squadra, oltre che nell'analisi delle tattiche utilizzate dagli avversari.

Fino alla fine del XX secolo, la valutazione fisica degli atleti avveniva principalmente attraverso tecniche ed evidenze mediche basate sulla storia clinica, caratterizzata quindi da un approccio più qualitativo. Il cambio di paradigma si verifica alla fine del XX secolo, quando l'analisi statistica e l'utilizzo di dati quantitativi iniziano a integrare le pratiche tradizionali, fino a diventare al giorno d'oggi il punto di partenza per impostare i piani di riabilitazione e di prevenzione per gli atleti.

Le prime applicazioni dell'analisi dei dati nello sport erano basate su dataset statici e su un approccio ancora rudimentale, che non riusciva a sfruttare pienamente il potenziale delle analisi *data-driven*. Intorno al 2010, con l'introduzione di software sempre più sofisticati, si iniziano a sviluppare sistemi avanzati per l'analisi delle *performance* atletiche. Ciò avviene anche grazie al crescente utilizzo di dispositivi indossabili che permettono di registrare e raccogliere i dati biometrici degli atleti in tempo reale.

Con l'arrivo sul mercato di questi strumenti, si è iniziato a parlare di un'intelligenza artificiale più avanzata, basata sul *machine learning*, migliorando la qualità dei suoi output proporzionalmente agli input che riceve. Il *machine learning* riveste un ruolo centrale nell'individuazione di pattern e fattori di rischio, permettendo così di elaborare strategie più efficaci per la prevenzione degli infortuni. È in questo contesto che si sviluppano le prime analisi AI-driven.

A partire dal 2020, assistiamo a programmi di allenamento iper-personalizzati che non prendono in considerazione solo i dati biometrici degli atleti ma integrano anche informazioni relative all'ambiente circostante, come le condizioni climatiche,

la qualità del terreno di gioco e altri fattori esterni che possono influire sulle prestazioni e sul rischio di infortunio.

Oggi, con l'espansione e la costante innovazione dei *Large Language Model* (LLM), parliamo di Intelligenza Artificiale Generativa, meglio conosciuta come GenAI. La GenAI svolge un ruolo cruciale nell'interpretazione dei dati e nel miglioramento della comprensione dei risultati prodotti dai modelli di IA da parte degli staff tecnici. Questo contribuisce a un processo decisionale più informato ed efficace. In particolare, la capacità della GenAI di spiegare in modo chiaro e comprensibile i risultati generati ha portato allo sviluppo di sistemi di *Explainable AI* (XAI), che garantiscono maggiore trasparenza nell'elaborazione delle informazioni e nelle previsioni fornite.

4. SIVIGLIA FC, IBM E META AI: UN CASO STUDIO ATTUALE

Sebbene questo caso studio si riferisca all'applicazione dell'intelligenza artificiale allo scouting, risulta emblematico per descrivere come le soluzioni basate su IA siano sempre più sofisticate ed utilizzate dai migliori club professionistici europei, grazie a collaborazioni con le principali multinazionali del settore come IBM e Meta.

Nel calcio moderno, la gestione della grande quantità di dati rappresenta una sfida sempre più rilevante. L'analisi di oltre 300.000 report di scouting archiviati e il tempo richiesto per elaborare una singola *shortlist* di giocatori – che può raggiungere le 300 ore – evidenziano la necessità di strumenti avanzati per ottimizzare i processi decisionali.

Un caso esemplare di applicazione dell'intelligenza artificiale in questo ambito è rappresentato dall'integrazione di sistemi basati su modelli di apprendimento automatico per il supporto allo scouting e alla selezione dei talenti. In questa prospettiva, la collaborazione tra Sevilla FC, IBM e Meta si configura come un modello innovativo di sinergia tra sport e tecnologia³⁸, in cui la trasformazione digitale non si limita al potenziamento delle capacità analitiche, ma si estende alla ridefinizione delle strategie di gestione e valorizzazione del capitale umano.

Uno degli strumenti più avanzati sviluppati in questo contesto è Scout Advisor, basato su IBM Watsonx e potenziato dal modello Llama 3.1 70B³⁹. L'adozione di tecniche di elaborazione del linguaggio naturale consente di tradurre richieste gene-

³⁸ META AI, *How Sevilla FC is discovering future soccer stars with Llama*, 3 marzo 2025, disponibile su: <https://ai.meta.com/blog/sevilla-fc-scout-advisor-llama-ibm-watsonx/> (ultimo accesso: 17/03/2025).

³⁹ IBM NEWSROOM, *Il Siviglia FC trasforma il processo di reclutamento dei giocatori grazie alla potenza dell'AI generativa di IBM watsonx*, 23 gennaio 2024, disponibile su: <https://it.newsroom.ibm.com/SevillaFC> (ultimo accesso: 17/03/2025).

riche in *query* contestualizzate, ottimizzando la ricerca nel rispetto del gergo tecnico utilizzato dagli analisti di settore.

L'implementazione dell'*Explainable AI* rappresenta un ulteriore elemento di rilievo, in quanto consente di ridurre l'asimmetria comunicativa tra gli specialisti dell'analisi dati e lo staff tecnico, agevolando l'interpretazione dei risultati e l'integrazione delle evidenze analitiche nei processi decisionali. L'accessibilità e la trasparenza del sistema favoriscono una più ampia adozione degli strumenti di intelligenza artificiale nel settore sportivo, contribuendo a migliorare l'efficacia delle valutazioni tecniche e strategiche.

L'intelligenza artificiale applicata allo scouting calcistico non si configura come un sostituto delle competenze umane, ma come un supporto volto a potenziarne le capacità analitiche. L'impiego di modelli avanzati permette di individuare pattern significativi nei dati, migliorando la capacità di previsione delle *performance* e l'identificazione di fattori di rischio. In questo scenario, la creazione di ecosistemi collaborativi basati sull'adozione di strumenti AI-driven rappresenta un elemento chiave per la trasformazione digitale dello sport, favorendo l'accesso a informazioni strutturate e ottimizzando la gestione delle risorse analitiche.

Lo sport, in quanto contesto caratterizzato da un'elevata variabilità dei dati e dalla necessità di decisioni tempestive, costituisce un laboratorio ideale per l'innovazione nel campo dell'intelligenza artificiale. L'integrazione di dati strutturati e valutazioni qualitative consente di affinare le metodologie di analisi e di sviluppare modelli predittivi sempre più accurati. L'adozione di soluzioni basate su *Explainable AI* e *machine learning* contribuisce a migliorare la comprensione delle dinamiche di gioco, rendendo le analisi più accessibili e favorendo una maggiore democratizzazione nell'uso dei dati sportivi.

5. L'INTELLIGENZA ARTIFICIALE PER LA PREVENZIONE DEGLI INFORTUNI: STRUMENTI E APPLICAZIONI

I modelli predittivi si basano su diverse tecniche di campionatura ed elaborazione dei dati. Abbiamo l'utilizzo delle reti neurali artificiali (ANN), le *Convolutional Neural Networks* (CNN), le *Random Forest* (RF), gli alberi decisionali e i processi di Markov. Tuttavia, ognuno di questi modelli ha delle peculiarità diverse, come ad esempio la tipologia di dati che riesce ad elaborare, la capacità di mettere in relazione informazioni differenti, la grandezza dei dataset che può analizzare. Per prevenire adeguatamente un infortunio è necessario integrare, elaborare e analizzare diverse tipologie di dati derivanti da dispositivi indossabili, esami clinici, video e altre fonti. Di seguito vedremo quali sono le tecniche che potrebbero offrire un risultato migliore nella prevenzione degli infortuni.

5.1. Modelli predittivi e interpretabilità dei dati

Tra i modelli predittivi più efficaci vi sono quelli delle reti neurali artificiali, che replicano il funzionamento del cervello, apprendono dai dati raccolti e individuano segnali precoci di affaticamento o sovraccarico muscolare. Tuttavia, in un contesto con competenze eterogenee, questo modello potrebbe risultare poco trasparente e di difficile interpretazione per lo staff medico e atletico. Un modello predittivo come gli alberi decisionali o le *Random Forest* potrebbe essere più adatto a questo scopo, grazie alla maggiore interpretabilità dei dati. Questi modelli evidenziano in modo chiaro i fattori che influenzano l'infortunio e forniscono indicazioni pratiche per l'allenamento.

5.2. Analisi video e *Federated Learning* per la sicurezza dei dati

Un'altra tecnologia fondamentale è rappresentata dall'analisi dei video tramite intelligenza artificiale. Oggi, grazie a software avanzati, è possibile esaminare i movimenti degli atleti durante le competizioni e gli allenamenti per individuare eventuali posture scorrette o movimenti dannosi. Questo tipo di analisi si basa su modelli in grado di riconoscere e tracciare il movimento del corpo umano, fornendo riscontri utili per correggere eventuali errori tecnici prima che si trasformino in problemi fisici. Questo modello di intelligenza artificiale è già utilizzato oggi anche per dinamiche regolamentari, con il sistema *Electronic Performance and Tracking System* (EPTS) che, oltre a fornire le statistiche degli atleti, viene utilizzato nel calcio per il fuorigioco semi-automatico.

Per questo motivo, si stanno sviluppando sistemi che consentono di analizzare i dati senza doverli trasferire su un server centrale, garantendo così maggiore sicurezza e rispetto della riservatezza. Ad esempio, il *Federated Learning* consente di archiviare i dati sui dispositivi locali e trasmettere solo gli aggiornamenti al modello centrale, senza inviare i dati originali che hanno determinato tali aggiornamenti.

6. LE SFIDE PER L'INTEGRAZIONE DELL'INTELLIGENZA ARTIFICIALE NELLO SPORT

L'integrazione dell'Intelligenza Artificiale (IA) nello sport presenta una serie di sfide operative e strategiche, che vanno oltre la semplice implementazione tecnologica. Se da un lato il suo utilizzo può migliorare significativamente la prevenzione degli infortuni e ottimizzare le *performance* atletiche, dall'altro richiede competenze specifiche e una *governance* efficace per gestire la crescente quantità di dati generati dagli atleti.

6.1. Gestione e accesso ai dati: un modello decentralizzato è necessario?

Uno degli aspetti meno esplorati riguarda chi dovrebbe detenere il controllo e la gestione dei dati generati dagli atleti. L'impiego di modelli di IA per la prevenzione degli infortuni si basa su grandi dataset provenienti da fonti eterogenee, che devono essere elaborati attraverso tecniche avanzate come l'*ETL* (*Extract, Transform, Load*) per garantirne un uso efficace. Tuttavia, il costo e la complessità di questi processi fanno sì che le società sportive e le organizzazioni non possano sempre permettersi di sviluppare soluzioni proprietarie, dovendo quindi dipendere da provider terzi.

Questa dipendenza solleva interrogativi critici: quanto controllo hanno realmente gli atleti e i club sui loro dati? Se i modelli di IA vengono addestrati utilizzando informazioni biometriche raccolte dagli atleti, questi dovrebbero poter decidere come e da chi vengono utilizzati. Il rischio, altrimenti, è che i fornitori di IA accumulino una quantità di dati tale da creare asimmetrie di potere nel settore sportivo, con potenziali implicazioni economiche e competitive.

6.2. IA e dinamiche di mercato: rischi di asimmetrie informative e vantaggi competitivi

L'adozione di sistemi di Intelligenza Artificiale nel settore sportivo introduce una serie di implicazioni economiche e strategiche, in particolare per quanto riguarda la gestione e l'accesso ai dati biometrici degli atleti. Poiché le analisi predittive fornite dai provider di IA possono incidere direttamente sulle decisioni di mercato, vi è il rischio concreto che le informazioni generate da questi sistemi possano determinare asimmetrie informative tra i club, con potenziali effetti distorsivi sul funzionamento del mercato sportivo.

Se un provider di IA gestisse i dati biometrici di più squadre concorrenti, i modelli predittivi da esso sviluppati potrebbero fornire *insight* rilevanti sulla condizione fisica e sul rischio infortunio degli atleti. In un sistema in cui il medesimo fornitore eroga servizi a più club, l'accesso privilegiato a queste informazioni potrebbe alterare le strategie di trasferimento, influenzando le valutazioni economiche e le decisioni di investimento sui giocatori.

Questa problematica è particolarmente rilevante nei contesti professionistici in cui le transazioni finanziarie legate agli atleti rappresentano asset economici di grande valore. L'eventualità che un'entità terza possa disporre di informazioni altamente sensibili su più squadre concorrenti solleva interrogativi sulla neutralità del fornitore di IA e sulla necessità di definire un quadro normativo che regolamenti la gestione dei dati biometrici a fini di mercato.

In assenza di regolamentazioni specifiche, si potrebbe assistere a una situazione in cui le società sportive con maggiori risorse economiche possano avvantaggiarsi

dell'accesso a modelli IA più avanzati o di una più ampia disponibilità di dati, consolidando il loro predominio sul mercato e riducendo le opportunità competitive per club con risorse più limitate.

6.3. IA e proprietà dei dati: il caso Grok di xAI

Un esempio emblematico che dimostra la crescente rilevanza della proprietà dei dati nel contesto dell'IA è il caso di Grok, il modello di Intelligenza Artificiale Generativa (*GenAI*) sviluppato da xAI, la società fondata da Elon Musk. Il 29 ottobre 2024, Musk ha pubblicamente invitato gli utenti di X (ex Twitter) a caricare immagini diagnostiche come RX, TAC e risonanze magnetiche, con l'obiettivo di migliorare la capacità del chatbot Grok nell'identificare pattern medici.

Questo episodio ha generato un acceso dibattito sulle implicazioni etiche e sulla *governance* dei dati: chi detiene il controllo delle informazioni fornite dagli utenti? Chi beneficia realmente dell'addestramento del modello? Nel settore sportivo, queste domande diventano ancora più rilevanti, poiché gli atleti producono enormi quantità di dati biometrici che potrebbero essere utilizzati per addestrare modelli predittivi senza alcuna forma di compensazione o controllo diretto.

6.4. Monetizzazione e redistribuzione del valore dei dati sportivi

La crescente raccolta di dati biometrici e clinici ha portato alla necessità di riconsiderare i modelli di monetizzazione e redistribuzione del valore. Attualmente, molti dati vengono raccolti, elaborati e utilizzati dai provider di IA per migliorare le loro tecnologie, senza che gli atleti e le organizzazioni che li generano ricevano alcun compenso o controllo sulle modalità di utilizzo.

Una possibile soluzione potrebbe essere l'adozione di modelli decentralizzati di gestione dei dati, che consentirebbero agli atleti e alle squadre di avere maggiore trasparenza e controllo sull'uso delle loro informazioni. Tuttavia, affinché ciò sia realizzabile, servirebbe una regolamentazione chiara che stabilisca chi può accedere ai dati, a quali condizioni e con quali diritti di utilizzo.

7. IA, REGOLAMENTAZIONE E INNOVAZIONE: LE SFIDE PER LA PREVENZIONE DEGLI INFORTUNI NELLO SPORT

Come abbiamo visto, uno dei temi principali riguardo il possibile sviluppo dell'Intelligenza Artificiale nella prevenzione degli infortuni, ma anche nell'intero comparto sanitario extra-sportivo, passa principalmente dal superamento degli ostacoli normativi imposti da AI Act e GDPR

La vera sfida è individuare un modello tecnologico che bilanci la tutela della privacy e il miglioramento dei modelli predittivi, elementi chiave per il successo di queste soluzioni. Lo sport è sempre stato un laboratorio per le innovazioni e il contesto italiano ed europeo, dove la tutela e la promozione della salute sono tra i principi fondamentali dello sport, potrebbero essere il giusto substrato per lo sviluppo di queste soluzioni.

7.1. L'European Health Data Space (EHDS) e la governance dei dati

Il Regolamento sullo Spazio europeo dei dati sanitari (EHDS – *European Health Data Space*) va ad inserirsi nel quadro normativo previsto dalla Strategia Europea per i Dati⁴⁰.

Uno spazio condiviso per i dati a livello europeo potrebbe standardizzare la formattazione dei dati e semplificare l'interoperabilità, rendendoli facilmente utilizzabili dai modelli IA. D'altro canto, le stringenti regolamentazioni potrebbero porre un freno all'innovazione, motivo per cui sarebbe auspicabile che nel futuro i prossimi sviluppi normativi si svolgano in concertazione con le principali aziende del settore, le università e i centri di ricerca.

Una normativa che non si limiti a imporre restrizioni, ma che definisca anche un *gold standard* per i settori di applicazione, potrebbe accelerare lo sviluppo di soluzioni basate sull'IA.

7.2. Blockchain, bias e trasparenza: le tecnologie per una IA sicura

Infine, considerare l'integrazione dell'intelligenza artificiale con tecnologie come la blockchain garantirebbe la completa e verificata tracciabilità del dato oltre che la privacy, grazie alle native soluzioni crittografiche. L'utilizzo combinato tra AI e blockchain è già stato oggetto di diversi studi e ricerche ed è già sviluppato e testato in ambito fintech.

Un'altra sfida importante è il riuscire a limitare eventuali bias, magari promossi a causa di interessi concorrenti e non dichiarati. L'intelligenza artificiale, per essere imparziale e oggettiva, dovrà essere necessariamente *open source*.

7.3. Conclusione: bilanciare innovazione e diritti

Bilanciare innovazione tecnologica, diritti fondamentali e principi etici non è semplice, ma è una strada che va percorsa al più presto. Questo settore potrebbe guidare lo sviluppo economico dei prossimi anni, così come è accaduto con internet.

⁴⁰ A. MICHINELLI, A. BOTTAZZO, *Spazio europeo dei dati sanitari: arriva la rivoluzione europea, ecco di che si tratta*, in *Cybersecurity360*, 27 gennaio 2025 (aggiornato il 6 marzo 2025), disponibile su: <https://www.cybersecurity360.it/legal/privacy-dati-personali/spazio-europeo-dei-dati-sanitari-arriva-la-rivoluzione-europea-ecco-di-che-si-tratta/> (ultimo accesso: 17/03/2025).

NOTIZIE SUGLI AUTORI

CARLO BOTTARI, professore Alma Mater nell'Università di Bologna e direttore della rivista *Diritto dello Sport*.

DAVIDE CARMELO CALDERONE, dottorando in Area Sport, Salute e Benessere, Dipartimento QUVI presso l'Università di Bologna.

LUCA DIMASI, avvocato e docente a contratto di Diritto dei servizi sociali, Fondamenti di diritto dei sistemi di welfare e Organizzazione dei sistemi sanitari presso l'Università di Bologna.

PACO D'ONOFRIO, professore associato di Diritto amministrativo presso l'Università di Bologna.

ANGELO FRANCINI, dottorando in Area Sport, Salute e Benessere, Dipartimento QUVI presso l'Università di Bologna.

LORENZO GASPARINI, dottorando di ricerca in Diritto amministrativo e sanitario presso l'Università di Bologna.

FEDERICO LAUS, ricercatore in diritto amministrativo, Dipartimento di Scienze biomediche e neuromotorie presso l'Università di Bologna.

STEFANO MANZINI, avvocato cassazionista.

ANTONIO ALFONSO PISANI, dottorando di ricerca in Diritto amministrativo e sanitario presso l'Università di Bologna.

QUADERNI DI DIRITTO DELLE ATTIVITÀ MOTORIE E SPORTIVE

Questo volume affronta le trasformazioni della prevenzione sanitaria nell'era digitale, con particolare riferimento all'impiego dell'intelligenza artificiale e della telemedicina. Vengono analizzati l'*Artificial Intelligence Act*, il Regolamento sullo Spazio europeo dei dati sanitari e le più recenti misure europee in materia di *cybersecurity* applicata al settore sanitario. Inoltre, viene proposta una lettura sistematica delle fonti, esaminando le implicazioni per la protezione dei dati personali, la responsabilità dei soggetti coinvolti e la tenuta dei principi fondamentali dell'ordinamento.

Nel quadro delle più recenti evoluzioni normative, viene approfondita anche la direttiva NIS2, considerata nella sua capacità di promuovere una maggiore consapevolezza istituzionale in tema di sicurezza informatica e modelli di *governance* digitale. Un contributo che vuole focalizzare il dibattito accademico sul governo giuridico dell'innovazione tecnologica in ambito sanitario.

Stefano Manzini, avvocato cassazionista, ha orientato la sua carriera verso l'innovazione giuridica e tecnologica, fondando lo studio legale QUBIT Law Firm, specializzato in *blockchain*, intelligenza artificiale e *cybersecurity*. Ha promosso la nascita dell'"organismo di ricerca" IRIS LAB, consorzio che sviluppa attività di R&D per primarie imprese italiane ed è socio fondatore di Cyske S.r.l., società attiva nella *cybersecurity* e nella *compliance* industriale, partecipata dal Gruppo Horsa.

€ 20,00

ISBN 979-12-5477-649-0

