Quaderni AISDUE - Rivista quadrimestrale
ISSN 2975-2698 - Fascicolo speciale n. 2/2024
La nuova disciplina UE sull'intelligenza artificiale

Prime riflessioni sull'applicazione del nuovo regolamento sull'intelligenza artificiale al settore sanitario

Sarah Lattanzi*

SOMMARIO: 1. Introduzione. – 2. I sistemi di IA impiegati in ambito sanitario e gli obblighi per i sistemi c.d. "ad alto rischio". – 3. Il problema della coerenza con altri strumenti legislativi. - 3.1. *Segue*: la coerenza con la legislazione verticale. - 3.2. *Segue*: la coerenza con il GDPR. - 3.3. *Segue*: la coerenza con il regolamento europeo sullo spazio europeo dei dati sanitari e con il regolamento relativo alla *governance* europea dei dati. – 3.4. *Segue*: la coerenza con la legislazione in via di adozione. – 4. Brevi riflessioni conclusive.

1. *Introduzione*

È verosimile che l'applicazione del nuovo regolamento sull'intelligenza artificiale[1] risulterà alquanto incisiva nei c.d. "settori

* Ricercatrice in diritto dell'Unione europea presso l'Università degli Studi di Napoli Parthenope.

[1] Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n. 300/2008, (UE) n. 167/2013, (UE) n. 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale). Per un commento si v. questo *fascicolo speciale* e C. SCHEPISI, *Brevi note sulla "dimensione europea" della regolamentazione dell'intelligenza artificiale: principi, obiettivi e requisiti*, in V.

ad alto impatto" tra cui figurano l'ambiente, la finanza e la sanità[2]. In quest'ultimo[3], numerose e promettenti appaiono le ipotesi applicative di sistemi e tecnologie basate sulla intelligenza artificiale (IA)[4].

Questi potranno essere usati in ambito sanitario per il miglioramento delle previsioni statistiche atte a valutare l'insorgenza e la diffusione di una pandemia; potranno coadiuvare il medico nella diagnosi e nella personalizzazione della cura; o ancora ottimizzare le operazioni di routine come l'assegnazione delle risorse nelle strutture ospedaliere[5]. Come è stato notato, in questo ambito i sistemi di intelligenza artificiale potranno essere sfruttati praticamente in tutte le fasi di assistenza, da quella della ricerca a quella dell'erogazione del servizio sanitario[6].

A seconda dei compiti che si intendono perseguire, diversi saranno i modelli di IA da sfruttare[7]: applicazioni di aumento della realtà virtuale per la scansione di immagini diagnostiche e delle radiografie,

---

FALCE (a cura di), *Strategia dei dati e intelligenza artificiale. Verso un nuovo ordine giuridico del mercato*, Torino, 2023, p. 53 ss.; C. CASONATO, B. MARCHETTI, *Prime osservazioni sulla proposta di regolamento dell'Unione europea in materia di intelligenza artificiale*, in *BioLaw Journal*, 2021, p. 415 ss.; O. POLLICINO, G. DE GREGORIO, F. PAOLUCCI, *La proposta di Regolamento sull'intelligenza artificiale: Verso una nuova governance europea*, in *Agenda Digitale*, 2021.

[2] Si v. 1.1: «Motivi e obiettivi della proposta», in proposta di regolamento del Parlamento europeo e del Consiglio che stabilisce regole armonizzate sull'intelligenza artificiale (legge sull'intelligenza artificiale) e modifica alcuni atti legislativi dell'Unione, COM (2021) 206final, 21 aprile 2021.

[3] Il settore sanitario è definibile come l'insieme di norme, istituti, servizi, attività e attori che contribuiscono alla creazione di un sistema di supporto destinato alla promozione, al mantenimento e alla cura della salute fisica e psichica della persona. Al suo interno si esplicano le attività degli ospedali, degli ambulatori, delle strutture di cura sia pubbliche che private e delle strutture di ricerca e formazione.

[4] Ancora ai sensi della proposta della Commissione, il termine intelligenza artificiale «indica una famiglia di tecnologie in rapida evoluzione in grado di apportare una vasta gamma di benefici economici e sociali in tutto lo spettro delle attività industriali e sociali». Torneremo *infra* sulla sua definizione giuridica definitiva.

[5] Si v. estensivamente sul punto A. BOHR, K. MEMARZADEH (eds.), *Artificial Intelligence in Healthcare*, Amsterdam, 2020.

[6] Si v. R. CALVARA, *Cosa pensa il Garante privacy italiano dell'uso dell'Intelligenza artificiale nel settore sanitario?*, in *Osservatorio sullo Stato digitale*, 29 novembre 2023; C. DI COSTANZO, *L'impiego delle nuove tecnologie nel settore della salute: problematiche e prospettive di diritto costituzionale*, in *Consulta Online*, 2023, p. 214 ss.

[7] Partendo dallo sfruttamento di algoritmi sino alla creazione delle reti neurali profonde utilizzate per i modelli di *deep learning*. Si v. sul tema P. TRAVERSO, *Breve introduzione tecnica all'Intelligenza Artificiale*, in *DPCE online*, n. 1, 2022, p. 155 ss.

impiego di agenti robotici, utilizzo dei sistemi di linguaggio naturale per sottoporre ai pazienti specifici questionari precedenti al ricovero, fino alla predisposizione di *chatbot* riproducenti la figura del medico-ologramma sul modello della "S.A.R.A.H", di recente sviluppata dall'OMS[8]. Inoltre, l'IA è anche alla base di tutta quella vasta gamma di applicazioni installabili sul cellulare, in grado di identificare le componenti dei prodotti della consumazione, di predire il numero di calorie e di fornire raccomandazioni *ad hoc*, anche attraverso dispositivi *hi-tech* "indossabili"[9].

Sebbene i sistemi citati siano molto diversi tra loro, per tipologia, per uso e per grado di complessità tecnica, essi sono tutti accomunati dall'impiego di un «sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali»[10]. Per questi motivi tali strumenti informatici sono assoggettati al regolamento IA di recente entrato in vigore.

Questo regolamento guarda a questi sistemi con favore, a fronte delle riconosciute potenzialità di incremento della qualità della vita delle persone che il loro impiego comporta[11]. D'altra parte, il legislatore UE tenta però anche di regolare, mitigandoli *in nuce*, i rischi provenienti dalla loro comprovata e strutturale «opacità, complessità, dipendenza dai dati …e capacità di produrre un comportamento autonomo»[12].

Il regolamento, inoltre, ammettendo l'impiego di questi sistemi in un settore sensibile come quello della salute, assume una sicura rilevanza costituzionale[13]. Questi sistemi tecnologicamente avanzati

---

[8] www.who-en.digitalhero.cloud/landing/index.html.

[9] In inglese, *wearable devices*, su cui S. GILBERT ET AL., *Citizen data sovereignty is key to wearables and wellness data reuse for the common good*, in *NPJ Digital Medicine*, n. 27, 2024, p. 27.

[10] Art. 3, par. 1, del regolamento IA, cit.

[11] M. DA SILVA, T. HORSLEY ET AL., *Legal concerns in health-related artificial intelligence: a scoping review protocol*, in *Systematic Reviews*, n. 11, 2022, p. 123 ss.

[12] C. SCHEPISI, *Le "dimensioni" della regolazione dell'intelligenza artificiale nella proposta di regolamento della Commissione*, in *I Post di AISDUE*, n. 16, 2022, p. 330.

[13] Sul tema si v. G. DI FEDERICO, *Digitalizzazione dei servizi sanitari e Unione Europea: uno sguardo d'insieme sullo stato dell'arte e sulle sfide future*, in C.

sono destinati ad avere un impatto elevato sugli assi portanti del diritto alla salute, per come declinato nel diritto interno[14] e nel diritto sovranazionale[15]. Infatti, questi sistemi influenzano l'accesso alle cure e la loro qualità[16], nonché la tutela del diritto fondamentale alla protezione dei dati personali[17]. Lo stesso principio di non discriminazione rischia di essere compromesso dall'impiego di sistemi di IA addestrati su dati che incamerino antichi e profondi pregiudizi culturali[18].

Quest'indagine intende analizzare come il nuovo regolamento classifichi e disciplini i vari sistemi di IA utilizzabili in ambito sanitario, e come tenti di risolvere alcune delle problematiche di ordine costituzionale sopra citate. A seguito di questa prima disamina, lo scritto intende porre una specifica attenzione sull'ambito sanitario e sui problemi di ordine costituzionale afferenti a questo specifico settore. Inoltre, ci soffermeremo sulla coerenza del nuovo quadro regolatorio con la legislazione già esistente al livello dell'Unione e con quella attualmente presentata e in discussione. Da ultimo, tenteremo di mettere l'accento sulle modalità e sull'efficacia dell'approccio regolatorio prescelto e sulla sua capacità di garantire un livello elevato di protezione della salute[19].

BOTTARI (a cura di), *La salute del futuro. Prospettive e nuove sfide del diritto sanitario*, Bologna, 2020, p. 17 ss.

[14] C. DI COSTANZO, *L'impiego delle nuove tecnologie nel settore della salute*, cit., p. 216.

[15] G. DI FEDERICO, S. NEGRI, *Unione europea e salute. Principi, azioni, diritti e sicurezza*, Padova, 2019.

[16] C. DI COSTANZO, *Access to Intensive and Artificial Intelligence. A Constitutional Perspective*, in *Italian Journal of Public Law*, 2021, p. 594 ss.

[17] Declinato sia alla luce della disciplina del regolamento sulla protezione dei dati personali (GDPR), sia alla luce delle norme di diritto interno che codificano le regole deontologiche volte a regolare il rapporto di fiducia e confidenzialità tra medico e paziente, in cui rileva un simile, ma diverso "consenso informato" al trattamento rispetto a quanto regolato dal GDPR. Sul punto si v. D. MORANA, T. BALDUZZI, F. MORGANTI, *La salute "intelligente": eHealth, consenso informato e principio di non-discriminazione*, in *federalismi.it*, n. 34, 2022, p. 127 ss.

[18] È questo un dibattito molto presente nel mondo anglosassone e in particolare statunitense, su cui R. R. FLETCHER, A. NAKESHIMANA, O. OLUBEKO, *Addressing fairness, bias, and appropriate use of artificial intelligence and machine learning in global health*, in *Frontiers in artificial intelligence*, vol. 3, 2021, p. 1 ss.

[19] Ovvero uno degli scopi del regolamento iscritti al considerando n. 1.

2. *I sistemi di IA impiegati in ambito sanitario e gli obblighi per i sistemi c.d. "ad alto rischio"*

Per prima cosa il regolamento definisce il suo oggetto e il suo ambito di applicazione. Esso, come anticipato, si applica a un gran numero di tecnologie, data l'ampissima definizione della nozione di «sistemi di IA» novellata dal regolamento[20]. Questa scelta, pur molto criticata dalla dottrina[21], va invero ponderata con la limitata struttura normativa del regolamento, basata sul c.d. *risk based approach*[22]. Essa finisce per regolamentare in maniera eteronoma e completa[23] solo i sistemi ritenuti davvero rischiosi. Fuori dalle applicazioni c.d. "ad alto rischio" e di alcuni sistemi di IA per finalità generali, infatti, il regolamento non impone obblighi normativamente vincolanti[24]. Ciò restringe non la portata stessa del regolamento, ma quella delle sue singole disposizioni e, in particolare, di quelle che pongono obblighi vincolanti.

Nella delimitazione del suo ambito di applicazione, il regolamento chiarisce anche che non si applica ai sistemi di IA usati «esclusivamente per scopi militari, di difesa o di sicurezza nazionale, indipendentemente dal tipo di entità che svolge tali attività, nonché alle attività di ricerca, sviluppo e prototipazione che precedono l'immissione sul mercato o a

[20] Art. 3, punto 1, del regolamento IA.

[21] Si v. per una ricostruzione delle posizioni a favore e a sfavore di una definizione così ampia di questa nozione, C. T. CASTÁN, *The legal concept of artificial intelligence: the debate surrounding the definition of AI System in the AI Act*, in *BioLaw Journal*, n. 1, 2024, p. 305 ss.

[22] G. DE GREGORIO, P. DUNN, *The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age*, in *CMLR*, 2022, p. 488 ss.; G. FINOCCHIARO, *La proposta di Regolamento sull'intelligenza artificiale: il modello europeo basato sulla gestione del rischio*, in *La via europea per l'Intelligenza Artificiale*, 2022, p. 215 ss.; C. QUELLE, *Enhancing compliance under the general data protection regulation: the risky upshot of the accountability-and risk-based approach*, in *European Journal of Risk Regulation*, n. 3, 2018, p. 502 ss.

[23] Ovvero i caratteri della "normatività", per cui si rimanda all'intramontabile categorizzazione di V. CRISAFULLI, *Atto normativo*, in *Enciclopedia del diritto*, vol. IV, 1959, p. 238 ss.

[24] Ma suggerisce l'adozione di regole di auto-condotta. Simoncini e Cremona ritengono si tratti di un «modello di etero-regolazione combinato con un modello di co-regolazione debole», in A. SIMONCINI, E. CREMONA, *La AI fra pubblico e privato*, in *DPCE online*, n. 1, 2022, p. 260.

persone che utilizzano l'IA per motivi non professionali»[25]. L'esclusione delle attività di ricerca è ribadita all'art. 1, par. 8 del regolamento, ai sensi del quale esso non si applica «alle attività di ricerca, prova o sviluppo relative a sistemi di IA o modelli di IA prima della loro immissione sul mercato o messa in servizio».

Questa esclusione, che toccherà da vicino le attività dei dipartimenti di ricerca e sviluppo dei nuovi prodotti, servizi ed app pensate per il settore medico, si ispira a quanto già avviene per la messa in commercio di nuovi farmaci, ove è solo il prodotto finale, già pronto per essere commercializzato, a essere oggetto di specifica regolazione[26]. Di conseguenza, le tecnologie di IA sviluppate dai dipartimenti di ricerca e sviluppo delle case farmaceutiche o dalle industrie della salute e del benessere risultano al momento prive di apposita regolamentazione sovranazionale. Esse potranno dunque essere disciplinate dal legislatore nazionale fintanto che questo "spazio" di normazione concorrente[27] non venga "occupato" dal legislatore dell'Unione.

L'obiettivo del regolamento è, come noto, di natura principalmente economica, volto cioè alla costituzione di un mercato unico per lo scambio e l'utilizzo di sistemi di intelligenza artificiale affidabili, da utilizzare però nel rispetto dei valori e dei diritti fondamentali dell'UE[28]. Questo rispetto passa, in particolare, attraverso la protezione di «un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Unione europea»[29].

Questo tentativo di contemperamento rispecchia la tecnica legislativa prescelta: quella di coniugare un approccio "classico" alla normazione, limitato a riprodurre quanto già esistente nella legislazione

[25] Art. 2, par. 3, regolamento IA.
[26] L. NOTTAGE, *Product safety regulation*, in AA.VV., *Handbook of Research on International Consumer Law*, Cheltenham, 2018, p. 231 ss.
[27] Indicata dalla scelta della base giuridica preminente del regolamento IA e cioè l'art. 114 TFUE, su cui si v. M. INGLESE, *Il regolamento sull'intelligenza artificiale come atto per il completamento e il buon funzionamento del mercato interno?*, in questo *fascicolo speciale*, pp. 12-13.
[28] A. ADINOLFI, *L'intelligenza artificiale tra rischi di violazione dei diritti fondamentali e sostegno alla loro promozione: considerazioni sulla (difficile) costruzione di un quadro normativo dell'Unione*, in AA. VV., *Intelligenza artificiale e diritto: una rivoluzione*?, Bologna, 2022, p. 127 ss.
[29] Considerando n. 1 del regolamento IA.

verticale sulla circolazione e sicurezza dei prodotti[30], con un approccio "nuovo" o "creativo", che si preoccupa di superare la logica del mercato mettendo in risalto considerazioni relative alla protezione dei diritti fondamentali, così come dei processi democratici e dello Stato di diritto[31].

Per mettere in comunicazione questi due diversi approcci, il regolamento predilige il già menzionato sistema di classificazione proporzionale del rischio, su cui graduare, con diverse intensità, numerosi obblighi tecnico-giuridici gravanti sia sugli «operatori» dei sistemi di IA, sia sugli «utilizzatori» (siano pubbliche amministrazioni o persone fisiche e giuridiche di natura privata)[32], nonché sugli Stati membri.

Sulla base di tale sistema di classificazione, i sistemi ad alto rischio saranno sottoposti a obblighi più gravosi, mentre quelli a rischio lieve o minimo a meri obblighi di auto-condotta[33]. Se così stanno le cose, la concreta efficacia del regolamento si giocherà tutta sulla corretta identificazione della classe di rischio e dei conseguenti obblighi, di natura eventualmente vincolante, scaturenti da tale classificazione[34].

---

[30] Una sorta di "vecchio nuovo approccio" per cui si v. S. DE VRIES, O. KANEVSKAIA, R. DE JAGER, *Internal Market 3.0: The "Old" New Approach for Harmonising AI Regulation*, in *EP*, n. 2, 2023, p. 583 ss.; S. DE VRIES, *Recent trends in eu internal market legislation. Bringing back the old concepts?*, in T. VAN DEN BRINK, V. PASSALACQUA (eds.), *Balancing unity and diversity in EU legislation*, Cheltenham, 2024, p. 17 ss.

[31] Questi due approcci sono evidenti in tutto il pacchetto UE per la digitalizzazione e quindi anche nel DMA e soprattutto nel DSA. Per quanto riguarda il regolamento IA, si v. l'intervista a Roberto Viola, reperibile qui. Sul punto anche F. FERRI, *Il giorno dopo la rivoluzione: prospettive di attuazione del regolamento sull'intelligenza artificiale e poteri della Commissione europea*, in questo *fascicolo speciale*, p. 1 ss.

[32] Torneremo *infra* su queste due nozioni.

[33] J. BLACK, *Decentring Regulation: Understanding the Role of Regulation and Self-regulation in "Post-Regulatory" Word*, in *Current Legal Problems*, n. 1, 2001, p. 112 ss.

[34] La classificazione e gli obblighi "spalmati" sulle diverse classi non appaiono pertanto poi così proporzionali poiché questa gradazione si muove solo su due poli, peraltro collocati apparentemente ai due estremi opposti. Tralasciamo qui però la categoria dei sistemi di IA per finalità generali, in parte assimilati ai sistemi ad alto rischio.

Prima però di entrare nel cuore di questa questione[35], occorre menzionare la categoria del rischio «inaccettabile», vietato dal regolamento[36].

Infatti, solo i sistemi il cui rischio, finanche molto alto, sia comunque considerato «accettabile» potranno circolare nel mercato unico. Viceversa, quando il rischio frutto dell'uso di quel sistema sia ritenuto inaccettabile, ad esempio perché tale da mettere a rischio la vita della persona, sarà completamente bandito dal mercato, con conseguente illiceità del suo utilizzo[37]. Inaccettabile non è dunque mai il sistema di IA in sé per sé, bensì il suo utilizzo o, meglio, «le pratiche» eccessivamente rischiose a cui esso può prestarsi.

Tra le pratiche vietate figurano, in particolare, l'identificazione biometrica remota in tempo reale, la lettura delle emozioni in base ai dati biometrici, l'uso di tecniche subliminali, la previsione dei reati o il c.d. *social scoring*. Tra queste, nessuna esclusione pertiene direttamente all'ambito sanitario[38]. Anzi, «motivi medici», presumibilmente di ordine psichiatrico o «di sicurezza», costituiscono deroghe al divieto posto all'art. 5, lett. *f)* in merito all'immissione sul mercato o alla messa in servizio dell'uso di sistemi di IA volti a inferire le emozioni di una persona nell'ambito del luogo di lavoro e degli istituti di istruzione.

Tuttavia, l'art. 5, par. 1, lett. *b)*, vieta «la messa in servizio o l'uso di un sistema di IA che sfrutta le *vulnerabilità* di una persona fisica o di uno specifico gruppo di persone, dovute all'età, alla *disabilità* o a una *specifica situazione sociale o economica*, con l'obiettivo o l'effetto di distorcere materialmente il comportamento di tale persona o di una persona che appartiene a tale gruppo in un modo che provochi o possa ragionevolmente provocare a tale persona o a un'altra persona un danno

[35] Che riguarda da vicino proprio i sistemi di IA applicabili in ambito sanitario che, come vedremo, dovrebbero per la maggior parte confluire nella classe di rischio più elevata. Da un lato perché essi saranno presumibilmente usati a fini diagnostici e terapeutici e saranno classificati come dispositivi medici, dall'altro in ragione dell'eventuale impatto che possono avere sulla sicurezza fisica delle persone e sui loro diritti fondamentali.

[36] La rappresentazione figurativa dell'approccio basato sul rischio è infatti quella di una piramide, la cui punta è costituita dal rischio inaccettabile e la base dal rischio nullo.

[37] Art. 5 del regolamento IA.

[38] *Ibidem*.

significativo»[39]. Nella nozione di «danno significativo» dovrebbe certamente rientrare il danno alla salute, mentre il «gruppo vulnerabile» potrebbe ragionevolmente essere identificato con quello dei pazienti affetti da una stessa patologia. Stando a questa lettura, è possibile immaginare che in futuro alcuni impieghi delle tecnologie basate sull'IA saranno bandite in ambito sanitario.

In tal senso soccorre il considerando n. 58 del regolamento, il quale, pur riferendosi ad alcuni degli usi da considerarsi ad alto rischio, annovera coloro che «ricevono prestazioni e servizi essenziali di assistenza pubblica dalle autorità pubbliche, *vale a dire servizi sanitari*, prestazioni di sicurezza sociale, servizi sociali che forniscono protezione in casi quali la maternità, la malattia (…)» tra le persone che «si trovano generalmente in una *posizione vulnerabile* rispetto alle autorità responsabili».[40]

Scendendo di un livello la piramide raffigurante l'approccio basato sul rischio, il regolamento definisce la classificazione dei sistemi ad alto rischio. È in questa classe che confluiranno molte delle tecnologie utilizzabili in ambito sanitario e ciò essenzialmente per due ordini di ragioni: la destinazione d'uso, eventualmente a fini diagnostici e terapeutici della tecnologia, e la sua qualificazione come dispositivo medico.

In particolare, riguardo al primo aspetto, sono considerati ad alto rischio, in ragione del loro uso:

a) «i sistemi di IA destinati a essere utilizzati dalle autorità pubbliche o per conto di autorità pubbliche per *valutare l'ammissibilità delle persone fisiche alle prestazioni e ai servizi di assistenza pubblica essenziali*, compresi i servizi di assistenza sanitaria, nonché per concedere, ridurre, revocare o recuperare tali prestazioni e servizi;

(….)

d) i sistemi di IA destinati a essere utilizzati *per valutare e classificare le chiamate di emergenza* effettuate da persone fisiche o per inviare servizi di emergenza di primo soccorso o per stabilire priorità in merito all'invio di tali servizi, compresi polizia, vigili del fuoco *e*

[39] Corsivo aggiunto.
[40] Corsivo aggiunto.

assistenza medica, nonché per i sistemi di selezione dei pazienti per quanto concerne l'assistenza sanitaria di emergenza»[41].

A proposito di queste diverse fattispecie menzionate dall'Allegato III del regolamento, vale la pena sottolineare il diverso ambito soggettivo delle disposizioni regolamentate alla lett. *a)*, la quale si rivolge espressamente alle autorità pubbliche o ad autorità private che operano per conto di autorità pubbliche, ovvero che siano oggetto di delega di poteri pubblici, e alla lett. *d)* la quale, invece, non menziona la natura pubblica o privata dell'ente ma solo la tipologia di servizio: l'assistenza sanitaria di emergenza, indipendentemente dalla natura del soggetto erogatore[42].

La diversa definizione dei sistemi ad alto rischio, basata, in un caso, sulla natura pubblica del prestatore e, nell'altro, sulla tipologia del servizio erogato, si spiega alla luce di vari ordini di ragioni. In primo luogo, nella maggior parte dei sistemi costituzionali degli Stati membri, è l'autorità pubblica che, in applicazione del fondamentale principio di solidarietà sociale, ha l'obbligo di assicurare l'erogazione di un efficiente servizio sanitario nazionale per i suoi cittadini[43], indipendentemente dalle modalità del suo finanziamento.

Inoltre, nella misura in cui il regolamento IA adotta un "approccio antropocentrico"[44], una tecnologia potenzialmente «disruptive»[45] dovrebbe sempre essere posta sotto la supervisione umana. L'essere umano è infatti l'unico agente in grado di effettuare una scelta "ragionevolmente orientata" a tutela dei diritti e della libertà delle persone, e quindi, ancor prima, della loro vita. Ciò è particolarmente rilevante nel caso dei servizi di urgenza, in cui la protezione di questo bene primario è richiesta a qualunque prestatore.

---

[41] Punto 1, Allegato III, del regolameno IA (corsivo aggiunto).
[42] Sul tema, O. M. PUIGPELAT, *The impact of the AI Act on public authorities and on administrative procedures*, in *Rivista interdisciplinare sul diritto delle amministrazioni pubbliche*, vol. 4, 2023, p. 238 ss.
[43] V. SALVATORE, *Il diritto alla salute. Una prospettiva di diritto comparato*, in *EPRS Servizio ricerca del Parlamento europeo*, 2021.
[44] Comunicazione della Commissione europea, Creare fiducia nell'intelligenza artificiale antropocentrica, COM (2019) 168final, dell'8 aprile 2019.
[45] R. GIRASA, *Artificial intelligence as a disruptive technology: Economic transformation and government regulation*, Berlin, 2020.

Infine, non rilevano né la natura giuridica dell'agente umano, in quanto il titolare degli obblighi può essere una persona fisica o giuridica, né, in questo ultimo caso, quella pubblica o privata. Conta, invece, la qualificazione oggettiva dell'attività erogata, che deve essere riconducibile a un "servizio essenziale". Questo profilo, come giustamente notato, rivela una "concezione funzionale di servizio essenziale", che ne valorizza il ruolo sociale, indipendentemente dal fatto che ad erogarlo sia un soggetto pubblico o uno privato, con conseguente «responsabilizzazione dei grandi player privati dell'era digitale»[46].

Sulla base di quanto esposto, ai sensi del regolamento IA, gli stessi identici programmi statistici e di linguaggio naturale usati per stabilire i turni dei medici e degli infermieri nelle strutture ospedaliere – generalmente considerati a rischio lieve o nullo – non potranno essere impiegati per determinare le preferenze di accesso in ospedale[47].

Dietro questa logica si annida l'idea della "neutralità" della tecnologia dal punto di vista del suo trattamento giuridico. Conformemente a tale logica, non è il programma in sé per sé a causare l'eventuale violazione dei diritti fondamentali, ma il suo specifico uso ragion per cui il programma può essere liberamente sviluppato da coloro che hanno gli strumenti e la conoscenza tecnica per farlo. Anzi, vi è un evidente incentivo allo sviluppo, dacché la sua presunta neutralità iniziale ripara il programma da eventuali illeciti, ponendolo invece in corsa verso uno sviluppo sempre più avanzato. Al contempo, però, ai sensi del regolamento, tale presunta iniziale neutralità retrocede in casi specificatamente determinati e, in particolare, dinanzi alla necessità di proteggere i diritti e le libertà delle persone che potrebbero essere degradati dall'uso concreto di tale tecnologia[48]. Ciò può accadere nel caso in cui il sistema di IA sia concretamente impiegato in settori sensibili, come quello della sanità, che hanno a che vedere con la tutela della vita, con il suo miglioramento e, più in generale, con l'inclusione

[46] A. SIMONCINI, E. CREMONA, *op. cit.*, pp. 259-260.
[47] Evidentemente qui il rischio è quello di una discriminazione di alcuni individui o gruppi sociali.
[48] Ovvero in un certo contesto, in uno specifico settore e rispetto a una determinata categoria di soggetti.

di tutti i cittadini indipendentemente dalla loro classe socioeconomico e culturale.

I c.d. sistemi ad alto rischio, però, non sono solo definiti in base a questo criterio "d'uso", volto a valorizzare i rischi concreti dell'applicazione di tecnologie presuntivamente neutre. L'art. 6 posto nel corpo del regolamento[49] menziona anzitutto i sistemi considerati ad alto rischio, perché coperti da una normativa di armonizzazione dell'UE[50]. Un sistema di IA sarà in base a tale disposizione considerato ad alto rischio quando soddisfa due condizioni cumulative:

a) «è destinato a essere utilizzato come componente di sicurezza di un prodotto, o il sistema di IA è esso stesso un prodotto, disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'allegato I;

b) il prodotto, il cui componente di sicurezza a norma della lettera a) è il sistema di IA, o il sistema di IA stesso in quanto prodotto, è soggetto a una valutazione della conformità da parte di terzi ai fini dell'immissione sul mercato o della messa in servizio di tale prodotto ai sensi della normativa di armonizzazione dell'Unione elencata nell'allegato I».

Tra le normative di armonizzazione più rilevanti per il nostro ambito figurano: il regolamento (UE) 2016/425 del Parlamento europeo e del Consiglio, del 9 marzo 2016, sui dispositivi di protezione individuale e che abroga la direttiva 89/686/CEE del Consiglio; il regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medici, che modifica la direttiva 2001/83/CE ; il regolamento (CE) n. 178/2002 e il regolamento (CE) n. 1223/2009 e che abroga le direttive 90/385/CEE e 93/42/CEE del Consiglio; e il regolamento (UE) 2017/746 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medico-diagnostici in vitro e che abroga la direttiva 98/79/CE; la decisione 2010/227/UE della Commissione[51].

In base ai regolamenti sui dispositivi medici, sono ad alto rischio tutti i dispositivi medici e i dispositivi medico-diagnostici che rientrano

[49] E quindi non in un Allegato.

[50] Da questo punto di vista anche qui vi è una integrazione tra un approccio "innovativo" o "antropocentrico" e un approccio "classico" ovvero obiettivo.

[51] A. VOLPATO, *Il ruolo delle norme armonizzate nell'attuazione del regolamento sull'intelligenza artificiale*, in questo *fascicolo speciale*, p. 1 ss.

nelle classi IIa, IIb o III e che sono, pertanto, sottoposti a una procedura di valutazione della conformità da parte di un organismo terzo, ai sensi del regolamento (UE) n. 2017/745[52]. Quelli collocati nella prima classe di rischio disciplinata da tale regolamento, viceversa, sono solo sottoposti a un'auto-valutazione, senza il coinvolgimento di un organismo indipendente, come disposto anche dal regolamento IA[53]. Quest'ultimo, infatti, stabilisce che, se non è previsto, dalla legislazione settoriale, il coinvolgimento di un organismo qualificato, la valutazione della conformità deve essere fatta in base «al controllo interno di cui all'Allegato VI» del regolamento[54]. Di tal fatta, la struttura della procedura di valutazione della conformità, stabilita nei due regolamenti, resta sostanzialmente la stessa[55].

Sono allora due i meccanismi di classificazione dei sistemi ad alto rischio. Il primo mette in risalto l'uso concreto o la pratica concreta del sistema, sposando così un approccio decisamente "innovativo" alla regolazione, che guarda alla tecnologia come neutra in astratto ma da supervisionare in concreto. Il secondo, viceversa, è basato sulle norme di armonizzazione ed è riconducibile nell'alveo di quell'approccio normativo da noi definito "classico", che si limita a riprodurre la logica già sperimentata in materia di circolazione e sicurezza dei prodotti. I due approcci sono destinati ad integrarsi e contemperarsi, a condizione che il regolamento IA assuma la funzione di "modello" nel quale è richiamata la struttura della legislazione verticale già esistente, la cui portata viene però estesa in ragione della valorizzazione di considerazioni di più ampia portata e di carattere sociale.

Ad esempio, in base al regolamento sui dispositivi medici, poiché rileva la destinazione d'uso dichiarata, i sistemi IA di monitoraggio o che forniscono consigli su come migliorare lo stato di salute (come è talvolta il caso dei dispositivi indossabili), non dovrebbero essere considerati «dispositivi medici», in base a quanto suggerito dal

[52] Allegato VIII del regolamento (UE) n. 2017/745, cit., il quale stabilisce regole di classificazione basate sulla destinazione d'uso medico.
[53] Sul punto A. KISELEVA, *AI as a Medical Device: Between the Medical Devices Framework and the General AI Regulation*, In *Time to Reshape the Digital Society. 40th Anniversary of the CRIDS*, Namur-Belgium, November 2021.
[54] Art. 43, par. 1, lett.) *a*.
[55] A. VOLPATO, *op. cit*.

considerando n. 19 del suddetto regolamento[56] e, di conseguenza, non dovrebbero rientrare nella categoria dell'«alto rischio» prevista dal regolamento IA.

Viceversa, i sistemi volti a monitorare i livelli di serotonina per determinare la reazione del paziente alle cure - normalmente usati per finalità diagnostiche e terapeutiche - dovrebbero, ai sensi dell'art. 2, par. 1, del regolamento sui dispositivi medici e della regola n. 11 ivi stabilita, essere considerati «accessori di un dispositivo medico» e quindi rientrare nella classe IIa[57]. Di conseguenza essi saranno classificati come ad alto rischio, ai sensi del regolamento IA.

Tuttavia, questi metodi di classificazione non sono così rigidi e potrebbero, nell'applicazione pratica, essere neutralizzati in virtù delle numerose deroghe introdotte nei successivi paragrafi dell'art. 6 del regolamento IA[58]. Queste deroghe permettono una mutazione della classe di rischio che potrebbe prodursi sia in presenza di un sistema di IA considerato ad alto rischio in virtù dell'Allegato III, sia quando si tratti di un sistema di IA non ad alto rischio che successivamente venga integrato in tale allegato in base al suo uso concreto[59].

Nel primo caso il sistema di IA astrattamente ad alto rischio potrebbe essere considerato concretamente non in grado di influenzare il risultato del processo decisionale e dunque essere escluso dai sistemi ad alto rischio in applicazione dell'art. 6, par. 3 del regolamento, poichè, ad esempio, è «destinato a migliorare il risultato di un'attività umana precedentemente completata»[60]. In questo caso, il fornitore effettua una

---

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

[57] J. VAN OIRSCHOT, G. OOMS, *Interpreting the EU Artificial Intelligence Act for the Health Sector*, Amsterdam, 2022, p. 10.

[58] Ciò che permette che un sistema di IA che rientra nell'allegato III non sia considerato ad alto rischio qualora non presenti «un rischio significativo di danno per la salute, la sicurezza o i diritti fondamentali delle persone fisiche, *anche* nel senso di non influenzare materialmente il risultato del processo decisionale».

[59] Le mutazioni delle classi di rischio sono quindi più facilmente realizzabili per i sistemi "indipendenti" o c.d. *stand-alone*.

[60] In applicazione dell'art. 6, par. 3, lett. *b)*, del regolamento IA.

auto-valutazione che dovrà eventualmente essere presentata alle autorità nazionali competenti su loro richiesta[61]. Ai sensi dello stesso articolo, il fornitore è inoltre soggetto all'obbligo di registrazione di cui all'articolo 49, par. 2, del regolamento.

Nel secondo caso, potrebbe trattarsi ad esempio di un'applicazione per il benessere che archivia dati di soggetti affetti da particolari disturbi psichici o che monitora il flusso mestruale delle donne e che, non qualificata come dispositivo medico, dovrebbe essere considerata a rischio lieve. Tuttavia, lo stesso dispositivo potrebbe essere successivamente ricondotto, magari per qualche ragione geopolitica, tra i sistemi ad alto rischio, in virtù di una modifica dell'allegato III inserita *ex post* dalla Commissione[62]. Queste considerazioni valgono in particolare per i c.d. «sistemi indipendenti» o *stand alone* che, non essendo componenti di prodotti dei dispositivi medici, sono assoggettati a procedure di auto-valutazione effettuate dallo stesso fornitore.

Avendo sommariamente delineato il sistema di definizione della classe ad alto rischio e le ragioni per le quali interessa da vicino i modelli di IA utilizzati in ambito sanitario, occorre ora analizzare gli obblighi più stringenti gravanti sugli operatori dei sistemi ad alto rischio.

Tali obblighi sono disciplinati dal Capo II del regolamento, il quale fa riferimento a doveri più specifici di trasparenza, accuratezza, robustezza e cibersicurezza e alla tutela dei diritti fondamentali[63]. Anzitutto, la documentazione tecnica di un sistema di IA ad alto rischio è redatta prima dell'immissione sul mercato o della messa in servizio e deve essere tenuta aggiornata nel tempo[64]. Se già prevista dalle norme di armonizzazione, essa sarà unica e integrerà gli obblighi delle diverse normative al fine di diminuire i costi e gli oneri gravanti su fornitori e produttori.

---

[61] *Ibidem*, art. 3, par. 4.
[62] Su cui F. FERRI, *op. cit*., p. 4 ss. Per alcune considerazioni sul binomio geopolitica e salute si v. risoluzione del Parlamento europeo, del 20 gennaio 2021, sull'intelligenza artificiale: questioni relative all'interpretazione e applicazione del diritto internazionale nella misura in cui l'UE è interessata relativamente agli impieghi civili e militari e all'autorità dello Stato al di fuori dell'ambito della giustizia penale (2020/2013(INI)).
[63] Art. 8 del regolamento IA.
[64] *Ibidem*, art. 11.

Lo stesso vale per la «valutazione della conformità» imposta ai sensi dell'art. 43 e per la marcatura CE, già prevista ai sensi della legislazione sulla commercializzazione e la sicurezza di alcuni prodotti[65]. Come anticipato, la valutazione della conformità diventa però una sorta di auto-valutazione, nel caso dei c.d. sistemi indipendenti che non sono classificati né come prodotti, né come componenti di sicurezza di un prodotto[66].

Per tutti i sistemi ad alto rischio, poi, occorre prevedere un sistema di gestione dei rischi ai sensi dell'art. 9 al fine di assicurare un aggiornamento costante e sistematico agli obblighi imposti. Inoltre, un obbligo di monitoraggio successivo all'immissione nel mercato è disciplinato all'art. 72 del regolamento.

Sono questi tutti obblighi che ci paiono essenzialmente di carattere procedurale. A questi si aggiungono però anche obblighi che potremmo definire sostanziali, quali gli obblighi di «trasparenza e fornitura di informazioni ai deployer» previsti ai sensi dell'art. 13. Quest'obbligo di trasparenza, corollario del c.d. «diritto alla spiegabilità», derivato dalla giurisprudenza sull'art. 22 del GDPR, è preposto allo scopo di rendere comprensibile il funzionamento del sistema, al fine di ingenerare un utilizzo – ed eventualmente un consenso all'utilizzo – consapevole. Quest'obbligo diviene "sostanziale" se e nella misura in cui è associato al c.d. diritto ad ottenere la spiegazione dei singoli processi decisionali ai sensi del GDPR[67].

Quest'obbligo di trasparenza declinato in senso sostanziale è assai diverso da quello previsto dall'art. 52 del regolamento IA, che si applica ad alcuni sistemi di IA per finalità generali, come le c.d. *chat boxes*. In questo caso, si richiede solo di rendere noto all'utente il fatto che si stia interagendo con un sistema di IA, ragion per cui esso, più che un vero

[65] Decisione (UE) n. 768/2008/CE del Parlamento europeo e del Consiglio, del 9 luglio 2008, relativa a un quadro comune per la commercializzazione dei prodotti e regolamento (UE) 2019/1020 del Parlamento europeo e del Consiglio, del 20 giugno 2019, sulla vigilanza del mercato e sulla conformità dei prodotti.
[66] Questi seguono le regole iscritte nell'Allegato VI ed eventualmente VII.
[67] Sul punto, G. CONTALDI, *Intelligenza artificiale e dati personali*, in *Ordine internazionale e diritti umani*, 2021, p. 1193 ss.

e proprio obbligo di trasparenza, dovrebbe rappresentare un obbligo informativo[68].

Particolare attenzione merita la c.d. valutazione di impatto sui diritti fondamentali (FRIA)[69]. Questa è stata fortemente voluta dal Parlamento europeo[70], il quale ha rafforzato la proposta avanzata dal Consiglio in sede di trilogo, la quale richiedeva ai *deployer* dei sistemi di IA ad alto rischio solo di prevedere e analizzare *ex ante* una lista di rischi potenziali per la salute, la sicurezza e i diritti fondamentali. Secondo la modifica voluta dal Parlamento europeo[71], ora confluita nell'art. 27 del regolamento, l'attuale FRIA, acronimo dell'inglese *fundamental rights impact assessment*, non si riduce a un mero elenco *ex ante* dei possibili rischi, ma tenta di coadiuvare anche una previsione *ex post* relativa all'uso concreto dei sistemi di IA[72]. Per far ciò prevede una serie di obblighi aggiuntivi per i *deployer* dei sistemi di IA, considerati «nella posizione migliore per comprendere come il sistema di IA ad alto rischio sarà utilizzato concretamente e possono pertanto individuare potenziali rischi significativi non previsti nella fase di sviluppo, in ragione di una conoscenza più puntuale del contesto di utilizzo e delle persone o dei gruppi di persone che potrebbero essere interessati, compresi i gruppi vulnerabili»[73].

I *deployer* obbligati dalla FRIA sono solo gli organismi di diritto pubblico o enti privati che forniscono servizi pubblici, ovvero *deployer* di sistemi di IA ad alto rischio, di cui all'allegato III, punto 5, lett. *b)* e

---

[68] A. KISELEVA, *Making ai's transparency transparent: notes on the EU proposal for the Ai Act*, in *European Law Blog*, 2021; e anche A. KISELEVA, D. KOTZINOS, P. DE HERT, *Transparency of AI in healthcare as a multilayered system of accountabilities: between legal requirements and technical limitations*, in *Frontiers in artificial intelligence*, 2022, p. 1 ss.

[69] J. MÖKANDER, M. AXENTE, F. CASOLARI, L. FLORIDI, *Conformity assessments and post-market monitoring: a guide to the role of auditing in the pro-posed European AI Regulation*, in *Minds and Machines*, vol. 32, 2021, p. 1 ss.

[70] www.eur-lex.europa.eu/legal content/EN/TXT/?uri=CELEX%3A52023AP0236.

[71] Su cui si v. anche E. CIRONE, *L'AI Act e l'obiettivo (mancato?) di promuovere uno standard globale per la tutela dei diritti fondamentali*, in questo *fascicolo speciale*, p. 14.

[72] Poiché in base considerando n. 58 *bis* introdotto dall'emendamento del Parlamento (ora considerando n. 93): «Se da un lato i rischi legati ai sistemi di IA possono risultare dal modo in cui tali sistemi sono progettati, dall'altro essi possono derivare anche *dal modo in cui tali sistemi di IA sono utilizzati*».

[73] Considerando n. 93 del regolamento IA.

lett. *c)*. Questi devono redigere una valutazione in cui vengano descritte le applicazioni del sistema ad alto rischio, il periodo di tempo e la frequenza di tale utilizzo, le categorie di persone fisiche e dei gruppi che possono essere interessati dal suo uso, i rischi specifici di danno che possono incidere su determinati gruppi o categorie di persone (minoranze, gruppi vulnerabili) e, infine, le misure di sorveglianza umana[74] e di rimedio alla concretizzazione dei rischi[75].

Di tutti gli obblighi che abbiamo citato, solo gli ultimi due gravano però sul *deployer*, mentre i primi gravano sul "fornitore". A riguardo, giova ricordare che, ai sensi dell'art. 1, par. 2, lett. *c)*, il regolamento stabilisce «requisiti specifici per i sistemi di IA ad alto rischio e obblighi per gli operatori di tali sistemi». La nozione di operatore e assai ampia. e include, ai sensi dell'art. 3, par. 8, «un fornitore, un fabbricante del prodotto, un *deployer*, un rappresentante autorizzato, un importatore o un distributore», laddove, in particolare, un fornitore è «una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che sviluppa un sistema di IA o un modello di IA per finalità generali o che fa sviluppare un sistema di IA o un modello di IA per finalità generali e immette tale sistema o modello sul mercato o mette in servizio il sistema di IA con il proprio nome o marchio, a titolo oneroso o gratuito»; mentre un *deployer* è «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».

In base all'art. 25, la nozione di "fornitore" è aperta, poiché si può diventare fornitori al verificarsi di una delle condizioni indicate dall'articolo in questione. Inoltre, le figure del *deployer* e del fornitore potrebbero anche sovrapporsi, in virtù dell'applicazione congiunta delle regole previste dal regolamento IA, in particolare quelle relative all'obbligo di adottare idonee misure tecniche e organizzative[76], e di

[74] In raccordo con l'art. 14 e il principio della c.d. «non esclusività della decisione algoritmica».
[75] Inoltre, l'operatore che è un'autorità pubblica o un'impresa di cui all'articolo 51, par. 1 *bis*, lett. *b)*, pubblica una sintesi dei risultati della valutazione d'impatto nell'ambito della registrazione dell'uso ai sensi dell'obbligo di cui all'articolo 51, par. 2.
[76] *Ibidem*, art. 70.

quelle del regolamento sulla protezione dei dati, il quale ammette la possibilità di una contitolarità di obblighi[77].

3. *Il problema della coerenza con altri strumenti legislativi*

È questo uno dei tanti aspetti che riguarda il più generale problema della c.d. «coerenza con le disposizioni vigenti nel settore normativo interessato»[78]. Il problema della coerenza si pone in maniera diversa in base alla tipologia della legislazione con cui il regolamento si confronta, sia essa verticale oppure trasversale.

3.1. Segue*: la coerenza con la legislazione verticale*

Il regolamento ha tentato di preservare la massima coerenza con le legislazioni verticali adoperando la tecnica del rinvio, la quale consente una vera e propria integrazione delle regole previste dal regolamento IA con le varie e assai complesse normative settoriali richiamate nel corpo del testo, nei considerando e negli appositi allegati[79].

Si pensi alla procedura di valutazione della conformità dei prodotti dei quali un sistema di IA costituisce una componente di sicurezza, o a quelle nelle quali il sistema di IA 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. In simili casi, l'articolo 43 del regolamento IA rinvia alle diverse normative di armonizzazione elencate nell'allegato I del regolamento stesso[80], assicurando la massima coerenza. Un sistema di IA potrà circolare nel mercato dell'UE solo se già risulta conforme a tutta la normativa di armonizzazione dell'Unione che gli è astrattamente applicabile[81].

---

[77] Sul punto G. CONTALDI, *La proposta di regolamento sull'intelligenza artificiale e la protezione dei dati personali*, in P. MANZINI, G. CONTALDI, G. CAGGIANO (a cura di), *Verso una legislazione europea su mercati e servizi digitali*, Bari, 2021, p. 207 ss.
[78] Si v. ancora COM (2021) 206final, cit.
[79] Sono ancora in corso di adozione le normative relative «ai requisiti essenziali di cibersicurezza di un prodotto» e ai «prodotti con elementi digitali critici».
[80] Su questo ampiamente A. VOLPATO, *op. cit*.
[81] Ai sensi del considerando n. 46, il regolamento si applica «senza pregiudizio» di tali normative.

Se in astratto questa "coerenza" è ottenuta tramite la tecnica del rinvio, il quale permette l'integrazione della normativa settoriale rinviata nella legislazione rinviante[82], nella pratica ciò consente anche di evitare la duplicazione di sforzi "amministrativi" o "burocratici" già inscritti nelle legislazioni precedenti e che potrebbero risultare particolarmente onerosi per le piccole e medie imprese. Ulteriori esempi di rinvio possono trovarsi negli obblighi di «marcatura CE», previsti dall'art. 48 del regolamento IA[83] e dall'art. 47, par. 3, che consentono di redigere un'unica dichiarazione di conformità per un prodotto già sottoposto ad altra normativa di armonizzazione.

3.2. Segue*: la coerenza con il GDPR*

Più difficoltosa appare la coerenza con le normative trasversali e in particolare con il GDPR[84]. Infatti, benché ai sensi del decimo considerando, «il presente regolamento non mira a pregiudicare l'applicazione del vigente diritto dell'Unione che disciplina il trattamento dei dati personali, inclusi i compiti e i poteri delle autorità di controllo indipendenti competenti a monitorare la conformità con tali strumenti», vi sono diverse sovrapposizioni tra queste due normative, non sempre risolte dal legislatore[85].

Sebbene egli abbia in astratto pensato a un approccio di tipo complementare[86], è evidente che, nella pratica, le due normative non sono sempre facilmente conciliabili, ispirandosi a principi e interessi

---

[82] Viceversa, come giustamente si sottolinea al considerando n. 124: «L'applicabilità dei requisiti del presente regolamento non dovrebbe pertanto incidere sulla logica, la metodologia o la struttura generale specifiche della valutazione della conformità a norma della pertinente normativa di armonizzazione dell'Unione».

[83] Conformemente ai principi generali di cui all'articolo 30 del regolamento (CE) n. 765/2008.

[84] Il fatto che sia il regolamento IA, sia il GDPR siano norme di applicazione trasversale (in un caso all'uso dei sistemi di AI in tutti gli ambiti eccetto che in quelli espressamente esclusi e nel GDPR nel caso di un qualsiasi trattamento di dati personali) assicura tra loro molte probabili sovrapposizioni o «cumuli» in G. CONTALDI, *Intelligenza artificiale e dati personali*, cit.

[85] E perciò probabilmente devolute a una risoluzione in via giudiziale.

[86] Su cui G. C. FERONI, *Intelligenza artificiale e ruolo della protezione dei dati personali*, 14 febbraio 2023, www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9855742.

parzialmente diversi[87]. Poiché esse però indubbiamente interagiscono, in particolare nel caso di sistemi di IA utilizzati per fini diagnostici e terapeutici che si basino anche sui dati sensibili[88], occorre domandarsi come il regolamento risolva queste "sovrapposizioni", tenendo anche presente che il fornitore di un sistema di IA potrebbe essere al contempo il «titolare del trattamento» ai sensi del GDPR.

Anzitutto, vi è parziale comunicazione tra i due atti rispetto all'obbligo di predisporre una valutazione d'impatto: sui diritti fondamentali ai sensi dell'art. 27 del regolamento IA e sulla protezione dei dati in base all'art. 35 del GDPR. Il par. 4 dell'art. 27 prevede che «se uno qualsiasi degli obblighi di cui al presente articolo è già rispettato mediante la valutazione d'impatto sulla protezione dei dati effettuata a norma dell'articolo 35 del regolamento (UE) 2016/679 o dell'articolo 27 della direttiva (UE) 2016/680, la valutazione d'impatto sui diritti fondamentali di cui al paragrafo 1 del presente articolo integra tale valutazione d'impatto sulla protezione dei dati». Ciò dovrebbe consentire al *deployer* del sistema ad alto rischio di ottimizzare gli sforzi, di fatto mimando quanto già fatto durante il DPIA, ma allargando la valutazione sulla protezione dei dati personali ad altri diritti fondamentali[89].

Sul punto, però, non possono sottacersi alcune criticità. Anzitutto, come appena anticipato, le due valutazioni, benché condividano uno stesso intento, hanno ambiti di applicazione diversi. Quindi, la FRIA non potrà limitarsi a richiamare la valutazione di impatto sulla protezione dei dati personali, ma dovrà anche preoccuparsi di altri diritti

[87] Molto si è detto sulle «*tensions and proximities between AI and data protection principles, such as, in particular, purpose limitation and data minimisation*», in G. SARTOR, F. LAGIOIA, *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*, EPRS_STU(2020)641530, 2020.

[88] Quest'uso è per altro doppio poiché: «*On the one hand, personal data may contribute to the data sets used to train machine learning systems, namely, to build their algorithmic models. On the other hand, such models can be applied to personal data, to make inferences concerning particularindividuals*», in G. SARTOR, F. LAGIOIA, *op. cit*.

[89] E che comprendono, in particolare, il diritto alla dignità, all'eguaglianza e alla non discriminazione, alla salute, ma anche ad alcuni diritti politici, come quelli alla libertà di espressione e all'elettorato passivo.

come la sicurezza, la salute e il principio di non discriminazione; per tacere in questa sede degli eventuali «rischi sistemici»[90].

In secondo luogo, la DPIA è richiesta alle condizioni e nei casi menzionati ai parr. 1 e 3 dell'art. 35 del GDPR, che non necessariamente coincidono con le condizioni (soggettive) stabilite ai sensi del regolamento sull'intelligenza artificiale. Come messo precedentemente in evidenza, infatti, la FRIA è richiesta solo a una categoria particolare di *deployer*, che siano, cioè, soggetti pubblici o che eroghino prestazioni essenziali[91]. Per questo, sarebbe stato allora forse più opportuno estendere la FRIA a tutti i sistemi ad alto rischio, come inizialmente richiesto dal Parlamento europeo, oppure prevedere un esplicito sistema di raccordo con il GDPR, ampliando l'applicazione della FRIA per tutti i titolari di trattamento di dati particolarmente sensibili, quali quelli sanitari.

Al GDPR si ispirano anche le misure tecniche ed organizzative necessarie a garantire la sicurezza dei sistemi di IA, improntate sul principio della sicurezza fin dalla progettazione, inscritto nell'art. 25 del GDPR, del quale, nondimeno, non si fa espressa menzione nel regolamento IA. Quest'ultimo richiama però la "pseudonimizzazione" in quanto «misura avanzata di sicurezza per la vita privata», anche ai sensi dell'art. 10, par. 5, lett. *b)* del regolamento IA.

In ambito sanitario, l'eventuale sovrapposizione dei due regolamenti solleva anche il problema dell'utilizzo dei dati sanitari (ai sensi dell'art. 9 del GDPR)[92], nell'ambito di un sistema incentrato su «processi decisionali automatizzati» (ai sensi dell'art. 22, par. 1, del GDPR), eventualmente anche al fine della «profilazione» (art. 4, par. 4 e art. 22, par. 4) del paziente.

In questi casi, i principi del GDPR sono rafforzati. Quello della "liceità" richiede che una espressa base giuridica per il trattamento venga rinvenuta, se non nel consenso espresso degli interessati, nelle lettere *g)* o *i)* del secondo paragrafo dell'art. 9 del GDPR e cioè nei

[90] Disciplinati dal regolamento.
[91] Si v. *supra.*
[92] Si tratterà in particolare di diagnosi, referti, immagini cliniche e informazioni genetiche. Lasciamo da parte il problema dei dati biometrici nonostante sia oggetto di grande attenzione da parte del regolamento IA nel caso in cui servano a identificare le persone (cosa che non dovrebbe riguardare l'ambito sanitario).

«motivi di interesse pubblico rilevante» o nei «motivi di interesse pubblico nel settore della sanità pubblica», i quali devono essere declinati sulla base del diritto dell'Unione o degli Stati membri. Questi ultimi, come noto, possono, ai sensi dell'ultimo paragrafo di questo articolo, porre «ulteriori limitazioni»[93].

L'intervento legislativo nazionale è auspicabile, secondo il «Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di Intelligenza Artificiale», al fine di assicurare un trattamento compatibile con il GDPR allorquando si operi senza il consenso esplicito dell'interessato. Come previsto anche dall'art. 22, par. 4, del GDPR. Infatti, le decisioni automatizzate, inclusa la profilazione, non possono basarsi sul trattamento di dati relativi alla salute, a meno che i dati siano trattati per motivi di pubblico interesse. Questa stessa base giuridica, inoltre, sarebbe anche in linea con quanto auspicato dalla Dichiarazione sui diritti e principi digitali, proclamata dal Parlamento europeo, dal Consiglio e dalla Commissione, nel 2023[94].

Questi motivi di interesse pubblico, però, non figurano espressamente nell'art. 10, par. 5 del regolamento IA, il quale consente ai fornitori l'utilizzo dei dati sensibili, inclusi quelli sanitari, «al fine di garantire il rilevamento e la correzione delle distorsioni in relazione ai sistemi di IA ad alto rischio», nel rispetto delle disposizioni del regolamento (UE) 2016/679, cioè dei principi della liceità e dell'espressa finalità del trattamento appena richiamati. Il corretto addestramento di un sistema di IA, posto che si tratti di «trattamento» ai sensi del GDPR, è una finalità di interesse generale? Questa domanda resta al momento inevasa. Con ogni probabilità, ad essa è destinato a dare risposta il legislatore nazionale, pur sempre nel rispetto del diritto dell'Unione.

In ultimo, sempre l'art. 22 del GDPR, questa volta al suo par. 3, richiede che sia assicurato «almeno l'intervento umano da parte del titolare del trattamento» in caso di una decisione basata unicamente sul trattamento automatizzato; mentre l'art. 14 del regolamento IA pone un

---

[93] Come è stato, in Italia, il caso dell'introduzione dell'art. 2-*sexies* del Codice della Privacy.

[94] Si v. in particolare il considerando n. 9 della Dichiarazione sui diritti e principi digitali. Sul tema, P. DE PASQUALE, *Sostenibilità e trasformazione digitale: paradigmi a confronto nella disciplina dell'Unione europea*, in *DUE*, n. 1, 2022, p. 67 ss.

obbligo di sorveglianza umana solo per l'uso di sistemi ad alto rischio, con conseguente sdoppiamento (o duplicazione?) dell'obbligo, per il titolare del trattamento ai sensi del GDPR e per il *deployer* di un sistema di IA.

3.3. Segue: *la coerenza con il regolamento sullo spazio europeo dei dati sanitari e con il regolamento relativo alla* governance *europea dei dati*

Infine, vi sono altri atti, almeno due, con i quali il regolamento sull'IA interagisce da vicino in ambito sanitario: il regolamento sullo spazio europeo dei dati sanitari (SEDS) e il c.d. *Data Governance Act*[95].

Infatti, il buon funzionamento di un sistema di IA è strettamente correlato alla quantità e qualità di dati che gli vengono forniti e dunque, per quel che qui in particolare ci interessa, con i meccanismi del c.d. «uso secondario» dei dati. Questi due atti, sebbene abbiano ambiti di applicazione diversi, intendono entrambi favorire lo scambio dei dati in spazi e condizioni sicure, al fine di creare un incentivo per la ricerca e l'innovazione.

In ambito sanitario, l'importanza della circolazione dei dati si accompagna al problema della loro qualità. Qui, infatti, eventuali inesattezze o errori contenuti *ab origine* nei dati trattati rischiano di produrre errori di profilassi, "*bias*" e gravi effetti discriminatori sul trattamento dei pazienti[96]. Si tratta di problemi da risolvere alla radice e, in tal senso, soccorre il regolamento sullo SEDS, il quale, ai sensi del considerando n. 43, persegue anche lo scopo di «sostenere lo sviluppo dell'IA in ambito sanitario». In base a tale regolamento è possibile rendere disponibili i dati relativi alla salute a fini diversi da quelli per i quali sono stati in principio raccolti, attraverso un meccanismo di

[95] Rispettivamente proposta di regolamento del Parlamento europeo e del Consiglio sullo spazio europeo dei dati sanitari e regolamento (UE) 2022/868 del Parlamento europeo e del Consiglio, del 30 maggio 2022, relativo alla *governance* europea dei dati e che modifica il regolamento (UE) 2018/1724 (regolamento sulla *governance* dei dati).

[96] Si tratta del problema della c.d. discriminazione algoritmica, su cui M. A. K., İBRAHIM, *Legal Challenges of Artificial Intelligence in Healthcare*, in M. KILIÇ, S. B. KAHYAOĞLU (eds.), *Algorithmic Discrimination and Ethical Perspective of Artificial Intelligence*, Singapore, 2023, p. 147 ss.

condivisione che, data la sua rilevanza di interesse pubblico, prescinde dal consenso del titolare dei dati[97].

In particolare, l'art. 34, par. 1, di questo regolamento elenca le finalità in base alle quali gli organismi responsabili possono fornire l'accesso ai dati sanitari elettronici a fini secondari. In particolare., le lettere *f), g) e h)* menzionano «attività di sviluppo e innovazione per prodotti o servizi che contribuiscono alla sanità pubblica o alla sicurezza sociale, oppure che garantiscono elevati livelli di qualità e sicurezza dell'assistenza sanitaria, dei medicinali o dei dispositivi medici»; «attività di addestramento, prova e valutazione degli algoritmi, anche nell'ambito di dispositivi medici, sistemi di IA e applicazioni di sanità digitale, che contribuiscono alla sanità pubblica o alla sicurezza sociale, oppure che garantiscono elevati livelli di qualità e sicurezza dell'assistenza sanitaria, dei medicinali o dei dispositivi medici»; l'«erogazione di un'assistenza sanitaria personalizzata che consiste nel valutare, mantenere o ripristinare lo stato di salute delle persone fisiche sulla base dei dati sanitari di altre persone fisiche».

Analogamente, il c.d. *Data Governance Act* consente il riutilizzo di categorie di dati detenuti da enti pubblici per finalità di interesse generale, come la ricerca scientifica e lo sviluppo di più efficienti politiche sanitarie. Esso si applica però solo ai c.d. «prodotti connessi» che saranno sviluppati in ambito sanitario[98] e consente all'utente che intende utilizzarli, o a un terzo indicato da quest'ultimo, di accedere ai dati ivi contenuti[99]. Inoltre, il capo IV regola il c.d. «altruismo dei dati», il quale consente il riutilizzo, senza consenso, dei dati forniti gratuitamente dall'utente per perseguire fini di interesse generale, tra i quali potrebbe, a ragione, rientrare il miglioramento della qualità delle cure e della salute delle persone[100].

In entrambi i casi, la possibilità di riutilizzo dei dati secondari dovrà sempre rispondere al rispetto del principio di esattezza iscritto nel

---

[97] Ma l'art. 33, par. 5, del regolamento SEDS prevede che il consenso può essere richiesto all'individuo sulla base del diritto nazionale qualora si tratti di fornire accesso ai suoi dati sanitari elettronici.
[98] Considerando n. 14 del regolamento (UE) 2022/868, cit.
[99] *Ibidem*, artt. 4 e 5.
[100] G. RESTA, *La dimensione collettiva dei dati personali*, in *Parolechiave*, 2023, p. 89 ss.

GDPR[101]. Ciò potrebbe comportare una riduzione *ex ante* del rischio di discriminazione, agendo direttamente sulla fase di addestramento degli algoritmi. In questa fase, come noto, la capacità del sistema di IA di effettuare predizioni corrette, relative, ad esempio, al rischio di sviluppare malattie o al decorso delle stesse, si basa sostanzialmente sul numero e sulla qualità dei dati forniti[102]. Questi ultimi sono tanto più accurati quanto più si basano su dati personali e sui c.d. *real world data experience*. Tutto ciò non può che avere un impatto benefico sul buon funzionamento dei sistemi di IA, garantendo il rispetto del regolamento.

3.4. Segue: *la coerenza con la legislazione in via di adozione*

Restano invece del tutto fuori dall'ambito di interferenza del regolamento IA una serie di atti e normative, sia da ridisegnare *ex novo*, come la proposta di direttiva sulla responsabilità per danno da prodotti difettosi in caso di danni prodotti dai sistemi di IA[103], sia da modificare, come nel caso del regolamento macchine[104] e della direttiva sulla sicurezza generale dei prodotti[105].

Lo stesso vale per le normative nazionali, destinate a integrare il regolamento IA, attraverso previsioni relative al diritto sulla responsabilità medica e al diritto penale.

In Italia, si segnala il disegno di legge in materia di «Disposizioni e delega al Governo in materia di intelligenza artificiale»[106], il quale emana norme che «si interpretano e si applicano conformemente al diritto dell'Unione Europea»[107]. Tra queste si segnalano in particolare le disposizioni relative al settore sanitario che prevedono il diritto dell'interessato ad essere informato circa l'utilizzo dei sistemi di IA; la

---

[101] Art. 5, par. 1., lett. *d)*, del GDPR.

[102] «*Data bias needs to be avoided by using appropriate algorithms based on un-biased real time data*» in N. NAIK ET AL., *Legal and Ethical Consideration in Artificial Intelligence in Healthcare: Who Takes Responsibility?*, in *Frontiers in Surgery*, vol. 9, 2022, p. 5.

[103] www.ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12979-Civil-liability-adapting-liability-rules-to-the-digital-age-and-artificial-intelligence/public-consultation_en

[104] www.ec.europa.eu/docsroom/documents/45508.

[105] www.eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0346.

[106] Disegno di legge S 1146, www.senato.it/service/PDF/PDFServer/DF/437373.pdf

[107] *Ibidem*, art. 2, par. 1.

spettanza dell'ultima decisione alla professione medica; la classificazione come «di rilevante interesse pubblico» dei trattamenti di dati, anche personali, da, parte di soggetti pubblici e privati senza scopo di lucro, «per la ricerca e la sperimentazione scientifica nella realizzazione di sistemi di IA per finalità di prevenzione, diagnosi e cura di malattie, sviluppo di farmaci, terapie e tecnologie riabilitative, realizzazione di apparati medicali, incluse protesi e interfacce fra il corpo e strumenti di sostegno alle condizioni del paziente, di salute pubblica, incolumità della persona, salute e sicurezza sanitaria, in quanto necessari ai fini della realizzazione e dell'utilizzazione di banche dati e modelli di base»[108].

4. *Brevi riflessioni conclusive*

È molto difficile, allo stato attuale, fare previsioni sul successo o meno del nuovo regolamento IA. Certo è che si tratta di uno sforzo di regolazione molto complesso e strutturato, che ha indubbiamente la grande aspirazione di fare da modello per la circolazione di una IA sicura ed affidabile. Questo modello si preoccupa di coniugare un approccio "classico" alla regolazione con uno particolarmente "innovativo". Quest'ultimo, come anticipato, tenta di integrare e allargare la normativa di armonizzazione dell'Unione sulla circolazione e sicurezza dei prodotti con considerazioni nuove, "sistemiche", volte a garantire la struttura portante del diritto dell'Unione: i suoi valori e i diritti fondamentali che esso garantisce.

La sicurezza e l'affidabilità dei sistemi di IA si basano su regole di "*compliance*", le quali, se rispettate, dovrebbero anticipare la protezione dei beni giuridici che l'Unione intende garantire in maniera "sistemica", tra i quali senz'altro rientra il diritto alla salute. La realizzazione di obiettivi così diversificati e ambiziosi, però, finisce col dipendere molto dalla buona volontà degli attori coinvolti[109], da una struttura di *governance* aperta e agile, dall'adozione di ulteriori atti

[108] *Ibidem*, art. 8, par. 1.
[109] Sul tema, A. SIMONCINI, E. CREMONA, *op. cit*.

delegati da parte della Commissione e di norme di attuazione da parte degli Stati membri[110].

La necessaria buona volontà degli attori coinvolti si deduce, in particolare, dalla tipologia di obblighi cui sono sottoposti i fornitori e i *deployer*. Obblighi che abbiamo definito come essenzialmente "procedurali", poiché volti a comprovare la coerenza dei comportamenti con le regole, al fine di garantire *ex ante* la sicurezza del sistema[111]. In alcuni casi, come quelli dei sistemi indipendenti, questo sforzo si concretizza però in una auto-valutazione non necessariamente obiettiva[112]. Per mitigare questo rischio, risulterà essenziale la definizione degli standard da parte di organismi come il CEN, il CENELEC e l'ETSI. Inoltre, lo stesso "*AI office*", di nuova creazione, si è già impegnato a fornire al più presto dei *templates* predefiniti al fine di certificare l'adeguatezza di tali sistemi.

Il regolamento, poi, potrebbe dar luogo a un'applicazione troppo lasca, anche a causa dell'inserimento di deroghe estremamente ampie. Ad esempio, i sistemi indipendenti, sebbene inseriti nell'Allegato III e dunque astrattamente classificabili come ad alto rischio, possono, in concreto, smarcarsi dall'applicazione degli ingenti obblighi scaturenti da tale livello di rischio, sulla base di una valutazione da essi stessi effettuata e non necessariamente sottoposta a verifica da parte di un organismo pubblico, in virtù dele deroghe inscritte nel par. 3 dell'art. 6 del regolamento.

Al momento mancano, in quest'ottica «proceduralizzante» ispirata al GDPR[113], adeguati controlli *ex post* sull'adeguatezza dei sistemi che

---

[110] Il regolamento, da questo punto di vista, costituisce infatti una sorta di "direttiva mascherata".

[111] Si tratta dunque di obblighi di "*compliance*", e per questo da noi definiti come essenzialmente procedurali. Si v. sul tema, G. GENTILE, *The (In)Effectiveness of EU Data Protection: A Rejoinder*, in I. SPIECKER, L. SCHERTEL FERREIRA MENDES, R. CAMPOS (eds.), *Digital Constitutionalism,* Baden-Baden, *forthcoming*.

[112] Tanto che in sede di parere il Comitato economico e sociale aveva suggerito di introdurre una valutazione della conformità da parte di un organo terzo per tutti i sistemi ad alto rischio.

[113] In senso favorevole alla proceduralizzazione, si v. F. DONATI, *Diritti fondamentali e algoritmi nella proposta di regolamento sull'intelligenza artificiale*, in *DUE*, nn. 3-4, 2021, pp. 456-457: «Nei sistemi di intelligenza artificiale, infatti, la tutela dei diritti deve essere garantita soprattutto nelle fasi di progettazione, di addestramento e di controllo sul funzionamento del software. A questa corretta filosofia si ispira la proposta di regolamento».

abbiano già ottenuto l'immissione nel mercato. Inoltre, l'idea di disciplinare *ex ante* la sicurezza di tali sistemi, al fine di prevenire *in nuce* la realizzazione di un rischio, mal si sposa con una applicazione del principio di precauzione, in particolare in materia sanitaria.

Infine, sempre nell'ottica "proceduralizzante" prescelta, lo spazio dedicato dal regolamento alla tutela della persona appare esiguo. Infatti, quest'ultima non figura come "beneficiario delle prestazioni" o come "destinatario delle decisioni algoritmiche" nel regolamento IA, neppure in presenza di una figura particolarmente vulnerabile come quella del paziente[114].

In quest'ultimo caso, la tutela della vita del paziente appare particolarmente complessa dacché, come noto, il diritto alle cure è un diritto "individuale" e "sociale", condizionato dalle capacità dello Stato di offrire un adeguato servizio sanitario. Quest'ultimo dovrà quindi necessariamente confrontarsi con lo sviluppo dei sistemi di IA da utilizzare nella rete del servizio sanitario, conformandosi al regolamento, ma al contempo definendo e implementando quegli obiettivi di interesse generale di cui rimane il principale garante.

[114] H. VAN KOLFSCHOOTEN, *EU regulation of artificial intelligence: Challenges for patients' rights*, in *CMLR*, n. 1, 2022, p. 81 ss.

ABSTRACT (ITA)

In questo scritto ci occupiamo di analizzare l'applicazione del regolamento sull'intelligenza artificiale dell'Unione europea all'ambito sanitario e della tutela della salute, considerati uno dei c.d. "settori ad alto impatto" che maggiormente saranno riguardati da tale nuova disciplina. Per questo, particolare attenzione è dedicata allo studio della classificazione dei sistemi c.d. "ad alto rischio" e degli obblighi gravanti sugli operatori. Successivamente è analizzata la coerenza di questo nuovo quadro regolatorio con le norme già in vigore, che disciplinano ambiti affini o che comunque a questo rischiano di sovrapporsi per oggetto o per scopo. In ultimo, tentiamo di ragionare sulle modalità e sull'efficacia dell'approccio regolatorio prescelto al fine di assicurare la tutela del diritto alla salute, in ossequio ai fini dichiarati dal legislatore stesso.

ABSTRACT (ENG)

In this paper, we analyze the application of the EU Artificial Intelligence Regulation in the field of health and health protection, considered one of the so-called "high-impact sectors" that will be most affected by this new discipline. For this reason, particular attention is dedicated to the study of the classification of so-called "high-risk" systems and the obligations on these burdens, as this class will include most of the AI systems to be used in the sector of our concern. Subsequently, we investigate the consistency of this new regulatory framework with the rules already in force, which regulate similar areas, or which can overlap with the AI Act by object or purpose. Still, a general framing is dedicated to the legislations of future entry into force. Finally, we try to think about the methods and effectiveness of the regulatory approach chosen and its capability to ensure the protection of the right to health, in accordance with the purposes declared by the EU legislator itself.