Le norme tecniche armonizzate nei sistemi di Intelligenza artificiale per la sanità*

Antonio Iannuzzi

Professore ordinario di Diritto costituzionale e Diritto pubblico presso l'Università di Roma Tre. Mail: antonio.iannuzzi@uniroma3.it

Trattare il tema delle norme tecniche armonizzate nella sanità digitale, impone di considerare anche la disciplina dei dati, dell'Intelligenza artificiale e della cybersicurezza, perché la sanità digitale non può essere considerata come un ambito materiale isolato, anzi è fortemente interrelata con gli altri settori della società digitale. Se si assume questa prospettiva l'ecosistema normativo di riferimento è davvero composito. La complessità del quadro normativo rende articolato anche il livello delle norme armonizzate e delle specifiche tecniche che dovranno implementare le fonti di *hard law*. Il compito che impegnerà noi giuristi nei prossimi mesi sarà, intanto, quello di comporre il variegato mosaico normativo, fornendo criteri interpretativi che possano orientare l'applicazione di tutte le disposizioni normative.

A partire dall'adozione della Strategia europea dei dati del 2020, l'approccio dell'UE alla regolazione delle tecnologie digitali ha cambiato passo. Mentre in passato l'approccio alle nuove tecnologie favoriva l'auto-regolazione privata in "luogo della legge", per via di un massiccio rinvio alle norme armonizzate prodotte da enti di normalizzazione, a partire dalla scorsa legislatura europea si è registrata, invece, una decisa inversione di tendenza che politicamente è stata squadernata come la volontà di affermare una «sovranità digitale» condivisa a livello di Ue. Questo indirizzo politico si è tradotto, dal punto di vista della politica delle fonti, in un deciso "riaccentramento delle fonti", come ho avuto modo di sostenere, che si caratterizza per un abbondante utilizzo dello strumento dei regolamenti e delle direttive. In questo nuovo quadro, le norme tecniche armonizzate finiscono per diventare uno strumento di co-regolazione, perché il loro spazio di intervento risulta delimitato da principi e norme che si affermano nei regolamenti e nelle direttive dell'Ue.

Nello specifico dei sistemi di AI per la sanità vengono in rilievo diversi atti normativi derivati dell'UE.

Nel Regolamento europeo n. 1689/2024, che stabilisce regole armonizzate sull'intelligenza artificiale (AI Act), i sistemi di AI ad alto rischio, tra i quali come si vedrà sono annoverati diversi sistemi di sanità digitale, se rispettano le norme armonizzate o parti di esse si presumono conformi ai requisiti essenziali di cui al capo II dello stesso regolamento, secondo quanto previsto dall'art. 40. L'immissione nel mercato di sistemi di intelligenza artificiale ad alto rischio è, in questo modo, subordinata ad una verifica che sarà operata attraverso la certificazione secondo la procedura di marchio di conformità europea (marchiatura CE), già in uso per regolare la circolazione di numerosi prodotti nel mercato europeo. Allo stesso modo, i sistemi di IA ad alto rischio che sono stati certificati o per i quali è stata rilasciata una dichiarazione di conformità nell'ambito di un sistema di cybersicurezza, a norma del regolamento (UE) 881/2019 del Parlamento europeo e del Consiglio, si presumono conformi ai requisiti di cybersicurezza di cui all'articolo 15 dell'AI Act, nella misura in cui tali

* La presente pubblicazione è finanziata dall'Unione europea – Next Generation EU, nell'ambito del bando PRIN 2022, progetto "MEDICINE+AI, Law and Ethics for an Augmented and Human-Centered Medicine" (2022YB89EH) – CUP E53D23007020006.

requisiti siano contemplati nel certificato di cybersicurezza o nella dichiarazione di conformità o in parti di essi (art. 42, par. 2)[1]. Com'è stato sottolineato, si esclude «l'autorizzazione pubblica», che avrebbe offerto «maggiori certezze e garanzie in ordine alle verifiche sulla sicurezza del prodotto, presentando però costi non irrilevanti in termini amministrativi e di efficienza», per affidarsi alla procedura di marchio di conformità europea, ponendo così i controlli a carico del produttore, in modo da rendere più agevole l'immissione del prodotto nel mercato e facendo transitare sugli operatori economici la responsabilità di assicurare il rispetto dei requisiti di sicurezza stabiliti dalla normativa[2]. Questo tema della sfiducia implicita verso l'amministrazione pubblica si ripete nel Regolamento (UE) 2022/868, che detta norme sulla governance dei dati (DGA), come risulta dalle relazioni di accompagnamento. Su queste reiterate dichiarazioni di sfiducia verso le capacità delle amministrazioni pubbliche pongo l'attenzione perché è un punto su cui riflettere. La sensazione è che stia emergendo la necessità di una amministrazione europea più strutturata che supporti la Commissione o in alternativa amministrazioni nazionali più competenti sulle questioni che pongono le tecnologie digitali.

La classificazione di molti sistemi di sanità digitale tra i sistemi di AI ad alto rischio dipende dall'art. 6 del Regolamento che li include in quanto prodotti che sono soggetti 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 queste normative sono indicate il Regolamento (UE) 2017/745 sui dispositivi medici e il Regolamento (UE) 2017/746 sui dispositivi medico-diagnostici in vitro. Pertanto, i sistemi di AI utilizzati in dispositivi medici o diagnostici in vitro rientrano nella categoria ad alto rischio. Le norme tecniche armonizzate che disciplineranno i sistemi di AI per la sanità, di conseguenza, dovranno essere conformi e coerenti anche a questi ultimi due regolamenti per assicurare uniformità di valutazione. Il compito delle norme tecniche armonizzate nella sanità digitale sarà delicato perché dovrà consentire di presumere la conformità ai principi ed alle norme dell'AI Act assicurando che non si verifichino discriminazioni o allucinazioni algoritmiche nelle diagnosi, evitando l'insorgenza di procedure algoritmiche e trattamenti di dati non trasparenti o risultati non supervisionati dall'uomo. Le norme tecniche armonizzate, in definitiva, divengono atti che, «pur essendo stati indubbiamente adottati da organi che non possono essere qualificati come «istituzioni, organi o organismi dell'Unione», presenta(va)no tuttavia la natura di misure di attuazione o di applicazione di un atto di diritto dell'Unione» e finiscono per dare «concretizzazione a un livello tecnico dei requisiti essenziali» delle fonti derivate dell'UE[3].

La categoria dei sistemi di AI ad alto rischio, a cui appunto appartengono i sistemi di IA per la sanità, poiché sono parte integrante di un prodotto già regolamentato dall'UE, sono già soggetti a una valutazione di conformità *ex ante*, sulla scorta della precedente normativa. Per questa ragione l'AI Act non aggiunge una nuova valutazione di conformità, ma prevede norme tecniche

[1] In tema v. E. LONGO, *Le pratiche di IA vietate e i sistemi di IA ad alto rischio: metodi e strumenti per la società del "rischio digitale"*, in F. PIZZETTI, S. CALZOLAIO, A. IANNUZZI, E. LONGO, M. OROFINO, *La regolazione europea dell'Intelligenza artificiale nella società digitale*, Torino, 2025, 87 ss.

[2] C. CASONATO, B. MARCHETTI, *Prime osservazioni sulla proposta di regolamento dell'Unione europea in materia di intelligenza artificiale*, in *BioLaw Journal*, 3, 2021, 430 ss.

[3] Corte di Giustizia, causa C-613/14, *James Elliott Construction Limited contro Irish Asphalt Limited*.

ISSN 2284-4503

armonizzate che vanno ad integrare le precedenti e ad aggiungere un obbligo di aggiornamento della normativa preesistente in tema di valutazione del rischio, di trasparenza, di qualità dei dati ed anche di sorveglianza post-commercializzazione, al fine di garantire un adeguato livello di sicurezza ed il rispetto dei diritti fondamentali degli utenti.

L'AI si alimenta di dati. In questo quadro già ricco, perciò, si innesta, oltre ovviamente al Regolamento (UE) 2016/679, Regolamento generale sulla protezione dei dati personali (GDPR), ora il Regolamento (UE) 2025/327 che istituisce lo Spazio europeo dei dati sanitari (EHDS), pubblicato il 18 marzo.

La creazione dello spazio settoriale comune dei dati sanitari costituisce l'attuazione di un pilastro importante della Strategia europea per i dati, che ha l'obiettivo di creare un mercato unico digitale orientato ad assicurare competitività globale e sovranità dei dati condivisa a livello di UE. In particolare, l'EHDS persegue la finalità di migliorare l'accesso, la gestione e la condivisione dei dati sanitari a livello transfrontaliero per assicurare maggiore sicurezza, efficienza e qualità dei servizi sanitari.

Sul piano delle regole sostanziali, l'EHDS rappresenta il primo banco di prova del nuovo bilanciamento che l'UE vuole individuare tra *data protection* e circolazione dei dati. Di fatti, è la prima concretizzazione settoriale del già citato DGA, che detta le regole trasversali o intersettoriali relative all'uso secondario dei dati. Il problema che si pone, però è che alla prima applicazione delle regole del DGA sul *data sharing* e sul *data altruism*, lo EHDS impone subito delle eccezioni, a prima vista comprensibili stante le particolarità del settore sanitario, alla regola generale, che se così è, rischia di non applicarsi ancora. Perché nelle intenzioni dell'UE la prima applicazione settoriale del DGA doveva essere proprio fornita dal settore sanitario. Ed invece il Considerando 59 dell'EHDS afferma, senza motivare, che gli intermediari di dati sanitari – che dovrebbero essere persone giuridiche in grado di trattare, rendere disponibili, registrare, fornire o scambiare dati sanitari elettronici per l'uso secondario forniti da titolari dei dati, o limitarne l'accesso – svolgono compiti diversi da quelli dei servizi di intermediazione dei dati nell'ambito del regolamento (UE) 2022/868.

Una questione problematica che si pone è la seguente: se già oggi si fa fatica a livello europeo ad individuare i soggetti terzi che dovranno favorire lo scambio o l'altruismo di dati, si può immaginare che dare effettiva applicazione a questi istituti nell'ambito sanitario potrebbe non essere operazione né semplice né immediata. L'EHDS, in particolare, istituisce *l'obbligo* per gli Stati membri di aderire alla piattaforma MyHealth@EU che mira a favorire la circolazione transfrontaliera dei dati sanitari. È opportuno ricordare che, al fine di perseguire tale finalità, nel quadro delle azioni volte al conseguimento degli obiettivi della direttiva (UE) 2011/24, era già stata istituita un'infrastruttura *volontaria* denominata appunto (MyHealth@EU). Attraverso detta infrastruttura digitale, gli Stati membri avevano iniziato ad offrire alle persone fisiche la possibilità di condividere i loro dati sanitari elettronici personali con prestatori di assistenza sanitaria in occasione di viaggi all'estero.

Le misure necessarie per lo sviluppo tecnico della piattaforma sanitaria europea riguardanti la sicurezza, la riservatezza e la protezione dei dati sanitari elettronici personali, nonché le condizioni per i controlli di conformità necessari per aderire e rimanere collegati a MyHealth@EU dovranno essere adottate dalla Commissione europea.

A livello nazionale non dovrebbero esserci particolari problemi per l'adeguamento alle misure

normative europee sia a livello infrastrutturale, sia a livello normativo.

Il riferimento va in particolare alla Piattaforma Nazionale di Telemedicina (PNT), il cui sviluppo è stato presentato il 4 febbraio da Agenas, quale soggetto attuatore della linea di investimento prevista dal Piano Nazionale di Ripresa e Resilienza (M6C1 Investimento 1.2.3.1), nonché come Agenzia Nazionale per la Sanità Digitale, ai sensi della Legge 28 marzo 2022 n. 25.

Il 31 dicembre 2024 il Ministero della Salute ha approvato il decreto dell'Ecosistema Dati Sanitari (EDS), che dal 2022 era oggetto di una interlocuzione "faticosa" con il Garante della Protezione dei dati personali. L'EDS è una piattaforma che costituisce "il collante della nuova sanità digitale" perché garantisce l'integrazione tra il Fascicolo sanitario elettronico (FSE), la telemedicina, il sistema Tessera sanitaria e l'utilizzo di AI, garantendo la gestione dei dati a livello nazionale, per finalità di cura, prevenzione, ricerca, governo e programmazione sanitaria. L'EDS consentirà di leggere storia clinica completa e il *Patient Summary*, permettendo così agli operatori sanitari di evitare prescrizioni ripetitive o inappropriate; la disponibilità di dati strutturati, sulle quali basare decisioni cliniche più accurate; un sistema di *alert* e notifiche, che avvisino il medico della presenza di referti e dati collegati a specifiche prestazioni.

Alla luce di questa ricostruzione dell'ecosistema normativo e infrastrutturale della sanità digitale, è ora possibile tornare ad esaminare il livello delle norme tecniche armonizzate.

Su questo versante, lo EHDS segue un modello diverso rispetto al favore che generalmente l'UE esprime per l'auto-regolazione privata e la co-regolazione, evidentemente partendo dall'idea dell'inopportunità politica di demandare ampi spazi di normazione agli enti privati di normazione in questo ambito materiale. Il Regolamento sugli spazi dati sanitari opta, piuttosto, per un affidamento ai pubblici poteri del potere di adozione di regole e specifiche tecniche, canalizzando questi poteri nelle mani della Commissione europea. Questo schema sembrerebbe in astratto garantire meglio la tutela dei numerosi diritti coinvolti. Immagino, però, che l'esercizio in concreto di queste competenze presupporrà l'impostazione di un metodo di lavoro improntato ad assicurare una virtuosa cooperazione fra pubblico e privato, perché faccio fatica a pensare che si possa pensare di escludere da questo processo gli enti di normazione che sono in possesso di conoscenze tecniche al momento non surrogabili dai poteri pubblici.

Questi poteri così penetranti della Commissione vanno ad aggiungersi a quelli che il Regolamento (UE) 1025/2012 sulla normazione europea le assegna nell'ambito della produzione delle norme tecniche armonizzate.

A norma del regolamento sulla normazione europea, la Commissione ha il potere di conferire il mandato di normazione. Dopo aver ricevuto il mandato, gli enti di normazione europei sono sottoposti all'obbligo di informazione verso la stessa su tutte le attività connesse all'elaborazione della norma richiesta. La commissione poi valuta la conformità dei documenti e la proposta che ha ricevuto rispetto alla richiesta iniziale. Se tale valutazione ha esito positivo la Commissione provvede alla pubblicazione degli estremi di tale norma sulla Gazzetta ufficiale dell'Unione europea. Un ruolo importante nell'organizzazione della Commissione è svolto dal *Joint Research Centre* (JRC), che ha il comito di assistere la Commissione in ogni questione concernente la normazione europea, «prestando la dovuta attenzione ai pareri degli esperti del settore» (Considerando 47), operando in collaborazione con le organizzazioni di normazione e con quelle dei soggetti interessati (art. 23).

Alla luce di quanto sin qui detto, affido la conclusione ad un ventaglio di domande. Viene da chiedersi, intanto, se la Commissione europea riuscirà a svolgere effettivamente e tempestivamente questo ruolo. Ma c'è da interrogarsi, anche, sull'adeguatezza della scelta normativa: è la Commissione europea la sede costituzionale ideale in cui operare questi contemperamenti di interessi o questa ancora non sconta nell'architettura istituzionale dell'Ue quel deficit di democrazia che sconsiglia l'attribuzione di poteri così intensi, spesso non eminentemente tecnici?[4]. Da ultimo, viene ancora da chiedersi, sotto il profilo della politica delle fonti del diritto, se gli atti di esecuzione della Commissione europea rappresentino la fonte più appropriata per dettare le regole e le specifiche tecniche armonizzate per i sistemi di AI in sanità, anche sotto il vantaggio della flessibilità che una fonte che detta queste norme deve necessariamente possedere.

[4] Sul punto v. O. POLLICINO, *Regolazione e innovazione tecnologica nell' "ordinamento della rete" (versione provvisoria)*, Relazione al XXXIX Convegno annuale dell'Associazione Italiana dei Costituzionalisti, "La libertà di manifestazione del pensiero", 15 e 16 novembre 2024, Università degli Studi di Salerno, reperibile al seguente link: https://www.associazionedeicostituzionalisti.it/images/convegniAnnualiAIC/2024_Salerno/Oreste_Pollicino.pdf.

ISSN 2284-4503