L'uso di sistemi di IA in ambito medico: qualche strategia per un'amministrazione sanitaria compliant con le regole europee e capace di affrontare la sfida*

Barbara Marchetti
Professoressa ordinaria di Diritto amministrativo, Università di Trento. Mail: barbara.marchetti@unitn.it

Mano a mano che le amministrazioni impegnate nel servizio sanitario si dotano di sistemi di IA che hanno un impatto sul rapporto medico paziente, sulle prestazioni di cura, sul lavoro organizzativo e burocratico delle strutture impegnate in tale ambito, sorge la necessità di apprestare misure e azioni capaci di affrontare tale sfida e di rispettare gli obblighi imposti dell'*Artificial Intelligence Act* europeo (reg. Ue 2024/1689), che come è noto riguarda sia chi fornisce sistemi e chi li impiega nello svolgimento dei propri compiti[1].

In questo breve scritto, vorrei fare qualche considerazione sull'impatto che la compliance alle regole europee avrà in termini organizzativi e di governance delle amministrazioni sanitarie, al fine di identificare compiti e adempimenti che queste ultime dovranno imparare a svolgere. Il focus di queste note non è dunque il rapporto tra medico e IA, ma è incentrato piuttosto sull'organizzazione amministrativa, la quale è chiamata ad assicurare le condizioni migliori affinché l'interazione tra personale sanitario e sistemi di IA sia fruttuosa e corretta.

In questa logica, un primo punto che vorrei toccare riguarda le decisioni che rilevano nella fase di programmazione: l'amministrazione deve anzitutto comprendere i bisogni tecnologici per lo svolgimento dei propri compiti e servizi, deve poi decidere come questi bisogni possano o debbano essere soddisfatti e, infine, disporre le attività necessarie per l'acquisizione delle applicazioni migliori a soddisfarli.

In questa fase, di grande rilevanza strategica, essa è dunque chiamata a considerare e soppesare numerosi fattori: accanto ad una valutazione costi/benefici (in cui rientrano l'interesse ad una gestione efficiente del servizio, le ricadute per il livello delle prestazioni di cura, i costi finanziari ed ambientali la cybersecurity, la gestione dei dati) l'amministrazione deve stabilire come procurarsi tali applicazioni (tramite autoproduzione, società in house, o il ricorso a fornitori privati esterni) e deve valutare il grado di rischio legato all'uso di determinate applicazioni di IA[2].

Con riguardo a queste ultime, il regolamento europeo adotta, come è noto, un approccio proporzionato al rischio, che distingue tra sistemi a rischio inaccettabile, cui corrisponde un regime di divieto, a rischio alto, cui corrispondono obblighi di conformità a taluni requisiti stabiliti negli artt. 9-15, a rischio non elevato, per i quali sono

* 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

[1] La bibliografia sull'AI Act è ormai vasta: tra i molti v. C. NOVELLI, F. CASOLARI, A. ROTOLO, M. TADDEO, L. FLORIDI, *AI Risk Assessment: A Scenario-based Proportional Methodology for the AI Act*, in *Digital Society*, 2024, scaricabile da https://link.springer.com/article/10.1007/s44206-024-00095-1; F. DONATI, *Diritti fondamentali e algoritmi nella proposta di regolamento sull'intelligenza artificiale*, in *Dir. un. eur.*, 2021, 3-4, 453. Sia consentito rinviare anche a C. CASONATO, B. MARCHETTI, *Prime osservazioni sulla proposta di regolamento dell'Unione europea in materia di intelligenza artificiale*, in *Biolaw Journal*, 3, 2021, 415.

[2] In argomento cfr. B. MARCHETTI, L. TORCHIA, *AI and Public Administration*, in F. DECAROLIS, B. MARCHETTI, L. TORCHIA (eds), *The EU Digital Regulation and its impact on member States*, Cham, 2025 (in stampa).

ISSN 2284-4503

previsti sostanzialmente solo obblighi di trasparenza, e a rischio minimo, per i quali vale un principio di libera circolazione nel mercato europeo, salva l'adozione spontanea a codici di condotta[3].
In termini generali, i sistemi di IA utilizzati in medicina sembrerebbero collocarsi tra i sistemi ad alto rischio, sia perché nella individuazione di tali applicazioni l'art. 6 del regolamento fa riferimento all'all. III, in cui rilevano i sistemi che sono impiegati per regolare l'accesso ai servizi pubblici essenziali (sanità, istruzione), sia perché la medesima norma rinvia, sotto altro profilo, ai sistemi destinati ad essere utilizzati come componenti di sicurezza di un prodotto (o ai sistemi che siano essi stessi un prodotto) disciplinati dalla normativa di armonizzazione dell'Unione elencata nell'allegato I, e per i quali è prevista una valutazione di conformità da parte di soggetti terzi. Tra queste norme di armonizzazione, rilevano in particolare i sistemi contemplati dal reg. 2017/745 sui dispositivi medici e il reg. 2017/746 sui dispositivi medico-diagnostici.
Tuttavia, l'appartenenza dei sistemi di IA per uso medico alla categoria dell'alto rischio sconta alcuni margini di incertezza. In particolare, a seguito del trilogo, l'articolo 6 ha subito una modifica significativa, perché, il terzo comma, superando la presunzione di alto rischio espressa nel comma precedente, stabilisce che non debba considerarsi ad alto rischio un sistema che, pure operante nei settori elencati dall'all. III, non presenta un rischio significativo di danno per la salute e la sicurezza o i diritti fondamentali delle persone fisiche, *anche nel senso di non influenzare materialmente il risultato del processo decisionale*. Quest'ultima situazione, più specificamente, si verificherebbe nelle seguenti circostanze: quando il sistema esegua solo un compito procedurale limitato, quando sia destinato a migliorare il risultato di un'attività umana precedentemente completata, quando sia destinato a rilevare agli schemi decisionali o deviazioni da schemi decisionali precedenti e non è finalizzato a sostituire e influenzare la valutazione; quando infine sia destinato a eseguire un compito preparatorio per una valutazione pertinente ai fini dei casi d'uso elencati nell'all. III.
Ora, tali fattispecie di esenzione dell'alto rischio implicano una valutazione complessa[4], dato che non pare compito semplice stabilire, in concreto, quando un sistema influenza materialmente una decisione o quando ha natura solamente preparatoria oppure è idoneo solo a migliorare una decisione umana. In attesa, dunque, che la Commissione provveda a fornire delle indicazioni per una corretta applicazione di queste classi di esenzione, e che la prassi inizi ad operare, le amministrazioni sanitarie sono chiamate ad operare una delicata classificazione, che ha come scopo l'inclusione o meno di una determinata applicazione all'interno del regime di alto rischio.
Ora, pare a chi scrive che sarebbe auspicabile che queste ultime optassero per un'interpretazione il più possibile estensiva del regime dell'alto rischio. In questo senso, le strutture sanitarie potrebbero "largheggiare" nel prevedere il necessario rispetto dei requisiti previsti dal regolamento europeo per la categoria dell'alto rischio ed esigere che tutti i sistemi che, pur apparentemente suscettibili di esserne esentati ai sensi delle lettere da a) a d) del comma terzo dell'art. 6, possano avere un impatto sulla relazione di

[3] C. Novelli, F. Casolari, A. Rotolo, M. Taddeo, L. Floridi, *AI Risk Assessment: A Scenario-based Proportional Methodology for the AI Act*, cit.
[4] Un discorso a parte meriterebbe, poi, il tema della classificazione dei c.d. chatbot medici, rappresentati da Large Language Model (LLM) in grado di fare diagnosi e indicare trattamenti di cura, il cui impiego crescente (ad esempio negli Stati Uniti) sia da parte di operatori sanitari e medici, sia da parte di pazienti, richiede distinguo e precisazioni che non possono essere compiutamente svolti in questa sede.

cura siano aderenti a quanto prescritto dal reg. Ue 2024/1689 agli artt. 9-15, rispondano cioè alle regole per i sistemi ad alto rischio.

Un tale approccio precauzionale, che ovviamente non sarebbe necessario per quei sistemi che svolgessero solo compiti operativi e burocratici (ad esempio, di smistamento della posta elettronica interna, di organizzazione degli appuntamenti medici o di fissazione dei turni di lavoro del personale) avrebbe l'effetto di rendere ammissibile l'impiego di tali dispositivi medici solo quando sviluppati in conformità a corrette policy di gestione dei dati, aderenti alle regole sulla sufficiente trasparenza e disegnati in modo da essere sorvegliati dal medico o dall'operatore sanitario, per il sol fatto di avere un qualche ruolo nella catena di formazione delle decisioni.

L'estensione delle regole sull'alto rischio anche al di là di quanto strettamente richiesto dal regolamento avrebbe, tra l'altro, la conseguenza di predisporre le azioni di mitigazione dei rischi previste dagli artt. 26 e 27 del regolamento in capo all'utilizzatore, ciò che imporrebbe all'amministrazione di effettuare anche la valutazione di impatto sui diritti fondamentali, la quale potrebbe rivelarsi importante per contenere i rischi di bias legati ai dati utilizzati nell'addestramento dei sistemi.

Un secondo aspetto, su cui preme richiamare l'attenzione, è relativo alle politiche rivolte al personale sanitario e prende spunto dall'art. 4 del regolamento europeo, intitolato *Alfabetizzazione in materia di IA*. La collocazione di questa disposizione tra le norme di apertura del regolamento esprime bene la rilevanza di questa sfida per il legislatore europeo, il quale considera il raggiungimento di questo obiettivo un presupposto fondamentale per garantire un'IA affidabile e umano-centrica. Stabilisce l'art. 4 che «I fornitori e gli utilizzatori dei sistemi di IA adottano misure per garantire nella misura del possibile un livello sufficiente di alfabetizzazione in materia di IA del loro personale nonché di qualsiasi altra persona che si occupa del funzionamento e dell'utilizzo dei sistemi di IA per loro conto, prendendo in considerazione le loro conoscenze tecniche, la loro esperienza, istruzione e formazione nonché il contesto in cui i sistemi di IA devono essere utilizzati, e tenendo conto delle persone o dei gruppi di persone su cui i sistemi di IA devono essere utilizzati».

Questo della formazione e delle competenze è, dunque, un altro tema fondamentale con cui le strutture sanitarie si devono confrontare apprestando percorsi convincenti che mirino a dotare il proprio personale delle conoscenze necessarie a comprendere l'IA, ma anche a garantirne il continuo aggiornamento, in considerazione della costante e rapida evoluzione della tecnologia.

Un terzo e ultimo punto, invece, riguarda l'applicazione dell'articolo 26 del regolamento, il quale prescrive gli obblighi del *deployer.*

Molto spesso l'amministrazione sanitaria non ha la capacità (sia per le limitate competenze interne sia per la mancanza di disponibilità finanziarie) di sviluppare in house il sistema di IA, ponendosi come mero utilizzatore dello stesso. L'art. 26, individuando gli obblighi che il *deployer d*eve osservare quando impiega un sistema ad alto rischio, fissa in particolare quattro ordini di azioni: egli deve adottare le misure necessarie per assicurare che l'impiego del sistema di IA avvenga in base alle istruzioni d'uso; deve affidare la sorveglianza umana a persone dotate delle competenze, della formazione, dell'autorità e del supporto necessari; deve assicurare che i dati di input siano sufficientemente rappresentativi e rilevanti per la finalità per cui il sistema è impiegato. E, quando ha ragione di ritenere che l'impiego del sistema in osservanza delle istruzioni d'uso presenta dei rischi, deve senza ritardo

informare il provider e l'autorità di vigilanza competente e sospenderne l'uso.

Come pare evidente dal tenore della legge e dalla natura delle obbligazioni, si tratta di azioni che debbono essere intraprese dalla struttura nel suo complesso e non dal singolo medico, benché spetti poi all'operatore sanitario il concreto ruolo di utilizzatore e controllore del sistema e dei suoi output.

Ora, benché la natura di tali azioni sia in gran parte chiara, sembra problematico esigere dall'utilizzatore il controllo sui dati di input. Stabilisce la norma che «nella misura in cui esercita il controllo sui dati di input, il *deployer* garantisce che tali dati di input siano pertinenti e sufficientemente rappresentativi alla luce della finalità prevista dal sistema di IA ad alto rischio».

Il punto, in particolare, parrebbe il seguente. Se il sistema è stato sviluppato in house, l'amministrazione ha chiaramente un controllo sui dati, in larga parte pubblici, e ne conosce le caratteristiche anche in termini di rappresentatività. Supponiamo che si tratti di un sistema di IA sviluppato da un consorzio di amministrazioni sanitarie e società in house pubbliche, con cui si predicono i possibili effetti di una malattia neuro-generativa, addestrato con dati provenienti dalle medesime istituzioni, tutte presenti sul territorio italiano.

Diverso però è il caso in cui il sistema sia stato acquistato sul mercato da un fornitore privato, in ipotesi statunitense o cinese. In questo caso, il *deployer* può non conoscere i dati di addestramento, vuoi perché il fornitore non glieli fornisce, vuoi perché l'algoritmo è coperto da privativa industriale.

In questo caso, come può essere rispettata questa obbligazione e garantita la rappresentatività? Nel Regno Unito, un caso simile, in cui un'autorità pubblica non era stata in grado di spiegare da dove provenissero i dati di addestramento di un sistema di riconoscimento facciale (nel caso di specie la società fornitrice aveva opposto un diniego), ha portato alla condanna dell'amministrazione per violazione delle regole di *fairness*[5].

Si tratta, anche in questo caso, di problemi interpretativi di non facile definizione, per i quali occorrerà vedere come il regolamento vivrà nelle prassi delle amministrazioni e nelle concrete applicazioni che ne faranno fornitori e utilizzatori, e per lo specifico settore indagato, società tech, strutture sanitarie e medici.

Certo è che le amministrazioni devono dotarsi rapidamente di efficaci meccanismi di governance interna dell'IA. Solo attraverso una adeguata capacità di programmazione e di gestione delle applicazioni tecnologiche ed una solida formazione degli operatori sanitari, infatti, l'IA potrà coniugarsi in modo virtuoso con i tratti più umani ed empatici delle professioni sanitarie.

[5] Si tratta del caso *R (Bridges) v. Chief Constable of South Wales.*

ISSN 2284-4503