Cosa pensa il Garante privacy italiano dell'uso dell'Intelligenza artificiale nel settore sanitario?

di Riccardo Calvara - pubblicato su "www.irpa.eu" - Osservatorio sullo Stato digitale, 29 novembre 2023

Lo scorso 10 ottobre 2023 il Garante italiano per la protezione dei dati personali ha pubblicato il "Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di Intelligenza artificiale". Il documento, di agevolissima lettura, si compone di dieci punti e raccoglie una serie di regole e principi atti a regolare la diffusione dei sistemi di Intelligenza artificiale nel mondo della sanità, con un particolare focus sulla tutela dei dati personali dei soggetti potenzialmente coinvolti.

L'impiego di strumenti di intelligenza artificiale nel settore della salute è destinato ad assumere un ruolo sempre più determinante. Gli algoritmi di intelligenza artificiale, infatti, possono essere impiegati con efficacia ed efficienza in tutte le fasi del servizio sanitario. Essi trovano agevole ingresso nella fase della programmazione della spesa e/o dell'offerta sanitaria, nelle fasi di presa in carico, diagnosi e cura del paziente, nei processi di rendicontazione dell'attività svolta dai medici e dalle strutture sanitare.

Per espletare le loro funzioni, tuttavia, gli algoritmi di intelligenza artificiale hanno bisogno di materia prima, ovvero, di dati: dati sui cui "girare", dati sui cui allenarsi, dati e informazioni da cui apprendere e migliorare le proprie capacità di risposta. Tuttavia, in ambito sanitario molti dei dati da trattare sono inevitabilmente dati relativi alla salute delle persone fisiche coinvolte. Ciò rende particolarmente complesso l'accesso alle banche dati da parte degli sviluppatori di sistemi di IA e delle strutture sanitarie I dati sanitari, infatti, sono una delle "categorie particolari di dati" che il Regolamento UE 2016/679 cd. GDPR disciplina in maniera stringente all'art. 9: il loro trattamento è espressamente vietato dal Legislatore, che nella seconda parte della norma elenca tassativamente i casi in cui tale divieto può non operare. È evidente, dunque, che il più grande ostacolo alla diffusione della IA in sanità sia proprio rappresentato dalla difficoltà di raccolta e trattamento dei dati dei pazienti.

Nel Decalogo pubblicato lo scorso 10 ottobre, l'Autorità garante si dimostra non solo, come era ovvio aspettarsi, conscia delle peculiarità dei dati personali trattati in tale ambito e della necessità di tutelare gli i pazienti interessati ma anche della difficoltà di accesso al mercato dell'IA da parte delle imprese pubbliche e private che concorrono all'offerta di un servizio (quello sanitario) che risponde ineludibilmente al soddisfacimento di un diritto costituzionalmente tutelato.

Al primo punto, dunque, il Garante chiarisce che la base giuridica più idonea al trattamento dei dati personali relativi alla salute per l'impiego di strumenti di IA da parte di soggetti istituzionalmente preposti al soddisfacimento di tali compiti è certamente il cd. '"interesse pubblico" (art. 9, par. 2, lett. g. GDPR). Tale base giuridica richiede l'esistenza all'interno dell'ordinamento di una disposizione di legge o di regolamento o di atti amministrativi generali che specifichino: i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Al secondo punto, il Garante esprime la necessità che in questo settore il trattamento dei dati sia conformato alle tecniche di privacy by design e by default ovvero sia compliant rispetto ai principi e a tutti gli adempimenti previsti dal GDPR. Dunque, fin dalla fase di progettazione e realizzazione dei sistemi di Intelligenza artificiale in ambito sanitario, devono essere adottate tutte le misure tecniche e organizzative adeguate ad attuare i principi di protezione dei dati e

devono essere integrate nel trattamento tutte le garanzie necessarie a tutelare i diritti e le libertà degli interessati.
Al terzo punto, l'Autorità sottolinea la necessità che in tali operazioni siano correttamente individuati i ruoli del "titolare del trattamento" e del "responsabile del trattamento", affinché possano essere circoscritti con precisione compiti e responsabilità in materia di protezione dei dati da attribuire ai soggetti coinvolti. L'assegnazione dei ruoli, indica il Garante, deve corrispondere alle attività che il soggetto svolge in concreto alla luce dei compiti istituzionalmente demandati allo stesso dal quadro giuridico che ordina il settore sanitario. Dunque, tenendo ferma la necessità che nel settore in esame la possibilità di effettuare il trattamento sia normativamente attribuita al titolare, ai fini della individuazione in concreto dei ruoli del trattamento che si intendono svolgere è indispensabile esaminare anche sul piano sostanziale le competenze attribuite ai diversi soggetti e, conseguentemente, le attività in concreto svolte dagli stessi.
Al quarto punto, il Garante riproduce quelli che, molto interessatamente, chiama "i tre principi cardine che devono governare l'utilizzo di algoritmi e di strumenti di IA nell'esecuzione di compiti di rilevante interesse pubblico".
Il primo è il principio di conoscibilità: l'interessato ha il diritto di conoscere l'esistenza di processi decisionali basati su trattamenti automatizzati e, in tal caso, il diritto di ricevere informazioni significative sulla logica utilizzata, sì da poterla comprendere.
Successivamente viene esplicato il cd. principio di non esclusività della decisione algoritmica, secondo cui deve comunque esistere nel processo decisionale un intervento umano capace di controllare, validare ovvero smentire la decisione automatica.
Il terzo principio è quello di non discriminazione algoritmica, secondo cui è opportuno che il titolare del trattamento utilizzi sistemi di IA affidabili che riducano le opacità, gli errori dovuti a cause tecnologiche e/o umane, verificandone periodicamente l'efficacia anche alla luce della rapida evoluzione delle tecnologie impiegate, delle procedure matematiche o statistiche appropriate per la profilazione, mettendo in atto misure tecniche e organizzative adeguate. Ciò, al fine di garantire che siano rettificati i fattori che comportano inesattezze dei dati e sia minimizzato il rischio di errori, visti i potenziali effetti discriminatori che un trattamento inesatto di dati sullo stato di salute può determinare nei confronti di persone fisiche.
Si tratta, in altre parole, del recepimento dei più noti principi in materia di regolazione dell'Intelligenza artificiale che, comparsi nei primi documenti di matrice eurounitaria, da circa un lustro innervano le discussioni dottrinali e giurisprudenziali sul punto. Tali principi, fatti propri dal Consiglio di Stato in più di una sentenza a partite dal 2019, oggi hanno fatto ingresso nel tessuto normativo italiano grazie all'art. 30 del nuovo Codice dei contratti pubblici, il d.lgs. 36 del 2023.
Al quinto punto, il Garante per la protezione di dati personali si pronuncia sulla necessità di effettuare o meno la cd. VIP, la valutazione di impatto sulla protezione dei dati che, in taluni casi, impegna il titolare del trattamento ai sensi dell'art. 35 del GDPR. L'Autorità chiarisce che la previsione di un sistema centralizzato a livello nazionale attraverso il quale realizzare servizi sanitari con strumenti di IA rientra senza dubbio tra i cd. trattamenti "ad alto rischio" per i quali una preventiva valutazione di impatto è necessaria. Essa, infatti, rappresenta uno strumento per l'individuazione delle misure più idonee a tutelare i diritti e le libertà fondamentali degli interessati nonché a garantire il rispetto dei principi generali del Regolamento e a consentire l'analisi della proporzionalità dei trattamenti effettuati.
L'autorità, quindi, individua taluni ambiti su cui l'attenzione del titolare deve concentrarsi: tra questi vi sono i rischi legati alla tenuta di una banca dati contenente informazioni sanitarie su larga scala (ovvero quelle di tutta o parte della popolazione assistita sul territorio nazionale). Qui possono essere celarsi, infatti, rischi legati alla qualità dei dati trattati, come ad esempio il mancato o erroneo allineamento o aggiornamento della banca dati; rischi legati all'eventuale

revoca del consenso degli interessati; rischi legati alla possibile reidentificazione degli interessati mediante l'incrocio di altre banche dati.
Proprio al concetto di "qualità dei dati" il Garante dedica il sesto punto del proprio Decalogo, precisando che la realizzazione di un sistema nazionale di IA destinato ad elaborare i dati sanitari di tutta la popolazione assistita, impone un rigoroso rispetto di specifiche misure volte a garantire in concreto l'esattezza e l'aggiornamento dei dati utilizzati. In questo ambito, infatti, i requisiti di esattezza, correttezza e aggiornamento del dato appaiono di particolare rilievo considerati i rischi e la finalità degli strumenti di IA impiegati ovvero la cura dei pazienti. Una banca dati non aggiornata, non bilanciata, inesatta o discriminatoria è senza dubbio idonea a influenza pesantemente l'efficacia e la correttezza del servizio offerto con rischi insopportabili per l'ordinamento.
Al sesto punto, il Garante si sofferma sui requisiti di "integrità" e "riservatezza" che devono caratterizzare i trattamenti eseguiti sui dati personali. Secondo l'Autorità nel settore in esame si deve pervenire a una puntuale descrizione dei trattamenti effettuati mediante la possibilità che soggetti terzi possano accedere e comprendere e valutare: le logiche algoritmiche utilizzate da suddetti sistemi di IA; le metriche utilizzate per l'addestramento dei modelli; la qualità del modello di analisi adottato; le verifiche svolte per rilevare la presenza di eventuali bias; le misure correttive eventualmente adottate.
Il principio della cd. comprensibilità algoritmica viene ripreso anche all'ottavo punto del Decalogo, ove il Garante si sofferma sui principi di "correttezza" e "trasparenza". L'uso di strumenti di IA in questo settore non può che passare per l'adozione di misure idonee a favorire la consapevolezza, nella collettività, che il sistema sanitario utilizza strumenti automatizzati così come non possono essere evitati momenti di partecipazione dei differenti stakeholder in relazione al ciclo di vita dei sistemi di IA. Solo così può essere favorito uno sviluppo di soluzioni automatizzate che sia veramente sostenibile, partecipato e rispettoso dei diritti e delle libertà fondamentali degli interessati. Per far questo, l'Autorità ritiene necessario che: la base giuridica del trattamento sia chiara, prevedibile e resa conoscibile agli interessati anche attraverso specifiche campagne di informazione; vengano consultati gli stakeholder e gli interessati nell'ambito dello svolgimento della valutazione d'impatto, e che questa venga almeno per estratto, pubblicata; vengano predisposte tutte le informazioni da rendere agli interessati, con gli elementi di cui agli artt. 13 e 14 del Regolamento in maniera chiara, concisa e comprensibile, e che gli stessi siano resi edotti circa la fase in cui il trattamento dei propri dati è effettuato (fase di apprendimento dell'algoritmo, sperimentazione e validazione; fase di applicazione dell'aritmo, etc…); vengano rappresentare le logiche e le caratteristiche di elaborazione dei dati; vengano chiariti gli eventuali obblighi e responsabilità dei professionisti sanitari che utilizzano servizi sanitari basati sull'IA.
Al nono punto il Garante cala nel concreto il principio dello cd. "human in the loop" e individua nella fase dell'addestramento dell'algoritmi il momento più idoneo in cui collocare la supervisione dell'uomo sulla macchina e sul suo operato. È qui che si ritiene necessario garantire un ruolo centrale del professionista sanitario al fine di non rimettere in toto alla macchina la decisione finale.
Il Decalogo, quindi, si conclude con un suggerimento affinché nel settore della salute si abbia "un atteggiamento eticamente corretto, sicuro e trasparente della tecnologia IA". Secondo il Garante, allo stato è opportuno preferire fornitori che sin da subito si siano preoccupati di svolgere una valutazione di impatto sulla protezione dei dati prima della commercializzazione dei propri, nonché che abbiano eventualmente anche condotto una specifica valutazione di impatto per l'IA, sicura, trasparente e affidabile. Quanto precisato, rientrerebbe negli specifici obblighi deontologici cui è tenuto il professionista sanitario che deve garantire al proprio paziente le migliori curi disponibili sul mercato.

Il Documento qui brevemente rappresentato sembra essere la risposta del Garante a più di un imput ricevuto. Da un lato, esistono certamente particolari contingenze economiche e politiche dettate dal momento storico: in attesa delle future norme europee e nazionali in materia (si pensi al cd. AI Act in corso di approvazione), l'ordinamento giuridico ha la necessità di disegnare un framework di riferimento per tutti quegli operatori economici privati interessati agli investimenti pubblici in tema di sanità digitale (si pensi, ad esempio, alla Piattaforma di intelligenza artificiale a supporto dell'assistenza primaria finanziata con i fondi del PNRR).
Dall'altro appare evidente l'intento dell'autority, non tanto celato, di proporsi come ente capofila dell'attività di regolazione del settore. Il Decalogo, infatti, oltre ad essere un'utilissima guida pratica per la protezione dei dati personali dei pazienti coinvolti in procedimenti automatizzati rappresenta, senza dubbio, un passo in avanti nella determinazione di un quadro giuridico organico in tema di regolazione dell'Intelligenza artificiale.