Intelligenza Artificiale (IA): rischi e vantaggi

Regolamento Europeo sull'IA e Decalogo del Garante della privacy in materia sanitaria

di Rita Rossodivita

L'Intelligenza Artificiale: evoluzione tecnologica e interazione uomo-macchina

Per Intelligenza Artificiale (IA) si intende un insieme di tecnologie che, grazie a grandi quantitativi di dati, algoritmi e potenza di calcolo, consentono alle macchine di operare in modo rapido ed efficiente per favorire e migliorare i processi decisionali, simulando l'intelligenza umana o superandone le potenzialità.
Negli anni Cinquanta del Novecento Alan Turing[1], nel suo articolo *Computing Machinery and intelligence*, già parlava di macchine in grado di imitare l'intelligenza umana. Nei decenni successivi i progressi compiuti nell'ambito dell'Intelligenza Artificiale, grazie a computer più potenti e in grado di archiviare ed elaborare grandi quantitativi di dati, hanno consentito prestazioni sempre più complesse: storica è la vittoria, nel 1997, di un computer IBM sul campione del mondo di scacchi Gary Kasparov.
L'evolversi della tecnologia ha permesso la creazione di macchine in grado di interagire con l'essere umano o di sostituirsi a esso, che hanno cambiato le società e gli stili di vita. Alcuni esempi sono i dispositivi digitali di uso quotidiano che si attivano con la voce; gli assistenti virtuali (*chatbot*), che possono conversare con l'essere umano e eseguirne le azioni, come Chat GPT (in grado di scrivere testi e risolvere operazioni matematiche); i mezzi di trasporto autoguidati.

Gli orientamenti dell'Europa in materia di Intelligenza Artificiale

Negli ultimi anni l'Unione Europea ha presentato, attraverso atti non vincolanti, una serie di misure volte a favorire lo sviluppo dell'IA in settori chiave, promuovendo centri di ricerca in tutta Europa, nella consapevolezza che «*Oltre a semplificarci la vita, i sistemi intelligenti ci aiutano a risolvere alcune delle più grandi sfide del mondo: curare le malattie croniche, combattere il cambiamento climatico e anticipare le minacce alla sicurezza informatica. L'Intelligenza Artificiale è una delle tecnologie più strategiche del 21° secolo*»[2].
L'IA, infatti, apporta notevoli benefici in molti settori: sanità, produzione industriale, sicurezza, servizi pubblici; tuttavia ne deve essere garantita un'applicazione affidabile, compatibile con la tutela dei diritti fondamentali dei cittadini alle libertà di espressione e di riunione, alla dignità umana, alla non discriminazione fondata sul sesso, sulla razza, sull'origine etnica, sulla religione o sulle convinzioni personali, sulla disabilità, sull'età o sull'orientamento sessuale, alla protezione dei dati personali e della vita privata, nonché alla tutela dei consumatori.
È importante, dunque, che nell'utilizzo dell'IA siano rispettati gli orientamenti etici della Carta dei diritti fondamentali dell'UE e soprattutto dell'**articolo 2 del Trattato sull'Unione**[3].

[1] Alan Turing, nato a Londra nel 1912, fu un brillante matematico e informatico, famoso per essere riuscito, durante la Seconda guerra mondiale, a decifrare i codici usati dai tedeschi nelle comunicazioni. Nei suoi studi egli ipotizzava che una macchina potesse considerarsi intelligente se l'essere umano con cui interagisce non riesce a distinguere se le risposte sono di un essere umano vero. Egli ipotizza una macchina "Macchina di Turing" che, opportunamente programmata, è in grado di eseguire ogni tipo di calcolo.
[2] Dalla Comunicazione della Commissione al Parlamento europeo, al Consiglio europeo, al Comitato economico e sociale europeo e al Comitato delle regioni «Intelligenza artificiale per l'Europa», Bruxelles, 2018.
[3] «L'Unione si fonda sui valori del rispetto della dignità umana, della libertà, della democrazia, dell'uguaglianza, dello Stato di diritto e dei diritti umani, soprattutto i diritti delle persone appartenenti a minoranze. Questi valori sono comuni agli Stati membri in una società caratterizzata dal pluralismo, dalla non discriminazione, dalla tolleranza, dalla giustizia, dalla solidarietà e dalla parità tra donne e uomini.»

Il Libro Bianco sull'Intelligenza Artificiale

Nel 2020 la Commissione Europea ha pubblicato il Libro Bianco sull'Intelligenza Artificiale, con il quale auspicava l'adozione di un quadro normativo sull'IA, al fine di promuovere la ricerca e gli investimenti in Europa, ma anche combattere i rischi di violazione dei diritti fondamentali legati al suo impiego. Ad esempio, l'utilizzo della tecnologia del riconoscimento facciale[4] può pregiudicare il diritto al rispetto della vita privata, alla protezione dei dati personali, alla non discriminazione; o ancora, alcuni algoritmi utilizzati per prevedere la recidiva criminale possono evidenziare pregiudizi di genere e razziali; i medesimi rischi riguardano l'utilizzo dell'IA per la sorveglianza di massa da parte di autorità statali o enti.
Il 19 febbraio 2020, unitamente alla pubblicazione del Libro Bianco sull'Intelligenza Artificiale, è stata avviata una consultazione pubblica online, rivolta a tutti i portatori di interessi coinvolti nel settore pubblico e in quello privato, con l'obiettivo di raccogliere opinioni e pareri su quanto previsto dal Libro Bianco.
La Commissione si è avvalsa anche dell'opera di un Gruppo di esperti di alto livello sull'IA (*AI HLEG*: *High-Level Expert Group on Artificial Intelligence*), che ha elaborato un *Elenco di valutazione per l'intelligenza artificiale affidabile*. L'IA viene considerata tale quando si basa su:

- **legalità**, in quanto ottempera a leggi e regolamenti già vigenti;
- **eticità**, in quanto applicata nel rispetto dei valori etici (autonomia umana, prevenzione dei danni, equità), e con attenzione alle situazioni che coinvolgono gruppi vulnerabili o che sono caratterizzate da asimmetrie (come quelle tra datore di lavoro e lavoratori, tra imprese e consumatori), nella salvaguardia da effetti negativi sulla democrazia e sulla libertà umana;
- **robustezza**, se garantisce, nella sua applicazione, affidabilità dal punto di vista tecnico e sociale, nel rispetto della sicurezza, trasparenza, diversità, e del benessere sociale e ambientale.

Regolamento europeo sull'Intelligenza Artificiale (*Artificial Intelligence Act*)

A dicembre 2023 il Consiglio e il Parlamento europeo hanno raggiunto un accordo sulla proposta di Regolamento europeo presentata dalla Commissione europea nel 2021, che stabilisce regole armonizzate sull'Intelligenza Artificiale. Sono previsti ulteriori lavori per definire i dettagli del nuovo Regolamento e la successiva approvazione da parte di entrambe le istituzioni.
Il Regolamento presuppone che l'IA sia una **tecnologia antropocentrica**, posta al servizio del bene comune, che non deve sostituire l'autonomia umana o limitarne la libertà individuale.
La legge prevede una regolamentazione dell'Intelligenza Artificiale in base al **livello di rischio**: maggiore è il rischio per i diritti fondamentali o la sicurezza delle persone, maggiori sono gli obblighi del sistema, al fine di garantire l'utilizzo di sistemi di IA affidabili, sicuri, trasparenti, etici, imparziali e sotto il controllo umano[5].
Si considerano sistemi di IA ad alto rischio quelli operativi nei seguenti ambiti.

1. **Identificazione biometrica e categorizzazione delle persone fisiche**.
2. **Gestione e funzionamento di infrastrutture critiche**: funzionamento del traffico stradale, fornitura di acqua, gas, riscaldamento, elettricità.
3. **Istruzione e formazione professionale**: accesso agli istituti di istruzione e formazione professionale, valutazione degli studenti e dei partecipanti ai test di ammissione.
4. **Occupazione e accesso al lavoro**: reclutamento e selezione di persone fisiche, promozione e cessazione dei rapporti contrattuali, valutazione di prestazioni e comportamenti in tali rapporti.
5. **Accesso ai servizi privati essenziali e pubblici**: valutazione dell'idoneità a benefici e servizi assistenziali e sanitari pubblici o revoca e riduzione degli stessi, valutazione di affidabilità creditizia.

[4] Questo tipo di identificazione consente il confronto tra l'immagine facciale di una persona e altri modelli memorizzati in una banca dati: vengono confrontati due modelli biometrici appartenenti allo stesso individuo, per determinare se la persona mostrata nelle immagini è la stessa. È una procedura utilizzata per i controlli automatizzati delle frontiere, come ad esempio negli aeroporti.
[5] Il Regolamento definisce l'Intelligenza Artificiale come un «*sistema automatizzato progettato per operare con livelli di autonomia variabili e che, per obiettivi espliciti o impliciti, può generare output quali previsioni, raccomandazioni o decisioni che influenzano gli ambienti fisici o virtuali*».

6. **Forze dell'ordine**: valutazione del rischio di commettere reati da parte di persone fisiche, rilevazione di stati emotivi, valutazione dell'affidabilità delle prove delle indagini, previsione del verificarsi o ripetersi di reati sulla base di profilazione o di valutazione dei tratti della personalità di persone fisiche.

In breve le **disposizioni** previste dal Regolamento europeo sull'IA[6].

- In quanto contrarie ai valori e ai diritti fondamentali dell'Unione, è opportuno che siano **vietate le pratiche** di IA con un elevato **potenziale di manipolazione** delle persone attraverso tecniche subliminali; le azioni a danno di particolari categorie – quali minori e disabili – al fine di **distorcerne i comportamenti**, con conseguente danno psicologico o fisico; le pratiche in violazione della normativa sulla **protezione dei dati** o di tutela dei consumatori; l'attribuzione di **punteggi sociali** basati sull'IA da parte di autorità pubbliche, che valutano o classificano l'affidabilità delle persone in base al loro comportamento sociale o a caratteristiche personali; le pratiche di **identificazione biometrica** remota in tempo reale o post[7] in spazi accessibili al pubblico (salvo situazioni di necessità per cui vi sia una autorizzazione eccezionale), che comportano il rischio di intrusione nella vita privata e ripercussioni sulla libertà all'anonimato e alla non sorveglianza, ponendo chi impiega i sistemi di controllo in una posizione di potere.
- I sistemi di IA ritenuti ad alto rischio devono essere sottoposti a **valutazione *ex ante*** sulla loro conformità prima di essere operativi all'interno del mercato europeo, soprattutto se utilizzati come componenti di sicurezza per particolari prodotti come macchine, giocattoli, dispositivi medici.
- L'**obbligo di trasparenza** richiede che debbano essere informate le persone ogni qualvolta si applicano dei sistemi di IA che generano o manipolano immagini, contenuti audio o video che assomigliano notevolmente a quelli autentici.
- Sono istituiti: un **Ufficio per l'IA** all'interno della Commissione incaricato della supervisione e del rispetto delle norme; un **gruppo scientifico di esperti indipendenti** con funzioni di consulenza; un **Comitato per l'IA** composto da rappresentanti degli Stati membri. Viene creata una **banca dati** a livello europeo **dei sistemi di IA ad alto rischio** e stabilita la designazione da parte degli Stati membri di un'autorità nazionale di controllo, oltre a un sistema di sanzioni.
- Per i sistemi di IA non ad alto rischio sono previsti **codici di condotta**, creati e attuati anche autonomamente dai fornitori.

La realizzazione di servizi sanitari nazionali attraverso sistemi di IA: il Decalogo del Garante per la protezione dei dati personali

L'IA è già ampiamente utilizzata nella sanità: ad esempio nella diagnosi assistita, dove consente ai medici un'analisi dei dati clinici e dei test laboratoriali più tempestiva e accurata; nella robotica chirurgica, dove aumenta la precisione negli interventi chirurgici più complessi; per l'identificazione di pazienti a rischio di sviluppare determinate patologie, ecc.
Il suo impiego nella sanità è in continua crescita ma, come già indicato dall'UE, comporta **rischi etici** e di rispetto dei diritti fondamentali legati alla privacy dei dati, all'uguaglianza nell'accesso alle cure mediche, al rapporto medico-paziente.
Un sistema di IA applicato ai servizi sanitari nazionali è considerato ad alto rischio, come previsto nella proposta di Regolamento UE sull'IA. Il Garante per la protezione dei dati personali, nel settembre 2023, ha emanato il *Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di Intelligenza Artificiale*, ribadendo la necessità che un sistema nazionale che utilizzi l'IA operi nel rispetto di **tre principi**

[6] Sulla proposta di Regolamento vi è anche il parere congiunto n. 5/2021 del Comitato europeo per la protezione dei dati (EDPB) e il Garante europeo della protezione dei dati (GEPD), che valutano positivamente i timori espressi dal legislatore europeo nell'affrontare la questione dell'utilizzo dell'Intelligenza Artificiale all'interno dell'UE e sottolineano che la proposta ha implicazioni estremamente rilevanti per la protezione dei dati.
[7] Il sistema di identificazione biometrica remota in tempo reale è un sistema che prevede l'uso di materiale dal vivo o quasi dal vivo (come riprese video, generate da una fotocamera o da altro dispositivo con funzionalità simili), in cui il rilevamento dei dati biometrici, il confronto e l'identificazione avvengono istantaneamente, o quasi; nel sistema di identificazione biometrica post, invece, i dati biometrici sono già stati rilevati e il confronto e l'identificazione avvengono solo con un notevole ritardo.

fondamentali: **trasparenza**, **supervisione** da parte dell'uomo, **non discriminazione**. Il paziente ha il diritto di conoscere e avere informazioni su interventi automatizzati che utilizzino l'IA; le elaborazioni effettuate attraverso l'IA devono prevedere una valutazione di impatto e una supervisione umana che ne verifichi l'efficacia, per evitare errori dovuti a trattamento di dati inesatti o incompleti che possano creare discriminazioni nell'accesso alle cure.

Esaminiamo sinteticamente il *Decalogo*, che recepisce quanto previsto dal Regolamento UE sulla protezione dei dati (2016/679).

1. **Le basi giuridiche del trattamento**: il Garante ritiene, come proposto dal Regolamento europeo sull'IA, in fase di approvazione, che l'uso dei sistemi di IA ritenuti ad alto rischio poiché incidono sulla salute, sul diritto alle cure e sulla fruizione dei servizi sanitari e di assistenza medica e la relativa elaborazione dei dati, anche se per fini di interesse pubblico, devono avere una valida base giuridica nel diritto europeo e degli Stati membri, previa valutazione di impatto e consultazione dell'Autorità di controllo.
2. **I principi di *accountability* e di privacy *by design* e *by default***: nella realizzazione di sistemi di IA in ambito sanitario devono essere adottate misure tecniche e organizzative fin dalla progettazione e per impostazione predefinita (*by design* e *by default*), a garanzia dei diritti e delle libertà degli interessati, e nel rispetto dello Stato di diritto e del governo democratico.
3. **I ruoli**: con riferimento al trattamento dei dati sanitari, occorre individuare in modo chiaro e trasparente i ruoli di titolare e responsabile, autorizzati e opportunamente istruiti al trattamento; l'attribuzione deve corrispondere ad attività dagli stessi svolte in concreto.
4. **I principi di conoscibilità, non esclusività e non discriminazione algoritmica**: tre principi che devono garantire il diritto di ogni soggetto di conoscere se un processo decisionale è frutto di un trattamento automatizzato; la supervisione da parte del personale sanitario; la verifica e rettifica dei fattori che comportano inesattezze dei dati al fine di evitare decisioni discriminanti.
5. **La valutazione d'impatto sulla protezione dei dati (VIP)**: la realizzazione di un sistema centralizzato di servizi sanitari con strumenti di IA, quindi su larga scala, deve prevedere una valutazione di impatto, al fine di valutare la proporzionalità e l'adeguatezza dei trattamenti effettuati, poiché presenta un rischio elevato per i diritti di soggetti vulnerabili.
6. **La qualità dei dati**: il titolare del trattamento deve garantire che i dati siano esatti; dati non aggiornati e inesatti inciderebbero su efficacia e correttezza dei servizi. Uno sviluppo non governato di sistemi di IA destinati a elaborare dati sanitari presenta potenziali rischi, come aspettative illusorie e fuorvianti e mancanza di validazione scientifica.
7. **I principi di integrità e riservatezza**: nella descrizione dei trattamenti dei dati sanitari su larga scala attraverso i sistemi di IA devono essere puntualmente indicate le logiche algoritmiche utilizzate nel generare i dati e i servizi, e le misure adeguate a mitigare i rischi correlati all'adozione di decisioni automatizzate.
8. **I principi di correttezza e trasparenza**: è necessario assicurare ampia informazione alla totalità degli assistiti dal sistema sanitario nazionale sull'impiego dei sistemi di IA e il loro funzionamento (ad esempio, vantaggi diagnostici e terapeutici, obblighi e responsabilità dei professionisti sanitari).
9. **La supervisione umana**: è necessario che in fase di addestramento degli algoritmi sia mantenuto il ruolo centrale dell'uomo e, nel caso di specie, del professionista sanitario e che non si rimetta in toto la decisione alle macchine, poiché le predizioni dell'IA possono essere sbagliate per imprecisione dei dati.
10. **Ulteriori profili rispetto alla disciplina sulla protezione dei dati personali connessi alla dignità e all'identità personale**: vi deve essere costante attenzione ai profili etici nell'elaborazione di strumenti di IA che trattano informazioni sulla salute. Rimangono fermi gli obblighi deontologici cui è tenuto il professionista sanitario nella scelta del percorso terapeutico appropriato; l'opportunità di scegliere fornitori che svolgano una valutazione d'impatto sicura e affidabile prima della commercializzazione dei propri prodotti. L'IA deve migliorare le prestazioni del SSN, senza ripercussioni in termini sociali.