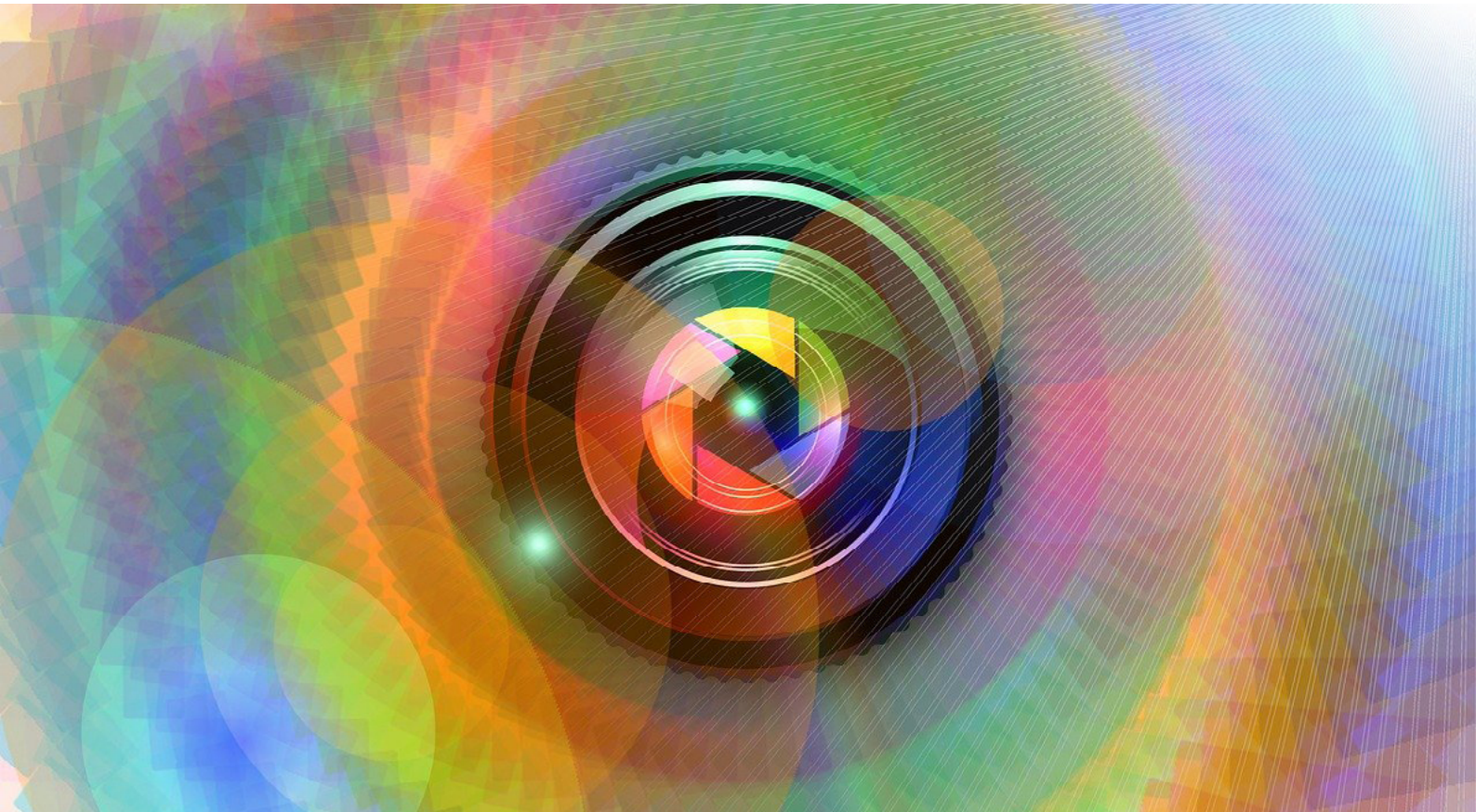
STEFANELLI & STEFANELLI STUDIO LEGALE

AI LEGAL,
un prisma da comporre



INTRODUZIONE

L'Intelligenza Artificiale è tema di grande attualità e fonte di dibattito in vari ambiti.

L'Unione europea ha deciso di darsi una normativa specifica con l'approvazione del nuovo regolamento (**AI ACT**).

L'AI ACT è una **disciplina di prodotto** che interviene sotto vari profili, non solo identificando i sistemi di AI vietati ma anche, e soprattutto, disciplinanndo i requisiti che i sistemi di AI devono rispettare per essere immessi in commercio nell'Unione.

Svariati e complessi sono poi i **profili di interconnessione** con le altre discipline quali GDPR, tutela della proprietà intellettuale e industriale e MDR, richiedendo quindi una lettura attenta e coordinata.

Il nostro studio ha dato vita ad una rubrica digitale che contiene articoli che approfondiscono l'argomento nelle sue **diverse sfaccettature**.

A due anni dall'avvio della rubrica abbiamo deciso di raccogliere i vari contributi in questo white paper, li troverete organizzati secondo le diverse prospettive:

AI E DATI

AI E REGOLAMENTAZIONE DA PRODOTTO

AI E SANITÀ

AI E PROFILI DI RESPONSABILITÀ

AI E IP LAW

AI E DIRITTO DEL LAVORO

AI E CONTRATTUALISTICA

AI - PUBBLICITÀ

AI - APPALTI

SOMMARIO

AI: LA DEFINIZIONE GIURIDICA 6

AI E DATI 10

Dati di qualità per lo sviluppo dell'intelligenza artificiale 10

Software medicali basati sulla IA: cosa è possibile fare con i dati dei pazienti 18

Il rapporto tra GDPR e i sistemi di IA 22

Pubblicato il decalogo sull'Intelligenza Artificiale in Sanità 26

Analisi del decalogo del Garante Privacy sull'Intelligenza Artificiale in sanità 29

Intelligenza artificiale e protezione dei dati: una convivenza possibile? 35

AI E REGOLAMENTAZIONE DA PRODOTTO 39

ISO 42001 per aziende biomedicali e AI ACT 39

Progettazione secondo MDR - norme tecniche requisito essenziale di sicurezza 43

Sistemi di IA ad alto rischio e dispositivi medici: la governance dei dati 46

I soggetti coinvolti dall'AI ACT: uno sguardo d'insieme 51

SOMMARIO

AI E SANITÀ 58

I soggetti coinvolti dall'AI ACT: il professionista sanitario è un "deployer?" 58

DDL Intelligenza Artificiale e sanità 62

AI E PROFILI DI RESPONSABILITÀ 66

Come cambia il risk management delle strutture sanitarie dopo l'avvento de ll'IA? 66

Il sistema sanzionatorio dell'AI Act 72

AI Act e responsabilità penale: cosa cambia per provider e deployer 76

AI E IP LAW 84

Riservatezza delle conversazioni con l'IA – qual è la sorte dei dati utilizzati come prompt? 84

Chi è l'autore? L'intelligenza umana o quella artificiale? 90

Tutela della proprietà intellettuale e sviluppo dei sistemi di AI: due posizioni inconciliabili? 93

L'Italia verso una propria strategia sull'intelligenza artificiale 97

Lo sviluppo dei sistemi di intelligenza artificiale non può prescindere dalla tutela dei dataset 100

SOMMARIO

AI E DIRITTO DEL LAVORO 104

Profilazione, controllo e decisioni automatizzate: i rischi AI in tema di lavoro 104

DDL Intelligenza Artificiale: le novità in materia di diritto del lavoro 111

AI E CONTRATTUALISTICA 116

I contratti per lo sviluppo e la commercializzazione dell'AI 116

AI E PUBBLICITÀ 123

Se utilizzo un sistema di IA per i miei contenuti devo dichiararlo? L'obbligo di trasparenza per i deployer 123

AI E APPALTI 127

Automatizzazione delle Procedure di Gara e Riserva di Umanità 127

AI: LA DEFINIZIONE GIURIDICA

Articolo di Avv. Silvia Stefanelli

11 Aprile 2024

Apriamo questo progetto dello Studio Stefanelli&Stefanelli sulla Intelligenza Artificiale con un primo articolo sulla definizione di Intelligenza Artificiale.

L'art. 3 lett. 1 (versione in italiano scaricata del sito del Parlamento UE) stabilisce che per Ai si intende

"sistema di IA": 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;"

Ma cosa significa esattamente?

Un approfondimento sul significato di questa definizione può essere tratto dal EXPLANATORY MEMORANDUM ON THE UPDATED OECD DEFINITION OF AN AI SYSTEM pubblicato dallOEDC.AI proprio a marzo 2024.

Dalla lettura di tale documento si possono trarre chiarimenti sugli elementi cardine della definizione sopra riportata.

Più esattamente vediamo i concetti fondamentali della definizione

SISTEMA AUTOMATIZZATO

La locuzione "sistema automatizzato" è volutamente ampia per poter ricomprendere varie tecniche tra cui l'apprendimento automatico e gli approcci basati sulla conoscenza, e altresì diverse aree di applicazione come la computer vision, l'elaborazione del linguaggio naturale, il riconoscimento vocale, i sistemi intelligenti di supporto alle decisioni, i sistemi robotici intelligenti, nonché l'applicazione innovativa di questi

strumenti a vari domini.

LIVELLI DI AUTONOMIA VARIABILE

Il sistema di AI disegnato al Regolamento è di natura antropocentrica: ci vuol dire che l'uomo è sempre in grado di sorvegliare ed intervenire sulla macchina. Ciò non fa venire meno la peculiarità della Ai: la presenza di una sua propria autonomia, che può presentare livelli diversi.

In altre parole il sistema è in grado di apprendere o agire senza coinvolgimento umano a seguito della delega di autonomia e automazione dei processi da parte dell'uomo stesso. La supervisione umana può avvenire in qualsiasi fase del ciclo di vita del sistema IA, ad esempio durante la progettazione, la raccolta ed elaborazione dei dati, lo sviluppo, la verifica, la convalida, la distribuzione o il funzionamento e il monitoraggio.

Alcuni sistemi IA possono poi generare output senza che questi output siano esplicitamente descritti nell'obiettivo del sistema IA e senza istruzioni specifiche da parte di un essere umano. Per i sistemi AI considerati "ad alto rischio", come ad esempio i dispositivi medici in classi IIa e superiori, l'articolo 14 del AI Act prevede misure dettagliate per garantire la supervisione umana sulla macchina. Per poter essere efficace, la supervisione umana si basa su alcuni pilastri fondamentali. Tra questi citiamo: la comprensione da parte dell'uomo delle capacità e delle limitazioni del modello; la consapevolezza da parte dell'uomo di un possibile bias tecnologico, cioè la tendenza a "fidarsi" della macchina; la autonomia da parte dell'uomo nel poter sia ignorare gli output della macchina sia interrompere in modo sicuro e in ogni momento il funzionamento della macchina.

ADATTABILITÀ DOPO LA DIFFUSIONE

L'adattabilità dopo la diffusione significa che i sistemi di AI basati sull'apprendimento automatico possono continuare ad evolversi attraverso l'interazione diretta (con input e dati) che può avvenire non solo prima della distribuzione ma anche dopo: solo a titolo di esempio un sistema di riconoscimento vocale può modificarsi adattandosi alla voce di un individuo.

L'addestramento del sistema può poi essere iniziale o periodico o continuativo, inferendo i modelli e le relazioni nei dati. Attraverso tale formazione, alcuni sistemi di IA possono sviluppare la capacità di eseguire nuove forme di inferenza non inizialmente previste dai loro programmatori.

Il Regolamento AIAct prevede, per garantire la sicurezza di questa formazione continua, che i provider si dotino di un sistema gestionale per la identificazione e la mitigazione dei rischi in tutta la vita del modello, anche dopo la prima messa a disposizione.

OBIETTIVI IMPLICITI O ESPLICITI

Gli obiettivi dei sistemi di IA possono essere espliciti o impliciti (obiettivi che possono sovrapporsi in alcuni sistemi:

- **Obiettivi espliciti e definiti dall'uomo**

sono i sistemi in cui lo sviluppatore codifica l'obiettivo direttamente nel sistema Esempi di sistemi con obiettivi espliciti sono i classificatori semplici, i sistemi di gioco, i sistemi di apprendimento per rinforzo, i sistemi di risoluzione di problemi combinatori, gli algoritmi di pianificazione e gli algoritmi di programmazione dinamica.

- **Obiettivo impliciti derivanti dalle regole tipicamente specificate dall'uomo**

le regole dettano l'azione che il sistema di intelligenza artificiale deve intraprendere in base alla situazione nella quale ci si trova: ad esempio, un sistema di guida potrebbe avere una regola: "Se il semaforo è rosso, fermati".

- **Obiettivi impliciti derivante dai dati di addestramento**

in questo caso l'obiettivo finale non è programmato esplicitamente, ma è "incorporato" attraverso i dati di addestramento e attraverso un'architettura di sistema che impara a emulare quei dati (ad esempio, premiando i modelli linguistici di grandi dimensioni per aver generato una risposta plausibile);

- **Obiettivi non completamente conosciuti in anticipo**

alcuni esempi includono i sistemi di raccomandazione che usano apprendimento per

rinforzo per restringere gradualmente il modello delle preferenze dei singoli utenti

OUTPUT

Gli output generati da un sistema di IA riflettono generalmente le diverse funzioni svolte dai sistemi di IA e comprendono generalmente le ampie categorie di raccomandazioni, previsioni e decisioni.

Queste categorie corrispondono a diversi livelli di coinvolgimento umano.

Più esattamente

- le “decisioni” rappresentano il tipo di output più autonomo (il sistema di IA agisce direttamente sull’ambiente o indirizza un’altra entità a farlo)
- le “previsioni” il meno autonomo.

I sistemi di intelligenza artificiale generativa producono invece “contenuti”, tra cui testo, immagini, audio e video.

Sebbene si possa, ad esempio, considerare la generazione di testo come una sequenza di “decisioni” di produrre parole particolari, i sistemi generativi sono diventati – dopo il lancio di OpenAI - una classe così importante di sistemi di IA da essere inclusi come categoria di output a sé stante nella definizione giuridica del Regolamento.

AI E DATI

Dati di qualità per lo sviluppo dell'intelligenza artificiale

Articolo di Avv. Eleonora Lenzi

25 Giugno 2024

I sistemi di Intelligenza Artificiale sono sviluppati sulla base di set di dati di addestramento, convalida e prova.

L'AI Act prevede che i set di dati debbano soddisfare i requisiti indicati ai paragrafi da 2 a 5 dell'art. 10 e, in particolare, richiede che siano soggetti a pratiche di governance e gestione dei dati adeguate alla finalità prevista dal sistema di IA. Tali pratiche riguardano in primo luogo i processi di raccolta dei dati e l'origine dei dati, nonché la finalità originaria della raccolta nel caso di dati personali (Art. 10, comma 2 lettera b).

L'AI Act prevede anche che i **fornitori di modelli di AI ad alto rischio e con finalità generali debbano dare informazioni dettagliate sui dati utilizzati per l'addestramento, la prova e la convalida**, compresi il **tipo** e la **provenienza dei dati** e le **metodologie di organizzazione**, il **numero di punti di dati**, la loro **portata** e le **principali caratteristiche**; il **modo in cui i dati sono stati ottenuti e selezionati** e tutte le altre misure per rilevare l'inadeguatezza delle fonti di dati e i metodi per rilevare distorsioni identificabili (Allegato IV punto 2d – Allegati IXa e IXb).

Da una ricerca condotta lo scorso anno del Center for Research on Foundation Models dell'Università di Stanford emerge che raramente i fornitori rendono noto in modo adeguato le fonti dei dati utilizzati, che spesso vengono reperiti su internet per lo più in violazione della normativa sul diritto d'autore.

È evidente che una tale modalità operativa non sia affatto adeguata ai requisiti richiesti

dall'AI Act, che a breve sarà legge e il cui rispetto sarà obbligatorio per tutti quei soggetti che intendano operare all'interno dell'Unione.

Eppure, **le fonti di dati utilizzabili sono numerose.**

L'Unione europea ha messo in campo da anni una propria strategia di digitalizzazione EU Digital Strategy - EU4Digital e **sono numerosi gli interventi normativi che riguardano i dati (personali e non).**

IL DATA GOVERNANCE ACT

Il Regolamento (UE) 2022/868 o più semplicemente DGA (Data Governance Act) mira a stabilire una cornice normativa per la gestione, lo scambio e l'utilizzo dei dati all'interno dell'UE.

Il DGA si applica a partire dal 24 settembre 2023 e fissa importanti linee guida per il riutilizzo all'interno dell'Unione di determinate categorie di dati detenuti da enti pubblici, nonché un quadro per la raccolta e fornitura di servizi di intermediazione di dati.

Il Regolamento si applica ai sensi dell'art. 3 ai dati **detenuti da enti pubblici** per ragioni di:

- riservatezza commerciale, inclusi segreti commerciali, professionali o aziendali;
- riservatezza statistica;
- protezione dei diritti di proprietà intellettuale di terzi; o
- protezione dei dati personali, nella misura in cui tali dati non rientrano nell'ambito di applicazione della direttiva (UE) 2019/1024 sugli Open Data.

Gli enti pubblici hanno la facoltà e non l'obbligo di permettere l'accesso ai dati protetti per il loro **riutilizzo**. In sede di riutilizzo, gli enti pubblici garantiscono ai sensi dell'art. 5 il rispetto dei seguenti requisiti:

- concedere l'accesso per il riutilizzo dei dati soltanto qualora l'ente pubblico abbia

garantito che i dati sono stati anonimizzati, nel caso di dati personali; e modificati, aggregati o trattati nel caso di informazioni commerciali riservate;

- accedere ai dati e riutilizzare gli stessi da remoto all'interno di un ambiente di trattamento sicuro, fornito o controllato dall'ente pubblico;
- accedere ai dati e riutilizzare gli stessi all'interno dei locali fisici in cui si trova l'ambiente di trattamento sicuro.

Il Regolamento intende pertanto favorire l'**atteggiamento altruista** dei titolari dei dati non personali e degli interessati, incoraggiando la condivisione dei dati per beneficio comune.

DATI PERSONALI E DATI NON PERSONALI

La politica europea dei dati ha, poi, i suoi cardini in due importanti regolamenti:

- regolamento (UE) 2016/679 relativo ai dati personali
- regolamento (UE) 2018/1807 relativo ai dati non personali

Il Regolamento (UE) 2016/679, noto anche come GDPR, dà una definizione intenzionalmente ampia di "dato personale", specificando che si tratta di «*qualsiasi informazione riguardante una persona fisica identificata o identificabile*».
Il GDPR, come noto, oltre alla tutela dei dati delle persone fisiche disciplina anche le modalità con cui tali dati possono circolare e possono essere legittimamente utilizzati.

Il Regolamento (UE) 2018/1807 disciplina la libera circolazione dei dati non personali nel territorio dell'Unione europea. Si tratta in particolare di dati che possono essere qualificati in base alla loro origine:

- dati anonimi ex-ante, ossia dati che in origine non si riferiscono ad una persona fisica identificata o identificabile;
- dati anonimi ex-post, ovvero dati che inizialmente erano personali e che successivamente sono stati resi non personali attraverso un processo di anonimizzazione.

L'obiettivo principale del Regolamento è quello di garantire che i dati non personali possano essere trattati liberamente su tutto il territorio dell'UE, che possano circolare liberamente e che ne venga garantita la portabilità in un formato strutturato, di uso comune e leggibile elettronicamente, anche in formati standard aperti ove necessario o richiesto dal fornitore di servizi che riceve i dati.

Spesso accade che dati personali e non personali siano raccolti in un **insieme di dati misti (es. i dati sanitari)**.
Ove sia possibile una separazione potranno essere applicate le normative di riferimento per ciascun insieme di dati (personali e non personali), laddove invece, l'insieme di dati misti contenga dati che tra loro risultino "indissolubilmente legati", l'art. 2, par. 2 del regolamento (UE) 2018/1807 prevede che si applichi il GDPR all'intero set di dati misti, anche nei casi in cui i dati personali ne rappresentino solo una minima parte.

La libera circolazione dei dati

Certamente, il dato comune tra i due regolamenti è la costante promozione del principio di libera circolazione dei dati all'interno del territorio dell'Unione europea, il quale però vede l'apposizione di limiti differenti:

- il regolamento sui dati non personali si basa sul principio del libero flusso transfrontaliero di dati personali e quindi sul divieto per gli Stati di imporre "obblighi di localizzazione" dei dati «*(...) a meno che non siano giustificati da motivi di sicurezza pubblica nel rispetto del principio di proporzionalità*». Inoltre, le norme del regolamento non si applicheranno qualora le attività di trattamento dei dati siano condotte al di fuori del territorio dell'UE.

- il regolamento sui dati personali dispone invece che la libera circolazione dei dati all'interno del territorio dell'Unione non possa essere limitata né vietata «*per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali*», e che le norme relative al trasferimento dei dati si applicheranno anche nelle interazioni verso paesi terzi ma impone importanti restrizioni al trasferimento dei dati personali verso Stati fuori dal territorio dell'UE o che non garantiscano un livello adeguato di protezione dei dati.

La portabilità dei dati

Entrambi i regolamenti disciplinano la portabilità dei dati mirando a facilitarne il loro trasferimento, e ciò al fine di evitare pratiche di "vendor lock-in", che si verificano quando gli utenti non possono cambiare il fornitore di servizi perché i dati risultano bloccati nel sistema del fornitore.

Il diritto alla portabilità dei dati assume connotazioni differenti a seconda che si tratti di:

- dati personali, nei quali la portabilità si riferisce al rapporto tra l'interessato e il titolare del trattamento, quindi in un rapport "business-to-consumer";
- dati non personali, nei quali invece la portabilità dei dati riguarda le interazioni "business-to-business" intercorrenti tra un utente professionale e un fornitore di servizi.

OPEN DATA

Il Considerando 9 della Direttiva (UE) 2019/1024 stabilisce che l'informazione del settore pubblico rappresenta una fonte straordinaria di dati che può contribuire al miglioramento del mercato interno e allo sviluppo di nuove applicazioni per i consumatori e le imprese.

Nello specifico, la direttiva fissa norme minime per favorire il riutilizzo dei documenti in possesso degli enti e delle imprese pubbliche, nonché dei dati della ricerca. Secondo il principio base introdotto dalla direttiva Open Data, i contenuti del settore pubblico accessibili in base alle norme nazionali sull'accesso ai documenti sono in linea di principio **liberamente disponibili per il riutilizzo, a fini commerciali o non commerciali**.

Gli enti pubblici che rendono disponibili i dati devono rispettare i principi di trasparenza, non discriminazione e non esclusività nella fornitura dei dati, garantendo altresì l'utilizzo di formati e modalità di diffusione adeguati.

La Direttiva (UE) 2019/1024 è stata recepita in Italia con il D.lgs. 8 novembre 2021, n. 200, che è entrato in vigore il 15 dicembre 2021.

Con questo decreto, le pubbliche amministrazioni e gli organismi di diritto pubblico si impegnano a garantire che i documenti siano riutilizzabili sia a fini commerciali che non commerciali. Le richieste di accesso ai documenti devono essere esaminate entro 30 giorni e, qualora venga negato l'accesso, deve essere fornita adeguata motivazione.

In particolare, il D.lgs. n. 200/2021 stabilisce le basi per la promozione dell'apertura dei dati pubblici in Italia, incoraggiando il riutilizzo dei dati e favorendo la trasparenza e l'efficienza delle pubbliche amministrazioni.

Nei primi mesi del 2023, è stato inoltre pubblicato il Regolamento di esecuzione (UE) 2023/138 che identifica un elenco specifico di dati ad elevato valore e le relative modalità di pubblicazione e riutilizzo.

Per questi specifici set di dati è prevista l'accessibilità alle condizioni della licenza Creative Commons BY 4.0 o di una licenza aperta equivalente o meno restrittiva.
Queste licenze consentono agli utenti di copiare, distribuire ed esporre pubblicamente i dati, nonché modificarli anche a fini commerciali, con l'obbligo di attribuire la paternità dei dati, fornire un collegamento alla licenza e indicare le eventuali modifiche apportate.

DATA ACT

Il 27 novembre 2023 il Consiglio dell'Unione europea ha approvato il Data Act "*norme di armonizzazione sull'accesso equo ai dati e sul loro utilizzo*", con lo scopo di regolare il riutilizzo dei dati rimuovendo gli ostacoli allo sviluppo dell'economia dei dati europea.

Alcuni punti chiave del Data Act includono:

- accesso e utilizzo dei dati, facilitando l'accesso ai dati e il relativo utilizzo da parte dei consumatori e delle imprese;
- interoperabilità dei dati e dei meccanismi e servizi di condivisione dei dati;
- adottare garanzie contro trasferimenti illeciti di dati;
- obblighi per i data holder quali: fornire informazioni complete sui dati generati, permettere agli utenti di accedere ai dati generati e condividere i dati generati con

altri soggetti indicati dagli utenti.

Particolare approfondimento è poi dedicato alla disciplina dei segreti commerciali o c.d. trade secrets, al fine di preservarne la riservatezza, anche mediante l'utilizzo di modelli contrattuali raccomandati dalla Commissione, accordi di riservatezza, rigidi protocolli di accesso, standard tecnici e l'applicazione di codici di condotta.

Questa iniziativa promuove pertanto l'apertura, la trasparenza e l'accessibilità dei dati generati dall'uso di un prodotto o di un servizio correlato al relativo utente, mettendo a disposizione un maggior numero di dati a vantaggio delle imprese, dei cittadini e delle pubbliche amministrazioni.

L'obiettivo del Data Act è quello di creare un ambiente in cui i dati siano considerati una risorsa strategica per prendere decisioni informate, stimolare l'innovazione e migliorare la collaborazione tra le diverse istituzioni.

SPAZIO EUROPEO DEI DATI SANITARI

La Proposta COM (2022) 197 del 3 maggio 2022 sullo "*spazio europeo dei dati sanitari*" (c.d. European Health Data Space - EHDS) mira a creare uno spazio europeo comune per i dati sanitari, consentendo la condivisione sicura e interoperabile delle informazioni mediche tra i paesi membri dell'Unione Europea.

L'obiettivo principale è agevolare la ricerca, l'innovazione e l'efficacia delle politiche sanitarie, nonché promuovere la salute pubblica.

L'EHDS si propone di garantire un alto livello di protezione dei dati e la fiducia dei cittadini nella gestione delle informazioni personali, assicurando al contempo il rispetto delle normative sulla privacy e la sicurezza dei dati. Questa iniziativa promette di rafforzare la cooperazione tra gli Stati membri UE e di contribuire a un sistema sanitario europeo più integrato ed efficiente.

In attesa quindi che vada a compimento la proposta di regolamento sull'European Health Data Space stanno nascendo molte iniziative pubbliche e private finalizzate alla creazione di Data Base aperti per la condivisione dei dati sanitari.

****

L'attenzione ai dati che compongono i data set di addestramento, convalida e prova dei sistemi di AI permetterà non solo una maggiore aderenza ai requisiti imposti dall'AI ACT ma anche risultati di out put migliori; un algoritmo addestrato con dati di buona qualità non potrà che generare output di qualità.

Software medicali basati sulla IA: cosa è possibile fare con i dati dei pazienti

Articolo di Avv. Silvia Stefanelli e Avv. Maria Livia Rizzo

18 Giugno 2024

L'AI ACT ha come obiettivo principale quelli di disciplinare l'immissione nel mercato e l'uso di sistemi di AI. È quindi regolamento verticale rispetto al GDPR, che è invece disciplina di natura orizzontale.

Ai fini però di garantire che i sistemi di AI siano correttamente progettati e realizzati, l'AI Act contiene una norma specifica dui dati: l'art. 10, che obbliga il fornitore del sistema ad impostare una corretta **governance dei dati**.

Il riferimento, in particolare, è ai dati utilizzati per addestramento, convalida e test dei modelli di AI.

Secondo il par. 2 dell'art. 10 dell'AI Act, questi dati devono "*essere pertinenti, sufficientemente rappresentativi e, per quanto possibile, privi di errori e completi in vista dello scopo previsto*".

Non sfugge, ovviamente, il parallelismo con l'art. 5, par. 2, lett. d) del GDPR che, nel definire il principio di esattezza prescrive che i dati personali debbano essere "*esatti e, se necessario, aggiornati*" e che debbano "*essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati*".

Questo aspetto è ancora più rilevante quando i dati sono trattati da software qualificati come dispositivi medici il cui utilizzo, se basato su dati inesatti, può compromettere la salute dei pazienti.

Ma l'AI Act va oltre questo concetto e non impone la "qualità dei dati" solo con riferimento ai dati personali (ossia riferiti a persone fisiche identificate o identificabili ex art. 4 GDPR) ma a tutti i dati, anche non personali, utilizzati per il training dei modelli

di AI.

Tuttavia, il legislatore dell'AI Act tiene bene in considerazione la differenza tra queste due categorie e, ancor più, non tralascia la disciplina specifica che il GDPR all'art. 9 ha previsto per le categorie particolari di dati personali, ossia quelli che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, i dati genetici, i dati biometrici intesi a identificare in modo univoco una persona fisica, i dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

Memore del fatto che il Regolamento Privacy di norma vieta il trattamento di questi dati, salvo in presenza di puntuali condizioni (par. 2 dell'art. 9) il legislatore dell'AI Act lancia il cuore oltre l'ostacolo e **introduce una base giuridica specifica per il loro trattamento**.

Al par. 5, l'art. 10 dell'AI Act è previsto infatti che "*nella misura in cui è strettamente necessario per garantire l'individuazione e la correzione degli errori in relazione ai sistemi di IA ad alto rischio [...] fornitori di tali sistemi possono eccezionalmente trattare categorie particolari di dati personali*".

Con riferimento ai software di medicina predittiva, ciò implica la possibilità di utilizzare, per lo scopo descritto, i dati di salute dei pazienti elaborati dall'applicativo.

Che non si tratti di un intervento fatto "alla leggera" lo si comprende già dalle espressioni "strettamente necessario" ed "eccezionalmente", a sottolineare un **obbligo di proporzionalità** che questo utilizzo deve garantire.

Il par. 5 aggiunge poi le **specifiche condizioni** da osservare per legittimare il trattamento dei dati ex art. 9 GDPR finalizzato a correggere le distorsioni del software di IA.

Nello specifico:

1. il rilevamento e la correzione delle distorsioni non devono poter essere realizzati efficacemente elaborando altri dati, compresi quelli **sintetici o anonimizzati**;
2. i dati particolari devono essere soggetti a limitazioni tecniche sul riutilizzo

e a misure di sicurezza e di tutela della privacy all'avanguardia, compresa la **pseudonimizzazione**;

3. i dati particolari devono essere **soggetti a misure di sicurezza e garanzie adeguate,** tra cui controlli rigorosi e documentazione dell'accesso, per evitare abusi e garantire che solo le persone autorizzate abbiano accesso a tali dati personali con obblighi di riservatezza adeguati;
4. i dati particolari **non devono essere trasmessi, trasferiti o altrimenti accessibili ad altri soggetti**;
5. i dati particolari **devono essere cancellati** una volta che l'errore è stato corretto o che i dati personali hanno raggiunto il termine del periodo di conservazione;
6. il **registro delle attività di trattamento deve includere la giustificazione** del motivo per cui il trattamento dei dati particolari era strettamente necessario per individuare e correggere i bias e tale obiettivo non poteva essere raggiunto trattando altri dati.

Si tratta di una importante novità in materia di riutilizzo dei dati da parte del responsabile del trattamento, tematica di estremo interesse nel settore dei software medicali.

Su questo tema già nel 2022 l'Autorità Garante francese per la protezione dei dati, Commission nationale de l'informatique et des libertés – CNIL aveva aperto una possibile strada al secondary use, con la pubblicazione della "**Guida sul riutilizzo dei dati personali da parte dei responsabili per i propri scopi**".

La guida del CNIL chiariva che i fornitori **possono riutilizzare i dati personali per i loro scopi, se sussistono le seguenti condizioni**:

- il titolare ha concesso un **permesso esplicito**, e
- il nuovo scopo è "**compatibile**" con lo scopo originale del trattamento sulla base del test da svolgere previsto dall'Opinion n. 3/2013 del Working Party Article 29.

Nella casistica indicata dall'art. 10, par. 5, dell'AI Act questa compatibilità diviene implicita e soprattutto non servono autorizzazioni da parte del titolare del trattamento a cui il software è stato fornito.

L'utilizzo di dati particolari è quindi consentito per assicurare l'eticità del funzionamento

del sistema di intelligenza artificiale.

L'obiettivo è chiaro: rispettare quanto stabilito dall'art. 10, par. 2 lett. f) e fbis) dell'AI Act ossia **individuare, prevenire e attenuare possibili pregiudizi** che possono incidere sulla salute e sulla sicurezza delle persone, avere un impatto negativo sui diritti fondamentali o portare a discriminazioni vietate dal diritto dell'Unione, soprattutto quando i dati prodotti influenzano gli input per le operazioni future. Input che, nel settore medicale, possono fare la differenza tra l'esito fausto o infausto di un trattamento medico.

Si tratta di una norma virtuosa che, sulla scia aperta dal GDPR in ottica di libera circolazione dei dati, consente di estrapolare – anche dai dati più delicati come quelli sanitari – il potenziale per garantire che tecnologie di frontiera possano essere affidabili e godere quindi della fiducia dei pazienti e dei mercati.

Senza però dimenticarsi di farlo sulla base di presupposti rigorosi stabiliti nel rispetto della *data protection*, che l'intero Regolamento AI non preguidica. E a cui, anzi, fa riferimento già all'interno di uno dei primi Considerando, laddove mantiene fermi "*gli obblighi dei fornitori e degli installatori di sistemi di IA in qualità di responsabili o incaricati del trattamento*" (Cons. 5aa).

Il rapporto tra GDPR e i sistemi di IA

Articolo di Avv. Silvia Stefanelli

10 Giugno 2024

Che rapporto intercorre tra GDPR e AI ACT?

Le due discipline corrono su binari paralleli, che in alcuni casi si toccano ma in altri presentano differenze di rilievo.

Vediamo allora i punti principali di questo rapporto.

TIPOLOGIA DI DISCIPLINA

Senza dubbio la natura dei due provvedimenti è diversa.

Il GDPR è un regolamento orizzontale, tecnologicamente neutro, che regola tutti i trattamenti dei dati personali con l'obiettivo di proteggere le persone fisiche nell'ambito di tali trattamenti (art. 1 GDPR) .

L'AI ACT è (per buona parte) una legislazione verticale di prodotto (che segue il New Legislative Framework comunitario) che disciplina nello specifico "*le regole armonizzate per l'immissione sul mercato, la messa in servizio e l'uso dei sistemi di IA nell'Unione*" (art. 1): quindi si applica solo ai sistemi che rientrano nella nozione di AI (art. 6)

AMBITO DI APPLICAZIONE

Il GDPR si applica non solo ai soggetti che trattano i dati sul territorio comunitario, ma altresì ai soggetti che hanno sede extra EU e che trattano dati di cittadini UE (art 3)

Analogamente l'AI ACT si applica a tutti i fornitori di sistemi di AI - sia UE ed extra Ue - che immettono sul mercato Ue i suddetti sistemi (art. 2 lett. a). Si applica altresì ai soggetti che non immettono sul mercato il sistema di AI ACT, ma il cui output dell'AI ACT viene utilizzato nell'Unione (art. 2. lett. c).

I RUOLI SOGGETTIVI NEI DUE REGOLAMENTI

I ruoli soggettivi possono mutare a seconda delle situazioni.

Il provider di un sistema di AI è senza dubbio titolare dei dati per tutta la fase di sviluppo e realizzazione del sistema. Dopo l'immissione sul mercato il sistema di AI, il provider resterà titolare dei dati che servono per migliorare il sistema o correggere i bias (art. 10 comma 5), mentre il deployer (art. 3 n. 4) diventerà titolare dei dati che raccoglie tramite il sistema AI (es. l'ospedale)

I PRINCIPI DA APPLICARE

L'art 5 del GDPR stabilisce i principi che devono essere applicati nel trattamento dei dati: la liceità, la correttezza, la trasparenza, la limitazione delle finalità, la minimizzazione dei dati, l'esattezza, la limitazione della conservazione, l'integrità e la riservatezza.

L'AI ACT contiene un elenco di principi che devono essere rispettati nel Considerando 27: azione umana e supervisione, solidità tecnica e sicurezza, privacy e governance dei dati, trasparenza, diversità, non discriminazione, equità, benessere sociale e ambientale.

Alcuni di questi principi (ma non tutti) si concretizzano già attraverso obblighi specifici della legge dell'UE sull'IA:

- l'articolo 10 della legge sull'IA dell'UE prescrive pratiche di governance dei dati per i sistemi di IA ad alto rischio,
- l'articolo 13 della legge sull'IA dell'UE riguarda la trasparenza,
- gli articoli 14 e 26 della legge dell'UE sull'IA introducono requisiti di sorveglianza e monitoraggio umano,
- l'articolo 27 della legge dell'UE sull'IA introduce l'obbligo di condurre valutazioni d'impatto sui diritti fondamentali per alcuni sistemi di IA ad alto rischio.

IL PROCESSO AUTOMATIZZATO E LA SUPERVISIONE UMANA

Questo è il tema in GDPR e AI ACT sembrano intersecarsi in maniera più importante

L'art. 22 del GDPR stabilisce che "*1. L'interessato ha il diritto di non essere sottoposto a*

una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona"

Tale previsione non si applica nei casi elencati all'art. 2 par. 2.

Chiaramente l'obiettivo è quello di permettere che l'uomo mantenga il controllo sugli effetti che un trattamento di dati può avere all'interno della Sua sfera giuridica.

Anche l'AI ACT ha come obiettivo quello di tenere l'uomo al centro (il cosiddetto effetto "human-in-the-loop")

Tale obiettivo si estrinseca nell'art. 14 il quale prevede che i sistemi di IA ad alto rischio siano progettati e sviluppati in modo tale da poter essere efficacemente supervisionati da persone fisiche durante il periodo in cui il sistema di IA è in uso (anche con adeguati strumenti di interfaccia uomo-macchina).

In altre parole, i fornitori devono adottare un approccio di "***supervisione umana fin dalla progettazione***" allo sviluppo di sistemi di intelligenza artificiale.

Inoltre l'art. 26, paragrafo 1, della legge dell'UE sull'IA, stabilisce che il deployer deve adottare misure tecniche e organizzative adeguate a garantire che l'uso di un sistema di IA sia conforme alle istruzioni per l'uso che accompagnano il sistema, anche per quanto riguarda la supervisione umana.

Chiaro che sotto questo profilo i due sistemi di intersecano in maniera importante.

Infatti il livello di supervisione e di intervento umano (maggiore o minore) esercitato da un utente di un sistema di IA può far sì che il sistema rientri o meno sotto l'alveo di applicazione dell'art. 22. In altre parole, un intervento significativo da parte di un essere umano in una fase chiave del processo decisionale del sistema di IA può essere sufficiente a garantire che la decisione non sia più completamente automatizzata ai fini dell'articolo 22 del GDPR.

LA FRIA E LA DPIA

Quali sono le differenze tra la "Valutazione d'impatto sui diritti fondamentali per i sistemi di IA ad alto rischio" (c.d. FRIA - art. 27 AI ACT) e la Valutazione d'impatto sulla protezione dei dati" (c.d. DPIA ex art. 35 GDPR)?

Si tratta di due strumenti che si pongono il medesimo obiettivo: valutare i rischi e decidere le possibili mitigazioni di tali rischi.

Presentano però alcune differenze.

L'esecuzione di una DPIA è richiesta solo quando vengono trattati dati personali e tale trattamento presenta un alto rischio (art. 35 par. 1)

La FRIA invece deve essere posta in essere dal deployer in tutti i casi in cui utilizza un sistema di AI (indipendentemente dalla natura del dato, personale o non personale - art. 27 AI ACT).

Inoltre la DPIA ha come obiettivo quello considerare solo i rischi per la privacy e i dati personali (art. 7 e art. 8 del Codice), mentre la FRIA ha un ambito di indagine più ampio perché deve verificare tutte le tipologie di rischi che possono impattare sulla persona fisica nell'utilizzo del sistema di AI.

Quindi

Il deployer che utilizza sistemi di AI deve sempre effettuare la FRIA (e magari può utilizzare la DPIA collegata al software per l'analisi dei rischi e degli impatti in relazione alla protezione dei dati).

L'utilizzatore di un software dovrà fare la DPIA solo se il trattamento è ad alto rischio (attenzione però perché l'interpretazione della nozione di "alto rischio" del nostro Garante è molto ampia), mentre non dovrà fare la FRIA se il software/apparecchio che sta utilizzando non rientra nella nozione di AI.

Pubblicato il decalogo sull'Intelligenza Artificiale in Sanità

Articolo di Avv. Maddalena Collini e Avv. Federica Pucarelli

29 Novembre 2023

Il 12 ottobre 2023 il Garante Privacy ha pubblicato sul suo sito web il "**Decalogo per la realizzazione di Servizi Sanitari Nazionali attraverso sistemi di intelligenza artificiale**".

Il documento evidenzia in dieci punti gli aspetti più rilevanti per la corretta progettazione ed utilizzo della AI da parte del Sistema Sanitario Nazionale, ciascuno relativo agli aspetti di protezione dei dati personali che in tale contesto assumono fondamentale importanza.

In questo articolo approfondiremo il punto relativo ai principi di *accountability* e di *privacy by design*, che costituiscono le premesse fondamentali per la corretta gestione degli aspetti in materia di protezione dei dati correlati alle attività di trattamento svolte dalle organizzazioni, siano esse pubbliche o private.

Il principio è uno dei 10 fondamentali punti previsti dal Garante nel nuovo Decalogo.

Con riguardo al punto n.2, il Garante privacy italiano riprende il concetto di "accountability", rammentando che il titolare del trattamento – in questo caso l'ente sanitario pubblico – deve "*conformarsi ed essere in grado di comprovare il rispetto dei principi e degli adempienti previsti dal Regolamento e di aver effettivamente tutelato il diritto alla protezione dei dati personali degli interessati fin dalla progettazione e per impostazione predefinita (artt. 5, par. 2, 24 e 25, par. 1, del Regolamento)*".

L'approccio adottato dal rinnovato quadro normativo in materia di protezione dei dati personali richiede, infatti, una preliminare valutazione dei rischi per i diritti e le libertà degli interessati correlati al trattamento dei dati svolto o che si intende svolgere.

Questa valutazione ha come primaria finalità quella di adottare un apparato di misure di sicurezza tecniche ed organizzative adeguato ed efficace a contrastare proprio quegli stessi rischi individuati nella prima fase valutativa.

Tutte le scelte che verranno assunte per proteggere in modo adeguato i diritti e le libertà degli interessati in relazione al trattamento dei loro dati dovranno poi essere

Questa "responsabilizzazione" dei titolari trova contenuto nell'altro principio richiamato dall'Autorità, quello di *privacy by design e by default*, che traduciamo con il concetto di "*protezione dei dati fin dalla progettazione e per impostazione predefinita*" (art. 25 del Regolamento), secondo cui:

- già in fase di progettazione devono essere integrate nel trattamento le garanzie necessarie per soddisfare i requisiti del Regolamento e tutelare i diritti e le libertà degli interessati, e
- tali misure devono garantire – per impostazione predefinita – che il trattamento sia proporzionato rispetto all'interesse perseguito e che siano trattati i soli dati necessari al raggiungimento di questo interesse.

In sostanza, il Sistema Sanitario Nazionale – già in fase di progettazione e nel funzionamento delle tecnologie di IA generativa per i servizi sanitari – dovrà integrare nel trattamento misure di sicurezza che consentano di rispettare i principi di protezione dei dati personali, richiamati proprio nei dieci punti del Decalogo dell'Autorità.

Appare quindi del tutto naturale e logico che tale principio veda coinvolti proprio i produttore di tecnologie IA per il contesto sanitario, anche alla luce del considerando 78 del Regolamento che afferma che: "*in fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte, a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati.*"

In sostanza, quindi, i produttori di tecnologie e software che integrano sistemi di IA generativa applicata al contesto sanitario dovranno creare sistemi e prodotti che consentano a chi li utilizza – in particolare la struttura sanitaria titolare dei dati – di rispettare le regole del GDPR, nonché le future regole in materia di IA.

Analisi del decalogo del Garante Privacy sull'Intelligenza Artificiale in sanità

Articolo di Avv. Maddalena Collini e Avv. Federica Pucarelli

21 Dicembre 2023

Il "Decalogo per la realizzazione di Servizi Sanitari Nazionali attraverso sistemi di intelligenza artificiale" è il recente documento che il Garante Privacy ha pubblicato per evidenziare in dieci punti gli aspetti privacy più rilevanti per la corretta progettazione ed utilizzo della AI da parte del Sistema Sanitario Nazionale. Il focus è sui profili privacy legati alla progettazione ed utilizzo si sistemi intelligenti in sanità.

Abbiamo approfondito i principi di accountability e di privacy by design e by default nel precedente capitolo.

Nel presente contributo parliamo degli altri principali punti affrontati nel Decalogo.

I PRINCIPI DI CONOSCIBILITÀ, NON ESCLUSIVITÀ E NON DISCRIMINAZIONE ALGORITMICA

Al punto n. 4 del Decalogo l'Autorità richiama i tre principi cardine che devono governare l'utilizzo di algoritmi e di strumenti di IA nell'esecuzione di compiti di rilevante interesse pubblico: **conoscibilità, non esclusività e non discriminazione algoritmica.**

Sul tema il Decalogo del Garante tiene conto non solo di alcune previsioni del GDPR e della giurisprudenza del Consiglio di Stato in materia di utilizzo di algoritmi di AI per l'adozione di decisioni di natura amministrativa, ma altresì delle norme e delle prescrizioni contenute nella Proposta di Regolamento per l'Intelligenza Artificiale (COM (2021) 206 final – d'ora in avanti "Regolamento AI").

Circa il *principio di conoscibilità*, il Garante rammenta che l'interessato ha diritto a conoscere l'esistenza di decisioni basate su trattamenti automatizzati, nonché a ricevere informazioni sulla logica utilizzata per raggiungerle. Tale principio è espressione di quello più generale di trasparenza previsto dall'art. 5 GDPR, nonché del diritto dell'interessato di ricevere informazioni relativamente al trattamento dei propri dati personali (art. 13

e 14 GDPR).

Il secondo principio è quello di *non esclusività della decisione algoritmica*, il quale enuncia il dovere di **mantenere un intervento umano per la convalida o la smentita della decisione finale** presa in un primo momento dal sistema di IA (c.d. principio di human in the loop).

In sostanza, l'Autorità riprende e sviluppa quanto già disposto dal GDPR all'art. 22, in cui si fa espresso divieto di adottare decisioni esclusivamente basate sul trattamento automatizzato dei dati dell'interessato: previsione che si sostanzia quindi in un divieto generale che opera ex ante, e non in un mero diritto di opposizione ex post la cui attuazione viene lasciata all'iniziativa dell'interessato.

Infine, richiamando il Considerando n. 71 GDPR, il Decalogo enuncia il *principio di non discriminazione algoritmica*. Tale principio richiede che vegano utilizzati sistemi di IA affidabili che riducano le **opacità e gli errori dovuti a cause tecnologiche o umane**. Il rispetto di tale principio richiede una verifica periodica dell'efficacia del sistema stesso alla luce delle evoluzioni tecnologiche, matematiche e statistiche in materia e l'adozione di misure tecniche e organizzative adeguate. Ciò, in particolare, in ragione del potenziale effetto discriminatorio che un trattamento inesatto di dati sullo stato di salute può determinare nelle persone fisiche.

Tale previsione porta con sé rilevanti conseguenze per i fornitori di software, in particolare con riferimento alla pretesa di riservatezza dell'algoritmo posto alla base del sistema di IA.

LA VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI ("VIP" O "DPIA")

Il Decalogo riprende, al punto n. 5, l'obbligo imposto dal GDPR per i Titolari di svolgere una preventiva valutazione di impatto sul trattamento che "prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (art. 35), e di consultare l´Autorità di controllo qualora le misure tecniche e organizzative individuate per mitigare l´impatto del trattamento sui diritti e le libertà

degli interessati non siano ritenute sufficienti, ovvero quando il rischio residuale per i diritti e le libertà degli interessati resti elevato (art. 36).

A tale riguardo, si ricorda che il Gruppo di Lavoro ex art. 29 ha pubblicato le Linee-guida concernenti la valutazione di impatto sulla protezione dei dati che contengono i criteri per stabilire se un trattamento "possa presentare un rischio elevato" e per i quali sarà appunto obbligatorio condurre una VIP.

Come ricordato dall'Autorità, infatti, la previsione di un sistema centralizzato a livello nazionale attraverso il quale realizzare servizi sanitari con strumenti di IA, determina un trattamento a "rischio elevato" per i diritti e le libertà degli interessati, dal momento che si tratta di un trattamento:

- sistematico,
- su larga scala,
- di particolari categorie di dati personali di cui all'art. 9 del Regolamento,
- di soggetti vulnerabili,
- attraverso l'uso di nuove tecnologie.

La valutazione di impatto costituisce allora uno strumento fondamentale per l'individuazione delle misure idonee a tutelare i diritti e le libertà fondamentali degli interessati e a garantire il rispetto dei principi generali del Regolamento, nonché per consentire l'analisi della proporzionalità dei trattamenti effettuati.

Trattandosi di adempimento dinamico, non sarà possibile svolgere una valutazione d'impatto una tantum, ma occorrerà necessariamente prevedere strumenti di monitoraggio e aggiornamento di tale valutazione.

L'Autorità infine precisa i potenziali rischi derivanti dalla costituzione e utilizzo di una banca dati contenente le informazioni sanitarie di tutta la popolazione assistita sul territorio nazionale, quali ad esempio quelli relativi alla "*perdita dei requisiti di qualità dei dati (es. mancato o errato allineamento e aggiornamento), alla revoca del consenso, ove lo stesso costituisca la base giuridica del trattamento originario, alla re-identificazione dell'interessato in considerazione delle possibili interconnessioni con molteplici sistemi*

informativi e banche dati e all'utilizzo dei dati per finalità non compatibili".

QUALITÀ DEI DATI

Sulla *qualità dei dati*, il Garante al punto n. 6 del Decalogo richiama l'obbligo per il Titolare di garantire che i dati siano esatti e, se necessario, aggiornati, adottando tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati non corretti rispetto alle finalità per le quali sono trattati (principio di «esattezza», di cui all'art. 5, par. 1, lett. d), del Regolamento).

Il principio della qualità dei dati mira, infatti, a tutelare anche l'efficacia e la correttezza dei servizi sanitari, evitando che gravi danni alla salute possano derivare dall'elaborazione di dati raccolti per finalità di cura che siano eventualmente diventati inesatti o non siano aggiornati con il passare del tempo, oppure che **non siano adeguatamente rappresentativi** della realtà in cui il sistema di IA è destinato ad operare.
Ciò rispetta il noto principio *garbage in – garbage out*, secondo cui se il dataset fornito in fase di addestramento dell'algoritmo o del sistema di IA è viziato e dunque composto da dati non corretti o non aggiornati, anche il prodotto finale e la decisione presa dall'IA sarà inevitabilmente non corretta.

A tale scopo, la valutazione d'impatto dovrà quindi necessariamente tenere in considerazione gli specifici rischi, quali ad esempio la discriminazione, legati all'elaborazione dei dati attraverso sistemi di IA.

INTEGRITÀ E RISERVATEZZA

Anche il punto n. 7 del Decalogo riprendono principi generali già previsti dal GDPR. Il Garante coglie l'occasione per approfondire i principi citati e porre un forte accento sulla concretezza delle valutazioni che ciascun Titolare è tenuto a svolgere. Non è sufficiente, infatti, adottare misure di sicurezza standard rispetto al rischio calcolato, ma al contrario è necessario **valutare in concreto** i rischi per i diritti e le libertà degli interessati derivanti dai trattamenti in esame: ciò significa, specifica l'Autorità, che è fondamentale tenere in considerazione le caratteristiche delle banche dati di volta in volta utilizzate e i modelli di analisi impiegati. L'attenzione è ancora maggiore se i

trattamenti riguardano dati sanitari, su larga scala, di soggetti vulnerabili che possono portare all'adozione di decisioni automatizzate.

Per rimanere su un piano sostanziale, quando si parla di AI e di machine learning, uno dei principali rischi da tenere in considerazione è quello della potenziale opacità nella fase di sviluppo degli algoritmi, errori e distorsioni (cc.dd. bias). Mitigare tali rischi significa, anzitutto, rendere trasparenti le logiche algoritmiche utilizzate al fine di "generare" i dati e i servizi attraverso i sistemi di IA, le metriche utilizzate per addestrare il modello, le verifiche per il rilevamento e la correzione dei bias.

CORRETTEZZA E TRASPARENZA

La necessità di chiarire le logiche algoritmiche ben si collega al principio di trasparenza approfondito al punto n. 8 del Decalogo. In particolare, è richiamato il concetto di "consapevolezza" che deve crescere nella collettività – in particolare tra gli assistiti del Sistema Sanitario Nazionale – in relazione all'impiego di sistemi intelligenti nel percorso di cura.

A questo proposito, il Garante elenca le informazioni che dovrebbero essere rese pubbliche al fine di rendere più trasparente, a partire dal coinvolgimento degli stakeholder e degli interessati, alla pubblicazione di un estratto della valutazione di impatto, alla redazione di informative chiare e complete di elementi aggiuntivi rispetto a quelli imposti dalle norme (ad esempio, l'indicazione dei vantaggi diagnostici e terapeutici, derivanti dall'utilizzo di tali nuove tecnologie).

SUPERVISIONE UMANA E DIGNITÀ DELLA PERSONA

Il Decalogo si chiude con due concetti legati tra loro e di fondamentale importanza, tanto da essere costantemente presenti nei dibattiti e nei dialoghi aventi ad oggetto l'IA. La necessità di una costante supervisione umana si intreccia infatti con i temi etici legati al ricorso di tecnologie intelligenti, e porta il Titolare a dover tenere sempre presente il diritto di ogni persona di non essere assoggettato a una decisione basata esclusivamente su un trattamento automatizzato. Per questo motivo la supervisione deve essere costante, sia nella fase di addestramento del software, sia durante il suo

utilizzo.
Questo al fine di garantire un trattamento – non solo di dati personali ma anche terapeutico – non discriminatorio, etico, di qualità.

Intelligenza artificiale e protezione dei dati: una convivenza possibile?

Articolo di Avv. Maddalena Collini e Avv. Federica Pucarelli

1 Febbraio 2023

L'obiettivo di una legislazione europea sull'IA è quello di assicurare – come si legge Relazione di accompagnamento della Proposta di Regolamento sull'IA – che "*i cittadini europei possano beneficiare di nuove tecnologie sviluppate e operanti in conformità ai valori, ai diritti fondamentali e ai principi dell'Unione*".

Tra questi diritti riveste certamente un ruolo primario quello alla **protezione dei dati personali.**

Ne è prova il fatto che i temi privacy sono di primaria importanza sui tavoli di lavoro europei sull'AI, dove si cerca di trovare un equilibrio sostenibile tra innovazione (responsabile, etica, equa) e tutela dei dati personali e, quindi, degli individui a cui si riferiscono.

Anche il Comitato europeo per la protezione dei dati (EDPB) e il Garante europeo della protezione dei dati (GEPD), nel loro parere congiunto del giugno del 2021, hanno dato il loro contributo con suggerimenti di emendamenti al fine di arricchire e migliorare la Proposta.

Oggi, nonostante EDPB e GEPD sottolineino che è "*ancora lungo il percorso da compiere affinché dalla proposta possa scaturire un quadro giuridico ben funzionante, in grado di integrare efficacemente l'RGPD*", possiamo leggere la Proposta e il GDPR per individuare i principali punti di contatto.

A ben vedere, le implicazioni con la disciplina in tema di dati personali si rinvengono fin dalla lettura dei primi Considerando.

Tra i temi più rilevanti, troviamo: l'approccio basato sull'analisi del rischio e il principio di *accountability*, la qualità ed esattezza dei dati, il principio di *privacy by design e by default*, il principio di trasparenza, il meccanismo sanzionatorio.

1. **Approccio basato sull'analisi del rischio**

La Proposta, in particolare l'art. 9 e il Considerando n. 42, prescrivono per ogni provider l'adozione di un sistema di gestione del rischio dai contorni simili a quello previsto dalla disciplina del GDPR.
Le norme della Proposta prescrivono infatti di **mappare i rischi conosciuti** e quelli **prevedibili**, di **mitigarli e gestirli**, **di informare** gli interessati della loro esistenza, di monitorare e aggiornare il sistema di gestione costantemente.
Un approccio che sembra scostarsi poco dall'analisi del rischio che il GDPR **prescrive agli articoli 25 e 35**.

2. **La qualità ed esattezza dei dati**

Quello della **qualità e dell'accuratezza dei dati** è uno dei requisiti per la messa in commercio dei sistemi di IA ad alto rischio.
È una specificità introdotta dall'art. 10 della Proposta, che prevede al comma 3 che i **set di dati** utilizzati per l'addestramento dei modelli debbano essere "*pertinenti, rappresentativi, esenti da errori e completi*".
Nonostante ogni principio debba essere letto nello specifico contesto dove è inserito, è immediato il parallelismo con i principi applicabili al trattamento dei dati personali elencati all'art. 5 GDPR, dove si trovano, tra gli altri, il principio di minimizzazione, di esattezza, di integrità.
Per un approfondimento sul tema dell'esattezza dei dati e sul differente significato del termine in campo privacy e AI, si veda il nostro articolo: "AI ed esattezza dei dati: il quadro giuridico è sufficiente?"

3. **Privacy by design e by default**

L'art. 10 della Proposta introduce anche un approccio che sembra riflettere (almeno in parte) il principio di privacy by design e by default di cui all'art. 25 GDPR.
È infatti previsto che i sistemi di AI, e in particolare quelli che prevedono l'uso di dati per l'addestramento di modelli, sono sviluppati tenendo conto di una serie di profili imprescindibili, come: la raccolta di dati (b); le operazioni di trattamenti pertinenti ai fini della preparazione dei dati, compresi la pulizia dei dati, l'aggregazione,

l'arricchimento (c); una valutazione preliminare della disponibilità, della quantità e dell'adeguatezza dei set di dati necessari (e); l'individuazione di eventuali lacune o carenze nei dati e il modo con cui possono essere colmate (g).
Un **metodo** che sembra ricalcare l'approccio concettuale di mappatura, **progettazione e analisi** preventiva che fa da bussola alla **disciplina sulla protezione dei dati personali**.

4. Principio di trasparenza

L'art. 13 della Proposta prevede obblighi di trasparenza laddove afferma che "*i sistemi di intelligenza artificiale ad alto rischio devono essere progettati e sviluppati in modo tale da garantire che il loro funzionamento sia sufficientemente trasparente da consentire agli utenti di interpretare l'output del sistema e utilizzarlo adeguatamente*".
Pur non prevedendo in modo esplicito l'intersecazione di tali adempimenti con il GDPR, pare logico il richiamo al principio di trasparenza previsto all'art. 5 del GDPR, che impone ai Titolari del trattamento di rendere gli interessati consapevoli di come saranno gestiti i dati in relazione allo specifico trattamento svolto, nonché dei rischi ad esso correlati.
Tale dovere di trasparenza si sostanzia nel rispetto dei doveri informativi di cui gli artt. 13 e 14 del GDPR che prevedono che il titolare informi gli interessati su come verranno gestiti i dati a lui riferiti e dei diritti esercitabili in materia di protezione dei dati.

5. I processi decisionali automatizzati

L'art. 14 della Proposta individua i casi in cui è necessaria un'attività di sorveglianza umana sul sistema di IA ad alto rischio, con l'obiettivo di prevenire o ridurre al minimo i rischi per la salute, la sicurezza o i diritti fondamentali degli individui. In tal senso, vengono quindi previste misure finalizzate a **rendere consapevoli** i soggetti a cui viene affidata la sorveglianza dei limiti del sistema di IA e di metterli in condizione di poter **valutare** criticamente **gli output** da esso prodotti, oltre che di discostarsene laddove necessario.
Anche in tal caso, tale previsione presenta affinità e, anzi, sembra porsi in contrasto,

con quanto disposto dall'**art. 22 del GDPR** che prevede il **diritto per gli interessati di non essere sottoposti ad una decisione basata unicamente sul trattamento automatizzato**, compresa la profilazione, che sia finalizzata all'assunzione di una decisione rilevante per la loro sfera giuridica.

L'art. 22 infatti non pone un divieto tout court, ma in deroga a tale limitazione prevede che il **titolare possa assumere una decisione basata su un sistema automatizzato** quando

- è **necessaria** all'esecuzione del contratto con l'interessato
- è **autorizzata dal diritto** dell'Unione, oppure
- vi sia il **consenso** dell'interessato.

Nel primo e nel terzo caso, l'interessato ha infatti il diritto a richiedere che nel processo decisionale automatizzato sia previsto l'intervento umano, di esprimere la propria opinione e di contestare la decisione.

Inoltre, tornando ai doveri informativi di cui al punto precedente, il titolare dovrà informare l'interessato dell'esistenza del sistema di decisione automatizzata, della logica che utilizza e delle conseguenze che tale trattamento avrà sulla sua persona, con ciò sollevando difficili problematiche correlate alla "spiegabilità" dei sistemi di IA.

6. Le sanzioni

L'art. 72 della Proposta di Regolamento prevede che il **Garante europeo della protezione dei dati possa infliggere sanzioni amministrative** pecuniarie alle istituzioni, alle agenzie e agli organismi dell'Unione che rientrano nell'ambito di applicazione del Regolamento IA, seguendo il **criterio del "tetto massimo"** come già previsto nel GDPR:

- fino a 500 0000 EUR per l'inosservanza del divieto delle pratiche di intelligenza artificiale di cui all'articolo 5;
- fino a 250 000 EUR per non conformità del sistema di IA ai requisiti di cui all'articolo 10 (dati e governance dei dati).

Nel commisurare la sanzione amministrativa, il Garante Europeo dovrà tenere conto della natura, della gravità e della durata della violazione, del grado di cooperazione con l'Autorità al fine di porre rimedio alla violazione e delle precedenti analoghe violazioni eventualmente commesse dal medesimo organismo.

AI E REGOLAMENTAZIONE DA PRODOTTO

ISO 42001 per aziende biomedicali e AI ACT

Articolo di Ing. Alice Ravizza

1 Ottobre 2024

L'AI Act è un regolamento dell'Unione Europea pensato per disciplinare i sistemi di intelligenza artificiale (IA) tra cui quelli ad alto rischio, con un focus particolare sulla sicurezza, conformità e trasparenza.
Questo Regolamento deve essere applicato anche dalle aziende biomedicali che si occupano di proporre sul mercato dispositivi medici con moduli basati su principi di IA: è prevista la applicazione in modo integrato rispetto al MDR.
Negli articoli del regolamento AI Act che descrivono le responsabilità delle aziende "fornitori di sistemi IA ad alto rischio" vi sono chiare assonanze con le responsabilità assegnate ai Fabbricanti dal MDR.

L'approccio integrato alla conformità regolatoria passa, innanzi tutto, dalla costruzione di un **sistema di gestione della qualità completo, che consenta all'azienda di affrontare le fasi di ideazione, progettazione, test e immissione in commercio in modo coordinato ed efficiente**.

Nell'articolo 16 del AI Act elenca i **principali obblighi dei fornitori di sistemi IA ad alto rischio,** che comprendono anche tutti i DM con IA che siano di classe superiore alla I.

Ne citiamo alcuni:

- Sistema di gestione della qualità: i fabbricanti/ fornitori devono avere un sistema di gestione della qualità conforme all'articolo 17 del AI Act, oltre che all'articolo 10 del MDR.

- Documentazione e registri: devono conservare documentazione tecnica e log di funzionamento generati automaticamente dai sistemi; gli articoli 18 e 19 del AI Act integrano i diversi articoli di MDR e l'Allegato II del MDR.

Il sistema di gestione della qualità, descritto come detto nell'articolo 17 del AI Act, deve essere strutturato per coprire le diverse fasi dello sviluppo e utilizzo del sistema IA, tra cui:

- **Progettazione e sviluppo**: devono essere previste procedure per la progettazione, verifica e controllo di qualità del sistema IA ad alto rischio;
- **Gestione dei dati**: le operazioni riguardanti i dati, come raccolta, analisi e conservazione, devono essere gestite con attenzione prima della messa in commercio del sistema;
- **Monitoraggio post-vendita**: il fornitore è tenuto a mantenere un sistema di monitoraggio continuo del sistema IA dopo la sua immissione sul mercato.

Possiamo dunque ipotizzare di costruire un sistema di gestione per la qualità che risponda a questi obblighi regolatori sovrapposti.

Lo standard ISO 42001 fornisce linee guida per le organizzazioni che sviluppano, utilizzano o forniscono sistemi di IA, promuovendo l'uso responsabile di tali tecnologie. Inoltre, sistemi IA che apprendono continuamente richiedono una gestione specifica per garantire che il loro comportamento, in evoluzione, rimanga conforme alle norme e agli standard di sicurezza, inclusi quelli relativi ad MDR nel caso di DM con IA.
Lo standard ISO 42001 non è immediatamente comparabile, nella struttura dei capitoli, allo standard ISO 13485 ma consente in diverse sezioni un approccio integrato.

Una delle prime attività richieste dalla norma ISO 42001 è la **valutazione del contesto**: ad esempio, si può utilizzare la metodologia PESTEL che appare particolarmente adeguata.

Un'analisi PESTEL applicata a una società che sviluppa software medico basato su IA evidenzia come fattori esterni, quali le regolamentazioni politiche, i fattori economici, l'opinione pubblica e i progressi tecnologici, influenzano direttamente lo sviluppo e la

commercializzazione di tali sistemi.

Questa attività può essere integrata con altre analisi di contesto e definizioni di ruoli regolatori, tipicamente presenti nei sistemi di qualità ISO 13485 di aziende che utilizzano la norma armonizzata ai fini di conformità al MDR.

La leadership e l'impegno della direzione sono identificati dalla ISO 42001 come aspetti fondamentali per il successo di un sistema di gestione dell'IA.
La direzione aziendale deve dimostrare il proprio impegno attraverso diverse azioni, tra cui:

- Stabilire una "politica di IA" e degli obiettivi compatibili con la direzione strategica dell'organizzazione;
- Integrare i requisiti del sistema di gestione IA nei processi aziendali (ad esempio la progettazione e la gestione dei dati di ritorno dal mercato);
- Garantire la disponibilità delle risorse umane e strumentali necessarie per il funzionamento del sistema di gestione IA;
- Comunicare l'importanza di una gestione efficace dell'IA e della conformità ai requisiti del sistema di gestione a tutto il personale coinvolto;
- Assicurarsi che il sistema di gestione IA raggiunga i risultati previsti, i cosiddetti "obiettivi di qualità";
- Promuovere il miglioramento continuo e supportare i collaboratori nel contribuire all'efficacia del sistema di gestione IA.

Come si vede, queste azioni di costruzione del sistema di qualità sono adatte ad essere integrate in un sistema ISO 13485 già esistente, così come la integrazione nella politica di qualità di un quadro di riferimento per fissare anche gli obiettivi IA, garantendo l'impegno al rispetto dei requisiti applicabili (MDR, AI Act ed altri requisiti tecnico-commerciali) e al miglioramento continuo del sistema.

Anche nella **gestione di ruoli e responsabilità interne** e nella gestione delle relazioni con terze parti e clienti, le norme ISO 13485 e ISO 42001 sono integrabili in un sistema coerente ed efficiente.

Infatti, per ISO 42001 la direzione deve garantire che i ruoli, le responsabilità e le autorità siano chiaramente assegnati e comunicati all'interno dell'organizzazione. Le responsabilità principali da aggiungere a un sistema ISO 13485 già esistente includono:

- Assicurare che il sistema di gestione IA sia conforme ai requisiti.
- Riferire alla direzione sulle prestazioni del sistema di gestione IA.

Questi aspetti gestionali sono presenti anche quando sono coinvolte terze parti nel ciclo di vita del sistema IA.
La gestione delle relazioni con fornitori e clienti deve riflettere l'impegno dell'organizzazione nello sviluppo e uso responsabile dei sistemi IA, assicurando che i fornitori seguano un approccio coerente con i principi dell'organizzazione e che le aspettative dei clienti siano considerate nel processo di sviluppo dei sistemi: nuovamente, un approccio integrato con la ISO 13485 e la identificazione dei "critical suppliers" si prospetta come possibile ed adeguato.

Le norme ISO 42001 e ISO 13485 non sono coerenti solo negli aspetti di costruzione dei sistemi di qualità, ma anche negli aspetti di operatività del sistema (dalla gestione del processo di progettazione in avanti).

È auspicabile dunque che tutti i portatori di interesse prendano in considerazione questo approccio integrato e che nuove buone pratiche di applicazione siano discusse da tutta la comunità che si occupa di scienze regolatorie.

Progettazione secondo MDR - norme tecniche requisito essenziale di sicurezza

Articolo di Ing. Alice Ravizza

4 Giugno 2024

Le norme tecniche rivestono un ruolo cruciale nella regolamentazione dei dispositivi medici, poiché forniscono ai Fabbricanti chiare indicazioni sui requisiti tecnici dei prodotti e sui metodi di test necessari per garantire il rispetto di tali requisiti.
Le norme tecniche armonizzate, inoltre, **garantiscono una presunzione di conformità** ai requisiti dei Regolamenti MDR ed IVDR; ciò implica che, se un fabbricante aderisce pienamente a tutte le parti applicabili di queste norme, si dà per assodato che tale dispositivo sia in linea con i requisiti del regolamento.
Questo aspetto facilita notevolmente il processo di dimostrazione della conformità durante le valutazioni, dato che le autorità competenti e gli organismi notificati trattano il rispetto di queste norme come prova sufficiente che i requisiti del regolamento sono stati rispettati.

Un esempio classico di queste norme armonizzate, utili in modo ampio sull'intero spettro delle categorie merceologiche di DM e IVD, sono le norme ISO 13485 e ISO 14971.
Queste norme sono facilmente applicabili anche al contesto di tecnologie innovative, come MD e IVD che ottengano la loro prestazione grazie a principi di AI.

Anche l**e norme tecniche non armonizzate forniscono indicazioni su come possano essere soddisfatti i requisiti di sicurezza** e performance richiesti dal regolamento.
L'uso di queste norme è commentato nella "Blue Guide" dell'Unione Europea, un documento che fornisce linee guida generali per l'attuazione di direttive e regolamenti. Sebbene non conferiscano una presunzione automatica di conformità, le norme non armonizzate servono comunque come importanti riferimenti per rispettare i requisiti. Infatti, rappresentano lo "stato dell'arte" e dunque rappresentano un chiaro e robusto criterio per la valutazione del rapporto rischio-beneficio.

Conseguentemente, in assenza attualmente di norme armonizzate che si rivolgano verticalmente ai MD e IVD "AI-powered", è ragionevole identificare le norme non armonizzate più adeguate.

La norma IEC 62304 è uno standard internazionale che stabilisce i requisiti relativi ai processi del ciclo di vita del software utilizzato nei dispositivi medici. Questa norma fornisce un framework metodologico per la gestione della sicurezza del software, che include lo sviluppo, la manutenzione e il controllo dei processi software per i dispositivi medici. Essa offre importanti indicazioni per aiutare i fabbricanti a conformarsi al requisito essenziale 17 del MDR, specifico per i SaMD. Analogamente si può dire per l'equivalente requisito essenziale 16 del IVDR.

Tuttavia, per i dispositivi medici che incorporano tecnologie avanzate come l'intelligenza artificiale (IA), specialmente quelli che si affidano a principi di IA per erogare la loro prestazione clinica o la performance diagnostica, aderire esclusivamente alla norma IEC 62304 può non essere sufficiente. Questo perché l'IA introduce variabilità e complessità che possono non essere completamente indirizzate dai requisiti standardizzati del software "statico", descritti nella IEC 62304.

I dispositivi medici che utilizzano l'IA, in particolare quelli basati su algoritmi di apprendimento automatico, possono subire modifiche nel loro comportamento a seguito dell'interazione con nuovi dati clinici, una caratteristica non coperta in modo esaustivo dalla gestione del ciclo di vita descritta in IEC 62304.

Per queste ragioni, **i fabbricanti di dispositivi medici che sfruttano l'IA come parte della loro funzionalità principale devono considerare ulteriori misure di conformità e valutazione del rischio**.

Questo potrebbe includere:

- **Validazione specifica per l'IA**: sviluppare e attuare protocolli di test che sono particolarmente disegnati per i sistemi di IA, in grado di valutare la robustezza, la sicurezza e l'efficacia degli algoritmi in scenari di utilizzo reali e su dataset variabili.
- **Trasparenza e spiegabilità**: fornire una documentazione dettagliata sui principi di

funzionamento dell'IA, inclusi gli algoritmi utilizzati, le modalità di addestramento dei modelli e le misure adottate per garantire la trasparenza e la comprensione dei processi decisionali automatici.

- **Valutazione continua dei dati in ingresso**: implementare strategie per la valutazione e il monitoraggio continuo dei dati utilizzati nel training degli algoritmi di IA, per assicurare che le prestazioni del dispositivo rimangano stabili e sicure anche di fronte a nuovi dati.

Vi sono alcune norme non armonizzate che rispondono particolarmente bene alla esigenza di strutturare un'analisi del rischio dedicata. Ad esempio, una dettagliata linea guida dell'ente BSI[1] propone una decina di standard relativi all'Intelligenza artificiale nell'industria. Tra quelli citati, se ne segnalano alcuni per la loro specifica possibilità di integrazione nel settore biomedicale, in particolare con la norma ISO 14971:

- ISO/IEC 23894 Artificial Intelligence – Risk Management
- ISO/IEC TR 24028 Overview of Trustworthiness in Artificial Intelligence
- ISO/IEC TR 24027 Bias in AI Systems and AI Aided Decision Making

Da ultimo, una considerazione di sistema: la corretta progettazione e convalida di dispositivi medici che utilizzano l'intelligenza artificiale necessitano di un approccio sistemico e metodico, dove la creazione di un sistema di gestione della qualità (SGQ) efficace è fondamentale.
La conformità a standard riconosciuti ed armonizzati come ISO 13485 può essere integrata con standard relativi alle specificità della AI. Infatti la ISO 42001 offre una solida base per sviluppare e mantenere un sistema qualità integrato per dispositivi medici che non solo soddisfano le esigenze cliniche ma anche garantiscono la gestione dei rischi e delle complessità tipiche dei prodotti che contengono principi di AI.

1 BSI White Paper – Overview of standardization landscape in artificial intelligence

Sistemi di IA ad alto rischio e dispositivi medici: la governance dei dati

Articolo di Avv. Silvia Stefanelli e Avv. Eleonora Lenzi

21 Febbraio 2024

La Proposta di regolamento sull'Intelligenza Artificiale presentata dalla Commissione fornisce all'art. 3 una definizione molto ampia di "*sistema di intelligenza artificiale*", di fatto ricomprendendo qualsiasi software che, per finalità determinate dall'uomo, sia in grado di generare output in grado di influenzare gli ambienti – quindi anche le persone – con cui interagiscono.

La Proposta è stata sottoposta al vaglio de Parlamento, di varie istituzioni comunitarie ed infine del Consiglio, che in data 6 dicembre 2022 è stato chiamato a esaminare un testo di compromesso (scaricabile qui); il cennato testo di compromesso riporta una **definizione di sistema di intelligenza artificiale sostanzialmente diversa rispetto a quella della Proposta**

> "*sistema di intelligenza artificiale" (sistema di IA): un sistema progettato per funzionare con elementi di autonomia e che, sulla base di dati e input forniti da macchine e/o dall'uomo, deduce come raggiungere una determinata serie di obiettivi avvalendosi di approcci di apprendimento automatico e/o basati sulla logica e sulla conoscenza, e produce output generati dal sistema quali contenuti (sistemi di IA generativi), previsioni, raccomandazioni o decisioni, che influenzano gli ambienti con cui il sistema di IA interagisce*".

Sarà quindi dirimente comprendere quale sarà la definizione definitiva di sistema di intelligenza artificiale al fine di stabilire quando un prodotto vi rientri o meno.

RISCHIO INACCETTABILE, ALTO O BASSO

La Proposta differenzia i sistemi di IA a seconda che determinino

i) un rischio inaccettabile;
ii) un rischio alto;

iii) un rischio basso o minimo, dedicando ampio spazio ai sistemi ad alto rischio.

QUANDO UN SISTEMA DI IA È AD ALTO RISCHIO?

L'art. 6 della Proposta stabilisce che un sistema di IA è considerato ad alto rischio **se sono soddisfatte entrambe le condizioni seguenti**:

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

Il testo di compromesso del 6/12/2022 riporta un articolo 6 modificato nella lettera ma non nella sostanza dei primi due paragrafi:

> Un sistema di IA che è esso stesso un prodotto disciplinato dalla normativa di armonizzazione dell'Unione elencata nell'allegato II è considerato ad alto rischio se 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 suddetta normativa.
> Un sistema di IA destinato a essere utilizzato come componente di sicurezza di un prodotto disciplinato dalla normativa di cui al paragrafo 1 è considerato ad alto rischio se è tenuto a essere oggetto di 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 suddetta normativa. Tale disposizione si applica a prescindere dal fatto che il sistema di IA sia immesso sul mercato o messo in servizio in modo indipendente rispetto al prodotto.

Quindi, ai fini della classificazione come ad alto rischio, è richiesta la coesistenza di **due condizioni**

- il sistema di IA deve essere un componente di sicurezza di un prodotto o essere esso stesso un prodotto sottoposto alla disciplina di armonizzazione

- contemporaneamente essere un prodotto soggetto alla valutazione di conformità di organismi terzi prima di poter essere immesso sul mercato.

I DISPOSITIVI MEDICI DOTATI DI SISTEMI DI IA SONO QUINDI DA CONSIDERARSI AD ALTO RISCHIO?

L'allegato II della Proposta di IA, citato dall'art. 6 comma 1 lettera a), include entrambi i Regolamenti UE 745/2017 e 746/2017 sui dispositivi medici e sui dispositivi medici in vitro nell'elenco della normativa di armonizzazione dell'Unione.

Sulla base delle regole di Classificazione contenute nell'Allegato VII al Reg. UE 745/2017 difficilmente i dispositivi medici che utilizzino un sistema di IA potranno rientrare in una classe di rischio che escluda la valutazione di conformità dell'Organismo notificato (sulle regole di classificazione si rimanda al nostro articolo "La qualificazione e la classificazione dei software come dispositivi medici").

Conseguentemente, i dispositivi medici che utilizzino un componente di sicurezza costituito da un sistema di IA o siano un sistema di IA devono essere considerati prodotti ad alto rischio ai sensi della proposta di regolamento.

D'altra parte, l'attenzione del legislatore europeo per i sistemi di IA che potrebbero avere ripercussioni negative per la salute delle persone è confermata anche nei considerando, dove al n. 28) leggiamo "*...nel settore sanitario, in cui la posta in gioco per la vita e la salute è particolarmente elevata, è opportuno che i sistemi diagnostici e i sistemi di sostegno delle decisioni dell'uomo, sempre più sofisticati, siano affidabili e accurati*".

REQUISITI PER I SISTEMI DI IA AD ALTO RISCHIO

Se un sistema di IA è classificato ad alto rischio la proposta di regolamento prevede il rispetto di tutta una serie di requisiti illustrati nel Capo 2 del Titolo III.

In particolare, l'**art. 10 disciplina l'uso dei dati e in particolare i data set.**

GOVERNANCE DEI DATI

Come noto uno dei problemi legati all'IA è proprio quello della "*data accuracy*", intesa

come *esattezza* della "modellazione statistica del software": in sostanza la nozione di *data accuracy* nei sistemi di AI riguarda non solo i dati inseriti, ma anche la logica ed il funzionamento dello stesso software di AI nonché l'output finale di tale elaborazione (per un approfondimento si rimanda a "AI ed esattvezza dei dati: il quadro giuridico è sufficiente?".

La qualità dei data set utilizzati è fondamentale.

Per questo motivo l'art. 10 prevede che i set di dati utilizzati per l'addestramento, la convalida e la prova del sistema di IA debbano rispettare i criteri di qualità di cui ai successivi commi da 2 a 5. In particolare, i set di dati devono essere pertinenti, rappresentativi, esenti da errori, completi e possedere proprietà statistiche appropriate, tenendo conto delle caratteristiche o degli elementi particolari dello specifico contesto geografico, comportamentale o funzionale all'interno del quale il sistema di IA ad alto rischio è destinato a essere usato.

È richiesta l'adozione di pratiche di gestione dei dati, che contemplino

- scelte progettuali pertinenti;
- le modalità di raccolta dei dati;
- le operazioni di trattamento pertinenti ai fini della preparazione dei dati, quali annotazione, etichettatura, pulizia, arricchimento e aggregazione;
- la formulazione di ipotesi pertinenti, in particolare per quanto riguarda le informazioni che si presume che i dati misurino e rappresentino;
- una valutazione preliminare della disponibilità, della quantità e dell'adeguatezza dei set di dati necessari;
- un esame atto a valutare le possibili distorsioni;
- l'individuazione di eventuali lacune o carenze nei dati e il modo in cui tali lacune e carenze possono essere colmate.

Infine, il comma 5 prevede che i fornitori dei sistemi di IA possano trattare categorie particolari di dati personali,

"*fatte salve le tutele adeguate per i diritti e le libertà fondamentali delle persone fisiche, comprese le limitazioni tecniche all'utilizzo e al riutilizzo delle misure più avanzate di sicurezza e di tutela della vita privata, quali la pseudonimizzazione o la cifratura, qualora l'anonimizzazione possa incidere significativamente sulla finalità perseguita*".

Dei collegamenti con il GDPR e delle implicazioni della proposta sull'IA sul tema del trattamento dei dati abbiamo già parlato nel precedente capitolo "Intelligenza artificiale e protezione dei dati: una convivenza possibile?"

Interessante sul punto un recente intervento dell'ICO (Information Commissioner's Office) che ha recentemente pubblicato le Linee guida "How to use AI and personal data appropriately ans lawfully".

Una prima sezione del documento "*How to improve and how to handle AI and personal information*" contiene una serie di consigli e di indicazioni pratiche su come rispettare la conformità al GDPR nella progettazione e nel funzionamento dei sistemi di IA.

Nella seconda sezione "*Artificial intelligence and personal information – frequently asked questions*" ICO fornisce una risposta a nove domande frequenti nel contesto dell'IA e della protezione dei dati.

I soggetti coinvolti dall'AI ACT: uno sguardo d'insieme

Articolo di Avv. Noemi Conditi

28 Maggio 2024

Il nuovo Regolamento sull'Intelligenza Artificiale è stato definitivamente approvato dal Parlamento europeo il 21 maggio 2024 e se ne attende ora la pubblicazione ufficiale nella Gazzetta dell'Unione Europea.

Nonostante, quindi, le sue norme non siano ancora applicabili, è utile sin d'ora fare una panoramica dei soggetti coinvolti dalla normativa, per arrivare adeguatamente preparati.

Nel primo articolo di questa raccolta abbiamo già analizzato la definizione di Intelligenza Artificiale contenuta nel Regolamento e nel capitolo precedente quando un sistema di AI sia da considerarsi "ad alto rischio".

Nel presente contributo, quindi, elencheremo le varie figure individuate dal Regolamento AI, per tracciarne i confini definitori ed evidenziarne obblighi e responsabilità.

IL FORNITORE

Definizione art. 3 para. 3

"*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*"

Riprendendo la definizione classica di "fabbricante" delle normative di prodotto del New Legislative Framework, il Regolamento AI lega il ruolo di Fornitore allo svolgimento di due attività:

- **sviluppare un modello di AI o farlo sviluppare a terzi, e contestualmente**

- **immetterlo sul mercato dell'Unione con il proprio nome o marchio commerciale** (a titolo oneroso o gratuito).

Quindi, se il sistema di Intelligenza Artificiale è immesso sul mercato o messo in servizio in Europa, non rileva dove il soggetto sia stabilito o ubicato (e dunque se dentro l'Unione o in un paese terzo) (art. 2 c. 1 lett. a)).

Da segnalare poi che il Regolamento AI si applicherà anche ai Fornitori stabiliti o situati extra UE quando l'output del sistema di AI viene utilizzato nell'Unione (art. 2 c. 1 lett. c.).

Attraverso questa previsione (analoga a quella contenuta nel GDPR), il legislatore comunitario allarga l'ambito di applicazione del Regolamento anche alle aziende extra UE, cercando di ottenere quello che comunemente si chiama "effetto Bruxelles": cioè l'indiretta estensione della disciplina comunitaria anche fuori dalla spazio UE.

Il Regolamento AI prevede poi in capo ai Fornitori numerosi obblighi che devono essere rispettati quando il sistema di Intelligenza Artificiale è considerato ad **alto rischio**.

In particolare, ai sensi dell'art. 16 questi devono:

- dotarsi di un sistema di gestione della qualità conforme all'art. 17, documentato in modo sistematico e ordinato sotto forma di politiche, procedure e istruzioni scritte;
- garantire che il sistema di IA ad alto rischio sia
  - conforme ai requisiti del Regolamento IA;
  - sottoposto alla pertinente procedura di valutazione della conformità (ex art. 43) per poter essere immesso in commercio;
- redigere una dichiarazione di conformità UE (ex art. 47);
- apporre la marcatura CE sul sistema di IA ad alto rischio oppure, se ciò non è possibile, su un imballaggio/documento di accompagnamento (ex art. 48);
- indicare sul sistema di IA o su un imballaggio/documento di accompagnamento siano indicati i propri dati identificativi, di contatto e il marchio commerciale;
- rispettare gli obblighi di registrazione (ex art. 49 para. 1);

- conservare la documentazione elencata nell'art. 18, e in particolare la dichiarazione di conformità UE e la documentazione
  - tecnica sul prodotto (art. 11);
  - del sistema di gestione della qualità (art. 17);
  - sulle modifiche approvate dagli ON;
  - sulle decisioni degli ON, e quella da questi ultimi eventualmente rilasciata;
- conservare, quando sono sotto il loro controllo, i log generati automaticamente dai sistemi di IA ad alto rischio di cui all'art. 19;
- garantire che il sistema di IA ad alto rischio sia conforme ai requisiti di accessibilità ex Direttive 2016/2102 e 2019/992;
- adottare eventualmente misure correttive relative ad un sistema di IA ad alto rischio che hanno immesso sul mercato e che ritengono non essere conforme, eventualmente informandone distributori e deployers (art. 20). Inoltre, i Fornitori dovranno indagare sulle cause di eventuali rischi del sistema di IA, di cui vengano a conoscenza, e fornire le informazioni necessarie, collaborando con deployers e informandone l'autorità di vigilanza e l'ON, se del caso (art. 20);
- cooperare con le autorità competenti, ai sensi dell'art. 21.

Inoltre, si continueranno ad applicare regolarmente gli obblighi previsti dal GDPR in materia di trattamento dei dati personali per i Fornitori, nel loro ruolo di titolari del trattamento o responsabili, eventualmente ricoperto (Considerando 10).

Infine, il Fornitore dovrebbe individuare le misure di sorveglianza umana adeguate prima dell'immissione in commercio (Considerando 73), che saranno poi adottate dai Deployers.

IL DEPLOYER

Definizione art. 3 para. 4

"*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*"

I Deployers sono quindi i soggetti che utilizzano sistemi di IA e sono assoggettati ai particolari obblighi elencati nell'art. 26 quanto tali sistemi siano ad alto rischio.

In particolare, essi dovranno adottare "idonee misure tecniche e organizzative per garantire di utilizzare tali sistemi conformemente alle istruzioni per l'uso che accompagnano i sistemi".

A questo riguardo, in particolare, essi dovranno nominare una persona fisica responsabile della sorveglianza umana del sistema di IA ad alto rischio (art. 14), che sia dotata di:

- Competenza e formazione idonee;
- Autorità necessaria;
- Sostegno necessario.

IL DISTRIBUTORE

Definizione art. 3 para. 7

"*una persona fisica o giuridica nella catena di approvvigionamento, diversa dal fornitore o dall'importatore, che mette a disposizione un sistema di IA sul mercato dell'Unione*"

Il Distributore è quindi il soggetto che compra il sistema di IA e lo rivende a terzi (c.d. messa a disposizione).

Il Regolamento AI prevede una serie di obblighi per i Distributori all'art. 24.

In particolare, dovrà verificare:

- che vi sia la marcatura CE, la dichiarazione di conformità UE e le istruzioni per l'uso;
- che il Fornitore sia dotato di un sistema di gestione della qualità e abbia apposto il proprio nome/marchio commerciale sul prodotto;
- che l'eventuale Importatore abbia apposto il proprio nome/marchio commerciale sul prodotto.

****

Ci sono, infine, due figure che esistono soltanto quando il Fornitore (del sistema di IA ad alto rischio o del modello di IA per finalità generali) sia situato extra UE.

IL RAPPRESENTANTE AUTORIZZATO

Definizione art. 3 para. 5

"*una persona fisica o giuridica ubicata o stabilita nell'Unione che ha ricevuto e accettato un mandato scritto da un fornitore di un sistema di IA o di un modello di IA per finalità generali al fine, rispettivamente, di adempiere ed eseguire per suo conto gli obblighi e le procedure stabiliti dal presente regolamento*"

Il Rappresentante Autorizzato è dunque un soggetto che agisce su suolo europeo per conto del Fornitore, per i compiti indicati nel mandato.

L'art. 22 prevede che venga conferito mandato scritto, con indicati i compiti da eseguire per conto del Fornitore extra UE. Tra questi, devono obbligatoriamente rientrare:

- Verificare che il Fornitore abbia redatto la dichiarazione di conformità UE e la documentazione tecnica, e che abbia seguito l'appropriata procedura di valutazione della conformità;
- Conservare per 10 anni dopo la data di immissione in commercio
  - I dati di contatto del Fornitore;
  - Copia della dichiarazione di conformità UE;
  - Documentazione tecnica;
  - Certificato CE (se presente);
- Fornire all'autorità competente su richiesta motivata tutte le informazioni e la documentazione necessarie per dimostrare la conformità di un sistema di IA ad alto rischio al Regolamento IA;
- Cooperare con le autorità competenti su richiesta motivata in merito a qualsiasi azione intrapresa da queste ultime in relazione al sistema di IA ad alto rischio, in particolare per ridurre/attenuare possibili rischi posti dal sistema;

- Rispettare gli obblighi di registrazione ex art. 49, se previsti;
- Interloquire, anche in sostituzione del Fornitore, con le autorità competenti.

L'IMPORTATORE

Definizione art. 3 para. 6

"*una persona fisica o giuridica ubicata o stabilita nell'Unione che immette sul mercato un sistema di IA recante il nome o il marchio di una persona fisica o giuridica stabilita in un paese terzo*"

Anche per la definizione di importatore, il Regolamento IA utilizza la definizione ordinariamente fornita dalle discipline di prodotto del nuovo approccio.

L'Importatore è una figura che partecipa al ciclo di vita del sistema di IA ad alto rischio soltanto quando il Fornitore o in generale il soggetto che appone il marchio commerciale sul prodotto sia stabilita extra UE.

Questa figura si occupa di immettere in commercio il sistema nel mercato europeo acquistandolo dal Fornitore extra UE, dal momento che è il soggetto che per la prima volta fornisce il prodotto per il consumo o l'uso in Europa.

I suoi obblighi sono quelli elencati nell'art. 23, e in particolare deve apporre il proprio nome o marchio commerciale sul sistema di IA e sull'imballaggio/documentazione di accompagnamento e verificare che:

- sia stata seguita la procedura di valutazione della conformità;
- sia stata redatta la documentazione tecnica del prodotto, il prodotto stesso rechi la marcatura CE e sia accompagnato dalla dichiarazione di conformità UE e dalle istruzioni per l'uso;
- sia stato nominato il Rappresentante Autorizzato.

Inoltre, l'Importatore dovrà anche evitare di immettere in commercio il sistema di IA ad alto rischio qualora abbia un motivo sufficiente per ritenere che non sia conforme al Regolamento o sia falsificato o sia accompagnato da documentazione falsificata. Allo stesso modo, dovrà informare il Fornitore, i Rappresentanti Autorizzati e le Autorità di

vigilanza se identifica un possibile rischio posto dal prodotto.

AI E SANITÀ

I soggetti coinvolti dall'AI ACT: il professionista sanitario è un "deployer?"

Articolo di Avv. Gaspare Castelli, Avv. Noemi Conditi, Ing. Alice Ravizza

16 settembre 2024

L'entrata in vigore del **Regolamento n. 1689/2024** (c.d. "AI Act") segna un cambiamento epocale nella regolamentazione dell'IA a livello europeo.
Dettando regole specifiche per i fornitori dei sistemi di IA (i c.d. *providers*) e anche per coloro che li utilizzano (i c.d. *deployers*), l'AI Act predispone una serie di obblighi che avranno diretta ripercussione sul settore sanitario e, in particolare, sui medici e gli altri esercenti la professione sanitaria.

Esaminiamo quali possono essere le novità e le ricadute dell'AI Act su alcuni operatori del settore, focalizzando la nostra attenzione sui possibili obblighi del medico e sulle nuove modalità di gestione del rischio clinico.

DEFINIZIONE DI "DEPLOYER"

La definizione di "*deployer*" è prevista dall'art. 3, par. 3, del nuovo Regolamento che lo definisce come la:

> "*persona fisica o giuridica, autorità pubblica, agenzia o 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*".

Si tratta di una definizione particolarmente ampia, che ricomprende al suo interno una vasta platea di soggetti.

Il regolamento, infatti, si riferisce non solo all'utilizzatore persona fisica, ma anche alle entità – incluse le P.A. – che utilizzano o rendono disponibili sotto la propria autorità sistemi di IA agli utenti sul mercato, tranne nei casi di utilizzo personale non professionale.

IL RUOLO DEL DEPLOYER: BASTA IL MERO UTILIZZO?

La norma, come visto, richiede il verificarsi di due condizioni cumulative ai fini della qualificazione di un utilizzatore come deployer:

- il soggetto deve utilizzare il sistema di IA;
- tale utilizzo deve avvenire sotto la sua responsabilità (come può ricavarsi dall'inciso "*sotto la sua autorità*").

Alla luce del dato normativo, quindi, **non dovrebbe essere considerato deployer chiunque utilizzi il sistema di IA in nome e per conto di un soggetto diverso**.

È dunque necessario valutare, nel settore sanitario, chi sia il soggetto responsabile del sistema e, in particolare, se tale debba essere considerata la struttura sanitaria, il professionista sanitario che del sistema si serve o, addirittura, entrambi.

IL DEPLOYER NEL SETTORE SANITARIO

Malgrado si tratti di una questione assai recente, che potrebbe quindi prestarsi a diverse interpretazioni, la soluzione più in linea con il dato normativo pare essere quella secondo cui il **ruolo di deployer sarà assunto dalla persona fisica o giuridica che si assumerà la responsabilità della prestazione sanitaria.**

Tale potrà essere, a seconda del caso concreto, l'azienda, l'ente o il singolo professionista sanitario.

Eventuale personale o altro soggetto incaricato del funzionamento del sistema, ma che non si assume direttamente la responsabilità della prestazione erogata, dovrà invece considerarsi escluso dalla definizione di deployer, in quanto mero soggetto ausiliario.

La soluzione è supportata da due considerazioni giuridiche.

La prima è rintracciabile, come detto, nel riferimento alla locuzione "***sotto la propria autorità***" contenuta nella definizione di deployer.

Da tale inciso si evince che non è soltanto dirimente, ai fini della qualificazione del soggetto come deployer, il materiale utilizzo del sistema di IA, ma occorre verificare anche chi sia il responsabile di tale utilizzo (rectius chi ne abbia l'"autorità"), e quindi della prestazione erogata tramite l'IA.

La seconda considerazione si ricava invece dall'art. 4 dell'AI Act e, in particolare, dalla parte della disposizione che regola il ruolo del personale del deployer nei seguenti termini:

"*I fornitori e i deployer 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*".

La norma è chiara nello stabilire che il personale, o altro soggetto incaricato di far funzionare il sistema, dovrà considerarsi un mero ausiliario o, comunque, un soggetto preposto al funzionamento della macchina, al quale sarà lo stesso deployer a dover fornire adeguata formazione e informazioni sufficienti.

Con riferimento al settore sanitario, quindi, la soluzione prospettata implicherà che il ruolo di deployer sarà rivestito dalla persona fisica o giuridica che si assumerà la responsabilità giuridica della prestazione erogata attraverso il sistema.

Dunque, deployer potrà essere

- la struttura sanitaria quando il contratto di cura è concluso da quest'ultima direttamente con il paziente, a proprio nome. Per la concreta erogazione della prestazione, poi, la struttura si avvale dell'opera del medico, che concretamente utilizzerà il sistema. Quest'ultimo si qualificherà dunque come soggetto facente

parte del "personale" della struttura o, comunque, quale "*persona che si occupa del funzionamento e dell'utilizzo dei sistemi di IA*" per conto della struttura;

- mentre sarà il medico o altro esercente la professione sanitaria direttamente, laddove non soltanto eroghi in primis la prestazione, ma abbia anche concluso a nome proprio con il paziente il contratto di cura.

Si precisa infine che, ai sensi del combinato disposto dell'art. 2, par. 1, lett. b) e c), tale ruolo sarà assunto non solo dai deployers "*che hanno il loro luogo di stabilimento o sono situati all'interno dell'Unione*", ma anche da quelli "*che hanno il loro luogo di stabilimento o sono situati in un paese terzo, laddove l'output prodotto dal sistema di IA sia utilizzato nell'Unione*".

Nel precedente capitolo "I soggetti coinvolti dall'AI ACT: uno sguardo d'insieme", abbiamo già dato atto di come, ai sensi dell'art. 26 dell'A.I. Act, i deployers dei sistemi di IA ad alto rischio siano tenuti al rispetto di una (ampia) serie di obblighi.

Pertanto, la violazione di questi nuovi obblighi, pertanto, oltre a comportare l'emissione di sanzioni amministrative pecuniarie per i deployer (cfr. il successivo contributo "Il sistema sanzionatorio dell'AI Act"), potrebbe aggravare la posizione processuale dell'azienda coinvolta in processi di malpractice sanitaria in quanto la mancata attuazione di sistemi preventivi potrebbe essere utilizzata come argomento a supporto della colpa dei medici nel danno cagionato al paziente attraverso il sistema IA.

DDL Intelligenza Artificiale e sanità

Articolo di Avv. Silvia Stefanelli

16 settembre 2024

Quali sono le proposte del nostro Governo per l'intelligenza artificiale che impatteranno sulla sanità?

Il disegno di legge presentato lo scorso 23 aprile dal Governo (che ora dovrà fare tutto il suo iter in Parlamento e quindi potrà cambiare in maniera significativa) si pone infatti l'obiettivo di individuare i principi generali in grado di equilibrare il rapporto tra le opportunità offerte dalle nuove tecnologie ed i rischi legati ad un uso improprio della AI.
Tra i settori impattati certamente la sanità.
Vediamo sotto gli articoli che interesseranno tale ambito.

ART. 7 – USO DELLA AI IN SANITÀ

L'art. 7 stabilisce che

- **l'uso dei sistemi di AI non può creare discriminazioni all'accesso alle prestazioni sanitarie**

Ciò vuol dire che i sistemi di AI per gestire gli accessi non devono presentare BIAS che possano discriminare diverse tipologie di pazienti

- **il paziente deve essere informato se nell'erogazione della cura vengono usati sistemi di AI e sulla logica decisionale che viene utilizzata dal software**

questo lo diceva già anche il GDPR all'art. 14 comma 2: è certamente molto corretto ma non si può non dare atto che comunicare "la logica decisionale" è molto complesso.

- **L'AI è un supporto al medico a cui spetta sempre la decisione finale**

Tale previsione è la conseguenza del sacro principi antropocentrico che informa tutta la disciplina.

Qui si apriranno le porte ai profili di responsabilità diversi da quelli attuali e a quanto il suggerimento della AI ha inciso sulla decisione del medico

- **i dati impiegati devono verificati periodicamente e aggiornati al fine di minimizzare il rischio di errori**

Qui non si capisce bene chi sia il soggetto al quale si riferisce questo obbligo

È la struttura sanitaria che utilizza l'AI? In questo caso il risk management della struttura sanitaria dovrebbe lavorare con il fabbricante del software as medical device (SAMD) contenente il componente di AI per svolgere questa attività

Più facilmente ritengo che il compito dovrebbe essere invece direttamente in capo al fabbricante del sistema di AI il quale dovrà effettuare (presumibilmente nell'ambito della propria sorveglianza post commercializzazione – art. 83 MDR) tale attività di controllo sui dati.

Si apre dunque un nuovo scenario nel quale nel quale il fabbricante (provider secondo l'AI ACT) sarà chiamato solo a verificare la sicurezza ed il beneficio dei dispostivi medici ex MDR ma anche la "qualità" dei dati in ingresso ed in uscita.

ART. 8 – RICERCA SCIENTIFICA E SPERIMENTAZIONE PER SISTEMI DI AI

L'articolo introduce norme specifiche per il trattamento dati nella ricerca scientifica e nella sperimentazione dei sistemi di AI che sono usati in ambito sanitario.

L'articolo presenta svariate criticità.

Tralasciando il fatto che nel mondo medical device la sperimentazione si chiama "indagine clinica" (art. 62 MDR), la norma introduce una disciplina ad hoc per soggetti pubblici e privati senza scopo di lucro (dimenticando che il GDPR ha fatto venir meno questa distinzione e ripescando dunque un approccio pre-GDPR).

Più esattamente l'articolo stabilisce che quando il titolare è un soggetto pubblico o un privato senza scopo di lucro ci sono due possibilità per il trattamento

- si applica l'art. 9 lett. g) in ragione del fatto che il trattamento dei dati è considerato

di rilevante interesse pubblico; la norma non fa poi alcun accenno all'art. 2-sexies del Codice privacy, che però essendo attuazione nazionale dell'art. 9 lett. g) del GDPR si deve intendere implicitamente applicabile;

oppure

- i dati, privi degli identificativi diretti (quindi direi pseudonomizzati), possono essere trattati per le finalità di cui sopra come uso secondario, con informativa sul sito web; qui la norma non lo dice ma occorrerà effettuare un test di compatibilità (art. 6 comma 4 GDPR)

In entrambi i casi poi i soggetti che trattano tali dati dovranno

- ottenere parere favorevole del Comitato Etico
- comunicare al Garante
  - chi è il titolare del trattamento
  - come è rispettata la privacy by design by default della AI,
  - le misure di sicurezza implementate
  - la DPIA effettuata
  - l'elenco dei responsabili ex art. 28

Il Garante ha 30 gg per bloccare il trattamento: dopo tale termine si forma il silenzio assenso

Alle aziende profit resta l'art. 110 Codice privacy, che nella sua nuova formulazione a seguito delle modifiche apportate dalla Legge 56/2024 (modifiche PNRR) non vede più la consultazione preventiva davanti al Garante ex art. 36, ma il rispetto delle regole deontologiche che verranno emanate dal Garante art. art. 106 Codice Privacy.

Sembra che il Garante stia già lavorando al documento contenente le misure di garanzia da rispettare.

ART. 9 – PIATTAFORMA AI

Da ultimo l'art. 9 sulla piattaforma di AI.

Come sicuramente ricorderete la piattaforma di AI finanziata dal PNRR è stata sospesa perché mancava la base giuridica del trattamento dei dati (si veda il nostro post LinkedIN su InsideAI)

Qui l'art. 9 sembra aprire la strada stabilendo quali soluzioni di AI saranno in piattaforma e quali professionisti potranno fruire dei servizi della piattaforma.

Agenas poi (in qualità di titolare dei dati) ha il compito di redigere un provvedimento che rispetti i requisiti dell'art. 2-sexies.

AI E PROFILI DI RESPONSABILITÀ

Come cambia il risk management delle strutture sanitarie dopo l'avvento dell'IA?

Articolo di Avv. Gaspare Castelli

8 Ottobre 2024

In un nostro articolo dell'aprile 2024 "Il risk management dei dispositivi medici alla luce della legge Gelli-Bianco sulla responsabilità sanitaria" avevamo approfondito gli obblighi di risk management delle strutture sanitarie e, in particolare, l'impatto che assume nelle attività di gestione del rischio clinico l'uso dei "dispositivi medici" ex Regol. UE 2017/745 (c.d. "MDR").

Ora, a seguito dell'oramai nota entrata in vigore del Regol. UE 1689/2024 (c.d. "AI ACT"), vorremmo provare a fare un passo avanti e **immaginare come cambieranno i sistemi di risk management per le strutture sanitarie che decideranno di usare (o già usano) sistemi di intelligenza artificiale**.

La ragione per cui è opportuno cominciare a porsi questi quesiti è la seguente: se è vero che per i sistemi di intelligenza artificiale vale sempre quanto detto per la gestione dell'uso dei dispositivi medici, si deve rilevare però come i maggiori rischi presentati dall'avvento dell'intelligenza artificiale impongano necessariamente un ripensamento delle attività di gestione del rischio clinico.

Vediamo perché e quali potrebbero essere questi nuovi rischi ed obblighi in materia di gestione del rischio clinico.

L'USO "CORRETTO" DEI SISTEMI DI IA COME PARTE INTEGRANTE DEL RISK MANAGEMENT

Già nel nostro precedente articolo richiamato all'inzio abbiamo descritto le leggi che regolano in Italia il risk management finalizzato ad assicurare lo svolgimento delle funzioni di monitoraggio, prevenzione e gestione del rischio clinico.

Sempre in quella sede, sebbene con riferimento ai dispositivi medici, si era precisato come **nell'ambito del risk management vi rientrino anche le attività finalizzate alla prevenzione, al controllo e alla manutenzione delle risorse tecnologiche e, quindi, anche dei sistemi di intelligenza artificiale.**
Che il risk management debba riguardare anche i rischi derivanti dall'uso di sistemi di intelligenza artificiale si ricava da plurime disposizioni nazionali di legge, alcune delle quali già esaminate nel già menzionato articolo e che per completezza si riepilogano:

- **1 della legge 24/2017** richiede l'utilizzo appropriato delle risorse strutturali, tecnologiche e organizzative nell'ambito delle attività finalizzate alla prevenzione e gestione del rischio clinico;
- **1, commi 537, 538 e 539, legge n. 208/2015** che obbliga tutte le regioni italiane ad assicurarsi che le strutture sanitarie attivino un'adeguata funzione di monitoraggio, prevenzione e gestione del rischio clinico;
- **71 e 73 del D.lgs. 81/2008** sanciscono, presi cumulativamente, l'obbligo di utilizzare attrezzature di lavoro conformi alle disposizioni di legge e oggetto di manutenzione a tutela della sicurezza nei luoghi di lavoro;
- **"Raccomandazione ministeriale n. 9" del Ministero della Salute** che obbliga le strutture sanitarie a manutenere le apparecchiature in modo da prevenire eventi avversi;
- **"Protocollo per il monitoraggio degli eventi sentinella del luglio 2024"** del Ministero della Salute volto appunto a identificare tra gli eventi sentinella proprio la "morte o grave danno conseguente ad errato utilizzo o utilizzo anomalo dei dispositivi medici/apparecchiature elettromedicali" (il quale fa rientrare negli eventi sentinella la scelta del "dispositivo medico sbagliato" e, quindi, quando sarà, anche del sistema di intelligenza artificiale sbagliato)

I NUOVI RISCHI DERIVANTI DAI SISTEMI DI INTELLIGENZA ARTIFICIALE

Prima di esaminare i nuovi obblighi, **è inoltre necessario provare a identificare quali potrebbero essere i nuovi rischi derivanti dall'uso di queste nuove tecnologie**.

È noto come, a differenza dei dispositivi medici, i sistemi di intelligenza artificiale hanno caratteristiche e potenzialità tali da rendere più complesso il loro utilizzo. La maggiore complessità – evidentemente - è dovuta in via principale alla **impossibilità totale o parziale di ricondurre l'uso dei sistemi d'un soggetto umano specifico** (es. machine learning, autonomia operativa e sostituzione dell'attività umana).

Non esiste ovviamente un elenco dei nuovi rischi derivanti dall'intelligenza artificiale, è però molto utile consultare le "Top 10 Health Technology Hazard for 2024" redatte dall'ECRI, cioè un organismo internazionale che ha l'obiettivo di far progredire l'assistenza sanitaria, a beneficio dei pazienti di tutto il mondo. **Tra questi nuovi rischi che l'ECRI ha ritenuto farvi rientrare si deve annoverare il "rischio di decisioni di assistenza sanitaria inappropriate" derivante da una governance insufficiente dell'intelligenza artificiale**.

Invero, il monito dell'ECRI appare più che opportuno in quanto consente di comprendere con una formula laconica ma efficace il nuovo rischio derivante dai sistemi di intelligenza artificiale. In altri termini, secondo questo importante organismo di indirizzo, **l'avvento dei sistemi di IA potrebbe avere ripercussioni sull'appropriatezza dell'assistenza sanitaria**, con incremento dei danni causati dall'utilizzo di sofisticatissime tecnologie strumentali alla cura del paziente. Si pensi, ad esempio, ad una **errata installazione, aggiornamento, manutenzione e/o collaudo**, ovvero all'**inadeguatezza del sistema di IA e/o dell'ambiente di utilizzo**, o, ancora, agli **errori di risultato che potrebbe generare il machine learning o l'autonomia decisionale e/o operativa del sistema di IA**.

Al di là della complessa questione che ruota attorno alla responsabilità di questi "errori" o eventi avversi, questi nuovi rischi hanno in comune un aspetto di fondamentale importanza per la corretta gestione del rischio clinico: **sono deviazioni che possono determinare o contribuire a determinare il fallimento del piano di cura e, dunque, un "nuovo" rischio clinico che le strutture sanitarie hanno l'obbligo di prevenire**.

I NUOVI OBBLIGHI DI RISK MANAGEMENT PER I SISTEMI DI INTELLIGENZA ARTIFICIALE

Vista l'esistenza di questi nuovi rischi, le strutture sanitarie, oltre a dover svolgere le solite attività di gestione del rischio clinico dei dispositivi medici, **dovranno iniziare a svolgere ulteriori attività e controlli per far fronte ai nuovi rischi clinici** generati dall'intelligenza artificiale.

Una descrizione di questi nuovi "obblighi" si può certamente ricavare dall'AI ACT e, in particolare, dai nuovi obblighi che il regolamento ha previsto a carico della figura del c.d. "Deployer", ossia la "persona fisica o giuridica, autorità pubblica, agenzia o 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" (art. 3, p. 3, AI ACT).
Difatti, posto che – come concluso nel nostro precedente contributo "I soggetti coinvolti dall'AI ACT: il professionista sanitario è un "deployer?" – tutte le strutture sanitarie rientrano nella definizione di "deployer", **i sistemi di risk management dovranno cominciare a tener conto di questi nuovi obblighi** (cfr. nostro precedente articolo), quali, in particolare, quelli previsti dal combinato disposto dell'art. 4 (per tutti i sistemi di IA) e dell'art. 26 AI ACT (solo per i sistemi di IA "ad alto rischio").

Queste nuovi adempimenti richiederanno alle strutture sanitarie dovranno adottate misure atte:

- ad assicurare che le persone coinvolte nel funzionamento e nell'utilizzo dei sistemi abbiano un adeguato livello di competenza in materia (**c.d. alfabetizzazione degli utilizzatori**)
- **ad adottare idonee misure tecniche e organizzative a garanzia dell'utilizzo dei sistemi, conformemente alle istruzioni per l'uso fornite dai fabbricanti** (es. disporre di un inventario dei sistemi di IA; selezionare i sistemi di IA compatibile con il target degli eventuali pazienti beneficiari a seconda della destinazione d'uso; fornire supporto ai pazienti che utilizzano il sistema di IA nelle cure domiciliari; consentire di svolgere attività di scelta d'acquisto, installazione, utilizzo e funzionamento, del

sistema soltanto a personale regolarmente formato; assicurarsi di avere tutta la documentazione a corredo del sistema richiesto dalla normativa vigente e, quindi, dall'AI Act e del MDR nei frequenti casi in cui detto sistema sarà anche dispositivo medico)

- **ad affidare la "*sorveglianza umana*" a persone fisiche che dispongono della competenza, della formazione e dell'autorità necessarie** nonché del sostegno necessario (es. scelta e individuazione del "sorvegliante" adatto, nonché modalità e tempi di comunicazione e contatto con il paziente)
- **a monitorare il funzionamento del sistema di IA sulla base delle istruzioni per l'uso** e, se del caso, fornire informazioni a tale riguardo (es. consentire di svolgere attività di manutenzione, collaudo, dismissione del sistema soltanto a personale regolarmente formato; eventuale conservazione di verbali e/o documenti che attestano il corretto svolgimento delle attività);
- **ad informare senza ritardo il fornitore o il distributore e la pertinente autorità di vigilanza** del mercato, sospendendone l'uso, **qualora abbiano motivo di ritenere che l'uso del sistema di IA in conformità delle istruzioni possa presentare un rischio per la salute, la sicurezza o i diritti fondamentali delle persone** (es. Dotarsi di personale che sia in grado di comprendere quando le istruzioni per l'uso del fabbricante siano incomplete e/o errate, come ingegneri e legali esperti nella materia regolatoria; programmare ispezioni e controlli sui sistemi);
- **ad informare immediatamente** il fornitore e successivamente l'importatore o il distributore e le pertinenti autorità di vigilanza del mercato, **qualora abbiano individuato un incidente grave**.

Sebbene gli ultimi 5 punti si applichino solo ai deployer dei sistemi di IA ad alto rischio (quindi ipoteticamente non a tutte le strutture sanitarie), si ritiene che occorrerà osservarli a prescindere in quanto la loro introduzione da parte del legislatore europeo è stata determinata proprio dalla necessità di scongiurare i rischi più frequenti dell'intelligenza artificiale. A prescindere che il sistema sia o meno ad alto rischio, **il complesso degli obblighi previsti dall'AI ACT resta dunque un utile indicazione che consente alle strutture sanitarie di creare un modello che assicuri prevenzione e controllo verso i nuovi rischi generati dall'intelligenza artificiale.**

Senza considerare, peraltro, come in sanità la maggior parte dei sistemi di IA saranno ad alto rischio, dal momento che per espressa previsione di legge (cfr. art. 6, p. 1, e All. 1, AI ACT) lo saranno tutti i dispositivi medici ex MDR per i quali è richiesto l'intervento dell'organismo notificato (e quindi quasi tutti i software medicali).

Infine, non si può escludere che **se ne potranno aggiungere di ulteriori e più specifici qualora previsti dalle singole e diverse legislazioni regionali** in materia di requisiti organizzativi e strutturali per l'accreditamento e/o l'autorizzazione sanitaria.

CONSEGUENZE IN CASO DI MANCATO RISPETTO

Pur non essendo prevista una sanzione diretta per la violazione degli obblighi sopraindicata, la loro violazione, **oltre a poter comportare in futuro l'emissione di sanzioni amministrative pecuniarie** per i deployer (cfr. il nostro precedente contributo "Il sistema sanzionatorio dell'AI Act"), **potrebbe aggravare la colpa e la responsabilità dell'azienda coinvolta nei processi di malpractice sanitaria** che hanno ad oggetto prestazioni sanitarie erogate attraverso sistemi di IA.

Non si può escludere infine che la scorretta gestione dei sistemi di IA nell'ambito delle attività dei risk management possa comportare per le Regioni Competenti il venir meno di requisiti organizzativi e strutturali, **con conseguenti effetti sull'efficacia dell'accreditamento e/o dell'autorizzazione sanitaria.**

Il sistema sanzionatorio dell'AI Act

Articolo di Avv. Eleonora Lenzi

16 luglio 2024

L'AI Act prevede un sistema sanzionatorio complesso e fortemente impattante in termine economici e non solo in caso di violazione delle norme del Regolamento.

NON SOLO SANZIONI PECUNIARIE

Innanzitutto, le sanzioni potranno essere pecuniarie ma possono essere previsti anche avvertimenti o altre sanzioni non pecuniarie; il compito di definire le sanzioni non pecuniarie è rimesso agli Stati membri per cui non troviamo al momento indicazioni su quali potranno essere in concreto.

Sulla scorta di altre normative ben note, quali ad esempio il GDPR, possiamo immaginare che le sanzioni possano arrivare a prevedere la sospensione o il divieto per un sistema di AI di continuare ad operare sul mercato dell'Unione o la revoca della certificazione CE, ove prevista.

Se, quindi, le sanzioni pecuniarie sono certamente molto onerose, **non sono da sottovalutare le altre possibili sanzioni che potrebbero anche bloccare l'attività di un operatore** o di un sistema di AI all'interno del mercato dell'Unione.

LE SANZIONI PECUNIARIE

Le sanzioni pecuniarie indicate nell'AI Act si differenziano a seconda del tipo di sistema di AI e anche in relazione ai soggetti che hanno posto in essere la violazione.

Sistemi di AI vietati – art. 5	Sanzione fino a **35.000.000 €** o **7% del fatturato mondiale annuale** riferito all'anno precedente
Violazioni poste in essere dai seguenti soggetti e relativi ad obblighi specifici: • **Obblighi dei fornitori** – art. 16 • **Obblighi dei rappresentanti autorizzati** – art. 25 • **Obblighi degli importatori** – art. 26 • **Obblighi dei distributori** – art. 27 • **Obblighi dei deployer** – art. 29, par 1 fino a 6° • **Obblighi degli organismi notificati** – art. 33, 34, 34° • **Obblighi di trasparenza per i fornitori e gli utilizzatori** – art. 52	Sanzione fino a **15.000.000 €** o **3% del fatturato mondiale annuale** riferito all'anno precedente
Trasmissione di informazioni non corrette, incomplete o fuorvianti agli organismi notificati	Sanzione fino a **7.500.000 €** o **1% del fatturato mondiale annuale** riferito all'anno precedente
Fornitori di sistemi di AI con finalità generali	Sanzione fino a **15.000.000 €** o **3% del fatturato mondiale annuale** riferito all'anno precedente

Per i sistemi di AI con finalità generali la sanzione viene erogata dalla Commissione.

Non possono essere superati gli importo massimi legali, ma sono previsti massimali statici e massimali dinamici (% del fatturato mondiale).

Si applica il massimale dinamico solo se superiore a quello statico.

CRITERI PER IL CALCOLO DELLA SANZIONE

L'art. 71 fornisce alcune indicazioni sui criteri con cui l'autorità nazionale incaricata di irrogare la sanzione dovrà valutare l'importo:

- la natura, la gravità e la durata della violazione e le conseguenze tenendo in considerazione lo scopo del sistema di AI, il numero di persone coinvolte e l'entità del danno da queste subito;
- se altre autorità hanno applicato al medesimo operatore sanzioni analoghe per la medesima violazione;
- se altre autorità hanno applicato al medesimo operatore sanzioni per la violazione di altre norme dell'Unione se tali violazioni sono connesse alle violazioni rilevanti per l'AI Act;
- il fatturato, la quota di mercato, la dimensione dell'operatore;
- il grado di cooperazione con le autorità nazionali
- le misure tecniche e organizzative implementate dall'operatore
- le modalità con cui l'autorità nazionale è venuta conoscenza della violazione
- la volontarietà o meno della violazione;
- qualsiasi azione posta in essere dall'operatore per mitigare l'impatto sui soggetti danneggiati.

Infine, le autorità dovranno valutare se l'importo determinato secondo i criteri illustrati sia efficace, proporzionato, dissuasivo.

LA SCELTA DELL'AUTORITÀ CHIAMATA A VIGILARE SUL FUNZIONAMENTO DEI SISTEMI DI AI

L'AI Act richiede agli Stati membri di indicare un'autorità caratterizzata da requisiti di indipendenza e competenza specifici.

Con il DDL "Norme per lo sviluppo e adozione di tecnologie di intelligenza artificiale" (cd. DDL sull' Intelligenza Artificiale) presentato lo scorso 23 aprile, l'Italia ha individuato

a l'Agenzia per l'Italia Digitale in qualità di responsabile della promozione dell'innovazione e dello sviluppo dell'intelligenza artificiale, nonché di definire le procedure ed esercitare le funzioni e i compiti in materia di notifica, valutazione, accreditamento e monitoraggio dei soggetti incaricati di verificare la conformità dei sistemi di intelligenza artificiale;

b l'Agenzia per la cybersicurezza nazionale (ACN) è invece responsabile per la vigilanza, ivi incluse le attività ispettive e sanzionatorie, dei sistemi di intelligenza artificiale nonché per la promozione e lo sviluppo dell'intelligenza artificiale relativamente ai profili di cybersicurezza.

Restano ferme le competenze, i compiti e i poteri del Garante per la protezione dei dati personali.

AI Act e responsabilità penale: cosa cambia per provider e deployer

Articolo di Dott.ssa Laura Anna Terrizzi

9 luglio 2024

pubblicato su AgendaDigitale

L'entrata in vigore del'AI Act, primo apparato normativo al mondo a disciplinare lo sviluppo, l'immissione sul mercato e l'uso dei sistemi di intelligenza artificiale, è ormai imminente.

Nonostante, ad oggi, in tema di responsabilità il dibattito si focalizzi per lo più sui **rimedi civilistici** – che, per le loro caratteristiche, rappresentano uno strumento particolarmente efficace per la tutela dei soggetti danneggiati dai sistemi artificiali – l'avvento dell'IA è destinato ad impattare anche sul versante della responsabilità penale.

In questo articolo evidenzieremo gli scenari aperti dal Regolamento con particolare riferimento alle implicazioni penalistiche per le figure del provider e del deployer.

PROVIDER E DEPLOYER NELL'AI ACT: RUOLI E DEFINIZIONI

Nell'intento di promuovere la diffusione di un'intelligenza artificiale sicura ed affidabile, il nuovo Regolamento detta specifiche regole non solo in capo ai fornitori dei sistemi di IA (i c.d. *providers*), ma anche ai loro utilizzatori (i c.d. *deployers*).
Partiamo quindi dalle definizioni.

Introdotte dall'art. 2, le figure del fornitore e dell'utilizzatore vengono poi ulteriormente specificate dall'art. 3, che ne traccia il perimetro di operatività.

Secondo la versione finale dell'A.I. Act:

- Il provider 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";

- Il deployer è invece la "*persona fisica o giuridica, autorità pubblica, agenzia o 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*".

Il regolamento, pertanto, si riferisce **non solo all'utilizzatore persona fisica, ma anche alle entità – incluse le P.A.** – che utilizzano o rendono disponibili sotto la propria autorità sistemi di IA agli utenti sul mercato, esclusi i fornitori o gli importatori, tranne nei casi di utilizzo personale non professionale.

Fondamentali, a questo proposito, due precisazioni:

1. il Regolamento si applica anche a providers e deployers di sistemi di IA stabiliti o situati in un **paese terzo**, in tutti i casi in cui l'output prodotto dal sistema venga utilizzato all'interno del territorio dell'Unione (art. 2, par. 1, lett. c);
2. ai sensi del Considerando 84, in specifiche circostanze (ad esempio: nel caso in cui venga apportata una modifica sostanziale a un sistema di IA ad alto rischio o nel caso in cui se ne modifichi la destinazione d'uso) qualsiasi distributore, importatore, utilizzatore o altra terza parte ("deployer") viene considerato un fornitore ("provider"). In tal caso, dato che il **ruolo di fornitore (provider) verrà concretamente assunto dal deployer, in capo a quest'ultimo ricadranno, di conseguenza, gli obblighi e le responsabilità che il Regolamento attribuisce al provider.** Sono però "fatte salve le disposizioni più specifiche stabilite in alcune normative di armonizzazione dell'Unione basate sul nuovo quadro legislativo, unitamente al quale dovrebbe applicarsi il presente regolamento. Ad esempio, l'articolo 16, paragrafo 2, del regolamento (UE) 2017/745, che stabilisce che talune modifiche non dovrebbero essere considerate modifiche di un dispositivo tali da compromettere la sua conformità alle prescrizioni applicabili, dovrebbe continuare ad applicarsi ai sistemi di IA ad alto rischio che sono dispositivi medici ai sensi di tale regolamento".

OBBLIGHI E RESPONSABILITÀ DEI PROVIDER SECONDO L'AI ACT

In base alla qualificazione in termini di provider o deloyer, l'AI Act contempla una serie diversi obblighi e responsabilità.

Sotto tale profilo, ruolo fondamentale va attribuito alla **classificazione dei sistemi di IA in base al rischio legato al loro utilizzo**.
Infatti, in ossequio ad un approccio marcatamente "risk-based" – elemento caratterizzante della nuova disciplina regolatoria – **maggiore è il rischio che l'utilizzo del sistema può comportare per l'utente, più stringente risulterà la relativa regolamentazione**.

Il Regolamento accorda particolare rilevanza ai **sistemi ad alto rischio** (art.6) – nel cui novero rientrano anche i dispositivi medici, in virtù del richiamo alla normativa di armonizzazione contenuto e nell'All. I, cui l'art. 6, par. 1, lett. a, rimanda espressamente) – imponendo ai providers **specifici adempimenti**.

Tra gli obblighi previsti in capo al provider dei sistemi ad alto rischio, elencati all'art. 16, si annoverano, ad esempio:

- garantire che i loro sistemi siano conformi ai requisiti espressamente previsti dal Regolamento;
- dotarsi di un sistema di gestione della qualità;
- conservare i log generati automaticamente dai sistemi di ad alto rischio, quando sono sotto il loro controllo;
- garantire che il sistema sia sottoposto alla procedura di valutazione della conformità prima della sua immissione sul mercato o messo in servizio;
- elaborare una dichiarazione di conformità UE e apporre la marcatura CE sul sistema di IA ad alto rischio oppure, ove ciò non sia possibile, sul suo imballaggio o sui documenti di accompagnamento per indicare la conformità al regolamento;
- rispettare gli obblighi di registrazione;
- adottare le necessarie misure correttive e fornire le informazioni necessarie;
- dimostrare, su richiesta motivata di un'autorità nazionale competente, la conformità del sistema di IA ad alto rischio ai requisiti del Regolamento;

Il Considerando 73 demanda, inoltre, al provider l'**individuazione di misure di sorveglianza umana** (art. 14) adeguate, prima dell'immissione del sistema sul mercato o della sua messa in servizio.

Queste dovranno dunque "garantire, ove opportuno, che il sistema sia soggetto a vincoli operativi intrinseci che il sistema stesso non può annullare e che risponda all'operatore umano, e che le persone fisiche alle quali è stata affidata la sorveglianza umana dispongano delle competenze, della formazione e dell'autorità necessarie per svolgere tale ruolo".

I DOVERI DEI DEPLOYER SOTTO L'AI ACT

I providers di sistemi di IA sono responsabili della conformità dei loro sistemi ai criteri stabiliti dall'AI ACT soprattutto in termini di sicurezza, affidabilità e trasparenza, ma il Regolamento introduce **specifiche regole per anche per i deployer, in qualità di utilizzatori dei sistemi di IA**.

Ai sensi dell'art. 26 tra i principali obblighi cui è tenuto il deployer del sistema di IA ad alto rischio, rientrano:

- **adottare** idonee misure tecniche e organizzative a garanzia dell'utilizzo dei sistemi, conformemente alle istruzioni per l'uso fornite dai providers;
- **affidare** la sorveglianza umana a persone fisiche che dispongono della competenza, della formazione e dell'autorità necessarie nonché del sostegno necessario;
- **monitorare** il funzionamento del sistema di IA ad alto rischio sulla base delle istruzioni per l'uso e, se del caso, informare i fornitori a tale riguardo;
- **informare** senza ritardo il fornitore o il distributore e la pertinente autorità di vigilanza del mercato, sospendendone l'uso, qualora abbiano motivo di ritenere che l'uso del sistema di IA ad alto rischio in conformità delle istruzioni possa presentare un rischio per la salute, la sicurezza o i diritti fondamentali delle persone;
- **informare** immediatamente il fornitore e successivamente l'importatore o il distributore e le pertinenti autorità di vigilanza del mercato, qualora abbiano individuato un incidente grave.

L'IMPATTO IN TERMINI DI RESPONSABILITÀ PENALE

Dalla panoramica appena svolta, si evince come l'AI Act predisponga, per providers e deployers dei sistemi di IA, un articolato ventaglio di standard di comportamento e obblighi di conformità e trasparenza, la cui violazione è sanzionata con la (sola) **irrogazione di sanzioni amministrative pecuniarie** il cui ammontare, nel rispetto dei parametri fissati dal Regolamento (artt. 99/101), sarà stabilito dai singoli Stati membri.

Grande assente dal nuovo assetto normativo è invece la responsabilità penale, con riferimento alla quale – in attesa di interventi legislativi di adeguamento – dovrà farsi riferimento alla disciplina esistente.

Vediamo quale.

Obblighi e attività funzionali alla gestione del rischio

Il sistema predisposto dall' **AI Act promuove un intervento di tipo "proattivo", più che "reattivo"**, imponendo ai soggetti coinvolti (e quindi, nella gran parte dei casi, alle imprese) una serie di **obblighi e di attività funzionali alla gestione del rischio**, che danno vita ad un articolato sistema di responsabilità.

In conformità all'approccio "risk-based", il Regolamento – pur privo di efficacia diretta in materia penale – delimita infatti **un'area di rischio consentito**, individuando una serie di requisiti in presenza dei quali il sistema di IA può considerarsi conforme e che saranno, dunque, quelli cui le imprese dovranno conformarsi per produrre e immettere sul mercato.

Il ruolo della compliance

In ottica di adeguamento alle nuove disposizioni dell' AI ACT decisivo sarà, quindi, il ruolo della **compliance**.

Sotto questo profilo, sarà fondamentale operare una **preventiva valutazione dei possibili rischi legati alle attività svolte da o tramite i sistemi di IA, che andranno "contenute" nei limiti del rischio consentito**.
Predisposte le adeguate cautele preventive, la responsabilità per gli eventi dannosi/

pericolosi eventualmente verificatisi in conseguenza del loro mancato rispetto, sarebbe quindi imputabile in capo ai singoli soggetti preposti alla loro adozione, nonché all'ente.

I modelli di organizzazione e gestione (MOG) ex. D.lgs. 231/01

Un ausilio concreto, in funzione di controllo del rischio, potrebbe allora individuarsi nei **modelli di organizzazione e gestione (MOG) ex. D.lgs. 231/01** attraverso i quali identificare le figure apicali cui spetta potere decisionale e le stesse modalità di intervento per le ipotesi in cui il reato – rientrante tra i reati "presupposto" della della responsabilità amministrativa dell'ente – venga in essere in conseguenza dell'utilizzo del sistema di IA.

Come ribadito anche dalla Cassazione, in presenza di un assetto organizzativo oggettivamente negligente nell'adottare le cautele necessarie a prevenire la commissione dei reati, l'evento dannoso è imputabile all'ente per "colpa di organizzazione" e nei suoi confronti potranno quindi essere comminate le sanzioni previste dal D.Lgs. 231/2001.

Come anticipato, il Regolamento nulla stabilisce invece in ottica "reattiva": **sebbene l'impiego di sistemi di IA possa dar vita alla commissione di fatti illeciti, il legislatore europeo non prevede alcun obbligo di incriminazione.**

Tuttavia, ciò non ne esclude la possibile ricorrenza.
Sotto tale punto di vista, nell'individuazione delle fattispecie di reato configurabili, è essenziale evidenziare come il fatto illecito possa avere rilevanza sia nella **dimensione individuale**, che **collettiva**.

LE SANZIONI DEL CODICE DEL CONSUMO

Infatti, in quanto generalmente prodotti in serie, i prodotti sono immessi sul mercato in grandi quantità e l'eventuale difettosità, non conformità o alterazione del loro stato fa sorgere un pericolo per la salute, l'incolumità o addirittura per la vita nei confronti non di un individuo, ma di una **collettività indistinta**. Fondamentale importanza rivestono, quindi, le sanzioni previste dalla legislazione speciale di protezione dei consumatori, ossia dal **Codice del consumo** (D.lgs. 206/2005).

Tra queste, in ambito penalistico, particolarmente rilevante è l'**art. 112, comma 2, del Cod. cons.**, ai sensi del quale "salvo che il fatto costituisca più grave reato, il produttore che immette sul mercato prodotti pericolosi è punito con l'arresto fino ad un anno e con l'ammenda da 10.000 euro a 50.000 euro". Il provider, dunque, potrebbe essere chiamato a rispondere ai sensi della predetta disposizione, tutte le volte in cui immettesse sul mercato un prodotto non rispondente alla definizione di "prodotto sicuro".

Alla dimensione collettiva si unisce, poi, quella **individuale**, relativa al pericolo o al danno che il prodotto può arrecare al singolo utente.

Con riferimento a tale ipotesi, benché non siano previste norme ad hoc a protezione del consumatore, possono comunque configurarsi le fattispecie di reato contro la vita e l'incolumità individuale.

Tra queste, le fattispecie di **omicidio e lesioni personali** – anche (e soprattutto) **in forma colposa** – sono quelle suscettibili di trovare maggiore applicazione, perché idonee a **tutelare gli interessi personali del soggetto che subisca un danno o incorra in un pericolo per la propria vita/per la propria incolumità, in conseguenza dell'uso del prodotto che presenti difetti o alterazioni**.

SORVEGLIANZA UMANA E RESPONSABILITÀ NEL CONTESTO DELL'AI ACT

Particolarmente rilevante, sotto questo aspetto, il concetto di **human oversight**, (art. 14). La **sorveglianza umana** – che ha l'obiettivo di " prevenire o ridurre al minimo i rischi per la salute, la sicurezza o i diritti fondamentali che possono emergere quando un sistema di IA ad alto rischio è utilizzato conformemente alla sua finalità prevista o in condizioni di uso improprio ragionevolmente prevedibile" – viene infatti **realizzata non solo mediante misure individuate e integrate nel sistema di IA ad alto rischio dal fornitore (provider) prima della sua immissione sul mercato o messa in servizio, ma anche attraverso misure che, individuate dal fornitore prima dell'immissione sul mercato o della messa in servizio, siano adatte ad essere attuate dal deployer**.

In virtù del ruolo centrale riconosciuto alla sorveglianza, dal punto di vista penalistico, potrebbe dunque prospettarsi una **responsabilità del "sorvegliante umano"** – sia esso

provider o deployer – **per l'omessa adozione di idonee misure volte ad impedire gli eventi lesivi verificatisi per effetto dell' "agire" del sistema di IA.**

AI E IP LAW

Riservatezza delle conversazioni con l'IA – qual è la sorte dei dati utilizzati come prompt?

Articolo di Avv. Eleonora Lenzi, Avv. Noemi Conditi

10 Dicembre 2024

Molte delle questioni e delle criticità su cui ci si interroga legate all'utilizzo di sistemi di Intelligenza Artificiale riguardano la tutela della proprietà intellettuale, ed in particolare:

- l'**uso indiscriminato di informazioni** che possono essere coperte da diritti di proprietà intellettuale per l'addestramento dei sistemi di AI;
- la **possibilità o meno di riconoscere tutela alle opere** generate dai sistemi di AI.

Troverete l'analisi di queste questioni nei pagine seguenti: "Tutela della proprietà intellettuale e sviluppo dei sistemi di AI: due posizioni inconciliabili?" e "Chi è l'autore? L'intelligenza umana o quella artificiale?".

Il presente contributo intende ampliare proprio questo ambito di indagine, e dunque analizzare quale sia la sorte dei dati di input che fornisce l'utente nel momento in cui interagisce con l'algoritmo, e se (ed eventualmente come) questi vengano utilizzati dopo essergli stati forniti.
Analizziamo la questione.

IL PROMPTING E LA RAG (RETRIEVAL AUGMENTED GENERATION)

I modelli di IA c.d. conversazionali, come ChatGPT, Claude, Gemini, così come quelli utilizzati per la creazione di immagini o musiche come Midjourney e Suno, ci stanno abituando a dialogare con un software. L'intento di tale "conversazione" è quello di ottenere un certo output desiderato dall'utente, formulando delle domande o dando

istruzioni particolari, le quali, entrambe, sono input che contengono dati o informazioni.

Gli attuali sistemi di IA possono accogliere ed elaborare qualsiasi input, partendo dalle normali stringhe testuali fornite dall'utente, come ad esempio nel caso in cui venga data un'istruzione o posta una domanda, fino ad arrivare anche a documenti, immagini, file audio, fogli di calcolo.

Tali informazioni di input utilizzate per generare l'output dal modello di IA, sono generalmente **note come prompt** (per quanto di questo termine non esista una definizione universalmente concordata)[1].
Sono proprio i prompt, dunque, che indirizzano la risposta (output) fornita dal sistema di IA, influenzandola in modo determinante. È possibile, infatti, che una imprecisa formulazione di tale input da parte dell'utente porti l'algoritmo a fornire output altrettanto impreciso, sia in termini oggettivi (quindi contenenti ad esempio errori), che soggettivi (perché invece non rispondenti ai desiderata dell'utente).

In alcuni settori, quindi, il semplice prompting non è sufficiente e, al fine di ottenere risposte più attinenti ed evitare le c.d. allucinazioni dei modelli, è necessario ricorrere a tecniche più complesse come la **Retrieval Augmented Generation (RAG**).
Tale tecnica fornisce al modello preaddestrato altre informazioni prese da una fonte esterna ed ulteriore rispetto all'utente stesso, come ad esempio una banca dati o una raccolta di documenti. Il modello, dunque, per fornire l'output combinerà sia le informazioni fornite dall'utente che quelle reperite attraverso le altre fonti, mirando in questo modo ad essere più preciso e completo nella risposta.

Di conseguenza, un sistema di IA accede a documenti, dati e informazioni, sia reperiti in rete o nella fonte sussidiaria eventualmente utilizzata con la RAG che (soprattutto) forniti dall'utente al momento della formulazione del quesito. Analogamente, questi e altri tipi di dati sono a monte impiegati nell'allenamento del modello stesso.

Occorre pertanto chiederci **qual è la sorte di tali informazioni ed in particolare**:
Le informazioni e i dati che forniamo ai modelli di AI rimangono riservati?

1 S. Schulhoff e altri, The Prompt Report: A Systematic Survey of Prompting Techniques

È difficile dare una risposta a questa domanda in astratto valida per tutti i sistemi di IA.

Può essere utile primariamente analizzare i Termini e Condizioni di alcuni dei sistemi maggiormente utilizzati, documenti complessi che vengono dagli utenti accettati al momento della registrazione, spesso attraverso l'apposizione di semplici flag.

Prendiamo dunque ad esempio OPEN-AI (https://openai.com/it-IT/policies/eu-terms-of-use/) leggiamo che:

"*Utilizzo dei Contenuti da parte nostra. Possiamo utilizzare i Contenuti dell'utente in tutto il mondo per fornire, mantenere, sviluppare e migliorare i nostri Servizi, rispettare la legge applicabile, applicare i nostri termini e le nostre politiche e mantenere i nostri Servizi sicuri*"

oppure Anthropic (https://www.anthropic.com/legal/consumer-terms)

"*Our use of Materials. We may use Materials to provide, maintain, and improve the Services and to develop other products and services*".

È chiaro, dunque, che l'accettazione di tali termini e condizioni comporta che il sistema di IA di volta in volta prescelto potrà utilizzare i dati forniti come input dall'utente per "fornire, sviluppare e migliorare" il servizio, qualunque sia la loro natura. Risulta pertanto fondamentale la lettura di tali condizioni, per poter

- scegliere il sistema e/o il tipo di abbonamento che offre maggior tutela della riservatezza e della confidenzialità delle informazioni fornite, o in alternativa
- essere comunque consapevoli di quali tipologie di dati ed informazioni non è opportuno inserire come prompt nell'utilizzo del sistema stesso.

Infatti, bisogna prestare particolare attenzione a cosa viene fornito come input al sistema, dal momento che potrebbero rivelarsi **dati personali o informazioni riservate,** e dunque informazioni protette dalla normativa in materia di dati personali (a livello sovranazionale, Regolamento 2016/679) quando riferite a persone fisiche identificate o identificabili, dal punto di vista della proprietà industriale o intellettuale, oppure su cui più in generale si possano vantare diritti c.d. escludenti.
Potrebbero infatti contenere elementi protetti dal diritto d'autore, banche di dati,

brevetti o segreti commerciali: tutti oggetto di diritti di privativa a tutela dei titolari dei diritti stessi.

Un ulteriore aspetto deve poi essere considerato. In molti casi, e soprattutto nello svolgimento di un'attività lavorativa, l'**utilizzatore di un sistema di IA può dover trattare dati personali**, e, di conseguenza, rispettare le applicabili norme in materia in qualità di Titolare o Responsabile ai sensi del GDPR, nell'ottica del bilanciamento dei diritti e degli interessi delle parti, in primis proprio quello alla riservatezza. Tali dati possono essere ad esempio di clienti, fornitori, collaboratori, ecc.
Cosa accade quindi se tale tipologia di dati viene fornita ad un sistema di IA come input?

Anche in questo caso, occorre riferirsi ai Termini e condizioni. Ad esempio, OPEN-AI precisa che:

"*L'utente è responsabile per i Contenuti, anche per quanto riguarda la garanzia che essi non violino le leggi vigenti o i presenti Termini. L'utente dichiara e garantisce di essere in possesso di tutti i diritti, le licenze e i permessi necessari per fornire l'Input ai nostri Servizi*".

Di conseguenza, dal momento che i fornitori di sistemi di IA dichiarano di utilizzare i dati di input per fornire, mantenere, addestrare i loro servizi, il soggetto che fornisce dati personali come input al sistema potrebbe star commettendo una violazione della normativa privacy applicabile.

È presumibile, inoltre (ed in verità è spesso questo il caso) che l'utilizzatore sia anche sottoposto a vincoli contrattuali, quali la sottoscrizione di una Nomina in qualità di responsabile esterno ai sensi dell'art. 28 del GDPR o di un Non Disclosure Agreement oppure ad obblighi deontologici di riservatezza.

In questo caso, e nella circostanza sopra descritta, quindi, si starebbero anche violando tali accordi, oltre che, come detto, la normativa vigente in materia di protezione dei dati personali.

Nel particolare settore della sanità, infine, le problematiche ora rilevate risultano ulteriormente ampliate.

Possono presentarsi, infatti, i seguenti scenari.
Da un lato, è possibile che il professionista sanitario utilizzi un sistema come quelli in commento come aiuto alla diagnosi, sostegno per attività burocratiche nell'ordinaria pratica clinica oppure per la gestione di indagini cliniche.
Dall'altro, è comunque possibile ipotizzare situazioni in cui fabbricanti di dispositivi medici intendano integrare tali sistemi all'interno di un dispositivo medico-software (SAMD) come elemento cardine per raggiungere la sua destinazione d'uso medicale.

Lasciando per altra sede le enormi problematiche giuridiche (in termini regolatori, di responsabilità dell'utilizzatore e del fabbricante, nonché relativamente al trattamento dei dati personali) sollevate da quest'ultima ipotesi, anche il mero utilizzo di tali sistemi da parte del professionista sanitario per lo svolgimento dell'ordinaria pratica clinica solleva diversi interrogativi.

In particolare, occorrerà valutare attentamente che nell'individuazione del prompt da fornire al sistema non si includano dati personali dei pazienti (e dunque dati che in qualche modo permettano di riconoscere le persone fisiche che egli ha in cura), pena la violazione non soltanto della normativa in materia di privacy, ma anche quella che impone il rispetto del segreto professionale (o medico).

Ancora, non potranno essere inseriti dati in qualche modo protetti a favore della struttura di cura presso cui il medico svolge la propria attività, relativi ad esempio ad attività di ricerca scientifica.

COME COMPORTARSI?

Il primo passo da fare sarà sicuramente quello di **valutare attentamente i Termini e condizioni d'uso** dei sistemi di IA e selezionare il sistema che dia le maggiori garanzie in merito all'utilizzazione e diffusione di dati, anche optando per abbonamenti a pagamento ove più idonei.

Nell'ambito lavorativo, la scelta di cui sopra dovrebbe essere fatta dal datore di lavoro o da suoi incaricati con **istruzioni precise ai dipendenti e collaboratori** di quali sistemi possono essere utilizzati per lo svolgimento delle attività lavorative.

Le medesime istruzioni dovrebbero contenere indicazioni anche in merito ai documenti, informazioni, file etc che possono essere utilizzati in fase di input e gli accorgimenti da porre in essere.

Certamente si tratta di valutazioni non semplici ma da cui i soggetti che utilizzano un sistema di IA difficilmente potranno esimersi se non vorranno esporsi al rischio di infrangere obblighi contrattuali o altri obblighi di riservatezza.

Un aiuto potrebbe arrivare dall'attuazione dell'art. 53 dell'AI ACT che prevede

1. L'adozione di politiche aziendali, codici di condotta che prevedano la tutela della proprietà intellettuale e, in particolare, garantiscano l'individuazione e il rispetto delle riserve espresse dai titolari dei diritti in modo appropriato, ad esempio attraverso strumenti che consentano lettura automatizzata in caso di contenuti resi pubblicamente disponibili online (art. 3 comma 4 Dir. UE 2019/790).
2. La redazione e pubblicazione di un documento di sintesi dei contenuti utilizzati per l'addestramento degli algoritmi.

Chi è l'autore? L'intelligenza umana o quella artificiale?

Articolo di Avv. Eleonora Lenzi

15 Ottobre 2024

In tema di rapporti tra AI e proprietà intellettuale, fondamentale domanda da porsi è se le opere generate tramite un sistema di AI possano considerarsi originali e autonome e, in tal caso, a chi spettino i diritti di proprietà intellettuale.

L'ESSERE UMANO AL CENTRO

La legge italiana sul diritto d'autore (Legge 633/1941 - LDA) prevede all'art. 1 che:

"*Sono protette ai sensi di questa legge le opere dell'ingegno di carattere creativo che appartengono alla letteratura, alla musica, alle arti figurative, all'architettura, al teatro ed alla cinematografia, qualunque ne sia il modo o la forma di espressione*".

Nell'attuale formulazione della norma non vi è quindi un riferimento al fatto che l'autore debba essere umano, anche se fino ad ora si è di fatto dato per scontato che la presenza dell'essere umano sia richiamata e data per implicita nel concetto di creatività. Non ci può essere creatività senza l'uomo.

La necessità della presenza dell'essere umano viene richiamata tanto nelle decisioni dei giudizi nazionali che in quelle della Corte di giustizia europea, che in più occasioni fa riferimento alla "creazione intellettuale dell'autore che ne riflette la personalità e si manifesta attraverso scelte libere e creative di quest'ultimo nella realizzazione dell'opera".

Anche nel diritto anglosassone l'interpretazione delle Corti e del Copyright office del concetto di authorship è sempre legata indissolubilmente all'uomo come persona fisica.

D'altra parte il DDL italiano sull'intelligenza artificiale propone all'art. 24 una modifica all'art. 1 della Legge sul diritto d'autore, il cui nuovo testo dovrebbe essere riformato come segue

"Sono protette ai sensi di questa legge le opere dell'ingegno umano di carattere creativo che appartengono alla letteratura, alla musica, alle arti figurative, all'architettura, al teatro ed alla cinematografia, qualunque ne sia il modo o la forma di espressione anche laddove create con l'ausilio di strumenti di intelligenza artificiale, purché il contributo umano sia creativo, rilevante e dimostrabile".

Anche in tema di brevetti, il Patent and Trade Mark Office degli Stati Uniti ha emanato la "Inventorship Guidance for AI-Assisted Inventions", in vigore dal 13 febbraio 2024, in cui viene stabilito che un'invenzione realizzata con l'assistenza di un sistema di AI non è, in quanto tale, non brevettabile ma è necessaria un'analisi approfondita dell'apporto umano, in quanto il brevetto può essere concesso solo a quelle invenzioni il cui apporto umano è significativo.

Ad oggi, quindi, possiamo ancora dire che la **tutela della proprietà intellettuale viene riconosciuta esclusivamente all'autore umano**, sia che si tratti di diritto d'autore sia che si tratti di proprietà industriale; quindi, è sempre necessario che ci sia un apporto umano significante.

L'APPORTO IN TERMINI DI CREATIVITÀ

L'altro elemento rievante riguarda l'effettività del contributo umano, che deve essere creativo, rilevante e dimostrabile rispetto all'apporto dato dalla macchina nella creazione dell'opera dell'ingegno.

Affinché sia riconosciuta la paternità di un'opera al suo autore umano, quest'ultimo deve poter dimostrare che il suo apporto creativo è stato rilevante rispetto all'apporto dato dalla macchina.

Si pone quindi il tema della prova.

L'autore dovrà, in primo luogo, essere in grado di dare prova delle istruzioni (prompt) fornite alla macchina nella fase di creazione dell'opera e quindi organizzare il proprio lavoro di conseguenza. La valutazione dei prompt porterà poi a definire se l'apporto umano è stato determinante in termini di creatività.

L'IMPORTANZA DEI PROMPT

Il tema dei prompt non si pone, peraltro, solo in relazione alla prova dell'apporto determinante dell'essere umano rispetto all'elaborazione della macchina.

Altra questione, diversa anche se strettamente legata, riguarda l'anteriorità di un'opera rispetto ad un'altra simile sempre creata dalla macchina.

È infatti possibile che un sistema di intelligenza artificiale generi due opere del tutto simili dopo avere ricevuto istruzioni da due autori diversi. Tanto è vero che i maggiori fornitori di sistemi di intelligenza artificiale per fini generali prevedono tale possibilità nelle condizioni generali di contratto che l'utilizzatore accetta, scrivendo chiaramente che, in considerazione delle modalità di addestramento dell'algoritmo, non è possibile escludere che vengano prodotti dalla macchina più risultati, out put, del tutto simili.

Anche in questo caso si pone un tema di prova: l'autore dovrà essere in grado di dimostrare quali istruzioni ha fornito alla macchina e anche di avere ottenuto quel determinato out put per primo.

L'IMPORTANZA DELLE CONDIZIONI GENERALI DI CONTRATTO DEI FORNITORI

Rimane, poi, sempre di fondamentale importanza conoscere le condizioni generali di contratto relative a qualunque sistema di AI si abbia intenzione di utilizzare, con particolare attenzione ai sistemi di AI per finalità generali.

In conclusione, il diritto di proprietà intellettuale viene per ora riconosciuto solo ad un essere umano ma solo se questo è in grado di provare che il suo apporto, le istruzioni date alla macchina, sono state determinanti in termini di creatività per l'elaborazione dell'opera.

Tutela della proprietà intellettuale e sviluppo dei sistemi di AI: due posizioni inconciliabili?

Articolo di Avv. Eleonora Lenzi

23 Settembre 2024

Sono due gli aspetti critici legati alla tutela della proprietà intellettuale sollevati dallo sviluppo e dall'uso dei sistemi di Intelligenza Artificiale.

Una prima questione è relativa all'**uso indiscriminato di informazioni anche coperte da diritti di proprietà intellettuale nell'addestramento dei sistemi di AI e riguarda fondamentalmente i fornitori**.
Per la definzione di fornitore si rimanda all'Art. 3 AI ACT:

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.

Il secondo tema concerne invece il **riconoscimento o meno della tutela delle opere generate dai sistemi di AI e coinvolge i deployer**.
Art. 3 AI ACT:

"*deployer*": *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 questo contributo ci occuperemo del primo aspetto.

LA TUTELA DELLA PROPRIETÀ INTELLETTUALE DEI DATI DI ADDESTRAMENTO

Per l'addestramento di algoritmi di intelligenza artificiale generativa, in particolare per i sistemi a finalità generali, gli sviluppatori ricorrono molto spesso ad attività di **web scraping.**

Informazioni e dati possono essere raccolti in maniera sistematica attraverso programmi (*web robot*) che operano in maniera automatizzata simulando la navigazione umana, a condizione che le risorse visitate da questi ultimi risultino accessibili al pubblico indistinto e non sottoposte a controlli di accesso. Uno studio (Imperva – Bad bot report) ha rivelato che, nell'anno 2023, il 49,6% di tutto il traffico Internet è stato generato dai bot con un aumento pari al 2,1% rispetto all'anno precedente, aumento che è stato parzialmente ricondotto alla diffusione di sistemi di intelligenza artificiale e, in particolare, dei modelli linguistici di grandi dimensioni (di seguito anche "LLM" - *Large Language Model*) sottesi all'intelligenza artificiale generativa (Provvedimento Garante per la tutela dei dati personali 20 maggio 2024 – nota informativa sullo web scraping).

In questa indiscriminata attività di raccolta di dati finiscono nella "rete", oltre ai dati personali, anche molte informazioni originariamente tutelate da diritti di proprietà intellettuale.

Da una parte abbiamo, quindi, i fornitori dei sistemi di intelligenza artificiale che hanno un interesse ad accedere in modo illimitato e senza costi a quell'enorme massa di dati presenti nel web; dall'altra parte i titolari dei diritti di proprietà intellettuale vorrebbero veder tutelati i loro diritti.

Il legislatore deve trovare una strada per contemperare le due esigenze, avendo ben presente che una normativa che, in questo momento storico, ostacoli o renda troppo oneroso lo sviluppo dell'intelligenza artificiale potrebbe tradursi in un ostacolo allo sviluppo competitivo.

L'Unione europea si è mossa su più fronti, mettendo in campo da anni una propria strategia di digitalizzazione EU Digital Strategy - EU4Digital (eufordigital.eu) e sono numerosi gli interventi normativi che riguardano i dati (personali e non).

Il recente Regolamento UE 1689/2024 (AI ACT) prevede all'art. 53 comma 1 che

"*I fornitori di modelli di AI per finalità generali:*
c) attuano una politica volta ad adempiere al diritto dell'Unione in materia di diritto d'autore e diritti ad esso collegati e, in particolare, a individuare e rispettare, anche attraverso

tecnologie all'avanguardia, una riserva di diritti espressa a norma dell'articolo 4, paragrafo 3, della direttiva (UE) 2019/790;
d) redigono e mettono a disposizione del pubblico una sintesi sufficientemente dettagliata dei contenuti utilizzati per l'addestramento del modello di IA per finalità generali, secondo un modello fornito dall'ufficio per l'IA".

L'AI ACT non si pone come scopo principale quello di disciplinare gli aspetti legati alla tutela del diritto d'autore, che infatti tratta solo marginalmente; nel quadro legislativo europeo però la Direttiva 2019/970 (Digital single market) all'art. 4 permette il text and data mining da opere o materiali a cui si abbia legalmente accesso almeno che l'autore non abbia espresso una riserva contro tali usi (c.d. op out).

La DSM viene esplicitamente richiamata dall'art. 53 dell'AI ACT.

L'art. 53 AI ACT impone, dunque, ai fornitori due adempimenti specifici in relazione al tema della tutela dei diritti IP.

1. L'adozione di politiche aziendali, codici di condotta che prevedano la tutela della proprietà intellettuale e, in particolare, garantiscano l'individuazione e il rispetto delle riserve espresse dai titolari dei diritti in modo appropriato, ad esempio attraverso strumenti che consentano lettura automatizzata in caso di contenuti resi pubblicamente disponibili online (art. 3 comma 4 Dir. UE 2019/790).
2. La redazione e pubblicazione di un documento di sintesi dei contenuti utilizzati per l'addestramento degli algoritmi. L'art. 53 prevede che un modello di documento sia reso disponibile dall'ufficio per l'IA e stabilisce che la sintesi debba essere sufficientemente dettagliata; al momento non è possibile dire quale sarà il livello di dettaglio richiesto, è prevedibile che non saranno accettati documenti totalmente generici tali da violare sostanzialmente l'obbligo di trasparenza previsto dal Regolamento.
   Probabilmente il modello che l'ufficio per l'IA dovrà predisporre fornirà un'utile guida non solo per la redazione del documento di sintesi ma anche per la predisposizione delle policy interne.

L'art. 53 AI ACT richiede, d'altro canto, anche ai titolari dei diritti di IP un adempimento

ovvero quello di segnalare in maniera appropriata se un contenuto è liberamente disponibile o meno (opt out).

Per quanto riguarda il Disegno di Legge sull'intelligenza artificiale italiano, l'attuale testo prevede all'art. 24 l'inserimento nella Legge 633/1941 dell'art. 70 septies:

«*La riproduzione e l'estrazione di opere o altri materiali attraverso modelli e sistemi di intelligenza artificiale anche generativa, sono consentite in conformità con gli articoli 70-ter e 70-quater*.»

ovvero

- da parte di istituti di ricerca o di istituti a tutela del patrimonio culturale per scopi di ricerca scientifica
- quando la riproduzione o estrazione non è stata espressamente riservata da parte dei titolari del diritto d'autore.

La strategia europea sui dati mette quindi a disposizione svariate fonti di dati per i fornitori di sistemi di AI e non è impedita neppure la possibilità di utilizzare i dati presenti nel web, nel rispetto delle prescrizioni (poche) dell'AI ACT.

L'Italia verso una propria strategia sull'intelligenza artificiale

Articolo di Avv. Eleonora Lenzi

7 Maggio 2024

Lo scorso 23 aprile il Governo ha approvato un disegno di legge sull'intelligenza artificiale, con l'intento di individuare criteri regolatori in grado di equilibrare il rapporto tra le opportunità offerte dalle nuove tecnologie con i rischi legati ad un uso improprio.

Il DDL contiene una definizione di "sistema di intelligenza artificiale"

"*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*".

La definizione di IA è identica a quella contenuta nell'art. 3 lett. 1 dell'AI ACT, esaminata nel dettaglio nel primo contributo di questo white paper "AI: la definizione giuridica".

Il DDL indica, poi, una serie di principi generali che i sistemi di intelligenza artificiale devono rispettare in un'ottica che rimane antropocentrica e fornisce al Capo II alcune disposizioni di settore, in particolare in ambito

- di tutela del diritto d'autore
- sanitario
- giuslavoristico

Ci occuperemo in questo articolo dei profili legati alla proprietà intellettuale, trovete nel white paper gli approfondiementi legati all'AI e Sanità e AI e Diritto del Lavoro

GLI ASPETTI LEGATI AL DIRITTO D'AUTORE

Il DDL affronta negli artt. 23 e 24 le diverse problematiche legate al diritto d'autore

Tutela delle opere utilizzate per l'addestramento

L'art. 24 lettera b) affronta la dibattuta questione della tutela del diritto d'autore dei contenuti utilizzati per l'addestramento dei sistemi di IA.

Il DDL prevede che la riproduzione e l'estrazione di opere o altri materiali sono consentiti in conformità agli artt. 70 ter e 70 quater della Legge sul diritto d'autore (R.D. 633/1941), introdotti dal D.Lgs. 177/2021 di recepimento della Direttiva UE 2019/790 (Direttiva Copyright), ovvero

- da parte di istituti di ricerca o di istituti a tutela del patrimonio culturale per scopi di ricerca scientifica
- quando la riproduzione o estrazione non è stata espressamente riservata da parte dei titolari del diritto d'autore.

In sostanza quindi, i contenuti coperti da diritto d'autore possono essere utilizzati per l'addestramento dei sistemi di IA generali almeno che l'autore abbia espresso una volontà contraria (opt out).

La previsione del DDL è in sostanza allineata con l'AI ACT, che nell'ultimo testo a disposizione stabilisce che i fornitori di modelli di AI per finalità generali devono conformarsi alla normativa europea in materia di diritto d'autore e in particolare all'art. 4 comma 3 della Direttiva Copyright.

Tutela delle opere realizzate dai sistemi di IA

L'art. 24 lettera a) va invece nella direzione di riconoscere la tutela del diritto d'autore solo alle opere dell'ingegno create dall'uomo o con un forte apporto dell'uomo. La norma infatti prevede l'aggiunta dell'aggettivo "umano" dopo la locuzione "opere dell'ingegno" di cui all'art. 1 della Legge sul diritto d'autore, aprendo però alla possibilità che l'opera dell'ingegno umano sia creata con l'ausilio dell'intelligenza artificiale purché il contributo umano sia creativo, rilevante e dimostrabile.

Tutela degli utenti che usufruiscono di contenuti generati dall'IA

L'art. 23 del DDL prevede l'apposizione di un elemento o segno identificativo che permetta agli utenti che usufruiscono di contenuti testuali, video, fotografici etc di

essere informati del fatto che tali contenuti sono stati creati o modificati con l'utilizzo di sistemi di IA.

È prevista l'adozione di un codice di regolamentazione.

Lo scopo è quello di salvaguardare gli utenti dal rischio di contenuti fake, sempre più difficili da distinguere rispetto a quelli reali e quindi dalla disinformazione.

In tema di diritto d'autore, il DDL si pone in linea con il diritto comunitario e le previsioni contenute nell'AI ACT, norma che, trattandosi di un regolamento, sarà direttamente applicabile nell'ordinamento nazionale.

Lo sviluppo dei sistemi di intelligenza artificiale non può prescindere dalla tutela dei dataset

Articolo di Avv. Eleonora Lenzi

8 Giugno 2024

Il tema dell'intelligenza artificiale è ormai all'ordine del giorno, molte sono le perplessità e le preoccupazioni sollevate dall'utilizzo di sistema di AI ma anche le opportunità che si aprono e le possibili applicazioni tecniche.

L'Unione europea è in prima linea con lo scopo di disciplinare in modo organico e unitario per l'intero territorio comunitario l'implementazione e l'utilizzo dei sistemi di AI, tanto che la proposta di Regolamento sull'intelligenza artificiale (c.d. IA Act o AIA) risale ormai all'aprile 2021.

La stessa proposta di Regolamento è oggetto di discussione e di emendamenti da parte delle istituzioni comunitarie.

Prima fra tutti è ancora controversa la definizione stessa di intelligenza artificiale, la quale ha già visto negli ultimi mesi, a causa delle numerose proposte ed emendamenti, diverse modifiche, non trovando tuttora una descrizione pacifica.

In ogni caso, dal punto di vista concreto, è possibile identificare un sistema di AI come **un insieme di creazioni tecnologiche complesse costituite alla base da uno o più algoritmi espressi da un "programma per elaboratore elettronico", ovvero un software**.

QUALI LEGAMI CON LA PROPRIETÀ INTELLETTUALE?

In tale contesto, uno dei problemi sollevati dai sistemi di AI concerne il rapporto con la proprietà intellettuale, in particolare in relazione alla possibile violazione di diritti di privativa nella creazione e nell'uso dei data set per l'addestramento e la validazione dell'algoritmo, tanto da diventare oggetto di attenzione politica a livello mondiale, come si evince da un estratto della dichiarazione finale del Summit del G7 di Hiroshima:

"Dato che le tecnologie di intelligenza artificiale generativa sono sempre più importanti

in tutti i paesi e settori, riconosciamo la necessità di fare un bilancio a breve termine delle opportunità e sfide di queste tecnologie e continuare a promuovere la sicurezza e la fiducia sullo sviluppo di tali tecnologie. Abbiamo in programma di convocare future discussioni del G7 sull'IA generativa che potrebbe includere argomenti come la governance, come salvaguardare i diritti di proprietà intellettuale compreso il diritto d'autore, promuovere la trasparenza, affrontare la disinformazione, anche straniera manipolazione delle informazioni e come utilizzare responsabilmente queste tecnologie".

In ambito comunitario, la tematica è stata presa in esame e inserita nel recente emendamento dell'AI Act pubblicato lo scorso 16 maggio, che prevede l'obbligo per i fornitori di sistemi di AI ad alto rischio di rivelare le opere utilizzate per il training dell'intelligenza artificiale.

In particolare, secondo il nuovo art. 16 lett. ac) dell'AIA, i fornitori di sistemi di IA ad alto rischio devono:

"*fornire le specifiche dei dati di input o qualsiasi altra informazione pertinente in termini di dataset utilizzati, comprese le loro limitazioni e ipotesi, tenendo in considerazione lo scopo previsto e gli usi impropri prevedibili e ragionevolmente prevedibili di tale sistema di IA*".

PER COMPRENDERE MEGLIO

Al fine di comprendere meglio i possibili obblighi e rischi in capo al fornitore conseguenti alla futura approvazione dell'IA Act poniamo un caso pratico, ipotizzando che l'obiettivo sia lo sviluppo di un dispositivo medico che utilizzi un sistema di AI.

Per l'addestramento dell'algoritmo, è necessaria la raccolta di dati grezzi presenti nei database messi a disposizione per esempio da ospedali, università o istituti di ricerca, i quali verranno estratti, anonimizzati e rielaborati da parte dei programmatori.

Successivamente, i dati dovranno essere selezionati, individuando la categoria di pazienti di interesse, i valori di riferimento e le relative diagnosi per lo sviluppo dell'algoritmo alla base del software.

Dall'elaborazione dei dati grezzi verrà poi costituita una banca dati utilizzata per il training dell'algoritmo predittivo e per lo svolgimento di test esterni, per poi giungere alla realizzazione del software che dovrà ottenere la certificazione MDR come "Software as a Medical Device" (SaMD).

I POSSIBILI NODI PROBLEMATICI

Alla luce dei passaggi tecnici ipotizzati sopra, il fornitore dovrà interrogarsi alla luce delle nuove indicazioni provenienti dall'AIA:

- sui regimi di tutela dei dataset utilizzato per il training dell'algoritmo
- sulla possibilità di utilizzare ed includere nella documentazione tecnica i dati utilizzati per l'addestramento e la validazione dell'algoritmo.

Per quanto riguarda il primo aspetto, è necessario richiamare brevemente quanto evidenziato nel nostro precedente contributo "La tutela giuridica delle banche dati: tra diritto d'autore e diritto sui generis".

Le banche dati, secondo la Direttiva 96/9/CE recepita poi Italia con il D.lgs. 6 maggio 1999, n. 169 possono trovare tutela nel:

1. **diritto d'autore**: se la banca dati è una creazione intellettuale originale, e conferirà all'autore il diritto esclusivo di riprodurre, adattare, distribuire la banca dati o variazioni della stessa. Il diritto d'autore tutelerà poi esclusivamente la struttura della banca dati e non si estenderà ai suoi contenuti, lasciando impregiudicati eventuali diritti esistenti su di essi. La tutela avrà inizio dal momento della creazione dell'opera fino a 70 anni dalla morte dell'autore.
2. **diritto sui generis**: esercitabile solo se la banca dati è frutto di un investimento ingente. La tutela concessa riguarderà l'investimento economico sostenuto, non la creatività dell'opera. La durata del diritto del costitutore della banca dati sarà poi di 15 anni.

Inoltre, è importante evidenziare che il diritto d'autore e il diritto sui generis possono in ogni caso applicarsi cumulativamente se le condizioni di protezione di ciascun diritto sono soddisfatte.

In riferimento alla seconda questione, sarà necessario verificare caso per caso l'origine dei dati utilizzati per il training dell'algoritmo, distinguendo a seconda che si tratti di dati personali o anonimizzati, ovvero di dati conferiti mediante licenza di utilizzo oppure open data.

A seconda dei casi, sarà doveroso provvedere mediante apposite regolamentazioni contrattuali allo scopo di rispondere all'obbligo di "*fornire le specifiche dei dati di input o qualsiasi altra informazione pertinente in termini di dataset utilizzati*" individuate dall'art. 16 dell'IA Act.

Successivamente sarà opportuno valutare quale regime di tutela può essere riconosciuto al dataset creato dal fornitore, in modo da proteggere adeguatamente quello che a tutti gli effetti può essere considerato un asset aziendale.

CONSIDERAZIONI CONCLUSIVE

Sebbene ad oggi l'IA Act si configuri solo come una proposta di Regolamento, in fase di modifica e approvazione, è già essenziale definire gli aspetti sulla raccolta e utilizzo dei dati presenti nei dataset posti alla base del sistema di intelligenza artificiale che il fornitore sta progettando o sviluppando.

La corretta disciplina delle banche dati sin dalla loro origine, consentirà infatti maggiori tutele all'autore e la riduzione del rischio di contenzioso sulla titolarità di tali dati.

AI E DIRITTO DEL LAVORO

Profilazione, controllo e decisioni automatizzate: i rischi AI in tema di lavoro

Articolo di Dott. Guido Lepore

4 Novembre 2024

Fra i settori maggiormente influenzati dalla introduzione e diffusione dei sistemi di intelligenza artificiale vi è sicuramente il **diritto e l'organizzazione del lavoro**.

L'utilizzo delle tecnologie AI in questo settore, infatti, può spaziare dalla **fase preassuntiva** (come la ricerca e la selezione del personale) sino alla **gestione del rapporto di lavoro** (come il mutamento delle mansioni, promozioni, trasferimenti, monitoraggio della performance etc.) e alla sua **cessazione** (ovvero nella scelta o meno di procedere con il licenziamento).

L'Intelligenza Artificiale può poi rappresentare anche un vero e proprio **strumento di lavoro**, implementando le funzionalità dei **dispositivi di salute e sicurezza sul lavoro** oppure affiancando gli stessi lavoratori nell'**esecuzione delle loro mansioni**.

Ma se da un lato le potenzialità di questo strumento sono vastissime, dall'altro è necessario prendere coscienza anche dei rischi che il suo utilizzo comporta.

Fra i pericoli concreti, infatti, vi sono sicuramente quello di un **controllo invasivo dei lavoratori**, di una loro **profilazione sistematica** e di **decisione automatiche** in grado di condurre a **trattamenti discriminatori.**

Osserviamoli nel dettaglio.

INTELLIGENZA ARTIFICIALE E LAVORO

Con l'avvento delle tecnologie AI nei luoghi di lavoro, il concetto giuslavoristico di "**controllo a distanza**" si è significativamente ampliato.

I sistemi di AI possono infatti **monitorare in modo continuo e dettagliato** le performance dei lavoratori, così come analizzare la loro produttività e le loro emozioni, valutare eventuali comportamenti anomali o persino prevedere errori o inefficienze. Tutto ciò determina sicuramente un **ampliamento del potere di controllo del datore di lavoro sui propri dipendenti** intollerabile in un' ottica giuslavoristica di protezione del lavoratore di fronte alle ingerenze datoriali.

Il tema dei controlli indiretti sul luogo di lavoro, infatti, è stato oggetto di regolamentazione sin dall'art. 4 dello Statuto dei Lavoratori del 1970, (come oggi modificato dal Job Act 2015): tale norma consente l'adozione di sistemi da cui deriva un controllo indiretto dei lavoratori (per esempio, le telecamere) in presenza di due situazioni:

- la sussistenza di specifiche causali, ovvero esigenze organizzative e produttive, sicurezza del lavoro e tutela del patrimonio aziendale, e
- la preventiva stipula di un accordo sindacale o all'ottenimento di una autorizzazione dell'ITL (comma 1).

Infine, l'utilizzo dei dati personali dei lavoratori raccolti per il tramite di detti strumenti è subordinato alla consegna ai dipendenti di una **apposita informativa ex art. 13 GDPR** (comma 3).

Nonostante il sofisticato apparato difensivo dello Statuto dei Lavoratori (ancora oggi attuale) la norma sopra citata non trova applicazione nel caso di **strumenti utilizzati per erogare la prestazione lavorativa**: in questo senso sussiste un rischio di controllo del lavoratore ove la tecnologia AI sia applicata in fase di esecuzione della mansione lavorativa.

PROFILAZIONE DEI LAVORATORI E DECISIONI AUTOMATIZZATE

Una ulteriore criticità derivante dall'utilizzo di sistemi di AI sul luogo di lavoro è quello di una **profilazione sistematica dei dipendenti**.

Ai sensi dell'art. 4 lett 4) GDPR per profilazione si intende la raccolta e il trattamento di dati personali di un individuo o gruppo di individui per analizzarne le caratteristiche, al fine di suddividerli in categorie, gruppi o **poterne fare delle valutazioni o delle previsioni.**

La profilazione (o anche rating) dei lavoratori trova larga applicazione già nella fase di **selezione preassuntiva**: numerose aziende, infatti, ricorrono a sistemi di AI in grado di analizzare i curricula dei candidati e metterli a confronto, con lo scopo di selezionare il candidato fra tutti più idoneo sulla base dei parametri utilizzati dall'algoritmo.

Nell'ambito del rapporto di lavoro, questa pratica viene utilizzata come metodo di **classificazione del personale**, in forza del quale successivamente **adottare decisioni rilevanti** inerenti al rapporto di lavoro (quale eventuali avanzamenti di carriera, accesso ad opportunità formative e/o lavorative, sino al trasferimento dei dipendenti e addirittura alla selezione del personale in esubero da licenziare).

La profilazione, soprattutto se utilizzata tramite sistemi di AI con il fine di adottare decisioni automatizzate, cela un altissimo rischio di porre in essere **condotte discriminatorie e/o situazioni di disparità di trattamento** (definite anche bias algoritmico).

E seppur l'art. 22 del GDPR preveda espressamente un diritto di non essere sottoposti a una decisione basata unicamente sul trattamento automatizzato e di ottenere un intervento umano, nel caso dell' utilizzo di sistemi di AI spesso tale diritto è difficile da garantire stante l'**opacità dell'algoritmo,** che rende estremamente arduo conoscere e "spiegare" il processo decisionale adottato.

Infine il ricorso a **strumenti di AI finalizzate ad adottare decisioni automatizzate** può trovare spazio nell'intero ciclo del rapporto lavorativo: dal ricorso a chatbots durante il colloquio di lavoro alla selezione automatizzata nella assegnazione di compiti, mansioni

e turni (ma anche promozioni e/o trattamenti retributivi) sino alla identificazione del personale da cessare.

In un contesto quasi distopico di **gestione totalmente automatizzata del lavoro** (anche definito in gergo "***management algoritmico***"), il rischio che possano essere violati i precetti fondanti del diritto del lavoro (come il divieto di atti discriminatori o il corretto esercizio dei poteri datoriali) si palesa come un'urgenza concreta con cui fare i conti.

LE NORME DELL' AI ACT E LA TUTELA DEI LAVORATORI

Chiarito quanto sopra vediamo ora come si inserisce il Reg. UE 1689/2024 (c.d. AI ACT) in questo contesto.

Il Legislatore Europeo infatti, ben consapevole di tutti questi rischi, ha introdotto una serie di disposizioni espressamente indirizzate alla materia del lavoro.

In primo luogo, l'AI ACT all'art. 5 ha identificato una serie di **pratiche di AI che devono considerarsi vietate.**

Tra questa non sono ammissibili

- l'immissione sul mercato, la messa in servizio per tale finalità specifica o l'uso di sistemi di IA per inferire le emozioni di una persona fisica nell'ambito del luogo di lavoro.. (art. 5 lett. f)
- l'immissione sul mercato e l'uso di sistemi di categorizzazione biometrica che classificano individualmente le persone fisiche sulla base dei loro dati biometrici per trarre deduzioni o inferenze in merito a razza, opinioni politiche, appartenenza sindacale… (art. 5 lett. g)

Per quanto attiene alla pratica di cui al primo punto, si precisa che il Considerando 18 esclude dalla nozione di "emozione" gli **stati fisici** (quali il dolore o l'affaticamento) e la mera individuazione di **espressioni, gesti e movimenti immediatamente evidenti** (se non utilizzati per inferire emozioni).

Tali pratiche sono state ritenute a monte troppo rischiose per i diritti dei lavoratori, al punto di vietarle, ovvero di ammetterle con eccezioni ristrette.

L'AI ACT ammette poi l'utilizzo di una serie di s**istemi di AI che però, per il loro possibile impatto, sono considerati ad Alto Rischio.**

Si tratta dei sistemi indicati all'art. 6.

Tale norma (tra quelle cardini del AI ACT) stabilisce che devono essere considerati Sistemi AI ad Alto Rischio non solo i componenti di sicurezza di un prodotto regolato da una disciplina di cui all'All. I (tra cui il Reg.UE DPI e il Reg. Ue Macchine) ma anche i sistemi di AI applicati nei settori elencati all'All. III

Nello specifico tale Allegato al punto 4) è intitolato "Occupazione, gestione dei lavoratori e accesso al lavoro autonomi".
In questo settore, sonoconsiderati sistemi ad alto rischio:

a *" i sistemi utilizzati per l'assunzione o la selezione di persone fisiche, in particolare per pubblicare annunci di lavoro mirati, analizzare o filtrare le candidature e valutare i candidati;*
b *i sistemi utilizzati per adottare decisioni riguardanti le condizioni dei rapporti di lavoro, la promozione o cessazione dei rapporti contrattuali di lavoro, per assegnare compiti sulla base del comportamento individuale o dei tratti e delle caratteristiche personali o per monitorare e valutare le prestazioni e il comportamento delle persone nell'ambito di tali rapporti di lavoro."*

Appare evidente lo sforzo del Legislatore Europeo di ricomprendere entro queste due ampie casistiche l'intero ciclo di vita del rapporto lavorativo, compresa la fase dell'accesso al lavoro.

Infine l'AI ACT è il primo regolamento comunitario di natura orizzontale che introduce una disciplina ad hoc per la figura dell' "utilizzatore", denominato "deployer" (art. 3 lett. 4).

I depolyer (cioè il datore di lavoro che decide di utilizzare sistemi di AI) sono infatti tenuti ad adempiere agli obblighi di cui all'art. 26, fra cui:

1. l'utilizzo e l'implementazione del sistema di AI in **conformità con le istruzioni**

fornite dal provider (o fornitore) (comma 1);

2. la **garanzia di una sorveglianza umana** ex art. 14, affidata a persone fisiche appositamente formate (commi 2 e 3);
3. gli obblighi di **monitoraggio e di segnalazione nel caso di incidenti gravi** (comma 5);
4. **informare i rappresentanti dei lavoratori e i lavoratori** interessati prima di mettere in servizio o utilizzare un sistema di IA ad alto rischio sul luogo di lavoro (comma 8).

Tale ultimo obbligo dimostra il lodevole intento di esaltare il ruolo delle organizzazioni sindacali, attribuendo loro un ruolo concreto nella introduzione e gestione di sistemi di AI sul luogo di lavoro.

Infine, sebbene l'obbligo di effettuare una **valutazione di impatto** sui diritti fondamentali degli interessati ex art. 35 GDPR (o DPIA) sia previsto al comma 9 **solo "se del caso",** la dottrina più recente ritiene che l'utilizzo di sistemi di AI ad alto rischio sul luogo di lavoro integra di per sé i presupposti per la DPIA, con l'effetto di rendere questa di fatto **obbligatoria per i deployer – datori di lavoro**.

LA TUTELA DEL LAVORO OLTRE L'AI ACT: FRA IL GDPR E NORMATIVA ITALIANA

Il Regolamento sull'intelligenza Artificiale, per quanto ampio ed esaustivo, è insufficiente di per sé a garantire la piena protezione dei lavoratori di fronte ai rischi dell'Intelligenza Artificiale.

Per questo motivo, esso necessita di essere integrato con altri testi normativi, primo fra tutti il Reg. 679/2016 (**GDPR**), in tema di tutela dei dati personali del lavoratori, con il quale il coordinamento risulta immediato: i due Regolamenti, infatti, condividono la medesima tecnica regolamentare (**approccio risked-based**), nonché **plurimi punti di coordinamento** (si pensi agli obblighi di preventiva informativa dei lavoratori in qualità di interessati al trattamento ex GDPR e in qualità di destinatari di sistemi di AI nell'AI Act).

Infine, a livello nazionale, l'AI Act necessita di essere integrato non solo con normative consolidate quali lo Statuto dei Lavoratori, ma anche con i **nuovi interventi normativi**

in materia, fra cui il D.D.L. sull'Intelligenza Artificiale e l'art. 1 bis del d.lgs. 152/1997 (come modificato dal d.lgs. 4 maggio 2023, o Decreto Lavoro), in tema di obblighi informativi nel caso di utilizzo di sistemi decisionali o di monitoraggio automatizzati.

CONCLUSIONI

Il Legislatore Europeo, nella formulazione dell'AI Act, dimostra di essere consapevole non solo della moltitudine di impieghi che l'AI può avere sul lavoro, ma anche dei rischi concreti che essa può comportare per i lavoratori.

Infatti, l'impiego di sistemi di AI in questo settore comporta nella quasi interezza dei casi che tali sistemi siano annoverati come ad alto rischio ai sensi dell'AI Act, rendendo tassativi gli adempimenti di cui all'art. 26 in capo al datore (la cui violazione comporta l'applicazione delle sanzioni di cui all'art. 99).
L'adozione di sistemi di Intelligenza Artificiale da parte dei datori di lavoro necessita quindi delle opportune **cautele e precauzione**, essendo necessaria una preventiva attività di adeguamento normativo (oltre che di **coinvolgimento delle rappresentanze sindacali** dei lavoratori).

DDL Intelligenza Artificiale: le novità in materia di diritto del lavoro

Articolo di Dott. Guido Lepore

21 Maggio 2024

In attesa della pubblicazione in GUCE dell'AI Act approvato il 13 marzo 2024, il governo italiano ha presentato in data 23/04/2024 un proprio disegno di legge dal titolo "Norme per lo sviluppo e adozione di tecnologie di intelligenza artificiale" (cd. DDL sull' Intelligenza Artificiale).

Mentre la normativa Europea in tema di intelligenza artificiale si occupa principalmente di disciplinare la progettazione e l'immissione sul mercato dei sistemi di intelligenza artificiale - considerati alla stregua di un prodotto -, il disegno di legge italiano detta invece i principi generali, le finalità e gli obiettivi in materia di intelligenza artificiale, disciplinandone poi l'utilizzo in diversi settori. Fra questi, vi è anche il diritto del lavoro.

Ripercorriamo, quindi, il testo normativo con gli "occhi" del giuslavorista.

AI E GIURISPRUDENZA

Prima di entrare nel merito del disegno di legge, occorre precisare che il diritto del lavoro è uno dei primi settori in cui sta già iniziando a formarsi un **orientamento giurisprudenziale in materia di intelligenza artificiale**.

Fra i primi ambiti di applicazione pratica dell'intelligenza artificiale, infatti, vi è stato sicuramente quello del settore produttivo: l'IA è entrata fin da subito nelle fabbriche e nelle aziende, con evidenti ripercussioni nella gestione dei rapporti di lavoro - soprattutto in tema di selezione del personale, trasparenza e discriminazioni.

Fra i precedenti giurisprudenziali più interessanti, troviamo infatti:

- **Bologna, ordinanza n. 2949/2022**, una fra le prime pronunce in materia di discriminazioni sul luogo di lavoro derivanti dall'utilizzo di sistemi di intelligenza artificiali;

- **Palermo, sentenza n. 14491/2023**, nella quale veniva accertata la natura antisindacale della mancata comunicazione, da parte del datore di lavoro nei confronti delle associazioni sindacali competenti, circa i criteri di funzionamenti dell'algoritmo di sistema artificiale impiegato per l'assegnazione degli incarichi ai riders.
- **Torino, sentenza n. 743/2023**, nella quale veniva accertata l'illegittimità dei criteri di scelta adottati da un sistema di intelligenza artificiale utilizzato dal Ministero dell'Istruzione per selezionare gli insegnanti a cui attribuire le supplenze.

Il disegno di legge in esame ha pertanto preso spunto dal lavoro della giurisprudenza più recente nel redigere le disposizioni più rilevanti in materia di lavoro, che di seguito si andranno ad esaminare.

IL DDL SULL'INTELLIGENZA ARTIFICIALE E IL DIRITTO DEL LAVORO: LE 5 DISPOSIZIONI FONDAMENTALI

Art. 1 Finalità e Obiettivi

Il Disegno di Legge ribadisce in incipit la necessità di proporre una **dimensione antropocentrica** dell'intelligenza artificiale, ovvero al **servizio dell'uomo**.

Nel diritto del lavoro, tale concetto assume chiaramente la declinazione di **un'intelligenza artificiale al servizio del lavoratore**, volta ad **accrescerne le condizioni di lavoro, promuoverne le potenzialità e tutelarne diritti**.

Art. 2 Definizioni

Con riferimento alle definizioni, l'art. 2, identicamente all'art. 3, par.1, n.1) dell'AI Act, introduce la definizione di "*sistema di intelligenza artificiale*", *considerato: "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*".

Un tipico esempio di sistema di intelligenza artificiale è "Siri", il noto assistente vocale

iPhone.

Il Disegno di Legge introduce poi una propria definizione di "**modelli di intelligenza artificiale**" (diversa da quella dell'AI Act di "modelli di intelligenza artificiale con finalità generali", art. 3, par. 1, n. 63), definendoli "*modelli che identificano strutture ricorrenti attraverso l'uso di collezioni di dati, che hanno la capacità di svolgere un'ampia gamma di compiti distinti e che possono essere integrati in una varietà di sistemi o applicazioni*".

Un esempio di modello di intelligenza artificiale è "Chat GPT".

Va precisato come **la difformità fra la definizione di "modelli di intelligenza artificiale con finalità generali" dell'AI Act e quella di "modelli di intelligenza artificiale" del DDL in esame potrebbe ingenerare problemi di armonizzazione fra normativa europea e nazionale.**

Art. 10 Disposizioni sull'utilizzo dell'intelligenza artificiale in materia di lavoro

Questa norma si focalizza espressamente sul lavoro, disciplinando l'utilizzo dell'Intelligenza Artificiale in questo settore nella già menzionata ottica antropocentrica.

Infatti, l'intelligenza artificiale deve:

- migliorare le condizioni di lavoro,
- tutelare l'integrità psico-fisica di lavoratori e
- accrescere la qualità delle prestazioni lavorative e la produttività delle persone.

Inoltre, l'utilizzo dell'intelligenza artificiale sul lavoro deve essere **sicuro, affidabile e trasparente**, nonché assicurare la **dignità** e la **riservatezza dei lavoratori**.

Consapevole della centralità del principio di trasparenza, il Legislatore italiano sancisce un **obbligo di informativa molto capillare** a carico del datore di lavoro o committente, estendendo i casi e le modalità di cui all'art. 1 bis, d.lgs. 152/1997 e s.m.i. ("Ulteriori obblighi informativi nel caso di utilizzo di sistemi decisionali o di monitoraggio automatizzati") – disposizione presente già da tempo nel nostro ordinamento -.

Infine, deve essere assicurato il pieno **rispetto dei diritti inviolabili** di tutti i lavoratori,

evitando discriminazioni basate su sesso, età, origini etniche, credo religioso, orientamento sessuale, opinioni politiche e condizioni personali, sociali ed economiche. Tale disposizione mira a contrastare il fenomeno della **c.d. discriminazione algoritmica,** ovvero la presenza errori sistematici e ripetibili nei sistemi di intelligenza artificiali che distorcano l'elaborazione degli input e generino output discriminatori per i lavoratori.

Appare evidente, in questa disposizione, il richiamo ai principi di diritto fissati dai precedenti giurisprudenziali summenzionati.

Art. 11. Osservatorio sull'adozione di sistemi di intelligenza artificiale nel mondo del lavoro

Il Disegno di legge, fra le sue novità, introduce presso il Ministero del Lavoro e delle Politiche Sociali uno specifico **Osservatorio sull'adozione di sistemi di intelligenza artificiale nel mondo del lavoro**.
Detto organismo dovrà definire una strategia sull'utilizzo dell'intelligenza artificiale nel mondo del lavoro, monitorarne l'impatto, identificare i settori lavorativi maggiormente interessati e promuovere la formazione dei lavoratori e dei datori di lavoro in materia di intelligenza artificiale.

Criticabile, tuttavia, la disposizione di cui al comma 3, laddove prevede che tali obiettivi non debbano comportare nuovi o maggiori oneri a carico della finanza pubblica, facendo di fatto ricadere i costi della formazione sui privati.

Art. 12. Disposizioni in materia di professioni intellettuali

Infine, strettamente contigua ai temi trattati è l'adozione di sistemi di intelligenza artificiale nelle **professioni intellettuali**, che è consentito esclusivamente per esercitare **attività strumentali e di supporto all'attività** professionale e con **prevalenza del lavoro intellettuale** oggetto della prestazione d'opera.
Mentre appare di facile intuizione il concetto della "strumentalità" nell'attività professionale, maggiormente, problematico potrebbe essere il giudizio, in concreto, circa la prevalenza del lavoro intellettuale "umano" su quello "artificiale".

Infine, l'articolo 12 estende anche nel rapporto fra il professionista e il cliente uno

specifico obbligo di informativa circa le caratteristiche dei sistemi di intelligenza artificiale utilizzati nella prestazione intellettuale.

Considerazioni conclusive

Riassumendo, l'approccio del governo promotore di questo disegno di legge non mira solamente a sancire i **principi e gli obiettivi fondamentali** alla base dell'utilizzo dell'intelligenza artificiale sul luogo di lavoro, ma introduce anche delle **previsioni di carattere operativo**, quali l'**obbligo di informativa** in capo al datore di lavoro/committente (e al professionista).

Lodevole, inoltre, è l'istituzione di un **Osservatorio volto a promuovere l'utilizzo consapevole di detti sistemi automatizzati nel mondo del lavoro**, i cui compiti e funzioni verranno determinati dal Ministero del Lavoro una volta diventato attuativo il Disegno di legge.

Se approvato integralmente dal Parlamento, il DDL sull'intelligenza artificiale potrebbe quindi entrare in vigore e diventare direttamente applicabile nel nostro ordinamento, rendendo l'Italia uno dei primi stati dell'Unione Europea ad adottare una normativa interna in materia di intelligenza artificiale.

AI E CONTRATTUALISTICA

I contratti per lo sviluppo e la commercializzazione dell'AI

Articolo di Avv. Gaspare Castelli e Avv. Noemi Conditi

2 Luglio 2024

Il Regolamento sull'IA (AI Act) introdurrà numerosissime prescrizioni che devono anche essere tenute in considerazione nei rapporti tra i vari operatori economici, con importanti conseguenze soprattutto sul contenuto dei contratti per lo sviluppo e la commercializzazione dei sistemi AI.

Ci riferiamo, in particolare, al contratto in cui un operatore economico (o più operatori economici) affida ad altro operatore economico (o ad altri operatori economici) l'incarico di realizzare concretamente un prototipo di sistema AI allo scopo di commercializzarlo a proprio nome e marchio commerciale.

Ma quali sono le clausole contrattuali che gli operatori economici dovrebbero valutare, concordare e dunque inserire In tali tipi di contratti?

Formulare una risposta in questo senso è complesso, dal momento che le ordinarie difficoltà che si incontrano nel regolare qualsiasi rapporto di durata che si sviluppi in più fasi (nel caso di specie, progettazione, sviluppo, realizzazione e infine commercializzazione) si sommano in questo ambito alla complessità tecnica (talvolta imprevedibilità) dei sistemi AI e a quella normativa della recente regolamentazione.

Pur nella consapevolezza di tali difficoltà, questo articolo intende condividere alcune prime riflessioni sull'opportuno contenuto di questi "nuovi" contratti, non tanto per fornire una soluzione definitiva alle problematiche che essi generano, ma per permettere agli operatori economici interessati al mondo dell'intelligenza artificiale di conoscere

alcuni profili di indubbio rilievo, giuridico e pratico.

I DIRITTI DI PROPRIETÀ INTELLETTUALE

Innanzitutto, si deve osservare come la complessa tecnologia tipica dei sistemi AI porrà molto probabilmente - se non inevitabilmente – questioni inerenti ai diritti di proprietà intellettuale.

La proprietà intellettuale si riferisce a un sistema di tutela giuridica del frutto dell'attività creativa e inventiva umana nel campo artistico, scientifico e industriale. I diritti di proprietà intellettuale non proteggono il bene fisico in cui la creazione o l'invenzione è contenuta, ma la creazione intellettuale in quanto tale.

Ad esempio, tra i diritti di proprietà intellettuale rilevanti per i sistemi AI e che le parti del contratto dovrebbero assolutamente considerare vi sono: diritto d'autore; brevetto; know-how.

Innanzitutto, le parti dovranno considerare che i sistemi AI, poiché destinati a funzionare per il tramite di un software, saranno sempre coperti dal diritto d'autore.

Difatti, il diritto d'autore tutela il linguaggio di programmazione e/o il codice sorgente contenuto in esso e, quindi, il software a prescindere dal fatto che abbia applicazione industriale o meno.

Pertanto, è opportuno che le parti

- concordino su chi sarà il titolare dei diritti di autore e
- predispongano, se del caso, accordi di cessione (trasferimento definitivo della proprietà) e/o licenza (concessione del mero permesso di utilizzare) dei diritti di sfruttamento economico del software che andranno a determinare la proprietà e i limiti di utilizzo dei diritti d'autore (sulle differenze tra cessione e licenza cfr. "Consigli pratici sulla redazione dei contratti nel trasferimento tecnologico diretto alla commercializzazione dei prodotti".)

Inoltre, il sistema AI potrà anche formare oggetto di brevetto, se presenta i caratteri della

- "***novità***" – una tecnologia non è ancora accessibile al pubblico,
- "***originalità***" – una persona esperta ritiene che il sistema AI non risulti in modo evidente dallo stato della tecnica,
- "***industrialità***" – il sistema AI può essere fabbricato o utilizzato in qualsiasi genere di industria.

Proprio in ragione di tale possibilità, le parti dovrebbero sin da subito concordare:

- se il sistema AI che si intende sviluppare possa essere oggetto di brevetto;
- quale parte avrà diritto di depositare la domanda presso gli enti nazionali e/o sovranazionali preposti alla registrazione dei brevetti e, se del caso, quali saranno questi enti;
- chi sarà il titolare del brevetto;
- se sia opportuno stipulare accordi di cessione (trasferimento definitivo della proprietà) e/o licenza (concessione del mero permesso di utilizzare) di brevetto.

Per ultimo, ma non per importanza, ulteriore elemento di valutazione avrà ad oggetto eventuali competenze ed esperienze messe a disposizione delle parti per eseguire il contratto di sviluppo e commercializzazione del sistema AI (c.d. "know-how", cioè il "patrimonio di conoscenze e abilità operative" a disposizione delle parti).

In particolare, tale aspetto rileverà quando lo sviluppo o anche la commercializzazione del sistema AI richieda delle competenze che rientrino nel patrimonio della conoscenza di una sola delle parti del contratto.

Le parti dovranno dunque

- valutare se esista un know how di cui l'altra parte non dispone, e successivamente
- determinare il suo contenuto preciso,
- stipulare eventuali accordi di cessione o licenza analogamente a quanto necessario per il brevetto e il diritto d'autore e, infine, in merito ad attività di formazione e/o assistenza tecnica correlata alla fase di sviluppo e di successiva commercializzazione del sistema AI.

LA CORRETTA QUALIFICA NORMATIVA APPLICABILE AL SISTEMA IA

Ulteriore aspetto fondamentale da valutare nel contratto riguarderà gli aspetti di qualificazione normativa del prodotto e di conseguenza gli obblighi di legge che le parti dovranno rispettare nella fase di commercializzazione del sistema AI.

Tale commercializzazione sarà infatti regolata dal nuovo AI Act, il quale – come noto – ha previsto in questo senso nuovi obblighi in capo agli operatori economici (cfr. "I soggetti coinvolti dall'AI ACT: uno sguardo d'insieme").

Tuttavia, qualora il sistema AI abbia una particolare destinazione d'uso, potrebbe anche essere parallelamente soggetto ad altra specifica normativa. E' questo, ad esempio, il caso dei sistemi AI destinati al settore sanitario e con destinazione d'uso medica, per cui si applicherà oltre all'AI Act anche il Regol. UE 2017/745.

Gli obblighi previsti dalla legge in capo alle parti del contratto saranno dunque maggiori, dal momento che deriveranno dall'intersezione (a volte sommatoria) di quelli previsti da entrambe le normative applicabili.

Il contratto, quindi, dovrà essere redatto tenendo in considerazioni i futuri obblighi delle parti per la commercializzazione del sistema AI, prendendo in considerazione, in particolare:

- tutte le normative di legislazione di prodotto applicabili al Sistema AI e, quindi, non solo le previsioni dell'AI Act ma anche quelle ulteriormente applicabile, come il Regol. UE 2017/745 in caso di destinazione d'uso medica;
- il ruolo e gli obblighi che le parti, alla luce delle normative applicabili al sistema AI, avranno con riguardo alla realizzazione e commercializzazione del prodotto, tenuto conto che ciò potrebbe dipendere dalla diversa legislazione di prodotto applicabile;
- la titolarità e la gestione del marchio commerciale che verrà apposto sul prodotto;
- la gestione e i limiti eventuali alle attività informative e promozionali;
- la regolazione delle attività di sorveglianza post-commercializzazione;
- la gestione di eventuali azioni correttive.

INFORMAZIONI CONFIDENZIALI

Occorrerà poi valutare quali siano le informazioni che le parti non intendano fornire all'altra parte perché ritenute confidenziali e/o strategiche (es. segreti commerciali garanzie dei sistemi di produzione e qualità delle parti; modalità e attrezzature necessarie per la realizzazione del Sistema AI; caratteristiche progettuali e tecniche del prodotto; diritti di proprietà intellettuale correlati al prodotto; informazioni relative ai partner commerciali che partecipano indirettamente alla partnership).

Ciò impone quindi di valutare accuratamente le informazioni necessarie per dare esecuzione al contratto di sviluppo e commercializzazione del sistema AI, onde evitare opposizioni della confidenzialità ingiustificati o addirittura strumentali.

Ad esempio, potrebbe accadere che la parte sulla quale grave un obbligo normativo di comunicazione di determinate informazioni risulti involontariamente a causa dell'opposizione dell'altra di fornire dette informazioni per timore di rivelare segreti commerciali.

DATI PERSONALI

Altro aspetto fondamentale da regolare tra le parti, anche a livello contrattuale, è la gestione dei dati personali, sia nella fase di sviluppo del sistema di IA che nella sua commercializzazione e utilizzo.

Infatti, da un lato per lo sviluppo di un sistema AI può essere necessario condurre un'indagine clinica, raccogliendo e trattando di conseguenza diversi dati personali. In questo senso, i ruoli privacy di tutti i soggetti coinvolti nell'indagine devono essere ben definiti, con l'indicazione dei conseguenti obblighi e responsabilità, per evitare inadempimenti o violazioni della normativa.

Dall'altro, è comunque necessario continuare a raccogliere dati durante tutto il ciclo di vita del sistema AI, per adempiere agli obblighi di sorveglianza post-commercializzazione previsti dalle normative applicabili. In particolare, tali dati saranno necessari per:

- Aggiornare il software, e

– Migliorarne la sicurezza e le prestazioni.

Disciplinare le modalità di tale raccolta nei contratti diventa necessario quando il fabbricante si avvalga di soggetti terzi per la fornitura del proprio prodotto o di providers. In questi casi, infatti, saranno proprio tali ultimi soggetti coloro che materialmente raccolgono i dati necessari e di conseguenza, occorrerà contrattualizzare il loro obbligo di fornirli (in forma anonima, o, ove possibile, pseudonimizzata) al fabbricante per adempiere ai suoi obblighi.

CONDIZIONI ECONOMICHE

Un profilo fondamentale è quello che riguarda la regolazione degli aspetti economici del contratto di sviluppo e commercializzazione del sistema AI.

Innanzitutto, le parti dovranno concordare chi sosterrà i costi di sviluppo e commercializzazione e, se del caso, in quale misura. Poi, occorrerà anche concordare l'utilità economica complessiva di questa forma di partnership commerciale e, quindi:

- pagamento corrispettivo per eventuali servizi resi (es. attività di sviluppo, formazione);
- utilità economiche derivante dalla "gestione" dei diritti di sfruttamento economico di brevetto, d'autore e/o di know-how.

LA DURATA E IL RECESSO

Le partnership commerciali di sviluppo e commercializzazione di Sistema AI sono composte sempre da più fasi che consentono di pervenire al risultato finale solo dopo aver superato tutti gli step preliminari richiesti. Sarà determinate, quindi, regolare il contratto per fasi, prevedendo, se del caso, condizioni contrattuali il cui avveramento consente:

- di passare alla fase successiva;
- di interrompere il contratto, per esempio, per mancato raggiungimento degli obiettivi prefissati, mancato superamento della fase, impossibilità tecnica ecc.

IL FALLIMENTO DELLA PARTNERSHIP

Infine, importante sarà regolare le conseguenze del fallimento della partnership e, in particolare, gli effetti che le parti vogliono dare al rapporto nel caso il contratto cessi per qualsiasi motivo. In questi casi, difatti, pur non essendo stato eseguito il rapporto come le parti si aspettavano, è plausibile che sussistano attività oramai svolte verso le quali le parti potrebbe rivendicare pretese e/o altri diritti.

AI E PUBBLICITÀ

Se utilizzo un sistema di IA per i miei contenuti devo dichiararlo? L'obbligo di trasparenza per i deployer

Articolo di Avv. Eleonora Lenzi e Avv. Giorgia Verlato

11 Novembre 2024

Sempre più spesso i sistemi di IA sono utilizzati per generare testi, creare immagini o contenuti audio e video.

Già Nel 2019 il gruppo di esperti di alto livello sull'intelligenza artificiale nominato dalla Commissione (AI HLEG) elaborò le Linee guida etiche per un'AI affidabile, indicando sette principi etici per un'AI affidabile e eticamente valida.

I sette principi sono: intervento e sorveglianza umana, robustezza tecnica e sicurezza, vita privata e governance dei dati, trasparenza, diversità, non discriminazione ed equità, benessere sociale e ambientale e responsabilità.

Il recente Regolamento UE 1689/2024 (AI ACT) conferisce poi estrema importanza a tale principio

In primo luogo chiarisce che per trasparenza, si intende che "*i sistemi di IA sono sviluppati e utilizzati in modo da consentire un'adeguata tracciabilità e spiegabilità, rendendo gli esseri umani consapevoli del fatto di comunicare o interagire con un sistema di IA e informando debitamente i deployer delle capacità e dei limiti di tale sistema di IA e le persone interessate dei loro diritti*" (Considerando 27 AI ACT), ma anche "*l'obbligo per i deployer di rendere noto in modo chiaro e distinto che il contenuto è stato creato o manipolato artificialmente etichettando di conseguenza gli output dell'IA e rivelandone l'origine artificiale*" (Considerando 134).

L'art. 50 prevede poi specificamente obblighi di trasparenza in capo sia ai fornitori che ai deployer, qualificati questi ultimi come "*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*" – art. 3 (Definizioni).

Nel presente contributo ci occuperemo nello specifico dell'obbligo di trasparenza relativo ai contenuti generati con l'ausilio di un sistema di IA posto in capo ai deployer.: quindi, gli obblighi che andremo ad analizzare nel prosieguo riguardano i soggetti che utilizzano un sistema di IA nell'esecuzione di un'attività professionale.

OBBLIGO DI TRASPARENZA PER I DEPLOYER

In relazione ai contenuti generati con l'ausilio di un sistema di AI, l'art. 50 comma 4 dell'AI ACT prevede in capo ai deployer i seguenti obblighi:

- *I deployer di un sistema di IA che genera o manipola immagini o contenuti audio o video che costituiscono un «deepfake» rendono noto che il contenuto è stato generato o manipolato artificialmente. (…) Qualora il contenuto faccia parte di un'analoga opera o di un programma manifestamente artistici, creativi, satirici o fittizi, gli obblighi di trasparenza di cui al presente paragrafo si limitano all'obbligo di rivelare l'esistenza di tali contenuti generati o manipolati in modo adeguato, senza ostacolare l'esposizione o il godimento dell'opera.*
- *I deployer di un sistema di AI che genera o manipola testo pubblicato allo scopo di informare il pubblico su questioni di interesse pubblico rendono noto che il testo è stato generato o manipolato artificialmente. Tale obbligo non si applica se l'uso è autorizzato dalla legge per accertare, prevenire, indagare o perseguire reati o se il contenuto generato dall'IA è stato sottoposto a un processo di revisione umana o di controllo editoriale e una persona fisica o giuridica detiene la responsabilità editoriale della pubblicazione del contenuto.*

Analizziamo le previsioni di cui sopra

I**n relazione alle immagini e ai contenuti audio o video**, il considerando 134 ci viene

in soccorso nel capire cosa si intende per deep fake e di conseguenza quando si applica l'obbligo di trasparenza, precisando che i deployer sono tenuti a rendere noto in modo chiaro e distinto che il contenuto è stato creato o manipolato artificialmente **quando le immagini o i contenuti audio e video assomigliano notevolmente a persone, oggetti, luoghi, entità o eventi esistenti che potrebbero apparire falsamente autentici o veritieri** a una persona (***deep fake***).

I deployer dovranno adempiere a questo obbligo **etichettando gli output** dell'AI e rivelandone l'origine artificiale.

Per quanto concerne invece i **testi generati con l'ausilio di un sistema di AI,** l'obbligo di rendere noto che il testo è stato creato con l'ausilio di un sistema di AI si applica se il testo ha lo scopo di informare il pubblico **su questioni di interesse pubblico**.

Si deve trattare quindi innanzitutto di testi rivolti al pubblico e che abbiano un contenuto e un intento di "informazione" in favore del pubblico.

L'obbligo non si applica se il testo è stato revisionato da un essere umano.

In questa ultima ipotesi la questione riguarderà le modalità con cui fornire la prova che il testo pubblicato non sia il mero output di una macchina ma il frutto di una elaborazione umana.

ANALISI DI UN CASO

Indagate le disposizioni che regolano un vero e proprio obbligo di trasparenza circa l'utilizzo di un sistema di intelligenza artificiale in capo ai deployer, concludiamo questo breve approfondimento con il riferimento ad **un caso pratico in cui potrebbero applicarsi le regole della normativa in esame.**

L'utilizzo dell'AI, come è facile immaginare, interessa diversi ambiti, tra cui quello **pubblicitario**.

Al riguardo è possibile per un brand realizzare immagini di **un determinato contesto** a fini pubblicitari e promozionali, tramite l'AI. Tuttavia, come abbiamo anticipato, deve essere data al pubblico una corretta informazione sull'origine dell'immagine e devono

essere rispettati i principi di trasparenza fatti propri dal Regolamento e già alla base della disciplina pubblicitaria, tra cui il **principio di non ingannevolezza**.

Sebbene, come noto, la disciplina in esame non sia ancora entrata in vigore, per ragioni di trasparenza sarebbe così opportuno (sin da ora) l'inserimento di un disclaimer come "immagine generata/modificata con AI".

Infine, prestando attenzione proprio all'ambito pubblicitario, si evidenzia che oltre all'applicazione dell'art. 50 sopra analizzato, occorre prestare attenzione anche ai contenuti dei cui all'art. 5 Regolamento UE 1689/2024.

L'art. 5 del Regolamento introduce infatti - in sintesi - il divieto di utilizzare sistemi che adottano tecniche manipolative per indirizzare la scelta dell'utente o per indurlo ad adottare comportamenti che, diversamente, non avrebbe adottato.

Tale regola assume particolare importanza se si considera che il contesto pubblicitario risulta finalizzato a promuovere tramite le più diverse tecniche e arti comunicative un determinato servizio, prodotto o brand rivolgendosi al pubblico e averne così l'approvazione.

Nonostante ciò, come precisato dallo stesso art. 5, l'autodeterminazione e quindi l'eventuale scelta del pubblico non può essere manipolata e quindi compromessa nemmeno a favore di una attività commerciale che per sua stessa naturale è volta ad attrarre una vasta platea di destinatari.

Sul punto, non si può fare a meno di evidenziare che il principio appena descritto, unitamente all'obbligo di trasparenza, risulta in perfetta armonia anche con i principi contenuti nelle norme nazionali che regolano la materia pubblicitaria (artt. 20 e ss, D.Lgs.n 206/2005, c.d. "Codice del Consumo"), quali il divieto di pubblicità subliminale a tutela dei consumatori.

AI E APPALTI

Automatizzazione delle Procedure di Gara e Riserva di Umanità

Articolo di Avv. Adriano Colomban

19 Novembre 2024

L'automatizzazione delle procedure di gara implica l'uso di algoritmi, e rappresenta certamente un'opportunità per ottimizzare la gestione delle risorse pubbliche, ridurre tempi di esecuzione e minimizzare errori di calcolo e valutazione. Tuttavia, questo processo deve essere opportunamente controbilanciato dalla cd. "riserva di umanità", un principio giuridico che assicura la supervisione umana e, quindi, la legittimità delle decisioni amministrative.

La "riserva di umanità" ha radici profonde nella teoria dell'organo e nel principio di imputazione dell'atto amministrativo. Tradizionalmente, la pubblica amministrazione opera tramite l'intervento di persone fisiche che agiscono come organi dell'ente pubblico. Questo modello, ben definito nella teoria dell'immedesimazione organica, garantisce che ogni atto amministrativo sia imputabile a una persona fisica. Con l'automatizzazione, invece, la mancanza di intervento umano nelle decisioni amministrative comporterebbe un rischio d'emanazione di atti potenzialmente privi di legittimità giuridica.

DEFINIZIONI CHIAVE: ALGORITMO, AUTOMAZIONE E INTELLIGENZA ARTIFICIALE

Un'efficace distinzione tra algoritmo, automazione e intelligenza artificiale permette di comprendere le diverse modalità di interazione tra tecnologia e l'attività amministrativa:

- **Algoritmo**: è una sequenza di istruzioni programmate che consente a un software di risolvere una serie di problemi in modo deterministico, ovvero offrendo lo stesso

output per lo stesso input.
Nelle gare pubbliche, l'algoritmo può ad esempio mettere in ordine le offerte secondo criteri prestabiliti, determinare punteggi, escludere offerte anomale e assistere nella verifica della documentazione, riducendo l'intervento umano nelle fasi preliminari della valutazione.

- **Automazione**: applicazione dell'algoritmo per eseguire attività senza intervento umano, delegando all'elaboratore elettronico l'operazione di calcolo o selezione. Si può distinguere tra automazione "tradizionale", basata su algoritmi chiusi che seguono regole predefinite, e intelligenza artificiale avanzata, che include algoritmi "aperti" in grado di apprendere e adattarsi.
  Nelle gare pubbliche può essere utilizzata nella verifica di requisiti formali delle offerte.
- **Intelligenza Artificiale (IA)**: insieme di tecnologie avanzate, come il machine learning, che permettono alla macchina di "apprendere" dai dati e affinare i propri risultati. A differenza dell'algoritmo tradizionale, l'IA può generare decisioni non predeterminate in fase di programmazione, aprendosi alla possibilità di interpretazioni più sofisticate delle informazioni.
  Nell'ambito delle gare pubbliche, l'IA può svolgere ruoli sempre più complessi, ad esempio identificando pattern di irregolarità nelle offerte o stimando l'affidabilità di un operatore economico sulla base di dati storici.

VIZI DELL'ATTO AMMINISTRATIVO: NULLITÀ E ANNULLABILITÀ NELLE DECISIONI AUTOMATIZZATE

Nelle decisioni adottate tramite algoritmi e automazione/IA, i concetti di nullità e annullabilità assumono particolare rilevanza, poiché un errore o un vizio tecnico possono compromettere la validità dell'intero procedimento di gara. La giurisprudenza ha tracciato distinzioni importanti in questo contesto:

- **Nullità**: nelle procedure automatizzate, la nullità può derivare da un difetto radicale, come la mancata attribuzione del potere decisionale a un organo competente o la violazione dei principi costituzionali. Ad esempio, l'utilizzo di un algoritmo che discrimini o violi i principi di imparzialità e trasparenza potrebbe condurre alla

nullità dell'atto, poiché comprometterebbe i principi fondamentali dell'azione amministrativa.

- **Annullabilità**: l'annullabilità, invece, è prevista per i vizi meno gravi che non invalidano radicalmente l'atto ma ne inficiano la legittimità. Nelle decisioni algoritmiche, i casi di annullabilità possono comprendere errori procedurali, valutazioni incomplete o omissioni. Per esempio, se un algoritmo omette di considerare informazioni rilevanti in base a istruzioni predefinite, il vizio sarebbe annullabile, poiché correggibile con una revisione e non tale da invalidare l'atto in modo irreversibile.

La "riserva di umanità" funge pertanto da strumento di tutela contro i rischi di nullità e annullabilità nelle decisioni algoritmiche. La necessità di un intervento umano non è solo una garanzia etica ma anche giuridica. È necessario che vi sia un contributo umano capace di verificare, modificare o correggere eventuali errori dell'algoritmo. L'assenza di tale intervento potrebbe portare a vizi insanabili, configurando la nullità dell'atto, specialmente se l'algoritmo agisce su decisioni discrezionali dove il controllo umano è indispensabile.

L'adozione di algoritmi che non rispettano la "riserva di umanità" potrebbe, quindi, provocare situazioni in cui viene dichiarata la nullità dell'atto, soprattutto in casi di discriminazione o di errori, con gravi conseguenze economiche e procedurali.

L'IMPUTABILITÀ DELLE DECISIONI

La "riserva di umanità" stabilisce altresì che ogni decisione amministrativa automatizzata debba essere riconducibile a una persona fisica o giuridica, che ne risponda giuridicamente e patrimonialmente. In caso contrario, si verrebbe a creare una lacuna di responsabilità, dove l'algoritmo opererebbe in modo indipendente, privo di un controllo efficace e senza possibilità di sanzionare eventuali errori.

I Giudice amministrativi in alcune occasioni hanno già affermato che il software, benché esegua calcoli e operazioni complesse, deve essere supervisionato e controllato da funzionari competenti. Questo significa che l'uso degli algoritmi non può esentare i responsabili amministrativi dall'assumersi la piena responsabilità delle scelte effettuate. La stessa impostazione è condivisa nel nuovo Codice Appalti, il quale specifica

che l'automazione è ammessa solo se accompagnata da garanzie di trasparenza e responsabilità.

In questo quadro, l'**art. 30 del nuovo Codice Appalti impone alle stazioni appaltanti di assicurare la comprensibilità delle logiche decisionali e la disponibilità del codice sorgente**, in modo che eventuali vizi possano essere individuati e corretti. Tale obbligo è pensato per ridurre il rischio di nullità, facilitando il controllo umano sull'operato degli algoritmi.

RISCHI E LIMITAZIONI DELLA DECISIONE ALGORITMICA

L'inserimento di algoritmi e intelligenza artificiale (IA) nelle gare d'appalto è una pratica che, pur offrendo vantaggi in termini di efficienza e uniformità delle valutazioni, comporta anche una serie di rischi specifici e limitazioni, che la giurisprudenza e il diritto amministrativo mirano a mitigare.

- **Discriminazione Algoritmica**: l'algoritmo può riflettere pregiudizi inconsapevoli se i dati di addestramento includono informazioni storicamente condizionate da discriminazioni. Ad esempio, un sistema automatizzato che favorisca certi fornitori in base a criteri quantitativi o a uno storico dei contratti precedenti potrebbe, inconsapevolmente, escludere nuovi partecipanti o realtà emergenti, consolidando un'inequità sistemica. A tale scopo, il D.Lgs. 36/2023 impone che siano in atto meccanismi di monitoraggio e revisione continua per prevenire effetti discriminatori, con la possibilità di interventi correttivi da parte del personale dell'amministrazione.
- **Inesattezza dei Dati**: poiché l'algoritmo si basa sui dati di input per generare risultati, la qualità e l'accuratezza di questi dati sono fondamentali. Errori o incongruenze nei dataset di input possono portare a decisioni errate, e quindi a valutazioni distorte delle offerte. Si evidenzia pertanto che anche la pubblica amministrazione deve predisporre audit regolari sui dati utilizzati e verificare che essi riflettano le informazioni necessarie e pertinenti alla gara. Le decisioni erronee dovute alla qualità dei dati non devono compromettere i principi di buon andamento e imparzialità che l'amministrazione è tenuta a rispettare.

GIURISPRUDENZA E RISERVA DI UMANITÀ: CASI ESAMINATI

Si prendono infine ad esempio alcune sentenze che hanno definito e circoscritto il ruolo dell'algoritmo e la necessità della supervisione umana nelle decisioni amministrative automatizzate, introducendo, già prima dell'emanazione del nuovo Codice Appalti, elementi volti a proteggere la trasparenza e la responsabilità dell'ente pubblico.

Cons. St., Sentenza n. 2270/2019

La sentenza, seppure precedente al nuovo Codice Appalti, analizza il caso di una procedura automatizzata per l'assegnazione di sedi a docenti assunti nell'ambito del piano straordinario previsto per legge. Gli appellanti lamentavano sostanzialmente l'**assenza di trasparenza sull'algoritmo** utilizzato per l'assegnazione delle sedi e l'irrazionalità e l'illogicità degli esiti, con assegnazioni che non rispettavano le preferenze indicate, a danno di soggetti meglio posizionati in graduatoria.

Gli appellanti evidenziavano anche l'**impossibilità di comprendere i criteri alla base delle decisioni automatizzate** e denunciavano l'**assenza di motivazione nei provvedimenti** derivanti dall'algoritmo.

L'algoritmo pertanto era percepito come una "scatola nera", inaccessibile e incomprensibile, che ha impediva il controllo sulla correttezza delle assegnazioni.

Il Consiglio di Stato ha dunque affermato che **l'algoritmo**, al contrario, **deve essere conoscibile in tutti i suoi aspetti**, inclusi: la logica sottostante, i criteri utilizzati per le decisioni, le modalità con cui i dati vengono elaborati. La conoscibilità rafforza il principio di trasparenza e consente il sindacato del giudice.

Inoltre in questa Sentenza viene espresso il concetto di **Algoritmo come "atto amministrativo informatico".** In pratica l'algoritmo non è un'entità autonoma, ma un'estensione della volontà amministrativa. Deve essere costruito e gestito in modo da rispettare i principi di proporzionalità, ragionevolezza e pubblicità. La discrezionalità amministrativa deve essere esercitata nella fase di programmazione dell'algoritmo, non nella sua esecuzione.

Dal canto suo il Giudice amministrativo deve poter valutare la logica e la ragionevolezza dell'algoritmo e la correttezza dei dati inseriti e delle decisioni prese. Questa possibilità garantisce il diritto di difesa dei cittadini e la piena effettività del controllo giudiziario.

In definitiva l'impiego di algoritmi sembrerebbe non liberare affatto l'amministrazione dalla responsabilità di garantire la correttezza e la legalità degli atti, sottolineando che qualsiasi errore nel processo automatizzato è imputabile al soggetto pubblico. La sentenza stabilisce inoltre che la pubblica amministrazione deve prevedere modalità di verifica dei risultati prodotti dagli algoritmi, così da poter correggere e rendere trasparenti eventuali errori o incoerenze nel processo decisionale.

TAR Lazio, Sentenza n. 3769/2017

Un caso similare, ma ancora più datato nel tempo, ha affrontato invece i**l tema dell'accesso agli atti amministrativi** in relazione all'algoritmo utilizzato dal Ministero dell'Istruzione, Università e Ricerca (MIUR) per la gestione della mobilità interprovinciale dei docenti nell'anno scolastico 2016/2017. **Il ricorrente richiedeva l'accesso ai codici sorgente** del software che gestiva l'algoritmo, dopo che l'amministrazione aveva negato tale accesso, limitandosi a fornire una descrizione generale del funzionamento dell'algoritmo.

Il TAR ha ritenuto invece insufficiente la mera descrizione dell'algoritmo fornita dall'amministrazione, sottolineando che la comprensione completa del funzionamento del sistema richiede l'accesso ai codici sorgente. Questo per garantire la verifica di eventuali errori o incongruenze nell'elaborazione automatizzata.

Sebbene, dunque, il software sia tutelato come opera dell'ingegno, tale tutela non prevale sul diritto di accesso quando ciò è necessario per garantire il rispetto dei diritti degli interessati, a condizione che l'accesso non comprometta lo sfruttamento economico del software.

CONCLUSIONI E PROSPETTIVE FUTURE

In conclusione, l'introduzione, oramai conclamata, di algoritmi nelle gare d'appalto comporta vantaggi evidenti, ma è essenziale che tali strumenti siano impiegati

con attenzione per prevenire possibili vizi di nullità e annullabilità. La "riserva di umanità" rappresenta una salvaguardia contro il rischio che un agire amministrativo completamente automatizzato perda di trasparenza e di legittimità. Per garantire la corretta applicazione degli algoritmi, è fondamentale che le amministrazioni assicurino la supervisione umana e la trasparenza delle logiche utilizzate.

È sancito l'obbligo imposto dal Codice Appalti di assicurare la comprensibilità delle logiche decisionali e la disponibilità del codice sorgente, in modo che eventuali vizi possano essere individuati e corretti.

In sintesi, l'equilibrio tra automazione ed etica giuridica è possibile, ma richiede un quadro normativo solido e una vigilanza costante, affinché l'efficienza tecnologica non comprometta la tutela dei diritti dei partecipanti alle gare e la legittimità dell'azione amministrativa.

STEFANELLI & STEFANELLI STUDIO LEGALE

avv. Siliva Stefanelli
s.stefanelli@studiolegalestefanelli.it

avv. Eleonora Lenzi
e.lenzi@studiolegalestefanelli.it

avv. Gaspare Castelli
g.castelli@studiolegalestefanelli.it

avv. Maddalena Collini
m.collini@studiolegalestefanelli.it

avv. Adriano Colomban
a.colomban@studiolegalestefanelli.it

avv. Noemi Conditi
n.conditi@studiolegalestefanelli.it

avv. Federica Pucarelli
f.pucarelli@studiolegalestefanelli.it

avv. Maria Livia Rizzo
ml.rizzo@studiolegalestefanelli.it

dott.ssa Laura Anna Terrizzi
la.terrizzi@studiolegalestefanelli.it

avv. Giorgia Verlato
g.verlato@studiolegalestefanelli.it

Lo studio ringrazia per la collaborazione
Ing. Alice Ravizza e Dott. Guido Lepore

Studio Legale Stefanelli&Stefanelli

www.studiolegalestefanelli.it

Bologna: Via Azzo Gardino 8/A - 40122
Milano: Via Nino Bixio, 31 - 20129
Roma: Palazzo Marignoli - Piazza di San Silvestro, 8 - 00187
Venezia: Sestiere Castello 2388 - 30122

Edizione: Gennaio 2025