L'Europarlamento ha approvato il regolamento sull'utilizzo dell'IA in base a livelli di rischio

Intelligenza artificiale in chiaro

L'utente deve sempre sapere se sta interagendo con robot

Pagina a cura di
ANTONIO CICCIA MESSINA

Intelligenza artificiale (IA) mai in incognito. Le persone devono sapere se parlano con un robot o se stanno leggendo un testo prodotto da un'IA. È uno degli strumenti di tutela previsti dal regolamento Ue sull'intelligenza artificiale, approvato dal parlamento Ue il 13 marzo 2024, che disciplina modalità di immissione e di utilizzo nell'area Ue di questi strumenti di elevata tecnologia. Il provvedimento deve passare ancora l'ultimo vaglio del Consiglio Ue, prima di essere pubblicato sulla *Gazzetta Ufficiale Ue*.

Cosa troviamo nel regolamento. Il regolamento, oltre alla esplicita messa al bando dei sistemi che violano i diritti fondamentali, prevede una fitta serie di regole, parametrate a diversi livelli di rischio (minimo, alto, sistemico), per avere sotto controllo il mercato dell'IA: le autorità devono sapere chi mette in circolazione apparati di IA e, per quelli ad alto rischio, vengono imposti standard di conformità (con apposita marcatura) sotto la vigilanza di autorità pubbliche.

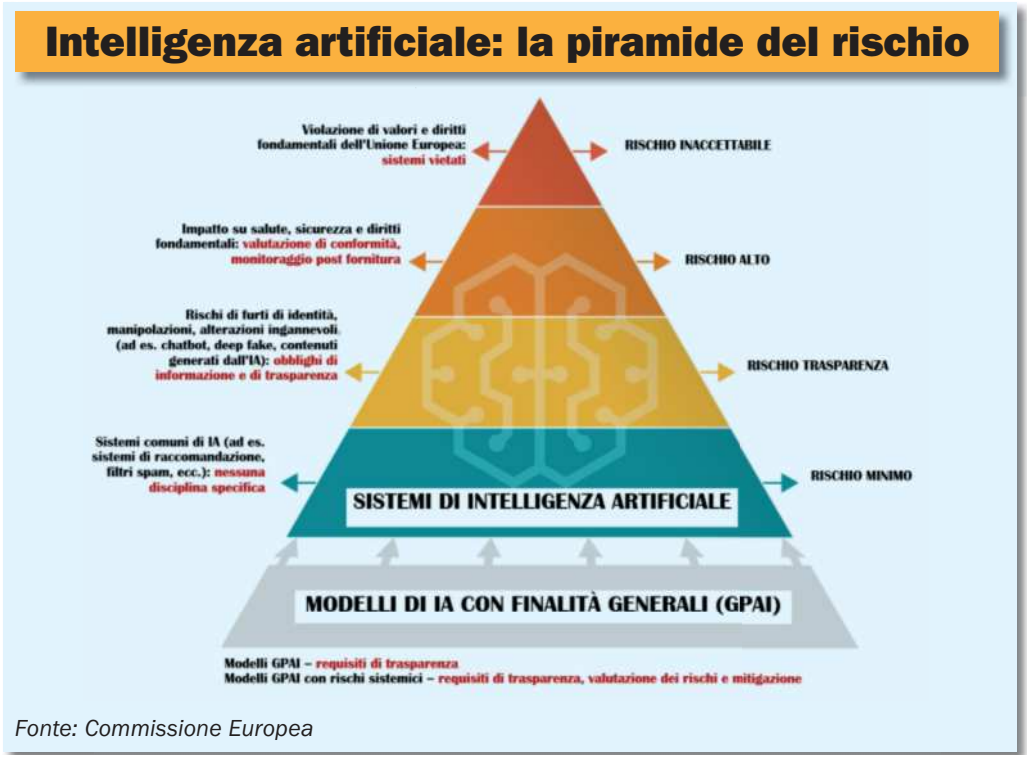
Completano il quadro le disposizioni sulle garanzie per le persone fisiche: devono essere in grado di individuare ciò che proviene da un robot, poter chiedere spiegazioni e informazioni quando si è soggetti a un'IA, ma soprattutto fruiscono di prerogative contro le autorità pubbliche, che usano l'IA per ragioni di contrasto alla criminalità e per la sicurezza.

Per fare in modo che l'IA non crei scompensi concorrenziali, il regolamento inserisce, poi, misure a sostegno dell'innovazione, in particolare per Pmi e start-up.

Per norma espressa, il regolamento non si applica alle persone fisiche che utilizzano sistemi di IA nel corso di un'attività non professionale puramente personale.

Trasparenza. Un aspetto di primaria importanza nel regolamento è la trasparenza per gli umani. Le persone devono essere informate e consapevoli che stanno dialogando e interagendo con un sistema di IA, salvo che ciò sia già evidente per un soggetto ragionevolmente attento.

I fornitori dei sistemi di IA devono comunque progettare e sviluppare i sistemi in maniera che non sorgano equivoci.



Fonte: Commissione Europea

Grava, sempre a carico dei fornitori di sistemi di IA, che generano contenuti audio, immagini, video o testuali sintetici, l'obbligo di garantire che ciò che è prodotto dall'IA sia marcato in un formato leggibile meccanicamente e rilevabile come generato o manipolato artificialmente.

L'obbligo di trasparenza è prescritto anche per gli operatori che utilizzano sistemi di IA di riconoscimento delle emozioni, sistemi di categorizzazione biometrica e sistemi di IA che generano o manipolano immagini o contenuti audio o video, che costituiscono un "deep fake". L'obbligo informativo non scatta, però, in alcuni casi: se si usano i sistemi per ragioni di giustizia penale o, nell'ambito editoriale, se c'è la revisione umana del testo scritto dall'IA e se c'è un responsabile della pubblicazione del contenuto.

Sistemi ad alto rischio. Sono elencati in un allegato al regolamento e comprendono questi settori: biometria, infrastrutture critiche, istruzione e formazione professionale, lavoro, servizi essenziali, attività di contrasto della criminalità, migrazione, e controllo delle frontiere, giustizia e processi democratici.

Peraltro, i sistemi di IA non saranno considerati ad alto rischio se non presentano un rischio significativo di danno alla salute, alla sicurezza o ai diritti fondamentali. Non sfuggono mai alla qualifica di alto rischio, invece, se effettuano la profilazione delle persone.

Per i sistemi di IA ad alto rischio, prima che i prodotti possano essere venduti e utilizzati nell'Ue, è prevista una procedura di valutazione della conformità, anche quanto a cibersicurezza.

Inoltre, sempre per i sistemi di IA ad alto rischio: deve essere predisposto un sistema di gestione dei rischi, deve essere redatta una idonea documentazione tecnica, la modalità d'uso deve essere compiutamente illustrata agli utilizzatori e la loro progettazione deve prevedere la sorveglianza umana commisurata ai rischi.

I fornitori di IA ad alto rischio devono dichiarare la conformità, apporre la marcatura Ce e istituire un sistema di qualità.

Se un sistema di IA comporta il trattamento di dati personali, deve essere dichiarata la conformità alle norme sulla privacy.

In alcuni casi dovrà essere stilata una valutazione d'impatto sui diritti fondamentali.

Prima di immettere sul mercato o mettere in servizio un sistema di IA ad alto rischio, di norma, il fornitore deve registrarsi in una banca dati dell'Ue.

Dopo l'immissione sul mercato di tali sistemi di IA, i fornitori devono assicurare il monitoraggio post-commercializzazione e, se necessario, adottare misure correttive.

Finalità generali. Se si tratta di IA con finalità generali e che presentano un rischio sistemico devono essere rispettati obblighi rafforzati in materia di analisi dei rischi e di valutazione di impatto.

Garantito il diritto di reclamo

L'IA non ha l'ultima parola. Le persone hanno diritto a presentare reclami e ricevere spiegazioni. Così prevede il regolamento Ue sull'intelligenza artificiale.

In dettaglio qualsiasi persona interessata da una decisione adottata dall'utilizzatore di sistemi di IA ad alto rischio, salvo alcune eccezioni, avrà il diritto di ottenere spiegazioni chiare e significative sul ruolo dell'IA nella decisione assunta.

La rete di tutela degli umani comprende anche i divieti all'utilizzo di molti sistemi di IA.

Così non si può ricorrere a IA che: usano tecniche subliminali o ingannevoli per distorcere il comportamento delle persone; sfruttano vulnerabilità dovute a età, disabilità o situazioni economiche; classificano le persone in base al comportamento sociale; prevedono la probabilità di commissione di reati (salvi ausili al giudizio umano su basi oggettive); creano o alimentano banche dati di riconoscimento facciale mediante scraping da Internet o da filmati di videosorveglianza; rilevano emozioni nei luoghi di lavoro o negli istituti di istruzione, salvo motivi medici o di sicurezza; classificano le persone su base biometrica per dedurre dati sensibili (salvo esigenze di contrasto penale); identificano le persone su base biometrica remota in tempo reale in spazi pubblici per attività di contratto penale (ad eccezione del rintraccio di vittime di rapimento, sfruttamento sessuale o persone scomparse, prevenzione da determinate minacce concrete e imminenti per la sicurezza o identificazione di sospetti di gravi reati).

A sorvegliare sull'osservanza dei divieti (assistita da pesanti sanzioni) e anche sul rispetto delle condizioni di utilizzo dell'IA lecita ci saranno autorità nazionali di vigilanza del mercato e di controllo sulla valutazione di conformità dei sistemi. Inoltre, nella Ue vengono istituiti l'ufficio per l'IA presso la commissione e il comitato europeo per l'intelligenza artificiale. Viene, infine, prevista una banca dati dell'Ue contenente le informazioni relative ai sistemi di IA ad alto rischio.

Peraltro, per far diventare effettivamente operativo il regolamento, occorrono numerosi atti e adempimenti attuativi di competenza della Commissione. Infine, per l'efficacia del regolamento si procederà per tappe. Prendendo a riferimento l'entrata in vigore del provvedimento, i sistemi vietati dovranno essere eliminati entro 6 mesi, le disposizioni relative alla IA con finalità generali e alle sanzioni si applicheranno decorsi 12 mesi, mentre quelle relative ai sistemi di IA ad alto rischio si applicheranno trascorsi 24 mesi (36 mesi per i sistemi di IA disciplinati della legislazione Ue sui prodotti).