



Questa è una traduzione automatica: [fa fede soltanto la lingua originale](#). La Commissione europea non si assume alcuna responsabilità per la qualità e la correttezza della traduzione automatica.

[Informazioni importanti sulla traduzione automatica](#)

Intelligenza artificiale — Domande e risposte *

Brussels, 1° agosto 2024

Perché dobbiamo regolamentare l'uso dell'intelligenza artificiale?

La legge dell'UE sull'IA è la prima legge globale in materia di IA al mondo. Mira ad affrontare i rischi per la salute, la sicurezza e i diritti fondamentali. Il regolamento tutela anche la democrazia, lo Stato di diritto e l'ambiente.

L'adozione dei sistemi di IA ha un forte potenziale in termini di benefici per la società, crescita economica e rafforzamento dell'innovazione dell'UE e della sua competitività a livello mondiale. Tuttavia, in alcuni casi, le caratteristiche specifiche di determinati sistemi di IA possono creare nuovi rischi connessi alla sicurezza degli utenti, compresa la sicurezza fisica, e ai diritti fondamentali. Alcuni potenti modelli di IA ampiamente utilizzati potrebbero persino comportare rischi sistemici.

Ciò comporta incertezza giuridica e un'adozione potenzialmente più lenta delle tecnologie di IA da parte delle autorità pubbliche, delle imprese e dei cittadini, a causa della mancanza di fiducia. Risposte normative disuguali da parte delle autorità nazionali rischierebbero di frammentare il mercato interno.

In risposta a tali sfide, era necessaria un'azione legislativa per garantire il buon funzionamento del mercato interno dei sistemi di IA, in cui i benefici e i rischi siano adeguatamente affrontati.

A chi si applica la legge sull'IA?

Il quadro giuridico si applicherà sia agli attori pubblici che a quelli privati all'interno e all'esterno dell'UE, purché il **sistema di IA** sia immesso sul mercato dell'Unione o il suo utilizzo abbia un impatto sulle persone situate nell'UE.

Gli obblighi possono interessare sia i fornitori (ad esempio uno sviluppatore di uno strumento di screening CV) sia gli operatori di sistemi di IA (ad esempio una banca che acquista questo strumento di screening). Vi sono alcune deroghe al regolamento. Le attività di ricerca, sviluppo e prototipazione svolte prima dell'immissione sul mercato di un sistema di IA non sono soggette a tali regolamenti. Inoltre, sono esentati anche i sistemi di IA progettati esclusivamente per finalità militari, di difesa o di sicurezza nazionale, indipendentemente dal tipo di entità che svolge tali attività.

Quali sono le categorie di rischio?

La legge sull'IA introduce un quadro uniforme in tutti gli Stati membri dell'UE, basato su una definizione lungimirante di IA e su un approccio basato sul rischio:

- **Rischio inaccettabile:** Un insieme molto limitato di usi particolarmente dannosi dell'IA che violano i valori dell'UE in quanto violano i diritti fondamentali e saranno pertanto vietati:
 - **Sfruttamento delle vulnerabilità delle persone, manipolazione e uso di tecniche subliminali;**
 - **Punteggio sociale** per scopi pubblici e privati;
 - **Attività di polizia predittiva individuale** basate unicamente sulla profilazione delle persone;
 - **Raschiatura non mirata** di Internet o CCTV per immagini facciali al fine di creare o ampliare banche dati;
 - **Riconoscimento delle emozioni sul luogo di lavoro e negli istituti di istruzione**, salvo per motivi medici o di sicurezza (ossia il monitoraggio dei livelli di stanchezza di un

pilota);

- **Categorizzazione biometrica** delle persone fisiche per dedurre o dedurre la razza, le opinioni politiche, l'appartenenza sindacale, le convinzioni religiose o filosofiche o l'orientamento sessuale. L'etichettatura o il filtraggio delle serie di dati e la categorizzazione dei dati nel settore delle attività di contrasto saranno ancora possibili;
 - **Identificazione biometrica remota in tempo reale in spazi accessibili al pubblico da parte delle autorità di contrasto**, fatte salve limitate eccezioni (cfr. infra).
- La Commissione pubblicherà orientamenti sui divieti prima della loro entrata in vigore il 2 febbraio 2025.
 - **Rischio alto:** Un numero limitato di sistemi di IA definiti nella proposta, che potrebbe avere un impatto negativo sulla sicurezza delle persone o sui loro diritti fondamentali (tutelati dalla Carta dei diritti fondamentali dell'UE), è considerato ad alto rischio. Sono allegati alla legge gli elenchi dei sistemi di IA ad alto rischio, che possono essere riesaminati per allinearsi all'evoluzione dei casi d'uso dell'IA.
 - Tali sistemi comprendono inoltre i componenti di sicurezza dei prodotti disciplinati dalla legislazione settoriale dell'Unione, Saranno sempre considerati ad alto rischio quando sono soggetti a una valutazione della conformità da parte di terzi ai sensi di tale legislazione settoriale.
 - Tali sistemi di IA ad alto rischio comprendono, ad esempio, sistemi di IA che valutano se qualcuno è in grado di ricevere un determinato trattamento medico, ottenere un determinato lavoro o un prestito per acquistare un appartamento. Altri sistemi di IA ad alto rischio sono quelli utilizzati dalla polizia per profilare le persone o valutarne il rischio di commettere un reato (a meno che non siano vietati a norma dell'articolo 5). E ad alto rischio potrebbero essere anche i sistemi di IA che gestiscono robot, droni o dispositivi medici.
 - **Rischiospecifico per la trasparenza:** Per promuovere la fiducia, è importante garantire la trasparenza sull'uso dell'IA. Pertanto, la legge sull'IA introduce requisiti specifici di trasparenza per determinate applicazioni di IA, ad esempio laddove vi sia un evidente rischio di manipolazione (ad esempio attraverso l'uso di chatbot) o deep fake. Gli utenti dovrebbero essere consapevoli del fatto che stanno interagendo con una macchina.
 - **Rischio minimo:** La maggior parte dei sistemi di IA può essere sviluppata e utilizzata nel rispetto della legislazione vigente senza ulteriori obblighi giuridici. I fornitori di tali sistemi possono scegliere di applicare, su base volontaria, i requisiti per un'IA affidabile e aderire a codici di condotta volontari.

Inoltre, la legge sull'IA prende in considerazione i **rischi sistemici** che potrebbero derivare dai **modelli di IA per finalità generali**, compresi i **grandi modelli di IA generativa**. Che possono essere utilizzati per una serie di compiti e stanno diventando la base di molti sistemi di IA nell'UE. Alcuni di questi modelli potrebbero comportare rischi sistemici se sono molto capaci o ampiamente utilizzati. Ad esempio, modelli potenti potrebbero causare incidenti gravi o essere utilizzati impropriamente per attacchi informatici di vasta portata. Molte persone potrebbero essere colpite se un modello diffonde distorsioni dannose in molte applicazioni.

Come posso sapere se un sistema di IA è ad alto rischio?

La legge sull'IA stabilisce una solida metodologia per la classificazione dei sistemi di IA come ad alto rischio. L'obiettivo è garantire la certezza del diritto per le imprese e gli altri operatori.

La classificazione del rischio si basa sulla finalità prevista del sistema di IA, in linea con la vigente legislazione dell'UE in materia di sicurezza dei prodotti. Ciò significa che la classificazione dipende dalla funzione svolta dal sistema di IA e dalla finalità e dalle modalità specifiche per le quali il sistema è utilizzato.

I sistemi di IA possono essere classificati come ad alto rischio in due casi:

- Se il sistema di IA è incorporato come componente di sicurezza in prodotti disciplinati dalla legislazione vigente in materia di prodotti (allegato I) o costituisce essi stessi tali prodotti. Potrebbe trattarsi, ad esempio, di un software medico basato sull'IA.
- Se il sistema di IA è destinato a essere utilizzato per un caso d'uso ad alto rischio, elencato in un allegato III della legge sull'IA. L'elenco comprende casi d'uso provenienti da settori quali l'istruzione, l'occupazione, l'applicazione della legge o la migrazione.

La Commissione sta preparando orientamenti per la classificazione ad alto rischio, che saranno pubblicati prima della data di applicazione di tali norme.

Quali sono gli esempi di casi d'uso ad alto rischio di cui all'allegato III?

L'allegato III comprende otto settori in cui l'uso dell'IA può essere particolarmente sensibile ed elenca casi d'uso concreti per ciascun settore. Un sistema di IA classifica come ad alto rischio se è destinato a essere utilizzato in uno di questi casi d'uso.

Esempi sono:

- I sistemi di IA utilizzati come componenti di sicurezza in determinate **infrastrutture critiche**, ad esempio nei settori del traffico stradale e della fornitura di acqua, gas, riscaldamento ed elettricità;
- **Sistemi di IA utilizzati nell'istruzione e nella formazione professionale**, ad esempio per valutare i risultati dell'apprendimento e orientare il processo di apprendimento e il monitoraggio delle truffe;
- **Sistemi di IA utilizzati nella gestione dell'occupazione e dei lavoratori** e nell'accesso al lavoro autonomo, ad esempio per collocare annunci di lavoro mirati, per analizzare e filtrare le domande di lavoro e per valutare i candidati;
- **Sistemi di IA utilizzati per l'accesso a servizi e benefici pubblici e privati essenziali** (ad esempio l'assistenza sanitaria), la **valutazione** del merito creditizio delle persone fisiche, la valutazione del rischio e la fissazione dei prezzi in relazione all' **assicurazione vita e sanitaria**;
- I sistemi di IA utilizzati nei settori dell' **applicazione della legge**, della migrazione e del **controllo delle frontiere**, nella misura in cui non siano già vietati, nonché nell'amministrazione della **giustizia** e nei **processi democratici**;
- I sistemi di IA utilizzati per l' **identificazione biometrica, la categorizzazione biometrica e il riconoscimento delle emozioni**, nella misura in cui non siano vietati.

Quali sono gli obblighi per i fornitori di sistemi di IA ad alto rischio?

Prima **di immettere un sistema di IA ad alto rischio sul mercato dell'UE**, o di farlo entrare in servizio, i fornitori devono sottoporlo a una **valutazione della conformità**. Ciò consentirà loro di dimostrare che il loro sistema è conforme ai requisiti obbligatori per un'IA affidabile (ad esempio qualità, documentazione e tracciabilità dei dati, trasparenza, sorveglianza umana, accuratezza, cibersecurity e robustezza). Tale valutazione deve essere ripetuta se il sistema o il suo scopo sono modificati in modo sostanziale.

I sistemi di IA che fungono da componenti di sicurezza dei prodotti disciplinati dalla legislazione settoriale dell'Unione saranno sempre considerati ad alto rischio se soggetti a valutazione della conformità da parte di terzi ai sensi di tale legislazione settoriale. Inoltre, tutti i sistemi biometrici, indipendentemente dalla loro applicazione, richiederanno una valutazione della conformità da parte di terzi.

I fornitori di sistemi di IA ad alto rischio dovranno inoltre **attuare sistemi di gestione della qualità e del rischio** per garantire la conformità ai nuovi requisiti e ridurre al minimo i rischi per gli utenti e le persone interessate, anche dopo l'immissione sul mercato di un prodotto.

I sistemi di IA ad alto rischio utilizzati da autorità pubbliche o soggetti che agiscono per loro conto dovranno essere **registrati in una banca dati pubblica dell'UE**, a meno che tali sistemi non siano utilizzati per le attività di contrasto e la migrazione. Queste ultime dovranno essere registrate in una parte non pubblica della banca dati che sarà accessibile solo alle autorità di controllo competenti.

Per garantire la conformità durante l'intero ciclo di vita del sistema di IA, le autorità di vigilanza del mercato effettueranno audit periodici e agevoleranno il monitoraggio successivo all'immissione sul mercato e consentiranno ai fornitori di segnalare volontariamente eventuali incidenti gravi o violazioni degli obblighi in materia di diritti fondamentali di cui siano venuti a conoscenza. In casi eccezionali, le autorità possono concedere deroghe per specifici sistemi di IA ad alto rischio da immettere sul mercato.

In caso di violazione, i requisiti consentiranno alle autorità nazionali di avere accesso alle informazioni necessarie per indagare se l'uso del sistema di IA sia conforme alla legge.

Quale sarebbe il ruolo della normazione nella legge sull'IA?

Ai sensi della legge sull'IA, i sistemi di IA ad alto rischio saranno soggetti a requisiti specifici. Le norme armonizzate europee svolgeranno un ruolo fondamentale nell'attuazione di tali requisiti.

Nel maggio 2023 la Commissione europea ha incaricato le organizzazioni europee di normazione CEN e CENELEC di elaborare norme per tali requisiti ad alto rischio. Tale mandato sarà ora modificato per

allinearlo al testo finale della legge sull'IA.

Le organizzazioni europee di normazione avranno tempo fino alla fine di aprile 2025 per elaborare e pubblicare norme. La Commissione valuterà ed eventualmente approverà tali norme, che saranno pubblicate nella Gazzetta ufficiale dell'UE. Una volta pubblicate, tali norme concederanno una "presunzione di conformità" ai sistemi di IA sviluppati in conformità delle stesse.

Come vengono regolamentati i modelli di IA per finalità generali?

I **modelli di IA per finalità generali**, compresi i **grandi modelli di IA generativa**, possono essere utilizzati per una serie di compiti. I singoli modelli possono essere integrati in un gran numero di sistemi di IA.

È fondamentale che un fornitore di un sistema di IA che integra un modello di IA per finalità generali abbia accesso a tutte le informazioni necessarie per garantire che il sistema sia sicuro e conforme alla legge sull'IA.

La legge sull'IA obbliga pertanto i fornitori di tali modelli a **divulgare determinate informazioni ai fornitori di sistemi a valle**. Tale **trasparenza** consente una migliore comprensione di tali modelli.

I fornitori di modelli devono inoltre disporre di politiche volte a garantire il **rispetto del diritto d'autore** nella formazione dei loro modelli.

Inoltre, alcuni di questi modelli potrebbero comportare **rischi sistemici**, in quanto sono molto capaci o ampiamente utilizzati.

Attualmente si ritiene che i modelli di IA per finalità generali formati utilizzando **una potenza di calcolo totale di oltre 10^{25} FLOP presentino** rischi sistemici. La Commissione può aggiornare o integrare tale soglia alla luce dei progressi tecnologici e può anche designare altri modelli che presentano rischi sistemici sulla base di ulteriori criteri (ad esempio il numero di utenti o il grado di autonomia del modello).

I fornitori di modelli con rischi sistemici sono tenuti a **valutare e attenuare i rischi**, a **segnalare gli incidenti gravi**, a **effettuare prove e valutazioni dei modelli all'avanguardia** e a garantire la **cybersicurezza** dei loro modelli.

I fornitori sono invitati a collaborare con l'Ufficio per l'IA e altri portatori di interessi per elaborare un codice di buone pratiche che specifichi le norme e garantisca in tal modo lo sviluppo sicuro e responsabile dei loro modelli. Tale codice dovrebbe rappresentare uno strumento centrale per i fornitori di modelli di IA per finalità generali per dimostrare la conformità.

Perché 10^{25} FLOP è una soglia adeguata per GPAI con rischi sistemici?

Flop è un indicatore delle capacità del modello e la soglia esatta del FLOP può essere aggiornata dalla Commissione al rialzo o al ribasso, ad esempio alla luce dei progressi compiuti nella misurazione obiettiva delle capacità del modello e degli sviluppi della potenza di calcolo necessaria per un determinato livello di prestazioni.

Le capacità dei modelli al di sopra di tale soglia non sono ancora sufficientemente comprese. Potrebbero comportare rischi sistemici, motivo per cui è ragionevole assoggettare i loro fornitori all'insieme aggiuntivo di obblighi.

Quali sono gli obblighi relativi alla filigrana e all'etichettatura dei risultati dell'IA stabiliti nella legge sull'IA?

La legge sull'IA stabilisce norme in materia di trasparenza per i contenuti prodotti dall'IA generativa al fine di affrontare il rischio di manipolazione, inganno e disinformazione.

Obbliga i fornitori di sistemi di IA generativi a contrassegnare gli output di IA in un formato leggibile meccanicamente e a garantire che siano rilevabili come generati o manipolati artificialmente. Le soluzioni tecniche devono essere efficaci, interoperabili, solide e affidabili nella misura in cui ciò sia tecnicamente fattibile, tenendo conto delle specificità e dei limiti dei vari tipi di contenuti, dei costi di attuazione e dello stato dell'arte generalmente riconosciuto, come possono riflettersi nelle norme tecniche pertinenti.

Inoltre, gli operatori di sistemi di IA generativa che generano o manipolano immagini o contenuti audio o video che costituiscono deep fake devono rivelare in modo visibile che il contenuto è stato generato o manipolato artificialmente. Gli operatori di un sistema di IA che genera o manipola testo pubblicato allo scopo di informare il pubblico su questioni di interesse pubblico devono anche rivelare che il testo è stato generato o manipolato artificialmente. Tale obbligo non si applica se il contenuto generato dall'IA è stato sottoposto a un processo di revisione umana o di controllo editoriale e se una

persona fisica o giuridica detiene la responsabilità editoriale della pubblicazione del contenuto.

L'Ufficio per l'IA pubblicherà orientamenti per fornire ulteriori orientamenti ai fornitori e agli operatori in merito agli obblighi di cui all'articolo 50, che saranno applicabili due anni dopo l'entrata in vigore della legge sull'IA (il 2 agosto 2026).

L'Ufficio per l'IA incoraggerà e agevolerà inoltre lo sviluppo di codici di buone pratiche a livello dell'Unione per razionalizzare l'efficace attuazione degli obblighi relativi all'individuazione e all'etichettatura dei contenuti generati artificialmente o manipolati.

La legge sull'IA è adeguata alle esigenze future?

La legge sull'IA stabilisce un quadro giuridico che risponde ai nuovi sviluppi, è facile e rapido da adattare e consente una valutazione frequente.

La legge sull'IA stabilisce requisiti e obblighi orientati ai risultati, ma lascia le soluzioni tecniche concrete e l'operatività alle norme e ai codici di condotta guidati dall'industria che sono flessibili per essere adattati ai diversi casi d'uso e consentire nuove soluzioni tecnologiche.

Inoltre, la legislazione stessa può essere modificata mediante atti delegati e di esecuzione, ad esempio per rivedere l'elenco dei casi d'uso ad alto rischio di cui all'allegato III.

Infine, vi saranno valutazioni frequenti di alcune parti della legge sull'IA e, in ultima analisi, dell'intero regolamento, garantendo che sia individuata l'eventuale necessità di revisione e modifica.

In che modo la legge sull'IA disciplina l'identificazione biometrica?

È vietato l'uso dell' **identificazione biometrica remota in tempo reale in spazi accessibili al pubblico** (ossia il riconoscimento facciale mediante CCTV) a fini di contrasto. Gli Stati membri possono introdurre eccezioni per legge che consentano l'uso dell'identificazione biometrica remota in tempo reale nei seguenti casi:

- Attività di contrasto relative a 16 reati molto gravi;
- Ricerca mirata di specifiche vittime, rapimento, tratta e sfruttamento sessuale di esseri umani e persone scomparse; oppure
- La prevenzione di una minaccia per la vita o l'incolumità fisica delle persone o la risposta alla minaccia attuale o prevedibile di un attacco terroristico.

Qualsiasi uso eccezionale sarebbe soggetto ad **autorizzazione preventiva da parte di un'autorità giudiziaria o amministrativa indipendente** la cui decisione è vincolante. In caso di urgenza, l'approvazione può essere concessa entro 24 ore; se l'autorizzazione è respinta, tutti i dati e i risultati devono essere cancellati.

Dovrebbe essere preceduta da una **valutazione preliminare dell'impatto sui diritti fondamentali** e dovrebbe essere **notificata all'autorità di vigilanza del mercato competente e all'autorità di protezione dei dati**. In caso di urgenza, l'uso del sistema può essere iniziato senza registrazione.

L'uso di sistemi di IA per **l'identificazione biometrica a distanza** (identificazione delle persone in materiale precedentemente raccolto) delle persone oggetto di indagine richiede l' **autorizzazione preventiva** di un'autorità giudiziaria o di un'autorità amministrativa indipendente, nonché la notifica all'autorità competente per la protezione dei dati e la vigilanza del mercato.

Perché sono necessarie regole particolari per l'identificazione biometrica remota?

L'identificazione biometrica può assumere varie forme. L'autenticazione e la verifica biometriche, ossia per sbloccare uno smartphone o per la verifica/autenticazione ai valichi di frontiera per verificare l'identità di una persona rispetto ai suoi documenti di viaggio (abbinamento uno a uno), rimangono non regolamentate, in quanto non rappresentano un rischio significativo per i diritti fondamentali.

Al contrario, l'identificazione biometrica può essere utilizzata anche a distanza, ad esempio per identificare le persone che si trovano in una folla che può avere un impatto significativo sulla vita privata nello spazio pubblico.

L'accuratezza dei sistemi di riconoscimento facciale può essere influenzata in modo significativo da un'ampia gamma di fattori, quali la qualità della fotocamera, la luce, la distanza, la banca dati, l'algoritmo e l'etnia, l'età o il genere del soggetto. Lo stesso vale per il riconoscimento vocale e dell'andatura e per altri sistemi biometrici. Il tasso di falsi positivi dei sistemi altamente avanzati è in continua diminuzione.

Sebbene un tasso di accuratezza del 99 % possa sembrare positivo in generale, è molto rischioso quando il risultato può portare al sospetto di una persona innocente. Anche un tasso di errore del 0,1 % può avere un impatto significativo se applicato a grandi popolazioni, ad esempio nelle stazioni ferroviarie.

In che modo le regole tutelano i diritti fondamentali?

Esiste già una forte protezione dei diritti fondamentali e della non discriminazione a livello dell'UE e degli Stati membri, ma la complessità e l'opacità di alcune applicazioni di IA ("scatole nere") possono rappresentare un problema.

Un approccio antropocentrico all'IA significa garantire che le applicazioni di IA rispettino la legislazione in materia di diritti fondamentali. Integrando i requisiti di responsabilità e trasparenza nello sviluppo di sistemi di IA ad alto rischio e migliorando le capacità di applicazione delle norme, possiamo garantire che tali sistemi siano progettati tenendo presente la conformità giuridica fin dall'inizio. Qualora si verificassero delle violazioni, tali requisiti consentirebbero alle autorità nazionali di avere accesso alle informazioni necessarie per indagare se l'IA è stata usata in modo conforme al diritto dell'UE.

Inoltre, la legge sull'IA prevede che alcuni operatori di sistemi di IA ad alto rischio effettuino una valutazione d'impatto sui diritti fondamentali.

Cos'è una valutazione d'impatto sui diritti fondamentali? Chi deve effettuare tale valutazione e quando?

I fornitori di sistemi di IA ad alto rischio devono effettuare una valutazione dei rischi e progettare il sistema in modo da ridurre al minimo i rischi per la salute, la sicurezza e i diritti fondamentali.

Tuttavia, alcuni rischi per i diritti fondamentali possono essere pienamente identificati solo a conoscenza del contesto di utilizzo del sistema di IA ad alto rischio. Quando i sistemi di IA ad alto rischio sono utilizzati in settori particolarmente sensibili di possibile asimmetria di potenza, sono necessarie ulteriori considerazioni in merito a tali rischi.

Pertanto, gli operatori che sono organismi di diritto pubblico o operatori privati che forniscono servizi pubblici, nonché gli operatori che forniscono sistemi di IA ad alto rischio che effettuano valutazioni del merito creditizio o valutazioni del prezzo e del rischio nell'assicurazione vita e malattia, effettuano una valutazione dell'impatto sui diritti fondamentali e notificano i risultati all'autorità nazionale.

In pratica, molti operatori dovranno anche effettuare una valutazione d'impatto sulla protezione dei dati. Per evitare sovrapposizioni sostanziali in tali casi, la valutazione d'impatto sui diritti fondamentali è condotta congiuntamente a tale valutazione d'impatto sulla protezione dei dati.

In che modo questo regolamento affronta le distorsioni nell'IA legate al genere o alla razza?

È molto importante sottolineare che i sistemi di **IA non creano o riproducono distorsioni**. Piuttosto, se adeguatamente progettati e utilizzati, i **sistemi di IA possono contribuire a ridurre le distorsioni e le discriminazioni strutturali esistenti**, portando così a decisioni più eque e non discriminatorie (ad esempio nelle assunzioni).

I nuovi requisiti obbligatori per tutti i sistemi di IA ad alto rischio serviranno a questo. I sistemi di IA devono essere **tecnicamente solidi** per garantire che siano adatti allo scopo e non producano risultati distorti, quali falsi positivi o negativi, che colpiscono in modo sproporzionato i gruppi emarginati, compresi quelli basati sull'origine razziale o etnica, sul sesso, sull'età e su altre caratteristiche protette.

I sistemi ad alto rischio dovranno inoltre essere **addestrati e testati con serie di dati sufficientemente rappresentative** per **ridurre al minimo il rischio di distorsioni inique** incorporate nel modello e garantire che tali distorsioni possano essere affrontate mediante adeguate misure di individuazione, correzione e altre misure di attenuazione dei pregiudizi.

Devono inoltre essere **tracciabili e verificabili**, garantendo che **sia conservata una documentazione** adeguata, compresi i dati utilizzati per addestrare l'algoritmo che sarebbero fondamentali nelle indagini ex post.

Il sistema di verifica della conformità prima e dopo l'immissione sul mercato dovrà garantire che tali sistemi siano **regolarmente monitorati** e che **i rischi potenziali siano prontamente affrontati**.

Quando sarà pienamente applicabile la legge sull'IA?

La legge sull'IA si applicherà due anni dopo l'entrata in vigore il 2 agosto 2026, ad eccezione delle seguenti disposizioni specifiche:

- I divieti, le definizioni e le disposizioni relativi all'alfabetizzazione in materia di IA si applicheranno 6 mesi dopo l'entrata in vigore, il 2 febbraio 2025;
- Le norme in materia di governance e gli obblighi per l'IA per finalità generali diventano applicabili 12 mesi dopo l'entrata in vigore, il 2 agosto 2025;
- Gli obblighi per i sistemi di IA ad alto rischio che si classificano come ad alto rischio perché incorporati in prodotti regolamentati, elencati nell'allegato II (elenco della normativa di armonizzazione dell'Unione), si applicano 36 mesi dopo l'entrata in vigore del 2 agosto 2027.

Come sarà applicata la legge sull'IA?

La legge sull'IA istituisce un sistema di governance a due livelli, in cui le **autorità nazionali** sono responsabili della supervisione e dell'applicazione delle norme per i sistemi di IA, mentre il livello dell'UE è responsabile della regolamentazione dei modelli di IA per finalità generali.

Per garantire la coerenza e la cooperazione a livello dell'UE, sarà istituito il **comitato europeo per l'intelligenza artificiale** (comitato per l'IA), composto da rappresentanti degli Stati membri, con sottogruppi specializzati per le autorità nazionali di regolamentazione e altre autorità competenti.

L' **Ufficio per l'IA**, l'organismo di attuazione della legge sull'IA della Commissione, fornirà orientamenti strategici al comitato per l'IA.

Inoltre, la legge sull'IA istituisce due organi consultivi per fornire contributi di esperti: il **gruppo di esperti scientifici** e il **forum consultivo**. Tali organismi offriranno informazioni preziose da parte dei portatori di interessi e delle comunità scientifiche interdisciplinari, informeranno il processo decisionale e garantiranno un approccio equilibrato allo sviluppo dell'IA.

Perché è necessario un comitato europeo per l'intelligenza artificiale e cosa farà?

Il comitato europeo per l'intelligenza artificiale comprende **rappresentanti di alto livello degli Stati membri** e del Garante europeo della protezione dei dati. In qualità di consulente principale, il comitato per l'IA fornisce orientamenti su tutte le questioni relative alla politica in materia di IA, in particolare la regolamentazione dell'IA, la politica in materia di innovazione ed eccellenza e la cooperazione internazionale in materia di IA.

Il comitato per l'IA svolge un ruolo cruciale nel garantire un'attuazione agevole, efficace e armonizzata della legge sull'IA. Il comitato fungerà da forum in cui le autorità di regolamentazione dell'IA, vale a dire l'ufficio per l'IA, le autorità nazionali e l'EPDS, possono coordinare l'applicazione coerente della legge sull'IA.

Quali sono le sanzioni in caso di violazione?

Gli Stati membri dovranno stabilire sanzioni effettive, proporzionate e dissuasive in caso di violazione delle norme relative ai sistemi di IA.

Il regolamento stabilisce le soglie da tenere in considerazione:

- **Fino a 35 milioni di EUR o al 7 %** del fatturato mondiale totale annuo dell'esercizio precedente (se superiore) per violazioni **relative a pratiche vietate o per l'inosservanza** di requisiti in materia di dati;
- **Fino a 15 milioni di EUR o al 3 %** del fatturato mondiale totale annuo dell'esercizio precedente per **l'inosservanza di qualsiasi altro** requisito o obbligo del regolamento;
- **Fino a 7.5 milioni di EUR o al 1,5 %** del fatturato mondiale totale annuo dell'esercizio precedente per la **fornitura di informazioni inesatte, incomplete o fuorvianti** agli organismi notificati e alle autorità nazionali competenti in risposta a una richiesta;
- Per ciascuna categoria di infrazione, la soglia sarebbe quella più bassa tra i due importi per le PMI e quella più elevata per le altre imprese.

La Commissione può inoltre applicare le norme sui fornitori di modelli di IA per finalità generali mediante sanzioni pecuniarie, tenendo conto della seguente soglia:

- **Fino a 15 milioni di EUR o al 3 %** del fatturato mondiale totale annuo dell'esercizio precedente per **inosservanza di uno qualsiasi degli obblighi** o delle misure richiesti dalla Commissione a norma del regolamento.

Le istituzioni, le agenzie o gli organi dell'UE dovrebbero dare l'esempio, ragion per cui saranno

soggetti anche alle norme e alle eventuali sanzioni. Il Garante europeo della protezione dei dati avrà il potere di imporre sanzioni pecuniarie in caso di inosservanza.

Come sarà scritto il codice di buone pratiche in materia di IA per finalità generali?

L'elaborazione del primo codice segue un processo inclusivo e trasparente. Sarà istituita una plenaria sul codice di buone pratiche per facilitare il processo di redazione iterativa, composto da tutti i fornitori di modelli di IA per finalità generali interessati e ammissibili, dai fornitori a valle che integrano un modello di IA per finalità generali nel loro sistema di IA, da altre organizzazioni del settore, da altre organizzazioni di portatori di interessi quali la società civile o le organizzazioni dei titolari dei diritti, nonché dal mondo accademico e da altri esperti indipendenti.

L'Ufficio per l'IA ha pubblicato un invito a manifestare interesse a partecipare all'elaborazione del primo codice di buone pratiche. Parallelamente al presente invito a manifestare interesse è avviata una consultazione multilaterale per raccogliere i pareri e i contributi di tutte le parti interessate sul primo codice di buone pratiche. Le risposte e le osservazioni costituiranno la base della prima iterazione redazionale del codice di buone pratiche. Fin dall'inizio, il codice si basa pertanto su un'ampia gamma di prospettive e competenze.

La plenaria sarà strutturata in quattro gruppi di lavoro per consentire discussioni mirate su temi specifici pertinenti per specificare gli obblighi per i fornitori di modelli di IA per finalità generali e di modelli di IA per finalità generali con rischio sistemico. I partecipanti alla plenaria sono liberi di scegliere uno o più gruppi di lavoro in cui desiderano partecipare. Le riunioni si svolgono esclusivamente online.

L'ufficio per l'IA nominerà presidenti e, se del caso, vicepresidenti per ciascuno dei quattro gruppi di lavoro della plenaria, selezionati tra gli esperti indipendenti interessati. I presidenti sintetizzeranno i contributi e le osservazioni dei partecipanti alla plenaria per elaborare iterativamente il primo codice di buone pratiche.

In quanto principali destinatari del codice, i fornitori di modelli di IA per finalità generali saranno invitati a seminari dedicati per contribuire a informare ciascun ciclo di redazione iterativa, oltre alla loro partecipazione alla plenaria.

Dopo 9 mesi, la versione definitiva del primo codice di buone pratiche sarà presentata in sessione plenaria conclusiva, prevista per aprile, e pubblicata. La plenaria conclusiva offre ai fornitori di modelli di IA per finalità generali l'opportunità di esprimere se intendono utilizzare il codice.

Se approvato, in che modo il codice di buone pratiche per i fornitori di modelli di IA per finalità generali funge da strumento centrale per la conformità?

Al termine del processo di elaborazione del codice, l'Ufficio per l'IA e il comitato per l'IA valuteranno l'adeguatezza del codice e pubblicheranno la loro valutazione. A seguito di tale valutazione, la Commissione può decidere di approvare un codice di buone pratiche e conferirgli la validità generale all'interno dell'Unione mediante atti di esecuzione. Se entro il momento in cui il regolamento diventa applicabile il codice di buone pratiche non è ritenuto adeguato dall'Ufficio per l'IA, la Commissione può stabilire norme comuni per l'attuazione dei pertinenti obblighi.

I fornitori di modelli di IA per finalità generali possono pertanto basarsi sul codice di buone pratiche per dimostrare il rispetto degli obblighi stabiliti dalla legge sull'IA.

Ai sensi della legge sull'IA, il codice di buone pratiche dovrebbe includere obiettivi, misure e, se del caso, indicatori chiave di prestazione (ICP).

I fornitori che aderiscono al codice dovrebbero riferire periodicamente all'Ufficio per l'IA in merito all'attuazione delle misure adottate e ai loro risultati, se del caso anche sulla base di indicatori chiave di prestazione.

Ciò facilita l'applicazione da parte dell'Ufficio per l'IA, che è sostenuto dai poteri conferiti alla Commissione dalla legge sull'IA. Ciò comprende la capacità di effettuare valutazioni dei modelli di IA per finalità generali, di richiedere informazioni e misure ai fornitori di modelli e di applicare sanzioni.

L'Ufficio per l'IA incoraggerà e agevererà, se del caso, la revisione e l'adeguamento del codice per tenere conto dei progressi tecnologici e dello stato dell'arte.

Una volta che una norma armonizzata è stata pubblicata e giudicata idonea a coprire i pertinenti obblighi dell'Ufficio per l'IA, la conformità a una norma armonizzata europea dovrebbe conferire ai fornitori la presunzione di conformità.

I fornitori di modelli di IA per finalità generali dovrebbero inoltre essere in grado di dimostrare la conformità utilizzando mezzi adeguati alternativi, se non sono disponibili codici di pratica o norme armonizzate, o se scelgono di non fare affidamento su di essi.

La legge sull'IA contiene disposizioni in materia di protezione dell'ambiente e sostenibilità?

L'obiettivo della proposta sull'IA è affrontare i rischi per la sicurezza e i diritti fondamentali, compreso il diritto fondamentale a un elevato livello di protezione dell'ambiente. L'ambiente è anche uno degli interessi giuridici esplicitamente menzionati e tutelati.

La Commissione è invitata a chiedere alle organizzazioni europee di normazione di produrre un prodotto della normazione sui processi di rendicontazione e documentazione per migliorare le prestazioni dei sistemi di IA in termini di risorse, come la riduzione del consumo di energia e di altre risorse del sistema di IA ad alto rischio durante il suo ciclo di vita, e sullo sviluppo efficiente sotto il profilo energetico di modelli di IA per finalità generali.

Inoltre, entro due anni dalla data di applicazione del regolamento e successivamente ogni quattro anni, la Commissione è invitata a presentare una relazione sull'esame dei progressi compiuti nello sviluppo dei prodotti della normazione relativi allo sviluppo efficiente sotto il profilo energetico dei modelli generali e valuta la necessità di ulteriori misure o azioni, comprese misure o azioni vincolanti.

Inoltre, i fornitori di modelli di IA per finalità generali, formati su grandi quantità di dati e quindi soggetti a un elevato consumo di energia, sono tenuti a comunicare il consumo energetico. Nel caso di modelli di IA per finalità generali con rischi sistemici, è inoltre necessario valutare l'efficienza energetica.

Alla Commissione è conferito il potere di elaborare una metodologia di misurazione adeguata e comparabile per tali obblighi di informativa.

In che modo le nuove regole possono sostenere l'innovazione?

Il quadro normativo può contribuire a una maggiore adozione dell'IA in due modi. Da un lato, l'aumento della fiducia degli utenti farà crescere la domanda di IA utilizzata dalle imprese e dalle autorità pubbliche. Dall'altro, la maggiore certezza del diritto e l'armonizzazione delle regole consentiranno ai fornitori di IA di accedere a mercati più grandi, con prodotti che gli utenti e i consumatori apprezzano e acquistano. Le regole si applicheranno solo laddove strettamente necessario e in modo da ridurre al minimo l'onere per gli operatori economici, con una struttura di governance leggera.

La legge sull'IA consente inoltre la creazione di spazi di **sperimentazione normativa** e di **prove in condizioni reali**, che forniscono un ambiente controllato per testare tecnologie innovative per un periodo di tempo limitato, promuovendo in tal modo l'innovazione da parte delle imprese, delle PMI e delle start-up conformemente alla legge sull'IA. Queste, insieme ad altre misure quali le ulteriori **reti di centri di eccellenza per l'IA e il partenariato pubblico-privato sull'intelligenza artificiale, i dati e la robotica, e l'accesso ai poli dell'innovazione digitale** e alle strutture di **prova e sperimentazione contribuiranno** a creare le giuste condizioni quadro per lo sviluppo e la diffusione dell'IA da parte delle imprese.

Le prove in condizioni reali dei sistemi di IA ad alto rischio possono essere effettuate per un massimo di 6 mesi (prorogabili di altri 6 mesi). Prima delle prove è necessario elaborare un piano e presentarlo all'autorità di vigilanza del mercato, che deve approvare il piano e le condizioni di prova specifiche, con approvazione tacita predefinita se non è stata data risposta entro 30 giorni. Le prove possono essere soggette a ispezioni senza preavviso da parte dell'autorità.

I test del mondo reale possono essere effettuati solo in presenza di garanzie specifiche: ad esempio, gli utenti dei sistemi sottoposti a test devono fornire il consenso informato, i test non devono avere alcun effetto negativo su di essi, i risultati devono essere reversibili o disattivabili e i loro dati devono essere cancellati dopo la conclusione del test. Una protezione speciale deve essere concessa ai gruppi vulnerabili, ad esempio a causa della loro età o della loro disabilità fisica o mentale.

Quale ruolo svolge il patto per l'IA nell'attuazione della legge sull'IA?

Avviato dal commissario Breton nel maggio 2023, il patto per l'IA mira a rafforzare l'impegno tra l'Ufficio per l'IA e le organizzazioni (pilastro I) e a incoraggiare l'impegno volontario del settore a iniziare ad attuare i requisiti della legge sull'IA prima del termine legale (secondo pilastro).

In particolare, nell'ambito del primo pilastro, i partecipanti contribuiranno alla creazione di una comunità collaborativa, condividendo le loro esperienze e conoscenze. Ciò comprende seminari organizzati dall'Ufficio per l'IA che forniscono ai partecipanti una migliore comprensione della legge

sull'IA, delle loro responsabilità e di come prepararsi alla sua attuazione. A sua volta, l'Ufficio per l'IA può raccogliere informazioni sulle migliori pratiche e sulle sfide cui devono far fronte i partecipanti.

Nell'ambito del secondo pilastro, le organizzazioni sono incoraggiate a divulgare proattivamente i processi e le pratiche che stanno attuando per anticipare la conformità, attraverso impegni volontari. Gli impegni sono intesi come "dichiarazioni di impegno" e conterranno azioni (pianificate o in corso) per soddisfare alcuni requisiti della legge sull'IA.

La maggior parte delle norme della legge sull'IA (ad esempio, alcuni requisiti relativi ai sistemi di IA ad alto rischio) si applicherà alla fine di un periodo transitorio (ossia il periodo che intercorre tra l'entrata in vigore e la data di applicabilità).

In tale contesto e nel quadro del patto per l'IA, l'Ufficio per l'IA invita tutte le organizzazioni ad anticipare e attuare proattivamente alcune delle disposizioni fondamentali della legge sull'IA, con l'obiettivo di attenuare quanto prima i rischi per la salute, la sicurezza e i diritti fondamentali.

Oltre 700 organizzazioni hanno già espresso il loro interesse ad aderire all'iniziativa del patto per l'IA, a seguito di un invito lanciato nel novembre 2023. Una prima sessione informativa si è tenuta online il 6 maggio, con 300 partecipanti. La firma ufficiale degli impegni volontari è prevista per l'autunno 2024. Nella prima settimana di settembre si terrà un seminario sul patto per l'IA.

Qual è la dimensione internazionale dell'approccio dell'UE?

L'IA ha conseguenze e sfide che vanno oltre i confini; pertanto, la cooperazione internazionale è importante. L'Ufficio per l'IA è responsabile dell'impegno internazionale dell'Unione europea nel settore dell'IA, sulla base della legge sull'IA e del piano coordinato sull'IA. L'UE mira a promuovere la gestione responsabile e la buona governance dell'IA in collaborazione con i partner internazionali e in linea con il sistema multilaterale basato su regole e i valori che esso difende.

L'UE si impegna a livello bilaterale e multilaterale per promuovere un'IA affidabile, antropocentrica ed etica. Di conseguenza, l'UE partecipa a forum multilaterali in cui si discute dell'IA — in particolare il G7, il G20, l'OCSE, il Consiglio d'Europa, il partenariato globale sull'IA e le Nazioni Unite — e l'UE intrattiene stretti legami bilaterali, ad esempio con Canada, Stati Uniti, India, Giappone, Corea del Sud, Singapore e la regione dell'America latina e dei Caraibi.

* *Aggiornato il 01/08/2024*

QANDA/21/1683

Contatti per la stampa:

[Thomas Regnier](#) (+32 2 29 9 1099)

[Patricia Poropat](#) (+32 2 298 04 85)

Informazioni al pubblico: contattare [Europe Direct](#) telefonicamente allo [00 800 67 89 10 11](tel:0080067891011) o per [e-mail](#)