Intelligenza artificiale — Domande e risposte*

Brussels, 1° agosto 2024

Perché è necessario regolamentare l'uso dell'intelligenza artificiale?

La legge dell'Unione europea sull'IA è la prima legge completa in materia di IA al mondo e mira ad affrontare i rischi per la salute, la sicurezza e i diritti fondamentali. Il regolamento tutela inoltre 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. In determinati casi le caratteristiche specifiche di alcuni sistemi di IA possono tuttavia creare nuovi rischi per quanto riguarda la sicurezza, anche fisica, degli utenti e i diritti fondamentali. Alcuni potenti modelli di IA il cui utilizzo è molto diffuso potrebbero persino comportare rischi sistemici.

Ciò determina una mancanza di certezza del diritto e un'adozione potenzialmente più lenta delle tecnologie di IA da parte delle autorità pubbliche, dovuta alla mancanza di fiducia. Risposte normative disuguali da parte delle autorità nazionali rischierebbero di frammentare il mercato interno.

Per rispondere a queste sfide era necessaria un'azione legislativa che garantisse il buon funzionamento del mercato interno per i sistemi di IA e tenesse adeguatamente conto sia dei benefici sia dei rischi.

A chi si applica la legge sull'IA?

Il quadro giuridico si applicherà ai soggetti pubblici e privati, all'interno e all'esterno dell'UE, a condizione che il **sistema di IA** sia immesso sul mercato dell'Unione o che il suo utilizzo abbia effetti su persone situate nell'UE.

Gli obblighi possono riguardare sia i fornitori (ad esempio, uno sviluppatore di uno strumento di screening dei CV) sia i deployer di sistemi di IA (ad esempio, una banca che acquista il suddetto strumento di screening). Il regolamento prevede alcune deroghe. Le attività di ricerca, sviluppo e prototipazione che hanno luogo prima dell'immissione sul mercato di un sistema di IA non sono soggette a tali regolamenti. Sono inoltre esenti 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 di IA che guarda al futuro e su un approccio basato sul rischio:

- **rischio inaccettabile**: una serie molto limitata di usi dell'IA particolarmente dannosi, che contravvengono ai valori dell'UE perché violano i diritti fondamentali e che saranno pertanto vietati:
  - **sfruttamento delle vulnerabilità delle persone, manipolazione e utilizzo di tecniche subliminali;**
  - **punteggio sociale** per finalità pubbliche e private;
  - **attività di polizia predittiva individuale** basate **unicamente sulla profilazione delle persone**;
  - **scraping non mirato** di immagini facciali da internet o telecamere a circuito chiuso per la creazione o l'ampliamento di banche dati;
  - **riconoscimento delle emozioni sul luogo di lavoro e negli istituti di istruzione**, eccetto per motivi medici o di sicurezza (ad esempio il monitoraggio dei livelli di stanchezza di un pilota);
  - **categorizzazione biometrica** delle persone fisiche sulla base di dati biometrici per

trarre deduzioni o inferenze in merito a razza, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche o orientamento sessuale. Sarà ancora possibile etichettare o filtrare set di dati e categorizzare i dati nell'ambito delle attività di contrasto;

- **identificazione biometrica remota in tempo reale in spazi accessibili al pubblico da parte delle autorità di contrasto**, fatte salve limitate eccezioni (v. sotto);

- la Commissione pubblicherà orientamenti sui divieti prima della loro entrata in vigore il 2 febbraio 2025;
- **rischio alto**: è considerato ad alto rischio un numero limitato di sistemi di IA definiti nella proposta, che possono potenzialmente avere ripercussioni negative sulla sicurezza delle persone o sui loro diritti fondamentali (tutelati dalla Carta dei diritti fondamentali dell'UE). Al regolamento è allegato l'elenco dei sistemi di IA ad alto rischio, che può essere riveduto per allinearsi all'evoluzione dei casi d'uso dell'IA;
- tali sistemi comprendono anche i componenti di sicurezza dei prodotti disciplinati dalla legislazione settoriale dell'Unione, che saranno sempre considerati ad alto rischio se 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, i sistemi di IA che valutano se qualcuno può 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). Potrebbero essere ad alto rischio anche i sistemi di IA che gestiscono robot, droni o dispositivi medici;
- **rischio specifico per la trasparenza**: per promuovere la fiducia, è importante garantire la trasparenza sull'uso dell'IA. Pertanto la legge sull'IA introduce specifici obblighi di trasparenza per determinate applicazioni di IA, ad esempio laddove esista un evidente rischio di manipolazione (ad esempio, attraverso l'uso di chatbot) o di deep fake, affinché gli utenti siano consapevoli del fatto che stanno interagendo con una macchina;
- **rischio minimo**: la maggioranza dei sistemi di IA possono essere sviluppati e utilizzati 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.

La legge sull'IA prende inoltre 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 un'ampia serie di compiti e stanno diventando la base di molti sistemi di IA nell'UE. Alcuni di questi modelli potrebbero comportare rischi sistemici se risultano particolarmente efficaci o molto utilizzati. Modelli potenti potrebbero ad esempio causare incidenti gravi o essere utilizzati impropriamente per attacchi informatici di vasta portata. Se un modello propagasse distorsioni dannose in molte applicazioni, le persone colpite potrebbero essere molte.

Come 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 dalle finalità e modalità specifiche di utilizzo di tale sistema.

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

- se il sistema di IA è integrato come componente di sicurezza in prodotti disciplinati dalla legislazione vigente in materia di prodotti (allegato I) o costituisce esso stesso un simile prodotto. Questo potrebbe essere, ad esempio, il caso 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, tra quelli elencati nell'allegato III della legge sull'IA. L'elenco comprende casi d'uso provenienti da settori quali l'istruzione, l'occupazione, le attività di contrasto 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 definiti nell'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 è classificato come ad alto rischio se

è destinato a essere utilizzato in uno di questi casi d'uso.

Alcuni esempi sono:

- 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 nel settore dell'istruzione e formazione professionale**, ad esempio per valutare i risultati dell'apprendimento, orientare il processo di apprendimento e monitorare i comportamenti disonesti;
- **sistemi di IA utilizzati nei settori dell'occupazione, della gestione dei lavoratori** e dell'accesso al lavoro autonomo, ad esempio per pubblicare annunci di lavoro mirati, analizzare e filtrare le candidature e valutare i candidati;
- **sistemi di IA utilizzati per l'accesso a servizi e a prestazioni pubblici e privati essenziali** (ad esempio l'assistenza sanitaria), la **valutazione dell'affidabilità creditizia** delle persone fisiche e la valutazione dei rischi e la determinazione dei prezzi in relazione ad **assicurazioni sulla vita e assicurazioni sanitarie**;
- sistemi di IA utilizzati nei settori delle **attività di contrasto**, della migrazione e del **controllo delle frontiere**, nella misura in cui sono consentiti, nonché nell'amministrazione della **giustizia** e nei **processi democratici**;
- sistemi di IA utilizzati per **l'identificazione biometrica, la categorizzazione biometrica e il riconoscimento delle emozioni**, nella misura in cui sono consentiti.

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 metterlo in servizio, i fornitori devono sottoporlo a una **valutazione della conformità**. Potranno così dimostrare che il loro sistema è conforme ai requisiti obbligatori per un'IA affidabile (ad esempio qualità dei dati, documentazione e tracciabilità, trasparenza, sorveglianza umana, accuratezza, cibersicurezza e robustezza). Tale valutazione deve essere ripetuta in caso di modifica sostanziale del sistema o della sua finalità.

I sistemi di IA che fungono da componenti di sicurezza di prodotti disciplinati dalla legislazione settoriale dell'Unione saranno sempre considerati ad alto rischio se soggetti a una 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 **implementare 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 che un prodotto è stato immesso sul mercato.

I sistemi di IA ad alto rischio utilizzati da autorità pubbliche o entità 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. Questi ultimi sistemi dovranno essere registrati 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 le norme, che saranno quindi valutate ed eventualmente approvate dalla Commissione e pubblicate nella Gazzetta ufficiale dell'UE. Una volta pubblicate, tali norme garantiranno una "presunzione di conformità" ai sistemi di IA sviluppati in conformità alle stesse.

Come sono 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 vari 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 suo sistema sia sicuro e conforme alla legge sull'IA.

La legge sull'IA obbliga di conseguenza i fornitori di tali modelli a **comunicare determinate informazioni ai fornitori di sistemi a valle**. Una siffatta **trasparenza** rende possibile una migliore comprensione di tali modelli.

È altresì necessario che i fornitori di modelli dispongano di politiche in essere atte a garantire il **rispetto del diritto d'autore** nel corso dell'addestramento dei loro modelli.

Alcuni di questi modelli potrebbero inoltre comportare **rischi sistemici**, in quanto particolarmente efficaci o molto utilizzati.

Attualmente si ritiene che i modelli di IA per finalità generali addestrati utilizzando una **potenza di calcolo totale di oltre 10^25 FLOPS** presentino rischi sistemici. La Commissione può aggiornare o integrare tale soglia alla luce dell'evoluzione tecnologica e può inoltre designare altri modelli che ritiene presentino rischi sistemici sulla base di ulteriori criteri (ad esempio il numero di utenti o il grado di autonomia del modello).

I fornitori di modelli che presentano rischi sistemici sono tenuti a **valutare e attenuare i rischi**, **segnalare incidenti gravi**, **condurre prove e valutazioni all'avanguardia dei modelli** e garantire la **cibersicurezza** degli stessi.

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 regole e garantisca così 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 al fine di dimostrarne la conformità.

Per quale motivo 10^25 FLOPS è una soglia adeguata per l'IA per finalità generali con rischi sistemici?

Il FLOPS è un indicatore delle capacità del modello e la soglia FLOPS esatta può essere aggiornata al rialzo o al ribasso dalla Commissione, ad esempio alla luce dei progressi nella misurazione obiettiva delle capacità dei modelli e dell'evoluzione della potenza di calcolo necessaria per un determinato livello di prestazione.

Le capacità dei modelli al di sopra di tale soglia non sono ancora sufficientemente comprese: potrebbero comportare rischi sistemici ed è pertanto ragionevole imporre l'insieme aggiuntivo di obblighi ai loro fornitori.

Quali sono gli obblighi relativi all'aggiunta di filigrane digitali e all'etichettatura dell'output 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.

Essa obbliga i fornitori di sistemi di IA generativa a contrassegnare gli output dell'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 possibile, tenendo conto delle specificità e dei limiti dei vari tipi di contenuti, dei costi di attuazione e dello stato dell'arte generalmente riconosciuto, come eventualmente indicato nelle pertinenti norme tecniche.

I deployer dei sistemi di IA generativa che generano o manipolano immagini o contenuti audio o video che costituiscono un "deep fake" devono inoltre rendere noto in modo visibile che il contenuto è stato generato o manipolato artificialmente. I deployer di un sistema di IA che genera o manipola testo pubblicato allo scopo di informare il pubblico su questioni di interesse pubblico devono anche rendere noto 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 una persona fisica o giuridica detiene la responsabilità editoriale della pubblicazione del contenuto.

L'ufficio per l'IA pubblicherà orientamenti per fornire un'ulteriore guida ai fornitori e ai deployer 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).

Inoltre l'ufficio per l'IA incoraggerà e agevolerà l'elaborazione di codici di buone pratiche a livello dell'Unione per facilitare l'efficace attuazione degli obblighi relativi alla rilevazione e all'etichettatura dei contenuti generati o manipolati artificialmente.

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.

Essa stabilisce requisiti e obblighi orientati ai risultati, ma affida la definizione delle soluzioni tecniche e di livello operativo concrete alle norme e ai codici di buone pratiche determinati dall'industria, che dispongono della flessibilità necessaria per essere adattati ai diversi casi d'uso e rendere possibili nuove soluzioni tecnologiche.

La legislazione stessa può inoltre 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.

Determinate parti della legge sull'IA e, in ultima analisi, l'intero regolamento, saranno infine oggetto di valutazioni frequenti, garantendo che siano individuate eventuali necessità di revisione e modifica.

Come è disciplinata l'identificazione biometrica nella legge sull'IA?

L'uso dell'**identificazione biometrica remota in tempo reale** **in spazi accessibili al pubblico** (ossia il riconoscimento facciale mediante telecamere a circuito chiuso) a fini di attività di contrasto è vietato. Gli Stati membri possono introdurre nel loro diritto eccezioni che consentano l'uso dell'identificazione biometrica remota in tempo reale nei seguenti casi:

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

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

L'autorizzazione dovrebbe essere preceduta da una **valutazione preventiva d'impatto sui diritti fondamentali** e dovrebbe essere **notificata alle pertinenti autorità di vigilanza del mercato e autorità per la protezione dei dati**. In situazioni di urgenza, è possibile iniziare a usare il sistema senza registrazione.

L'uso di sistemi di IA per l'**identificazione biometrica remota a posteriori** (identificazione di persone in materiale raccolto in precedenza) delle persone oggetto di indagine richiede l'**autorizzazione preventiva** da parte di un'autorità giudiziaria o di un'autorità amministrativa indipendente, nonché la notifica all'autorità per la protezione dei dati e all'autorità di 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, ad esempio per sbloccare uno smartphone o per la verifica/autenticazione ai valichi di frontiera dell'identità di una persona rispetto ai suoi documenti di viaggio (corrispondenza "uno a uno"), rimangono non regolamentate, in quanto non rappresentano un rischio significativo per i diritti fondamentali.

L'identificazione biometrica può essere utilizzata anche a distanza, ad esempio per identificare le persone in una folla, e ciò, al contrario, può avere un impatto significativo sulla tutela della vita privata nello spazio pubblico.

L'accuratezza dei sistemi per il riconoscimento facciale può essere significativamente influenzata 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 sesso 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.

Tuttavia se un tasso di accuratezza del 99% può sembrare buono in generale, esso è notevolmente rischioso quando il risultato può condurre a sospettare di una persona innocente. Anche un tasso di errore dello 0,1% può avere un impatto significativo se applicato a un gran numero di persone, ad esempio nelle stazioni ferroviarie.

In che modo le regole tutelano i diritti fondamentali?

A livello dell'UE e degli Stati membri esiste già una forte tutela dei diritti fondamentali e della non discriminazione, ma la complessità e l'opacità di determinate applicazioni di IA (le cosiddette "scatole nere") possono porre 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 della legislazione, possiamo garantire che tali sistemi siano progettati sin dall'inizio tenendo conto del rispetto degli obblighi normativi. Qualora si verifichino delle violazioni, tali requisiti consentiranno alle autorità nazionali di avere accesso alle informazioni necessarie per indagare se l'IA è stata usata in modo conforme al diritto dell'UE.

La legge sull'IA prevede inoltre che alcuni deployer 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? Quando deve essere effettuata?

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 individuati solo conoscendo il contesto di utilizzo del sistema di IA ad alto rischio. Quando i sistemi di IA ad alto rischio sono utilizzati in settori particolarmente sensibili in cui possono verificarsi asimmetrie di potere, tali rischi vanno tenuti ulteriormente in considerazione.

Pertanto i deployer che sono organismi di diritto pubblico o gli operatori privati che forniscono servizi pubblici, nonché gli operatori che forniscono sistemi di IA ad alto rischio che effettuano valutazioni dell'affidabilità creditizia o valutazioni dei rischi e determinazione dei prezzi per assicurazioni sulla vita e assicurazioni sanitarie, devono effettuare una valutazione d'impatto sui diritti fondamentali e comunicarne i risultati all'autorità nazionale.

Nella pratica anche molti deployer dovranno effettuare una valutazione d'impatto sulla protezione dei dati. In tali casi, per evitare sovrapposizioni sostanziali, la valutazione d'impatto sui diritti fondamentali è effettuata congiuntamente alla 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**. Anzi, se adeguatamente progettati e utilizzati, **i sistemi di IA possono al contrario contribuire a ridurre le distorsioni e le discriminazioni strutturali esistenti**, portando così a decisioni più eque e non discriminatorie (ad esempio nella selezione del personale).

I **nuovi requisiti obbligatori per tutti i sistemi di IA ad alto rischio serviranno a questo**. I sistemi di IA devono essere **tecnicamente robusti** 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 set di dati sufficientemente rappresentativi** per **ridurre al minimo il rischio di integrare distorsioni inique** nel modello e garantire che, se presenti, queste possano essere risolte mediante opportune misure di rilevazione, correzione e attenuazione.

Tali sistemi devono inoltre essere **tracciabili e verificabili**, garantendo la **conservazione dell'opportuna documentazione**, compresi i dati utilizzati per addestrare l'algoritmo, fondamentali per le 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 il 2 agosto 2026, due anni dopo l'entrata in vigore, ad eccezione che per le 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 integrati in prodotti regolamentati, elencati nell'allegato II (elenco della normativa di armonizzazione dell'Unione), si applicano 36 mesi dopo l'entrata in vigore, il 2 agosto 2027.

In che modo 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 l'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 **consiglio europeo per l'intelligenza artificiale** (consiglio 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 della Commissione per l'attuazione della legge sull'IA, fornirà orientamenti strategici al consiglio per l'IA.

La legge sull'IA istituisce inoltre due organi consultivi per consentire agli esperti di fornire il loro contributo: il **gruppo di esperti scientifici** e il **forum consultivo**. Tali organismi consentiranno ai portatori di interessi e alle comunità scientifiche interdisciplinari di fornire spunti preziosi, che informeranno il processo decisionale e garantiranno un approccio equilibrato allo sviluppo dell'IA.

Perché è necessario un consiglio europeo per l'intelligenza artificiale e di cosa si occuperà?

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

Il consiglio per l'IA svolge un ruolo cruciale nel garantire un'attuazione agevole, efficace e armonizzata della legge sull'IA. Il consiglio per l'IA fungerà da forum in cui le autorità di regolamentazione dell'IA, ossia l'ufficio per l'IA, le autorità nazionali e il Garante europeo della protezione dei dati, 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 € 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 € 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 € o all'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 violazione, la soglia per le PMI sarebbe l'importo più basso tra i due previsti, mentre per le altre imprese sarebbe l'importo più elevato.

La Commissione può inoltre applicare le norme sui fornitori di modelli di IA per finalità generali

mediante sanzioni pecuniarie, tenendo in considerazione la seguente soglia:

- **fino a 15 milioni di € o al 3%** del fatturato mondiale totale annuo dell'esercizio precedente per **l'inosservanza di qualsiasi obbligo** o misura richiesta dalla Commissione a norma del regolamento.

Le istituzioni, le agenzie o gli organismi dell'UE sono chiamate a dare l'esempio e saranno quindi soggette anch'esse alla normativa e a eventuali sanzioni. Il Garante europeo della protezione dei dati avrà il potere di infliggere loro sanzioni pecuniarie in caso di non conformità.

In che modo sarà elaborato 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 iterativo di elaborazione e sarà costituita da tutti i fornitori interessati e ammissibili di modelli di IA per finalità generali, 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 da rappresentanti del mondo accademico e da altri esperti indipendenti.

L'ufficio per l'IA ha pubblicato un invito a manifestare interesse per partecipare all'elaborazione del primo codice di buone pratiche. Parallelamente a tale invito a manifestare interesse, è stata avviata una consultazione multilaterale per raccogliere i pareri e i contributi di tutti i portatori di interessi sul primo codice di buone pratiche. Le risposte e le osservazioni costituiranno la base della prima iterazione per l'elaborazione del codice di buone pratiche. Il codice si basa quindi fin dall'inizio su una vasta gamma di prospettive e competenze.

La plenaria sarà strutturata in quattro gruppi di lavoro per consentire discussioni mirate su temi specifici finalizzati a 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 a cui desiderano partecipare. Le riunioni si svolgono esclusivamente online.

L'ufficio per l'IA nominerà i presidenti e, se del caso, i vicepresidenti di 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 iterativo di elaborazione, oltre che a partecipare alla plenaria.

La versione definitiva del primo codice di buone pratiche sarà presentata dopo 9 mesi, in una sessione plenaria conclusiva prevista per aprile, e pubblicata. La plenaria conclusiva offrirà ai fornitori di modelli di IA per finalità generali l'opportunità di esprimersi e dichiarare 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 di buone pratiche, l'ufficio per l'IA e il consiglio per l'IA ne valuteranno l'adeguatezza e pubblicheranno la loro valutazione. In seguito a tale valutazione, la Commissione può decidere di approvare il codice di buone pratiche e conferirgli validità generale all'interno dell'Unione mediante atti di esecuzione. Se, nel 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 degli obblighi pertinenti.

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 di buone pratiche dovrebbero riferire periodicamente all'ufficio per l'IA in merito all'attuazione delle misure adottate e ai loro risultati, anche sulla base di indicatori chiave di prestazione, se del caso.

Ciò facilita l'applicazione della normativa da parte dell'ufficio per l'IA, che si avvale dei poteri conferiti alla Commissione dalla legge sull'IA. Tali poteri includono 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 agevolerà, se del caso, la revisione e l'adeguamento del codice per tenere conto dei progressi tecnologici e dello stato dell'arte.

Quando una norma armonizzata è pubblicata e ritenuta idonea a disciplinare i pertinenti obblighi da parte 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 buone pratiche o norme armonizzate, oppure se tali fornitori scelgono di non fare affidamento su tali codici e norme.

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

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

La Commissione è invitata a chiedere alle organizzazioni europee di normazione di elaborare un prodotto di normazione sui processi di documentazione e segnalazione per migliorare le prestazioni dei sistemi di IA in termini di uso delle 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.

Entro due anni dalla data di applicazione del regolamento, e successivamente ogni quattro anni, la Commissione è inoltre invitata a presentare una relazione sul riesame dei progressi compiuti nell'elaborazione dei prodotti della normazione relativi allo sviluppo efficiente sotto il profilo energetico di modelli per finalità generali e a valutare la necessità di ulteriori misure o azioni, anche vincolanti.

In aggiunta a ciò, i fornitori di modelli di IA per finalità generali, che sono addestrati su grandi quantità di dati e quindi soggetti a un elevato consumo di energia, sono tenuti a comunicare il consumo di energia. Nel caso di modelli di IA per finalità generali con rischi sistemici, occorre inoltre valutare l'efficienza energetica.

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

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 **prova 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 nel rispetto della legge sull'IA. Queste, insieme ad altre misure quali le **reti dei centri di eccellenza per l'IA** aggiuntive, 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 affinché le imprese sviluppino e utilizzino l'IA.

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 deve essere elaborato un piano che deve essere presentato all'autorità di vigilanza del mercato, la quale deve approvare il piano e le condizioni di prova specifiche; in caso di mancata risposta entro 30 giorni, il piano si considera automaticamente approvato in modo tacito. Le prove possono essere oggetto di ispezioni senza preavviso da parte dell'autorità.

Le prove in condizioni reali possono essere effettuate solo se sono presenti garanzie specifiche, ad esempio gli utenti dei sistemi sottoposti a prova in condizioni reali devono fornire un consenso informato, le prove non devono avere alcun effetto negativo sugli utenti, gli esiti delle prove devono essere reversibili o devono poter essere ignorati, e i loro dati devono essere cancellati dopo la

conclusione delle prove. Una protezione speciale deve essere concessa ai gruppi vulnerabili, ad esempio a causa della loro età o della 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 la collaborazione 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 (pilastro II).

In particolare, nell'ambito del pilastro I, i partecipanti contribuiranno alla creazione di una comunità collaborativa, condividendo le loro esperienze e conoscenze. In tale contesto l'ufficio per l'IA provvederà a organizzare seminari per fornire 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 pilastro II le organizzazioni sono incoraggiate a rendere noti proattivamente i processi e le pratiche che stanno attuando per la conformità anticipata alla legge sull'IA, attraverso impegni volontari. Gli impegni sono intesi come "dichiarazioni di impegno" e conterranno azioni (pianificate o in corso) per soddisfare alcuni dei 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 relativo al patto per l'IA.

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

Le conseguenze e le sfide dell'IA trascendono i confini, per questo motivo la cooperazione internazionale è fondamentale. 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 essa 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 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 l'1.8.2024.*

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 o per e-mail