

AI Act: la Commissione UE pubblica le Linee Guida sulle pratiche proibite



Prosegue l'impegno dell'Unione Europea nella regolamentazione dell'Intelligenza Artificiale con la pubblicazione delle Linee Guida sulle pratiche proibite dall'AI Act.

A un anno dall'approvazione dell'AI Act, nel mese di febbraio 2025 la Commissione ha pubblicato le prime Linee Guida *"in materia di pratiche ritenute inaccettabili a causa del potenziale rischio per i valori e i diritti fondamentali dell'UE"*.

I presupposti delle Linee Guida: il Regolamento AI

Anche noto come AI Act (AIA), il Regolamento Europeo 2024/1689 è il primo testo normativo al mondo a disciplinare compiutamente l'uso dell'Intelligenza Artificiale.

Entrato in vigore nello scorso agosto, prevede una serrata serie di scadenze per l'operatività dei propri contenuti, dando priorità agli aspetti che il legislatore comunitario ha ritenuto maggiormente urgenti.

In particolare, l'approccio risk-based adottato nell'AI Act ha portato a identificare **quattro livelli di rischio**:

1. **Inaccettabile** – limitato agli strumenti AI che possono minacciare i diritti umani fondamentali, quali sistemi di social scoring o sorveglianza biometrica di massa.
2. **Alto** – identificato rispetto ad utilizzi dell'AI capaci di impattare sulla privacy degli utenti, come software

usati in campo sanitario o per la selezione di personale.

3. **Specifico per la trasparenza** – inerente a sistemi come chatbot o assistenti vocali.
4. **Minimo** – relativo all'AI utilizzata da strumenti come videogiochi o filtri antispam.

Gli impieghi dell'AI che evidenziano il primo livello di rischio sono espressamente proibiti dall'AI Act, in quanto incompatibili con i principi fondativi dell'Unione Europea; mentre quelli rientranti nell'ultimo livello non sono soggetti ad alcuna prescrizione, in ragione della loro ridotta pericolosità.

Le pratiche rientranti nei due livelli intermedi, invece, restano consentite purché rispettino determinati requisiti.

Ai sensi del Regolamento le tecnologie che presentano “rischi specifici per la trasparenza” devono infatti includere una chiara informativa per gli utenti, nonché palesare quali contenuti siano generati dall'AI.

Gli strumenti catalogati “ad alto rischio”, dal canto loro, devono rispettare rigorosi requisiti per il contenimento e la gestione del rischio stesso.

Come ribadito nelle Linee Guida, le limitazioni stabilite dall'AI Act non si applicano al campo militare e giudiziario, nonché alle attività di Ricerca&Sviluppo e alle tecnologie rilasciate sotto licenza libera od Open Source.

Le nuove Linee Guida della Commissione UE, come definite dall'AI Act

Coerentemente con l'approccio descritto, la Commissione ha elaborato prioritariamente le indicazioni relative alle

pratiche proibite dal Regolamento, poiché rientranti nel livello di rischio “inaccettabile”.

Si tratta delle *“AI practices that are deemed unacceptable due to their potential risks to European values and fundamental rights”*, fra le quali l’art. 5 AIA include:

- *Harmful manipulation and deception;*
- *Harmful exploitation of vulnerabilities [...] due to age, disability or a specific social or economic situation;*
- *Social scoring AI systems that evaluate or classify natural persons or groups of persons based on social behaviour or personal characteristics;*
- *Individual criminal offence risk assessment and prediction;*
- *Untargeted scraping to develop facial recognition databases;*
- *Emotion recognition;*
- *Biometric categorisation;*
- *Real-time remote biometric identification (RBI).*

Rispetto a tali impieghi dell’Intelligenza Artificiale, le Linee Guida forniscono chiarimenti ed esempi operativi rivolti a ogni stakeholder – da chi sviluppa gli strumenti fino alle società che li commercializzano – per facilitare una piena comprensione del Regolamento, così da assicurarne l’uniforme applicazione in tutti gli Stati membri dell’Unione.

Pur ribadendo che l’interpretazione autoritativa dell’AI Act resta di competenza esclusiva della Corte di Giustizia UE, con queste nuove Linee Guida la Commissione dichiara di voler continuare a costruire *“a safe and ethical AI landscape”* nel continente europeo.

Monitoraggio e compliance

Per garantire il rispetto delle disposizioni dell’AI Act, l’Unione Europea ha previsto un sistema di monitoraggio ed

enforcement che coinvolge le autorità nazionali competenti, coordinate dal futuro European Artificial Intelligence Office.

Il mancato rispetto delle normative può comportare sanzioni significative, proporzionali alla gravità della violazione.

In caso di violazioni relative ad applicazioni di strumenti AI non consentite, le sanzioni possono arrivare fino a 35 milioni di euro o al 7% del fatturato annuo globale dell'azienda (a seconda di quale importo sia superiore).

Per altre violazioni degli obblighi del regolamento le multe possono raggiungere i 15 milioni di euro, o il 3% del fatturato annuo globale; mentre per la fornitura di informazioni inesatte, incomplete o fuorvianti possono arrivare fino a 7,5 milioni di euro o all'1,5% del fatturato annuo globale.

È importante notare che l'AI Act prevede sanzioni più proporzionate per le piccole e medie imprese (PMI) e le start-up in caso di violazioni delle sue disposizioni.

Un contesto normativo in evoluzione

L'AI Act rappresenta un punto di riferimento globale nella regolamentazione dell'intelligenza artificiale, influenzando anche altre giurisdizioni.

Negli Stati Uniti, ad esempio, l'Executive Order on AI emanato dall'ex Presidente Biden e le linee guida della Federal Trade Commission (FTC) miravano a regolamentare l'uso dell'AI mediante principi di trasparenza e accountability, sebbene senza un framework vincolante come quello europeo; tuttavia, nelle ultime settimane la nuova amministrazione di Washington ha già revocato gran parte delle limitazioni allo sviluppo dell'AI, confermando le forti implicazioni politiche legate a questa tecnologia.

Anche la Cina ha adottato regolamenti sull'AI generativa e il

social scoring, con un approccio maggiormente incentrato sul controllo governativo.

Verso un'AI sicura e responsabile

La pubblicazione delle Linee Guida si inserisce in un più ampio processo di consolidamento normativo volto a garantire che l'intelligenza artificiale sviluppata e utilizzata nell'Unione Europea sia sicura, trasparente ed eticamente allineata ai valori comunitari.

Nei prossimi anni – unitamente alla definitiva entrata in vigore dell'AI Act – ulteriori aggiornamenti e nuove direttive potrebbero affinare il quadro comunitario, adattandolo all'evoluzione delle tecnologie nonché alle esigenze emergenti del mercato e della società.

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/notizie/ai-act-linee-guida-ue/>