EMANATO L'AI ACT: L'INTELLIGENZA ARTIFICIALE TRA INNOVAZIONE E TUTELA DEI DIRITTI FONDAMENTALI

In data 13 marzo 2024 è stato approvato dal Parlamento Europeo l'"AI Act", destinato a regolare, per la prima volta, alcune applicazioni dei sistemi di intelligenza artificiale. Il legislatore europeo, al fine di garantire un'utilizzazione sicura dell'intelligenza artificiale, ha anche previsto la costituzione all'interno della Commissione Europea dell'AI Office.

Il Regolamento entrerà in vigore venti giorni dopo la pubblicazione nella Gazzetta Ufficiale dell'Unione Europea ed inizierà ad applicarsi due anni dopo tale pubblicazione, salvo alcune eccezioni. I divieti relativi alle pratiche vietate, infatti, troveranno applicazione dopo sei mesi dall'entrata in vigore dell'AI Act. È previsto, inoltre, un periodo di conformità volontaria (AI Pact), che permetterà alle aziende di adeguarsi al Regolamento prima dell'effettiva entrata in vigore dello stesso.

L'AI Act, non solo è il primo testo normativo al mondo di questo tipo, ma è anche riuscito a garantire un equilibrio tra innovazione e protezione dei diritti fondamentali dell'Unione Europea, utilizzando un approccio "basato sul rischio".

I sistemi di intelligenza artificiale saranno categorizzati in base al loro profilo di rischio: rischio inaccettabile, per i sistemi espressamente vietati dal Regolamento; rischio alto, per i sistemi che saranno soggetti ad una valutazione; rischio basso, per i sistemi tenuti solo ad obblighi di trasparenza; rischio minimo, per i sistemi esenti da obblighi.

I sistemi espressamente vietati sono quelli utilizzati per:

a) categorizzare le persone sulla base di caratteristiche sensibili, quali l'etnia, le convinzioni politiche o religiose;

b) fare *scraping* non mirato di immagini. È vietato, quindi, raccogliere immagini da internet o da telecamere a circuito chiuso per creare un *database* di riconoscimento senza specifici obiettivi;

c) riconoscere le emozioni in luoghi di lavoro o istituti formativi;

d) *social scoring* e/o tecniche manipolative;

e) colpire le persone vulnerabili;

f) la polizia predittiva.

Per le forze dell'ordine, in particolare, sono state previste alcune indicazioni speciali: sono state elaborate eccezioni per il riconoscimento biometrico, che

potrà essere utilizzato in caso di minaccia terroristica imminente o per ricercare una persona condannata o sospettata di aver commesso un reato grave. In tali casi, però, le forze dell'ordine dovranno notificare l'utilizzo dell'intelligenza artificiale alle autorità preposte al controllo della stessa, le quali ne monitoreranno l'utilizzo. In caso di utilizzazione di sistemi di intelligenza artificiale per analizzare dati relativi a crimini, inoltre, tali sistemi dovranno operare su dati anonimi e non dovranno essere utilizzati per profilare individui specifici.

I sistemi ad alto rischio, invece, sono quelli che possono incidere sui diritti fondamentali dei cittadini: si pensi, ad esempio ai sistemi di intelligenza artificiale per valutare i comportamenti elettorali. Per tali sistemi, non solo è previsto che i relativi produttori forniscano una documentazione tecnica dettagliata, che includa tutti i processi operativi e le misure di sicurezza utilizzate, ma anche che i sistemi siano sottoposti ad una valutazione di impatto sui diritti fondamentali (per evitarne la compromissione) e siano soggetti alla supervisione umana.

In ogni caso, è bene precisare che:

- i sistemi di intelligenza artificiale, durante le fasi di addestramento degli stessi, dovranno comunque rispettare le norme comunitarie sul diritto d'autore;

- le immagini e i contenuti audio/video artificiali o manipolati (c.d. *deepfake*) dovranno essere chiaramente etichettati come tali;

- ai cittadini è riconosciuta la possibilità di presentare reclami sulle decisioni prese utilizzando sistemi ad alto rischio.

L'AI Act, oltre a regolamentare l'utilizzazione dei sistemi di intelligenza artificiale, si è anche preoccupato di prevedere delle norme che incentivino lo sviluppo di tale settore. È stata prevista, infatti, la creazione di *sandbox* regolamentari, ambienti in cui le aziende possono sperimentare soluzioni di intelligenza artificiale in condizioni reali, con la possibilità di beneficiare di deroghe alle norme di settore. Inoltre, sono state previste eccezioni specifiche per le piccole e medie imprese per facilitarne l'adeguamento alle nuove previsioni normative.

È bene, poi, fare un cenno al regime sanzionatorio previsto dal Regolamento in caso di violazione delle norme dello stesso.

Le sanzioni previste dall'AI Act variano in base alla gravità della violazione ed alla dimensione dell'azienda:

a) per le violazioni relative alle pratiche vietate o alla non conformità ai requisiti sui dati, sono previste sanzioni che possono arrivare fino 35 milioni di euro o al 7% del fatturato totale annuo dell'esercizio finanziario precedente;

b) per la mancata osservanza di uno qualsiasi degli altri requisiti o obblighi del regolamento, compresa la violazione delle norme sui modelli di intelligenza artificiale per uso generale, le sanzioni possono arrivare a 7 milioni e mezzo di euro o all'1,5% del fatturato totale annuo dell'esercizio finanziario

precedente;

c) se a seguito di una richiesta degli organi competenti, vengono fornite informazioni inesatte, incomplete o fuorvianti, le sanzioni possono arrivare fino a 7,5 milioni di euro o all'1,5% del fatturato totale annuo dell'esercizio finanziario precedente.

Da ultimo, si noti che l'AI Act ha introdotto una serie di obblighi significativi che coinvolgono direttamente i fornitori di intelligenza artificiale ad alto rischio; tra i principali:

a) garantire la conformità ai requisiti tecnici specifici indicati dal Regolamento, indicare le informazioni essenziali sul sistema, disporre di un sistema di gestione della qualità, elaborare una dichiarazione di conformità UE, adottare misure correttive, se necessario, e fornire tutte le informazioni richieste alle Autorità competenti;

b) adottare misure tecniche ed organizzative adeguate ad un utilizzo conforme, affidare la sorveglianza umana dei sistemi a persone competenti, monitorare il funzionamento dei sistemi e cooperare con le autorità di vigilanza e controllo.

Per i fornitori di modelli di intelligenza artificiale per finalità generali (inclusi i modelli di intelligenza artificiale generativa di grandi dimensioni) sono poi previsti specifici obblighi, tra cui redigere, mantenere aggiornata e mettere a disposizione del pubblico la documentazione tecnica del modello, compresi i dettagli del processo di addestramento e prova dello stesso, nonché i risultati della sua valutazione.

Per importatori e distributori di intelligenza artificiale, invece, tali obblighi sono previsti solo se questo soggetto ha apposto il proprio nome o marchio sul sistema dopo che è stato già messo sul mercato, se ha apportato modifiche sostanziali dopo la sua commercializzazione (purché il sistema rimanga ad alto rischio), o se ha modificato lo scopo previsto del sistema di intelligenza artificiale rendendolo ad alto rischio.

Paola Sangiovanni, Partner
Email: paola.sangiovanni@grplex.com

Falvio Monfrini, Partner
Email: flavio.monfrini@grplex.com

Marco Blei, Counsel
Email: marco.blei@grplex.com

Arianna Rizza, Junior Associate
Email: arianna.rizza@grplex.com