

Intelligenza artificiale, le aziende chiamate a mappare i rischi

Pagina a cura di Marilisa D'Amico

Il 2 febbraio sono entrati in vigore i divieti previsti dal regolamento europeo sull'intelligenza artificiale (regolamento 2024/1689, detto "AI Act"), pubblicato sulla Gazzetta Ufficiale lo scorso 1° agosto.

Si tratta del primo passo nell'attuazione graduale della disciplina. Il regolamento, rammentiamo, adotta un approccio all'intelligenza artificiale basato sul rischio, individuandone quattro livelli che possono comportare lesioni dei diritti umani o compromissione dei principi fondamentali dell'Unione europea. Si tratta del rischio inaccettabile (articolo 5), del rischio elevato o alto, per cui è prevista la valutazione di impatto di cui all'articolo 27, del rischio limitato, ossia relativo a sistemi che richiedono obblighi di trasparenza specifici, e del rischio minimo o nullo, riferito a sistemi che non presentano rischi significativi e per i quali non sono previsti obblighi aggiuntivi.

La tappa in commento riguarda la prima categoria di rischio, quello inaccettabile e si sostanzia nell'entrata in vigore del divieto di immissione sul mercato, di messa in servizio o di uso di sistemi che rientrino in questa categoria. Infatti, l'entrata in vigore delle norme sulla governance e degli obblighi per l'IA di uso generale ("GPAI") alla cui elaborazione, peraltro, partecipa chi scrive, è prevista per il 2 agosto 2025.

Tutte le altre disposizioni, ivi compreso l'obbligo di valutazione di impatto per i sistemi ad alto rischio, saranno pienamente applicabili solo a partire dal 2 agosto 2026.

Occorre sottolineare che il rischio può riguardare lesioni a beni materiali e immateriali, compreso il pregiudizio fisico, psicologico, sociale o economico. In presenza di rischio inaccettabile, a partire dal 2 febbraio, l'attività di IA si intende vietata dal regolamento.

Stando alla lettera della norma in commento, lo stesso regolamento identifica una serie di rischi considerati inaccettabili, fra i quali possiamo citare:

i sistemi di IA volti a conseguire manipolazione degli utenti, e che comportino da parte degli stessi comportamenti non voluti o che conducano ad assumere decisioni viziate nel processo di scelta;

i sistemi che adottano tecniche manipolative che possano causare danni significativi, per la salute fisica, psicologica o per gli interessi finanziari;

tutti sistemi che praticino "social scoring", che classifichino le emozioni o praticino profilazione della propensione a delinquere su base emozionale eccetera.

Particolarmente interessante per le aziende è la declinazione del divieto in ambito del marketing, che sia “AI marketing” o “neuromarketing”.

Nel primo caso, è vietata la profilazione dei consumatori quando avviene «veicolando convincimenti non supportati da fondamenti nel reale». Non si tratta necessariamente di introdurre informazioni errate, ma anche semplicemente di omettere determinate informazioni che, se conosciute dal consumatore, porterebbero il convincimento dello stesso verso diverse determinazioni.

Nel caso del neuromarketing, invece, il divieto colpisce quelle attività di IA volte a profilare i gusti dei consumatori attraverso la raccolta di dati biometrici, qualora tali dati vengano raccolti per trarre deduzioni o inferenze in merito alle opinioni politiche, all'appartenenza sindacale, alle convinzioni religiose o filosofiche, alla razza, alla vita sessuale o all'orientamento sessuale di una persona.

Sicuramente il grado di astrazione della norma appare elevato, pertanto, per facilitare le aziende nella transizione al nuovo quadro normativo, la Commissione ha lanciato l'AI Pact, un'iniziativa volontaria volta a sostenere la futura attuazione e a invitare gli sviluppatori di IA, in Europa e oltre, a conformarsi in anticipo agli obblighi chiave dell'AI Act, insistendo sulla creazione di una comunità che condivida conoscenze e best practices. Tale AI Pact conta già l'adesione di grandi aziende come “Adobe”, “Amazon”, “IBM” e tante altre e si occupa di formazione e sostegno alle imprese.

Per essere pronte per l'entrata in vigore di questo divieto, nonché per l'applicazione definitiva del regolamento (e di tutte le sanzioni da esso previste), le aziende dovranno, al più presto, mappare i propri sistemi di IA per verificare se rientrano nelle categorie di rischio e, più in generale, intraprendere tutta una serie di attività prodromiche alla conformità con la nuova normativa.

© RIPRODUZIONE RISERVATA