SCLA
STUDIO LEGALE

AI ACT: COSA PREVEDE E COSA CAMBIA DAL 2 AGOSTO PER LE AZIENDE

Avv. Martina Vancini

Il 2 agosto 2026 è la prossima scadenza operativa prevista dall'AI Act per le aziende.

Da questa data diventa pienamente applicabile la parte più rilevante del regolamento europeo sull'intelligenza artificiale: gli obblighi di trasparenza dell'articolo 50.

In poche parole, chi mette a disposizione o utilizza determinati sistemi di intelligenza artificiale deve informare gli utenti.

Dunque, se aziende utilizzano un chatbot, un assistente virtuale o un agente AI che interagisce direttamente con persone fisiche, dovranno assicurarsi che l'interlocutore sappia di avere davanti un sistema di intelligenza artificiale.

Inoltre, se aziende utilizzano sistemi biometrici o di riconoscimento delle emozioni, devono informare le persone esposte al sistema.

Infine, se aziende diffondono testi generati o manipolati con l'AI su questioni di interesse pubblico, devono segnalarlo a meno che non vi sia stata una revisione umana effettiva.

L'era dell'incertezza, in cui un utente non sa se sta guardando una foto reale o una creazione dell'intelligenza artificiale sta, dunque, per finire. Nasce infatti il diritto di sapere, in modo preciso, se ciò con cui si interagisce, che si legge o che si guarda è opera di una persona o è stato generato da un'intelligenza artificiale.

Molte imprese utilizzano già sistemi di intelligenza artificiale nella propria attività quotidiana, spesso senza essersi date regole interne per il loro utilizzo.

Non tutti i sistemi di AI comportano però gli stessi obblighi.

L'AI Act prevede infatti quattro categorie di rischio: inaccettabile, alto rischio, rischio limitato e rischio minimo. Il rischio viene determinato in relazione al potenziale impatto che l'AI può avere sui diritti fondamentali, sulla sicurezza e sugli interessi delle persone.
I sistemi a rischio inaccettabile sono vietati. Tra questi vi rientrano i sistemi di *social scoring* che classificano le persone sulla base del comportamento sociale e i sistemi che manipolano le scelte individuali tramite tecniche subliminali.

I sistemi ad alto rischio sono ammessi ma sottoposti a determinati requisiti, a gestione del rischio e a supervisione umana. All'interno di questa categoria vi rientrano i software utilizzati per la selezione del personale, quelli che analizzano i curricula e quelli che filtrano le candidature.

I sistemi a rischio limitato sono soggetti principalmente a obblighi di trasparenza: l'utente deve essere informato del fatto che sta interagendo con un sistema di intelligenza artificiale. Vi rientrano, per esempio, i chatbot sopra richiamati.

I sistemi a rischio minimo, infine, comprendono la maggior parte degli strumenti di uso comune: filtri antispam, assistenti virtuali generici, ecc. Il loro utilizzo resta sostanzialmente libero.

L'AI Act non deve essere rispettato soltanto da chi sviluppa e mette sul mercato sistemi di intelligenza artificiale (*provider*) ma anche da chi utilizza questi sistemi sviluppati da terzi (*deployer*). È sufficiente usare ChatGPT per predisporre offerte, o Gemini per redigere documenti, per essere soggetti agli obblighi dell'AI Act.

Per cominciare ad adeguarsi all'AI Act, il primo passo consiste nell'individuare dove viene già utilizzata l'intelligenza artificiale all'interno dell'azienda. Successivamente, occorre fare formazione relativamente al funzionamento dei sistemi, ai loro limiti e ai rischi per la privacy. Infine, è necessario redigere una policy AI per stabilire quali strumenti possono essere utilizzati, quali dati non devono essere inseriti e quando è obbligatoria la revisione umana del prodotto generato dall'AI.

Il presente articolo non intende fornire un parere legale e, per l'effetto, non può essere considerato sostitutivo di una consulenza legale specifica.

Clicca qui per scaricare l'articolo in PDF