29 luglio 2026

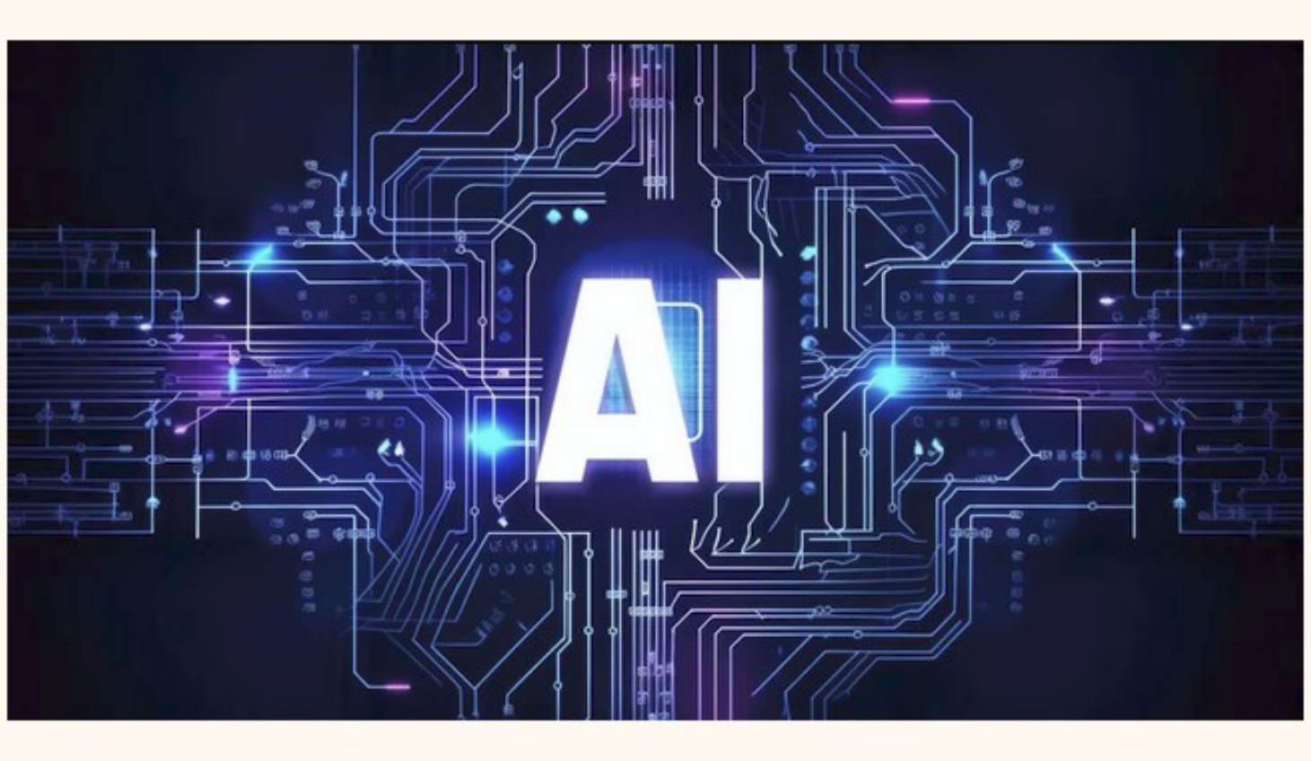
Analisi

Ai Act, cosa cambia davvero per aziende e startup dal 2 agosto

Più tempo per i sistemi ad alto rischio, ma nessuna pausa generale. Giulio Coraggio, Partner di DLA Piper: «Il calendario è cambiato, non le responsabilità».

Servizio ***di Luca Tremolada***

Aggiungi Il Sole 24 Ore
ai preferiti su Google



I PUNTI CHIAVE

1. Cosa succede dopo il 2 agosto?
2. Cosa cambia per aziende e startup
3. Cosa non è stato rinviato.
4. Dal 2 agosto chatbot e assistenti virtuali devono presentarsi
5. Stesso discorso per deepfake e contenuti sintetici
6. Il rinvio non cambia la classificazione del rischio
7. Contratti, responsabilità e fornitori
8. E poi c'è la governance.

Ascolta la versione audio dell'articolo

6 min

La prima cosa da capire è semplice: una parte dell'AI Act slitta. Il resto no. Con il Digital Omnibus sull'intelligenza artificiale, entrato in vigore il 27 luglio, l'Unione europea ha rinviato gli obblighi più complessi per alcuni sistemi classificati ad alto rischio.

Chiedilo al Sole

○ ○

Quali rischi, oltre a quelli legali e finanziari, corrono le aziende che utilizzano sistemi di IA ad alto rischio senza un'adeguata governance?

Cosa ha comportato, in sintesi, il Digital Omnibus sull'intelligenza artificiale per le scadenze dell'AI Act?

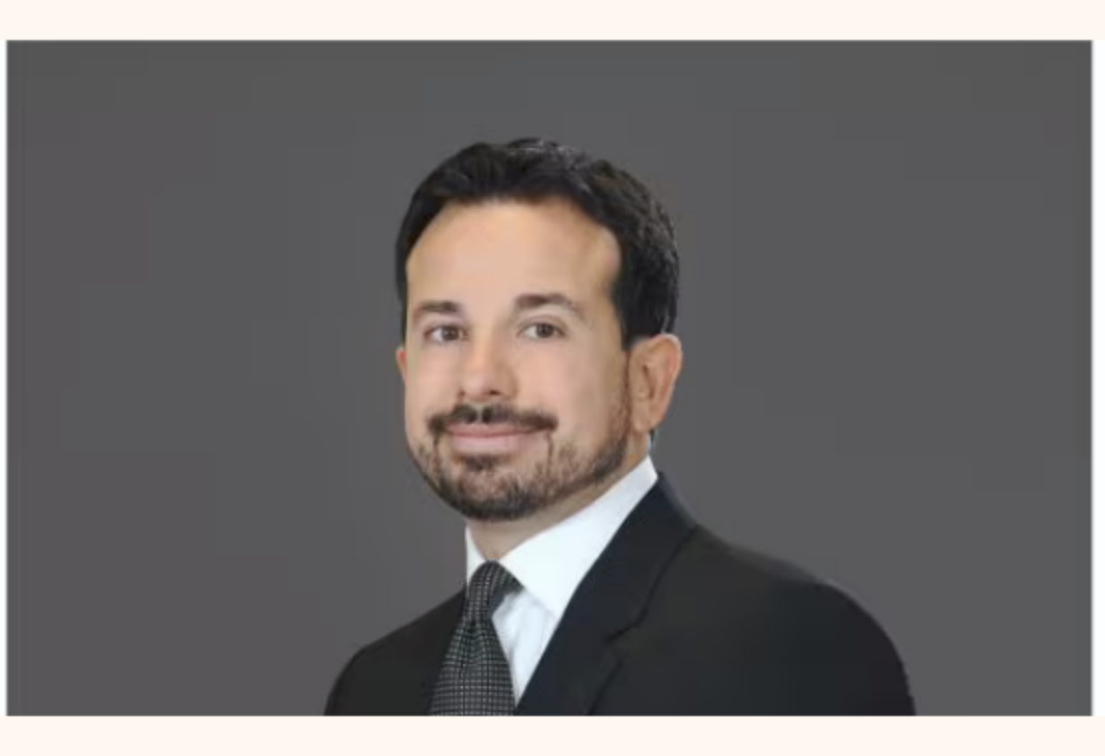
Perché, secondo l'avvocato Giulio Coraggio, non bisogna interpretare il rinvio delle scadenze come una moratoria?

Domande di approfondimento generate da 24Ore AI

Per i sistemi "autonomi" indicati nell'Allegato III, la nuova scadenza passa dal 2 agosto 2026 al 2 dicembre 2027. Parliamo, tra gli altri, di strumenti usati nella selezione del personale, nella valutazione dei dipendenti, nello scoring creditizio e nell'accesso a servizi essenziali.

Per i sistemi di intelligenza artificiale integrati in prodotti già regolamentati, come dispositivi medici, macchinari e veicoli, la data si sposta invece al 2 agosto 2028.

«Le scadenze più temute dell'AI Act - spiega l'avvocato **Giulio Coraggio, Partner di DLA Piper** - si spostano ufficialmente in avanti. Circa un anno e mezzo di respiro in più, concesso perché standard tecnici e strumenti attuativi non erano pronti. Il rischio però - avverte - è leggere questo rinvio come una moratoria. Non lo è. Il calendario è cambiato, non le responsabilità: le regole restano quelle, si sposta solo il momento in cui la non conformità inizia a costare. E costa molto, fino a 35 milioni di euro o al 7% del fatturato globale».



Bruxelles insomma non ha cambiato idea sull'AI Act, standard tecnici, procedure e strumenti applicativi non erano ancora pronti. L'Europa ha spostato alcune scadenze, non ha spento il regolamento. Ha rallentato il treno nei tratti più complicati. I binari restano gli stessi.

1 Cosa succede dopo il 2 agosto?

«Le pratiche vietate, le regole sui modelli di IA generici e l'obbligo di formazione del personale sono già operativi. E gli obblighi di trasparenza dell'articolo 50 dell'AI Act, dall'informare gli utenti che stanno interagendo con un'IA al segnalare i contenuti deepfake, restano fissati al 2 agosto 2026, come da calendario originario: solo il watermarking dei contenuti sintetici per i sistemi già sul mercato scivola al 2 dicembre 2026. Chi utilizza un sistema di selezione del personale, di scoring creditizio o di valutazione dei dipendenti è già oggi dentro il perimetro dei sistemi ad alto rischio, con o senza proroga». In altre parole, dal prossimo 2 agosto con l'applicazione dell'articolo 50 dell'AI Act europeo chatbot, avatar e contenuti sintetici dovranno dichiarare la propria natura artificiale.

2 Cosa cambia per aziende e startup

Per imprese e startup il rinvio significa soprattutto una cosa: più tempo per prepararsi. Chi sviluppa o utilizza sistemi di intelligenza artificiale ad alto rischio avrà qualche mese in più per costruire documentazione, procedure di controllo, sistemi di gestione del rischio e meccanismi di supervisione umana.

È una buona notizia soprattutto per le startup, che spesso lavorano con team piccoli, capitali limitati e prodotti in continua evoluzione. Adeguarsi all'AI Act significa infatti fare molto più che aggiungere una clausola alle condizioni d'uso.

Bisogna capire quali sistemi sono presenti in azienda, come vengono utilizzati, con quali dati sono addestrati, chi controlla i risultati e quali conseguenze possono produrre sulle persone.

Poi occorre stabilire il ruolo dell'impresa nella catena del valore. Un'azienda può essere fornitore del sistema, utilizzatore, distributore o importatore. Ogni posizione porta con sé obblighi differenti.

Anche modificare un sistema esistente, integrarlo in un prodotto o venderlo con il proprio marchio può cambiare la responsabilità dell'azienda. L'AI Act segue il software come il fisco segue una fattura: vuole sapere chi lo ha prodotto, chi lo ha venduto e chi lo usa.

«La vera sfida per le imprese - commenta Coraggio - è di usare questi mesi per costruire un modello di AI governance, non per rimandare adempimenti prima dell'approcciarsi della prossima scadenza quando sarà troppo tardi per conformarsi in modo corretto. In concreto questo significa mappare e classificare tutti i sistemi di IA in uso o in sviluppo nell'azienda, individuare quali ricadono nell'alto rischio, rivedere i contratti con i fornitori, su chi gravano responsabilità e obblighi documentali, e investire sulle competenze interne. Sono attività che richiedono mesi, non settimane, e che non si improvvisano alla vigilia della scadenza».

3 Cosa non è stato rinviato.

Le pratiche vietate dall'AI Act sono già soggette alle nuove regole. Lo stesso vale per gli obblighi relativi ai modelli di intelligenza artificiale per finalità generali, i cosiddetti GPAI, la categoria nella quale rientrano i grandi modelli linguistici alla base dei servizi generativi.È già operativo anche l'obbligo di garantire un adeguato livello di alfabetizzazione sull'intelligenza artificiale per il personale.Non vuol dire trasformare tutti i dipendenti in data scientist. Significa insegnare loro cosa può fare un sistema, dove può sbagliare, quali dati non devono essere inseriti e quando serve il controllo di una persona. Il corso aziendale con dieci slide potrebbe non essere sufficiente.

4 Dal 2 agosto chatbot e assistenti virtuali devono presentarsi

Un chatbot, un assistente vocale o un agente automatico che interagisce con una persona deve rendere chiaro che dall'altra parte non c'è un essere umano, salvo che la natura artificiale del sistema sia evidente dal contesto. È una specie di cartellino digitale.

Per le aziende significa rivedere le interfacce, i messaggi iniziali, gli script vocali e i sistemi di assistenza clienti. L'informazione deve essere chiara e fornita al momento giusto. Nasconderla nelle condizioni generali di servizio non basta.

5 Stesso discorso per deepfake e contenuti sintetici

Chi pubblica un deepfake deve dichiarare che il contenuto è stato generato o manipolato dall'intelligenza artificiale. La regola riguarda video, immagini e audio che possono sembrare autentici e rappresentare persone, oggetti, luoghi o avvenimenti mai esistiti. Sono previste eccezioni e regole specifiche per opere artistiche, satira e contenuti creativi. Ma il principio resta: chi guarda deve poter capire che ciò che vede potrebbe non essere reale.

Qui la tecnologia incontra un problema concreto. Un watermark deve sopravvivere a compressioni, modifiche, screenshot e riconversioni. È come mettere una targa a un'automobile sapendo che chiunque può ritagliarla con Photoshop.

Anche i testi generati dall'intelligenza artificiale e pubblicati per informare il pubblico su questioni di interesse generale devono essere segnalati, salvo che siano stati sottoposti a controllo umano o editoriale e che una persona si assuma la responsabilità della pubblicazione. L'algoritmo può scrivere. Qualcuno deve comunque firmare.

6 Il rinvio non cambia la classificazione del rischio

Una delle confusioni più pericolose riguarda i sistemi già utilizzati nelle risorse umane, nel credito o nella valutazione dei lavoratori.

Un software che seleziona curriculum, assegna punteggi ai candidati o misura le prestazioni dei dipendenti resta classificato come sistema ad alto rischio. La proroga non modifica la natura del sistema. Sposta soltanto il momento in cui alcuni obblighi specifici diventeranno pienamente applicabili.

«Chi utilizza un sistema di selezione del personale, di scoring creditizio o di valutazione dei dipendenti è già oggi dentro il perimetro dei sistemi ad alto rischio, con o senza proroga», spiega Coraggio.

Per un'impresa significa che non conviene aspettare il 2027 per cominciare a studiare il problema. Un algoritmo che discrimina candidati o lavoratori può già produrre conseguenze legali, reputazionali e organizzative.

Per le startup il rischio non è soltanto economico. Un prodotto non conforme può diventare più difficile da vendere, soprattutto a banche, assicurazioni, pubbliche amministrazioni e grandi aziende.

Investitori e clienti inizieranno a chiedere non soltanto quanto è potente il modello, ma anche come è stato addestrato, quali dati utilizza e chi controlla le sue decisioni.

Il primo passo per le aziende è capire quali sistemi di intelligenza artificiale sono già presenti. Può sembrare banale. Non lo è. L'Ai può nascondersi nel software delle risorse umane, nel CRM, nel sistema antifrode, negli strumenti di marketing, nel servizio clienti o in una funzione aggiunta automaticamente da un fornitore cloud.

Serve quindi una mappa che indichi almeno il nome del sistema, la sua finalità, i dati utilizzati, il fornitore, il responsabile interno e il possibile impatto sulle persone.

7 Contratti, responsabilità e fornitori

Il secondo fronte riguarda i contratti. Molte aziende utilizzano sistemi sviluppati da soggetti esterni. Questo non significa che tutte le responsabilità rimangano automaticamente in capo al fornitore. Occorre chiarire chi deve conservare i log, chi produce la documentazione, chi comunica gli incidenti, chi verifica la qualità dei dati e chi interviene quando il modello cambia comportamento. I sistemi di intelligenza artificiale vengono aggiornati spesso. A volte senza che l'utilizzatore si accorga davvero della differenza. Un modello può cambiare versione, dati di addestramento, filtri o modalità di risposta. Il software ha lo stesso nome. Il motore sotto il cofano, però, è diverso. Per questo le imprese devono prevedere controlli periodici e procedure per gestire modifiche sostanziali.

8 E poi c'è la governance.

Nelle startup non sarà sempre possibile creare un ufficio dedicato. Ma deve comunque esistere un processo. Anche leggero. Purché reale. Le decisioni importanti non possono rimanere disperse tra il fondatore, il programmatore, il consulente esterno e il fornitore cloud. «Sono attività che richiedono mesi, non settimane, e che non si improvvisano alla vigilia della scadenza», aggiunge Coraggio.

Per una startup, presentarsi a un investitore o a un grande cliente con una mappa dei sistemi, una classificazione del rischio e una documentazione chiara significa ridurre l'incertezza. «Chi tratterà il rinvio come un'occasione per attrezzarsi arriverà pronto e con un vantaggio competitivo - commenta l'avvocato di DLA Piper - chi invece lo leggerà come un permesso per fermarsi si ritroverà, nel dicembre 2027, esattamente dove è oggi, ma con molto meno tempo. In un mercato in cui l'Ai è ormai un fattore produttivo, la compliance non è un costo ma un abilitatore di fiducia verso clienti, investitori e autorità».

PER SAPERNE DI PIÙ