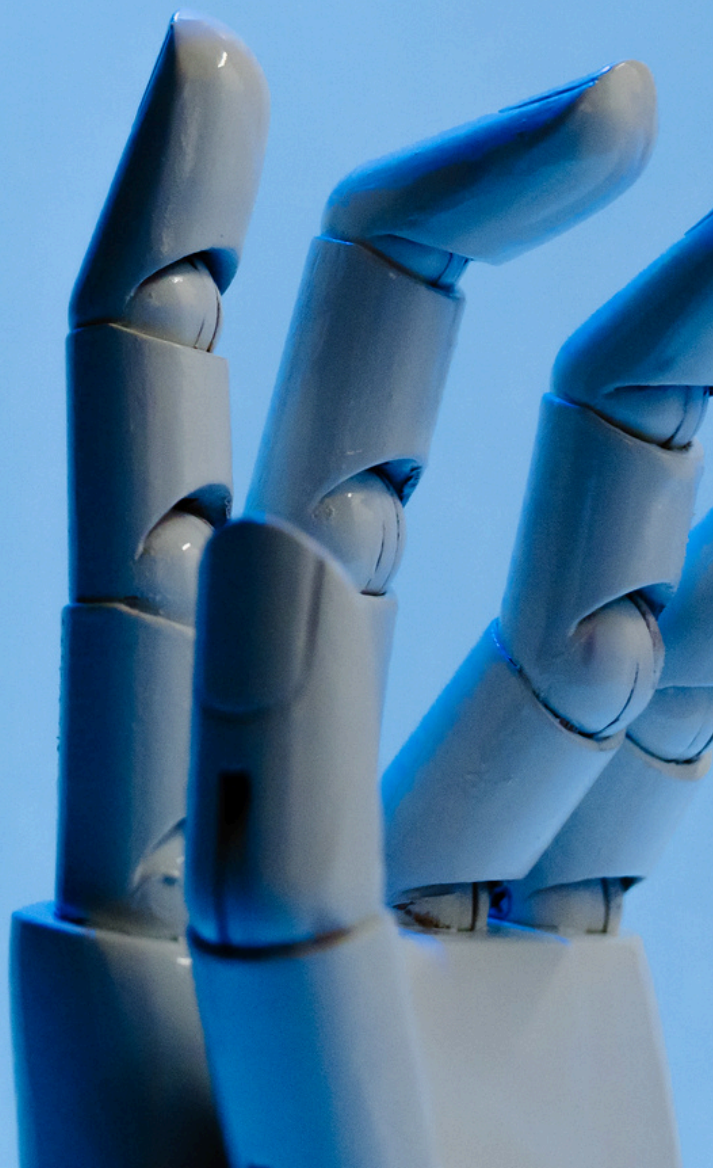
AI Act

Cosa prevede e a chi si applica l'AI Act



DLA PIPER

AI Act - Cosa prevede e a chi si applica

Il testo relativo all'**AI Act**, la prima legislazione che regolamenta la tanto discussa intelligenza artificiale (*Artifical Intelligence*, o AI, in inglese), ha raggiunto la versione finale.

Dopo l'approvazione definitiva dell'AI Act da parte del Parlamento Europeo il 13 marzo 2024 e del Consiglio dell'UE il 21 maggio 2024, **l'AI Act è stato pubblicato nella Gazzetta Ufficiale dell'UE il 12 luglio 2024**.

La definizione di sistema di intelligenza artificiale ai sensi dell'AI Act

Esiste una nuova definizione di sistema di intelligenza artificiale che differisce leggermente da quella fornita dalle linee guida dell'OCSE ed è la seguente:

> *"un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali"*

Le tre componenti principali che copre la definizione sono:

1. i sistemi in cui l'AI opera **in piena autonomia e con input umani**;
2. i sistemi che possono **adattarsi come conseguenza delle informazioni che vengono loro fornite;** e
3. i sistemi che, in base alle informazioni ricevute, **imparano a generare output**.

L'obiettivo del legislatore europeo è quello di **adottare una definizione di sistemi di AI che sia la più ampia possibile**. Viene pertanto conferita alla definizione di AI un ampio campo di applicazione, poiché l'intelligenza artificiale potrebbe avere un impatto su ogni settore, escludendo dalla sua applicazione alcuni sistemi già soggetti alla legislazione di armonizzazione, nonché quelli utilizzati esclusivamente per scopi militari, di difesa o di sicurezza nazionale, oltre ai sistemi utilizzati per la ricerca scientifica, lo sviluppo e l'uso puramente personale non professionale.

Un'ulteriore eccezione molto discussa all'applicabilità dell'AI Act opera in relazione ai **sistemi di intelligenza artificiale che sfruttano software gratuiti e open source**, ai quali non si applicherà la normativa a meno che il sistema di intelligenza artificiale:

1. sia immesso nel mercato o messo in servizio come **sistema di AI ad alto rischio**; e
2. sia soggetto agli **obblighi di trasparenza stabiliti dall'AI Act**.

In ogni caso, le esenzioni per i software gratuiti e open source non si applicano se il sistema di AI è designato per finalità generali con rischio sistemico.

La classificazione dei sistemi di AI

Il quadro giuridico riguardante l'AI è caratterizzato da un doppio regime che distingue tra (i) sistemi di AI a rischio limitato e (ii) sistemi ad alto rischio. La definizione di rischio è "*la combinazione della probabilità del verificarsi di un danno e la gravità del danno stesso*" e, sulla base di tale definizione, **esiste una distinzione tra**

Sistemi di AI vietati

Questi sistemi includono

- tecniche che manipolano la cognizione e il comportamento individuale;
- la raccolta casuale di dati di riconoscimento facciale da Internet o attraverso le telecamere a circuito chiuso;
- l'uso di sistemi di riconoscimento delle emozioni nei luoghi di lavoro e nei contesti educativi;
- l'attribuzione di un punteggio sociale; e
- il trattamento biometrico per l'inferenza di dati personali sensibili come l'orientamento sessuale o le credenze religiose

Tali sistemi di AI sono semplicemente vietati.

Sistemi di AI ad alto rischio

Questi sistemi includono

- i sistemi di AI destinati ad essere utilizzati come **componente di sicurezza di un prodotto**,
- i sistemi di AI a cui si applica la normativa di armonizzazione elencata nell'**Allegato II dell'AI Act**, e
- alcuni sistemi di AI utilizzati nel **settore dell'istruzione**, nei **processi di recruiting**, nonché **per scopi di valutazione dell'affidabilità creditizia**, a meno che non vi sia uno scopo di rilevamento delle frodi, e di valutazione del rischio e dei prezzi relativi alle persone fisiche nel caso di assicurazioni sulla vita e sulla salute e per i sistemi di AI utilizzati per altri scopi elencati nell'Allegato III dell'AI Act.

Tali categorie non sono tuttavia rigide, in quanto il fornitore può dimostrare che il sistema specifico non è ad alto rischio a causa delle sue peculiarità.

In relazione ai sistemi di AI ad alto rischio, **deve essere stabilito, implementato, documentato e mantenuto un sistema di gestione del rischio** per identificare i rischi e adottare azioni di mitigazione durante l'intero ciclo di vita del sistema di AI, eseguendo anche test per comprendere il funzionamento del sistema in condizioni reali. Se il sistema di AI ad alto rischio prevede l'addestramento dei modelli con i dati, dovrà essere sviluppato sulla base di set di dati di addestramento, convalida e test soggetti ad appropriate pratiche di gestione e governance dei dati elencate nell'AI Act. L'esecuzione di queste attività in relazione ai sistemi di intelligenza artificiale ad alto rischio dovrà essere dimostrata **attraverso la documentazione tecnica** da predisporre prima dell'immissione del sistema sul mercato o della sua messa in servizio e dovrà essere mantenuta aggiornata. Tale documentazione tecnica dovrà contenere almeno le informazioni di cui all'Allegato IV dell'AI Act. Si tratta comunque di **un'autovalutazione, senza alcun riferimento a una valutazione di terzi**. Tale valutazione dovrà essere supportata anche da prove ottenute attraverso la registrazione automatica di eventi ('log') durante la vita del sistema, che il sistema dovrà tecnicamente consentire.

I sistemi di intelligenza artificiale ad alto rischio dovranno essere progettati e sviluppati in modo da

- garantire che il **loro funzionamento sia sufficientemente trasparente** da consentire agli utenti di interpretare i risultati del sistema e di utilizzarli in modo appropriato, anche grazie alle istruzioni che accompagneranno il sistema;
- consentire una **supervisione efficace da parte di persone fisiche** durante il periodo in cui il sistema di IA è in uso, anche con strumenti di interfaccia uomo-macchina appropriati;
- raggiungere un **livello adeguato di accuratezza, robustezza e cybersicurezza**, e funzionare in modo coerente sotto questi aspetti durante il loro ciclo di vita;
- essere in grado di fornire alle **persone**, in caso di decisioni automatizzate, **una spiegazione della procedura decisionale** e degli elementi principali della decisione presa;

Sistemi di AI per finalità generali (GPAI)

Questi sistemi sono "*basati su un modello di IA per finalità generali e che ha la capacità di perseguire varie finalità, sia per uso diretto che per integrazione in altri sistemi di IA*" e sono destinati a **portare un rischio sistemico** (i.e., un rischio con effetti negativi sulla salute pubblica, la sicurezza, la pubblica sicurezza, i diritti fondamentali o la società nel suo complesso, che può essere propagato su scala attraverso la catena del valore), quando sono identificati come tali dalla Commissione UE o quando la quantità cumulativa di calcolo utilizzata per la sua formazione, misurata in operazioni in virgola mobile (FLOP), è superiore a 10^25.

I sistemi GPAI che generano un rischio sistemico devono essere notificati alla Commissione UE. Inoltre, i fornitori di sistemi GPAI dovranno:

- redigere e mantenere aggiornata la **documentazione tecnica del modello** e mettere a disposizione informazioni e documentazione ai fornitori di sistemi di AI che intendono integrare il modello di AI per finalità generali nel loro sistema di AI. Tale documentazione tecnica dovrà essere redatta elencando, tra l'altro, le modalità seguite per sviluppare il sistema, le attività svolte e il consumo energetico stimato, e – nel caso di sistemi GPAI che comportano un potenziale rischio sistemico – le strategie di valutazione seguite e i test avversariali (ad esempio, il red teaming) effettuati;
- attuare una **policy di rispetto della legge sul diritto d'autore dell'Unione** e redigere e rendere disponibile al pubblico un riassunto sufficientemente dettagliato dei contenuti utilizzati per l'addestramento del modello di intelligenza artificiale generale, secondo un modello fornito dall'AI Office; e
- in caso di **GPAI con rischio sistemico**, (i) eseguire la **valutazione del modello**, (ii) valutare e **mitigare i possibili rischi sistemici** a livello di Unione, (iii) tenere **traccia, documentare e riferire** le informazioni pertinenti sugli incidenti gravi e le possibili misure correttive per affrontarli e (iv) garantire un **livello adeguato di protezione della cybersecurity**.

Sistemi AI di base

T**utti i sistemi di AI, a prescindere dal livello di rischio, sono soggetti a obblighi minimi.**
Sono soggetti a obblighi di trasparenza di base per garantire un livello minimo di chiarezza e comprensione a tutti, informando le persone che stanno interagendo con un sistema di AI.

Quali sono i soggetti obbligati ai sensi dell'AI Act ?

L'AI Act finalizzato ha un effetto transnazionale, in quanto si applica a

1. fornitori (*provider*) che immettono sul mercato o mettono in servizio sistemi di AI o che immettono sul mercato modelli di AI di uso generale nell'Unione, **indipendentemente dal fatto che tali fornitori siano stabiliti o situati nell'Unione o in un Paese terzo**;
2. utilizzatori (*deployers*) di sistemi di AI **che hanno la loro sede o che sono situati all'interno dell'Unione**;
3. fornitori ed utilizzatori di sistemi di AI **con sede o ubicati in un paese terzo, dove l'output prodotto dal sistema viene utilizzato nell'Unione**;
4. importatori e distributori di sistemi di AI;
5. fabbricanti di prodotti che immettono sul mercato o mettono in servizio un sistema di AI insieme al loro prodotto e con il loro nome o marchio;
6. rappresentanti autorizzati di fornitori che non sono stabiliti nell'Unione; e
7. persone interessate che si trovano nell'Unione Europea.

In particolare, le **definizioni più rilevanti delle categorie di soggetti** di cui sopra sono quelle di:

A) Fornitore (*provider*)

> Il "*fornitore*" è "*una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che* ***sviluppa*** *un sistema di IA o un modello di IA per finalità generali o che* ***fa sviluppare*** *un sistema di IA o un modello di IA per finalità generali* ***e immette tale sistema o modello sul mercato o mette in servizio il sistema di IA con il proprio nome o marchio****, a titolo oneroso o gratuito*"

Il ***provider*** è l'entità giuridica soggetta agli **obblighi più rilevanti ai sensi dell'AI Act**, poiché deve garantire che i propri **sistemi di AI ad alto rischio siano conformi** ai requisiti di legge, e, allo stesso tempo:

- avere un sistema di gestione della qualità,
- conservare la documentazione per poter dimostrare la conformità con il sistema di AI,
- adottare le azioni correttive se il sistema AI non è conforme all'AI Act,
- redigere una dichiarazione di conformità UE scritta a lettura ottica, fisica o firmata elettronicamente per ogni sistema di AI ad alto rischio; e
- registrare i sistemi di AI ad alto rischio nel database dell'UE, e rispettare gli obblighi applicabili ai sistemi GPAI.

B) *Deployer*

> Il *"deployer" è "una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che utilizza un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale" che include qualsiasi azienda che riceve un sistema di AI da un fornitore per gestire le proprie attività.*

Per quanto riguarda i ***deployer***, l'AI Act stabilisce che essi devono

- adottare **misure tecniche e organizzative adeguate** per garantire l'utilizzo dei sistemi in conformità alle istruzioni d'uso che li accompagnano;
- assegnare la **supervisione umana a persone fisiche** che abbiano la competenza, la formazione e l'autorità necessarie, nonché il supporto necessario;
- **monitorare il funzionamento del sistema di AI**; e
- r**ispettare gli obblighi di informazione** prima della messa in funzione del sistema di AI, nonché eseguire una DPIA quando richiesto dal tipo di trattamento dei dati personali.

Inoltre, gli implementatori di sistemi di AI ad alto rischio che sono utilizzati per il *credit scoring*, nonché per la valutazione del rischio e la determinazione dei prezzi in relazione alle persone fisiche nel caso dell'assicurazione sulla vita e sulla salute, devono eseguire la **valutazione d'impatto sui diritti fondamentali (FRIA)** che dovrà essere notificata all'autorità di vigilanza del mercato con i risultati della valutazione, presentando il relativo modello compilato di cui alla Legge.

Governance centrale e locale dell'AI

In termini di governance e conformità, l'AI Act ha istituito un **Ufficio europeo per l'AI per monitorare i modelli di AI più complessi**. Viene prevista la creazione di un panel scientifico e di un forum consultivo per integrare le prospettive delle diverse parti interessate. Ciò garantisce che la normativa sia sempre informata e aggiornata rispetto agli sviluppi del settore.

Ma un argomento di notevole discussione sarà quello di quali poteri in concreto saranno conferiti alle autorità locali per l'AI e quali enti saranno nominati come autorità nazionali. Come è successo con il GDPR, le autorità locali non vorranno rinunciare ai loro poteri. **L'Ufficio AI dovrebbe ridurre il rischio di approcci incoerenti in tutta l'UE tra le autorità locali**, ma non si possono escludere attriti politici tra le diverse autorità locali.

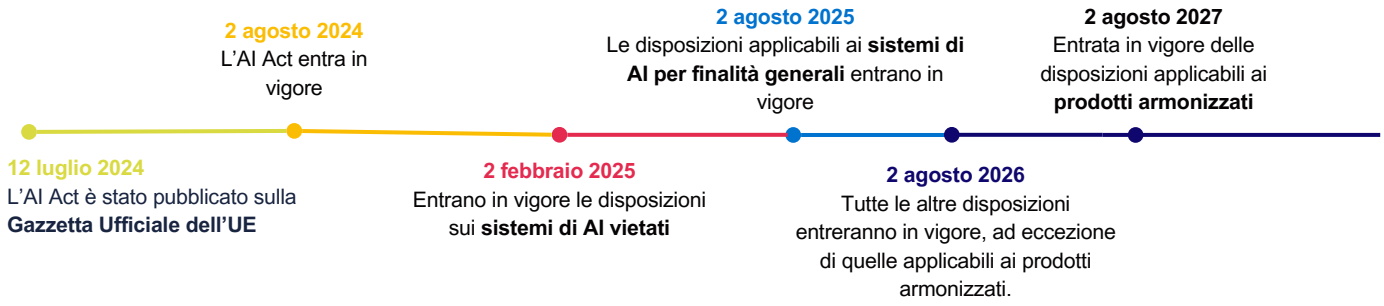
Le potenziali sanzioni basate sul fatturato

L'AI Act stabilisce anche, ovviamente, un sistema di sanzioni che, come nel caso di diverse recenti normative europee, si basa sul fatturato globale delle aziende o su un importo predeterminato, a seconda di quale sia più alto.

Violazioni di pratiche vietate o non conformità ai requisiti delle applicazioni di AI vietate.	fino a **35 milioni di euro** o al **7% del fatturato globale annuo** dell'esercizio precedente
Inosservanza di qualsiasi altro requisito o obbligo, compresa la violazione delle norme sulle GPAI.	**15 milioni di euro** o il **3% del fatturato globale annuo** dell'esercizio precedente
Fornitura di informazioni inesatte, incomplete o fuorvianti agli enti notificati e alle autorità nazionali competenti in risposta a una richiesta	**7,5 milioni di euro** o l'**1% del fatturato globale annuo** dell'esercizio precedente

Sono previste eccezioni per le aziende più piccole, con sanzioni limitate per le PMI e le startup. Quindi, anche per quanto riguarda le sanzioni, è stato trovato un equilibrio tra la necessità di regolamentare l'AI e l'obiettivo di non limitare lo sviluppo di questa tecnologia nell'UE. Per lo stesso motivo, sono previste le cosiddette soluzioni di 'sandboxing', dove le soluzioni possono essere testate beneficiando di un regime speciale.

La tempistica dell'AI Act



Dopo aver ricevuto l'approvazione finale del Parlamento Europeo il 13 marzo 2024 e del Consiglio dell'UE il 21 maggio 2024, l'AI Act è stato pubblicato nella Gazzetta Ufficiale dell'UE il 12 luglio 2024.

La data di applicazione dell'AI Act segue un calendario preciso, con un **periodo di transizione di sei mesi per l'introduzione dei divieti, di un anno per i sistemi GPAI** e di **due anni per le restanti disposizioni**, ad eccezione di quelle applicabili ai dispositivi **già regolamentati da altri regolamenti di armonizzazione dell'UE**, per le quali il **termine è di 36 mesi**, come nel settore farmaceutico e dei dispositivi medici.

Tuttavia, non c'è dubbio che, a prescindere dalla durata del periodo di transizione, nessuna azienda sarà disposta ad adottare soluzioni di AI non conformi all'AI Act che la costringerebbe a dismettere la tecnologia in tempi brevi.

Abbiamo creato una soluzione innovativa per supportare le aziende nel garantire la conformità dell'intelligenza artificiale in modo economico ed efficiente; per saperne di più, potete leggere QUI e contattarci per avere maggiori informazioni. Inoltre, è possibile guardare QUI un webinar organizzato da DLA Piper sull'argomento.

Giulio Coraggio
Partner, Milano
M + 39 33 46 88 11 47
giulio.coraggio@dlapiper.com

Alessandro Ferrari
Partner, Milano
M + 39 33 16 64 56 52
alessandro.ferrari@dlapiper.com

Elena Varese
Partner, Milano
M: +39 36 65 86 47 51
elena.varese@dlapiper.com

Gualtiero Dragotti
Partner, Milano
M: +39 33 58 23 29 37
gualtiero.dragotti@dlapiper.com

Roberto Valenti
Partner, Milano
M: +39 33 57 36 61 84
roberto.valenti@dlapiper.com

Ginevra Righini
Partner, Milano
M: +39 34 82 35 64 48
ginevra.righini@dlapiper.com

Marco de Morpurgo
Partner, Roma
M: +39 34 27 74 00 23
marco.demorpurgo@dlapiper.com