# Il Parlamento europeo approva il Regolamento europeo sull'Intelligenza Artificiale: le implicazioni per il business

## I Approvazione e tempistiche di applicazione

In data 13 marzo il Parlamento europeo ha votato, a larga maggioranza, in favore della proposta di **Regolamento UE** recante regole armonizzate sull'intelligenza artificiale ("**Regolamento**"), meglio conosciuto come *Artificial Intelligence Act* ("**AI Act**").

Sebbene l'*iter* legislativo del testo finale del Regolamento non sia ancora concluso, essendo ancora soggetto a controllo finale a livello giuridico-linguistico e alla approvazione formale da parte del Consiglio, sembra ormai probabile la sua definitiva adozione entro l'estate.

Il Regolamento rappresenta il primo testo normativo organico del mondo in materia di intelligenza artificiale ed **entrerà in vigore dopo 20 giorni dalla pubblicazione sulla Gazzetta ufficiale dell'Unione**.

L'AI Act diverrà quindi **direttamente applicabile due anni dopo la sua entrata in vigore, fatta eccezione per alcune specifiche disposizioni**:

- le previsioni in materia di **divieti assoluti** saranno applicabili **sei mesi** dopo l'entrata in vigore;

- le previsioni relative ai **codici di condotta** diverranno applicabili **nove mesi** dopo l'entrata in vigore;

- le previsioni in materia di modelli di c.d. ***General Purpose AI*** ("**GPAI**") saranno applicabili **dodici mesi** dopo l'entrata in vigore;

- gli obblighi per i **sistemi ad alto rischio**, infine, diverranno applicabili **trentasei mesi** dopo l'entrata in vigore.


*Fonte: https://futurium.ec.europa.eu/fi/european-ai-alliance/open-discussion/more-visual-guide-proposed-eu-artificial-intelligence-act?language=en*

Cionondimeno, gli operatori economici europei ed extra-europei potranno decidere – **su base volontaria** - di **anticipare l'attuazione della disciplina** rispetto alle scadenze legali di cui *supra*, aderendo al cd. "**Patto sull'AI**" avviato dalla Commissione europea.

Tale sistema di attuazione precoce della normativa è volto a incoraggiare la *compliance* con le nuove regole **già a partire da quest'anno**, tramite l'adozione di dichiarazioni di impegno e piani di attuazione.

## II Ambito applicativo e principali previsioni del nuovo Regolamento

L'AI Act mira a promuovere lo sviluppo e l'utilizzo di **sistemi di AI sicuri e affidabili all'interno del mercato unico europeo**, garantendo il rispetto dei diritti fondamentali degli individui, dei principi democratici e della sostenibilità ambientale.

Alla luce della prossima pubblicazione del Regolamento, si fornisce di seguito una visione di sintesi delle principali previsioni della nuova disciplina.

**(1) Ambito di applicazione.** La definizione di "*AI systems*" adottata dal Regolamento risulta **allineata a quella da ultimo proposta in ambito OCSE**[1]. Essa include quindi quei sistemi progettati per operare con vari livelli di autonomia e che possono mostrare capacità di adattamento i quali, per obbiettivi espliciti o impliciti, deducono dagli *input* ricevuti come generare *output* quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali.

Risultano invece esclusi da tale definizione i ***software* di natura meno complessa**, gli **approcci di programmazione** e i sistemi che si basano su regole definite esclusivamente da persone fisiche per eseguire automaticamente le operazioni, nonché i sistemi di AI utilizzati unicamente per **scopi militari, di difesa, di ricerca e innovazione, ovvero per usi non professionali** (e, a determinate condizioni, quelli forniti con licenze *open-source*).

Dal punto di vista soggettivo, riveste particolare importanza la **natura extra-territoriale** della nuova disciplina: Il Regolamento troverà infatti applicazione **anche nei confronti dei soggetti e delle organizzazioni extra-UE**, sia nel caso in cui questi abbiano uno stabilimento all'interno dell'Unione, sia laddove questi – pur in assenza di uno stabilimento – offrano beni o servizi nel mercato unico.

**(2) Classificazione dei sistemi di AI: *risk-based approach*.** L'AI Act adotta un approccio basato sul rischio, **vietando anzitutto alcune pratiche il cui livello di rischio è considerato inaccettabile**. Tra di esse vi sono gli utilizzi per fini di **manipolazione comportamentale** cognitiva, ***social scoring***, **riconoscimento delle emozioni** in ambito lavorativo o educativo, ovvero per lo sfruttamento di **vulnerabilità** degli individui e di categorie vulnerabili.

Fermi tali divieti, l'architettura dell'AI Act distingue inoltre:

**(i) Sistemi di AI ad alto rischio**: quali ad esempio i sistemi utilizzati nell'ambito di dispositivi medici, veicoli, processi di *recruiting*, infrastrutture critiche, ovvero dell'accesso a servizi pubblici o privati essenziali (*e.g.* servizi sanitari, accesso al credito). Tali sistemi dovranno rispettare obblighi e requisiti specifici in materia di *risk & quality management*, *data governance*, trasparenza e *human oversight*, nonché di accuratezza, robustezza e *cybersecurity*. Inoltre, i sistemi *high-risk* – da iscriversi in un apposito pubblico registro europeo - potranno essere immessi sul mercato UE solo a fronte della conduzione di una valutazione di impatto sui diritti fondamentali e del superamento di una procedura di *conformity assessment*.

[1]Secondo tale definizione, "AI system" indica "*a machine-based system that, far exp/icit or imp/icit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments*" .

**(ii) Sistemi di AI a rischio minimo**: ricavabili in negativo a fronte della loro mancata inclusione tra i sistemi a rischio inaccettabile o alto, in relazione ai quali la disciplina non introduce nuovi obblighi – fatta salva la casistica di cui al successivo punto (*iii*) e salva in ogni caso la facoltà per le imprese di aderire a codici di condotta su base volontaria.

**(iii) Sistemi di AI soggetti a specifici rischi di trasparenza**: ovverosia i sistemi di AI destinati ad interagire direttamente con le persone fisiche, in relazione ai quali gli operatori dovranno adempiere ad obblighi significativamente meno onerosi, per lo più di natura informativa (ad esempio, in relazione all'uso di *chatbot*, chiarendo agli utenti che stanno conversando con una macchina a meno che ciò non sia ovvio dal punto di vista di una persona fisica ragionevolmente informata, attenta e prudente alla luce di circostanze e contesto di utilizzo).

**(3) *General-purpose AI models* (GPAI).** Uno dei punti maggiormente controversi delle negoziazioni relative all'AI Act ha riguardato la **disciplina applicabile ai c.d. GPAI**, ivi inclusi i *Large Generative Models* che possono essere utilizzati per molteplici scopi distinti, come la generazione di video, immagini e testi (si pensi ad esempio a ChatGPT, Gemini, Midjourney, etc.). In relazione a tali sistemi, il nuovo Regolamento prevede **degli obblighi trasversali a tutti i GPAI**, tra i quali quelli di rispettare la disciplina europea in materia di **diritto d'autore** e obblighi di natura documentale quali quello di mettere a disposizione del pubblico una sintesi dettagliata dei **contenuti utilizzati per l'addestramento dell'IA**. In aggiunta, sono stati introdotti dei criteri per determinare se i GPAI comportino dei **rischi sistemici**[2], nel qual caso i relativi sistemi sono sottoposti a requisiti aggiuntivi in materia di valutazione del modello, valutazione e mitigazione del rischio sistemico, test avversariali, *cybersecurity*, efficienza energetica e reporting di incidenti gravi alla Commissione europea.

[2]Secondo ii testo del Regolamento, la classificazione dei modelli GPAI come sistemi che comportano rischi sistemici dipendera inizialmente dalla capacita di calcolo di tali sistemi - basata su una soglia quantitativa della quantita cumulativa di calcolo utilizzata per l'addestramento e misurata in operazioni in virgola mobile (*Floating point operations per second* - FLOPs) - ovvero su una decisione di designazione individuale della Commissione. La soglia inziale di FLOPs e stata a tal fine fissata a $10^{25}$ FLOPs e la Commissione sara obbligata ad adattare tale soglia alla luce dell'evoluzione tecnologica .

**(4) *Regulatory sandboxes***. Il Regolamento prevede espressamente un obbligo in capo agli Stati membri (da soli, o in collaborazione tra loro) di **istituire delle *sandbox* regolamentari**, al fine di promuovere lo sviluppo di sistemi di AI in "ambiente protetto" - in particolar modo da parte delle PMI europee - prima della loro immissione sul mercato. Si tratta di un punto sul quale i parlamentari europei hanno posto particolare enfasi al fine di favorire l'emergere di attori europei nell'ambito dei sistemi di AI.

**(5) *Governance***. Il Regolamento prevede in primo luogo l'istituzione di un ***AI Board***, che fungerà da organo consultivo della Commissione europea. In seno alla Commissione europea è stato già istituito - con decisione dello scorso 24 gennaio - un ***AI Office***, il quale supervisionerà tra l'altro l'applicazione delle disposizioni per i modelli GPAI. Accanto ad essi, saranno costituiti ***(i)*** un ***Advisory Forum*** composto da *stakeholder* rappresentativi di industria, società civile e accademia, con funzioni consultive e ***(ii)*** uno ***Scientific Panel of independent experts***, con il compito di sostenere l'implementazione e l'attuazione delle previsioni applicabili ai modelli GPAI. Infine, ciascuno Stato membro è chiamato a individuare l'autorità di controllo competente a livello nazionale per l'*enforcement* dell'AI Act.

**(6) Non discriminazione**. Il Regolamento mira ad assicurare il rispetto dei **principi in materia di non discriminazione** (inclusa la parità di genere), introducendo requisiti specifici volti a ridurre al minimo il rischio di discriminazione algoritmica in relazione alla progettazione e alla qualità dei *data set* utilizzati per lo sviluppo dei sistemi di AI. Detti sistemi dovranno essere sviluppati in modo tale **evitare effetti discriminatori e pregiudizi ingiusti** e supportare la diversità, la non discriminazione e l'equità.

**(7) Sanzioni**. La violazione dell'AI Act comporterà **sanzioni di natura pecuniaria** che - secondo un approccio simile a quello del GDPR - potranno essere **parametrate al fatturato annuo globale** riferito all'esercizio finanziario precedente della società cui la violazione è contestata.

Segnatamente, si prevedono sanzioni fino a un importo massimo corrispondente:

> ***(i)* a 35 milioni di Euro o al 7% del fatturato** (qualunque sia il più alto) per la violazione delle norme in materia di pratiche vietate;
>
> ***(ii)* a 15 milioni di Euro o al 3% del fatturato** (qualunque sia il più alto) per la gran parte delle altre violazioni, ivi incluse quelle relative

alle disposizioni in materia di GPAI; e

***(iii)*** **a 7.5 milioni di Euro o a11'1% del fatturato** (qualunque sia il più alto) per la violazione di obblighi informativi.

Per le violazioni commesse da PMI e start-up, inoltre, si prevede un criterio di favore nella quantificazione di una sanzione pari all'importo inferiore tra quelli risultanti dall'applicazione delle percentuali o degli importi massimi applicabili alla specifica violazione, di cui supra.

## III Implicazioni per gli operatori economici

Seppure l'applicazione in concreto del Regolamento sia soggetta alla *timeline* di cui al paragrafo 1 che precede, è opportuno delineare sin d'ora le coordinate della strategia di *compliance* in materia di AI e talune azioni cruciali ai fini dell'adozione progressiva e prospettica dei presidi richiesti dall'AI Act.

• **Piani d'azione**. Poiché l'adeguamento alla normativa richiederà del tempo, è opportuno che gli operatori economici comincino a predisporre delle *roadmap di compliance*, anche alla luce della circostanza che alcuni degli obblighi di cui all'AI Act troveranno applicazione anticipata rispetto al termine generale di 24 mesi dall'approvazione.

• **Mappatura**. L'implementazione di azioni di *compliance* con la normativa implica lo svolgimento di valutazioni preliminari in relazione, tra gli altri, al novero e alle caratteristiche dei sistemi di AI che si intendono sviluppare, commercializzare e/o adottare, agli utilizzi previsti di tali sistemi (inclusi i relativi rischi) e al ruolo giocato dall'operatore economico in relazione ad essi. A tal riguardo, ad esempio, sarà fondamentale determinare se i sistemi di AI presi in considerazione possano essere ritenuti ricadere nelle ipotesi di divieto, ovvero in quelle considerate "ad alto rischio", o "discriminatorie", circostanze dalle quali possono discendere importanti conseguenze in termini di requisiti di *compliance*.

• **Modelli di *governance***. L'adozione e l'utilizzo di sistemi di AI dovrebbero trovare adeguato riflesso nella strutturazione di modelli di *governance* volti a garantire una chiara allocazione dei connessi poteri decisionali e di gestione all'interno dell'organizzazione dell'ente, garantendone *l'accountability* (se del caso, anche mediante il coinvolgimento di esperti esterni alla società).

• **Policy e procedure**. Senza pregiudizio per gli obblighi previsti dall'AI Act, gli operatori economici sono incoraggiati a verificare le proprie iniziative di *compliance* anche alla luce delle buone prassi di settore e ai principi generali in materia di utilizzo responsabile di sistemi di AI ricavabili da documenti adottati in sedi sovranazionali (tra i quali le "*Ethics guidelines for trustworthy AI*" adottate in ambito UE[3], gli "*AI Principles*" adottati in sede OCSE[4], ovvero ancora alla proposta di "*Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law*[5]" del Consiglio d'Europa), così come a modelli virtuosi adottati o in fase di adozione da parte di grandi *player* di mercato. Una prima revisione delle policy e procedure può estendersi, ad esempio, alla gestione del *procurement* da parte di fornitori terzi, nonché alle attività di *audit* sui fornitori stessi, anche al fine di incoraggiare l'uso etico dell'AI e non discriminatorio.

• **Documentazione**. Che si tratti di valutazioni preliminari circa la possibile adozione di strumenti di AI o dell'implementazione di *use-case* circoscritti e poi sempre più ambiziosi, quella di documentare tutte le valutazioni e le scelte effettuate in relazione ai sistemi di AI rappresenta una *best-practice* consolidata, al fine di rendere più agevole la *compliance* con la nuova normativa e garantire una robusta *accountability*. A tal fine rilevano, ad esempio, le valutazioni in relazione ai rischi dell'utilizzo di sistemi di AI per i diritti fondamentali degli individui.

• **Formazione continua e mirata**. Le competenze tecniche richieste ai fini dell'adozione di sistemi di AI e i rischi correlati al loro utilizzo rendono opportuna la strutturazione di percorsi formativi mirati e documentabili per tutti i soggetti che, a diverso titolo, sono o saranno coinvolti nell'implementazione tali sistemi.

• **Rapporto con le altre normative**. Lo sviluppo e l'adozione di sistemi di AI sono sottoposti all'applicazione di ulteriori fonti normative già esistenti, quali ad esempio il GDPR. A tal proposito, gli operatori economici sono incoraggiati a valutare soluzioni e processi che permettano di efficientare la gestione degli adempimenti e dei rischi di conformità normativa in un'ottica di *compliance* integrata.

---

[3] *Disponibile al seguente link: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai*

[4] Disponibile al seguente link: https://oecd.ai/en/ai-principles.

[5] Disponibile al seguente link: https://rm.coe.int/cai-2023-28-draft-framework-convention/1680ade043.

• **Patto per l'AI**. Lo strumento di *compliance* anticipata previsto dalla Commissione europea rappresenta un'opportunità per gli operatori economici che, strutturando un piano di conformità graduale, avrebbero il vantaggio di ***(i)*** avere già avviato le prime fasi del percorso di adeguamento e strategia di compliance quando l'AI Act diverrà applicabile, ***(ii)*** rafforzare la propria posizione competitiva sul mercato, nonché ***(iii)*** aumentare la relazione di fiducia con i propri clienti e/o *stakeholder*. La Commissione ha già predisposto una piattaforma online dedicata[6] per raccogliere le manifestazioni di interesse al progetto.

---

## Contatti

**Pierluigi Perri**
Of Counsel – Chiomenti
Data Protection & Cybersecurity
T. +39.02.721.571
pierluigi.perri@chiomenti.net

**Marilena Hyeraci**
Of Counsel – Chiomenti
Data Protection & Cybersecurity
T. +39. 02.721.571
marilena.hyeraci@chiomenti.net

**Matteo Leffi**
Associate - Chiomenti
Data Protection & Cybersecurity
T. +39. 02 72157 717
matteo.leffi@chiomenti.net

**Tommaso Bratina**
Trainee - Chiomenti
Data Protection & Cybersecurity
T. +39. 02 72157 717
tommaso.bratina@chiomenti.net

---

[6] *Si riporta di seguito il link della piattaforma: https://ec.europa.eu/eusurvey/runner/68fd7335-f477-b1a7-f52f-e51b60a825b5.*