Il testo in arrivo si applicherà a un numero limitato di sistemi di intelligenza artificiale

IA, la rivoluzione che non c'è: il regolamento Ue è per pochi

Pagina a cura
DI MATTEO RIZZI

Intelligenza artificiale, la rivoluzione regolamentare che non c'è. Il tanto atteso regolamento sull'intelligenza artificiale (AI Act), definito dai legislatori europei come la prima legge al mondo che disciplina il funzionamento dei sistemi di IA, sembra lontano dall'essere una norma impregnante che andrà a impattare lo sviluppo della tecnologia. Tanto che è la stessa Commissione europea a sottolineare come "la maggior parte dei sistemi di intelligenza artificiale presenta rischi minimi o nulli" ed è quindi escluso dai contenuti del regolamento. Tuttavia, è altrettanto importante ricordare che il testo si preme di indirizzare i potenziali rischi derivanti dall'intelligenza artificiale in relazione alla salute, la sicurezza e i diritti fondamentali, così come tutela anche la democrazia, lo stato di diritto e l'ambiente.

Il testo definitivo è stato approvato il 2 febbraio 2024 dal Comitato dei rappresentanti permanenti dei governi degli Stati membri dell'Unione europea (Coreper I), il principale organo preparatorio del Consiglio Ue, e ora dovrà essere approvato formalmente dal Consiglio e anche dalla plenaria del Parlamento europeo in aprile. Ma nonostante siano ancora necessari alcuni passaggi formali prima che il testo dell'AI act sia pubblicato nella Gazzetta ufficiale dell'Ue, la versione del testo ad oggi pervenuta è quella definitiva a cui si è giunti all'inizio di dicembre dopo lunghi negoziati all'interno del trilogo tra Consiglio, Parlamento e Commissione.

I soggetti interessati. Il regolamento si applicherà sia agli attori pubblici che privati all'interno e all'esterno dell'Ue, purché il sistema di intelligenza artificiale sia posto sul mercato dell'Unione o il suo utilizzo interessi persone situate nell'Ue.

Ciò può riguardare sia i fornitori (ad esempio, uno sviluppatore di uno strumento di screening dei CV) che gli utilizzatori di sistemi di intelligenza artificiale ad alto rischio (ad esempio, una società che acquista questo strumento di screening). Gli importatori di sistemi di intelligenza artificiale dovranno, inoltre, garantire che il fornitore straniero abbia già effettuato la procedura di valutazione della conformità appropriata, porti la marcatura di conformità europea (CE) e sia accompagnato dalla documentazione e dalle istruzioni d'uso richieste.

I fornitori di modelli gratuiti e open-source sono esentati dalla maggior parte delle obbligazioni, esenzione che comunque non copre le obbligazioni per i fornitori di modelli di intelligenza artificiale a uso generale con rischi sistemici.Il regolamento, in aggiunta, non si applicherà alle attività di ricerca, sviluppo e di prototipi precedenti la commercializzazione. Inoltre, il regolamento esclude i sistemi di intelligenza artificiale a scopo esclusivamente militare, di difesa o di sicurezza nazionale, indipendentemente dal tipo di entità che svolge tali attività.

I modelli GpAI. Oltre ai sistemi di AI ad alto rischio e quelli proibiti (si veda pagina seguente), il regolamento assegna regole speciali per i modelli GpAI (modelli generali), quei modelli addestrati su una grande quantità di dati su larga scala, in grado di eseguire una serie di compiti e che possono essere integrati in altri sistemi di intelligenza artificiale, alcuni esempi sono proprio ChatGpt di OpenAI o Bard (ora Gemini) di Google. Alcuni di questi modelli generali, inoltre, creano un "rischio sistemico" e quindi soggetti a requisiti ancora più stringenti.

Gli obblighi per i modelli GpAI (articoli 52a – 52e), includono requisiti di trasparenza lo sviluppo e la messa a disposizione, su richiesta, di documentazione tecnica all'Ufficio AI istituito in sede Ue e alle autorità nazionali competenti. Includono anche la fornitura di informazioni e documentazione ai fornitori a valle ai fini del rispetto della legge sull'AI. Per quanto riguarda il diritto d'autore, il regolamento stabilisce che i fornitori di modelli GpAI dovranno attuare una politica per rispettare la normativa dell'Unione sul diritto d'autore, nonché rendere pubblicamente disponibile una sintesi sufficientemente dettagliata del contenuto utilizzato per la formazione del modello di IA.

I requisiti aggiuntivi per i modelli con rischi sistemici, includono la notifica alla Commissione europea della presenta di un rischio sistemico nel proprio modello, la valutazione del rischio e la conseguente adozione di misure di mitigazione del rischio, la garanzia di un livello adeguato di protezione della sicurezza informatica e la segnalazione di incidenti gravi all'Ufficio AI e alle autorità nazionali competenti. Il rispetto di questi requisiti può essere raggiunto attraverso codici di condotta, che saranno sviluppati dall'industria, con la partecipazione degli stati membri (attraverso il Consiglio sull'IA istituito in sede Ue) e facilitati dall'AI Office.

Attualmente, la classificazione dei modelli GpAI con rischi sistemici dipende dalla capacità, sia sulla base di una soglia quantitativa della quantità cumulativa di calcolo utilizzato per l'addestramento misurato in Flop (FLoating point Operations Per Second indica il numero di operazioni in virgola mobile eseguite in un secondo dalla Cpu), sia su una decisione di designazione individuale della Commissione che tiene conto dei criteri elencati nell'allegato IXc (ad esempio il numero di parametri, la qualità e la dimensione del set di dati, le modalità di input e output o le misure di portata negli utenti aziendali). La soglia Flop iniziale è stata fissata a 10^25, tuttavia, la Commissione sarà obbligata ad adattare la soglia alla luce dell'evoluzione degli sviluppi tecnologici.

I punti chiave del regolamento sull'intelligenza artificiale *(AI Act)*

Definizione	Per "sistema di intelligenza artificiale" si intende un sistema basato su una macchina progettato per operare con vari livelli di autonomia e che può mostrare capacità di adattamento dopo l'implementazione e che, per obiettivi espliciti o impliciti, deduce, dagli input ricevuti, come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali
Ambito di applicazione	• Si applica lungo la catena del valore dell'IA: a fornitori (cioè, sviluppatori e aziende che istruiscono lo sviluppo), importatori, distributori, produttori e utilizzatori (cioè, utenti commerciali) di determinati sistemi di intelligenza artificiale • Colpiti anche imprese e individui al di fuori dell'Ue che "per la prima volta mettono sul mercato" o installano per primi sistemi di intelligenza artificiale nell'Ue
Categorie di rischio	Più alto è il rischio, più severe sono le regole • Sono vietati i sistemi di intelligenza artificiale che presentano un "rischio inaccettabile" • Alcuni sistemi di intelligenza artificiale, compresi quelli che interagiscono direttamente con le persone, sono soggetti ad obblighi di trasparenza • Se un sistema di intelligenza artificiale non rientra in nessuna delle categorie di rischio, non è soggetto all'AI Act: l'Ue prevede che la maggior parte dei sistemi di intelligenza artificiale ricada in questa categoria
Sanzioni	• 35 milioni di euro o il 7% del fatturato annuo globale per la violazione delle regole sui sistemi di intelligenza artificiale vietati • 15 milioni di euro o il 3% del fatturato annuo globale per le violazioni di altri obblighi • 7,5 milioni di euro o l'1% del fatturato annuo globale per la fornitura di informazioni errate
Scadenze	Periodo di transizione di due anni per la conformità a partire dall'entrata in vigore, ad eccezione… • I sistemi di intelligenza artificiale vietati saranno bandati da 6 mesi dopo l'entrata in vigore del regolamento • Le regole per l'IA a scopi generali si applicheranno 12 mesi dopo l'entrata in vigore del regolamento
Governace	• L'applicazione e l'implementazione dell'AI Act a livello nazionale saranno gestite dalle autorità designate dallo stato membro pertinente • Un Ufficio AI dell'Ue si occuperà dell'impostazione degli standard, dell'applicazione e delle attività amministrative a livello dell'Ue • Un Consiglio AI dell'Ue faciliterà l'applicazione coerente ed efficace • Sarà istituito un panel scientifico di esperti indipendenti con "competenze scientifiche o tecniche aggiornate"