AI Act, il 2 agosto entrano in vigore le regole per l'intelligenza artificiale generativa

Più trasparenza sui dati utilizzati e rispetto del diritto d'autore. Dal 2 agosto i Paesi membri dovranno dotarsi di un'autorità di vigilanza (Fonte: https://www.corriere.it/ 1°agosto 2025)

Le prime regole - e i primi divieti - imposti dall'Artificial Intelligence Act dell'Unione europea sono già entrate in vigore lo scorso febbraio. Erano le più urgenti, dato che riguardavano applicazioni ed usi «**a rischio inaccettabile**» e che dunque dovevano essere banditi al più presto. Tra queste, il social scoring, la polizia predittiva, l'analisi delle emozioni a scuola o sul luogo di lavoro. Siamo ora arrivati al secondo importante momento di protagonismo della **nuova regolamentazione europea** e che riguarda la categoria di «**sistemi ad alto rischio**» e in particolare le **limitazioni sull'intelligenza artificiale ad uso generale**. Noi la chiamiamo più comunemente intelligenza artificiale generativa. Per chi la sviluppa, dal **2 agosto** ci saranno dei paletti da rispettare, che hanno l'obiettivo di salvaguardare gli utenti ma anche il diritto d'autore.

Il codice di condotta

Per aiutare le aziende a conformarsi a ciò che chiede l'AI Act, la Commissione europea ha chiesto a un gruppo di esperti di creare un documento: **una sorta di codice di condotta** che contiene le linee guida da seguire e i moduli necessari per poter trasmettere tutte le informazioni richieste. L'aiuto è pensato anche per dare dei vantaggi a chi decide di collaborare in modo proattivo. Chi firma il documento potrà anche avere un «**onere amministrativo ridotto e una maggiore certezza giuridica**». Insomma, tutti dovranno seguire le regole se vogliono operare in Europa, ma chi

aderisce al codice di condotta - e dunque vuole aderire a pieno, con le forme proposte dall'Europa stessa - rientrerà in una sorta di «gruppo speciale» con più libertà e meno occhi puntati addosso. L'invito è però non è stato accolto da tutti. Tra i colossi dell'intelligenza artificiale generativa, al momento **OpenAI** ha già firmato, mentre **Google, Microsoft e Anthropic** hanno dichiarato che lo faranno. Gli altri ci stanno ancora pensando. Mentre un rifiuto netto è arrivato al momento da **Meta**, da sempre molto critica verso l'AI Act.

Le regole per l'AI generativa in Europa

L'AI generativa è considerata **ad alto rischio**, in quanto può recare **danno ai cittadini e alla democrazia** stessa. In particolare perché potenziale creatrice di **Deep Fake**, e dunque di immagini, video e audio manipolati ma che appaiono come reali. Qualora il contenuto generato da ChatGpt o altri strumenti simili ritragga persone, oggetti, luoghi o altre entità ed eventi reali, dovrà essere **dichiarato in modo evidente con una etichetta** che quel contenuto è stato creato da un software. L'affondo sulla trasparenza non si esaurisce qui. Per questi sistemi si dovrà anche spiegare nel dettaglio **quali dati sono stati utilizzati** per allenare i modelli di linguaggio su cui si basano, le risorse computazionali e il consumo energetico. E poi c'è il rispetto delle leggi europee sul **copyright**. L'articolo di riferimento è il **numero 53**.

L'altro tema affrontato dal codice di condotta è quello relativo alla sicurezza. Un grande cappello dentro cui stanno diversi obblighi e richieste, alcuni piuttosto chiari altri più complessi da mettere in pratica. Le società firmatarie del documento si impegnano a condurre **test periodici per identificare e mitigare i «rischi sistemici»** dei loro modelli. Per farlo, gli si richiede di creare un «**framework**», un processo ben definito da adottare per evitare che l'intelligenza artificiale da loro sviluppata possa essere sfruttata per creare rischi o danni alla sicurezza pubblica. Nel documento di riferimento c'è **un lungo elenco di rischi sistemici considerati inaccettabili,** ovvero di «capacità» che i modelli non possono avere e devono essere identificati. Più complesso è il tema della **mitigazione dei rischi di diffusione di disinformazione e contenuti dannosi**. Su questo punto il codice di condotta non è preciso.

L'autorità vigilante

Sempre il 2 agosto diventa effettivo anche un altro obbligo richiesto dall'AI Act, che in questo caso riguarda i Paesi membri. **Tutti e 27 dovranno dotarsi di autorità di vigilanza** dedicate a monitorare se le disposizioni del regolamento vengono rispettate nel territorio nazionale. Sono tre i filoni di controllo: **una sorveglianza del mercato**, un soggetto in grado d'**identificare e mettere a terra tutte le procedure di notifiche** su possibili situazioni di non conformità e infine **un'autorità nazionale** che si concentri soprattutto sui sistemi ad alto rischio. I Paesi membri avevano un anno di tempo per organizzarsi dall'entrata in vigore dell'AI Act (fino, appunto, al 2 agosto 2025). A novembre 2024 erano solo tre i Paesi che avevano spiegato in modo concreto come

intendono procedere: la Lituania, il Lussemburgo, Malta. Nel caso dell'**Italia**, l'identificazione dell'Autorità di Vigilanza è parte del **disegno di legge** «**Disposizioni e deleghe al governo in materia di intelligenza artificiale**», al momento in discussione al Senato. All'articolo 18 si nominano due enti «per garantire l'applicazione e l'attuazione della normativa»: **l'Agenzia per l'Italia digitale e l'Agenzia per la cybersicurezza nazionale.**