Avvenire 09.12.2023
Ilaria Solaini

Dopo un negoziato durato oltre 36 ore, il cosiddetto "trilogo" formato dalla Commissione europea, il Consiglio dell'Unione europea e il Parlamento hanno **raggiunto l'accordo sul testo dell'*AI Act*, la legge europea sull'intelligenza artificiale.** Si tratta del primo quadro normativo sui sistemi di IA nel mondo che vorrebbe garantire che i sistemi di intelligenza artificiale immessi sul mercato europeo e utilizzati nell'Ue siano sicuri e rispettino i diritti fondamentali e i valori dell'Ue. E, allo stesso tempo, stimolare gli investimenti e l'innovazione nell'AI in Europa.

***AI Act*, come si regolamenta l'utilizzo dell'IA**
L'idea alla base del testo concordato è quella di regolamentare l'intelligenza artificiale in base alla capacità di quest'ultima di causare danni alla società seguendo un approccio "basato sul rischio": si va dal rischio minimo a quello inaccettabile; maggiore è il rischio, più severe sono le regole. La stragrande maggioranza dei sistemi di intelligenza artificiale rientra nella categoria del rischio minimo e beneficeranno di un free-pass.

I sistemi di intelligenza artificiale identificati come ad alto rischio saranno tenuti invece a rispettare requisiti rigorosi, tra cui sistemi di mitigazione del rischio, alta qualità dei set di dati, registrazione delle attività, documentazione dettagliata, informazioni chiare sugli utenti, supervisione umana e un alto livello di robustezza, accuratezza e sicurezza informatica. Esempi di sistemi di intelligenza artificiale ad alto rischio includono alcune infrastrutture critiche, ad esempio nei settori dell'acqua, del gas e dell'elettricità; dispositivi medici; sistemi per determinare l'accesso alle istituzioni educative o per reclutare persone; o alcuni sistemi utilizzati nei settori delle forze dell'ordine, del controllo delle frontiere, dell'amministrazione della giustizia e dei processi democratici. Inoltre, anche i sistemi di identificazione biometrica, categorizzazione e riconoscimento delle emozioni sono considerati ad alto rischio.

Il rischio inaccettabile riguarda i sistemi di intelligenza artificiale considerati una chiara minaccia ai diritti fondamentali delle persone e saranno vietati. Questa blacklist include sistemi o applicazioni di intelligenza artificiale che manipolano il comportamento umano per aggirare il libero arbitrio degli utenti, come giocattoli che utilizzano l'assistenza vocale che incoraggiano comportamenti pericolosi dei minori o sistemi che consentono il "punteggio sociale" da parte di governi o aziende e alcune applicazioni di polizia predittiva.

Riconoscimento biometrico: quando è permesso utilizzarlo?
Nel corso dei tre giorni di negoziati si è faticato a trovare una mediazione sul sistema di riconoscimento biometrico. Alcuni usi dei sistemi biometrici saranno vietati, ad esempio i sistemi di riconoscimento delle emozioni utilizzati sul posto di lavoro e alcuni sistemi per la categorizzazione delle persone o il riconoscimento facciale in tempo reale ai fini delle forze dell'ordine in spazi accessibili al pubblico (con eccezioni ristrette). L'accordo raggiunto chiarisce gli obiettivi in cui tale uso è strettamente necessario ai fini dell'applicazione della legge e per i quali le autorità incaricate dell'applicazione della legge dovrebbero quindi essere eccezionalmente autorizzate a utilizzare tali sistemi. **L'accordo prevede ulteriori garanzie e limita queste eccezioni ai casi di vittime di determinati reati, alla prevenzione di minacce reali, presenti o prevedibili, come gli attacchi terroristici e alla ricerca di persone sospettate dei crimini più gravi.**

Vi è poi la **categoria dei rischi specifici**, quali le ormai famose **chatbot**. Quando le utilizzano, gli utenti dovrebbero essere consapevoli che stanno interagendo con una macchina. I deepfake e altri contenuti generati dall'IA dovranno essere etichettati come tali e gli utenti devono essere informati quando vengono utilizzati sistemi di categorizzazione biometrica o di riconoscimento delle emozioni. Inoltre, i fornitori dovranno progettare sistemi in modo che i contenuti audio, video, testo e immagini sintetici siano contrassegnati in un formato leggibile dalla macchina e rilevabili come generati o manipolati artificialmente.

***AI Act*, dove si applicherà la nuova legge?**

Salutato come un modello per gestire la tecnologia IA a livello globale l'*AI Act* potrebbe fungere da punto di riferimento per quei Paesi che cercano un'alternativa all'approccio soft degli Stati Uniti e alle regole provvisorie della Cina. Il regolamento non si applica a settori al di fuori del campo di applicazione del diritto dell'Ue e non dovrebbe, in ogni caso, pregiudicare le competenze degli Stati membri in materia di sicurezza nazionale o qualsiasi entità incaricata di compiti in questo settore.

Le multe per le violazioni della legge sono state fissate come percentuale del fatturato annuo globale della società incriminata nell'anno finanziario precedente o come un importo predeterminato, a seconda di quale sia il più alto. Si tratterebbe di 35 milioni di euro o del 7% per le violazioni delle applicazioni vietate, di 15 milioni di euro o del 3% per le violazioni degli obblighi della legge e di 7,5 milioni di euro o dell'1,5% per la fornitura di informazioni errate. Tuttavia, l'accordo provvisorio prevede massimali più proporzionati sulle ammende amministrative per le Pmi e le start-up in caso di violazioni delle disposizioni della legge sull'intelligenza artificiale. Per alleviare l'onere amministrativo per le imprese più piccole, l'accordo provvisorio include un elenco di azioni da intraprendere a sostegno di tali operatori e prevede alcune deroghe limitate e chiaramente specificate.

L'accordo prevede che la *AI Act* si applichi due anni dopo la sua entrata in vigore, con alcune eccezioni per disposizioni specifiche, nel contempo, l'Autorità per la concorrenza e i mercati del Regno Unito (CMA) sta valutando se avviare **un'indagine sulla partnership tra Microsoft e OpenAI, cercando di accertare se la collaborazione tra le due aziende in qualche modo possa avere un impatto sul mercato e in qualche misura minacciare la concorrenza**.