Ue. AI Act approvato, l'Europa avrà il primo regolamento sull'intelligenza artificiale
I.Sol. venerdì 2 febbraio 2024

Manca il voto all'Europarlamento.
Nella riunione dei Rappresentanti Permanenti dei 27 (Coreper I) è stato votato il testo sull'intelligenza artificiale, sul quale a dicembre era stata trovata l'intesa

La riunione dei Rappresentanti Permanenti dei 27 (Coreper I) ha dato l'atteso **via libera** all'***AI Act***, il nuovo **sistema di regole dell'Ue sull'intelligenza artificiale.** Lo scorso 9 dicembre era stato trovato l'accordo politico sul primo insieme di regole vincolanti al mondo per l'intelligenza artificiale.

L'Unione Europea si avvia a diventare la prima grande potenza mondiale che dispone di un quadro normativo sui sistemi di IA. L'Ue è la prima a stabilire norme vincolanti per la tecnologia dell'intelligenza artificiale in rapida evoluzione. Anche se molti Paesi e organizzazioni internazionali – dall'OCSE al G7 – hanno passato gli ultimi anni a riflettere su come regolamentare l'intelligenza artificiale, la maggior parte si è attenuta a linee guida o codici di condotta volontari.

Cosa succederà ora? Il testo passerà all'Europarlamento dove la partita dovrebbe essere più semplice. Il percorso si dovrebbe concludere entro aprile, ma ciò non vuol dire che tutte le nuove regole entreranno in vigore immediatamente. Si procederà per gradi: dopo sei mesi si attueranno i divieti e dopo altri sei le norme sui modelli fondativi. Insomma, ci vorrà un anno.

Il regolamento 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. Allo stesso tempo, continuando a favorire gli investimenti e l'innovazione nell'ambito dell'IA in Europa. 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. Se la stragrande maggioranza dei sistemi di intelligenza artificiale rientra nella categoria del rischio minimo e dunque non creerà problemi alla società e non ne avrà nell'adeguamento alla normativa, 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. Nello specifico, tra gli esempi di sistemi di intelligenza artificiale ad alto rischio ci sono alcune infrastrutture critiche, come nei settori dell'acqua, del gas e dell'elettricità; ma anche i dispositivi medici; i 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. **Uno dei nodi su cui maggiormente si è discusso riguardava i sistemi di identificazione biometrica, considerati ad alto rischio.** Alcuni usi dei sistemi biometrici saranno vietati, ad esempio i sistemi di riconoscimento delle emozioni utilizzati sul posto di lavoro, alcuni sistemi di profiling delle persone basati su sesso o etnia e 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 necessario ai fini dell'applicazione della legge e per i quali le autorità incaricate dell'applicazione della legge dovrebbero essere eccezionalmente autorizzate a utilizzare tali sistemi. È il caso, ad esempio, di attacchi terroristici imminenti, di ricerca di vittime, di indagini che riguardano reati gravi come omicidi, sequestri, violenza sessuale.

Il rischio inaccettabile riguarda i sistemi di intelligenza artificiale considerati una minaccia ai diritti fondamentali delle persone, che 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, incoraggiando comportamenti pericolosi dei minori o sistemi che consentono il "punteggio sociale" da parte di governi e aziende, oltre ad alcune applicazioni di polizia predittiva assolutamente vietate. Vi è

poi la categoria dei rischi specifici, che riguardano i sistemi di intelligenza artificiale generativa, le note 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 dovranno 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.

Le multe per le violazioni possono essere da 7,5 milioni di euro o l'1,5% del fatturato a 35 milioni di euro o il 7% del fatturato globale.

Il gruppo imprenditoriale DigitalEurope aveva criticato già a dicembre scorso le regole stabilite dall'Unione Europea definendole un ulteriore onere per le aziende. «Abbiamo un accordo, ma a quale costo?», aveva affermato il direttore generale di DigitalEurope, Cecilia Bonefeld-Dahl. Altrettanto critico era stato il gruppo per i diritti sulla privacy European Digital Rights. «È difficile essere entusiasti di una legge che, per la prima volta nell'Ue, ha adottato misure per legalizzare il riconoscimento facciale pubblico in tempo reale», aveva affermato la sua consulente politica senior Ella Jakubowska. «Il Parlamento si è battuto duramente per limitare i danni, ma il pacchetto complessivo sulla sorveglianza biometrica e sulla profilazione è, nella migliore delle ipotesi, tiepido».