La tecnologia e le leggi

Regolare l'intelligenza artificiale È l'Europa la prima a provarci

ILARIA SOLAINI


Avvenire PRIMO piano

La tecnologia e le leggi

Regolare l'intelligenza artificiale È l'Europa la prima a provarci

«La biometria sarà possibile soltanto in casi molto gravi»

Servono norme a livello globale. Per ora abbiamo solo intese di principio

Milano Dopo un negoziato durato oltre 36 ore è stato raggiunto l'accordo sul testo dell'AI Act, laprima legge europea sull'intelligenza artificiale (IA). Con quest'intesa tutta politica, maturataattraverso un'estenuante discussione durata tre giorni, nel quinto e ultimo "trilogo" formato dallaCommissione europea, dal Consiglio dell'Unione europea e dal Parlamento europeo, l'Unione Europea siavvia a diventare la prima grande potenza mondiale che dispone di un quadro normativo sui sistemi diIA. L'accordo andrà votato, solo alcuni dettagli potrebbero ancora cambiar forma nel testo di leggefinale, che dovrà essere adottato dal Parlamento e dal Consiglio per diventare legge. Il commissarioeuropeo al mercato interno, Thierry Breton nel riconoscere il ruolo regolatore e di «pioniera»dell'Unione Europea ha definito quella di ieri una «giornata storica». Ma cosa prevede l'accordopolitico raggiunto? E quali sono i punti critici per le aziende tecnologiche che sviluppano sistemi diintelligenza artificiale? Intanto il regolamento vorrebbe garantire che i sistemi di intelligenzaartificiale immessi sul mercato europeo e utilizzati nell'Ue siano sicuri e rispettino i dirittifondamentali e i valori dell'Ue. E che continuino, allo stesso tempo, a favorire gli investimenti el'innovazione nell'ambito dell'IA in Europa. L'idea alla base del testo concordato è quella diregolamentare l'intelligenza artificiale in base alla capacità di quest'ultima di causare danni allasocietà 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 diintelligenza artificiale rientra nella categoria del rischio minimo e dunque non creerà problemi allasocietà e non ne avrà nell'adeguamento alla normativa, i sistemi di intelligenza artificialeidentificati come ad alto rischio saranno tenuti, invece, a rispettare requisiti rigorosi, tra cuisistemi 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 dirobustezza, accuratezza e sicurezza informatica. Nello specifico, tra gli esempi di sistemi diintelligenza artificiale ad alto rischio ci sono alcune infrastrutture critiche, come nei settoridell'acqua, del gas e dell'elettricità; ma anche i dispositivi medici; i sistemi per determinarel'accesso alle istituzioni educative o per reclutare persone; o alcuni sistemi utilizzati nei settoridelle forze dell'ordine, del controllo delle frontiere, dell'amministrazione della giustizia e deiprocessi democratici. L'ultimo nodo a essere sciolto nella discussione durata tre giorni riguardava isistemi di identificazione biometrica, considerati ad alto rischio. Alcuni usi dei sistemi biometricisaranno vietati, ad esempio i sistemi di riconoscimento delle emozioni utilizzati sul posto di lavoro,alcuni sistemi di profilazione delle persone basati su sesso o etnia. Così come vietato sarà il

riconoscimento facciale in tempo reale e in spazi pubblici, con eccezioni ristrette per le forzedell'ordine autorizzate a utilizzare tali sistemi solo in casi specifici. Ad esempio in caso diattacchi terroristici imminenti, di ricerca di vittime, di indagini che riguardano reati gravi comeomicidi, sequestri, violenza sessuale.

Il rischio inaccettabile riguarda i sistemi di intelligenza artificiale considerati una minaccia aidiritti fondamentali delle persone, che saranno vietati. Questa "lista nera" include sistemi oapplicazioni di intelligenza artificiale che manipolano il comportamento umano per aggirare il liberoarbitrio degli utenti, come giocattoli che utilizzano l'assistenza vocale, incoraggiando comportamentipericolosi 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 deirischi specifici, che riguardano i sistemi di intelligenza artificiale generativa, le note chatbot.Quando le utilizzano, gli utenti dovrebbero essere consapevoli che stanno interagendo con unamacchina. I deep fake e altri contenuti generati dall'IA dovranno essere etichettati come tali e gliutenti dovranno essere informati quando vengono utilizzati sistemi di categorizzazione biometrica o diriconoscimento delle emozioni. Inoltre, i fornitori dovranno progettare sistemi in modo che icontenuti audio, video, testo e immagini sintetici siano contrassegnati in un formato leggibile dallamacchina e rilevabili come generati o manipolati artificialmente. Le multe per le violazioni possonoessere da 7,5 milioni di euro o l'1,5% del fatturato a 35 milioni di euro o il 7% del fatturatoglobale. L'associazione delle imprese tecnologiche Digital Europe ha criticato le regole definendoleun ulteriore onere per le aziende. «Abbiamo un accordo, ma a quale costo? », ha affermato il direttoregenerale Cecilia Bonefeld-Dahl. Altrettanto critico il gruppo per i diritti sulla privacy EuropeanDigital Rights. «È difficile essere entusiasti di una legge che, per la prima volta nell'U, haadottato misure per legalizzare il riconoscimento facciale pubblico in tempo reale», ha affermato lasua consulente politica senior Ella Jakubowska. «Il Parlamento si è battuto duramente per limitare idanni, ma il pacchetto complessivo sulla sorveglianza biometrica e sulla profilazione è, nellamigliore delle ipotesi, tiepido». RIPRODUZIONE RISERVATA I parlamentari Dragoş Tudorache e BrandoBenifei, la ministra spagnola Carme Artigas e il commissario Ue Thierry Breton presentano l'AI Act.