PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 25 - numero 5528 di Mercoledì 20 dicembre 2023

Legge sull'intelligenza artificiale

L'accordo tra Consiglio e Parlamento definisce, primo al mondo, le regole per l'utilizzo della IA. Gli elementi principali dell'accordo provvisorio.

I titoli di molti prestigiosi quotidiani hanno annunciato che ormai è pronto il documento dell'unione europea, che indica come gestire gli applicativi di intelligenza artificiale. Forse è il caso di chiarire meglio cosa vi è dietro questi titoli.

Ricordo ai lettori che un documento legislativo europeo viene ufficialmente pubblicato solo quando si raggiunge un accordo fra tre enti dell'unione europea. Questo accordo viene stipulato ad un livello preliminare, che permette di elaborare una proposta di norma; successivamente questa proposta deve essere approvata dal parlamento europeo. Solo a questo punto siamo in presenza di una disposizione legislativa, valida per tutti paesi dell'unione europea. La disposizione legislativa può essere di indirizzo, e si chiama in tal caso **direttiva**, oppure vincolante, e si chiama **regolamento**.

Dopo una maratona di tre giorni, la presidenza del Consiglio della unione Europa (non il Consiglio d'Europa) e i negoziatori del Parlamento europeo hanno raggiunto **un accordo provvisorio** sulla proposta di norme armonizzate sull'intelligenza artificiale (IA), la cosiddetta legge sull'intelligenza artificiale. La bozza di regolamentazione mira a garantire che i sistemi di IA, immessi sul mercato europeo e utilizzati nell'UE, siano sicuri e rispettino i principi fondamentali, i diritti e valori dell'UE. La legge sull'intelligenza artificiale è un'iniziativa legislativa, che ha il potenziale per promuovere lo sviluppo e l'adozione di un' intelligenza artificiale sicura e affidabile nel mercato unico dell'UE, da parte di attori pubblici e privati. L'idea principale è quella di regolamentare la IA in base alla capacità di quest'ultima di causare danni alla società, seguendo un approccio "basato sul rischio": maggiore è il rischio, più severe sono le regole. Come prima proposta legislativa, unica al mondo, essa può stabilire uno standard globale per la regolamentazione della IA in altri paesi, proprio come ha fatto il GDPR, promuovendo così l'approccio europeo alla regolamentazione tecnologica sulla scena mondiale.

Pubblicità
<#? QUI-PUBBLICITA-MIM-[ALDIG02] ?#>

Gli elementi principali dell'accordo provvisorio

Rispetto alla proposta iniziale della Commissione, i principali elementi di novità dell'accordo provvisorio possono essere così riassunti:

- norme sui modelli di IA di carattere generale ad alto impatto, che possono causare rischi sistemici in futuro, nonché sulla IA ad alto rischio sistemico
- un sistema di governance rivisto, con alcuni poteri esecutivi a livello UE

- ampliamento dell'elenco dei divieti, ma con la possibilità di utilizzare l'identificazione biometrica a distanza da parte delle forze dell'ordine negli spazi pubblici, soggetta a garanzie
- una migliore tutela dei diritti, attraverso l'obbligo per gli utilizzatori di sistemi di IA ad alto rischio di rispettare i diritti fondamentali e sviluppare la valutazione dell'impatto, prima di attivare un sistema IA.

Più concretamente, l'accordo provvisorio riguarda i seguenti aspetti.

Definizioni e ambito

Garantire che la definizione di un sistema di IA fornisca criteri sufficientemente chiari per distinguere la IA da software più semplici. L'accordo di compromesso allinea la definizione all'approccio proposto dall'OCSE. L'accordo provvisorio chiarisce inoltre che il regolamento non si applica a settori che esulano dall'ambito di applicazione del diritto comunitario e non dovrebbe, in ogni caso, incidere sulle competenze degli Stati membri, in materia di sicurezza nazionale. Inoltre, la legge sull'IA non si applica ai sistemi utilizzati esclusivamente per scopi militari o di difesa. Allo stesso modo, l'accordo prevede che il regolamento non si applicherà ai sistemi di IA utilizzati esclusivamente a fini di ricerca e innovazione, o alle persone che utilizzano l'IA per motivi non professionali.

Classificazione di sistemi di IA come attività ad alto rischio e vietate

L'accordo di compromesso prevede un livello orizzontale di protezione, inclusa una classificazione ad alto rischio, per garantire che i sistemi di IA, che potrebbero causare gravi violazioni dei diritti fondamentali o altri rischi significativi, sfuggano ai controlli.

Sistemi AI, che presentino solo un rischio limitato, sarebbero soggetti a obblighi di trasparenza meno impegnativi, ad esempio rivelando che il contenuto è stato generato dall'intelligenza artificiale, in modo che gli utenti possano prendere decisioni informate sull'ulteriore utilizzo. Verrebbe autorizzata un'ampia gamma di sistemi di IA ad alto rischio, ma soggetti ad una serie di requisiti e obblighi per poter accedere al mercato dell'UE. Tali requisiti sono stati chiariti, in modo tale da renderli tecnicamente fattibili e meno onerosi da rispettare per le parti interessate, ad esempio per quanto riguarda la qualità dei dati, o in relazione alla documentazione tecnica che dovrebbe essere redatta dalle PMI per dimostrare la conformità dei loro sistemi di IA ad alto rischio con i requisiti indicati dalla UE.

Poiché i sistemi di intelligenza artificiale sono sviluppati e distribuiti attraverso complesse catene del valore, l'accordo di compromesso prevede modifiche, onde chiarire la ripartizione delle responsabilità e dei ruoli dei vari attori presenti in tali catene, in particolare fornitori e utenti dei sistemi di IA. Si chiarisce inoltre il rapporto tra le responsabilità, ai sensi della legge sull'AI, e le responsabilità già esistenti in altra legislazione, come la protezione dei dati dell'UE o la legislazione settoriale. Per alcuni usi dell'IA, il rischio è ritenuto inaccettabile e, pertanto, questi sistemi saranno banditi dall'UE. L'accordo provvisorio vieta, ad esempio, la manipolazione cognitiva o comportamentale e la rimozione non mirata di immagini facciali da Internet o filmati CCTV, il riconoscimento delle emozioni sul posto di lavoro e nelle istituzioni educative, il social scoring, la categorizzazione biometrica per dedurre dati sensibili, come l'orientamento sessuale o religioso.

Eccezioni per le forze dell'ordine

Considerando le specificità delle forze di polizia e la necessità di preservare la loro capacità di utilizzare l'intelligenza artificiale nel loro lavoro vitale, sono state concordate diverse modifiche alla proposta della Commissione, relative all'uso dei sistemi di IA a fini di contrasto della criminalità; tali modifiche intendono riflettere la necessità di rispettare la riservatezza delle operazioni sensibili ed i dati relativi a tali attività. Ad esempio, è stata introdotta una procedura di emergenza che consente alle forze dell'ordine di utilizzare, in caso di urgenza, uno strumento di IA ad alto rischio, che non ha superato la procedura di valutazione

della conformità. È stato inoltre introdotto un meccanismo per garantire che i diritti fondamentali siano sufficientemente protetti da qualsiasi potenziale abuso dei sistemi di intelligenza artificiale. Inoltre, per quanto riguarda l'utilizzo di sistemi di identificazione biometrica a distanza, in tempo reale e negli spazi accessibili al pubblico, l'accordo provvisorio chiarisce i limiti in cui tale utilizzo è strettamente necessario per scopi di contrasto e con quale legge le forze di polizia dovrebbero pertanto essere eccezionalmente autorizzate a utilizzare tali sistemi. L'accordo di compromesso prevede garanzie aggiuntive e limita tali eccezioni ai casi di vittime di determinati reati, alla prevenzione di rischi reali o minacce prevedibili, come attacchi terroristici, e ricerche di persone sospettate di gravi crimini.

Sistemi di intelligenza artificiale per scopi generali e modelli di base

Sono state aggiunte nuove disposizioni per tenere conto delle situazioni, in cui i sistemi di IA possono essere utilizzati per vari e diversi scopi (IA per scopi generali) e laddove la tecnologia dell'IA per scopi generali viene successivamente integrata in un altro sistema ad alto rischio. L'accordo provvisorio affronta anche i casi specifici dei sistemi di IA per scopi generali (GPAI). Sono state concordate regole specifiche anche per i grandi sistemi, in grado di sviluppare un'ampia gamma di compiti specifici, come generare video, testi, immagini, elaborare calcoli o generare codici informatici. L'accordo provvisorio prevede che questi sistemi debbano ottemperare a specifici obblighi di trasparenza, prima di essere adottati ed immessi nel mercato. È stato introdotto un regime più severo per i sistemi "ad alto impatto". Questi sistemi operano su grandi quantità di dati e con complessità avanzata, con capacità e prestazioni ben al di sopra della media, il che può far diffondere i rischi sistemici lungo la catena del valore.

Una nuova architettura di governance

A seguito delle nuove norme sui modelli IA e dell'evidente necessità della loro applicazione a livello UE, un ufficio IA all'interno della Commissione avrà il compito di supervisionare questi modelli di IA più avanzati, contribuire a promuovere standard e pratiche di test, e applicare le regole comuni in tutti gli Stati membri. Un comitato scientifico di esperti indipendenti fornirà consulenza all'Ufficio AI, contribuendo allo sviluppo di metodologie per valutare le capacità degli applicativi, fornendo consulenza sulla individuazione di applicativi ad alto impatto e sul monitoraggio dei possibili rischi ad essi collegati. Il Comitato per l'AI, che comprenderà i rappresentanti degli Stati membri, costituirà una piattaforma di coordinamento ed un organo consultivo per la Commissione e attribuirà un ruolo importante agli Stati membri nell'attuazione del regolamento, compresa la progettazione dei codici di condotta per i sistemi più significativi. Infine, sarà istituito un forum consultivo tra le parti interessate, come rappresentanti dell'industria, PMI, le start-up, la società civile e il mondo accademico, per fornire competenze tecniche al Consiglio AI.

Sanzioni

Le sanzioni pecuniarie per le violazioni della legge sull'AI erano state fissate, nella precedente edizione, in percentuale del fatturato annuo globale dell'impresa incriminata, o un importo predeterminato, se superiore. Si tratterebbe di 35 milioni di euro o del 7% per l'uso di applicativi IA proibiti, 15 milioni di euro o il 3% per violazioni degli obblighi della legge IA e 7,5 milioni di euro o 1,5% per la fornitura di documenti errati di informazione. Tuttavia, l'accordo provvisorio prevede massimali più proporzionati alle sanzioni amministrative per le PMI e start-up, in caso di violazione delle disposizioni della legge sull'AI. L'accordo di compromesso chiarisce inoltre che una persona fisica o giuridica può presentare un reclamo alla rilevante autorità di vigilanza, in merito al mancato rispetto della legge sull'IA, e può aspettarsi che tale denuncia venga trattata in modo conforme alle apposite procedure di tale autorità.

Trasparenza e tutela dei diritti fondamentali

L'accordo provvisorio prevede una valutazione d'impatto sui diritti fondamentali, prima che venga inserito sul mercato un sistema di IA ad alto rischio. L'accordo provvisorio prevede inoltre una maggiore trasparenza riguardo all'uso di sistemi ad alto rischio. In particolare, alcune disposizioni della proposta della Commissione sono state modificate, per indicare ad alcuni utenti

la presenza di una IA ad alto rischio Anche i soggetti pubblici saranno obbligati a registrarsi nella banca dati UE per i sistemi di IA ad alto rischio. Inoltre, sono state aggiunte disposizioni, che pongono l'accento sull'obbligo, per gli utenti di un sistema di riconoscimento delle emozioni, di informare le persone fisiche esposte a tale sistema.

Misure a sostegno dell'innovazione

Al fine di creare un quadro giuridico più favorevole all'innovazione e di promuovere l'apprendimento normativo basato su dati concreti, le disposizioni relative alle misure a sostegno dell'innovazione sono state sostanzialmente modificate, rispetto a quelle proposte dalla Commissione. Inoltre, sono state aggiunte nuove disposizioni che consentono di testare i sistemi di intelligenza artificiale in condizioni reali e con garanzie specifiche. Per alleggerire gli oneri amministrativi per le imprese più piccole, l'accordo provvisorio comprende un elenco di azioni da intraprendere a sostegno di tali operatori e prevede alcune limitate e chiaramente specificate deroghe.

Entrata in vigore

L'accordo provvisorio prevede che la legge sull'AI si applichi due anni dopo la sua entrata in vigore, con alcune eccezioni e disposizioni specifiche.

Prossimi passi

A seguito dell'accordo provvisorio odierno, nelle prossime settimane proseguiranno i lavori a livello tecnico, per finalizzare i dettagli del nuovo regolamento. Quando questo lavoro sarà concluso, la presidenza sottoporrà il testo di compromesso ai rappresentanti degli Stati membri (Coreper) per l'approvazione, L'intero testo dovrà essere confermato da entrambe le istituzioni e sottoposto a revisione giuridico-linguistica, prima dell'adozione formale da parte dei colegislatori.

Adalberto Biasiotti

Licenza Creative Commons

www.puntosicuro.it