PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 26 - numero 5666 di Venerdì 19 luglio 2024

Pubblicato il regolamento europeo sugli applicativi di intelligenza artificiale

Dopo una lunga discussione e confronto fra i tre organismi che, nell'unione europea, concorrono alla approvazione di disposizioni legislative, si è trovato finalmente un accordo sul regolamento afferente agli applicativi di intelligenza artificiale.

Ricordo ai lettori che le disposizioni legislative europee si articolano in due categorie, a seconda che siano direttive, oppure regolamenti. Le direttive devono essere recepite in ogni singolo paese europeo con una specifica disposizione di legge, mentre i regolamenti vengono recepiti in forma automatica, senza bisogno di approvazione da parte dei parlamenti nazionali dei vari paesi europei.

Come parte di una strategia digitale, che coinvolge tutti i paesi europei, l'unione europea ha evoluto regolare gli applicativi di intelligenza artificiale, per consentire un uso affidabile e sicuro di questa nuova tecnologia. Che questi applicativi possano offrire molti benefici, è fatto ben noto: meno noto è il fatto che invece gli stessi applicativi possano anche creare problemi non indifferenti.

Risale all'aprile 2021 il primo passo verso una regolamentazione del settore, quando la commissione europea propose un primo documento di riferimento. L'elemento fondamentale di questo documento è legato alla elencazione dei diversi livelli di rischio, nell'applicazione di questi software, con individuazione di relative e proporzionate garanzie.

Un altro aspetto fondamentale della bozza di documento prevedeva il fatto che questi applicativi fossero sempre governati da una persona fisica, e non potessero operare in forma assolutamente automatica, proprio per prevenire possibili conseguenze negative.

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

Le nuove regole stabiliscono degli obblighi per coloro che sviluppano questi applicativi, e per i loro utenti, a seconda del livello di rischio attribuito all'applicativo di intelligenza artificiale. Questa esigenza di classificare il rischio si applica qualunque tipo di applicativo, indipendentemente dalla criticità degli aspetti esaminati.

Sono considerati i rischi non accettabili, che comportano quindi il blocco di qualsiasi applicativo di intelligenza artificiale, quelli che possono portare a interventi su questi settori:

- manipolazione del comportamento cognitivo delle persone e di gruppi etnici specifici; ad esempio giocattoli azionati dalla voce, che possono incoraggiare i bambini ad effettuare azioni pericolose;
- classificazione sociale, basata su modelli di comportamento, stato socioeconomico o caratteristiche personali;
- identificazione biometrica e categorizzazione delle persone,
- sistemi biometrici di identificazione, come ad esempio applicativi di riconoscimento facciale.

Sono previste alcune eccezioni, ma solo per finalità legate al rispetto di leggi e regolamenti ed a sostegno alle attività delle forze dell'ordine. Ad esempio, alcuni applicativi di riconoscimento biometrico potranno essere utilizzati per esaminare delle immagini videoregistrate, solo dopo l'approvazione della magistratura inquirente.

Sono considerati applicativi ad alto rischio quelli che ricadano in queste due categorie:

- sistemi che ricadono nell'ambito delle vigenti disposizioni in tema di sicurezza dei prodotti;
- sistemi che ricadono in aree specifiche, come ad esempio gestione di infrastrutture critiche, educazione, accesso ai siti di servizi pubblici e privati, tutela della legge, gestione della migrazione e attività connesse e via dicendo.

Tutti i sistemi ad alto rischio devono essere specificamente valutati prima di essere immessi sul mercato e devono essere tenuti sotto controllo durante tutto il periodo di vita.

Le esigenze di trasparenza dell'uso di questi applicativi fanno sì che sia obbligatorio mettere in evidenza come determinati test e risultati siano frutto di applicativi di intelligenza artificiale; occorre inoltre inserire nell'applicativo delle garanzie, che non vengano sviluppati contenuti illegali o tutelati da copyright.

Infine, il documento offre alle imprese di piccole e medie dimensioni l'opportunità di sviluppare modelli di intelligenza artificiale, prima della diffusione al pubblico; ecco perché il regolamento impone che le autorità nazionali mettano a disposizione di queste aziende un ambiente di prova, che simuli condizioni simili a quelle che gli applicativi incontreranno nella pratica operativa.

Il documento, approvato nel maggio 2024, entrerà in pieno vigore 24 mesi dopo, ma alcune parti potrebbero entrare in vigore a distanza più breve.

REGOLAMENTO (UE) 2024/1689 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 13 giugno 2024 che stabilisce regole armonizzate sull'intelligenza artificiale e modifica i regolamenti (CE) n, 300/2008, (UE) n, 167/2013, (UE) n, 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e le direttive 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (regolamento sull'intelligenza artificiale) (PDF)

Adalberto Biasiotti

 Licenza Creative Commons

www.puntosicuro.it