PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 26 - numero 5608 di Lunedì 29 aprile 2024

Come difendersi da usi impropri dell'intelligenza artificiale

La diffusione degli applicativi di intelligenza artificiale pone i responsabili della sicurezza davanti a problemi che devono essere affrontati e risolti rapidamente. Cosa sta facendo lo Stato italiano e cosa possono fare i security manager?

Il parlamento italiano, primo in Europa, ha già presentato un disegno di legge, riportato in allegato, che prende in esame e mette sotto controllo i possibili usi negativi, per non dire addirittura criminosi, degli applicativi di intelligenza artificiale:

DISEGNO DI LEGGE n.917 "Misure sulla trasparenza dei contenuti generati da intelligenza artificiale"

Il ministro della giustizia, Nordio, ha sottolineato come l'utilizzo di questi applicativi in attività criminose può costituire una significativa aggravante ed ecco perché questo disegno di legge è stato rapidamente presentato all'attenzione delle camere. Nel frattempo, in attesa dell'approvazione, vediamo cosa possono fare altri soggetti coinvolti nella tutela della trasparenza e correttezza delle attività, svolte nell'ambito della società civile.

È sufficiente intervistare qualche docente universitario per rendersi conto come oggi molte tesi di laurea vengano compilate non tanto dai laureandi, quanto dagli applicativi di intelligenza artificiale. Questo problema si pone anche in altri aspetti della vita in relazione, in particolare nella elaborazione di offerte tecnologiche, in risposta capitolati di gara. Ecco come è possibile tenere sotto controllo questo fenomeno.

Chi scrive già da tempo ha inserito nei capitolati, che sviluppa per conto di amministrazioni pubbliche e private, uno specifico articolo, che vieta all'offerente di inserire, nella propria offerta, testi elaborati da applicativi di intelligenza artificiale. I motivi sono numerosi e facilmente intuibili: un'offerta, elaborata in risposta ad un capitolato, deve rispondere a specifiche esigenze e deve essere in grado di soddisfare le prestazioni di servizi, o la fornitura di beni, previste nel capitolato. Il fatto di utilizzare un applicativo di intelligenza artificiale può rendere l'offerta più astratta e meno idonea a rispondere alle specifiche esigenze del committente.

Lo stesso problema si pone nella valutazione delle tesi di laurea, quando il testo non è elaborato dal laureando, ma elaborato da applicativi, che evidentemente non possono successivamente aiutare il laureando a sviluppare al meglio le sue attività professionali.

Ecco perché negli ultimi tempi sono apparsi sul mercato degli applicativi, progettati per il riconoscimento della presenza di testi, elaborati da applicativi di intelligenza artificiale, in lingua italiana.

Questi applicativi dichiarano di avere un'accuratezza di riconoscimento estremamente elevata, dell'ordine del 99,7%, anche se chi scrive ha qualche dubbio sul fatto che il modello possa raggiungere una così elevata percentuale di riconoscimento.

I motivi per cui è importante riconoscere testi sviluppati da applicativi di intelligenza artificiale sono numerosi, tra i quali si pone in particolare evidenza il fatto che spesso questi applicativi forniscono informazioni non veritiere o fuorvianti, che non vengano debitamente controllate da chi elabora il testo finale. Inoltre, è possibile che alcuni elaborati siano coperti da diritti d'autore e pertanto non possano essere inseriti in altri documenti, se non dopo aver messo chiaramente in evidenza l'origine del testo stesso.

È possibile che in ulteriori versioni di bozze di capitolati di gara sia possibile inserire non solo un articolo afferente alla proibizione di utilizzo di testi elaborati da applicativi di intelligenza artificiale, ma anche di mettere in guardia l'offerente, circa il fatto che l'ente appaltante potrebbe utilizzare questi applicativi di controllo per verificare la presenza di elaborati di intelligenza artificiale, non dichiarati come tali dall'offerente.

Una situazione del genere potrebbe portare alla immediata esclusione dell'offerta dalla gamma delle offerte, che verranno successivamente sottoposte all'attenzione della commissione di gara.

Ancora una volta, questi applicativi di intelligenza artificiale possono essere molto utili in alcune circostanze, ma debbono essere utilizzati con estrema prudenza e con costante verifica della qualità delle informazioni fornite.

DISEGNO DI LEGGE n.917 "Misure sulla trasparenza dei contenuti generati da intelligenza artificiale" (pdf)

Adalberto Biasiotti