IL FOGLIO
quotidiano

La sfida di ChatGPT per adempiere alle richieste del Garante

ilfoglio.it - 01/04/2023

Lucio Scudiero

Tra i punti contestati ad OpenAI c'è la verifica adeguata dell'età degli utenti. Un'operazione che per paradosso richiede più intelligenza artificiale e complica ancora di più la gestione dei dati personali raccolti. Ora la società americana ha fino a metà aprile per comunicare la sua risposta all'autorità Nessuno avrebbe immaginato questa corrispondenza ideale tra Elon Musk e Pasquale Stanzione, presidente del Garante per la protezione dei dati personali italiano. Eppure con la decisione di bandire chatGPT dal territorio italiano il vertice dell'autorità privacy italiana ha di fatto recepito la richiesta di moratoria sull'Intelligenza Artificiale generativa formulata dal proprietario di Tesla e altri in una lettera aperta di pochi giorni fa. Con buona pace di Musk, l'incontro-scontro tra ChatGPT e le leggi europee sui dati era comunque solo questione di tempo, e lo si era capito dalla veemenza con cui ChatGPT, fin dalla data del suo rilascio pubblico lo scorso anno, aveva impattato la discussione in corso sulla proposta di regolamento europeo sull'intelligenza artificiale: i chatbot, che nella iniziale tassonomia del rischio della Commissione Europea erano stati ritenuti a basso rischio, con la pubblicazione di ChatGPT sono diventati terreno di divisione politica nel Parlamento Europeo e nel Consiglio, tra chi ne teme le capacità manipolative e li vorrebbe assimilati ai sistemi ad alto rischio e chi invece ha un approccio meno allarmato e ne ammetterebbe una regolazione più leggera. Con il provvedimento di limitazione a ChatGPT, il Garante Privacy ha ricordato al pubblico che una regolazione dell'intelligenza artificiale c'è già, ed è nella disciplina europea a protezione dei dati personali. La decisione è prima nel suo genere ed è piuttosto dirompente, perché di fatto dispone che l'interfaccia ChatGPT non dovrà più essere accessibile dall'Italia. Inoltre, è stata presa seguendo una particolare procedura d'urgenza: il Garante Privacy ha infatti adottato un provvedimento eccezionale direttamente tramite il suo presidente; la misura andrà convalidata dall'intero collegio - composto da 4 membri - entro un mese, altrimenti decadrà. Nel merito, l'autorità contesta a OpenAI, la società statunitense proprietaria di ChatGPT, di non informare gli utenti sul trattamento dei loro dati personali utilizzati per allenare l'algoritmo, di non disporre di una valida base giuridica (ad esempio un consenso esplicito preventivo) e di non verificare in maniera adeguata l'età degli utenti, con il rischio che il servizio possa essere utilizzato anche dai minori di tredici anni, che è l'età limite al di sotto della quale la stessa OpenAI dichiara di non voler fornire il servizio. Applicando le norme italiane, quell'età dovrebbe essere almeno fissata a quattordici anni, ma poco importa, perché il vero problema sul punto rimane che ad oggi nessuno ha trovato il modo di verificare in modo soddisfacente l'età dei minori online. Lo sa bene Tik Tok, il social più popolare tra i giovani, sempre più al centro della disputa geopolitica tra il mondo occidentale e la Cina, che a inizio 2021 aveva subito un analogo provvedimento di blocco da parte dell'autorità italiana, rimosso solo a seguito dell'impegno della società di rinforzare il proprio sistema di age verification. Il paradosso è che per rafforzare i controlli sull'età degli utenti serve proprio l'intelligenza artificiale, come scrive lo stesso Garante Privacy nel comunicato stampa di rimozione del blocco a TikTok del 3 febbraio 2021: "Per identificare con ragionevole certezza gli utenti sotto i 13 anni, successivamente a questa prima verifica, la società si è impegnata a valutare ulteriormente l'uso di sistemi di intelligenza artificiale". La sfida, che adesso è anche di ChatGPT, sarà quella di utilizzare l'IA per distinguere chi è al di sotto della "maggiore età" digitale, attraverso un

IL FOGLIO
quotidiano

monitoraggio dei comportamenti degli utenti, la loro rielaborazione sotto forma di un modello informatico di riferimento e la successiva attività di verifica automatizzata dei comportamenti o degli attributi degli utenti rispetto a tale modello. E' un attività delicatissima di bilanciamento tra diritti e di design legale della soluzione tecnica, perché se da un lato va assicurato che i minori non utilizzino i servizi per i quali non hanno ancora la capacità legale di agire, dall'altro va evitata l'accumulazione eccessiva di dati personali e ridotto il rischio di decisioni automatizzate sbagliate da parte dell'intelligenza artificiale. OpenAI ha fino a metà aprile per comunicare all'autorità italiana i rimedi che intende approntare, e con ogni probabilità ciò non le risparmierà una sanzione amministrativa pecuniaria. Da ultimo, un dato tecnico. La società americana non ha stabilimenti sul territorio dell'Unione Europea, ma solo un rappresentante designato e questo, per ipotesi, apre alla possibilità per le autorità privacy dei 27 stati membri di seguire l'esempio del Garante Privacy italiano, senza neppure doversi coordinare tra loro attraverso il meccanismo di coerenza previsto dal GDPR. C'è da augurarsi che non accada, perché il tema è transnazionale e sarebbe meglio che le risposte ai problemi comuni fossero comuni.

Nessuno avrebbe immaginato questa corrispondenza ideale tra Elon Musk e Pasquale Stanzione, presidente del Garante per la protezione dei dati personali italiano. Eppure con la decisione di bandire chatGPT dal territorio italiano il vertice dell'autorità privacy italiana ha di fatto recepito la richiesta di moratoria sull'Intelligenza Artificiale generativa formulata dal proprietario di Tesla e altri in una lettera aperta di pochi giorni fa. Con buona pace di Musk, l'incontro-scontro tra ChatGPT e le leggi europee sui dati era comunque solo questione di tempo, e lo si era capito dalla veemenza con cui ChatGPT, fin dalla data del suo rilascio pubblico lo scorso anno, aveva impattato la discussione in corso sulla proposta di regolamento europeo sull'intelligenza artificiale: i chatbot, che nella iniziale tassonomia del rischio della Commissione Europea erano stati ritenuti a basso rischio, con la pubblicazione di ChatGPT sono diventati terreno di divisione politica nel Parlamento Europeo e nel Consiglio, tra chi ne teme le capacità manipolative e li vorrebbe assimilati ai sistemi ad alto rischio e chi invece ha un approccio meno allarmato e ne ammetterebbe una regolazione più leggera.

https://www.ilfoglio.it/tecnologia/2023/04/01/news/la-sfida-di-chatgpt-per-adempiere-alle-richieste-del-garante-5128065/