

intelligenza artificiale

L'allarme del Garante: DeepSeek può violare la privacy

ATTUALITÀ

31_01_2025



**Ruben
Razzante**



Il Garante per la protezione dei dati personali ha recentemente lanciato un allarme riguardante l'applicazione DeepSeek, un servizio di chatbot basato su intelligenza artificiale (IA), accessibile tramite piattaforma web e applicazione mobile. Il rischio

riguarda la gestione dei dati personali degli utenti italiani, i quali potrebbero essere trasferiti a server ubicati in Cina, un Paese che non è sotto la giurisdizione dell'Unione Europea in materia di protezione dei dati. A tale riguardo, il Garante ha richiesto alle società cinesi che forniscono DeepSeek, ovvero Hangzhou DeepSeek Artificial Intelligence e Beijing DeepSeek Artificial Intelligence, di fornire dettagli sul tipo di dati personali raccolti, sulla loro fonte, sulle finalità del trattamento, sulla base giuridica del trattamento e sulla conservazione dei dati stessi.

L'allarme sollevato dal Garante italiano si inserisce in un contesto di crescente preoccupazione per la protezione dei dati sensibili degli utenti, soprattutto considerando che i sistemi di IA, come quelli che alimentano il chatbot di DeepSeek, possono raccogliere una grande quantità di informazioni, inclusi dati personali. Inoltre, sono stati richiesti chiarimenti su come i dati vengono utilizzati per addestrare l'intelligenza artificiale e, in caso di web scraping, su come gli utenti siano informati circa l'utilizzo dei loro dati. La risposta delle aziende deve arrivare entro 20 giorni, al fine di permettere un approfondimento da parte dell'Autorità.

L'incidente è emblematico di una più ampia questione che riguarda la governance e la protezione dei dati nell'ambito dell'intelligenza artificiale. Il Garante della Privacy italiano non è il solo a esprimere preoccupazioni; anche il Garante irlandese ha sollevato questioni simili, facendo emergere una problematica comune all'interno dell'Unione Europea: la protezione dei dati in un contesto globale sempre più interconnesso, dove le piattaforme basate su IA operano a livello transnazionale.

Il caso di DeepSeek pone in evidenza una delle difficoltà principali nell'affrontare la gestione dei dati personali in un'era digitale globalizzata: quando i dati degli utenti finiscono su server in paesi con normative meno restrittive sulla privacy, come la Cina, si rischia di compromettere la tutela dei diritti fondamentali. In questo contesto, l'UE, pur avendo stabilito delle normative stringenti come il Regolamento Generale sulla Protezione dei Dati (GDPR), si trova a dover fare i conti con le differenze normative tra i paesi membri e le realtà extraeuropee.

A livello legislativo, le norme europee che riguardano la protezione dei dati e l'intelligenza artificiale sono state recentemente integrate dall'AI Act, una regolamentazione che stabilisce le linee guida per la gestione dei sistemi di IA in Europa. Tuttavia, la questione rimane complessa: se da un lato l'AI Act impone che i sistemi IA ad alto rischio siano regolamentati e monitorati in modo rigoroso, dall'altro la competenza specifica sulla vigilanza di questi sistemi rimane oggetto di dibattito. Il Garante italiano per la protezione dei dati ha fatto valere la sua posizione, sottolineando

l'interconnessione tra IA e protezione dei dati, in quanto le tecnologie basate su intelligenza artificiale utilizzano, per loro natura, dati personali. Il Garante ha anche suggerito che, alla luce dell'impatto che queste tecnologie hanno sui diritti individuali, sia necessario un organismo indipendente con competenze specifiche per garantire la tutela dei diritti fondamentali in questo nuovo scenario tecnologico.

Il dibattito, però, non riguarda solo il livello nazionale. La sfida globale tra le intelligenze artificiali sviluppate da potenze come la Cina e gli Stati Uniti sta mettendo sotto pressione l'Europa, che, con il suo approccio regolatorio severo, rischia di rimanere schiacciata tra due superpotenze. La regolamentazione stringente dell'UE sulla protezione dei dati personali e sulla governance dell'intelligenza artificiale potrebbe frenare l'innovazione, mentre la Cina e gli Stati Uniti proseguono nello sviluppo di sistemi sempre più potenti e senza le stesse limitazioni. In questo scenario, l'Europa deve decidere se continuare a imporre un controllo rigoroso o cercare un compromesso per favorire la competitività tecnologica.

Un altro aspetto cruciale riguarda la gestione dei dati da parte delle grandi piattaforme tecnologiche e dei loro algoritmi. Il GDPR, insieme all'AI Act, rappresenta un tentativo di mettere ordine in questo campo, ma nonostante gli sforzi normativi, permangono incertezze riguardo l'applicabilità delle regole in un mondo in cui i dati viaggiano liberamente tra continenti e giurisdizioni diverse. La scomparsa dell'app di DeepSeek dall'App Store, che ha attirato l'attenzione degli utenti, potrebbe essere interpretata come una mossa di cautela da parte dei produttori. Sebbene non sia chiaro se si tratti di una decisione definitiva o di una sospensione temporanea, la scelta sembra una risposta indiretta alle preoccupazioni sollevate dalle autorità di regolamentazione, ma potrebbe anche indicare il rischio di azioni legali da parte delle autorità competenti.

Il caso di DeepSeek solleva quindi interrogativi importanti sulla governance dei dati, sul ruolo delle autorità nazionali nella supervisione dell'intelligenza artificiale e sull'efficacia delle normative in un mondo sempre più interconnesso e globale. L'Europa, pur dotata di uno dei quadri normativi più avanzati, rischia di trovarsi in una posizione di svantaggio in un contesto internazionale caratterizzato da regolamenti meno stringenti e da un mercato altamente competitivo. La protezione dei dati e dei diritti fondamentali continua a essere una priorità, ma l'equilibrio tra innovazione tecnologica e tutela della privacy diventa sempre più una questione delicata e complessa.

Oggi alle 14 l'incontro dei "Venerdì della Bussola" sarà dedicato al tema (Poca) intelligenza (molto) artificiale, con Tommaso Scandroglio - segui la diretta

sul nostro sito e sul nostro canale YouTube: