Intelligenza artificiale: la privacy non esiste più (e non ce ne siamo accorti)

Data 22 ottobre 2023
Categoria Medicinadigitale

In diverse occasioni su questa piattaforma abbiamo evidenziato i possibili problemi riferibili alla privacy nei confronti dei modelli linguistici di grandi dimensioni (LLM) della intelligenza artificiale

L'enorme diffusione di piattaforme come chatGPT, Bard, Bing, Claude, Perplexity ed altre ancora, in grado di "conversare" e instaurare una conoscenza estesa su informazioni personali sensibili quali pensieri, interessi, domande, timori, ha enfatizzato la centralità della protezione dei dati personali e il suo fortissimo legame con lo sviluppo e l'affermazione delle nuove tecnologie (1).
I dati, proiezione digitale delle nostre persone, sono input fondamentali per produrre avanzamenti in ambito medico e per migliorare le politiche sanitarie. Il concetto di dato personale e anonimo è peraltro ormai sparito in una sorta di far web di schedature e profilazioni ossessive, fuori controllo, nelle quali la violazione della privacy sembra sistematica.
Essere controllati è diventato qualcosa di normale e naturale, il potere associato alla digitalizzazione controlla lasciando le persone fare esattamente ciò che vogliono, mantenendo un'illusione di libertà. Noi stessi infatti postiamo sui principali social network immagini di ospedale, referti diagnostici, informazioni sull'andamento delle malattie, vissuti di lutto, momenti cruciali della propria e della altrui esistenza. Inoltre, in virtù della sempre maggiore diffusione del cosiddetto "internet delle cose", per cui oggetti, dispositivi, sistemi diventano "smart", cioè dotati di software che consentono loro di identificarsi elettronicamente, connettersi e comunicare direttamente tra loro, internet è sempre più trasformata da rete di comunicazione tra persone a rete di controllo, incorporata nel mondo fisico.
Un recente studio della Università della Carolina del Nord evidenzia le complessità riferibili alla sottrazione dei dati sensibili dai LLM (2). La struttura stessa dei modelli rende la protezione dei dati sensibili estremamente complessa. I ricercatori hanno proposto nuovi metodi di difesa ma non hanno trovato un sistema universalmente efficace.Nonostante l'utilizzo di metodi avanzati come il ROME (Rank-One Model Editing, un metodo per aggiornare una rete neurale senza nuovi addestramenti), le informazioni "eliminate" possono essere recuperate nel 38% dei casi, utilizzando tecniche che sfruttano le tracce di informazioni rimosse negli strati intermedi delle reti neurali. Ciò è importante perché, come affermato dagli stessi ricercatori, anche tassi di successo dell'attacco relativamente bassi possono avere implicazioni gravi in un contesto come quello sanitario.

Conclusioni
La difesa del diritto al controllo dei propri dati dovrebbe essere la tutela della libertà dell'individuo e di una società che, consapevole di sé stessa e delle proprie capacità, dovrebbe poter dissentire rispetto al potere tecnologico, o almeno evitare di essere sempre più identificata secondo le forme e le regole del sistema. La soluzione peraltro non sta nella semplice riappropriazione dei propri dati mediante norme rigide. Secondo S. Zuboff, sociologa della Harvard Business School, queste non toccano il punto nodale della questione. Anzi, la spinta ad introdurre regolamenti sempre più inflessibili, paradossalmente, «non fa che istituzionalizzare e legittimare ancora di più la raccolta dei dati. È come negoziare il numero massimo di ore lavorative quotidiane di un bambino di sette anni, piuttosto che contestare la legittimità del lavoro minorile»(3).
La protezione della riservatezza, anche in ambito sanitario, richiede la concezione di nuovi costrutti, maggiormente allineati agli attuali contesti ontologici prodotti dalle sempre più affascinanti/inquietanti intelligenze computazionali, peraltro indispensabili, a causa delle loro immense potenzialità, per fornire risposte in ambiti ad elevata complessità e incertezza, come quelli della salute/malattia (4,5).
La risposta deve essere culturale, mediante il recupero e la promozione dei diritti delle persone, compreso quello di rinunciare, consapevolmente, alla fruizione del diritto alla privacy, per chi voglia partecipare al flusso dell'attualità tecnologica ed essere costantemente on line anziché on life.

Giampaolo Collecchia, Riccardo De Gobbi, Roberto Fassina

Riferimentibibiografici

1) http://www.pillole.org/public/aspnuke/news.asp?id=8197
2) Patil V et al. Can Sensitive Information Be Deleted From LLMs? Objectives For Defending Against Extraction Attacks. arXiv:2309.17410v1 29 Sep 2023
3) Zuboff S., Il capitalismo della sorveglianza, Roma, LUISS, 2019.
4) Collecchia G., Intelligenza umana e artificiale: culture a confronto/scontro, IsF 2018; 4: 28-31.
5) Dall'habeas corpus all'habeas data. In: Collecchia G., De Gobbi R., Intelligenza artificiale e medicina digitale, Roma, Il Pensiero Scientifico Editore, 2019.

© 2004 - 2026 Pillole - Registrazione T. di Roma n. 2/06 | stampato il 13/11/2026 alle ore 1:27 | Pagina 1 di 1