Il Sole 24 ORE

CONTAMINAZIONI

QUELLO CHE SANNO I CHATBOT DI NOI

di **Luca Tremolada**

Noi di lui (o lei) sappiamo ancora troppo poco. Per esempio non sappiamo chi lo ha allevato, che libri ha letto, chi lo corregge e come. E non sappiamo soprattutto quanto consuma. Lui (o lei) invece di noi potrebbe sapere moltissimo. I chatbot possono imparare molto, forse troppo, da noi, dalle nostre domande. Robin Staab, Mark Vero, Mislav Balunovic e Martin Vechev del dipartimento di Computer Science del Politecnico di Zurigo Eth hanno dimostrato in uno studio (in pre-print) che i modelli linguistici di grandi dimensioni (Llm) che alimentano i chatbot più popolari possono dedurre una quantità sorprendente di informazioni personali sugli utenti. Come ad esempio, etnia, posizione, occupazione e altro ancora, studiando le domande che gli poniamo.

Come hanno raccontato i ricercatori di Zurigo a Wired questa capacità di deduzione potrebbe essere utilizzata per carpire dai commenti sui social informazioni sensibili come ad esempio lo stato di salute e quindi le malattie di una persona. Per fortuna almeno in Europa esiste una normativa

sulla privacy che disciplina il trattamento dei dati personali dentro a questi software. Quello che questi sistemi sanno di noi resta tra loro. Almeno fino a quando lo vogliamo. In alcuni chatbot, come si legge nella informativa sulla privacy di ChatGpt, possiamo decidere di cancellare i nostri dati. Ma non è detto che sarà così per tutti. Ancora più complicato il caso in cui non ci sia neppure un consenso da fornire. Come nel caso della lettura del pensiero. Non è fantascienza. Meta sarebbe al lavoro su un sistema di Ai in grado di decodificare quasi istantaneamente le rappresentazioni visive create nel cervello.

È uno studio e va preso come tale. Ma immaginiamo cosa accadrebbe se questi strumenti fossero utilizzati come tecniche investigative, interrogatori (civili o militari) o colloqui, testimonianze. Il limite non sarebbe più tecnologico ma di ordine etico e giuridico. «Pensare di trovare una soluzione legislativa capace di regolare questo fenomeno una volta per tutte può essere complesso, se non impossibile» scrive Ugo Ettore Di Stefano, responsabile del dipartimento Privacy & Corporate Compliance di Lexellent. Costruire un baluardo giuridico che consenta di regolare il fenomeno è però complesso per molti fattori. Il sistema normativo sembra non riuscire più a stare al passo con l'innovazione: le leggi che nasceranno dall'Unione Europea saranno già vecchie; la distanza di regolamenti e norme tra ciò che è internazionale, europeo, ma anche locale; infine, vi è un tema di conformità e bilanciamenti con i principi costituzionali. Una strada efficace, sottolinea Di Stefano, «può essere quella di istituire organismi internazionali di confronto, dotati di autorevolezza in campo etico, giuridico e informatico, che diventino abituali interlocutori dei legislatori».

Valletta
RELAZIONI PUBBLICHE

Rassegna Stampa

LEXELLENT
Your partner in law.