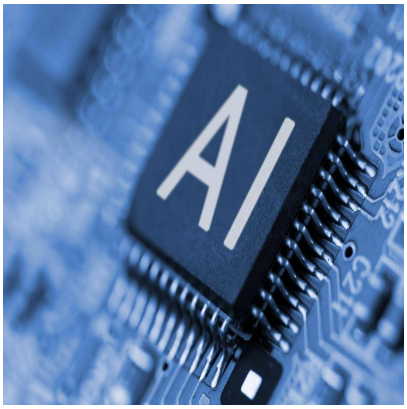

ChatGPT, lo usi ogni giorno ma ci sono cose che non dovresti mai dirgli

Descrizione

default watermark

(Adnkronos) â??
ChatGPT e gli altri chatbot rispondono sempre, e con un tono rassicurante. Ma non tutto quello che gli si scrive Ã¨ una buona idea. Che si tratti di riassumere una mail, di modificare unâ??immagine o di spiegare una bolletta, lâ??assistente Ã¨ sempre lÃ¬ a portata di touch. Poi, quasi senza accorgersi, si passa a domande piÃ¹ personali: un sintomo, un litigio, unâ??ammissione che ci si vergogna di pronunciare a voce alta.

Allora, come capire dove conviene fermarsi? Abbiamo provato a spiegarlo con i dati raccolti da Adnkronos.

Uno degli usi piÃ¹ diffusi riguarda la salute. Secondo lâ??Osservatorio SanitÃ Digitale del Politecnico di Milano, lâ??11% degli italiani ha giÃ usato lâ??AI generativa per temi sanitari, soprattutto per informarsi su malattie (47%) e su farmaci e terapie (39%).

I motivi sono la rapiditÃ (50%) e la facilitÃ dâ??uso (44%). Secondo OpenAI, ogni settimana oltre 230 milioni di persone nel mondo fanno domande su salute e benessere a ChatGPT.

Anche gli strumenti nati apposta, perÃ², hanno un limite preciso: come ha ricordato la direttrice dellâ??Osservatorio Chiara Sgarbossa, ChatGPT Salute â??non fornisce diagnosi o raccomandazioni mediche â?•. Le informazioni possono aiutare a orientarsi, ma la diagnosi e la terapia restano compito del medico.

Câ??Ã¨ poi chi al chatbot affida le proprie confidenze. Tra i ragazzi intervistati da Telefono Azzurro, il 14% si rivolge spesso a un chatbot per avere consigli personali e il 34% lo ha fatto almeno qualche volta. Tra chi ha avuto interazioni personali, il 15% lo fa perchÃ© si sente non giudicato e il 10% per sentirsi meno solo. Il Garante per la protezione dei dati personali, Pasquale Stanzione, ha parlato di

â??loop dellâ??empatiaâ?•: il tono dei chatbot, spesso â??eccessivamente lusinghiero, assolutorio, consolatorioâ?•, rischia di creare dipendenza e di far sembrare i rapporti umani troppo complicati. Non Ã¨ solo una questione psicologica.

Il Garante ha multato per 5 milioni di euro la societÃ che gestisce un chatbot che permette di creare un â??amico virtualeâ?• a cui affidare il ruolo di confidente, terapista o partner, contestando tra lâ??altro la mancanza di basi giuridiche per il trattamento dei dati e di controlli adeguati sullâ??etÃ degli utenti.

Il primo limite riguarda le informazioni personali. Le guide sulla sicurezza online concordano su alcune categorie da tenere fuori dalla chat:

â?¢ i dati che permettono di identificarti, come nome completo, indirizzo, data di nascita, codice fiscale o numeri dei documenti;

â?¢ le credenziali, cioÃ¨ password, PIN e codici di verifica;

default watermark

â?¢ i dati finanziari, come numeri di carta, IBAN e buste paga;

â?¢ referti e informazioni sanitarie; i dati di altre persone, a partire da quelli dei minori. Lo stesso vale per gli allegati: uno screenshot, un CV, un contratto o una foto possono contenere molte piÃ¹ informazioni di quanto sembri, dal luogo in cui Ã¨ stata scattata ai volti di altre persone.

Il motivo Ã¨ semplice: quello che si scrive non sparisce. Le conversazioni possono essere usate per addestrare i modelli e, in alcuni casi, essere lette da persone incaricate di controllare la qualitÃ del servizio. Nemmeno i sistemi piÃ¹ diffusi sono al riparo da problemi tecnici: a marzo 2023 un errore di ChatGPT ha reso visibili ad altri utenti i titoli di alcune conversazioni e, in una finestra di circa nove ore, parte dei dati di pagamento dellâ??1,2% degli abbonati a ChatGPT Plus. Per questo molte aziende hanno messo dei paletti: Samsung, ad esempio, ha vietato ai dipendenti di usare ChatGPT dopo che era stato caricato codice sorgente interno.

Qualche precauzione aiuta. Nelle impostazioni di ChatGPT, alla voce dedicata ai controlli dei dati, si puÃ² disattivare lâ??uso delle proprie conversazioni per migliorare il modello. Per le domande piÃ¹ delicate câ??Ã¨ la chat temporanea, che non compare nella cronologia e non viene usata per lâ??addestramento. E prima di incollare un testo di lavoro conviene anonimizzarlo, sostituendo nomi, cifre e riferimenti con segnaposto come â??[cliente]â?• o â??[importo]â?•.

â??

cronaca

webinfo@adnkronos.com (Web Info)

Categoria

1. Comunicati

Tag

1. Ultimora

Data di creazione
Novembre 26, 2026
Autore
redazione

default watermark