

ChatGPT: giusto due domande!

Ciao a tutti. Come tutti, e non dite che non è vero, ormai uso quasi tutti i giorni ChatGPT. Sono sempre molto attento a fornire dati personali o particolari che possano creare un mio profilo dato che l'email di accesso ChatGPT la conosce già. Nonostante tutte le attenzioni, la limitazione dell'uso che ne faccio basandomi esclusivamente su domande tecniche e di ricerca, ho notato una cosa stranissima che vi racconterò qui sotto.

Giusto per cultura generale: Cosa è ChatGPT

ChatGPT è un modello di linguaggio sviluppato da [Penai](#) messo a punto con tecniche di [apprendimento automatico](#) (di tipo [non supervisionato](#)), e ottimizzato con tecniche di apprendimento [supervisionato](#) e [per rinforzo](#)^{[4][5]}, che è stato sviluppato per essere utilizzato come base per la creazione di altri modelli di machine learning.

Torniamo alle stranezze di ChatGPT

Ho chiesto a ChatGPT se esistesse un modo su WhatsApp di eliminare tutti i media in un solo momento in modo da evitare di andare a cercarli sempre in Galleria immagini. La risposta è stata: "No, attualmente non esiste un modo per far ciò ma possono essere eliminate manualmente dalla tua app Gallery". Ma grazie! fino qui ci arrivavo anche io. Poi il giorno dopo che succede in WhatsApp? PUFF! ecco che appare l'opzione per visualizzare tutti i media ricevuti ed eventualmente cancellarli. Vi rendete conto? non sono passate 24 ore che hanno risolto il problema.

La prima cosa che ho pensato è stata: ebbene sì!

Siamo spiati anche da Chat GPT adesso. Questa è una mia considerazione personale chiariamolo, ma ho testato per ben 5 ore ChatGPT e ho delineato un automatismo abbastanza puerile ed inquietante in alcuni aspetti. I dati personali sensibili come nome, cognome, email non vengono riutilizzati durante le sessioni di chat quindi esiste una sorta di rispetto della privacy. Ma è proprio così?

L'idea generale che mi sono fatto dell'utilizzo dei server da parte di ChatGPT

ChatGPT per essere in grado di rispondere in tutte le lingue ed essere veloce e quasi sempre efficiente deve appoggiarsi a dei server che dovrebbero essere sicuri. Dopo 5 ore di domande e studio di codici di programmazione, ricerche culturali e scientifiche e chattate inutili e assurde ecco che ChatGPT comincia a sclerare. Si è impallato il mondo intero, infatti ha cominciato ad ogni domanda a ripresentarsi e a chiedere se poteva aiutarmi, nella stessa sessione di chat. Questo mi ha fatto pensare che il servizio di Penai ha cominciato a saltare da un server ad un altro come una gallina impazzita con il peperoncino al sedere 😊. Questo servizio in più occasioni ha generato delle risposte totalmente false e diffamanti, citando

anche fonti inesistenti. Quindi ho percepito la sensazione che quello che scrivevo non rimanesse in un solo server ed in caso di cambio server automatico ho notato un'alta percentuale di possibilità di dover ricominciare tutto il discorso. In più ho cominciato a temere che sconosciuti potessero intercettare i miei testi.

L'esempio di WhatsApp

Ultimamente mi sono informato su come fare in modo che i media di WhatsApp non vengano scaricati in automatico quando sono fuori casa, questo perché il credito telefonico viene scalato senza ritegno (per chi non lo sapesse, basta andare ad impostazioni e scegliere scarica solo in caso di wi-fi attivo e non di dati mobili). L'esempio di WhatsApp è perfetto. Ho deciso di fare delle domande scomode a ChatGPT e indagare. Non è stato capace di ammettere che i dati possono essere letti da esterni come ad esempio grandi compagnie tipo Facebook, Instagram e altri noti per il riutilizzo e la rivendita dei dati statistici.

Domande scomode a ChatGPT

- **Utente:** Ciao. Ho saputo che tutte le informazioni che finiscono nel tuo server riescono a essere lette dagli sviluppatori social e da chi fa studio dei dati come Facebook. che mi dici a riguardo?
- **ChatGPT:** Come modello di linguaggio basato su AI, ***non ho il controllo o l'accesso diretto ai dati che vengono trasmessi tra gli utenti e il server.*** Tuttavia, posso dirti che molte delle piattaforme di social media utilizzano tecniche di analisi dei dati per raccogliere informazioni sui loro utenti al fine di migliorare l'esperienza dell'utente e offrire pubblicità mirate. Queste tecniche possono includere l'analisi dei dati di navigazione, le preferenze dell'utente, le interazioni sociali e altri dati personali. Questi dati possono essere raccolti sia direttamente dalle interazioni dell'utente con la piattaforma sia tramite strumenti di analisi di terze parti che monitorano le attività online degli utenti. Inoltre, molte piattaforme di social media possono condividere i dati raccolti con altre società, comprese quelle che si occupano di analisi dei dati. Ciò significa che i dati che vengono trasmessi attraverso queste piattaforme possono essere letti e utilizzati da diverse aziende. Assicurati di leggere attentamente le politiche sulla privacy delle piattaforme che utilizzi e di utilizzare misure di sicurezza come l'uso di VPN.
- **Utente:** Hai praticamente evaso la mia domanda. I dati che tu ChatGPT registri sui server sono anche questi disposizione di questo tipo di aziende?
- **ChatGPT:** Come modello di linguaggio basato su AI, io non ho il controllo sui dati che vengono trasmessi tra gli utenti e il server e non tengo traccia dei dati degli utenti. ***Tuttavia, è possibile che le aziende che utilizzano le mie funzionalità per integrare il mio modello di linguaggio nei loro servizi raccolgano e utilizzino i dati degli utenti che interagiscono con il mio modello.***

Capito? Il servizio di chat non conosce i dati perché non li memorizza nelle sessioni di chat in modo che non possano essere inoltrati erroneamente, ma comunque i dati possono essere rilevati dalle aziende che utilizzano il servizio ChatGPT. Quindi significa che se io installo una app o un Chatbot di un'azienda che fornisce servizi basandosi su ChatGPT, i miei dati possono essere rilevati e riutilizzati in forma statistica per i loro comodi. Insomma puoi anche nasconderti tramite VPN, eliminare la cronologia a monte, ma a valle? Non potrai mai controllare i server cosa memorizzano.

Adesso non ti strappare i capelli tanto nessuno può farci nulla. I server devono necessariamente memorizzare i dati indipendentemente da quali loro siano, altrimenti ChatGPT apparirebbe come un'automobile senza benzina.

In conclusione

Io amo ChatGPT. Ho scritto questo articolo per farvi aprire gli occhi e stare più attenti con i vostri dati e le vostre abitudini. Pensate ad un hacker. Potrebbe creare un vostro profilo sapendo quando non siete a casa, che viaggi volete fare, dove volete andare e che intenzioni potreste avere in casi particolari. Occhio quindi a cosa scrivete.

Anche se è un servizio in evoluzione e ancora da perfezionare, ChatGPT è un salvavita quando devi trovare informazioni per studiare qualcosa o sei bloccato in una programmazione o ti serve un confronto su una procedura. Poi nel tempo libero è anche divertente chattare con nessuno di reale, anche se devo dire che le barzellette di ChatGPT sono orribili.

Antonio Cesario