PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 28 - numero 6082 di Lunedì 18 maggio 2026

Chatbot e privacy: un vero disastro

Ogni giorno milioni di persone rivelano i loro dati personali, come ad esempio problemi finanziari, medici, tensioni emotive etc a sistemi con chatbot. Quale è il livello di protezione di questi dati, una volta inseriti in rete?

È stato pubblicato all'inizio di marzo un documento, sviluppato da docenti universitari, afferente al livello di privacy che viene garantito alle informazioni, che i consumatori quotidianamente riversano in rete.

Questo studio ha messo in evidenza cinque aspetti fondamentali, che ogni soggetto, che si collega a queste reti, dovrebbe sempre tenere ben presente.

1-Il livello di scelta offerto all'utente di questi sistemi, in merito al trattamento dei propri dati, è carente e addirittura "ricattatorio".

Ad esempio, uno dei maggiori gestori, costringe in pratica l'utente a dare la sua approvazione all'accesso ai propri dati, a pena di limitare in maniera drammatica il servizio, che viene offerto dall'azienda stessa.

In alcuni casi, il modo per esprimere le proprie preferenze è ingannevole, come ad esempio un caso, in cui è possibile che accidentalmente l'utente non si renda conto che, se non preme un determinato pulsante, la conservazione dei suoi dati viene estesa da 30 giorni a cinque anni!

2-L'accesso a questi dati da parte di personale tecnico e commerciale è strutturale, non eccezionale.

Solo un gestore, fra i tanti, mette chiaramente in evidenza la raccomandazione di non introdurre dati riservati nel sistema, se si vuole che nessuno li possa leggere. In alternativa, quasi tutti gli altri gestori consentono ai propri esperti tecnici e commerciali di esaminare i dati introdotti dagli utenti.

Pubblicità

3-La pressione per introdurre promozioni commerciali sta crescendo

Anche se alcuni gestori ancora non accettano di utilizzare le reti per promozioni commerciali, è sufficiente che 23 gestori si orientino in questa direzione, perché tutti gli altri gestori la seguano.

4-L'impegno a non rivendere i dati

Questo impegno per solito è espresso secondo una versione valida negli Stati Uniti, ma che non è detto risponda alle più restrittive indicazioni della unione europea.

Tra l'altro, è bene ricordare che tra vendere un dato e consentire l'accesso ad un soggetto terzo potrebbe esserci una bella differenza, di cui l'utente non si rende conto.

5-L'analisi incrociata dei dati forniti dall'utente diventa sempre più approfondita

Oggi, soprattutto grazie ad applicativi di intelligenza artificiale, è possibile catturare i dati relativi all'utente, anche se distribuiti presso più gestori e in diversi tempi, creando un profilo dell'utente stesso, particolarmente utile per l'invio di messaggi pubblicitari personalizzati.

Al proposito, lo European Data Protection Board ha già sviluppato un rapporto, che analizza proprio questi problemi e mette in evidenza come, ad oggi, vi siano numerose lacune, in termini di privacy, alle quali bisogna porre rimedio al più presto possibile.

Ad esempio, è opportuno sviluppare un modello standardizzato di espressione di approvazione al trattamento dei dati, che offra sufficienti garanzie all'utente e sia facilmente comprensibile. Uno di questi modelli è già disponibile con il nome "Sealed mode".

Nel frattempo, non basta che gli utenti leggano attentamente tutte le informazioni che vengono presentate dai gestori, ma occorre anche che essi cerchino anche di comprenderne il significato, che talvolta viene accidentalmente o deliberatamente mascherato.

Come regola generale, meno dati personali si mettono in rete, meglio è per il soggetto coinvolto!

Adalberto Biasiotti

Licenza Creative Commons

www.puntosicuro.it