PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 25 - numero 5443 di Lunedì 31 luglio 2023

L'uso di applicativi di intelligenza artificiale di tipo generativo

Otto raccomandazioni sull'uso di applicativi di intelligenza artificiale generativi, come ChatGPT, offerte da uno dei massimi esperti del settore.

Il rispetto del regolamento generale in materia di protezione dei dati personali rappresenta uno dei maggiori punti di debolezza dell'utilizzo delle applicazioni di intelligenza artificiale, di tipo generativo.

Si tratta di un problema che turba gli enti regolatori anche di là dell'Atlantico, tanto è vero che la Federal Trade Commission ha inviato alla società OpenAI un questionario con 20 quesiti, afferenti proprio alle modalità con cui l'applicativo di intelligenza artificiale cattura dati personali e li tratta, per successivamente mettere a disposizione dei clienti, che abbiano posto quesiti specifici.

Ecco il motivo per cui un esperto di protezione dati personali, con sede in Europa, ha elaborato otto quesiti, ai quali occorre dare appropriata risposta, prima di utilizzare questi strumenti, tanto attraenti, almeno in via potenziale, quanto pericolosi.

1-Prima di utilizzare questi applicativi, avete effettuato un'analisi di compatibilità con il regolamento generale europeo sulla protezione dei dati personali?

È bene ricordare che la protezione dei dati si applica anche quando le informazioni personali, che vengono trattate dal titolare, sono estratte da documenti pubblici. L'utilizzo degli applicativi di intelligenza artificiale, che trattano questi dati, deve essere basato su una valida motivazione, come ad esempio il consenso del soggetto interessato o la prova dell'esistenza di interessi legittimi.

2-Siete un titolare, un contitolare od un responsabile del trattamento di dati?

È bene ricordare che la responsabilità nell'utilizzo di applicativi di intelligenza artificiale ricade sul titolare del trattamento. Anche se quest'ultimo utilizza modelli sviluppati da altri soggetti, la responsabilità finale circa un appropriato utilizzo è sempre in carico al titolare, al contitolare o ad un responsabile.

3-È stata elaborata una valutazione di impatto, in conformità all'articolo 35 del G d.p.r.?

I rischi legati all'utilizzo di questi applicativi, che possono coinvolgere dati personali, devono essere valutati e messi sotto controllo con una valutazione di impatto, da portare a termine prima dell'inizio del trattamento dei dati. Il documento inoltre deve essere mantenuto costantemente aggiornato, in funzione dell'evoluzione del trattamento dei dati stessi.

4-Come viene garantita la trasparenza del trattamento dei dati?

Salvo i ridotti casi, per cui esistono esenzioni, il titolare deve rendere edotti tutti i soggetti potenzialmente coinvolti dei tipi di trattamento, cui egli sottopone i loro dati personali. La soluzione più soddisfacente è certamente quella nella quale il titolare comunica queste informazioni ai singoli titolari.

5-Come vengono messi sotto controllo i rischi afferenti alla sicurezza?

Oltre ai rischi legati a una possibile perdita di dati, il titolare deve valutare e mitigare tutti i rischi afferenti a un possibile inquinamento dei dati ed a un possibile attacco per sottrazione dei dati stessi.

6-Vengano attuate procedure che limitano il trattamento alle sole attività necessarie?

È bene ricordare che il titolare può solo prendere i dati che sono necessari per soddisfare dichiarate esigenze del trattamento.

7-Come viene soddisfatto il diritto di accesso degli interessati coinvolti?

Il titolare deve essere in grado di soddisfare non solo il diritto di accesso degli interessati coinvolti, ma anche il diritto di rettifica, cancellazione e altri diritti previsti dal regolamento generale europeo.

8-Gli applicativi generativi di intelligenza artificiale vengono utilizzati per assumere decisioni automatizzate?

Prestare la massima attenzione a questi scenari, per le possibili pericolose conseguenze. Si pensi ad esempio al fatto che in alcune strutture sanitarie vengono usati questi applicativi per diagnosi di malattie. Il regolamento generale europeo tiene sotto strettissimo controllo qualunque decisione automatizzata, non opportunamente validata da un titolare o responsabile.

Infine ...

Può essere opportuno ricordare ai lettori che, nella elaborazione di recenti capitolati, sono stati già inserite delle clausole che specificamente proibiscono all'offerente di inserire nel testo della sua offerta documenti o porzioni di documenti, che siano stati elaborati dalla intelligenza artificiale generativa. Parimenti, si chiede uno specifico impegno all'aggiudicatario della gara di non inserire analoghi documenti in relazioni od altri testi, che l'aggiudicatario debba elaborare nel corso della prestazione del servizio.

In sintesi, attenzione, attenzione ed ancora attenzione!

Adalberto Biasiotti

www.puntosicuro.it