Domani

NON È COME SEMBRA

Qual è la vera posta in gioco su privacy e intelligenza artificiale

VITALBA AZZOLLINI
giurista

Il provvedimento di «limitazione provvisoria del trattamento dei dati personali degli interessati stabiliti nel territorio italiano», adottato dal Garante per la Protezione dei dati personali (Garante Privacy) nei riguardi di OpenAI, società statunitense sviluppatrice e gestrice di ChatGpt, ha suscitato reazioni per lo più negative, quasi che l'Autorità stesse ponendo ostacoli al progresso tecnologico.
La sensazione è quella di un ritorno al marzo del 2020 quando, all'inizio della pandemia, a fronte di obiezioni poste dal Garante, ad esempio, riguardo ad alcune iniziative di *contact tracing*, le istanze di tutela dei dati personali venivano qualificate come "fisima".
All'epoca si riteneva che tali istanze ostacolassero la tutela della salute così come oggi si pensa intralcino l'evoluzione scientifica. Le cose non stanno in questo modo.

Il provvedimento

"Limitazione del trattamento" significa individuare alcuni dati personali e renderli inaccessibili agli utenti, così che «non siano sottoposti a ulteriori trattamenti» (considerando 67 del Regolamento europeo sulla protezione dei dati personali, Gdpr). Dunque, l'Autorità non ha imposto il blocco del servizio offerto da OpenAI, come qualcuno ha detto.
Il Garante contesta alla società, in primo luogo, l'assenza di informativa sul trattamento dei dati tramite ChatGpt, cioè di una comunicazione preventiva e trasparente sulle finalità e le modalità del trattamento stesso.
In secondo luogo, la mancanza di «idonea base giuridica», vale a dire ciò che rende lecito l'utilizzo dei dati personali; in terzo luogo, l'inesattezza del trattamento dei dati, «in quanto le informazioni fornite da ChatGpt non sempre corrispondono al dato reale», come lamentato da molti interessati.
Infine che, secondo i termini pubblicati da OpenAI, il servizio ChatGpt è giudicato inappropriato a chi non abbia compiuto almeno 13 anni, ma manca «qualsivoglia verifica dell'età degli utenti», e ciò espone i minori di tale età a risposte «inidonee rispetto al grado di sviluppo e autoconsapevolezza degli stessi».
Entro 20 giorni, OpenAI deve comunicare le iniziative «intraprese al fine di dare attuazione a quanto prescritto» e «fornire ogni elemento ritenuto utile a giustificare le violazioni sopra evidenziate».

Le critiche

Nonostante l'Autorità non abbia posto il blocco, ma la limitazione provvisoria del trattamento dei dati degli utenti in Italia, come detto, la società ha comunque bloccato l'uso del servizio dall'Italia.
OpenAI avrebbe potuto continuare a offrire il suo servizio, escludendo i dati degli utenti indicati dal Garante. Ma non l'ha fatto.
Questa, più che una scelta, pare la constatazione di un fatto: il meccanismo implementato dall'intelligenza artificiale non consente di isolare i dati di specifici utenti e di escluderli dal sistema.
E ciò è un problema, non solo al fine di assolvere alle richieste del Garante e proseguire il servizio, ma in quanto forse significa che la società non sarebbe in condizione di isolare tali dati nemmeno se singoli utenti ne chiedessero l'aggiornamento, la rettifica la cancellazione oppure volessero ottenere la limitazione del loro uso (proprio ciò che ha chiesto il Garante).
Questa impossibilità si tradurrebbe in una violazione del Gdpr, poiché quelli elencati sono diritti che il Gdpr stesso attribuisce agli interessati (artt. 15-22), e chi tratta i loro dati deve poterne consentire l'esercizio.
Ma se OpenAI non può isolare i dati degli utenti italiani per ottemperare alle richieste del Garante, evidentemente non potrebbe isolarli nemmeno per ottemperare alle richieste degli utenti stessi circa i

loro dati, come invece dovrebbe essere in grado di fare ai sensi del Gdpr.

L'informativa

Il Garante contesta la mancanza di informativa resa a coloro i quali utilizzano il servizio fornito da OpenAI.
Qualcuno obietta che un'informativa è presente. Ma essa è comunque, è carente di elementi essenziali.
Inoltre, se pure è notorio che i dati sono elaborati a fini di sviluppo e miglioramento del sistema, tuttavia non sono chiariti né esclusi altri scopi.
Ciò viola uno dei principi fondanti del Gdpr, secondo cui i dati personali devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità.
Il Garante rileva, altresì, che non sono indicate le basi giuridiche del trattamento dei dati. Tra tali basi, il Gdpr (art. 6) indica il consenso o il contratto, di cui tuttavia nel caso in esame non c'è traccia.
Ma non può nemmeno ritenersi che ricorra un "legittimo interesse" di OpenAI a trattare i dati degli utenti: questa base giuridica, pure indicata dal Gdpr, giustifica il trattamento quando il legittimo interesse di chi tratta i dati risulti coincidente o analogo rispetto agli interessi dei soggetti cui i dati appartengono.
Ciò presuppone che il trattamento non rechi un danno a tali soggetti.
Ma siccome non sempre ChatGpt restituisce dati corretti, ciò significa che un pregiudizio esiste.
Tanto più perché con quei dati errati il sistema opera ulteriori elaborazioni, amplificando l'errore, e con esso il pregiudizio.

Il problema inesattezze

Circa l'inesattezza dei risultati rilasciati dal sistema, si potrebbe obiettare che ciò accade con qualsiasi motore di ricerca.
Quest'obiezione non è del tutto fondata.
Infatti, mentre sul motore di ricerca è l'utente che deve valutare i risultati offerti e, vagliate le fonti, decidere di quali avvalersi, ChatGpt offre un prodotto preconfezionato, le cui fonti si perdono nel processo di addestramento.
Ma, soprattutto, i dati forniti da un qualunque motore di ricerca possono essere isolati, per correggerli, modificarli o eliminarli su richiesta degli interessati. Cosa che non pare possibile per ChatGpt.
Infine, secondo taluni, l'inadeguatezza del Gdpr rispetto ai sistemi di intelligenza artificiale dovrebbe indurre il Garante ad evitare interventi "eccessivi" come quello che, invece, avrebbe fatto nel caso in esame.
Attenzione: l'applicazione della legge non è un'opzione per un'autorità amministrativa.
Quest'ultima deve innanzitutto intervenire affinché i diritti delle persone siano tutelati.
Solo dopo può instaurare quel dialogo collaborativo con la controparte, che in molti auspicano e che di certo il Garante avvierà dopo la risposta di OpenAI.