

GDPR e intelligenza artificiale, il Report della task force europea su ChatGPT

Quali sono i principi di protezione dei dati personali applicabili a ChatGPT? È la domanda a cui risponde il Report sul lavoro della task force del Comitato europeo (EDPB), creata lo scorso anno per promuovere la cooperazione tra le Autorità di protezione dei dati personali che indagano a livello nazionale sul chatbot di OpenAI.

Nel valutarne la liceità, il Report suggerisce di distinguere le diverse fasi del trattamento: raccolta dati per addestramento, compresi web scraping o riutilizzo di set di dati; pre-elaborazione, compreso il filtraggio; addestramento; prompt e output di ChatGPT; addestramento di ChatGPT con prompt.

Particolare attenzione viene riservata al web scraping. Per la raccolta dei dati, OpenAI ha individuato come base giuridica il legittimo interesse del titolare. Una condizione che – ricorda l'EDPB – deve essere bilanciata con diritti e le libertà fondamentali degli interessati. Benché le istruttorie siano ancora in corso, il Comitato europeo suggerisce alcune garanzie che potrebbero rendere lecito il legittimo interesse, come la definizione di criteri di raccolta e l'esclusione di determinate categorie di dati e fonti (es: profili pubblici sui social). Ulteriori misure adottabili potrebbero essere la cancellazione o l'anonimizzazione dei dati personali prima della fase di addestramento.

Per quanto riguarda le categorie particolari di dati, per le quali è necessario un consenso specifico e caratterizzato da

un'azione positiva, le misure potrebbero prevedere un filtraggio, da applicare sia alla raccolta dei dati, selezionandone ad esempio i criteri, sia immediatamente dopo, eliminandoli.

Oltre alla liceità della raccolta dei dati per l'addestramento di ChatGPT, il Report sul lavoro della task force analizza il principio di correttezza, in base al quale spetta a OpenAI garantire la conformità al GDPR; il principio di trasparenza e quello di esattezza, secondo i quali il titolare del trattamento dovrebbe fornire informazioni adeguate sulla natura probabilistica dell'output chatbot e fare esplicito riferimento al fatto che il testo generato potrebbe essere parziale o inventato. Sempre in base al principio di trasparenza, OpenAI dovrebbe informare gli interessati che il contenuto prodotto dell'utente, vale a dire l'input fornito al sistema, viene usato per addestrare il chatbot.

Il Comitato europeo sottolinea infine come sia obbligatorio che gli interessati possano esercitare i loro diritti in modo efficace. Il Report è il risultato di valutazioni preliminari che non pregiudicano l'analisi che verrà effettuata da ciascuna Autorità nazionale nell'ambito delle istruttorie in corso, aperte prima del 15 febbraio 2024, quando OpenAI ha posto stabilimento in Europa. Da quella data le attività di trattamento transfrontaliero della società Usa rientrano nell'ambito di applicazione dello Sportello unico (One-stop shop).

<https://www.key4biz.it/gdpr-e-intelligenza-artificiale-il-report-della-task-force-europea-su-chatgpt/493468/>