NORME E TRIBUTI Il Sole 24 Ore lunedì 03 FEBBRAIO 2025

Un modello è anonimo solo se non consente di estrarre dati personali

Per essere considerato anonimo, un modello di intelligenza artificiale deve soddisfare almeno due condizioni: la pressoché nulla o insignificante probabilità di estrazione diretta di dati personali da parte del modello e l'impossibilità di ottenere, intenzionalmente o meno, informazioni personali tramite domande o specifiche query. A chiarirlo è lo European Data Protection Board (Edpb) con l'Opinion n. 28 del 18 dicembre 2024 che rappresenta un tassello cruciale nell'applicazione della protezione dei dati personali nel contesto dello sviluppo dei modelli di Ia. Il parere, richiesto dall'autorità irlandese per la protezione dei dati, si concentra su una serie di aspetti legati alla fase di sviluppo dei modelli di Ia.

Secondo l'Edpb la progettazione e la documentazione di conformità del modello di Ia giocano un ruolo chiave e sono essenziali per garantire la selezione accurata delle fonti, la minimizzazione dei dati, l'implementazione di misure tecniche e organizzative da adottare ai processi di machine-learning e le scelte metodologiche durante l'addestramento, nonché le misure adottate per prevenire l'identificazione di dati personali riferiti, direttamente o indirettamente, a persone fisiche.

Per quanto riguarda l'utilizzo dell'interesse legittimo come base giuridica per il trattamento dei dati personali durante le fasi di sviluppo e implementazione dei modelli di Ia, il parere evidenzia come non esista una gerarchia definita tra le basi giuridiche previste dal Regolamento europeo sulla protezione dei dati (Gdpr), ma che spetta ai titolari identificare quella più appropriata (principio di *accountability*).

Per i modelli di Ia, il legittimo interesse può essere una base di liceità astrattamente valida e spendibile, purché sia sottoposto ad un rigoroso bilanciamento basato su un test tripartito: l'interesse legittimo deve essere concreto, e quindi reale, legale e attuale, il trattamento deve esser necessario per perseguire tale interesse, e non deve prevaricare i diritti e le libertà fondamentali degli interessati, le cui ragionevoli aspettative devono essere rispettate, tenuto conto del contesto e delle possibili implicazioni pratiche.

Il parere affronta inoltre il tema delle conseguenze del trattamento illecito di dati personali durante la fase di sviluppo di modelli di Ia e delinea tre scenari. In particolare, il terzo riguarda il caso in cui un titolare utilizzi dati personali raccolti illecitamente durante la fase di sviluppo di un modello di Ia, ma successivamente applichi misure per garantire l'anonimizzazione del modello e, a seguire, avvii ulteriori trattamenti di dati personali nel contesto dell'implementazione del modello.

In tale circostanza, se il titolare del trattamento riesce a dimostrare che il modello è stato effettivamente anonimizzato e che l'operatività successiva non comporta più il trattamento di dati personali, il quadro sanzionatorio previsto dal Gdpr non si applica a questo utilizzo.

Questo approccio "sostanzialistico", si basa sul fatto che un'anonimizzazione efficace (e adeguatamente documentata) trasforma irreversibilmente i dati personali in informazioni che non permettono più di identificare gli interessati, neppure indirettamente, con la conseguenza che l'illiceità del trattamento iniziale non produce effetti sull'operatività successiva del modello (ferme restando le sanzioni relative all'invalidità delle operazioni di raccolta originaria dei dati).

Il parere si inserisce in un contesto più ampio che include l'Ai Act e le sinergie tra Gdpr e e Ai Act saranno sempre più alla base di una regolamentazione digitale integrata e dinamica, capace di rispondere alle sfide poste dall'innovazione tecnologica, garantendo che lo sviluppo di sistemi di Ai sia etico e conforme ai diritti fondamentali e alla protezione dei dati dei cittadini europei.