ChatGPT, verso un sistema per tutelare diritti e innovazione

Ia e privacy

L'intervento del Garante evidenza lacune normative ed esigenze di formazione

Marco Bassini
Oreste Pollicino

Come bilanciare tutela dei diritti fondamentali e promozione dell'innovazione nell'era dell'intelligenza artificiale? La decisione del Garante per la privacy su ChatGPT, datata 2 novembre 2024, è un esempio emblematico delle sfide che l'Europa si trova ad affrontare nel regolare l'uso dell'Ia generativa. La decisione, nata dall'istruttoria su un data breach, non si limita a censurare alcune pratiche di OpenAI, ma a ben vedere suggerisce a un approccio ai problemi emergenti più ampio e strutturato (si veda «Il Sole24 Ore» del 21 dicembre).

Il caso

Un incidente del 20 marzo 2023 ha permesso ad alcuni utenti di ChatGPT di accedere alla cronologia di conversazioni altrui, rivelando informazioni personali anche sensibili. La reazione del Garante è stata immediata: avviare un'istruttoria e imporre misure correttive che evidenziano la centralità dello strumentario della protezione dei dati personali. Ma è nel contenuto del provvedimento che emerge il vero punto di svolta: non si tratta solo di sanzionare una violazione, ma di proporre un modello di gestione dei rischi connessi alle tecnologie emergenti. Un'esigenza molto sentita, per la necessità di calare le regole del Gdpr nella dimensione peculiare dei sistemi di Ia generativa, la cui imprevedibilità rende talvolta complesso applicare gli schemi normativi immaginati prima del boom dell'Ia.

OpenAI, rimediando al suo approccio iniziale lacunoso, ha dovuto adeguarsi alle strettoie della normativa sulla protezione dati, introducendo per esempio misure per garantire la trasparenza e la verifica dell'età degli utenti, oltre a migliorare la gestione delle informazioni trattate. Il provvedimento, così, ma punta a promuovere pratiche responsabili.

L'approccio allargato

Ne emerge che l'Ia generativa non si può regolare efficacemente senza coinvolgere attivamente i suoi principali attori: sviluppatori, utilizzatori e utenti. Si conferma l'importanza di una co-regolamentazione che integri il tradizionale approccio command-and-control fondato su sanzioni, formulando codici di condotta che trovano esplicito riconoscimento nel quadro normativo Ue. Come accade già col Digital services act nel campo dei servizi digitali, tali strumenti permettono di personalizzare le misure in base ai rischi specifici posti dai sistemi in questione.

La decisione del Garante evidenzia come il Gdpr rimanga il pilastro del costituzionalismo digitale europeo, ma anche come necessiti di evolversi per cogliere e governare le peculiarità dell'Ia. Se la tecnica non può imporsi sul diritto, essa può tuttavia evidenziarne lacune e precarietà. Così, la complessità dei modelli linguistici generativi pone problemi inediti: dalla definizione della base giuridica del trattamento di dati, specie in fase di addestramento dei modelli, alla rettifica di informazioni inesatte o non più attuali, fino alla trasparenza delle operazioni algoritmiche.

Inoltre, il principio «One Stop Shop», che dovrebbe facilitare la cooperazione tra le autorità nazionali di protezione dati, si è rivelato un punto debole in questo caso: la notifica del data breach all'autorità irlandese, individuata da OpenAI come riferimento, ha generato tensioni giurisdizionali che richiedono interventi per migliorare il coordinamento tra Stati.

Un altro aspetto fondamentale che emerge dal provvedimento è la necessità di formare cittadini e imprese a comprendere e utilizzare consapevolmente le tecnologie di Ia. L'*Ai literacy* deve diventare una priorità, integrando percorsi educativi e iniziative aziendali per garantire che l'interazione con queste tecnologie sia informata e responsabile da parte di tutti.

Il provvedimento del Garante su ChatGPT è dunque, e a ragion veduta, molto più di una risposta a una violazione di dati personali occasionata da un incidente informatico; è un esempio di come l'Europa stia cercando di definire un equilibrio tra diritti fondamentali e innovazione, puntando su un modello di governance che coinvolga tutti i portatori di interessi. Il percorso è complesso e richiede risorse, ma è l'unica via per garantire che lo sviluppo tecnologico avvenga nel rispetto dei valori fondamentali della società europea.