ChatGPT, privacy e Copyright. Problemi e opportunità

Tuesday 16 May 2023

Il diffondersi di ChatGPT porta con sé molte opportunità e problemi, quali privacy e tutela della privacy. A che punto siamo?

ChatGPT: cos'è e cosa significa l'acronimo

ChatGPT è uno degli strumenti di **intelligenza artificiale conversazionale più noti e discussi al mondo.**

In pratica, si tratta di una chat bot in grado di rispondere in maniera coerente e molto più approfondita delle precedenti versioni di sistemi di conversazione con intelligenza artificiale, con una capacità non solo di apprendimento ma, anche, esperienziale. ChatGPT, in pratica, è in grado di imparare e di tarare la sua capacità di risposta in base all'esperienza dettata da documenti, video e altro materiale inerente alla materia sulla quale si effettua l'interrogazione.

ChatGPT è l'acronimo di **Generative Pretrained Transformer**, ovvero uno strumento di **Natural Language Processing molto avanzato** che utilizza **algoritmi complessi di apprendimento automatico** per generare risposte il più possibile simili a quelle che darebbe un essere umano competente nell'ambito di un discorso.

ChatGPT è stata realizzata dalla OpenAI, un'organizzazione no profit per la ricerca sull'intelligenza artificiale (AI, appunto).

Oltre alle evidenti problematiche morali e pratiche che un massivo uso di tale strumento potrebbe comportare (si pensi soltanto alla capacità teorica di sostituirsi a buona parte delle professioni intellettuali oggi esistenti), **ChatGPT ha messo in luce diverse criticità anche sul lato privacy e diritto alla riservatezza. Vediamo quali.**

Chat GPT e lo stop Garante italiano per la protezione dei dati personali

Il Garante per la protezione dei dati personali ha disposto la limitazione al trattamento dei dati degli utenti italiani nei confronti di OpenAI, la società statunitense che, come abbiamo visto, ha sviluppato la piattaforma. L'Autorità ha contestualmente aperto un'istruttoria.

Il provvedimento del Garante per la privacy (Registro dei provvedimenti n. 112 del 30 marzo 2023) ha disposto, dunque, "in via d'urgenza, nei confronti di OpenAI L.L.C., società statunitense sviluppatrice e gestrice di ChatGPT, in qualità di titolare del trattamento dei dati personali effettuato attraverso tale applicazione, la misura della limitazione provvisoria, del trattamento dei dati personali degli interessati stabiliti nel territorio italiano".

Tutto ciò è dovuto al fatto che il 20 marzo 2023 ChatGPT aveva subito una perdita di dati (c.d. *data breach*) relativa alle conversazioni degli utenti e alle informazioni riguardanti il pagamento degli abbonati al servizio a pagamento.

In pratica, nel provvedimento in commento il Garante privacy rileva la mancanza di una informativa agli utenti e a tutti gli interessati i cui dati vengono raccolti da OpenAI, ma soprattutto l'assenza di una base giuridica che giustifichi la raccolta e la conservazione dei dati personali, con la funzione di insegnare agli algoritmi a rispondere in maniera complessa, articolata e più approfondita.

ChatGPT: quali sono le violazioni rilevate dal Garante?

Oltre a quanto sopra, il Garante Privacy sottolinea che manca in concreto una informativa agli utenti e agli interessati del trattamento dei dati personali raccolti dalla società OpenAI. Inoltre, il trattamento dei dati risulta non esatto, poiché spesso le informazioni fornite da ChatGPT non corrispondono al dato reale.

Infine, nonostante sia dichiarato che il servizio è rivolto ai maggiori di 13 anni, risulta assente in ChatGPT un filtro di verifica dell'età degli utenti.

Il Garante ha concesso ad OpenAI fino al 30 aprile per adempiere alle prescrizioni imposte.

ChatGPT: il secondo provvedimento del Garante dell'11 aprile.

Il Garante Privacy, con provvedimento registrato al n. 114 dell'11 aprile 2023 ha sospeso la limitazione provvisoria adottata col precedente provvedimento, a patto che Open AI realizzi quanto previsto dal provvedimento in commento.

Ovvero dovrà:

*1. **predisporre e pubblicare sul proprio sito internet un'informativa** che, nei termini e con le modalità di cui all'art. 12 del Regolamento, spieghi agli interessati anche diversi dagli utenti del servizio ChatGPT, i cui dati sono stati raccolti e trattati ai fini dell'addestramento degli algoritmi, le modalità del trattamento, la logica alla base del trattamento necessario al funzionamento del servizio, i diritti loro spettanti in qualità di interessati e ogni altra informazione prevista dal Regolamento;*

*2. mettere a disposizione, sul proprio sito Internet, almeno agli interessati, anche diversi dagli utenti del servizio, che si collegano dall'Italia, uno **strumento attraverso il quale possano esercitare il diritto di opposizione rispetto ai trattamenti dei propri dati personali**, ottenuti da terzi, svolti dalla società ai fini dell'addestramento degli algoritmi e dell'erogazione del servizio;*

*3. mettere a disposizione, sul proprio sito Internet, almeno agli interessati, anche diversi dagli utenti del servizio, che si collegano dall'Italia, uno **strumento attraverso il quale chiedere e ottenere la correzione di eventuali dati personali che li riguardano trattati in maniera inesatta nella generazione dei contenuti** o, qualora ciò risulti impossibile allo stato della tecnica, la cancellazione dei propri dati personali;*

*4. **inserire un link all'informativa rivolta agli utenti dei propri servizi nel flusso di registrazione in una posizione che ne consenta la lettura prima di procedere alla registrazione**, attraverso modalità tali da consentire a tutti gli utenti che si collegano dall'Italia, ivi inclusi quelli già registrati, al primo accesso successivo all'eventuale riattivazione del servizio, di prendere visione di tale informativa;*

*5. **modificare la base giuridica del trattamento dei dati personali degli utenti ai fini dell'addestramento degli algoritmi**, eliminando ogni riferimento al contratto e assumendo come base giuridica del trattamento il consenso o il legittimo interesse in relazione alle valutazioni di competenza della società in una logica di accountability;*

6. mettere a disposizione, sul proprio sito Internet, almeno agli utenti del servizio, che si collegano dall'Italia, uno ***strumento facilmente accessibile attraverso il quale esercitare il diritto di opposizione al trattamento dei propri dati acquisiti in sede di utilizzo del servizio per l'addestramento degli algoritmi*** *qualora la base giuridica prescelta ai sensi del punto 5 che precede sia il legittimo interesse;*

7. ***in sede di eventuale riattivazione del servizio dall'Italia, inserire la richiesta, a tutti gli utenti che si collegano dall'Italia, ivi inclusi quelli già registrati, di superare, in sede di primo accesso, un age gate che escluda, sulla base dell'età dichiarata, gli utenti minorenni****;*

8. sottoporre al Garante, entro il 31 maggio 2023, un ***piano per l'adozione di strumenti di age verification idoneo a escludere l'accesso al servizio agli utenti infratredicenni e a quelli minorenni in assenza di un'espressa manifestazione di volontà da parte di chi esercita sugli stessi la responsabilità genitoriale*** *. L'implementazione di tale piano dovrà decorrere, al più tardi, dal 30 settembre 2023;*

9. ***promuovere, entro il 15 maggio 2023, una campagna di informazione, di natura non promozionale, su tutti i principali mezzi di comunicazione di massa italiani*** *(radio, televisione, giornali e Internet) i cui contenuti andranno concordati con il Garante, allo scopo di informare le persone dell'avvenuta probabile raccolta dei loro dati personali ai fini dell'addestramento degli algoritmi, dell'avvenuta pubblicazione sul sito internet della Società di un'apposita informativa di dettaglio e della messa a disposizione, sempre sul sito internet della Società, di uno strumento attraverso il quale tutti gli interessati possono chiedere e ottenere la cancellazione dei propri dati persona*li;

In risposta a quanto sopra, OpenAi ha introdotto la modalità incognito e altre novità per venire incontro alle richieste privacy del Garante italiano. Ma quanto messo in atto pare insufficiente e al limite dell'applicabilità concreta, anche tenuto conto dei meccanismi di funzionamento su cui si basano chat bot come ChatGPT.

ChatGPT e privacy: il Garante dà spunti "risposte" importanti

Nel provvedimento con cui il Garante ha sospeso la limitazione provvisoria di ChatGPT, l'**Autorità sembra lasciarsi scappare "risposte" importanti sulla base giuridica del trattamento dei dati personali degli utenti ai fini dell'addestramento degli algoritmi**.

Riassumendo: **il contratto no**. Il titolare scelga tra il consenso o il legittimo interesse, "*in relazione alle valutazioni di competenza della società in una logica di accountability*".

Ben conscio del fatto che **difficilmente in un tale contesto la base giuridica possa essere rappresentata validamente dal consenso** – tra i profili critici, si pensi al problema della sua revocabilità quando ormai i dati sono "irrimediabilmente" stati appresi da ChatGPT o, ancora, le probabili difficoltà applicative relative al requisito della libertà di un tale consenso (sarebbe possibile che ChatGPT non apprenda nulla dalla mia sessione ove non dia il consenso al trattamento?) – nel punto subito successivo (punto 6), **il Garante specifica che, ovviamente, ove la base giuridica scelta sia il legittimo interesse, l'interessato deve conservare l'esercizio del diritto di opposizione**.

Queste prescrizioni dell'Autorità sono molto importanti perché offrono **considerazioni su aspetti privacy mutuabili anche per tutti i sistemi di AI e/o machine learning che imparano e si addestrano grazie alla mole di dati raccolta presso gli stessi utilizzatori**.

Sarà interessante vedere come il **punto di equilibrio tra legittimo interesse al training di ChatGPT e diritti degli utilizzatori** sarà raggiunto nei casi in cui l'utente eserciti l'opposizione al trattamento.

Come farà ChatGPT a "dimenticare" ciò che ha imparato quando l'utente esercita il diritto di opposizione?

In quali casi concreti ChatGPT sarà legittimata a dire all'utente "no, il mio legittimo interesse prevale sulle tue libertà"?

Ragionando a voce alta, presumiamo che la "chiave di volta" sarà individuata nell'applicazione di **tecniche di anonimizzazione capaci di salvare il risultato appreso da ChatGPT svincolandolo dall'identità dell'utente**.

ChatGPT ed editoria: problemi di copyright?

Per ChatGpt, dunque, i problemi non finiscono qui. L'editoria mondiale, infatti, sta alzando le proprie barricate per fermare lo sfruttamento dei contenuti digitali ad opera delle chat bot e di piattaforme quali ChatGpt o Bard.

Equo compenso a parte, questione ancora tutta da definire in maniera certa e concreta, **il problema si sposta sullo spostamento del traffico Internet dalle principali testate mondiali di informazione**, con particolare riferimento agli investimenti effettuati dall'editoria su SEO (Search engine optimization) per essere "trovati" e visualizzati sui motori di ricerca (leggi Google) e sui paywall realizzati per monetizzare i contenuti digitali a pagamento delle testate.

In pratica, l'utilizzo di massa di ChatGpt potrebbe far saltare il banco dei principali editori mondiali cartacei e digitali e dei motori di ricerca stessi, Google in primis.

Microsoft – che sta lavorando per integrare ChatGpt al suo motore di ricerca Bing – sta già valutando l'inserimento di annunci pubblicitari nelle chat di risposta agli utenti, i cui proventi saranno ripartiti con gli editori.

D'altro canto OpenAi sta lavorando parallelamente per realizzare un accordo strategico con i giornali. Ha infatti annunciato **una alleanza con alcune aziende di servizio, tra cui Expedia, Shopify e Klarna, con il risultato di inserire collegamenti ipertestuali nelle risposte di ChatGPT alle ricerche degli utenti sui brand oggetto di accordo** (ad esempio, al quesito: dove posso dormire a Londra? ChatGPT risponde con l'inserimento di un collegamento diretto al sito di Expedia che contestualmente elabora la proposta di un viaggio nel luogo cercato).

ChatGPT: le nuove frontiere giudiziarie

Per chiudere questa carrellata del tutto preliminare sull'universo ChatGPT, segnaliamo due nuovi fronti.

Il primo, quello della giustizia, in cui l'intelligenza artificiale sembra prendere sempre più il posto dell'uomo.

In Perù, infatti, la Corte superiore di Giustizia di Lima Sud è ricorsa a ChatGPT per risolvere una controversia tra i genitori di un minore per determinare l'assegno di mantenimento per i figli.

L'algoritmo di ChatGPT ha infatti deciso che il padre dovrà versare il 20 per cento del proprio reddito alla figlia minore. A corredo della decisione, il 27 marzo 2023 la Corte di Lima Sud ha emanato una sentenza su l'expediente 00052-2022-18-3002-Jp-Fc-0.

L'altro, quello della proprietà intellettuale. D'altronde, **ChatGPT ha già scritto il finale di un episodio del noto cartoon South Park** (episodio 4 della stagione 26, **no spoiler**), in cui ChatGPT viene utilizzato per scrivere ottimi temi scolastici, per parlare col partner quando non si ha voglia e, udite udite, addirittura per capire l'altro sesso!

Sulla tutela dell'opera realizzata dall'AI il tema è più che mai aperto e non si limita a ChatGPT.

Ad oggi, **in Europa l'AI non può essere considerata inventore di un'opera**. Al massimo, è inventore la persona fisica che utilizza l'AI come strumento per realizzare un'opera (è il caso di SouthPark). **La potenza di ChatGPT e degli altri sistemi di AI arriverà al punto da segnare la necessità di un'inversione di rotta**?

Infine, ultima ma non ultima, la notizia **del primo libro scritto interamente dall'intelligenza artificiale**.

Sul *New York Times*, *infatti*, è uscita la prima recensione di un romanzo breve scritto interamente dall'AI. Il romanzo, con una voluta ironia, si intitola "*Death of an Author*", **è un giallo ed è il risultato del lavoro combinato di tre diversi software, ChatGPT, Sudowrite e Cohere**, coadiuvati dai prompt inseriti dal giornalista e scrittore Stephen Marche.

Insomma, chatGPT segnerà davvero la morte degli scrittori? Forse, ma resta un dubbio: come potrà firmarsi?

Per questo libro, è stato scelto uno pseudonimo, **Aidan Marchine**, gioco di parole che mette assieme i nomi di tutti e quattro i coautori del romanzo. Per eventuali bestseller, invece, vedremo cosa accadrà.

Insomma, le possibilità applicative di ChatGPT sono infinite, e ognuna porta con sé altrettante considerazioni su aspetti legali e non solo. Immense praterie a nostra disposizione. Saremo in grado di percorrerle tutte in sicurezza?