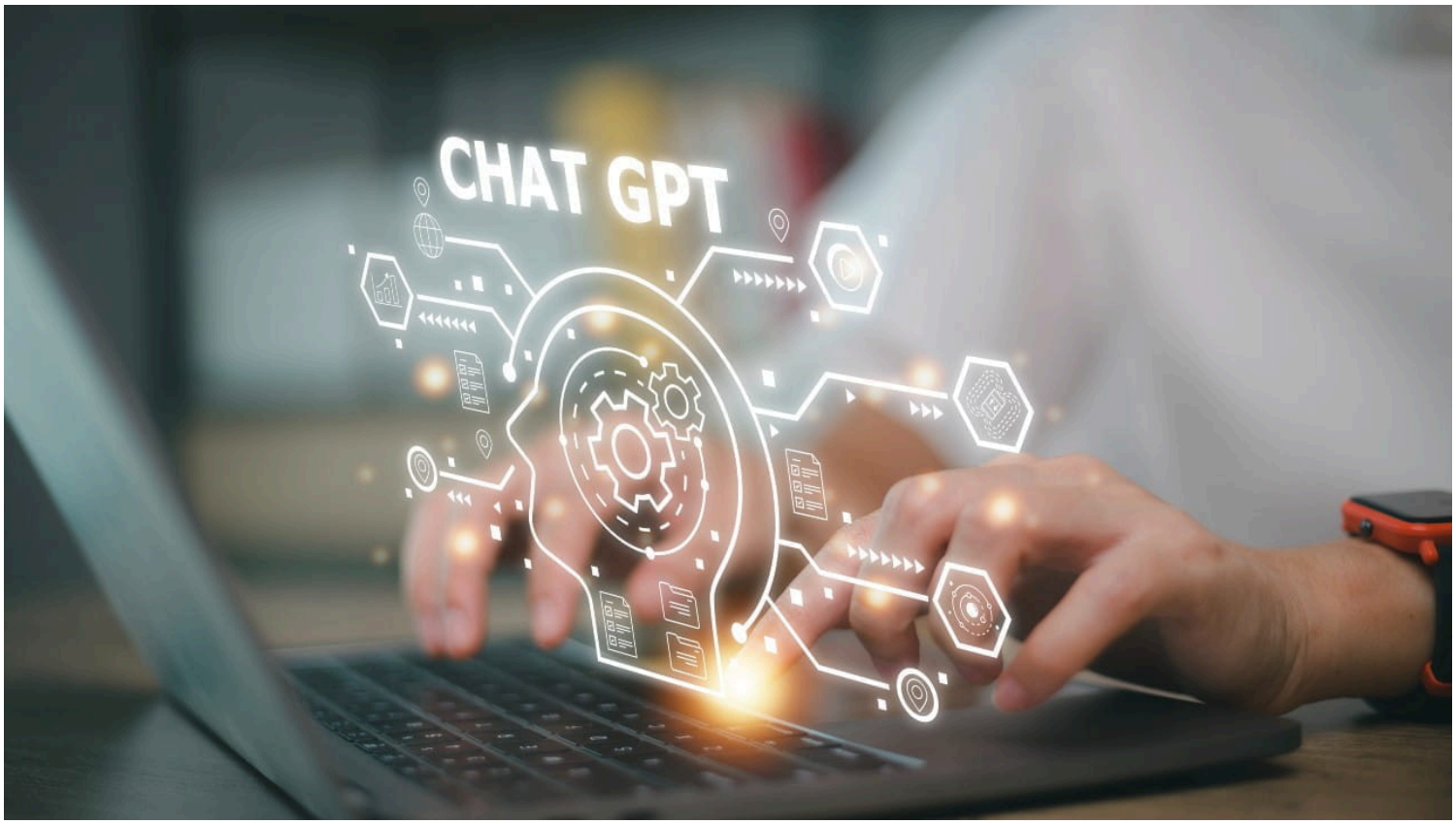
Fintech | Digital transformation & tech | Normativa | Fiscal e legal

Chat Gpt: l'intelligenza artificiale e i rischi per la privacy degli utenti

Alessandro Foti, Adriano Garofalo

17.3.2023

Tempo di lettura: 3'



ChatGpt sta catalizzando l'interesse dell'opinione pubblica confermando la centralità delle questioni connesse alla protezione dei dati personali e al contempo il fortissimo legame che essa ha con lo sviluppo delle nuove tecnologie. Come bilanciare le due facce della stessa medaglia?

ChatGpt, acronimo di Generative pretrained transformer, è un **modello di intelligenza artificiale realizzato da OpenAI**, basato sul machine learning e in grado di comunicare con gli utenti a un livello di umanizzazione mai visto prima. Sin dai primi giorni di release online il software sottoforma di chat box ha interagito con milioni di utenti mostrando **potenzialità** e **insidie** che sono argomento di grande attualità nella rete per operatori del settore, giuristi e istituzioni.

Tra gli operatori le aspettative sono ampie al punto da aver indotto a un'accelerazione nello **sviluppo e rilascio di software** basati o integrati su modelli IA, come ad esempio Microsoft, con **Azure**, o Alphabet (già Google) con **Bard Chatbot** o lo studio legale Allen&Overy con **Harvey**. C'è poi anche chi caldeggia prudenza, come il guru informatico Steve Wozniak cofondatore di Apple durante una recente intervista alla Cnbc.

Il dibattito sul piano giuridico e istituzionale, che a dire il vero ha origini ben più risalenti sull'IA, involge varie tematiche facendo emergere **vari profili di rischio**. Si pensi al fronte dei **diritti degli autori** da cui ChatGpt attinge per generare output, alle responsabilità di questi e degli sviluppatori e, non da ultimo, della **protezione dei dati personali**. Insomma, come spesso accade in occasione dell'avvento di nuove tecnologie (si ricordi quanto accaduto con i sistemi basati su Dlt e blockchain), il relativo entusiasmo sulle potenzialità è affiancato dall'**incertezza su conseguenze e rischi per i soggetti coinvolti dalla nuova tecnologia** (come fruitori, sviluppatori, editori dei contenuti). ChatGpt non fa eccezione. Questo nuovo fenomeno digitale offre lo spunto per condividere alcune riflessioni in merito ai rischi per la privacy degli utenti, tenuto conto delle stringenti norme europee in materia, primo fra tutti il Regolamento generale sulla protezione dei dati o Gdpr.

I rischi per la privacy degli utenti

Poiché le condizioni d'uso, l'informativa agli utenti e le varie policy di ChatGpt risultano fruibili interagendo con il medesimo software, ai fini della nostra indagine abbiamo anzitutto **chiesto** a questo strumento digitale **cosa ne pensasse dei rischi privacy** connessi al suo utilizzo. Sorprendentemente la **risposta** generata dal software delinea una **certa "consapevolezza"** specie in merito al fatto che il sistema su cui si basa può conservare la trascrizione dei dati scambiati con gli utenti, al fine dell'autoapprendimento tipico dei modelli IA e che consente di potenziarne le performance. Ma non è questo l'unico scopo, infatti, ChatGpt prosegue specificando come le **chat incamerate potrebbero essere utilizzate anche per altri scopi, senza il consenso dell'utente**.

Emerge dunque che i **dati personali degli utenti potrebbero essere elaborati in modi che sfuggono** alla visibilità e al controllo degli stessi utenti. Ma se è chiaro che tali dati saranno "dati in pasto" all'IA al fine di migliorarla e svilupparla, è altrettanto chiaro che il loro utilizzo potrebbe non essere limitato a questo scopo.

Il software, tuttavia, non si spinge oltre nelle spiegazioni alimentando i nostri dubbi.

Al fine di avere una visione più chiara del percorso che i nostri dati intraprendono, consultiamo la **privacy policy** presente sul sito di OpenAI, la quale, in ossequio all'art. 13 del Gdpr, dovrebbe fornirci tutti i chiarimenti del caso. Ma ciò non è. Come anche segnalato dal Garante per la protezione dei dati personali, la privacy policy non è, in realtà, di grande aiuto. Il Garante ha infatti sottolineato come "neppure a leggere la stringata informativa sulla privacy messa a disposizione degli utenti, [si è in grado di comprendere] cosa i "padroni" del robot facciano dei dati personali, talvolta personalissimi, particolari secondo le previsioni del Gdpr, raccolti".

Le non rassicuranti osservazioni del Garante confermano le perplessità sui rischi legati alla privacy che si annidano nell'opacità del modello di gestione dei dati. Se si considera che le chat tra utenti e intelligenza artificiale possono riguardare qualsiasi aspetto della vita privata di un individuo, non si può sottovalutare l'enorme mole e la vastissima natura dei dati personali che potrebbero essere archiviati da OpenAI. La creazione di archivi così ampi potrebbe attirare l'attenzione di malintenzionati che puntano a sfruttare le informazioni personali per scopi deprecabili, come attacchi di phishing o ingegneria sociale.

Curiosamente ChatGpt appare del tutto "**consapevole**" anche quando interpellato su questo specifico aspetto del **potenziale uso improprio dei dati personali**.


Leggi anche

ChatGPT creerà un nuovo monopolio nell'intelligenza artificiale?

I rischi di un trasferimento di dati personali verso gli Usa

Un ulteriore aspetto che viene in rilievo è **l'uscita dei dati personali degli utenti dai confini europei**, i quali intraprendono un rischioso viaggio con destinazione gli Stati Uniti. OpenAI Llc, è, infatti, una società statunitense.

La Corte di Giustizia europea, con la **sentenza denominata "Schrems II"**, ha infatti sancito l'invalidità dell'accordo Usa-Eu sulla protezione dei dati personali, il cosiddetto "**Privacy shield**". Questa decisione è stata presa per motivi principalmente connessi agli ingentissimi poteri di accesso ai dati personali di cui godono taluni apparati dello stato americano, come la National security agency, per finalità di sicurezza nazionale e antiterrorismo. Nell'ottica europea questi poteri sono sproporzionati rispetto alle finalità perseguite e non permettono una reale tutela del dato rispetto alla possibilità che lo stato possa visionarlo, acquisirlo ed elaborarlo. Per questi motivi, ad oggi, trasferire lecitamente i dati personali dall'Europa agli Stati Uniti è particolarmente complicato e richiede l'attuazione di imponenti misure sia dal punto di vista legale che in materia di misure di sicurezza, tecniche e organizzative, per la protezione dei dati.

Europa e Stati Uniti stanno **trattando per conseguire un nuovo accordo**, tuttavia il Parlamento europeo ha recentemente espresso un parere negativo sulla bozza del medesimo pubblicata dalla Commissione europea il 13 dicembre 2022, lasciando intendere che la soluzione al problema qui descritto non sarà raggiunta a breve.

Conclusioni

Questa breve analisi pone l'accento su alcuni rischi particolarmente rilevanti per la riservatezza delle nostre informazioni, la cui conoscenza permetterebbe agli utenti di approcciarsi a ChatGpt in maniera più accorta e consapevole, calibrando cosa condividere con l'IA e cosa, invece, sarebbe meglio tenere lontano da occhi indiscreti.

In tale prospettiva sono da condividere le dichiarazioni del Garante laddove ha specificato come i rischi per la privacy degli utenti non devono spaventare, né limitare l'entusiasmo verso il progresso e lo sviluppo di tecnologie affascinanti come ChatGpt.

Il **Garante** ha, tra l'altro, affermato: "Per carità, nessun terrorismo psicologico e nessun invito a smettere di sperimentare, solo non lasciamoci prendere troppo la mano e non dimentichiamoci che, al di là del fatto che conosce il linguaggio umano, ChatGpt non è una persona in carne e ossa e, soprattutto, non è un nostro amico ma un prodotto commerciale realizzato da soggetti che, nella vita, in maniera del tutto legittima, fanno gli imprenditori".

Ebbene, ChatGpt sta canalizzando l'interesse dell'opinione pubblica su scala globale confermando la centralità delle questioni connesse alla protezione dei dati personali e al contempo il fortissimo legame che essa ha con lo sviluppo e l'affermazione delle nuove tecnologie. Insomma, le due facce della stessa medaglia che caratterizzano lo sviluppo su scala mondiale di un modello basato su IA. Questo è un pattern ricorrente, tanto che possiamo osservarlo in presenza di ogni altro analogo fenomeno globale digitale (tra tutti Meta/Facebook).

In definitiva, ChatGpt conferma l'importanza per gli utenti di **"maneggiare con cura"** software del genere e la necessità, per tutti gli altri soggetti a vario titolo interessati - quali le software house, gli sviluppatori, gli editori dei contenuti, i professionisti, le istituzioni etc. - di valutare attentamente eventuali impatti legali anche alla luce delle tutele poste dal Gdpr a presidio dei fruitori.

(Articolo scritto in collaborazione con Adriano Garofalo, studio legale De Berti Jacchia Franchini Forlani)

Leggi anche

Oltre Chat GPT: i titoli per investire sull'intelligenza artificiale

Alessandro Foti, Adriano Garofalo

Opinione personale dell'autore

Avvocato tributarista senior presso lo studio De Berti-Jacchia in Milano, si occupa della materia sia in ambito nazionale sia internazionale con particolare attenzione a Hnwi e multinazionali altamente digitalizzate, quali quelle operanti nei settori big data, Ai, cloud, cybersecurity, IoT, blockchain.

La redazione vi consiglia altri articoli

SU FINTECH

- La Cina è la terra dell'innovazione
- Fintech, anche nel 2019 una corsa senza freni
- Intelligenza artificiale: un mercato senza crisi

SU DIGITAL TRANSFORMATION & TECH

- Fintech, a segno il miglior anno di sempre
- IoT: il mercato italiano rallenta ma resiste alla pandemia
- Cashback Natale, rimborsi per 222 milioni: le regole da gennaio

Cosa vorresti fare?

Ascoltare | *Leggere* | *Guardare*

Apprendere

Cercare un consulente

Scoprire i Talents

Seguire i Brands

Pleasure Assets

Millennials

We Wealth
Chi siamo
Contatti
FAQ

Top Pagina
Home
news
voices
podcasts
Cerca un consulente
Scopri i Talents
Segui i Brands

Categorie
Investimenti
Consulenza patrimoniale
Filantropia
SRI-impact investing
Pleasure asset
Fintech
Aziende & protagonisti
Secret places
Agorà

Live broadcast
Weekly Bell
Chiedilo ai Talents
We Wealth Must

Domanda
Iscriviti alla newsletter
Abbonati al mensile
Privacy investitori
Privacy professionisti
T&C investitori
T&C professionisti

Partner di:

TORNA SU