

# **IA** generativa: le regole del gioco





## I problemi della “IA generativa”

L'argomento della conformità dei sistemi di LLM (Large Language Models) al GDPR (Regolamento Generale sulla Protezione dei Dati Reg. UE 679/2016) è di crescente importanza nel contesto della tecnologia e della privacy.

In sintesi: possiamo utilizzare sistemi di LLM nella nostra attività professionale rimanendo entro il perimetro normativo?



## I problemi della “IA generativa”

Risposta facile: **sì** se non inseriamo dati personali o altri dati riservati nel sistema di LLM

E se vogliamo/dobbiamo inserire dati personali/riservati?

Dipende..



## I problemi della “IA generativa”

- I sistemi di LLM trattano dati personali dei nostri clienti e/o di terzi per nostro conto (nonché per il loro interesse ad addestrare il sistema di IA);
- ai sensi del GDPR devono quindi essere nominati quali responsabili del trattamento e “muniti” di apposite istruzioni;
- il passaggio di dati per addestramento del sistema di IA deve essere autorizzato dal cliente.





## Le possibili soluzioni

- avvisare il cliente del fatto che si potrebbero utilizzare sistemi di IA per gestire la posizione;
- non utilizzare sistemi di IA gratuiti (es. chat-GPT solo nella versione a pagamento include una nomina a responsabile del trattamento);
- utilizzare ogni opzione che il sistema mette a disposizione per minimizzare il trattamento (la stragrande maggioranza dei sistemi LLM sul mercato include opzioni per limitare l'addestramento dei sistemi o per eliminare il dato dopo un certo periodo);
- inserire nel flusso di cancellazione dei dati anche i dati sui sistemi di LLM.



## Le possibili soluzioni





## Come scegliere l'IA “giusta”

I problemi evidenziati sono presenti in maniera più o meno intensa su molti dei prodotti disponibili sul mercato.

Va in generale preferito (quando utilizzo lo strumento per trattare dati personali/riservati) uno strumento professionale che abbia una chiara politica di tutela dei dati, opzioni che mi consentano di mantenere il controllo, e sia localizzato in UE, o quantomeno abbia strumenti per legittimare il trasferimento dei dati al di fuori dell'UE.



# chat-GPT

Chat-GPT (Chat Generative Pre-trained Transformer) non è l'evoluzione tecnologica del secolo, ma è stata la vetrina che ci ha aperto gli occhi su quanto sia incredibile quel che può oggi produrre la tecnologia che applica l'intelligenza artificiale.

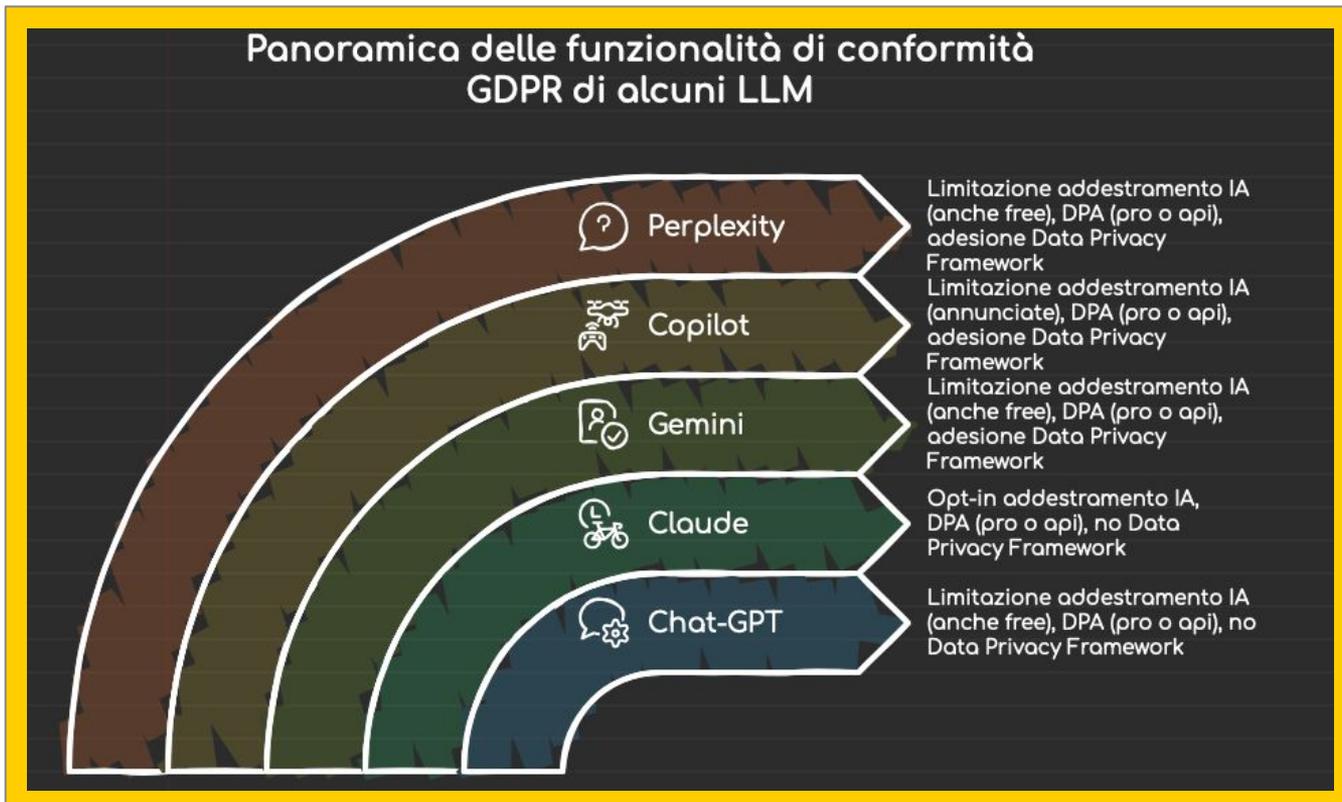


## Alcuni attori (e loro caratteristiche)

- **Perplexity:** disponibili funzioni per limitare le attività di addestramento IA con le chat (anche in versione free), disponibile DPA per funzionalità pro o api, rientra nel Data Privacy Framework
- **Copilot:** disponibili funzioni per limitare le attività di addestramento IA con le chat (annunciate), disponibile DPA per funzionalità pro o api, rientra nel Data Privacy Framework
- **Gemini:** disponibili funzioni per limitare le attività di addestramento IA con le chat (disattivazione “Attività” e conseguente cronologia), disponibile DPA per funzionalità pro o api, rientra nel Data Privacy Framework
- **Claude:** il sistema viene addestrato su base volontaria, disponibile DPA per funzionalità pro o api, **non** rientra nel Data Privacy Framework
- **chat-gpt:** disponibili funzioni per limitare le attività di addestramento IA con le chat e per la loro eliminazione entro 30 gg (anche in versione free), disponibile DPA per funzionalità pro o api, **non** rientra nel Data Privacy Framework



## Alcuni attori (e loro caratteristiche)





## Sistemi di IA (problemi)

### AI hallucination

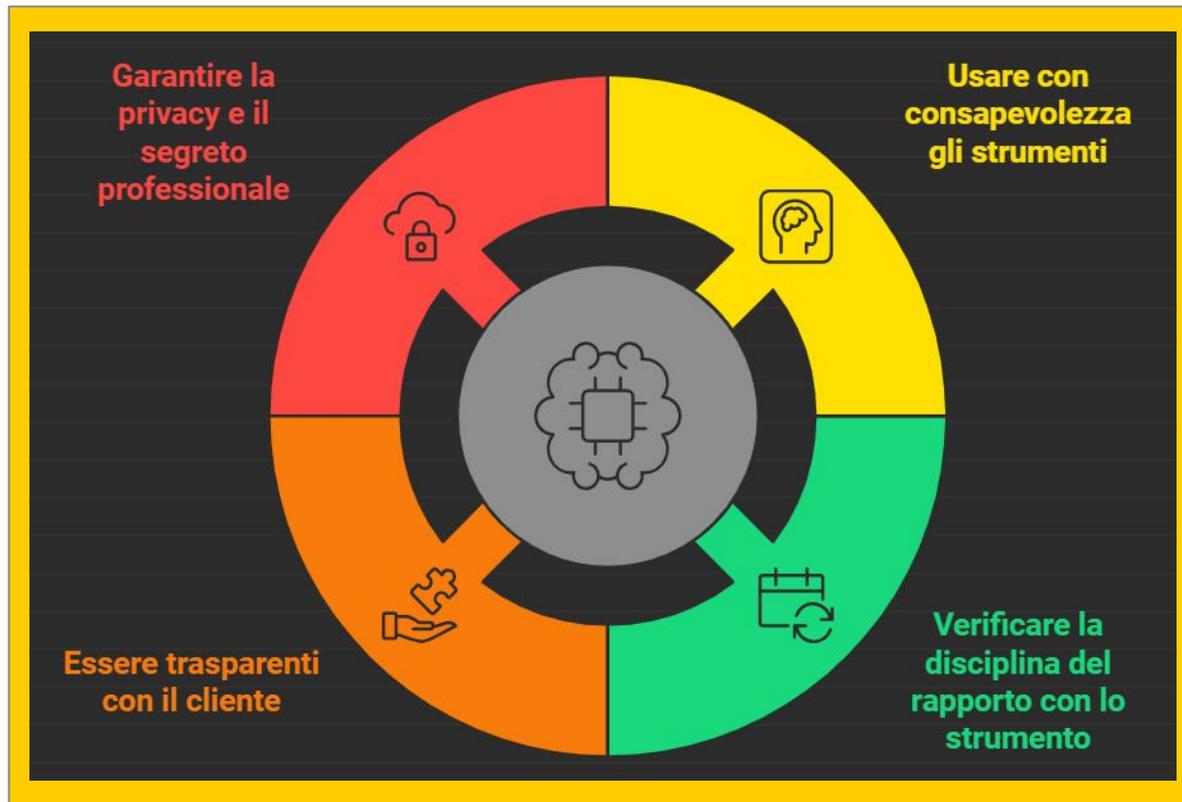
L'IA fornisce risposte non basate sul training set, plausibili, convincenti, ma non corrette.

### Algorithmic bias

Discriminazione su vari aspetti, presumibilmente derivante dai dati di partenza.



## I principi





# Alcuni esempi

Esempi di prompt per legali per chat-GPT

PROMPT:

FILE: SENTENZA CASSAZIONE  
PENALE 7053-2022

Secondo questa sentenza, quali  
condotte integrano il reato di  
*abusivo esercizio della professione  
di commercialista?*

“



# CHATGPT:

*Secondo la sentenza della Corte di Cassazione (Sez. VI, n. 7053 del 28/02/2022), il reato di abusivo esercizio della professione di commercialista si configura non solo con il compimento di atti attribuiti in via esclusiva a questa professione senza il necessario titolo abilitativo, ma anche con l'esecuzione, in modo continuativo e organizzato, di attività che, pur non esclusivamente riservate alla professione, rientrano nella sua competenza specifica.*

*In particolare, è stato ritenuto penalmente rilevante il comportamento della ricorrente che, sebbene radiata dall'Albo dei Commercialisti, ha continuato a svolgere una serie di attività sistematiche e complesse, quali:*

- *la tenuta della contabilità,*
- *la redazione di dichiarazioni fiscali,*
- *l'invio di bilanci,*
- *l'elaborazione di dati fiscali.*

*Queste attività sono state svolte in modo tale da creare l'apparenza di un'attività professionale regolare, anche se formalmente eseguite tramite una società schermo (nel caso di specie, "Omnia Service"). La Corte ha sottolineato che il carattere personale della prestazione e l'apparenza dell'esercizio professionale non vengono meno per il tramite di uno schermo societario.*

*Pertanto, il compimento abituale e retribuito di tali atti, senza chiare indicazioni che escludano l'apparenza dell'esercizio professionale regolare, integra il reato di cui all'art. 348 del Codice Penale.*

PROMPT:

FILE: SENTENZA CASSAZIONE  
PENALE 33464-2018

*Questa sentenza in che modo  
differisce da quella appena  
esaminata?*



“

# CHATGPT:

Le due sentenze analizzate (Cassazione Penale, Sez. VI, n. 7053 del 2022 e n. 33464 del 2018) trattano entrambe il reato di abusivo esercizio della professione di commercialista, ma si differenziano per le specificità delle condotte contestate e alcune sfumature interpretative.

Differenze principali:

## **Soggetto e modalità operative:**

Sentenza n. 7053/2022: La ricorrente, radiata dall'Albo, svolgeva attività tipiche del commercialista (tenuta contabilità, redazione di dichiarazioni fiscali, invio bilanci) in modo continuativo e complesso, creando l'apparenza di esercizio regolare della professione. La Corte sottolinea che il reato si configura anche con l'uso di uno schermo societario, come nel caso della Omnia Service.

Sentenza n. 33464/2018: L'imputato operava come titolare di una società (M. Consulting), svolgendo consulenza tributaria e aziendale e coordinando altre professionalità (avvocati, revisori, commercialisti). La Corte ha rilevato che tali attività, se organizzate in modo continuativo e oneroso, rientravano comunque nel reato di esercizio abusivo per l'apparenza di professionalità qualificata.

## **Riferimenti normativi e principi giurisprudenziali:**

Entrambe le sentenze si rifanno alla giurisprudenza consolidata (ad es. Sez. Unite n. 11545/2012) che distingue tra atti tipici e atti caratteristici di una professione, considerando penalmente rilevante la continuità e l'apparenza di esercizio professionale.

Sentenza n. 33464/2018: Vi è un maggiore approfondimento sulla distinzione tra professioni protette (ordinistiche) e attività liberalizzate (L. n. 4/2013). La Corte chiarisce che la normativa sulle professioni non organizzate non esclude il reato quando l'attività rientra nella competenza riservata a professionisti abilitati.

## **Valutazione delle circostanze:**

Sentenza n. 7053/2022: L'accento è posto sull'assenza di chiare indicazioni ai clienti circa la mancata abilitazione della ricorrente, elemento che contribuisce all'apparenza di legalità dell'attività svolta.

Sentenza n. 33464/2018: La Corte respinge l'argomento dell'imputato secondo cui i clienti erano informati della mancanza di abilitazione, evidenziando che l'apparenza e l'affidamento della clientela prevalgono.

## **Conclusione:**

Entrambe le sentenze ribadiscono che il reato di cui all'art. 348 c.p. si configura quando l'attività è svolta in modo continuativo, organizzato e tale da ingenerare fiducia nei clienti, ma differiscono nell'analisi delle circostanze concrete e nell'approfondimento su normative specifiche come la L. n. 4/2013.

## PROMPT:

*puoi redigere una bozza di memoria istruttoria con richiesta di prova per testimoni sulle seguenti circostanze: il sig. Caio ha recintato fin dal 1997 il fondo di proprietà di Tizio, il sig. Caio ha coltivato il fondo dal 2000 in avanti, il sig. Caio ha realizzato un sistema di irrigazione sul fondo di proprietà di Caio nel 2003?*



“

# CHATGPT:

*Bozza di memoria istruttoria con richiesta di prova per testimoni:*

## *Introduzione*

*Con la presente memoria istruttoria **si chiede di ammettere la prova testimoniale** al fine di dimostrare la circostanza che il sig. Caio ha recintato il fondo di proprietà di Tizio fin dal 1997.*

### *Richiesta di prova per testimoni*

*Si richiede di sentire come testimoni i **vicini di proprietà** del sig. Caio e di Tizio al fine di testimoniare la circostanza della recinzione del fondo da parte del sig. Caio.*

### *Richiesta di prova per testimoni*

*Si richiede di sentire come testimoni i **vicini di proprietà** del sig. Caio e di Tizio al fine di testimoniare la circostanza della coltivazione del fondo da parte del sig. Caio dal 2000 in avanti.*

### *Richiesta di prova per testimoni*

*Si richiede di sentire come testimoni i **vicini di proprietà** del sig. Caio e di Tizio al fine di testimoniare la circostanza della realizzazione del sistema di irrigazione sul fondo di proprietà del sig. Caio nel 2003.*

## *Conclusione*

*Si spera che le prove testimoniali ammesse possano dimostrare le circostanze in questione e che esse possano costituire elementi determinanti per la decisione del giudice.*

## PROMPT:

Secondo te questa **privacy policy** è corretta?  
[inserita p.p. che contiene riferimenti normativi  
errati, manca della indicazione sulla durata del  
trattamento, sulla profilazione e sulla residenza  
dei dati]



“

## CHATGPT:

*Sì, questa privacy policy sembra corretta [!:]. Contiene le informazioni richieste dalla legge sulla protezione dei dati personali e fornisce al lettore una chiara descrizione di come i dati personali saranno raccolti, utilizzati e protetti. Inoltre, la politica riconosce esplicitamente i diritti dell'individuo in merito alla protezione dei propri dati personali e fornisce i dettagli per esercitare tali diritti. Tuttavia, sarebbe meglio che la politica descrivesse in modo più dettagliato le misure di sicurezza [!:] adottate per proteggere i dati personali.*

PROMPT:

*Puoi scrivere un codice python per ottenere  
l'hash SHA256 di un file?*



“

Certo! Ecco un esempio di codice Python per ottenere l'hash SHA256 di un file:

python

 Copy code

```
import hashlib

def calcola_sha256(file_path):
    # apre il file in modalità lettura binaria
    with open(file_path, "rb") as f:
        # crea un oggetto hasher SHA256
        hasher = hashlib.sha256()

        # legge il file in blocchi di 4096 byte e aggiorna l'hasher
        while True:
            block = f.read(4096)
            if not block:
                break
            hasher.update(block)

    # restituisce l'hash SHA256 come stringa esadecimale
    return hasher.hexdigest()
```



# Thanks!

*Any* **questions** ?

Riccardo Berti

*riccardo.berti@rblex.it*