

The background features a pattern of teal hexagons of various sizes and shades, some solid and some outlined. Grey lines of varying lengths and orientations are scattered across the background, creating a geometric, network-like aesthetic.

IA, diritto d'autore e uso responsabile dell'intelligenza artificiale



- Avvocato Cassazionista, Socio dello Studio Previt Associazione Professionale, Responsabile Dipartimento “Diritto della proprietà intellettuale, Diritto di internet e concorrenza sleale”- Cofounder SpTech
- Si occupa prevalentemente di diritto delle nuove tecnologie, proprietà intellettuale e diritto industriale, data protection, Artificial Intelligence, social media law, informatica giuridica, diritto delle comunicazioni, diritto civile e commerciale.
- Già Componente della Commissione Protezione dei dati personali del Consiglio Nazionale Forense.
- Co-founder Salotto Privacy, Direttore Esecutivo di Lex Digital e dell'Osservatorio Diritto di Internet, membro di IAIC Italian Academy of Internet Code e del Centro Studi Informatica Giuridica, è stato inoltre presidente del Circolo Giuristi Telematici. Socio del Centro Studi Privacy e Nuove tecnologie.



- * Avvocato cassazionista - Array.eu
- * Informatica Giuridica – UniPG
- * Centro d'Eccellenza Jean Monnet – BALDUS - UniPG
- * Module Leader - Jean Monnet - CIBER - UniPG
- * Master I liv. “Cybercrime e Digital Forensics” - UniPG
- * Consigliere dell’Ordine degli Avvocati di Cagliari
- * CINI - Cyber Security National Lab - UniPG
- * GdL della Fondazione Italiana per l'Innovazione Forense (FIIF) presso il CNF
- * Commissione CNF per la valutazione degli avvocati specialisti in “Diritto dell'informazione, della comunicazione digitale e della protezione dei dati personali”

some of typical features of artificial intelligence systems

80px



Analysis of vast amounts of data



Speed in analysis and task execution



Machine Learning



Adaptability to unforeseen situations



Identifying correlations



Scale up operations (defensive / offensive purposes) by parallelising it

60px

AI e hype

E' fondamentale comprendere le limitazioni dei LNLM (Large Neural Language Models) o dei **Foundation Models** e contestualizzare il loro successo:

- **Non comprendono il significato del prompt**
- **Non comprendono il significato dell'output**
- **I risultati vengono generati sulla base di calcoli statistici**
- **Non individuano causalità ma, eventualmente, correlazioni spurie**

Artificial intelligence was asked to make a picture of Mother Teresa fighting against poverty.

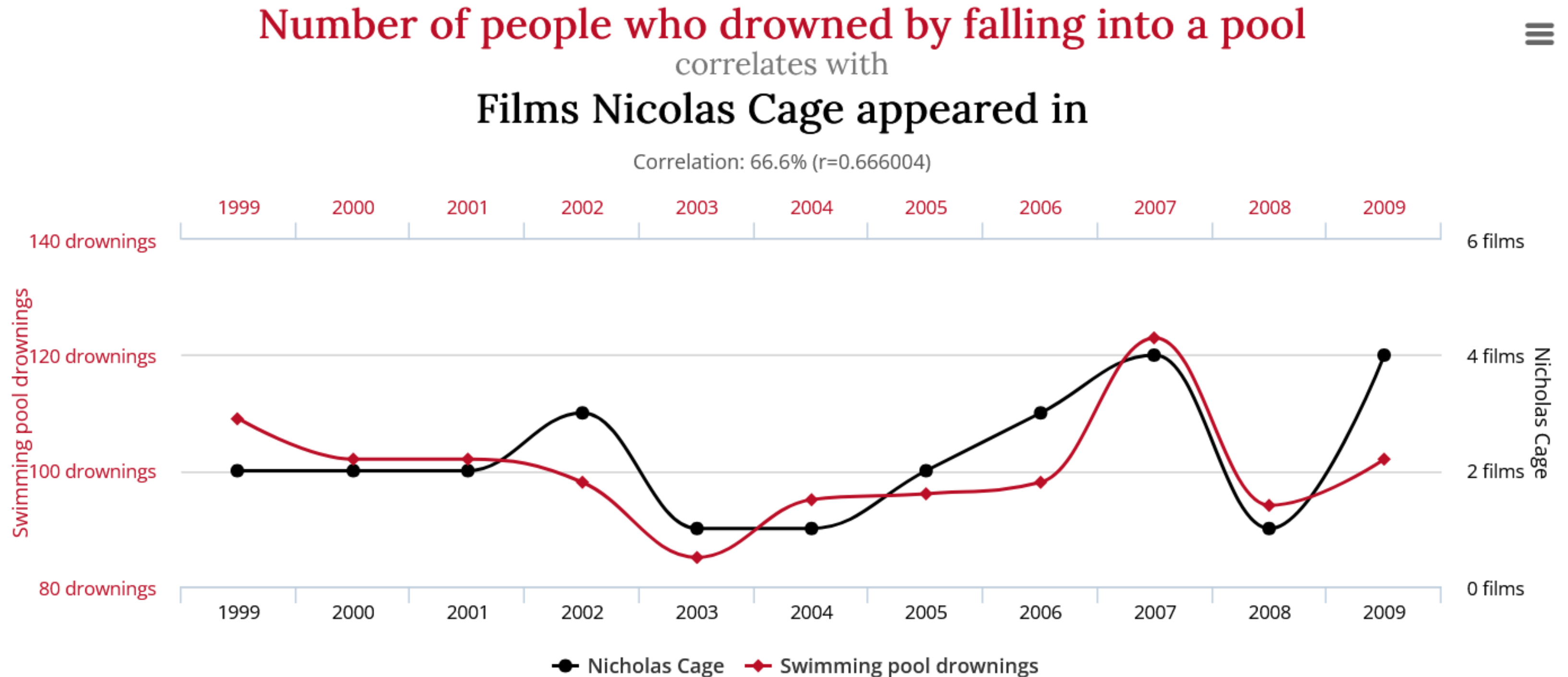




HOW TO CONFUSE MACHINE LEARNING



Causalità e correlazione

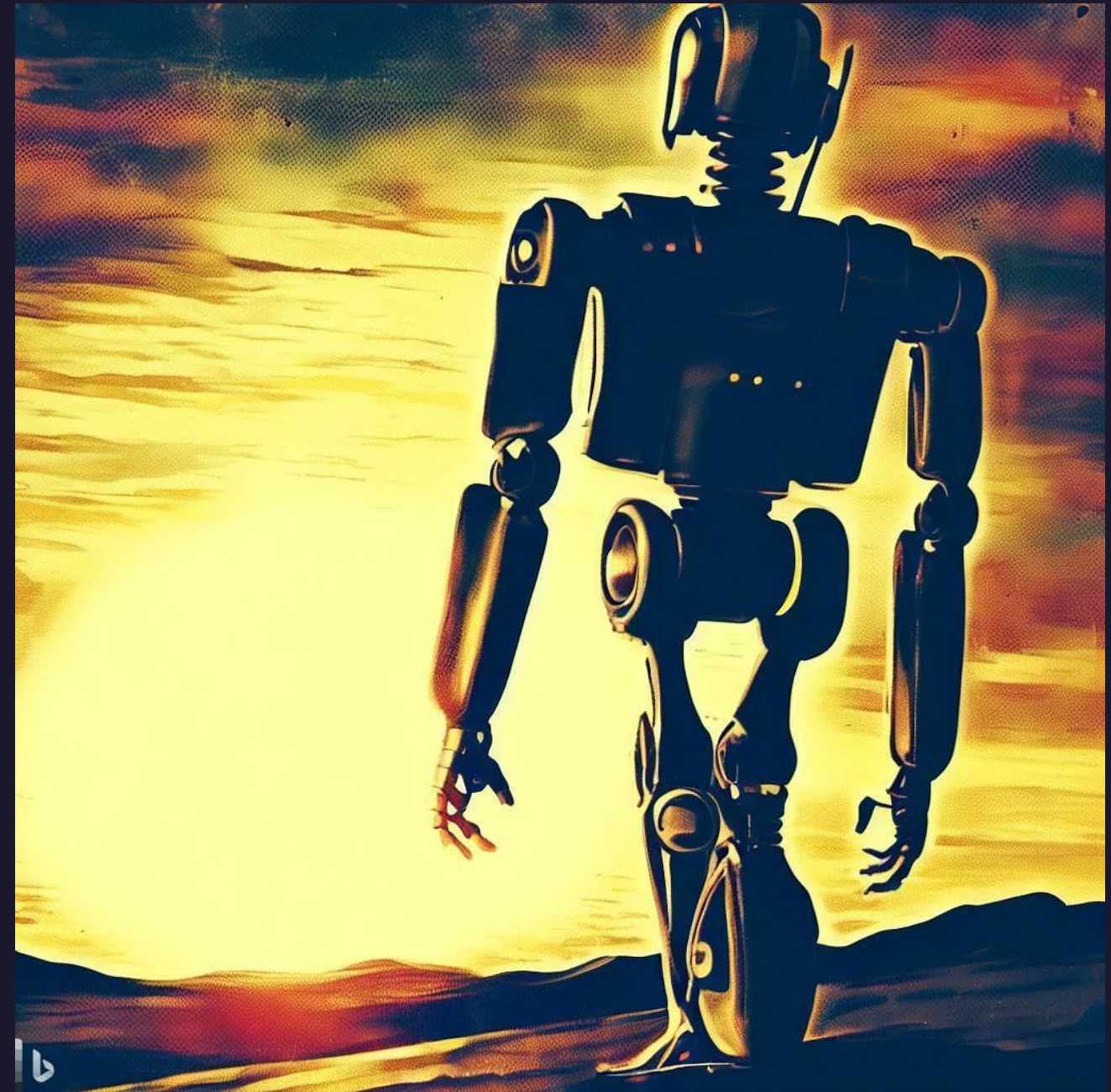


Data sources: Centers for Disease Control & Prevention and Internet Movie Database

tylervigen.com

AI e hype e la singolarità tecnologica

La cosiddetta **Intelligenza Artificiale Generale** (AGI – Artificial General Intelligence o «strong AI») ossia la AI cosciente di sé ed in grado di emulare (se non superare) le capacità cognitive ed intellettuali di esseri umani o altri animali è, ancora, **fantascienza**.



Pappagalli stocastici



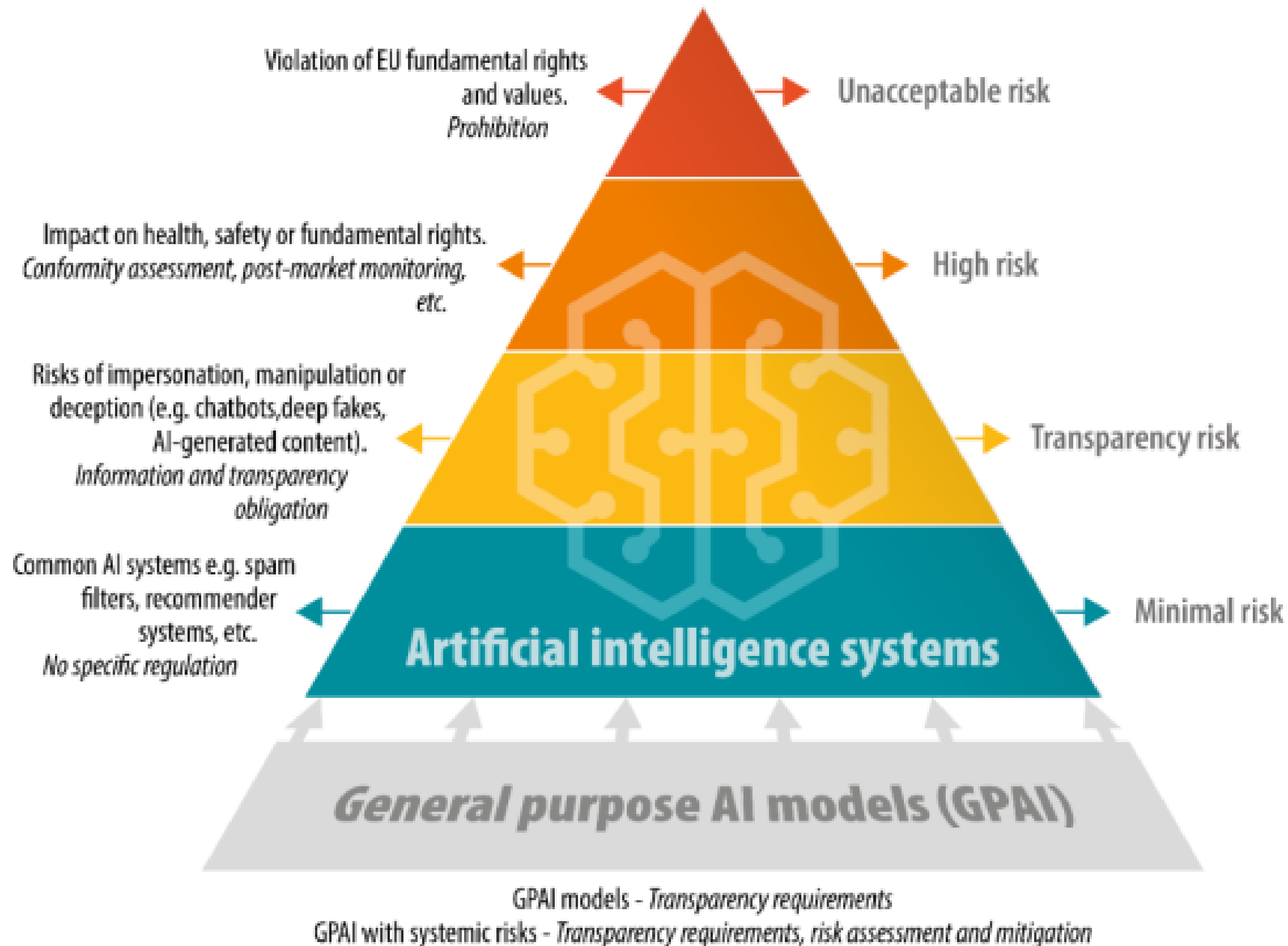
Un LM è un sistema che mischia, seguendo regole probabilistiche di combinazione del testo (senza alcun riferimento al significato), sequenze di parole e frasi che ha avuto modo di osservare all'interno della vasta mole di dati impiegati per il suo addestramento: è, a tutti gli effetti, un «pappagallo stocastico»

an LM is a system for haphazardly stitching together sequences of linguistic forms it has observed in its vast training data, according to probabilistic information about how they combine, but without any reference to meaning: a stochastic parrot (On the Dangers of Stochastic Parrots: Can Language Models Be Too Big? <https://dl.acm.org/doi/10.1145/3442188.3445922> Bender e altri)

AI Act e sistemi destinati all'amministrazione della giustizia

sistemi di IA destinati all'**amministrazione della giustizia** e ai processi democratici dovrebbero essere classificati come **sistemi ad alto rischio**, in considerazione del loro impatto potenzialmente significativo sulla democrazia, sullo Stato di diritto, sulle libertà individuali e sul diritto a un ricorso effettivo e a un giudice imparziale (cons. 61)

Risk based approach



L'utilizzo di sistemi di intelligenza artificiale nelle professioni intellettuali è finalizzato al solo esercizio delle **attività strumentali e di supporto** all'attività professionale e con prevalenza del lavoro intellettuale oggetto della prestazione d'opera

Nei casi di impiego dei sistemi di intelligenza artificiale nell'attività giudiziaria è sempre **riservata al magistrato ogni decisione** sull'interpretazione e sull'applicazione della legge, sulla valutazione dei fatti e delle prove e sull'adozione dei provvedimenti.

IA E DDA

Francesco Paolo Micozzi

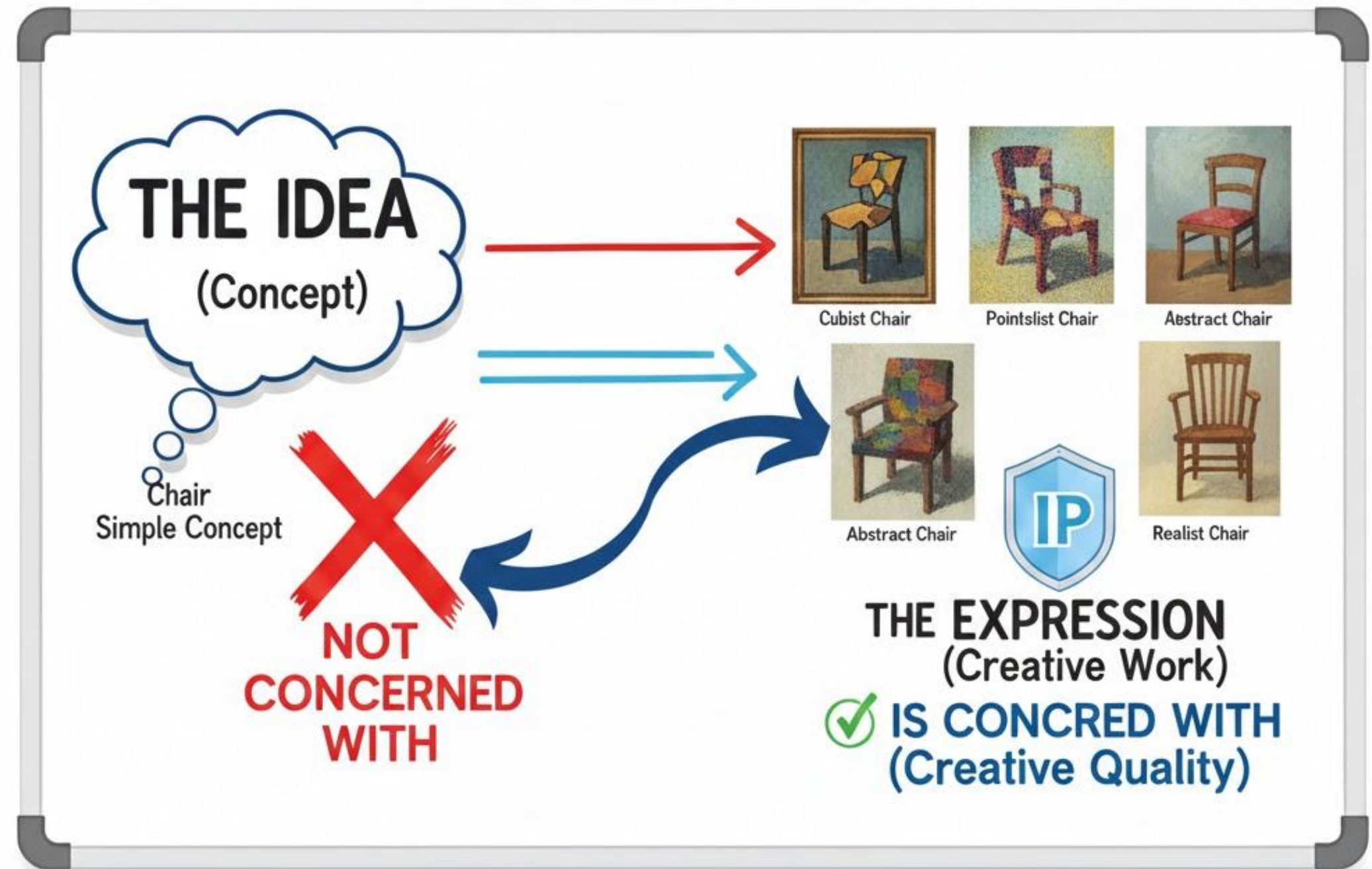
Profili problematici su DDA e IA

- 1 Posso addestrare un LLM con opere tutelate dal DDA?**
- 2 Se creo delle opere per mezzo dell'IA, chi è il titolare del DDA? La IA? Io? Altri?**
- 3 L'IA può violare il DDA attraverso i suoi output?**
- 4 ...e cosa succede se l'IA imita lo “stile” di un autore?**

Premessa 1: processo creativo e opera protetta

Il diritto della proprietà intellettuale non si occupa del processo creativo in quanto tale (l'**idea**), bensì della qualità (creativa) dell'opera che ne costituisce il risultato (l'**espressione** dell'idea creativa).

Tradizionalmente, secondo la teoria giuridica italiana, un'opera è considerata creativa se è sufficientemente originale e nuova. In modo schematico, si potrebbe dunque affermare: "carattere creativo = originalità + novità".



Premessa 2: Differenze tra Copyright e Diritto d'autore

“Copyright” e “diritto d'autore” sono termini che si riferiscono alla tutela giuridica delle opere creative, ma con origini e impostazioni leggermente diverse: il “**diritto d'autore**” (tipico dei Paesi di Civil Law) tutela l'autore e la sua creazione dal momento stesso in cui l'opera viene ad esistenza, includendo diritti morali perpetui (paternità, integrità) e diritti patrimoniali; il **Copyright** (tipico dei Paesi di Common Law, come gli Stati Uniti e il Regno Unito) si concentra maggiormente sul “diritto di copia” e sul valore economico, sorgendo tradizionalmente con la pubblicazione e la registrazione. Tuttavia, entrambi i sistemi proteggono le opere (letterarie, artistiche, musicali, software) per un lungo periodo di tempo.

Premessa 3: Uso di opere protette

In base alla regola generale non si può usare l'opera altrui senza permesso, **a meno che**

- Rientri in una specifica eccezione prevista per legge,
- non vi sia una licenza da parte del titolare dei diritti

Posso addestrare un LLM con opere tutelate dal DDA?

Ci sono diversi modi in base ai quali un Sistema di IA può essere addestrato con opere protette dal diritto d'autore:

- Sfruttando l'eccezione del **Text and Data Mining (TDM)**
- Attraverso una licenza

Posso addestrare un LLM con opere tutelate dal DDA?

L'eccezione **Text and Data Mining (TDM)** della Direttiva Copyright (art. 4, [Directive 2019/790/EU](#) – artt. 70-ter e 70-quater, L. 633/1941) consente l'uso di opere legittimamente accessibili per l'addestramento dell'IA.

Ciò significa che, **di default, le società che producono IA possono fare “scraping” sul web al fine di addestrare i loro modelli.**

Text and data mining (TDM): opt-out

Rightholders can “expressly reserve their rights” (opt-out).

If they do this using machine-readable means (like a `robots.txt` file or metadata), AI developers must exclude that content from their training sets.

```
User-agent: PetalBot
Disallow: /

User-agent: Yandex
Disallow: / # prohibits crawling for the entire site

User-agent: GPTBot
Disallow: /

User-agent: CCBot
Disallow: /

User-agent: anthropic-ai
Disallow: /
```

Text extracted from <https://www.corriere.it/robots.txt>



In addition to data obtained through **TDM processes**, the development, training, and use of AI datasets can also be achieved through **specific licences** granted by rights holders.

Many “open” licences (such as **Creative Commons**) already allow their use for training AI systems.

Home / News / The Walt Disney Company and OpenAI Reach Landmark Agreement to Bring Beloved Characters from Across Disney's Brands to Sora

The Walt Disney Company and OpenAI Reach Landmark Agreement to Bring Beloved Characters from Across Disney's Brands to Sora

BRAND | DECEMBER 11, 2025 | 6 MIN. READ

- As part of this three-year licensing agreement, Sora will be able to generate short, user-prompted social videos that can be viewed and shared by fans, drawing on more than 200

OpenAI Shutting Down Sora
Data Centers
A.I. Agents
White House Policy
Pentagon

OpenAI Is Shutting Down Sora, Its A.I. Video Generator

The start-up said it would discontinue Sora just three months after signing a multiyear deal to bring Disney characters to the service.

Francesco Paolo Micozzi

Titolarità, violazioni e stile nell'output generato da IA

Dopo la rivoluzione di internet, i due nuovi principali “stress test” del diritto d’autore imposti dall’AI generativa

La tutelabilità dell’opera d’ingegno generata con l’AI

L’utilizzo delle opere per l’addestramento dei sistemi di AI

La tutela delle opere generate da intelligenza artificiale

IA a supporto dell'essere umano nel processo creativo.

Per la tutela dell'opera d'ingegno occorrono 4 CRITERI DA SODDISFARE:

- **Ambito letterario, scientifico o artistico della creazione**
- **Intervento umano nel processo creativo dell'opera**
- **Originalità nella realizzazione dell'invenzione**
- **Espressione umana nella creazione finale**



Opere create dall'IA autonomamente

Nel caso di **apporto umano totalmente assente o molto limitato**: elaborazione frutto della capacità di *agency* dell'IA

Dalla lettura degli **artt. 2580 c.c., 23 LDA e art. 25 L. 132/2025**:

- tutela di tipo autoriale all'IA che crea un'opera **esclusa**;
- l'**autore** viene identificato in una persona fisica avente capacità giuridica



Due casi a confronto

U.S Copyright Office 21 FEBBRAIO 2023
«ZARYA OF THE DAWN»



Corte di Cassazione Italia, Ordinanza N°
1107 del 16 gennaio 2023

L'IA può essere considerata autrice di opere creative?

(CASSAZIONE ITALIANA vs USCO)

1

CORTE DI CASSAZIONE
Ordinanza N° 1107 del
16.1.2023

Ricorso volto a cassare una sentenza del Tribunale d'Appello di Genova che, secondo la rappresentazione della ricorrente (RAI), avrebbe classificato erroneamente come opera intellettuale un'immagine generata mediante l'ausilio di AI. **La Corte ha affermato la necessità di verificare se l'uso del *software* avesse assorbito la rielaborazione creativa dell'artista che lo aveva utilizzato e in quale misura.**

Occorre quindi indagare la misura dell'apporto creativo umano.

2

US COPYRIGHT OFFICE (U.S.
Copyright Office 21.2.2023

Si è pronunciato sulla questione della protezione dei diritti d'autore concessa a una *graphic novel* scritta da una persona fisica con immagini generate dal sistema di IA MidJourney. L'USCO ha stabilito che la protezione offerta dalla legislazione sul diritto d'autore deve certamente estendersi alla componente testuale, ma **escludersi per quanto riguarda le singole immagini, poiché queste non possono essere configurate come prodotto della creatività dell'autore.**

Un'indagine non nuova per la giurisprudenza sul diritto d'autore

Le scelte creative su cui indagare l'apporto umano possono verificarsi a vari livelli della creazione dell'opera mediante l'ausilio dell'AI, ed in particolare in 3 fasi:

- a) concezione/preparazione
- b) esecuzione
- c) finalizzazione

Tali criteri erano già stati individuati nella giurisprudenza dell'UE, per esempio, rispetto alla qualificazione di “opera fotografica” rispetto alle fotografie non tutelate.

*"Durante la **fase preparatoria** l'autore potrà scegliere lo sfondo, la messa in posa della persona da fotografare o l'illuminazione. Nel fotografare potrà scegliere l'inquadratura, l'angolo di ripresa o ancora l'atmosfera creata. Infine, al momento dello **sviluppo**, l'autore potrà scegliere tra diverse tecniche esistenti quella da adottare, o ancora pro cedere, eventualmente, all'impiego di programmi informatici".*

(Caso “**Painer**”, C-145/10, in curia.europa.eu.)

L'approccio adottato dalla Cassazione italiana non solo è il più elastico rispetto all'evoluzione tecnologica ma a ben vedere è anche quello che meglio valorizza l'impostazione “antropocentrica” dichiarata nell'AI Act e successivamente nella Legge 132/2025

Peraltro, una radicale esclusione della tutelabilità degli output dell'AI ai sensi del diritto d'autore danneggerebbe anche gli autori delle opere dell'ingegno eventualmente utilizzate per addestrare i sistemi di AI

➤ **Per essere “opere derivate” devono essere considerate opere dell'ingegno**

Il nuovo art. 1 LDA (post Legge n. 132/2025)

*“Sono protette ai sensi di questa legge le opere dell'ingegno umano di carattere creativo che appartengono alla letteratura, alla musica, alle arti figurative, all'architettura, al teatro ed alla cinematografia, qualunque ne sia il modo o la forma di espressione, **anche laddove create con l'ausilio di strumenti di intelligenza artificiale**, purché costituenti risultato del lavoro intellettuale dell'autore”.*

L'utilizzo delle opere
per l'addestramento dei
sistemi di AI

Le nuove sfide imposte dall'addestramento dei sistemi AI

DATA/WEB SCRAPING:

Raccolta di dati e diverse creazioni artistiche contenute in varie banche dati; Estrazione di immagini dal web; Addestramento di algoritmi per riconoscere schemi e relazioni a partire da immagini di origine al fine di generarne di nuove;

TEXT AND DATA MINING:

Estrazione e analisi automatizzate di dati digitali; generazione di informazioni; disponibilità e utilizzo delle informazioni per diversi scopi;

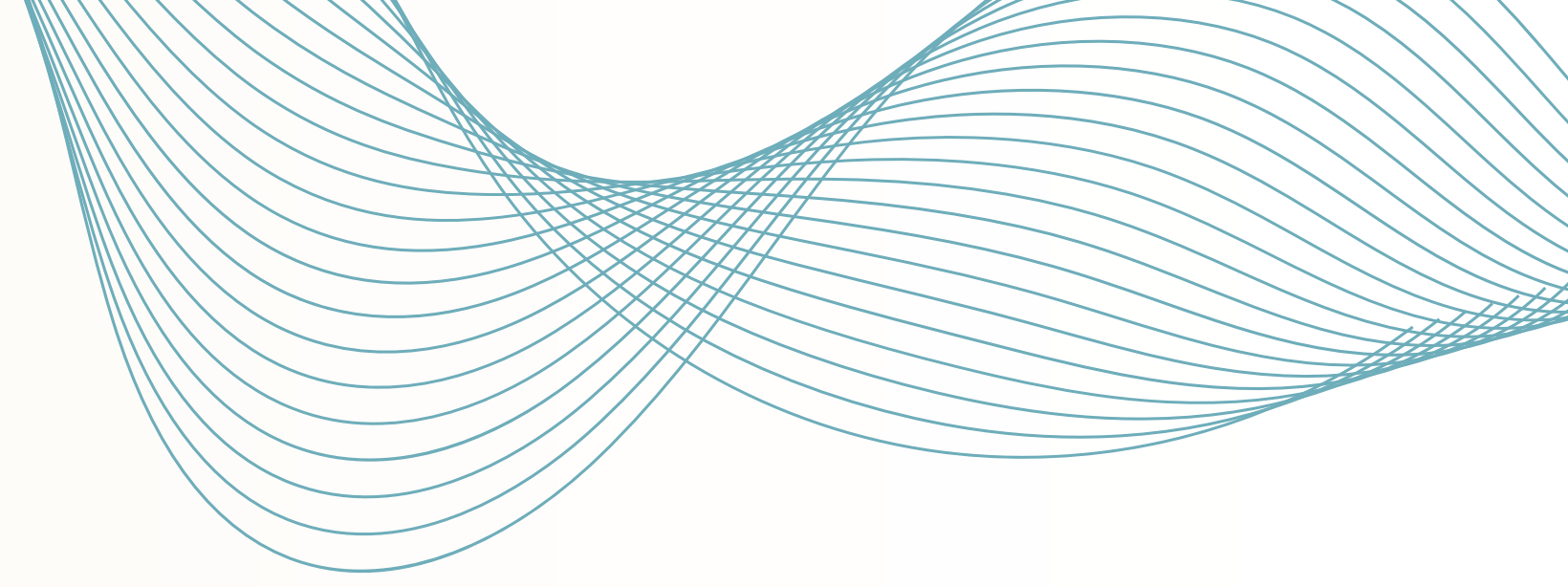
Art. 4 della Direttiva UE 2019/790

*Gli Stati membri pongono un'eccezione o una limitazione ai diritti di cui all'articolo 5, lettera a), e all'articolo 7, paragrafo 1, della direttiva 96/9/CE, all'articolo 2 della direttiva 2001/29/CE, all'articolo 4, paragrafo 1, lettere a) e b), della direttiva 2009/24/CE e all'articolo 15, paragrafo 1, della presente direttiva per le **riproduzioni e le estrazioni** effettuate da opere o altri materiali cui si abbia **legalmente accesso** ai fini dell'estrazione di testo e di dati.*

Le riproduzioni e le estrazioni effettuate a norma del paragrafo 1 possono essere conservate per il tempo necessario ai fini dell'estrazione di testo e di dati.

***L'eccezione o la limitazione** di cui al paragrafo 1 **si applica** a condizione che l'utilizzo delle opere e di altri materiali di cui a tale paragrafo **non sia stato espressamente riservato dai titolari dei diritti in modo appropriato, ad esempio** attraverso strumenti che consentano lettura automatizzata in caso di contenuti resi pubblicamente disponibili online.*

Il presente articolo non pregiudica l'applicazione dell'articolo 3 della presente direttiva.



Opt Out vs Opt In

Opt-out: il TDM è libero per default; il titolare può esprimere un rifiuto esplicito per impedire l'uso.
Modalità di riserva dei diritti: tramite indicazioni tecniche o termini d'uso chiari.

Opt-in (modello tradizionale): l'uso è consentito solo dopo autorizzazione preventiva.

➤ **L'art. 4 sposta la logica da “autorizzazione necessaria” a “libertà condizionata”, promuovendo innovazione e data analysis, ma garantendo la possibilità di controllo del titolare dei diritti**

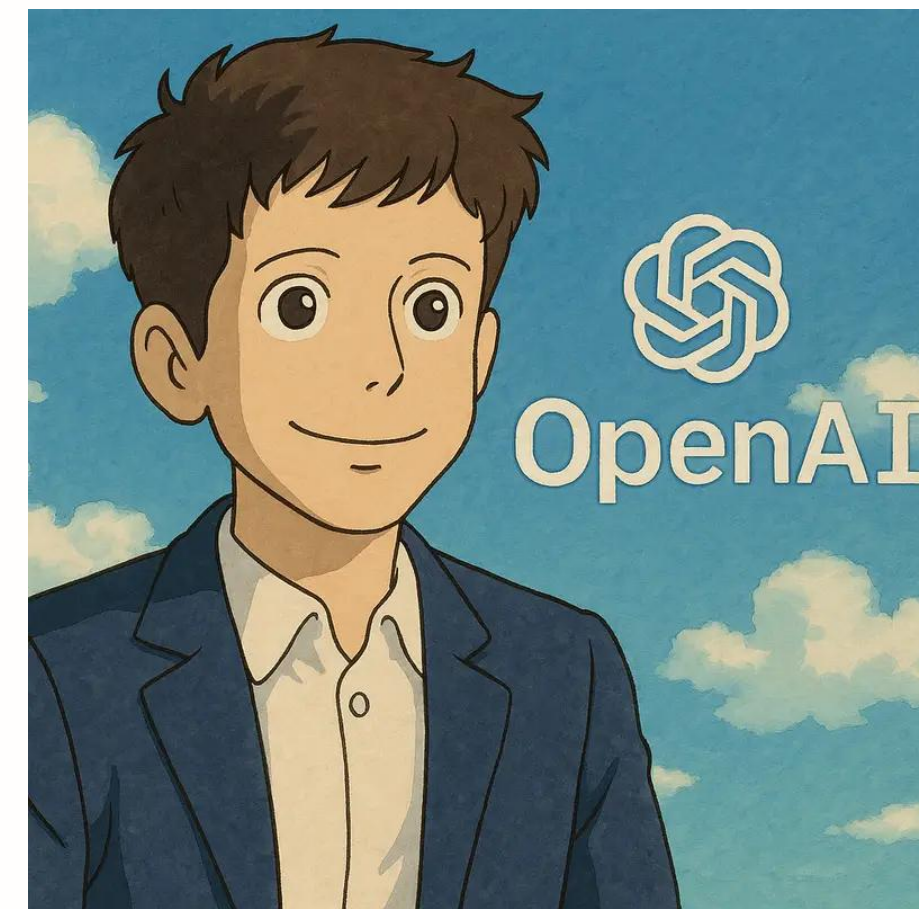
Il caso Ghibli ("Ghiblification")

Rispetto alle preoccupazioni sorte con il «caso Ghibli» occorre distinguere due diversi piani:

- In via generale, uno **stile grafico/estetico** non è tutelato dal diritto d'autore.

(Cass. civ., Ord. n. 11413/2024: «*La protezione del diritto d'autore postula il requisito dell'originalità e della creatività, consistente non già nell'idea che è alla base della sua realizzazione, ma nella forma della sua espressione, ovvero dalla sua soggettività*»)

- Diversa questione è quella dell'addestramento dei sistemi AI: per raggiungere un livello di fedeltà tanto elevato è plausibile che i sistemi si siano nutriti di **milioni di fotogrammi** contenuti nei film dello Studio, **senza il consenso dell'autore**



IL BANDO DELLA CE PER UNO STUDIO SUL RIESAME DELLA DIRETTIVA COPYRIGHT

Lo studio dovrà esaminare:

- il corretto funzionamento dell'eccezione per il **text and data mining (TDM)** (art. 3)
- miglioramento delle **pratiche di licenza** (artt. 8–13)
- i **diritti e le piattaforme online correlate** (artt. 15 e 17)
- la **remunerazione di autori e artisti** (capitolo 3)

Valutare se la Direttiva ha raggiunto i suoi obiettivi, in particolare:

- **facilitare l'uso digitale dei contenuti protetti** per l'istruzione, la ricerca e la conservazione
- **migliorare le pratiche di concessione delle licenze**, garantendo così un accesso più ampio ai contenuti
- l'impatto dell'introduzione dell'**art. 17 sulla concessione di licenze di contenuti protetti dal diritto d'autore da parte delle piattaforme di condivisione di contenuti online**, sulla remunerazione dei titolari dei diritti e sugli usi legittimi dei contenuti protetti dal diritto d'autore

La Commissione presenterà la **relazione finale** entro il **7 giugno 2026**.

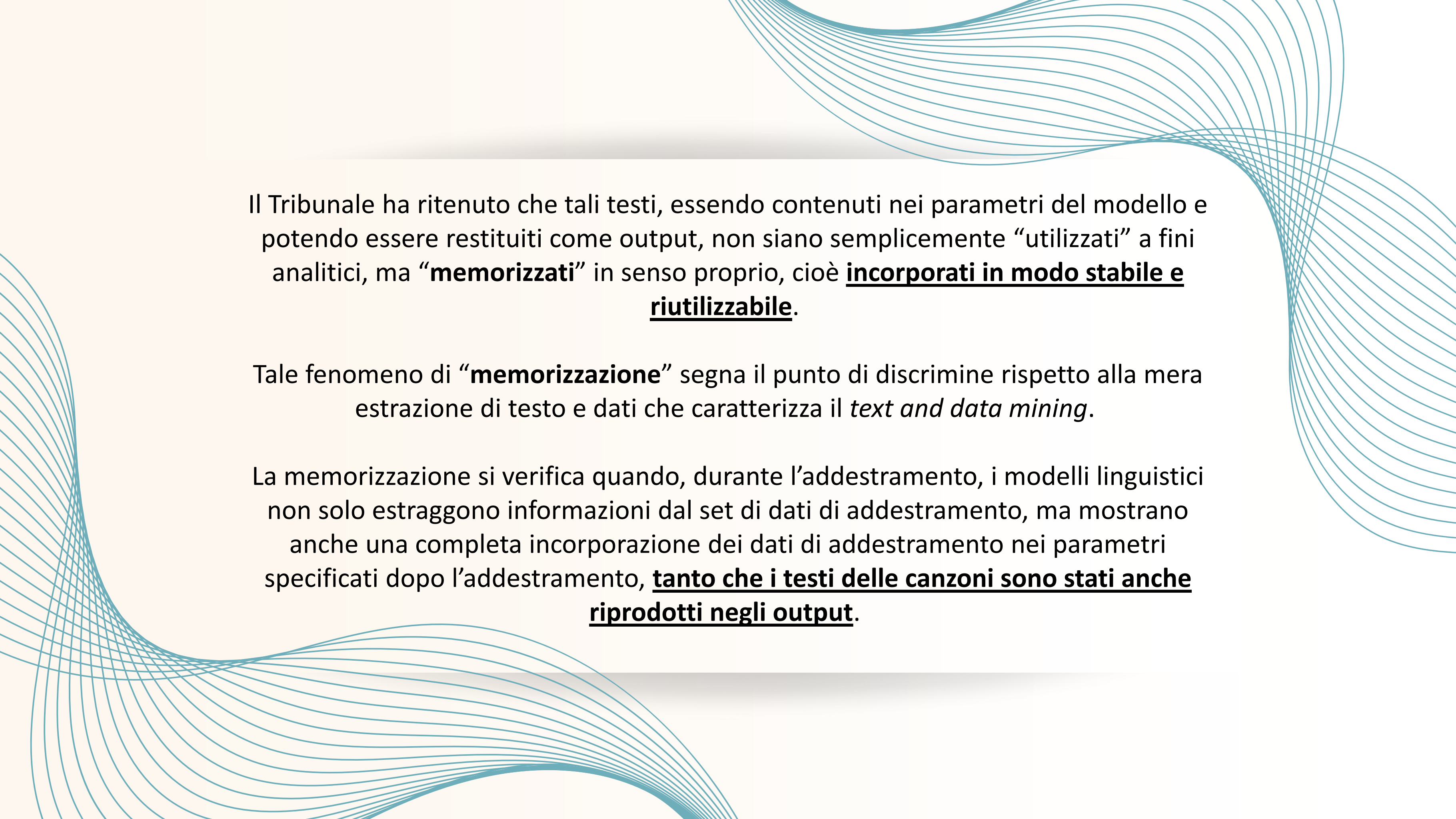
Ai confini del «TDM»: il caso GEMA vs. OPEN AI

L'11 novembre 2025 il Tribunale di Monaco I (*Landgericht München I*) ha condannato OpenAI nella causa promossa dalla società "*collecting*" tedesca GEMA.

Il tribunale ha in particolare sancito che l'utilizzo di testi di canzoni da parte della piattaforma ha violato il diritto d'autore:

- memorizzando testi (di canzoni)
- visualizzando parti dei testi nell'output.

Il Tribunale ha dunque stabilito che **non** si applica la **limitazione** di text-and-data mining ai sensi dell'art. 4 della direttiva 790/2019.



Il Tribunale ha ritenuto che tali testi, essendo contenuti nei parametri del modello e potendo essere restituiti come output, non siano semplicemente “utilizzati” a fini analitici, ma “**memorizzati**” in senso proprio, cioè **incorporati in modo stabile e riutilizzabile.**

Tale fenomeno di “**memorizzazione**” segna il punto di discriminare rispetto alla mera estrazione di testo e dati che caratterizza il *text and data mining*.

La memorizzazione si verifica quando, durante l’addestramento, i modelli linguistici non solo estraggono informazioni dal set di dati di addestramento, ma mostrano anche una completa incorporazione dei dati di addestramento nei parametri specificati dopo l’addestramento, **tanto che i testi delle canzoni sono stati anche riprodotti negli output.**

La decisione riguarda quindi l'applicabilità delle limitazioni in materia di text and data mining

Il Tribunale ha distinto tra:

- Riproduzioni meramente preparatorie, necessarie per l'analisi dei dati
- Riproduzioni che danno luogo a un'incorporazione stabile dell'opera nel modello.

Nel primo caso, la legge ammette la riproduzione temporanea in quanto funzionale alla successiva analisi.

Nel secondo, invece, la riproduzione permanente inciderebbe sui diritti di sfruttamento economico dell'autore.

Landesgericht Monaco

Sentenza 11.11.2025 - 42 O 14139/24

1. Le convenute **OpenAI USA e OpenAI Ireland** sono **condannate a cessare:**

- di **riprodurre**, in tutto o in parte, **senza il consenso dell'attrice GEMA**, i testi delle canzoni allegati nel fascicolo K1

all'interno di modelli linguistici (Large Language Models) e/o di far **eseguire tali atti da terzi**;

- di **rendere pubblicamente accessibili e/o riprodurre**, in tutto o in parte e/o sotto forma di **elaborazioni**, **senza il consenso dell'attrice**, i **testi delle canzoni** allegati nel fascicolo K1 negli output ("Outputs") di un chatbot, e/o di far eseguire tali atti da terzi (fascicolo K2) tali atti da terzi (fascicolo K2).

2. Le **convenute** vengono condannate a fornire all'attrice le **informazioni sull'estensione delle condotte descritte** e quali **introiti** esse ne abbiano ricavato, indicando:

- il **numero e l'entità delle condotte**;
- i **ricavi** per ciascuna delle convenute.

Si accerta che le convenute sono obbligate a **risarcire all'attrice ogni danno che le è già derivato e/o le deriverà dalle condotte descritte** al punto 1, secondo quanto risulterà dalle informazioni rese ai sensi del punto 2.

Nuove sfide e un criterio di riferimento già ben noto: Il Three-step test (art. 9(2) Convenzione di Berna; art. 5 Dir. 2001/29/CE)

Il ricorso alle eccezioni e limitazioni al diritto d'autore è ammesso alle seguenti condizioni:

- **Caso speciale**
(L'uso rientra in un'eccezione chiaramente definita e di natura circoscritta).
- **Assenza di conflitto con il normale sfruttamento dell'opera**
(L'eccezione non deve compromettere il mercato attuale o potenziale dell'opera).
- **Nessun pregiudizio ingiustificato agli interessi legittimi del titolare**
(L'impatto sui diritti dell'autore deve rimanere proporzionato e non irragionevole).

In ogni caso «*Le eccezioni e le limitazioni non possono essere applicate in modo da arrecare pregiudizio agli interessi legittimi dei titolari dei diritti o da essere in contrasto con la normale utilizzazione economica delle loro opere o materiali protetti ... È pertanto possibile che la portata di alcune eccezioni o limitazioni debba essere **ulteriormente limitata** nel caso di taluni nuovi utilizzi di opere e materiali protetti* (considerando 44)

Orientamenti giurisprudenziali non univoci

- Il caso **Getty Images VS Stability AI**: modello IA non memorizza né riproduce le immagini;
- il caso **Bartz/Anthropic** il Giudice Federale ha effettuato una distinzione: l'addestramento di **Large Language Model** costituisce un uso “*spettacolarmente trasformativo*” protetto dalla dottrina del **fair use** quando i contenuti vengono acquisiti legalmente, ma diventa illecito quando si basa su materiali attinti da piattaforme illegali come **BitTorrent**

Focus: input? Output? entrambi? Modalità di esercizio dell'opt-out?

La **sfida**: trovare l'equilibrio tra tutela del copyright e l'evoluzione tecnologica, senza che la creatività venga soffocata dalla ferocia dell'innovazione...

Gestione e limitazione del traffico di crawler

Misure di sicurezza preventive e idonee al fine di classificazione/analisi del traffico

(come peraltro previsto dalla seconda parte dell'art. 4, par. 3 della Direttiva Copyright):

classificazione/analisi del traffico, tramite analisi di molteplici fattori quali:

- *HTML headers* delle richieste al sito,
- indirizzi IP di provenienza delle richieste e
- comportamento degli utenti (es. la mappatura di *log* che, per caratteristiche, suggeriscano l'azione di un utente non umano).

Misure di sicurezza preventive e idonee al fine di classificazione/analisi del traffico

- risoluzione dei CAPTCHA/reCAPTCHA che saggiavano l'identità "umana" o "automatizzata" dell'utente
- L'uso di file:
 - ✓ ***robots.txt***, che indica ai *crawler* dei motori di ricerca a quali URL del sito possano accedere, specificando i singoli sottodomini "fruibili" o "vietati" per gli *user-agent*
 - ✓ ***human.txt***, che fornisce informazioni sull'uso del sito e sulla richiesta, formulata dal suo titolare, di rispettare precise condizioni di utilizzo (non raccogliere taluni contenuti)

Misure di sicurezza preventive e idonee al fine di classificazione/analisi del traffico

L'inserimento di **porzioni di codice** (es. *html*) che vietino la **deindicizzazione** dei contenuti, come “*noindex*” e/o “*disallow*”, ovvero un *set* di regole, con un *tag* o un'intestazione di risposta *http*, che viene utilizzato per impedire l'indicizzazione da parte dei motori di ricerca che supportano la regola (es. Google).

In questo modo, ad esempio quando *Googlebot* (*crawler* di Google) eseguirà la scansione di quella pagina ed estrarrà il *tag* o l'intestazione, Google eliminerà completamente la pagina dai risultati della ricerca Google, con il relativo pregiudizio per l'indicizzazione dei contenuti.

Regimi di licenza applicabili agli output di IA in ambito forense

OpenAI

- **Titolarità degli output:** cliente mantiene la proprietà degli input e acquisisce la titolarità degli output; eventuali diritti residui sono assegnati contrattualmente al cliente.
- **Uso dei dati:** nei piani business/enterprise i contenuti del cliente non vengono utilizzati per addestrare i modelli salvo consenso esplicito.
- **Limitazioni d'uso:** divieto di utilizzare output o servizio per sviluppare modelli concorrenti o sistemi che replicano funzionalità sostanziali del servizio.
- **Responsabilità professionale:** l'utente resta responsabile della verifica dell'accuratezza, liceità e adeguatezza dell'output prima dell'uso professionale o decisionale.
- **Indemnity (IP):** copertura per pretese di terzi relative a violazione di diritti di proprietà intellettuale derivanti dall'uso del servizio e, in determinate condizioni, dell'output.
- **Principali esclusioni dell'indemnity:** modifiche dell'output da parte del cliente; combinazioni con sistemi o dati di terzi; uso di input non autorizzati; utilizzo di servizi beta; uso in ambito marchi/commercio quando il rischio deriva dal cliente.

Anthropic

- **Titolarità degli output:** cliente possiede gli output generati; Anthropic assegna ogni diritto eventualmente maturato su contenuto generato.
- **Titolarità degli input:** piena proprietà e controllo restano al cliente
- **Uso dei dati:** dichiarazione esplicita che i contenuti dei clienti nei servizi commerciali non sono utilizzati per addestrare modelli
- **Limitazioni d'uso:** divieto di sviluppare o addestrare modelli concorrenti o prodotti che competano direttamente con il servizio.
- **Responsabilità professionale:** l'utente resta responsabile della verifica dell'accuratezza, liceità e adeguatezza dell'output prima dell'uso professionale o decisionale.
- **Indemnity (IP):** copertura contro rivendicazioni di terzi per violazione di diritti IP derivanti dall'uso del servizio e degli output nei servizi a pagamento.
- **Principali esclusioni dell'indemnity:** output modificati; combinazione con tecnologia o contenuti di terzi; input forniti dal cliente che generano la violazione; uso consapevole o prevedibilmente illecito; rivendicazioni su brevetti o marchi derivanti dall'uso commerciale dell'output

Meta – Llama Community License

- **Struttura del regime:** licenza sui materiali del modello (pesi, codice, documentazione), non un contratto di servizio cloud centralizzato.
- **Diritti concessi:** licenza non esclusiva, mondiale e royalty-free per utilizzare, modificare e distribuire i materiali del modello secondo i termini della community license.
- **Output e derivati:** la proprietà delle modifiche e dei derivati creati dall'utente rimane all'utente; la licenza non prevede una cessione esplicita degli output analoga ai contratti SaaS.
- **Limitazioni d'uso:** divieto di utilizzare i materiali o gli output per migliorare modelli linguistici diversi da quelli della stessa famiglia; altre restrizioni previste dalle acceptable use policies.
- **Garanzie:** materiali e output forniti “as is”, con esclusione estesa di garanzie su accuratezza, affidabilità o idoneità a scopi specifici.
- **Indemnity:** assenza di una copertura di indemnity del fornitore per gli output; obblighi di manleva generalmente a carico dell'utilizzatore verso Meta in caso di pretese di terzi.
- **Clausole di scala:** per operatori con base utenti estremamente ampia (soglia MAU elevata) può essere richiesta una licenza aggiuntiva

Uno sguardo generale

- Tutti i regimi contrattuali esaminati attribuiscono all'utilizzatore professionale la responsabilità finale sull'uso degli output
- Nei modelli SaaS enterprise (OpenAI, Anthropic, Google Cloud) la titolarità dell'output è generalmente riconosciuta al cliente, con coperture di indemnity IP **condizionate e con numerose esclusioni**
- Nel modello open-weight (Meta Llama) la flessibilità tecnica è maggiore, ma la protezione contrattuale del fornitore è significativamente più limitata e il rischio giuridico resta in capo all'utilizzatore.
- Per l'impiego forense è necessario:
 - ✓ utilizzare servizi con **termini enterprise chiari**;
 - ✓ evitare funzionalità beta o non coperte da indemnity;
 - ✓ documentare il processo di verifica umana degli output;
 - ✓ mantenere tracciabilità degli input, versioni del modello e condizioni contrattuali applicabili al momento della generazione.

If I create a work using AI, who is the holder of the copyright? The AI?

2



UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

NARUTO, a Crested Macaque, by and
through his Next Friends, People for
the Ethical Treatment of Animals,
Inc.,
Plaintiff-Appellant,

v.

DAVID JOHN SLATER; BLURB, INC., a
Delaware corporation; WILDLIFE
PERSONALITIES, LTD., a United
Kingdom private limited company,
Defendants-Appellees.

No. 16-15469

D.C. No.
3:15-cv-04324-
WHO

OPINION



The question of PETA's next-friend standing was squarely before our panel. It was briefed and argued. By both concluding that next-friend standing is nonjurisdictional *and* reaching the merits of the Copyright Act question, the Majority allows PETA (with no injury or relationship to the real party in interest) to sue on Naruto's behalf, because it obtained legal counsel to allegedly represent Naruto. I cannot support this conclusion.¹¹

Francesco Paolo Micozzi

If I create a work using AI, who is the holder of the copyright?

The AI?

Compendium of the U.S. Copyright Office Practices

Section 306: “The Human Authorship Requirement”

“[t]o qualify as a work of ‘authorship’ a work **must be created by a human being**. Works that do not satisfy this requirement are not copyrightable”

The Copyright Office will not register works produced by “nature, animals, or plants” including, by specific example, a “photograph taken by a monkey.”

Likewise, the Office cannot register a work purportedly created by divine or supernatural beings, although the Office may register a work where the application or the deposit copy(ies) state that the work was inspired by a divine spirit. Examples:

- A photograph taken by a monkey.
- A mural painted by an elephant.
- A claim based on the appearance of actual animal skin.
- A claim based on driftwood that has been shaped and smoothed by the ocean.
- A claim based on cut marks, defects, and other qualities found in natural stone.
- An application for a song naming the Holy Spirit as the author of the work.

If I create a work using AI, who is the holder of the copyright?

The AI?

Art. 1, L. 633/1941

2 Sono protette ai sensi di questa legge le **opere dell'ingegno umano di carattere creativo** che appartengono alla letteratura, alla musica, alle arti figurative, all'architettura, al teatro ed alla cinematografia, **qualunque ne sia il modo o la forma di espressione, anche laddove create con l'ausilio di strumenti di intelligenza artificiale, purché costituenti risultato del lavoro intellettuale dell'autore.**

Sono altresì protetti i programmi per elaboratore come opere letterarie ai sensi della Convenzione di Berna sulla protezione delle opere letterarie ed artistiche ratificata e resa esecutiva con legge 20 giugno 1978, n. 399, nonché le banche di dati che per la scelta o la disposizione del materiale costituiscono una creazione intellettuale dell'autore.

If I create a work using AI, who is the holder of the copyright? Me?

Cass. Civ., ord. 1107/2023

2 la protezione del diritto d'autore postula il requisito dell'**originalità** e della **creatività**, consistente non già nell'idea che è alla base della sua realizzazione, ma nella forma della sua espressione, ovvero dalla sua soggettività, presupponendo che l'opera rifletta la personalità del suo autore, manifestando le sue **scelte libere e creative**; la consistenza in concreto di tale autonomo apporto forma oggetto di una valutazione destinata a risolversi in un giudizio di fatto, come tale sindacabile in sede di legittimità soltanto per eventuali vizi di motivazione (Sez. 1, n. 10300 del 29.5.2020; Sez. 1, n. 13524 del 13.6.2014; Sez. 1, n. 20925 del 27.10.2005)

If I create a work using AI, who is the holder of the copyright? Me?

Cass. Civ., ord. 1107/2023

2 Non è certamente sufficiente a tal fine l'ammissione della controparte di aver utilizzato un software per generare l'immagine, circostanza questa che, come ammette la stessa ricorrente, è pur sempre compatibile con l'elaborazione di un'opera dell'ingegno con un tasso di creatività che andrebbe solo scrutinato con maggior rigore (cfr ricorso, pag.17), se, com'è avvenuto nel caso concreto, la (OMISSIS) non ha chiesto ai giudici di merito il rigetto della domanda per quella ragione.

E infatti si sarebbe reso necessario un accertamento di fatto per verificare se e in qual misura l'utilizzo dello strumento avesse assorbito l'elaborazione creativa dell'artista che se ne era avvalsa

If I create a work using AI, who is the holder of the copyright?
Me?

2

How can the **level of human contribution** to a work generated with the assistance of an AI system be demonstrated?



Francesco Paolo Micozzi

If I create a work using AI, who is the holder of the copyright?
Me?

2

Come può essere dimostrato il **livello di contributo umano** a un'opera generata con l'assistenza di un sistema di IA?

Proviamo a scomporre le fasi di un'opera creata mediante IA:

1. Definizione dell'idea artistica
2. Selezione del prompt per il sistema di IA
3. Scelta tra i diversi output proposti dall'IA
4. Modifica (editing) dell'output generato dall'IA

If I create a work using AI, who is the holder of the copyright?
Me?

2

Per determinare **se un prompt possa essere tutelato come opera dell'ingegno**, è necessario verificare se esso sia il risultato del lavoro intellettuale dell'autore (e soddisfi il requisito della “creatività”) e non consista meramente in un'istruzione tecnica o in una frase banale.

L'IA può violare il DDA attraverso i suoi output?

Affinché si configuri una violazione del diritto d'autore, l'output dell'IA deve presentare un grado di somiglianza tale da poter essere considerato un'opera derivata o una riproduzione sostanziale di un'opera protetta preesistente.

- Se un utente utilizza deliberatamente l'IA per creare contenuti che copiano un'opera protetta — ad esempio chiedendo esplicitamente “scrivimi una canzone con lo stesso testo di X” — la responsabilità ricadrà generalmente sull'**utente**.
- Se un sistema è progettato in modo tale da generare violazioni anche in assenza di input specifici dell'utente, oppure se il modello è stato addestrato su dati protetti senza licenza, **le società produttrici** (come OpenAI, Google o Midjourney) possono essere ritenute responsabili.
- **Non l'IA:** l'IA non ha personalità giuridica (è considerata uno strumento di creazione, non un soggetto di diritto).

...and what if the AI imitates an artist's “style”?

An **author's style**, as an abstract and replicable element, does not identify a single work and therefore does **not constitute the concrete expressive form of a work**.

Protecting “style” would be akin to protecting an idea (remember the example of the idea of a chair from a few slides ago?)

See also **Article 17(7)(b) of the Directive (EU) 2019/790** on this point (for further reading: Mezei, P., Senftleben, M., Sganga, C. et al. *Opinion of the European Copyright Society on the Scope of the Pastiche Exception in EU Copyright Law (CG and YN v Pelham GmbH and Others, Case C-590/23)*. IIC 56, 381–397 (2025). <https://doi.org/10.1007/s40319-025-01563-y>

Violazioni negli output generati dell'AI. Il caso dei deepfake

Cosa sono i Deepfake

- Dal punto di vista tecnologico

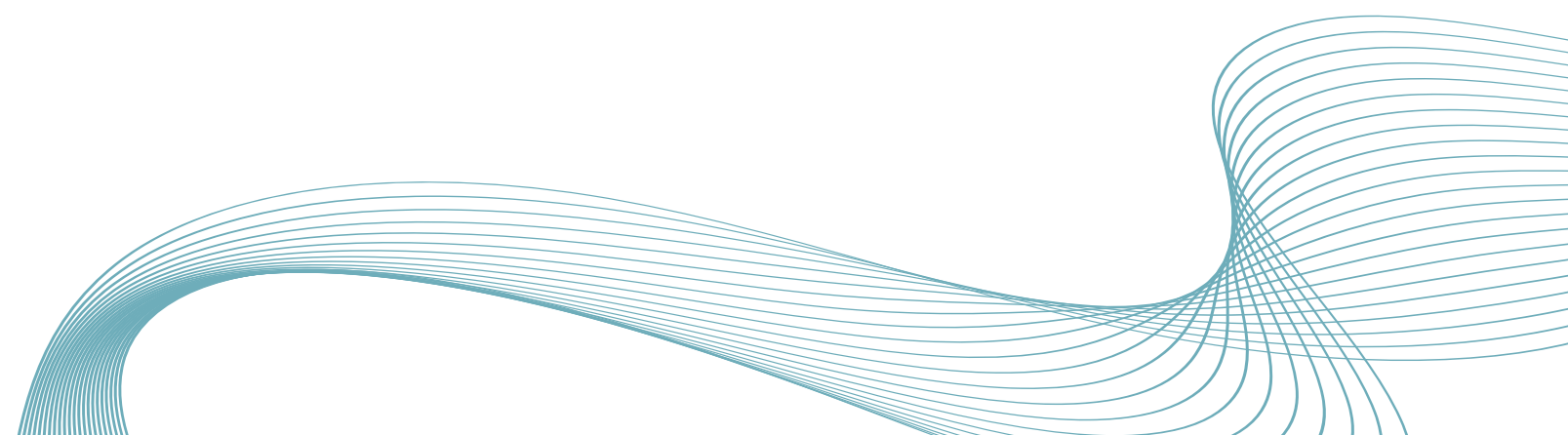
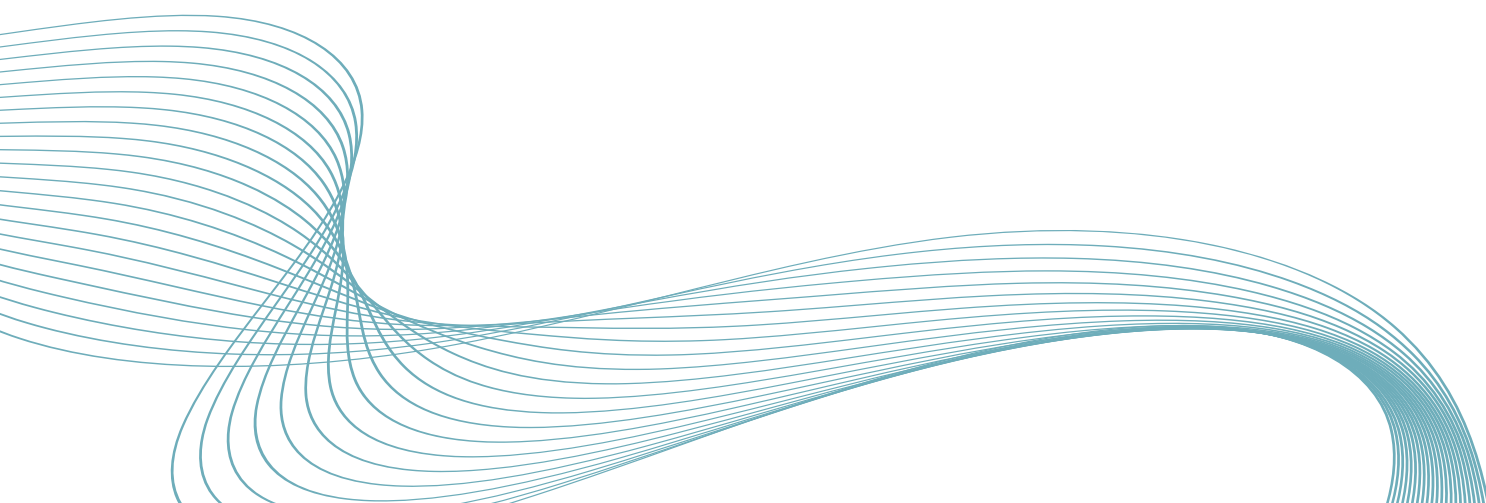


i deepfake costituiscono una sofisticata manipolazione di contenuti audio, video e immagini realizzata tramite avanzate tecniche di intelligenza artificiale e reti neurali (GAN - Generative Adversarial Network).

- Dal punto di vista legale

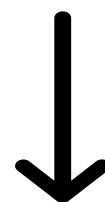


vengono descritti come *«un'immagine o un contenuto audio o video generato o manipolato dall'IA che assomiglia a persone, oggetti, luoghi, entità o eventi esistenti e che apparirebbe falsamente autentico o veritiero a una persona»* (AI Act, Art. 3 n. 60)



Come si crea un deepfake con l'AI?

Le **Generative Adversarial Network** (cosiddette «**GAN**» e tradotte «**Reti Generative Antagoniste**») sono un tipo di **modello di apprendimento automatico** basato su un **sistema a due reti neurali** che competono tra loro per **creare dati sempre più realistici**



- competono in un gioco a somma zero:
- una genera immagini verosimili (generatore)
- l'altra cerca di distinguere queste immagini da quelle reali (discriminatore).
- l'obiettivo è produrre immagini indistinguibili da quelle reali per diverse finalità

Tipologie di deepfake



1. **Persuasivi:** sfruttano la credibilità dell'individuo (es. autorevolezza, simpatia) attribuendogli falsi giudizi o dichiarazioni per influenzare e indirizzare le scelte del pubblico.
2. **Denigratori:** alterano l'immagine dell'individuo o del contesto rilevante per screditare / umiliare il soggetto (caso ulteriore: i deepfake pornografici)
3. **Satirici / Iudici:** alterano, in chiave comica, i tratti fisici o intellettuali dell'individuo, provocando ilarità negli spettatori
4. **Commerciali:** legittimamente utilizzati per finalità promozionali (es. Virtual influencer) o imprenditoriali (es. Waymo, produzioni cinematografiche...)

AI ACT: art. 50

Obblighi di trasparenza per i fornitori e i deployers di determinati sistemi di IA

- Obbligo di rendere noto che il contenuto del deepfake è stato generato / manipolato artificialmente
- Obbligo non si applica se l'uso è autorizzato dalla legge per accertare / prevenire / perseguire reati
- In caso di opere / programmi manifestamente creativi / satirici /artistici tali obblighi non ostacolano il godimento dell'opera
- Tali informazioni devono essere fornite alle persone fisiche interessate in maniera chiara ed accessibile, e al più tardi al momento della **prima interazione o esposizione**
- Tali obblighi lasciano impregiudicati obblighi di cui al **capo III (alto rischio)** e altri obblighi di trasparenza (UE o nazionali)

La Legge italiana sull'AI (L. n. 132/2025)

Art. 612 quater c.p.

"Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale":

- Chiunque cede, pubblica o diffonde contenuti altrui alterati dall'IA
- Il contenuto deve essere **idoneo a ingannare sulla sua autenticità** e deve causare **un danno ingiusto alla persona**
- **Assenza di consenso della persona danneggiata**
- **Reclusione da 1 a 5 anni**
- Reato generalmente punibile a querela (**ma in alcuni casi d'ufficio**)

La Legge italiana sull'AI (L. n. 132/2025)

Art. 612 quater c.p. - Illecita diffusione di contenuti generati o alterati con sistemi di intelligenza artificiale

*Chiunque cagiona un **danno ingiusto** ad una persona, cedendo, pubblicando o altrimenti diffondendo, senza il suo consenso, immagini, video o voci falsificati o alterati mediante l'impiego di sistemi di intelligenza artificiale e **idonei a indurre in inganno sulla loro genuinità**, è punito con la reclusione da uno a cinque anni. Il delitto è punibile a querela della persona offesa. Si procede tuttavia d'ufficio se il fatto è connesso con altro delitto per il quale si deve procedere d'ufficio ovvero se è commesso nei confronti di persona incapace, per età o per infermità, o di una pubblica autorità a causa delle funzioni esercitate*

AUTORITÀ GIUDIZIARIA

Azione cautelare (tutela inibitoria)

Azione risarcitoria

- danni patrimoniali (es. prezzo del consenso per l'immagine)
- non patrimoniali (presunzioni e quantificazione in via equitativa)



AUTORITÀ COMPETENTI OLTRE A QUELLA GIUDIZIARIA

1. Garante per la protezione dei dati personali (art. 77 GDPR)
2. AGCM competente ex art. 27 Cod. Cons.
3. AGCOM
4. CONSOB, *art. 7-octies, comma 1-bis del Testo Unico della Finanza – TUF (d.lgs. 58/1998)*

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

- **art 77 GDPR:** *"Fatto salvo ogni altro ricorso amministrativo o giurisdizionale, l'interessato che ritenga che il trattamento che lo riguarda violi il presente regolamento ha il diritto di proporre reclamo a un'autorità di controllo, segnatamente nello Stato membro in cui risiede abitualmente, lavora oppure del luogo ove si è verificata la presunta violazione".*



AUTORITÀ GARANTE DELLA CONCORRENZA E DEL MERCATO

(art. 27 Cod. Cons.)

- L'AGCM è competente a contrastare le **pratiche commerciali scorrette**.
- L'Autorità può indagare, ordinare la cessazione della pratica illecita e vietarne la continuazione, adottando i provvedimenti necessari per eliminarne gli effetti e irrogando sanzioni amministrative nei confronti dell'operatore economico responsabile



AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI (AGCOM)

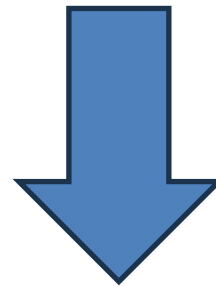
- Vigilanza sui contenuti audiovisivi (TUSMA) -> controllo sul rispetto di diritti fondamentali, tutela dei minori, divieto di contenuti lesivi.
- Ordini di rimozione o adeguamento (TUSMA + DSA) -> possibilità di imporre misure correttive o cessazione della diffusione
- Sanzioni amministrative (TUSMA + DSA) -> nel DSA fino al 6 % del fatturato.



COMMISSIONE NAZIONALE PER LA SOCIETÀ E LA BORSA (CONSOB)

Può vietare campagne pubblicitarie condotte tramite ogni mezzo di comunicazione (tra cui internet) quando hanno ad oggetto, direttamente o indirettamente, servizi e attività di investimento prestati da soggetti non abilitati ai sensi dell'art. 18 del Testo Unico della Finanza

(art. 7-octies, comma 1-bis del Testo Unico della Finanza – TUF (d.lgs. 58/1998))



Disposizione rilevante in quanto una grande quantità di deepfake persuasivi sono utilizzati per promuovere illecitamente «piattaforme finanziarie» truffaldine.

AND NOW
FOR SOMETHING
COMPLETELY
DIFFERENT



REALTÀ

Francesco Paolo Micozzi

IA non è un «motore di ricerca»

Un LLM:

- non interroga archivi di sentenze né recupera documenti specifici;
- **non “ricorda” testi giuridici come fonti consultabili;**
- genera l’output prevedendo, parola dopo parola, la sequenza linguisticamente più probabile in base ai dati di addestramento.

Il risultato è un testo **plausibile e coerente**, ma non necessariamente:

- completo,
- aggiornato,
- corretto sul piano fattuale o giurisprudenziale,
- riferibile a una sentenza effettivamente esistente.

Retrieval-Augmented Generation (RAG)

Il collegamento di un modello di intelligenza artificiale a una banca dati giuridica dà luogo a un sistema di generazione assistita da recupero documentale (RAG), destinato a supportare l'analisi e la comprensione del diritto, ma non assimilabile a un motore di ricerca né a una banca dati giurisprudenziale in senso proprio.

La Black Box

I sistemi di intelligenza artificiale vengono classificati come **black box** quando manifestano una **opacità epistemologica intrinseca** nella relazione tra input e output. Questa caratteristica si riferisce alla difficoltà o impossibilità di tracciare una mappatura esplicita e interpretabile del processo decisionale interno del modello.

Pur essendo formalmente descrivibili tramite equazioni matematiche, tali modelli operano attraverso un elevato numero di parametri (pesi) e **trasformazioni non lineari**, distribuite su molti strati, la cui interazione complessiva non consente una spiegazione intuitiva, simbolica o semanticamente trasparente del processo decisionale.

Opacità della Black Box

Ciò che rende impossibile risalire dall'output all'input è:

- **Non invertibilità delle funzioni.** Funzioni come la ReLU azzerano i valori negativi. Una volta ottenuto 0, l'informazione sul valore originale (se fosse -5 o -1000) è persa per sempre.
- Esistono **infiniti input** che possono produrre lo stesso output (non-iniettività della funzione).
- **Alta dimensionalità:** un LLM opera in spazi vettoriali N-dimensionali (dove N può consistere in migliaia di dimensioni). Cercare l'input inverso sarebbe come cercare un atomo specifico nell'oceano senza una mappa.
- **Perdita di informazione.** Il modello comprime e trasforma l'input in modi che non preservano tutte le caratteristiche originarie.
- **Instabilità numerica:** L'accumulo di errori di arrotondamento nell'aritmetica floating-point su miliardi di parametri rende il calcolo inverso instabile, producendo solo rumore privo di significato.
- **Dimensione del modello:** ricostruire il percorso richiederebbe analizzare miliardi di operazioni.

Cosa possono fare le XAI?

La **Explainable Artificial Intelligence (XAI)** è il corpus di metodologie, algoritmi e tecniche finalizzate a rendere il comportamento dei sistemi di intelligenza artificiale — in particolare i modelli black box — comprensibile, interpretabile e affidabile per l'osservatore umano.

Le tecniche di XAI offrono **illuminazioni parziali e probabilistiche**, utili per debugging e auditing, ma **non raggiungono una comprensione causale completa**. La ricerca futura deve affrontare il trade-off fondamentale tra capacità espressiva (che richiede alta complessità) e interpretabilità (che richiede semplicità strutturale).

Come funzionano i sistemi di IA per avvocati? (AI legal-centric)



Francesco Paolo Micozzi

Terza legge di Arthur C. Clarke

Any sufficiently
advanced technology
is indistinguishable
from magic.



Come vengono creati gli strumenti di IA per Avvocati?

Normalmente questi sistemi si compongono di:



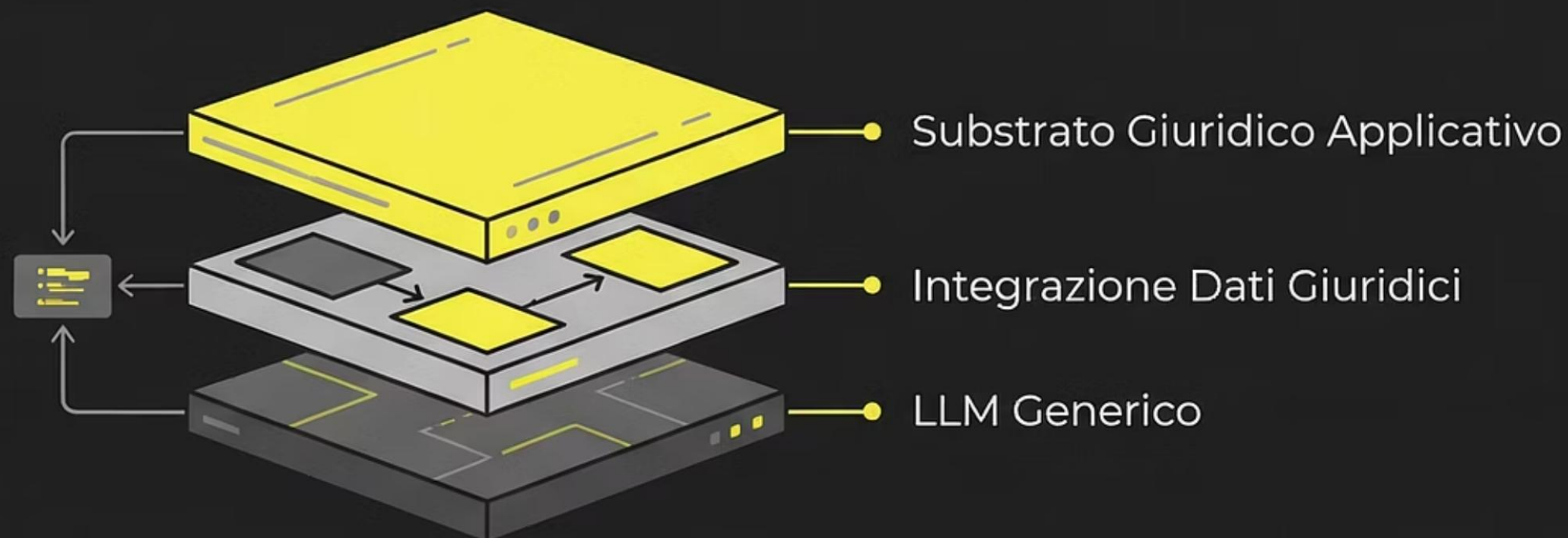
1. Un LLM generico (commerciale o opensource)



2. Integrazione con banche dati giuridiche (tramite RAG)



3. Substrato giuridico applicativo (normalmente limitazioni a determinati settori o territori, obbligo o meno di citare la fonte etc).



A cosa possono essere utili gli strumenti di IA per Avvocati?

Normalmente questi sistemi possono avere utilità per:



1. Individuare un orientamento giurisprudenziale;



2. Individuare precedenti;



3. Fare una sintesi degli orientamenti giurisprudenziali;



4. Fornire supporto alla redazione degli atti;

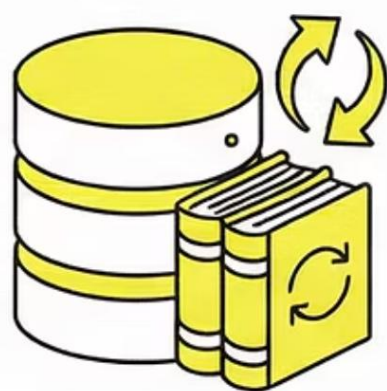


5. Esplorare in modo semplice un tema giuridico.

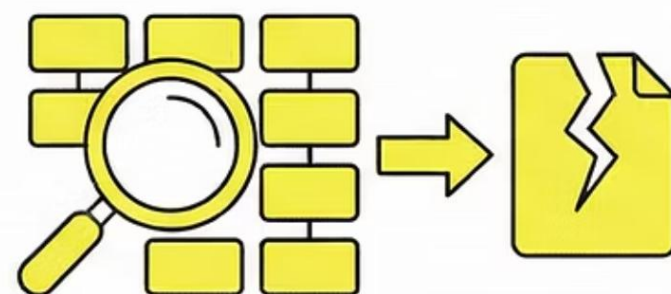
RICORDIAMO SEMPRE: non sono motori di ricerca e non sono banche dati giuridiche!

Da cosa dipende la qualità dei diversi strumenti di IA per Avvocati?

Normalmente questi sistemi variano per:



1. Qualità e aggiornamento della banca dati giuridica (prima della fase di embedding);



2. Qualità di embedding e retrieval (se non viene individuato il documento corretto, l'LLM non può usarlo)



3. Vincoli imposti dal substrato giuridico applicativo.

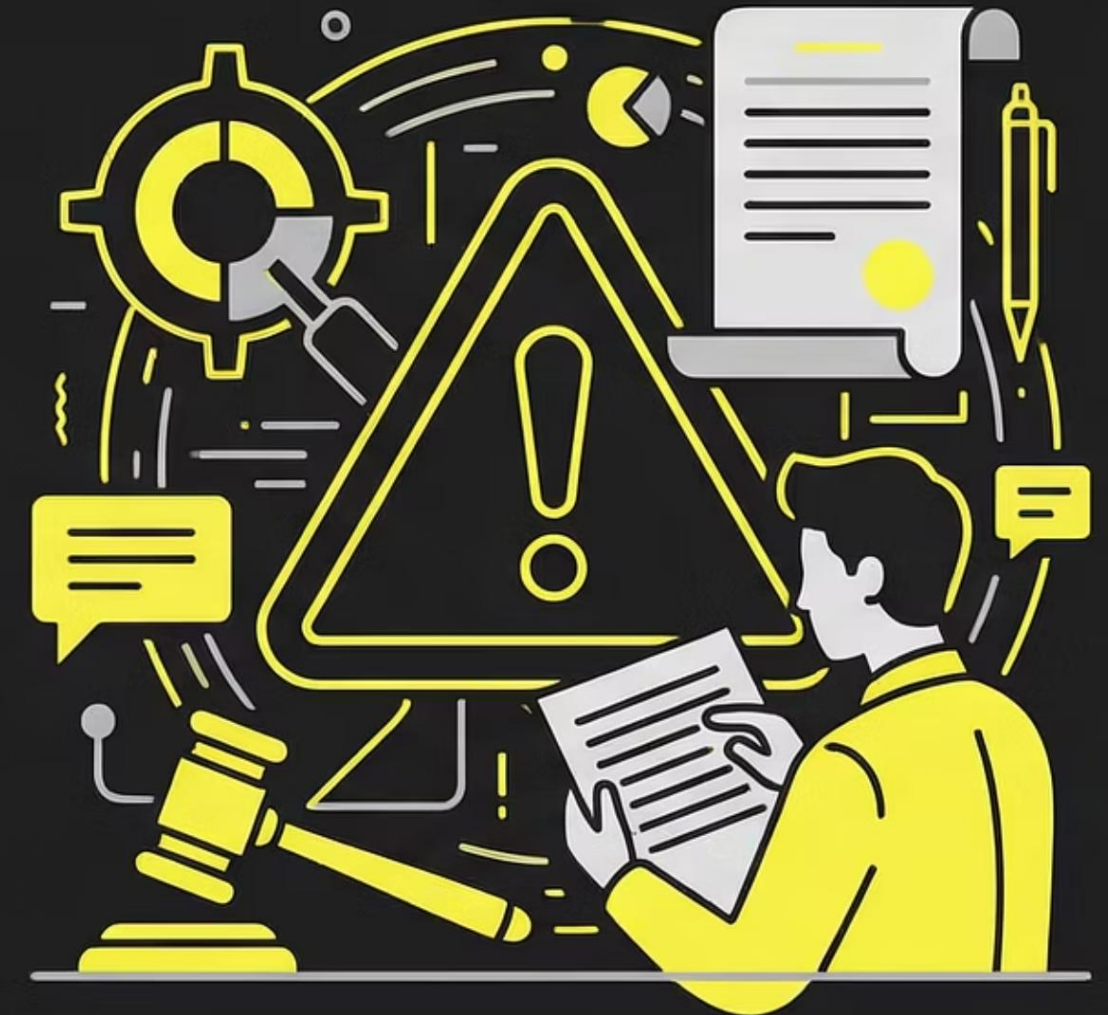
RICORDIAMO SEMPRE: sono più affidabili di un LLM generico, ma si basano sempre su sistemi generativi su base statistica e sono comunque meno affidabili di una ricerca giuridica «tradizionale»!

Quindi gli strumenti di IA per Avvocati sono immuni dalle allucinazioni?

No. Le allucinazioni possono diminuire ma non si eliminano. Cambiano un po' la loro natura...

I rischi maggiori dipendono da:

- ⚠ 1. Interpretazioni sovrabbondanti del testo recuperato;
- ⚠ 2. Generalizzazioni errate;
- ⚠ 3. Sintesi che omettono condizioni o limiti decisivi;
- ⚠ 4. Attribuzione di «granitico» a ciò che in realtà è orientamento minoritario



Definizione di RAG – Retrieval Augmented Generation

La **RAG** (acronimo di *Retrieval-Augmented Generation*, **Generazione Migliorata dal Recupero**) è un framework architetturale utilizzato per migliorare l'accuratezza, la pertinenza e l'affidabilità dei modelli LLM.

La RAG permette a un'intelligenza artificiale di consultare una «biblioteca» (db vettoriale) di dati esterni aggiornati o proprietari prima di rispondere a una domanda, invece di affidarsi esclusivamente alla sua memoria interna (i dati su cui è stata addestrata).

Panoramica del processo

7 fasi dal documento PDF alla risposta RAG



01

Documento PDF Originale

INPUT GREZZO



Il documento PDF contiene testo, tabelle, immagini e metadati strutturati in pagine. È il punto di partenza dell'intera pipeline di ingestione nel sistema RAG.

Dettagli tecnici

- Formato strutturato a pagine con layout complesso
- Può contenere testo, tabelle, immagini, form, allegati
- I metadati (autore, titolo, data) vengono preservati
- Supporto OCR per documenti scansionati





Mediante librerie specializzate il testo viene estratto pagina per pagina, preservando la struttura logica (titoli, paragrafi, tabelle).

Dettagli tecnici

- Librerie: PyMuPDF, pdfplumber, Unstructured
- Estrazione strutturata: titoli, paragrafi, tabelle
- OCR con Tesseract / Azure Document Intelligence
- Preservazione gerarchia sezioni e layout



Il testo estratto viene normalizzato: rimozione header/footer, fix encoding, merge righe spezzate, eliminazione artefatti di formattazione. Si conservano i metadati.

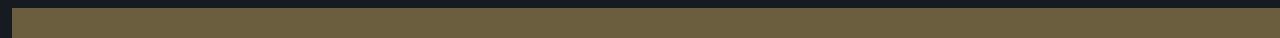
Dettagli tecnici

- Rimozione header/footer ripetuti e artefatti
- Fix encoding e caratteri speciali (\x0c, etc.)
- Merge righe spezzate e paragrafi frammentati
- Arricchimento metadati: n° pagina, sezione, titolo





Il testo pulito viene suddiviso in chunk di dimensione controllata con overlap per garantire continuità contestuale tra segmenti adiacenti.



Dettagli tecnici

- Fixed-size: 256-1024 token con overlap 50-200
- Recursive character splitting (LangChain)
- Semantic chunking: coerenza tematica via embeddings
- Structure-aware: rispetto titoli/sezioni/paragrafi



Ogni chunk viene trasformato in un vettore numerico ad alta dimensionalità tramite un modello di embedding che cattura il significato semantico.



Dettagli tecnici

- Modelli: OpenAI ada-002/3-small, Cohere, BGE
- Dimensioni tipiche: 768, 1024, 1536
- Il vettore codifica il significato semantico
- Batch processing per efficienza



I vettori, insieme ai chunk di testo e ai metadati, vengono indicizzati in un database vettoriale con algoritmi ANN per ricerca ad alta velocità.

Dettagli tecnici

- DB: Pinecone, Weaviate, Qdrant, ChromaDB, pgvector
- Indici ANN: HNSW, IVF-PQ per ricerca in ms
- Storage: vettore + chunk originale + metadati
- Namespace/collection per organizzazione multi-doc



La query utente viene vettorializzata e confrontata per similarità. I top-k chunk recuperati vengono iniettati come contesto nel prompt dell'LLM per la risposta finale.



Dettagli tecnici

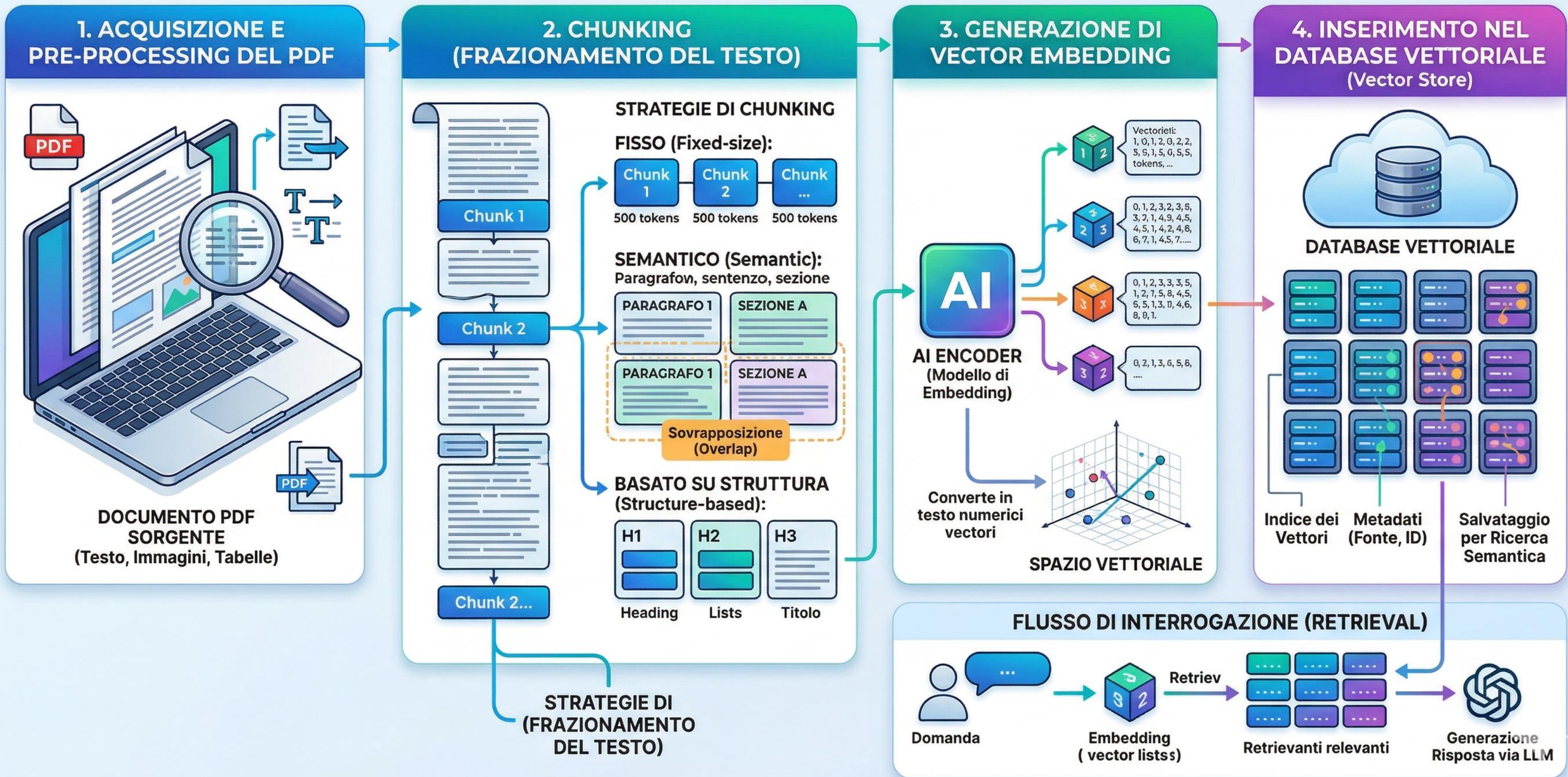
- Query → embedding → cosine similarity / dot product
- Top-k retrieval (tipicamente $k = 3-10$)
- Re-ranking opzionale (Cohere, cross-encoder)
- Prompt augmentation → LLM → risposta contestuale

Funzionamento della RAG – Retrieval Augmented Generation

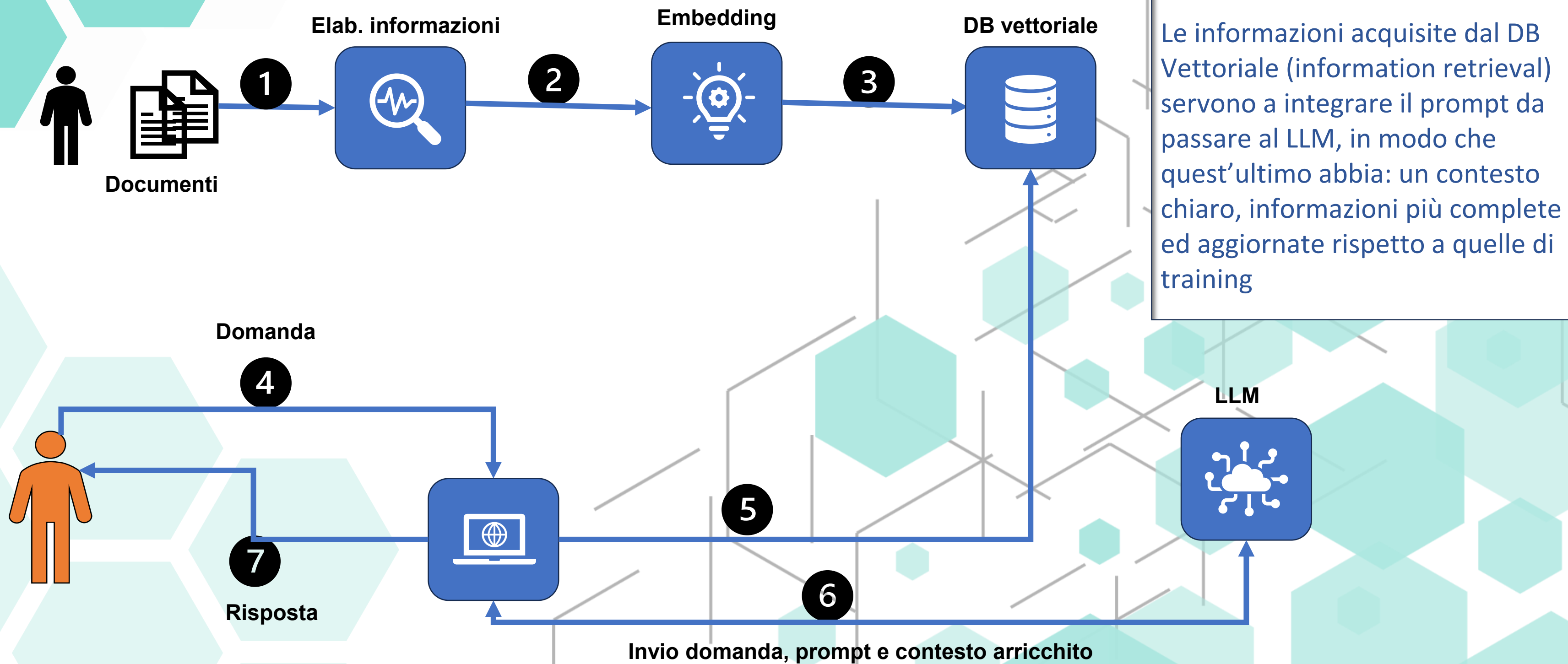
Con la RAG, in sostanza, si incide sul momento di creazione del prompt da inviare al LLM:



PROCESSO DI CHUNKING DI UN DOCUMENTO PDF PER UN DATABASE VETTORIALE RAG



Come funziona una RAG

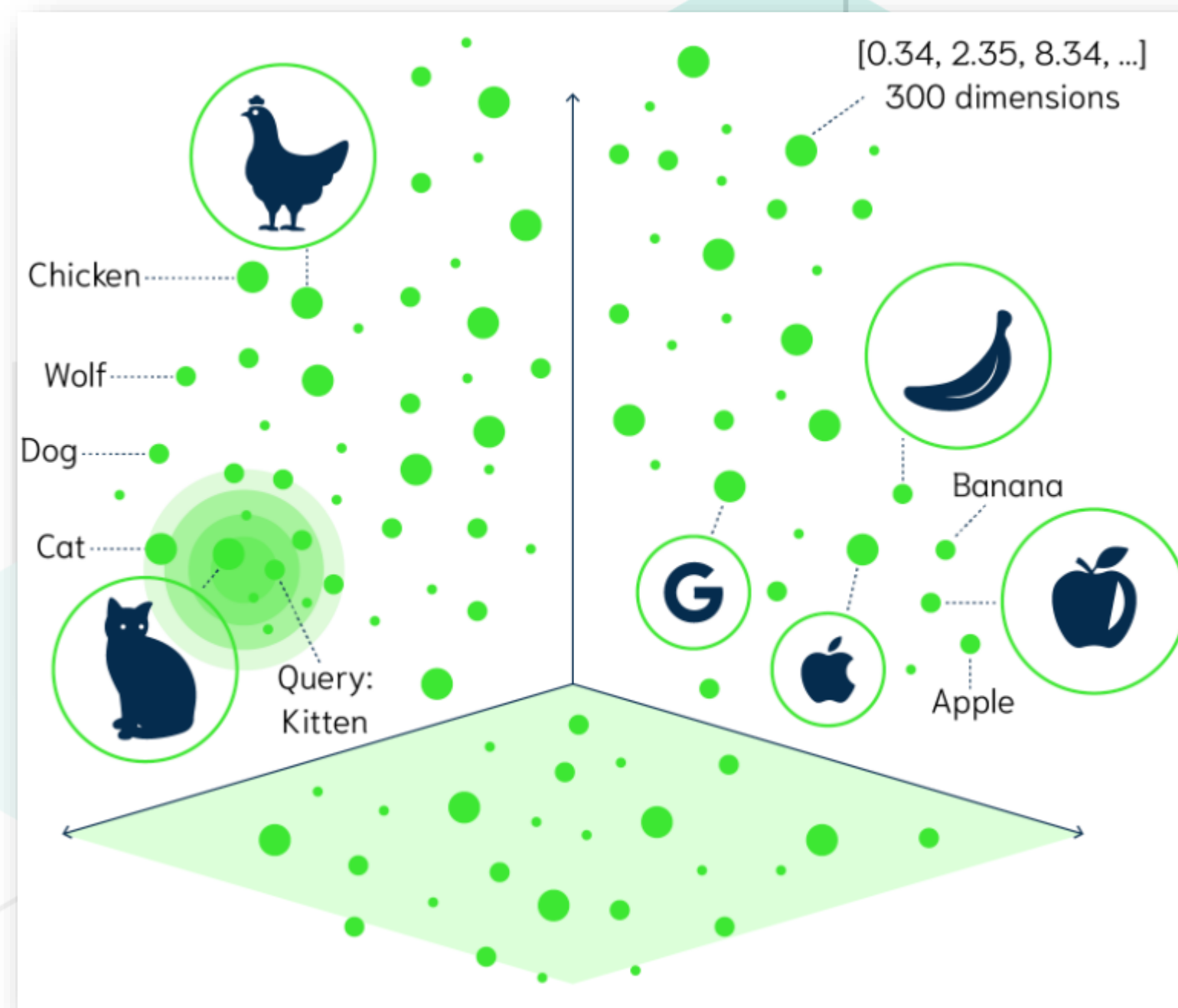


Cosa è l'embedding model



E' un modello di IA che si occupa di trasformare un testo in vettori numerici, in base ai quali un concetto viene inserito all'interno di una dimensione.

Lo spazio vettoriale non è, però, quello tridimensionale «x-y-z» ma $v=(v_1, v_2, v_3, \dots, v_N)$, dove N è fissato dal modello di embedding (e solitamente è molto elevato). Si parla di «**Spazio N-Dimensionale**»



Le dimensioni di un embedding



Il database **non “capisce” il testo**, ma:

1. Vettorializza l'informazione che cerchi (query)
2. Calcola una **misura matematica di distanza** rispetto ai vettori «embeddati» (di solito):
 - similarità coseno
 - distanza euclidea
3. Restituisce i vettori **più vicini**
4. **Costruisce il prompt per LLM**

Esempio (in realtà le dimensioni sono molte più di 5)

Query A: «**il contratto è stato firmato digitalmente**»

$A = [0.12, 0.85, 0.33, 0.91, 0.44]$

Query B: «**Il documento è stato sottoscritto con firma digitale**»

$B = [0.11, 0.82, 0.30, 0.89, 0.47]$

Query C: «**Ricetta per la torta al cioccolato**»

$C = [0.77, 0.05, 0.91, 0.02, 0.88]$

Dimensione	A	B	Differenza
1	0.12	0.11	0.01
2	0.85	0.82	0.03
3	0.33	0.30	0.03
4	0.91	0.89	0.02
5	0.44	0.47	0.03

Dimensione	A	C	Differenza
1	0.12	0.77	0.65
2	0.85	0.05	0.80
3	0.33	0.91	0.58
4	0.91	0.02	0.89
5	0.44	0.88	0.44

Cosa è il database vettoriale



Un database vettoriale è un sistema informatico che gestisce rappresentazioni numeriche ad alta dimensionalità per consentire interrogazioni basate sulla **similarità**, e non sull'uguaglianza, dei dati.

Il database vettoriale opera sul piano della **prossimità semantica** e dell'interpretazione computazionale, mentre i sistemi tradizionali di hashing, firma digitale e conservazione documentale operano sul piano dell'**identità, integrità e certezza giuridica**. I due ambiti sono complementari, ma non sovrapponibili.

```
{
  "id": "doc_RG_1234_2023_memoria_01",
  "vector": [
    0.0123,
    -0.8871,
    0.4420,
    0.1934,
    -0.2217,
    0.9042,
    -0.1189,
    0.5576
  ],
  "metadata": {
    "tipo_documento": "atto_giudiziario",
    "procedimento": "RG_1234_2023",
    "ufficio": "Tribunale Civile di Roma",
    "data_deposito": "2024-11-12",
    "parte": "ricorrente",
    "hash_sha256": "9f86d081884c7d65c28bce9294e0193f...",
    "firmato_digitalmente": true,
    "fonte": "deposito_telematico",
    "lingua": "it"
  }
}
```

Differenza tra query e prompt generato da RAG

4 QUERY dell'Utente: "La firma digitale garantisce l'integrità del documento?"



6 PROMPT generato da RAG: Usa esclusivamente le informazioni fornite nel contesto per rispondere alla domanda.

Se le informazioni non sono sufficienti, dichiaralo esplicitamente.

Contesto:

[Documento 1 – Estratto CAD, art. 20]

"La firma digitale garantisce l'integrità del documento informatico..."

[Documento 2 – Linee guida AgID]

"La validità della firma digitale è subordinata alla verifica del certificato..."

[Documento 3 – Nota tecnica]

"L'integrità è assicurata tramite funzioni di hash..."

Domanda:

"La firma digitale garantisce l'integrità del documento?"

Come cambia, quindi, la professione con l'uso di AI specifiche?

L'output derivante dall'uso di tali strumenti, rispetto all'output di un LLM generico, è:

- ✓ più probabile che sia corretto;
- ✓ più facile verificarlo;
- ✓ più difficile che sia arbitrario.



GENERIC LLM



SPECIALIZED LEGAL AI

In ogni caso...

Se l'avvocato usa un LLM o un RAG:

- **non può invocare l'IA come fonte infallibile;**
- **non può trasferire la responsabilità sull'algoritmo;**
- **resta l'unico soggetto responsabile (si veda L. 132/2025).**

Grazie
per la tensione!

