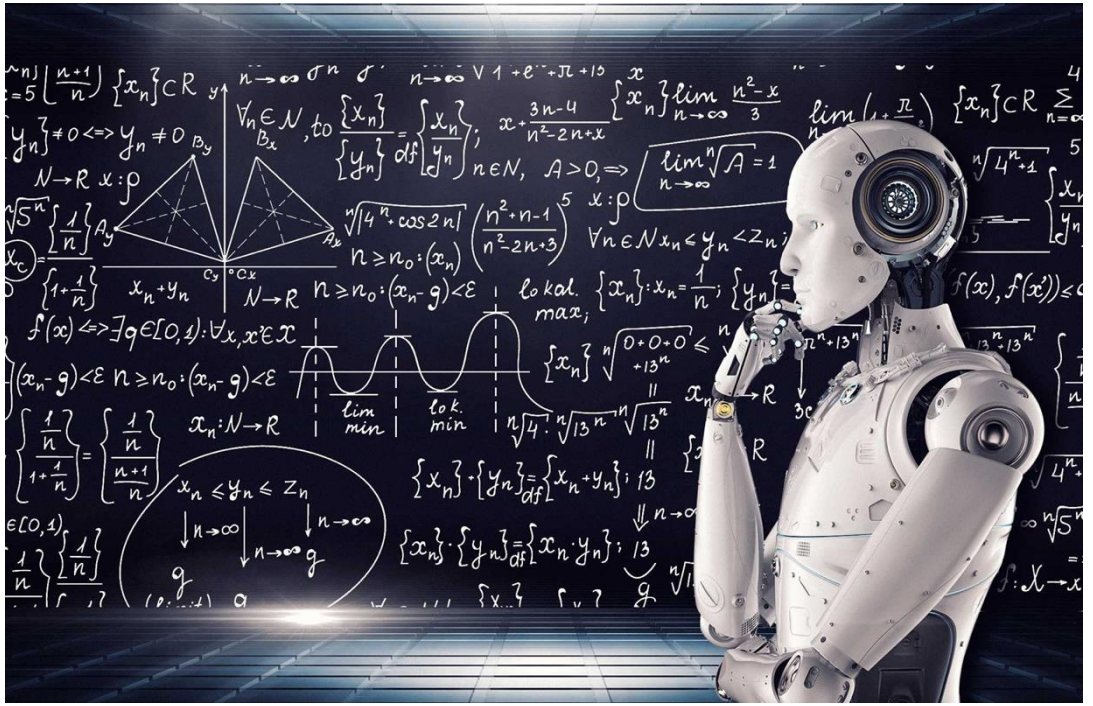
L’ uso dell’intelligenza artificiale nella pubblica amministrazione

dal prompt alla responsabilità dell’atto



FABRIZIO FRATONI

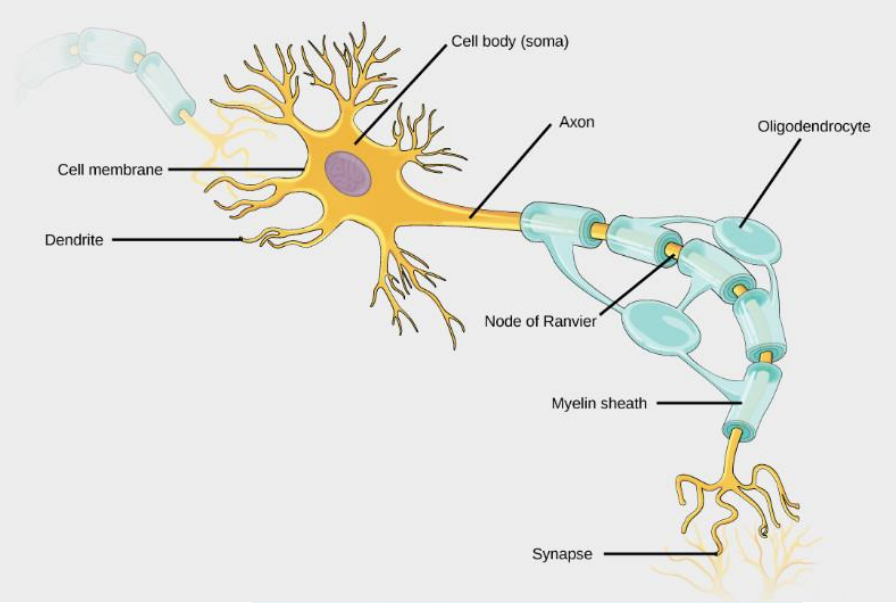
Colonnello dei Carabinieri e Criminologo Senior
certificato norma UNI 11783/2020

INTELLIGENZA ARTIFICIALE

si intende l'abilità di un sistema computerizzato di svolgere funzioni ed effettuare i ragionamenti tipici della mente umana.

Algoritmi che **permettono alle macchine di mostrare attività intelligente, dando loro definizioni formali di ragionamento ed apprendimento.**

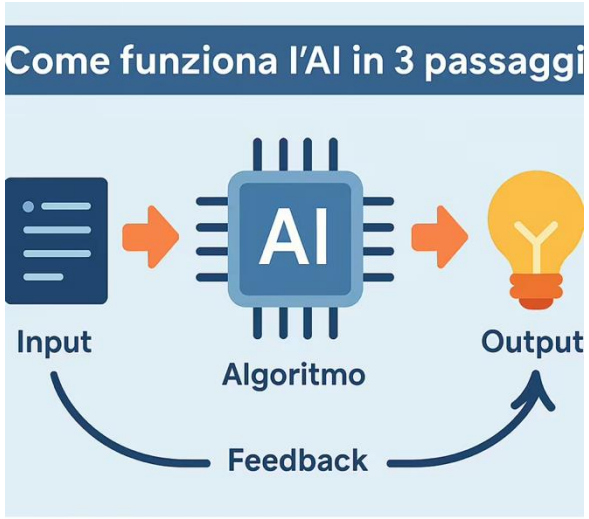
- 1950 Alan Turing con **macchina di turing**
- **Frank Rosemblatt** Percettrone ***(come neurone)***
- 1943 Warren Mc Culloch e Walter Pitty progettano rete neurali e ogni calcolatore come se fosse un neurone celebrale programma con linguaggio lisp
- 1973 **Linguaggio Prolog** si basa sull0 utilizzo di predicate e consente dialogare con interlocutori esterni con architetture parallele e data center e processori potenti

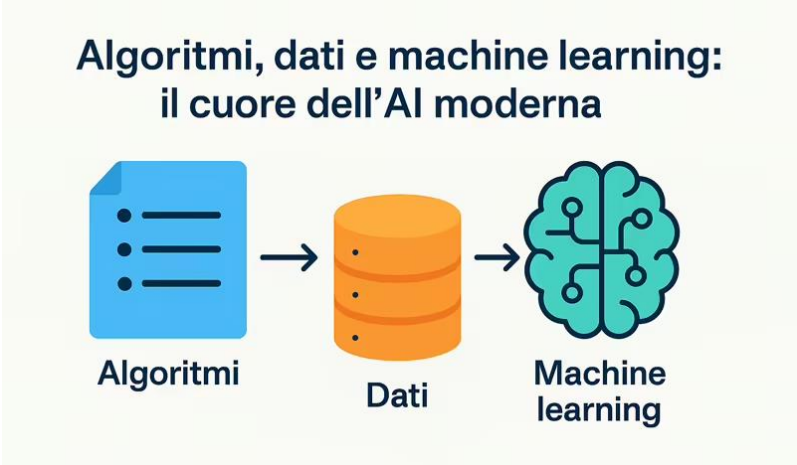


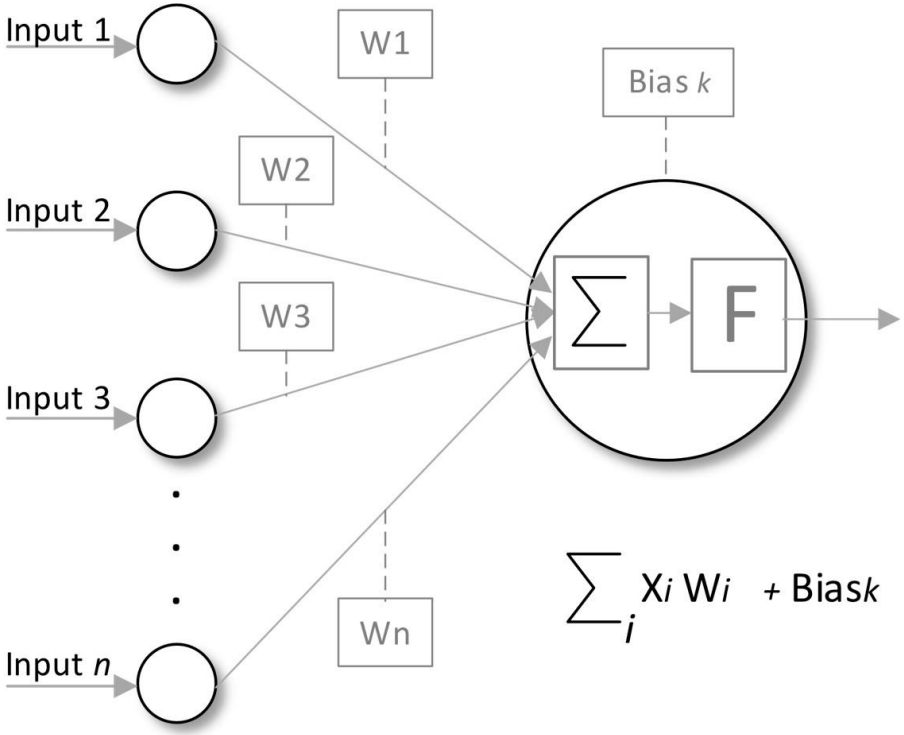


La capacità inferenziale dei sistemi di IA, li distingue dai sistemi software tradizionali, **che consente loro di generare output significativi da dati, permettendo previsioni e decisioni**, con vari livelli di autonomia e adattabilità,

Simula comportamenti tipicamente umani: apprendere, ragionare, risolvere problemi, prendere decisioni.







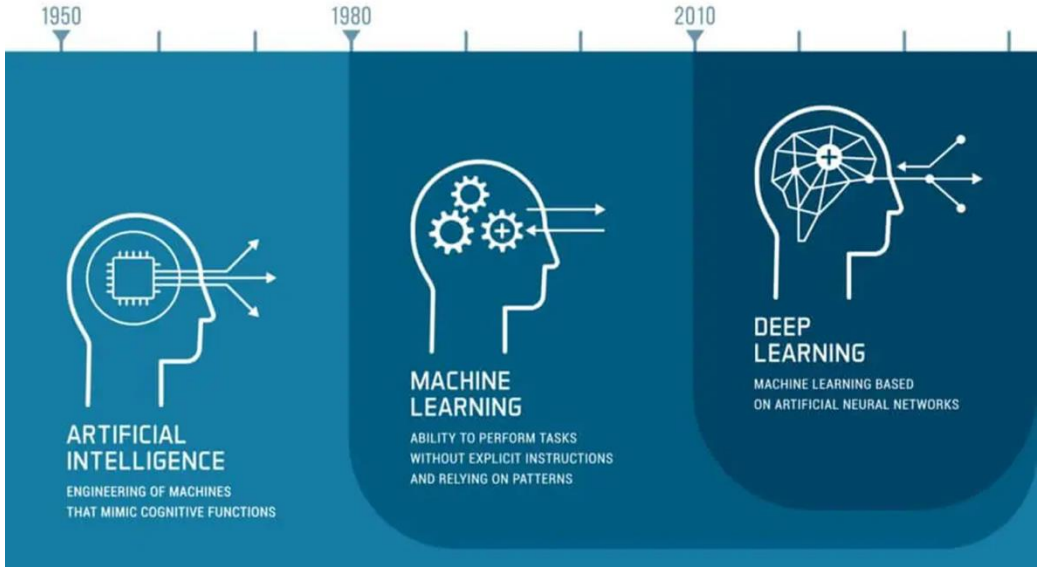




Sistema di IA automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione **e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output** quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali.

Token blocco di testo categorizzato, normalmente costituito da caratteri indivisibili chiamati lessemi permette **interfaccia linguaggio.**

I 2 sottoinsiemi dell'intelligenza artificiale

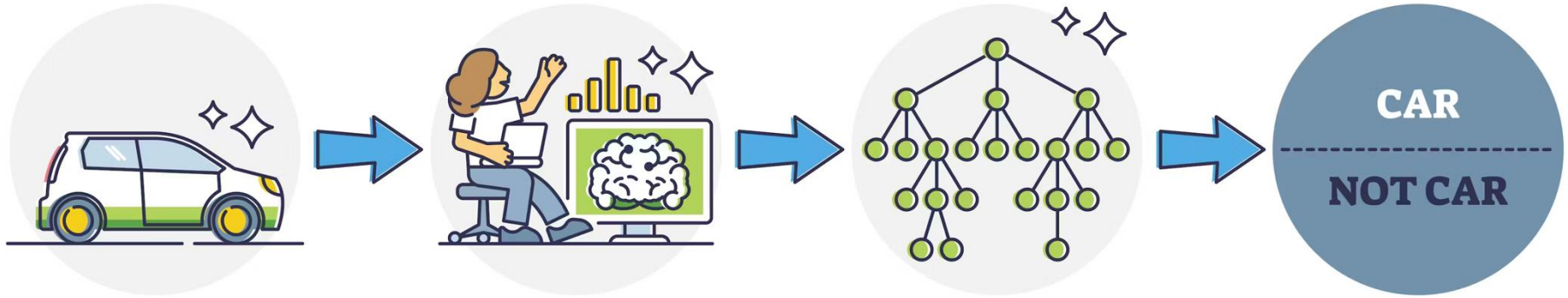


Il **Machine Learning** è un insieme di metodi che permettono al software di adattarsi e apprendere autonomamente senza essere preventivamente programmato, con tre modelli di apprendimento: supervisionato, non supervisionato e **reinforcement learning**.

Il Deep Learning si ispira alla struttura del cervello umano e **utilizza reti neurali artificiali per emulare la mente umana,** richiede una **capacità computazionale elevata** per gestire strati multipli di calcolo e analisi, utilizzato in applicazioni come il riconoscimento vocale e delle immagini e nel **Natural Language Processing (NLP).**

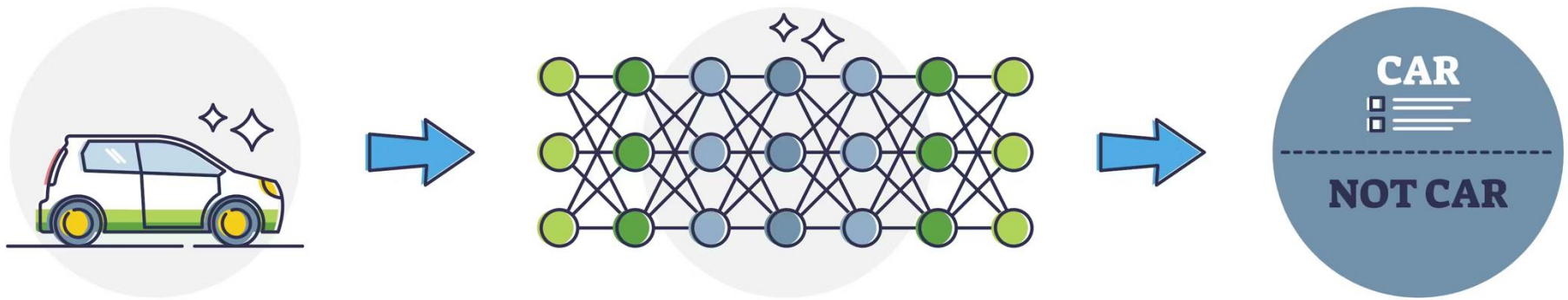
- differenze nel **grado di intervento umano** **e il tempo necessario per ottenere risultati e il metodo di apprendimento, il Machine Learning richiede più intervento umano e utilizza algoritmi tradizionali**, mentre il **Deep Learning richiede meno intervento umano, ma più tempo per l'impostazione**

MACHINE LEARNING



INPUT | FEATURE EXTRACTION | CLASSIFICATION | OUTPUT

DEEP LEARNING



INPUT | FEATURE EXTRACTION + CLASSIFICATION | OUTPUT

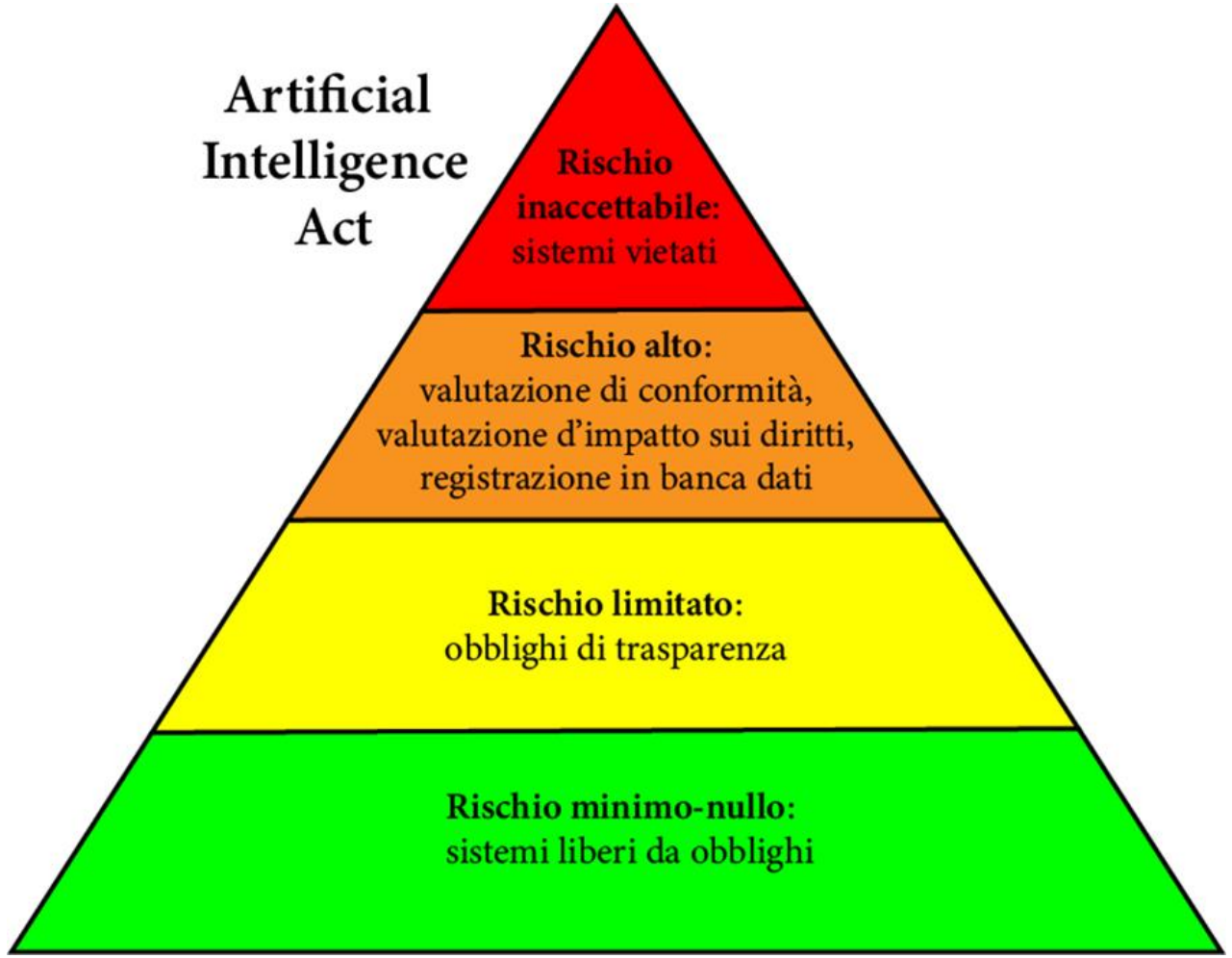
Il Regolamento UE 2024/1689



- **garantisce sicurezza e rispetto dei diritti fondamentali e promuove l'innovazione,**
- **protegge la democrazia, lo Stato di diritto e la sostenibilità ambientale dai sistemi di IA ad alto rischio e assicurando all'UE ruolo guida nel settore**
- **regolare utilizzo dei sistemi per creare algoritmi di AI, generativa,**
- **tutelare dalla pervasività della digitalizzazione** intrapreso dall'UE per dal Digital Governance Act, al Data Act, 2023, Digital Services Act, 2022 e al Digital Markets Act, 2022

Approccio basato sul rischio su 4 livelli di per i sistemi di IA:

- **inaccettabile** sono u**na chiara minaccia per la sicurezza, i mezzi di sussistenza e i diritti delle persone e pertanto vietati**,
- **rischio alto** *richiesta valutazione conformità e impatto, e registrazione banca dati*
- **limitato** ***(solo obblighi trasparenza);***
- **minimo o nullo.**



Rischio minimo o nullo

- **l'AI Act consente l'uso gratuito dell'IA** a rischio minimo, ma con codice condotta
- App come videogiochi abilitati per l'IA o filtri antispam NPC generativo (NPC = non playing character), ero operare al di fuori dell'ambito previsto, (*potrebbero essere considerati a rischio. l'uso di sistemi di riconoscimento delle emozioni tramite webcam)*
- maggioranza dei sistemi di IA attualmente utilizzati nell'UE rientrano in questa categoria.





Per i sistemi a rischio limitato



- introduce specifici obblighi di comunicazione

per i rischi associati alla mancanza di trasparenza

nell'utilizzo dell'IA,

- garantisce che le persone **siano informate, promuovendo la fiducia**
- **se chatbot**, **avvisare che si sta interagendo con una macchina** in modo da prendere una decisione informata
- i fornitori devono garantire che i contenuti **generati dall'IA siano identificabili**
- il testo generato dall'IA pubblicato con lo scopo di informare deve essere etichettato chiaramente
- anche per i contenuti audio e video che costituiscono falsi



Regole comuni per i sistemi di IA ad alto rischio



- garantendo un livello elevato di protezione degli interessi pubblici.
- le norme devono essere coerenti con la Carta e gli impegni internazionali.
- **devono essere non discriminatorie e in linea con gli impegni commerciali internazionali.**
- riferimento alla dichiarazione europea sui diritti digitali e agli orientamenti etici per un'IA affidabile.
- norme armonizzate si applicano a tutti i settori e non pregiudicano il diritto dell'Unione esistente.

ROAD MAP

1 agosto 2027:
Applicazione completa del Regolamento per tutte le categorie di rischio, inclusi gli obblighi dettagliati nell'Allegato II.

1 agosto 2026:
il Regolamento diventa pienamente applicabile, incluse le norme per i sistemi di IA ad alto rischio.

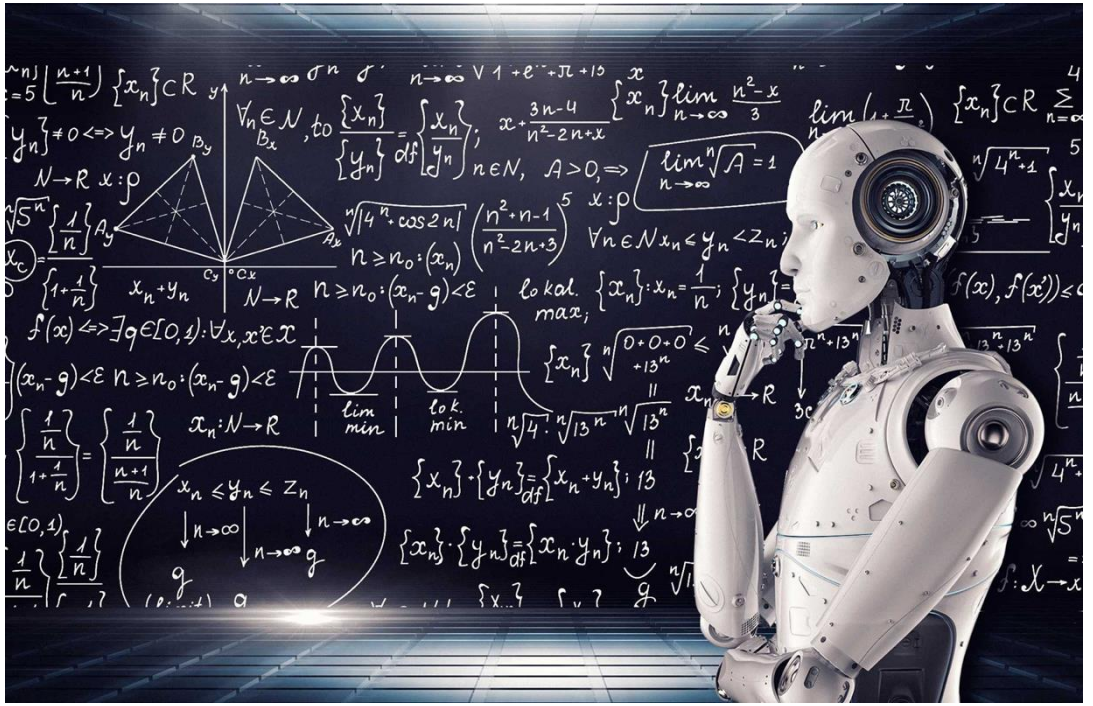
2 agosto 2025:
norme di governance e degli obblighi per i modelli di IA a uso generale

2 febbraio 2025:
disposizioni generali (Capi I e II), comprese definizioni, ambito di applicazione e principi fondamentali



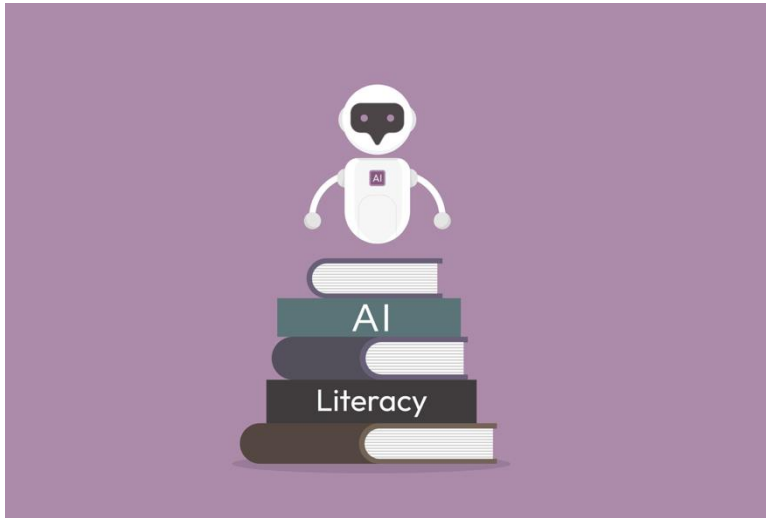
L’ uso dell’intelligenza artificiale nella pubblica amministrazione

dal prompt alla responsabilità dell’atto

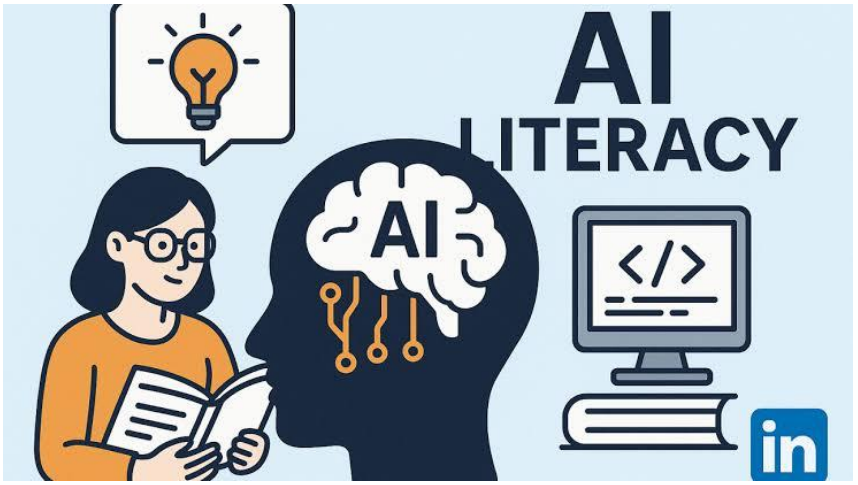


FABRIZIO FRATONI

Colonnello dei Carabinieri e Criminologo Senior
certificato norma UNI 11783/2020



AI literacy

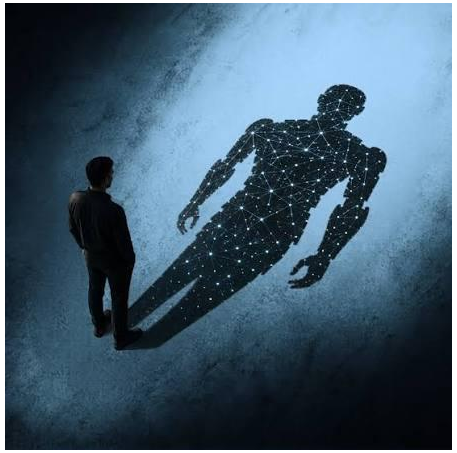


Art 4. dispone di garantire un **livello adeguato di alfabetizzazione su IA** per i dipendenti delle aziende che sviluppano o utilizzano tali sistemi.

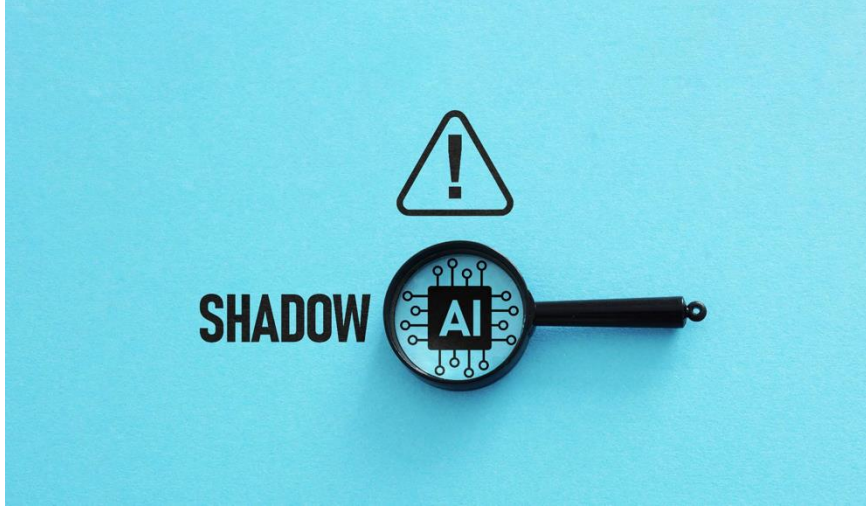
Prevenzione fuga di dati riservati e le conseguenze legali che ne derivano. Infatti, il Report 2025 di LayerX, il 77% dei dipendenti incolla dati sensibili aziendali dentro strumenti come Claude o ChatGPT, aumentare l'alfabetizzazione aiuta a prevenire questi danni.

In vigore dal 2 febbraio 2025 **Regolamento (UE) 2026/1744 chiede a chi utilizza sistemi di IA di sostenere l'alfabetizzazione del proprio personale**

Crescita del fenomeno dei danni per la mancata formazione dei dipendenti, che inseriscono documenti, dati di clienti o informazioni riservate in strumenti LLM senza alcun orientamento, spesso senza rendersi conto di dove vanno i dati.



“Shadow AI”



Crescita del fenomeno di strumenti AI che i dipendenti adottano senza ricevere un’autorizzazione . *Secondo il report Soldo, questo è accaduto a circa il 27% dei dipendenti, persone che inseriscono documenti, dati di clienti o informazioni riservate in strumenti LLM mai approvati, spesso senza rendersi conto di dove finiscano quelle informazioni*

Se il chatbot l’ha attivato il dipendente , tra l’ente e il fornitore non c’è un rapporto formale: nessuna istruzione, nessun impegno sulla sicurezza, nessuna regola su che fine fanno i dati quando il servizio cessa. Il GDPR chiede all’ente di affidare i dati solo a chi presenta garanzie sufficienti (art. 28, par. 1), e quelle garanzie si leggono in un contratto

Aumentare l’alfabetizzazione aiuta a prevenire questi danni.

Legge 132/2025 normativa nazionale IA





Legge 132/2025 prima normativa nazionale IA



a) uso antropocentrico, trasparente e sicuro dell'IA

b) cura aspetti di innovazione, cybersicurezza, accessibilità

c) responsabilità, equità e rispetto per i diritti fondamentali, tali da garantire un equilibrio tra le opportunità che offrono le nuove tecnologie e i rischi legati al loro uso improprio, al loro impiego dannoso **divieti di talune pratiche di IA;**

c) regole di trasparenza armonizzate con regolamento europeo IA

d) rispetto del principio di uguaglianza e all'accessibilità per le persone con disabilità, *affinché nessuno resti escluso dall'uso delle nuove tecnologie* e al loro pregiudizievole sottoutilizzo

e) prevede garanzie di tracciabilità, responsabilità umana e centralità della decisione finale di una persona fisica

Obiettivo promuovere IA antropocentrica e affidabile



migliorare il funzionamento del mercato interno, garantendo livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali e promuovendo l'innovazione, con:

a) regole **armonizzate per l'immissione sul mercato**, messa in servizio e uso dei sistemi di IA;

b) **divieti di talune pratiche di IA;**

c) **requisiti specifici per i sistemi di IA ad alto rischio** e obblighi per gli operatori ;

d) regole di trasparenza armonizzate per determinati sistemi di IA;

e) regole armonizzate per l'immissione sul mercato di modelli di IA per finalità generali;

f) **regole per monitoraggio del mercato, vigilanza, governance ed esecuzione**;

g) misure a sostegno dell'innovazione, con particolare attenzione alle PMI, e start-up.

Legge 132/2025



Per governare delicata fase dove la realtà economica e sociale subiscono sempre di più gli effetti dell'interazione con i sistemi di AI la legge istituisce:

- **l'Autorità nazionale per l'intelligenza artificiale deputata a vigilare sulla corretta applicazione delle norme**
- **il Comitato interministeriale per l'intelligenza artificiale**, ha il compito di definire le strategie nazionali e garantire che lo sviluppo dell'IA sia allineato con gli interessi del Paese
- ruolo di fondamentale importanza non solo per le aziende del settore, ma per la tutela ogni cittadino che si troverà più frequentemente ad interagire con sistemi sempre più intelligenti



Particolare attenzione è dedicata ad alcuni ambiti cruciali:



- **Sanità ove l'uso dell'IA per la diagnosi e la terapia viene incoraggiato, ma con limiti precisi, evidenziando in tema di trattamento e diagnosi sanitaria la decisione finale spetterà sempre al professionista sanitario, al fine di evitare che l'algoritmo si sostituisca al giudizio umano**
- **lavoro,** la normativa riconosce l'impatto che l'IA sta avendo ed avrà sul mercato del lavoro, prevedendo l'obbligo per le aziende di informare i sindacati sull'adozione di sistemi IA che potrebbero modificare le mansioni dei dipendenti
- **giustizia la legge precisa che l'utilizzo di sistemi di "giustizia predittiva" può essere ammesso solo come strumento di supporto per l'analisi dei dati, senza influenzare la decisione del giudice**

Rapporto tra IA e il diritto d'autore



- Chi sviluppa sistemi di IA, utilizzando opere protette dal diritto d'autore per l'addestramento dei propri modelli ha l'obbligo di dichiararlo esplicitamente.
- I contenuti generati, modificati o ottimizzati tramite IA dovranno essere, sempre, chiaramente identificati con la dicitura "generato con IA",
- per rendere effettivo principio di trasparenza, che mira a proteggere tanto i creatori originali quanto gli utenti finali, che hanno il diritto di conoscere l'origine dei contenuti digitali, o da questi derivati, di cui fruiscono
- i contenuti generati, modificati o ottimizzati tramite IA dovranno essere, chiaramente identificati con la dicitura "generato con IA

La legge 132/2025

oltre che specificare le modalità d'uso dei sistemi AI promuovendo un uso corretto, trasparente e responsabile, lo sviluppo e l'uso dei sistemi AI per finalità generali devono avvenire nel rispetto dei principi costituzionali e dei diritti fondamentali, e in piena coerenza con l'AI Act



sul piano della governance designa:

- **l'Agenzia per la Cybersicurezza Nazionale (ACN) deve vigilare – con poteri ispettivi – sull'adeguatezza e la sicurezza dei sistemi,**
- **AgID avrà cura di gestisce le notifiche e promuovere ca**

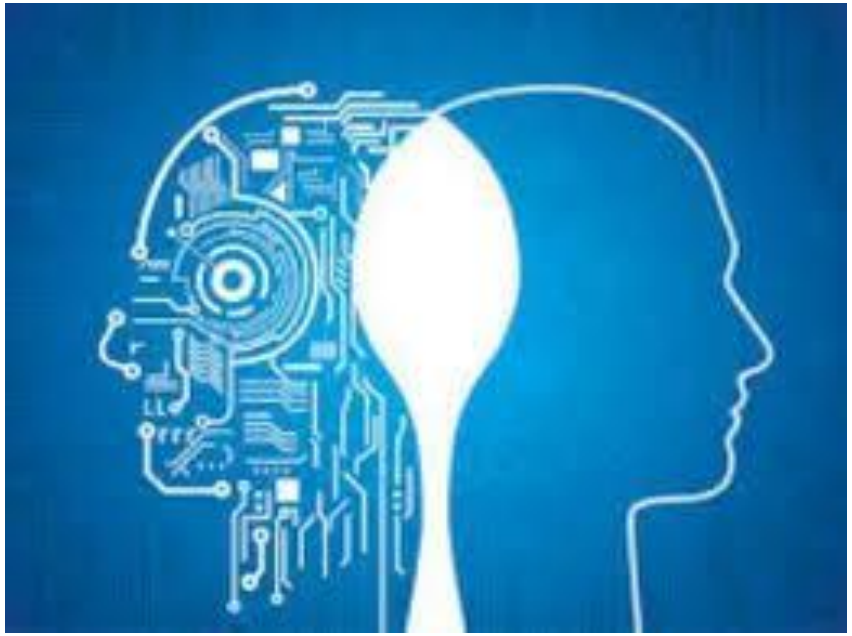
d'uso sicuri per cittadini e imprese, in un quadro di uno stabile coordinamento interistituzionale.

AGID | Agenzia per l'Italia digitale

Sistemi di IA ad alto rischio devono possedere prima di poter essere immessi sul mercato:



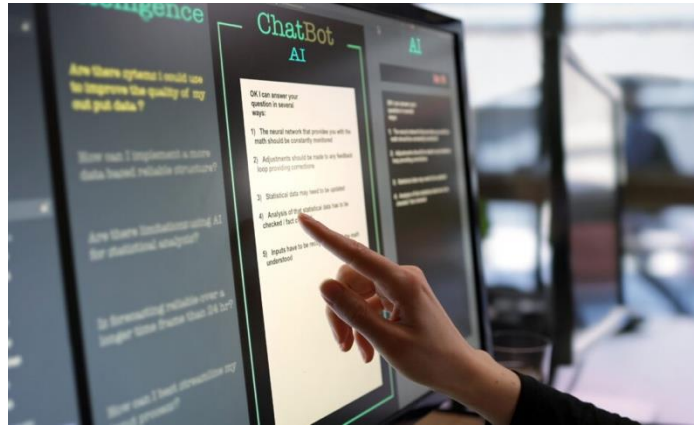
- **adeguati sistemi di valutazione e mitigazione dei rischi d'impatto FRIA ;**
- **elevata qualità delle serie di dati** che alimentano il sistema per ridurre al minimo i rischi e i risultati discriminatori;
- **registrazione dell'attività per garantire la tracciabilità dei risultati;**
- **documentazione dettagliata di tutte le informazioni necessarie sul sistema e sullo scopo per valutarne** la conformità parte autorità;
- **informazioni chiare e adeguate all'operatore**;
- **adeguate misure di sorveglianza umana** per ridurre al minimo il rischio;
- elevato livello di robustezza, sicurezza e precisione.



Obblighi per i sistemi ad alto rischio



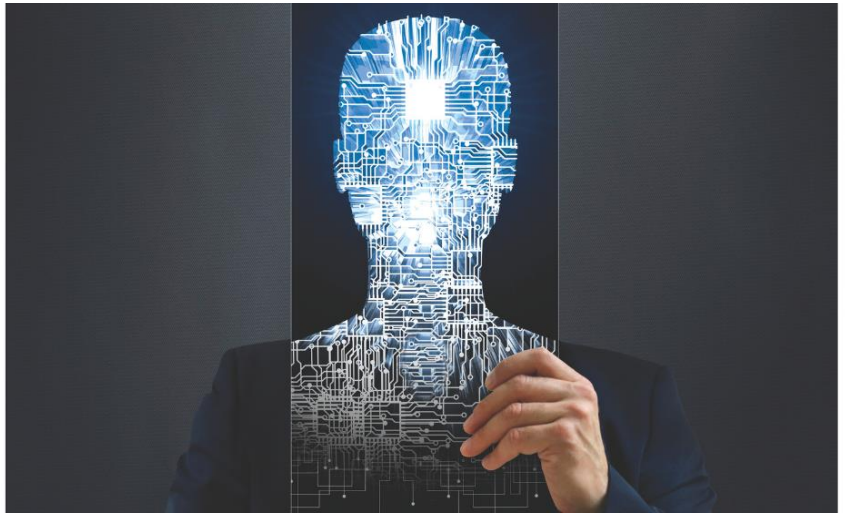
- che potrebbero **arrecare danni significativi alla salute, alla sicurezza, ai diritti fondamentali, all'ambiente, alla democrazia** e allo Stato di diritto
- a infrastrutture critiche, istruzione e formazione professionale, occupazione, servizi pubblici e privati di base (ad esempio assistenza sanitaria, banche, ecc.), alcuni sistemi di contrasto, migrazione e gestione delle frontiere, giustizia e processi democratici (come nel caso di sistemi usati per influenzare le elezioni)
- **valutare e ridurre i rischi, mantenere registri d'uso, essere trasparenti e accurati e garantire la sorveglianza umana.**
- **cittadini hanno diritto a presentare reclami** e a **ricevere spiegazioni sulle decisioni** basate **su sistemi di IA ad alto rischio che incidono sui loro diritti.**



Divieto di determinate tipologie di applicazioni

- che minacciano i diritti dei cittadini, **sistemi di categorizzazione biometrica** basati su caratteristiche sensibili
- **l'estrapolazione indiscriminata di immagini facciali da internet o dalle registrazioni dei sistemi di telecamere** per creare banche dati di riconoscimento facciale.
- i sistemi di riconoscimento delle emozioni sul luogo di lavoro e nelle scuole, i sistemi di credito sociale, le pratiche di polizia predittiva (*se basate esclusivamente sulla profilazione o sulla valutazione delle caratteristiche di una persona)* e i sistemi che manipolano il comportamento umano o sfruttano le vulnerabilità delle persone





La normativa sul piano concreto richiederà



- competenze sempre più specialistiche e un approccio multidisciplinare, in grado di affrontare i problemi che nell'applicazione;
- un contesto giuridico operativo complesso, ma necessario per garantire che l'IA sia sicura, etica e rispettosa dei diritti fondamentali dell'uomo;
- l'uso dei sistemi AI, in particolare deve, sempre, garantire il trattamento lecito, corretto e trasparente dei dati personali;
- di conseguenza le informazioni relative al trattamento dei dati devono essere fornite in modo chiaro e semplice per consentire all'utente di conoscere i relativi rischi e di opporsi al trattamento dei propri dati personali;
- l'accesso ai sistemi AI è vietato ai minori di 14 anni, senza il consenso dei genitori

Legge 132 Art. 4 riservatezza dei dati





L'utilizzo di sistemi IA garantisce il trattamento lecito, corretto e **trasparente dei dati personali** e la **compatibilità con le finalità per le quali sono stati raccolti**, al diritto dell'UE **su dati personali e di tutela della riservatezza.**

Le informazioni e le comunicazioni **relative al trattamento dei dati vanno rese con linguaggio chiaro e semplice**, in **modo da garantire all'utente la conoscibilità dei relativi rischi e il diritto di opporsi ai trattamenti autorizzati** dei propri dati personali.

L'accesso alle tecnologie IA e il trattamento dei dati personali da parte minori:

- di 14 anni quattordici solo con consenso di chi esercita la responsabilità genitoriale sensi REG UE 2016/679 e DL 196/96.
- con più di 14 può esprimere il proprio consenso, solo se le informazioni e le comunicazioni siano facilmente accessibili e comprensibili.

Art 13 Uso IA 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
- per assicurare il **rapporto fiduciario tra professionista e cliente**
- le informazioni relative metodologie d'impiego dal professionista **sono comunicate al soggetto destinatario della prestazione intellettuale con linguaggio chiaro, semplice ed esaustivo**

Art. 15 Impiego IA 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

Ministero Giustizia disciplina

- gli impieghi dei sistemi per l'organizzazione dei servizi relativi per la semplificazione del lavoro giudiziario e per le attività accessorie.
- l'elaborazione delle linee programmatiche sulla formazione e sugli impieghi dei sistemi nell' attività giudiziaria, finalizzate alla formazione digitale di base e avanzata, all'acquisizione e alla condivisione di competenze digitali, nonché alla sensibilizzazione sui benefici e rischi.

Art 16. Delega al Governo in materia di dati, algoritmi e metodi matematici per l'addestramento di sistemi di intelligenza artificiale



- entro 12 dall' entrata in vigore legge **deve emanare decreti legislativi** per definire una disciplina organica relativa all'utilizzo di dati, algoritmi e metodi matematici nel **rispetto** del **Reg UE 2024/1689,**
- per fissare diritti e gli obblighi per chi intenda procedere all' utilizzo;
- prevedere strumenti di tutela, di carattere risarcitorio o inibitorio, e individuare un apparato sanzionatorio in caso **di violazione delle disposizioni**
- attribuire **alle sezioni specializzate in materia di impresa** le controversie relative alla disciplina

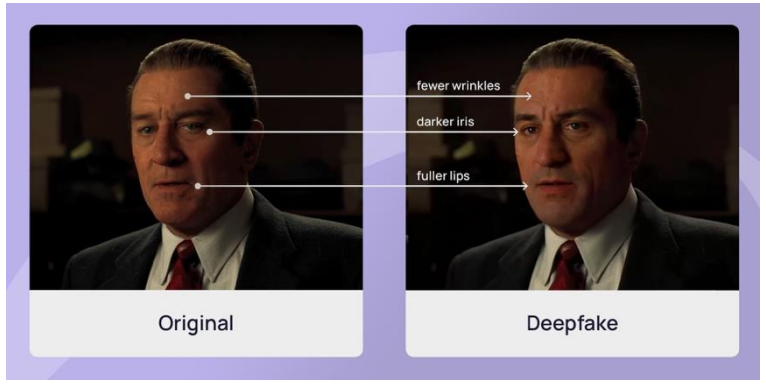


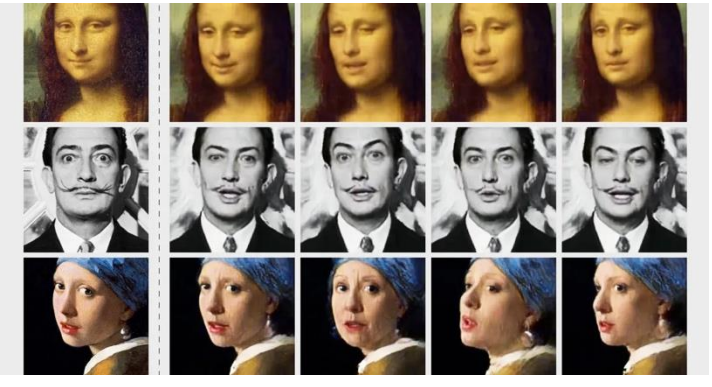
Contrasto al fenomeno deepfake



- inserimento l'art. 612-quater nel codice penale,
- per contrastare la recrudescenza del grave fenomeno di condotte particolarmente lesive della dignità altrui oltre che dell'affidamento dei cittadini
- prevedendo per chi pubblica deepfake (immagini, audio e video) senza il consenso dell'interessato fino a cinque anni di reclusione







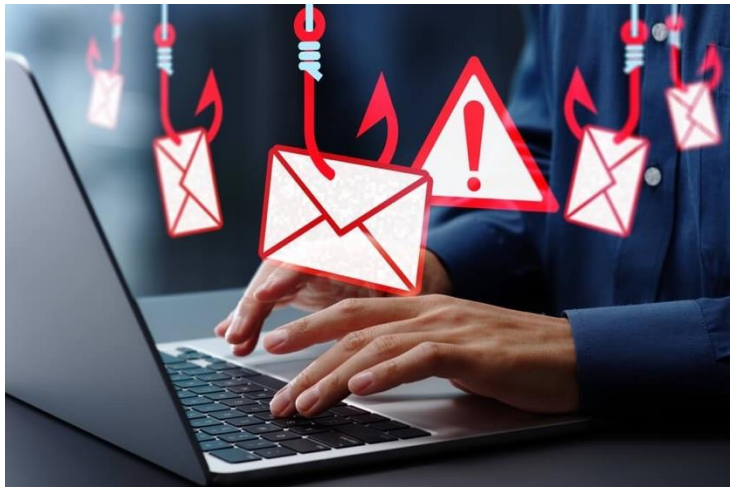
Inserimento circostanza aggravante all’art. 61, cp l’11-decies

“l'avere commesso il reato **mediante l'impiego di sistemi di intelligenza artificiale**, quando gli stessi, per la loro natura o per le modalità di utilizzo, abbiano **costituito mezzo insidioso, ovvero quando il loro impiego** abbia **comunque ostacolato la pubblica** o **la privata difesa**, ovvero **aggravato le conseguenze del reato**

Aumento di 1/3 della pena

Per frenare a recrudescenza dei cyber crimes con modalità di aggressione sempre più incisive e personalizzate grazie IA

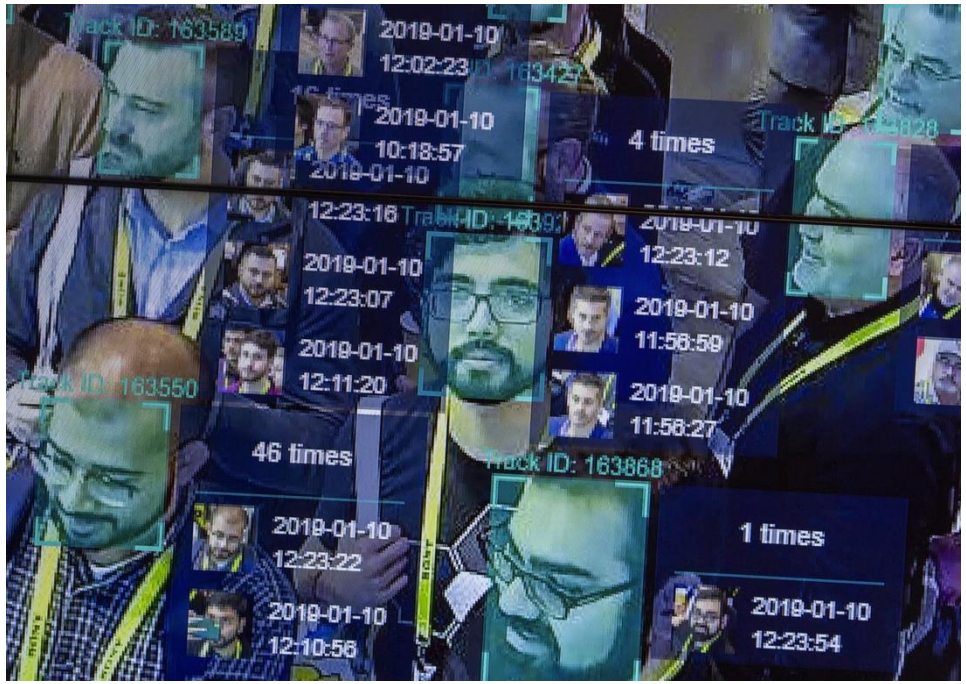




Le forze dell’ordine

- potranno fare **ricorso ai sistemi di identificazione biometrica, nei casi espressamente previste dalla legge**,
- all'identificazione "in tempo reale**" potrà essere utilizzata solo se saranno rispettate garanzie rigorose**, **limitato nel tempo e nello spazio** e **previa autorizzazione giudiziaria**
- usi ammessi includono la ricerca di una persona scomparsa o la prevenzione di un attacco terroristico.
- essendo ad alto rischio, **l'autorizzazione giudiziaria dovrà essere collegata a un reato**.





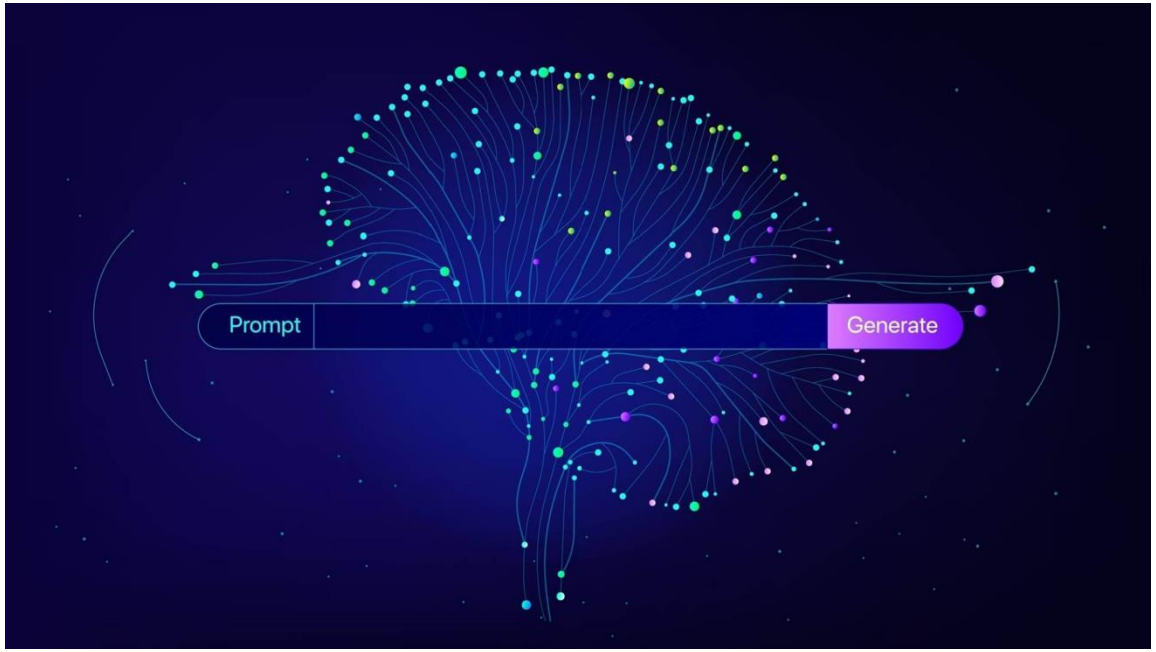
L’ Art. 5 legge 132/2025

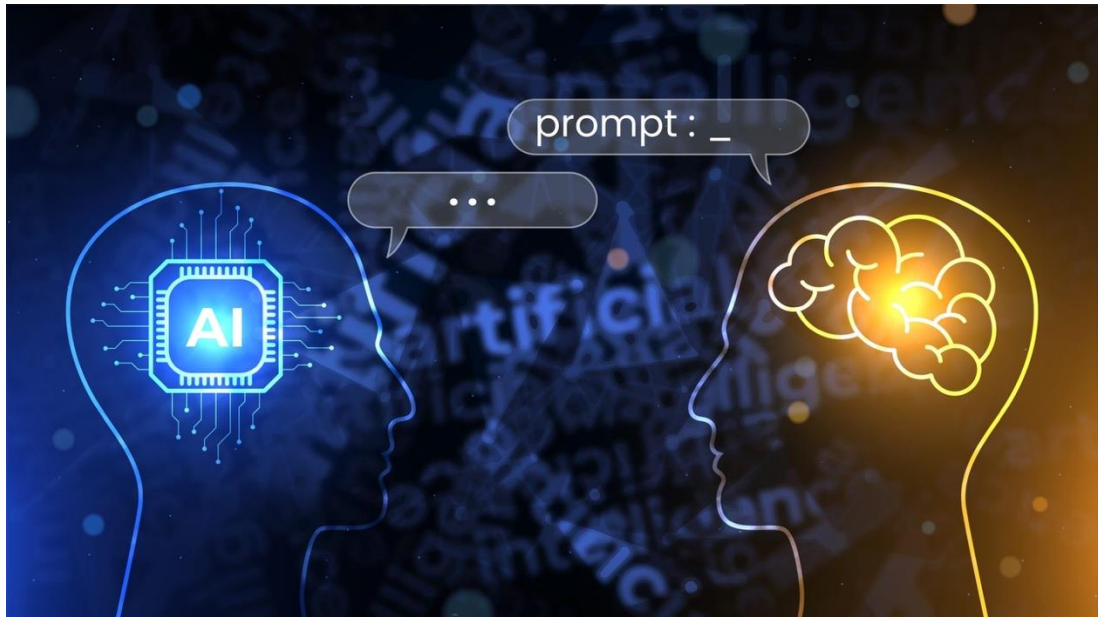


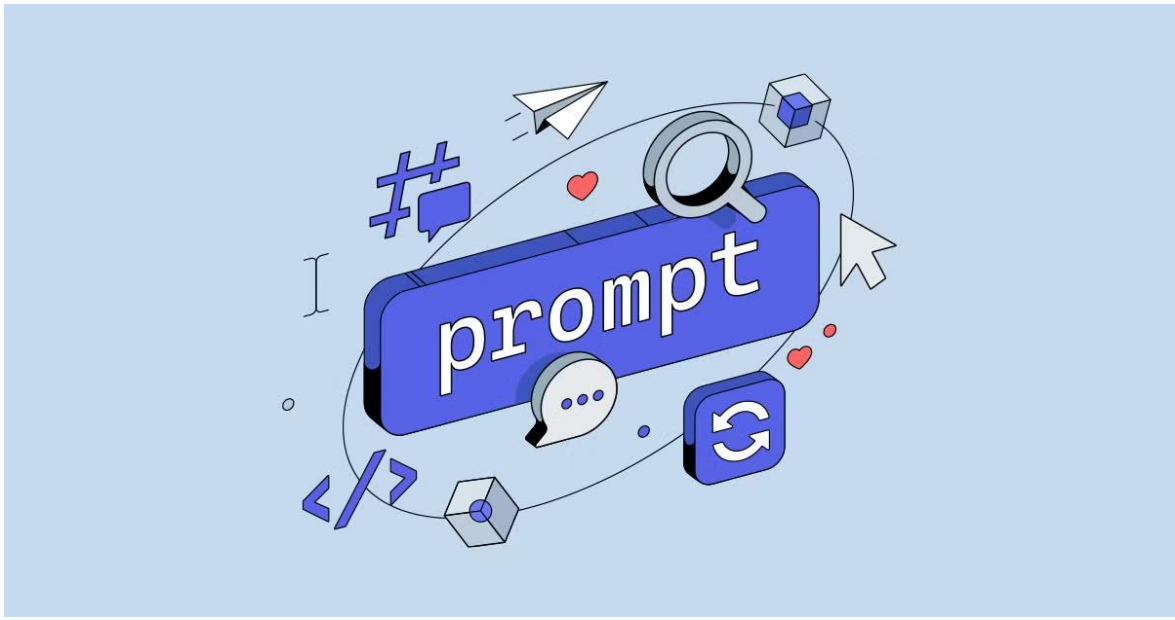
Lo Stato indirizza le piattaforme di e-procurement delle PA in modo che, **nella scelta dei fornitori di sistemi e di modelli IA possano essere privilegiate soluzioni che garantiscono la localizzazione e l'elaborazione dei dati strategici presso data center posti nel territorio nazionale**, le cui procedure di disaster recovery e business continuity siano implementate in data center posti nel territorio nazionale, nonché **modelli in grado di assicurare elevati standard in termini di sicurezza e trasparenza** nelle modalità' di addestramento e di sviluppo delle applicazioni nel **rispetto della normativa sulla concorrenza e dei principi di non discriminazione e proporzionalità**.



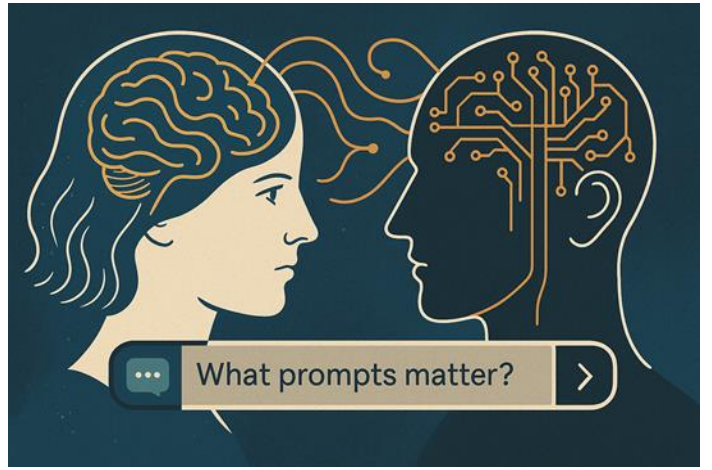
Il prompt
e la responsabilità
dell’atto





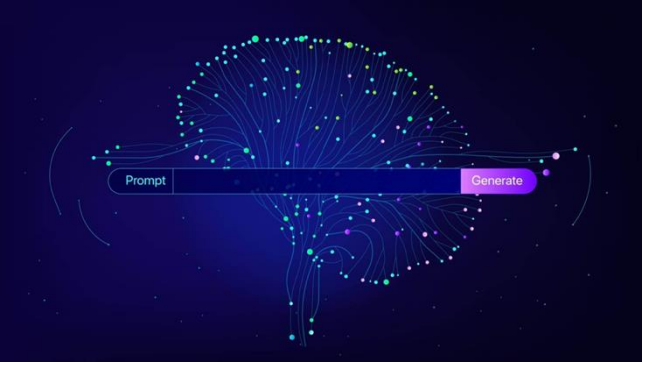


Prompt
per atti di diniego/concessione



1. Per la motivazione di un diniego o di una concessione le **servono i fatti rilevanti**, il procedimento e le norme; **quasi mai il nome della persona**. **È il principio di minimizzazione: solo i dati adeguati, pertinenti e limitati a quanto necessario (art. 5, par. 1, lett. c, GDPR).**
2. Prepara una copia di lavoro, **prima di caricare il documento, sostituisci nomi, codici fiscali, indirizzi e IBAN con segnaposto come [RICHIEDENTE] o [FIGLIO 1] togliere i dati sanitari o giudiziari che non incidono sulla decisione. Attenzione anche ai dettagli che identificano senza nominare: commenti e revisioni, svuota le proprietà del documento, dove restano spesso nomi e versioni precedenti.**

L'originale resta nel fascicolo, in chat la copia. Rimettere i dati reali alla fine, quando la bozza è verificata, nei segnaposto nel gestionale dell'ente, fuori dalla chat.

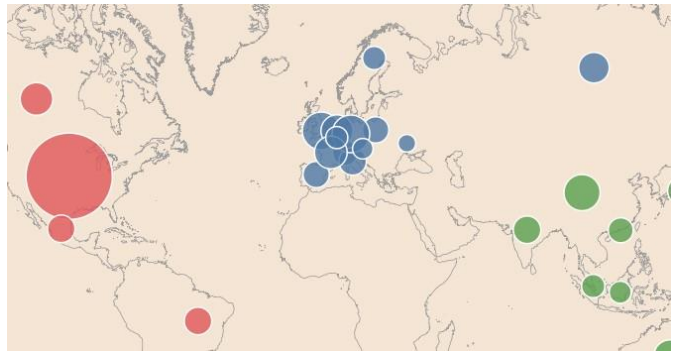


Quale USO dei DATI ?



- **L’uso dei dati degli utenti per addestrare i modelli è escluso per contratto? Chi può vedere cosa si carica? Dove finiscono i documenti caricati, quanto restano nella cronologia e chi può aprirli.**
- Il **GDPR chiede misure tecniche e organizzative adeguate al rischio, tra cui la capacità di assicurare la riservatezza dei sistemi (art. 32)** **accordo sul trattamento dei dati (DPA).**
- **Nella PA l’IA ha funzione strumentale e di supporto all’attività provvedimentale**, e che **la persona resta l’unica responsabile dei provvedimenti (art. 14, comma 2, L. 132/2025);**
- Gli enti devono assicurare agli la **conoscibilità del funzionamento dell’IA** e **la tracciabilità del suo utilizzo (comma 1) e di adottare misure tecniche, organizzative e formative per un uso responsabile (comma 3). un prompt di sistema, attivo per impostazione predefinita, definisce il ruolo IA come supporto**
- IA coaudiva nella redazione dell’atto, ma non compete nelle valutazioni e la responsabilità I **prompt possono aggiungere regole specifiche ,come segnalare i dati mancanti o scovare le allucinazioni**.

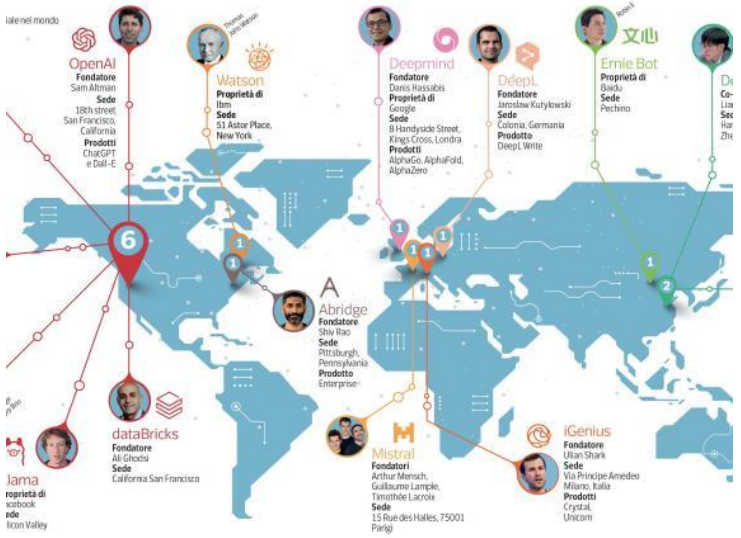
Dove vengono trattati i dati?

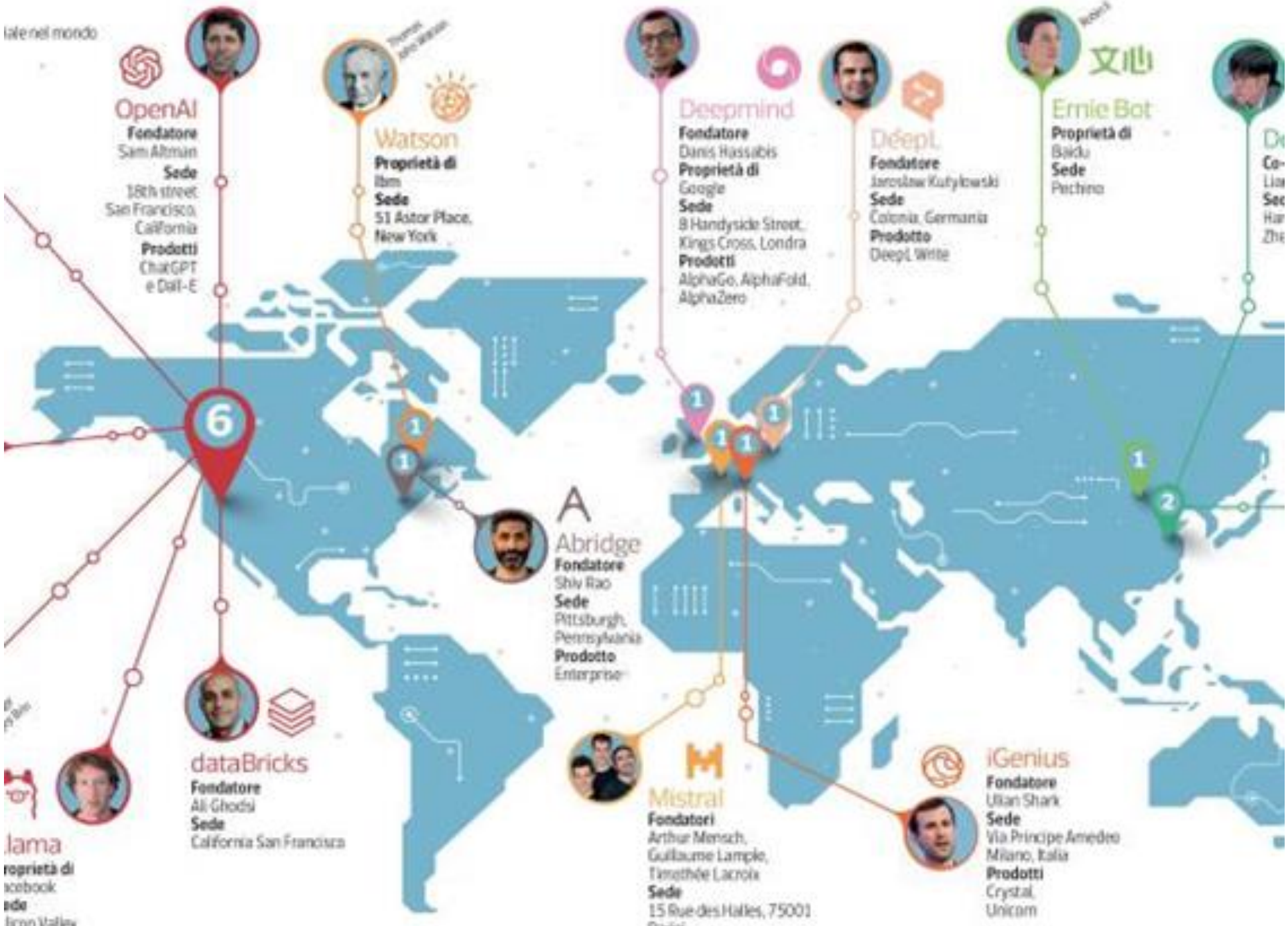


- Dove si trovano i server ? Il GDPR ammette i trasferimenti verso Paesi terzi solo a condizioni precise (artt. 44 e seguenti); nei chatbot generalisti con account personale, quelle condizioni le fissa il fornitore. **Chi può accedere ai dati e da dove, per esempio per assistenza o manutenzione Preferibile cloud con server nell'UE.**



- **Le mie conversazioni addestrano il modello? Controllare le impostazioni dell'account e le condizioni d'uso**, in diversi servizi l'uso delle conversazioni per migliorare i modelli **resta attivo finché l'utente non lo disattiva**.
- Per Il GDPR la **protezione dei dati deve essere assicurata per impostazione predefinita**, senza che sia l'utente a doversene ricordare (art. 25, par. 2).
- Se AI usa le **conversazioni per i propri fini, dati personali consegna a un terzo**, per finalità che l'ente non ha deciso e per le quali difficilmente esiste una base giuridica.



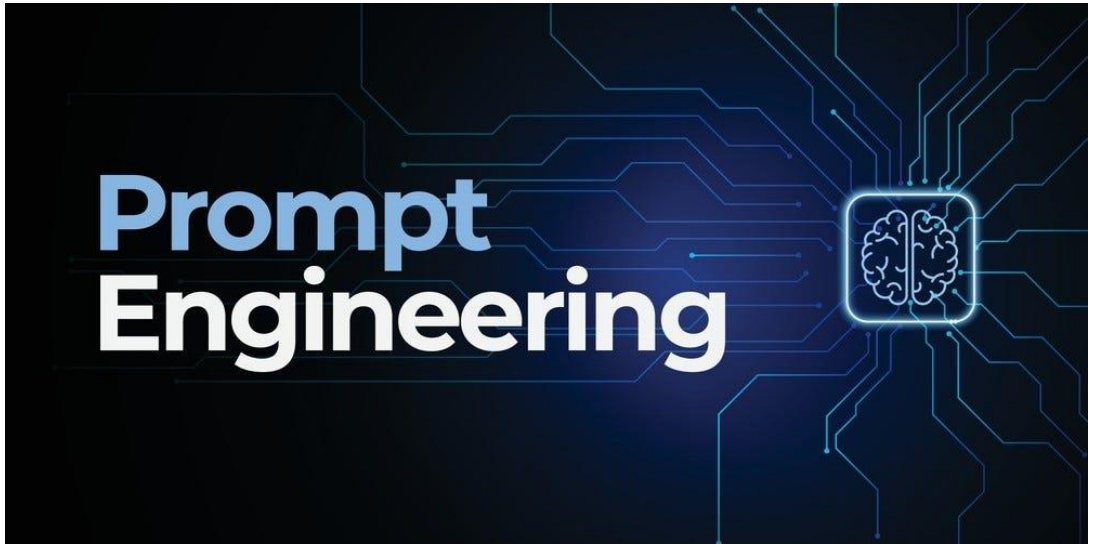

OpenAI
Fondatore
Sam Altman
Sede
18th street
San Francisco,
California
Prodotti
ChatGPT
e Dall-E
Watson
Proprietà di
Ibm
Sede
51 Astor Place,
New York
Deepmind
Fondatore
Danis Hassabis
Proprietà di
Google
Sede
8 Handyside Street,
Kings Cross, Londra
Prodotti
AlphaGo, AlphaFold,
AlphaZero
DéepL
Fondatore
Jarosław Kutylowski
Sede
Colonia, Germania
Prodotto
DeepL Write
Ernie Bot
Proprietà di
Baidu
Sede
Pechino
Abridge
Fondatore
Shiv Rao
Sede
Pittsburgh,
Pennsylvania
Prodotto
Enterprise
dataBricks
Fondatore
Ali Ghodsi
Sede
California San Francisco
Mistral
Fondatori
Arthur Mensch,
Guillaume Lample,
Timothée Lacroix
Sede
15 Rue des Halles, 75001
iGenius
Fondatore
Uljan Shark
Sede
Via Principe Amedeo
Milano, Italia
Prodotti
Crystal,
Unicam

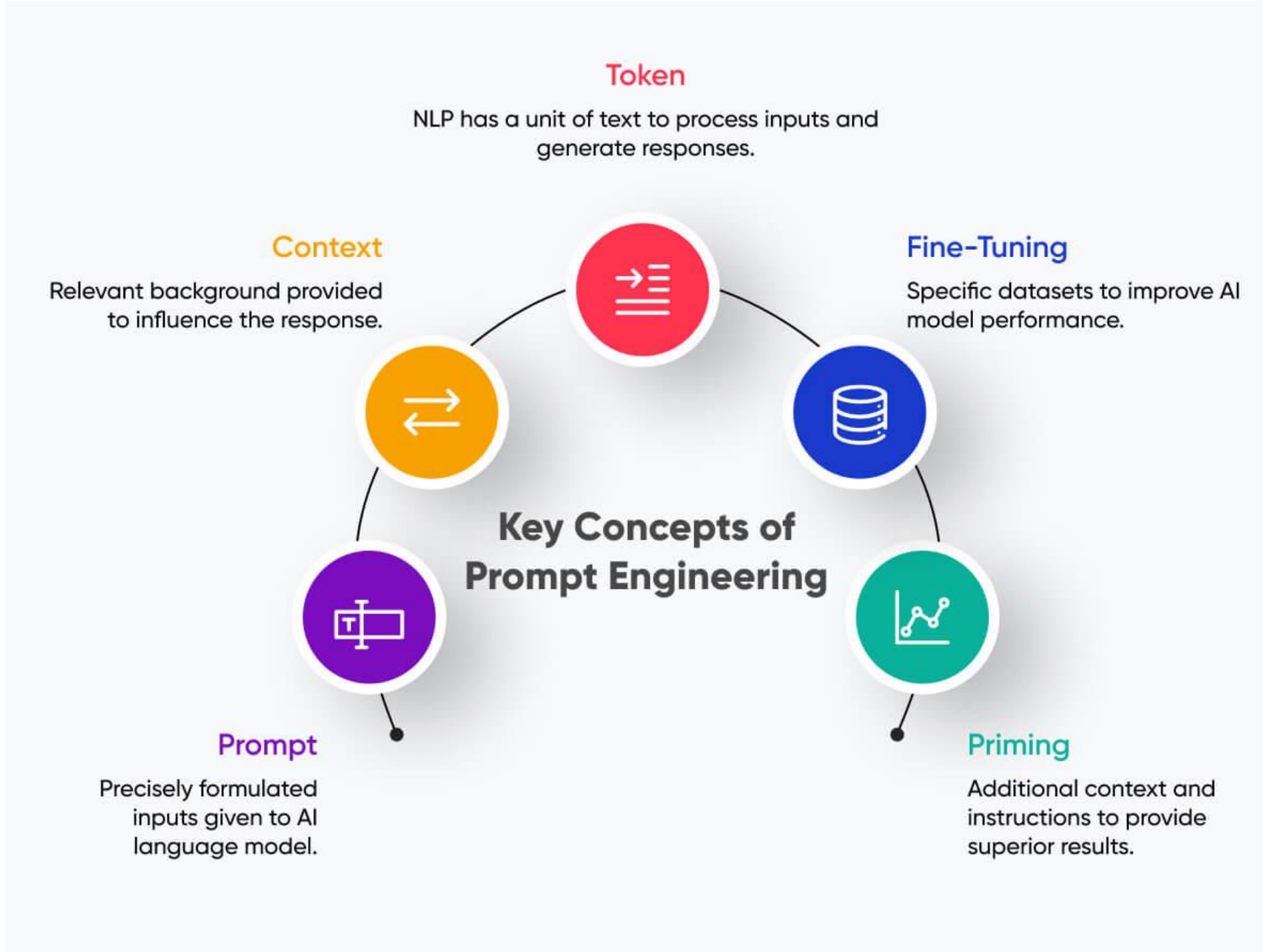
Cos’è il Prompt Engineering

L’arte e la scienza di creare istruzioni che guidano gli LLM a **generare risposte accurate, pertinenti e di alta qualità.** **Chiedere bene a l’AI un assistente efficace ma per ottenere il massimo occorre imparare a comunicare in modo chiaro, preciso e strategico**

Saper scrivere prompt perfetti è una necessità, padroneggiare questa skill permetterà di:

- Ottenere risultati migliori e più velocemente.
- Automatizzare compiti complessi con precisione.
- Sperimentare nuove idee e innovare.
- Sbloccare la creatività e la produttività in modi nuovi.




Token
NLP has a unit of text to process inputs and generate responses.
Context
Relevant background provided to influence the response.
Fine-Tuning
Specific datasets to improve AI model performance.
Key Concepts of Prompt Engineering
Prompt
Precisely formulated inputs given to AI language model.
Priming
Additional context and instructions to provide superior results.

Architettura del prompt

AI non pensa, ma agisce in base alle istruzioni operatore che assume la responsabilità della documentazione

Workflow AI il processo in cui *input, modelli, output, fallback, interventi umani sono registrati e analizzabili*

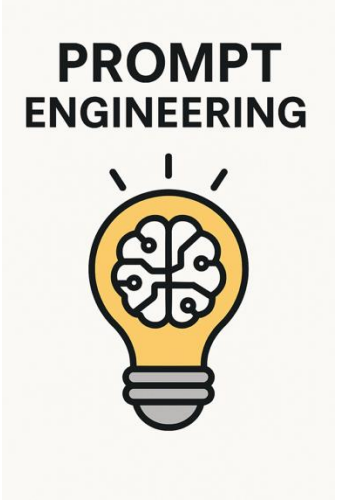
Utilizzo mirato nel rispetto delle norme e ottimizzazione dei prompt

Importanza Contesto :

1. **Epistemico conoscere fatti e dati concreti**
2. **Interpretativo chiarimento termini ambigui**
3. **Operativo definizione dei confini (limiti e vincoli)**
4. **Continuativo mantenere la coerenza**

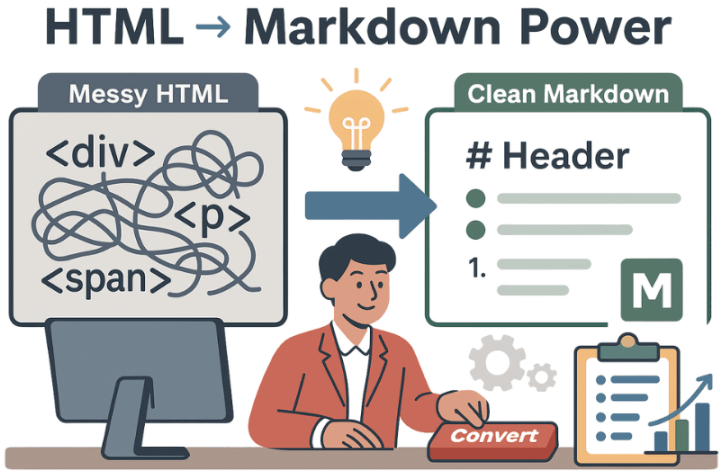


Metodo diagnostico 4 pilastri 4W



- **WHO (Chi è coinvolto e chi agisce**). Definisce sia il ruolo diagnostico che l'IA deve assumere (es. consulente esperto, analista di sistema), sia gli attori colpiti o responsabili del problema. Serve a calibrare il livello tecnico e la prospettiva dell'analisi.
- **WHAT (Cosa sta accadendo e quali sono le prove)**. Delimita la natura esatta del fenomeno, i sintomi osservabili, i dati disponibili e le metriche alterate. Impedisce al modello di fare supposizioni su elementi non presenti nel contesto.
- **WHERE (Dove e in quale contesto si verifica).** Circoscrive il perimetro operativo, l'ambiente (tecnico, aziendale, geografico o di processo) e le condizioni al contorno in cui il problema si manifesta.
- **WHY (Perché è rilevante e qual è l'obiettivo).** Esplicita l'impatto del problema, la sua gravità e il risultato finale desiderato dalla diagnosi (es. individuare la causa radice, valutare i rischi, proporre azioni correttive

Regole per ottimizzare l'efficacia



Separare i fatti dalle interpretazioni. Nel blocco WHAT solo dati oggettivi e lascia che sia l'IA a dedurre le correlazioni nella fase di ragionamento.•

Attivare la modalità "Self-Ask" (Auto-interrogazione). Se non hai tutti i dati delle 4W, aggiungi un'istruzione che imponga all'IA di farti delle domande mirate per colmare i vuoti informativi prima di emettere il verdetto.•

Includere il "When" (Quando) se necessario. In diagnosi tecniche o di processo dove la sequenza temporale è decisiva (es. dopo un ggiornamento software o un cambio di gestione), puoi espandere il blocco WHERE in WHERE & WHEN

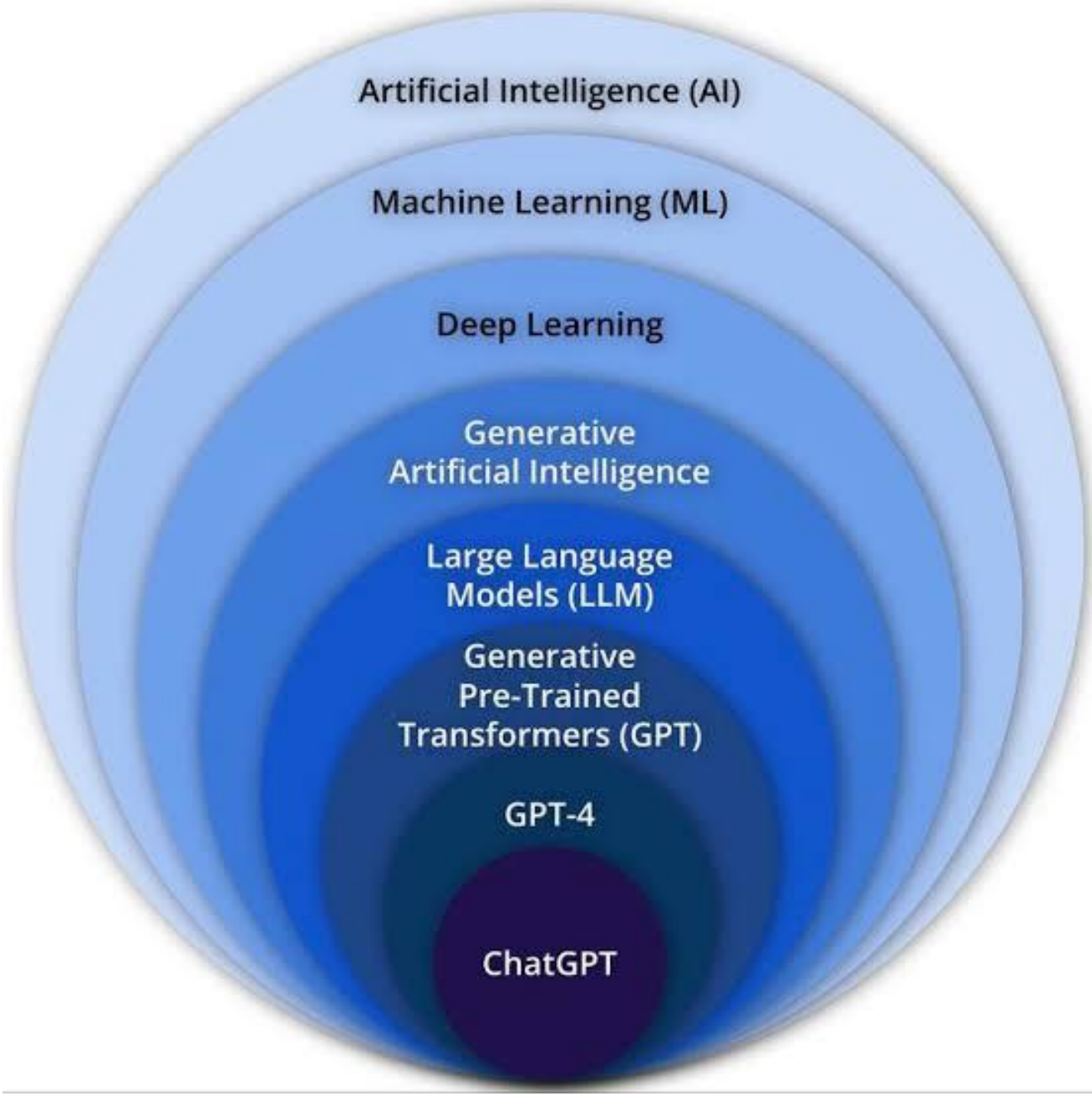
Template operativo pronto all'uso Markdown



Linguaggio di marcatura leggero (creato nel 2004 da John Gruber e Aaron Swartz) che permette di formattare il testo (grassetto, corsivo, elenchi, link) usando simboli semplici, senza scrivere codice HTM

- # RUOLO E OBIETTIVO Agisci come un [inserire ruolo, es. Senior Business Analyst / Ingegnere di Sistema]. Il tuo compito è eseguire una diagnosi strutturata del seguente scenario utilizzando rigorosamente il metodo delle 4W, prima di proporre qualsiasi soluzione.
- # CONTESTO DIAGNOSTICO (4W)* **WHO (Attori e Target):** [Chi riscontra il problema, chi gestisce il processo, chi sono gli utenti finali]* **WHAT (Sintomi ed Evidenze):** [Descrizione oggettiva dell'anomalia, dati raccolti, cosa non funziona come previsto]* **WHERE (Perimetro e Ambiente):** [Sistema, reparto, fase del processo o canale in cui si verifica il problema]* **WHY (Impatto e Urgenza):** [Conseguenze sul business/progetto, perché è critico risolverlo ora, obiettivo da raggiungere]
- # ISTRUZIONI DI RAGIONAMENTO 1. Analizza le interazioni tra le 4W sopra elencate ed evidenzia eventuali informazioni mancanti o ambigue. 2. Formula 3 ipotesi sulle possibili cause radice (Root Cause), ordinandole per probabilità. 3. Indica quali verifiche pratiche effettuare per confermare o escludere ciascuna ipotesi
- # FORMATO DI OUTPUT Presenta analisi in modo schematico usando elenchi puntati e una tabella

- # RUOLO E OBIETTIVO Agisci come un [inserire ruolo, es. Senior Business Analyst / Ingegnere di Sistema]. Il tuo compito è eseguire una diagnosi strutturata del seguente scenario utilizzando rigorosamente il metodo delle 4W, prima di proporre qualsiasi soluzione.
- # CONTESTO DIAGNOSTICO (4W)
- * **WHO (Attori e Target):** [Chi riscontra il problema, chi gestisce il processo, chi sono gli utenti finali]
- * **WHAT (Sintomi ed Evidenze):** [Descrizione oggettiva dell'anomalia, dati raccolti, cosa non funziona come previsto]
- * **WHERE (Perimetro e Ambiente):** [Sistema, reparto, fase del processo o canale in cui si verifica il problema]
- * **WHY (Impatto e Urgenza):** [Conseguenze sul business/progetto, perché è critico risolverlo ora, obiettivo da raggiungere]
- # ISTRUZIONI DI RAGIONAMENTO
- 1. Analizza le interazioni tra le 4W sopra elencate ed evidenzia eventuali informazioni mancanti o ambigue.
- 2. Formula 3 ipotesi sulle possibili cause radice (Root Cause), ordinandole per probabilità.
- 3. Indica quali verifiche pratiche effettuare per confermare o escludere ciascuna ipotesi.
- # FORMATO DI OUTPUT
- Presenta la diagnosi in modo schematico usando elenchi puntati e una tabella finale di sintesi (Ipotesi | Evidenza a supporto | Test di verifica).



GUIDA PER SCRIVERE PROMPT EFFICACI

1. OBIETTIVO

Qual è il risultato desiderato?

2. RUOLO / PERSONA

Es: "Agisici come un esperto di..."

3. CONTESTO

Dai informazioni rilevanti

4. ISTRUZIONE PRINCIPALE

L'azione chiara da compiere

5. FORMATO DELL'OUTPUT

Lista, Tabella, Codice...

6. VINCOLI E LIMITI

Regole e restrizioni

7. ESEMPI

Mostra esempi utili

8. ITERAZIONE

Migliora e perfeziona

Predisposizione Prompt efficaci:

1. **Chiarezza e Specificità**: Più sei specifico, migliori saranno i risultati: "*Genera un breve riassunto (massimo 150 parole) degli aspetti ….. sulle cause principali e sulle sue conseguenze*"

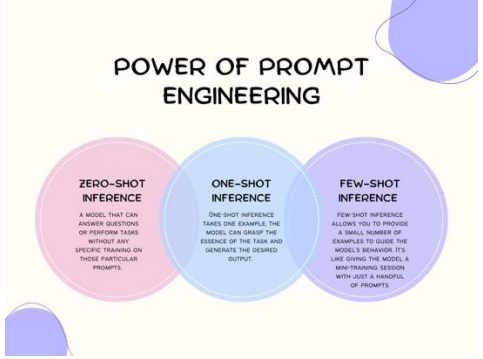
2. Definire il Ruolo (Persona): Chiedere all'LLM di assumere un ruolo specifico può influenzare drasticamente il tono, lo stile e il contenuto della sua risposta, fondamentale per ottimizzare i prompt. *Es. "Agisci come un esperto di marketing digitale specializzato in SEO. Forniscimi 5 idee per argomenti di blog su 'content marketing per piccole imprese' che siano ottimizzati per i motori di ricerca e che includano keyword a bassa concorrenza."*

3. **Fornire Contesto**: **dare un quadro generale l'** LLM non conosce background o esigenze specifiche a solo con contesto rilevante aiuterà l'AI a capire la richiesta e a generare una risposta più utile. *Es: "Sono il proprietario di un piccolo caffè artigianale a Milano. Vorrei delle idee per campagne promozionali su Instagram per attirare nuovi clienti durante il weekend. Concentrati su promozioni per la colazione e il brunch."*

4 Specificare il Formato dell'Output: non lasciare che l'LLM decida il formato. Se hai bisogno di una lista, di un testo formattato in Markdown, di un codice o di una tabella, chiedilo esplicitamente. *Es.: "Elenca i 3 principali benefici dell'esercizio fisico regolare come una lista puntata. Per ogni beneficio, scrivi una breve frase esplicativa di massimo 20 parole*."

5. Impostare Limiti e Vincoli: dare delle regole chiare, non aver paura di specificare limiti di lunghezza, numero di elementi, o di escludere certi argomenti. Questo è cruciale per scrivere prompt perfetti. *Esempio: "Genera un tweet (massimo 280 caratteri, senza hashtag) che annunci il lancio di un nuovo software di gestione progetti, evidenziando la sua facilità d'uso."*

Iterazioni con gli LLM:



6. Iterazione e Raffinamento: il primo tentativo raramente è perfetto Il Prompt Engineering è un processo iterativo, esaminare, controllare migliorare, modificare il prompt, aggiungi dettagli, cambia il ruolo, specifica il formato, **ogni iterazione avvicinerà al risultato migliore.**

Es.per la Generazione di Contenuti Marketing: "*Sei un copywriter esperto in annunci Facebook. Crea 3 varianti di testo per un annuncio che promuove un webinar gratuito sul 'cloud computing per startup'. Il target è costituito da CEO di piccole imprese. Ogni variante deve essere concisa (max 100 parole), includere un forte invito all'azione e una emoji pertinente. Evita il gergo eccessivamente tecnico.*"

Per lo Sviluppo Software: "*Agisci come uno sviluppatore Python senior. Scrivi una funzione Python per convalidare un indirizzo email, verificando la presenza di '@' e '.' e che non contenga spazi. Includi un docstring che spieghi la funzione e fornisci 2 esempi di utilizzo.*"

Per la Ricerca e la Sintesi: "*Riassumi i punti salienti del rapporto IPCC 2023 sul cambiamento climatico in non più di 200 parole. Presenta le informazioni come tre paragrafi distinti: risultati principali, impatti previsti e raccomandazioni. Utilizza un linguaggio accessibile, adatto a un pubblico non scientifico.*"

Forme di Prompt Engineering più evolute:

Few-shot prompting: Fornire all'LLM alcuni **esempi di input-output desiderato** prima della richiesta.

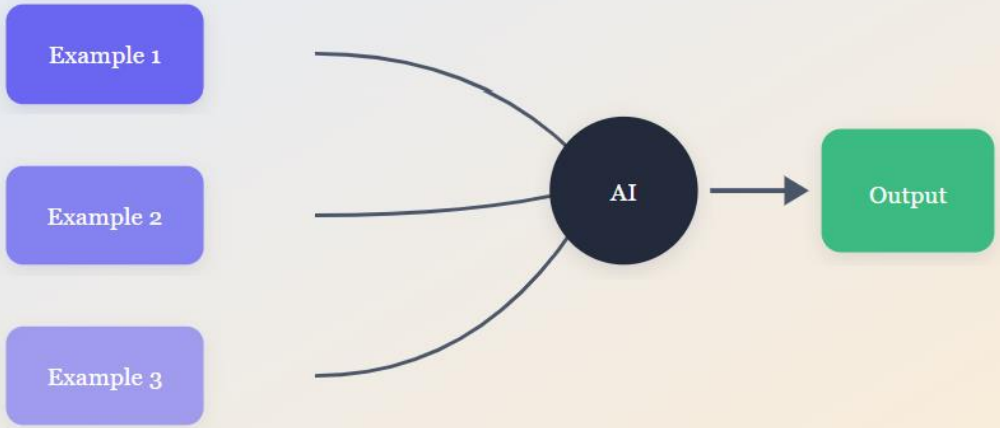
Chain-of-thought prompting: Chiedere all'LLM di **"pensare ad alta voce"** o di **spiegare il suo ragionamento passo dopo passo, migliorando l'accuratezza per problemi complessi.**

Tree-of-thought prompting: Una tecnica ancora più avanzata che permette all'LLM **di esplorare diversi percorsi di ragionamento, come un albero decisionale.**

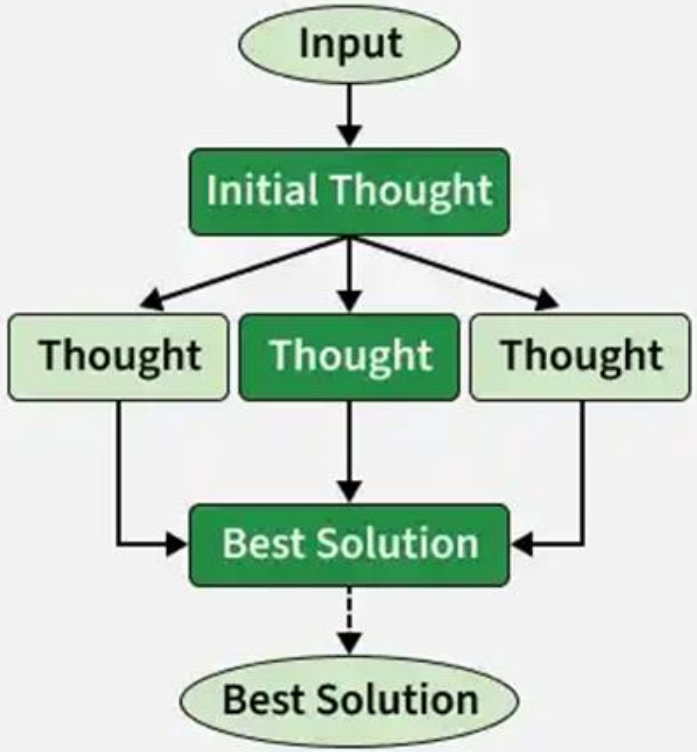


Few-Shot Prompting

Show a few, learn the pattern



Tree of Thought (ToT) Prompting



Obblighi di trasparenza

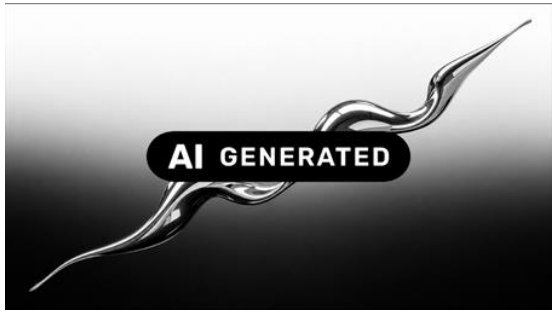
Art.50 impone obblighi di trasparenza adimensionali per fornitori , imprese e Pubbliche Amministrazioni, **l'obiettivo è rendere chiaro agli utenti l'origine sintetica dei contenuti.**

Commissione ha rilasciato un Code of Practice:

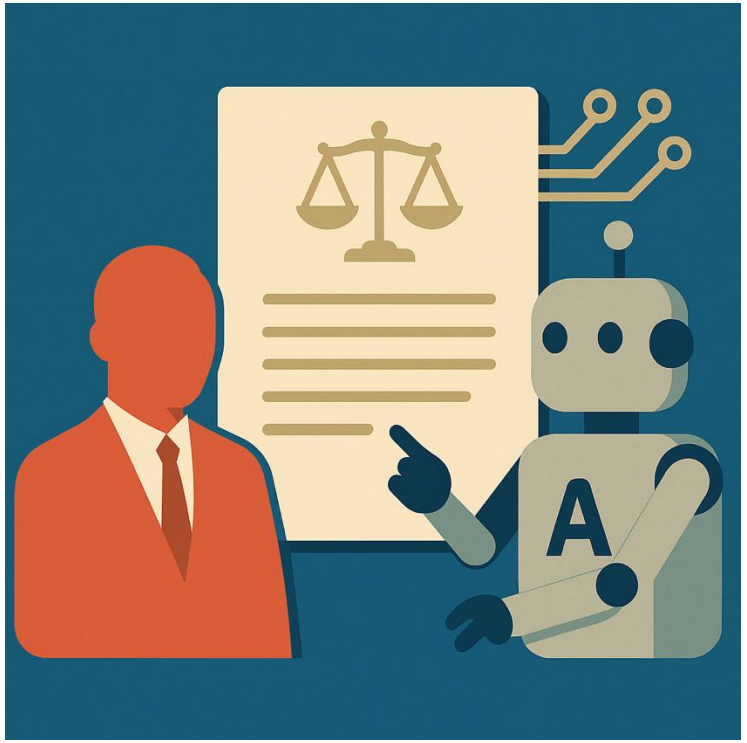
- **Sistemi che interagiscono con persone fisiche come i *chatbot"servizio di informazioni gestito da intelligenza artificiale"..***
- **Generazione di contenuti audio/video, immagini o testi vanno marcati tecnicamente, garantirne la rilevabilità e la resistenza alle modifiche con metadati protetti da firma digitale e watermark steganografici.**
- **Riconoscimento, categorizzazione e trattamento di emozioni, dati biometrici, dati personali, per sistemi alto rischio.**
- **Deep fake contenuti visivi o acustici che alterano la realtà apparendo falsamente autentici. l'applicazione delle icone "AI Generated", "AI Modified»**

Scadenza con Digital Omnibus del 29 giugno 2026 .

- dal 2 agosto 2026, sono gli sui contenuti generati dall'AI;
- per quelli già immessi nel mercato al 2 dicembre 2026,



IL TRACCIAMENTO
l'uso dell'IA va tracciato

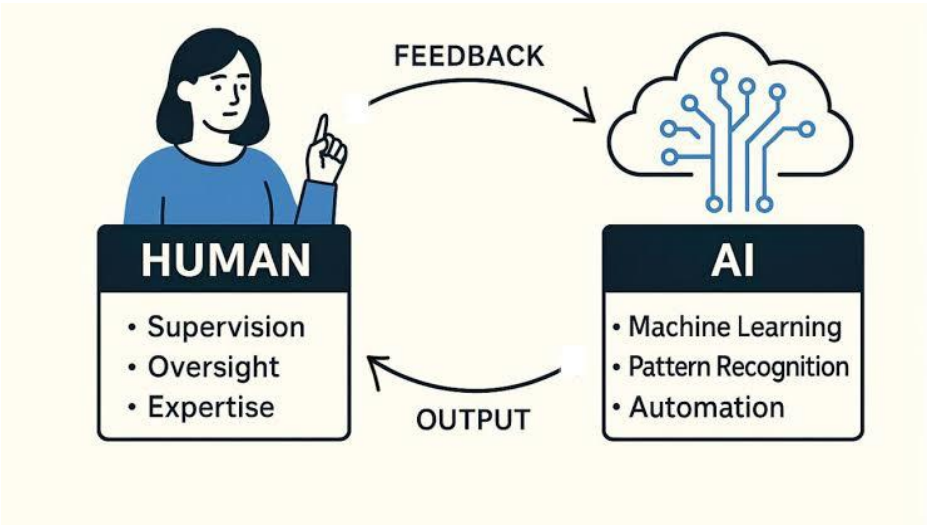


Art. 14 della legge 132/2025, chiede alle PA di usare l'intelligenza artificiale «**assicurando agli interessati la conoscibilità del suo funzionamento e la tracciabilità del suo utilizzo»**

L'etichetta riguarda il singolo testo pubblicato e, come abbiamo visto, può non servire; **la tracciabilità riguarda l'ente e vale anche per l'atto rivisto e firmato,**

Annotando nel fascicolo, o in un registro interno, quali atti sono stati preparati con il supporto AI e chi li ha rivisti.

Human in the loop





Etichetta



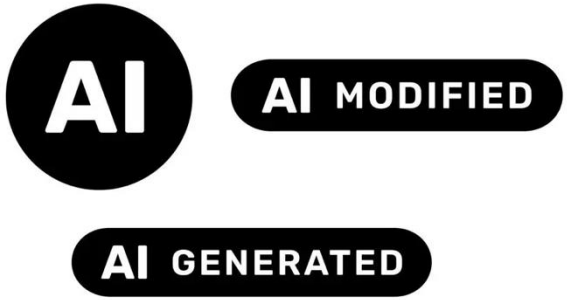
Il Codice di buone pratiche EU sulla trasparenza dei contenuti generati dall'IA, adeguato a dimostrare il rispetto dell'articolo 50 se vi sono tre requisiti:

1. **Pubblicato: testo è accessibile a un numero indeterminato di persone, come accade per il sito istituzionale**, i profili social dell'ente o una pagina pubblica. *la PEC di risposta a un cittadino, la comunicazione al singolo richiedente e la mail interna non sono pubblicate, quindi restano fuori dal perimetro*.

2. Scopo di informare il pubblico: testo serve a comunicare fatti, conoscenze o opinioni a chi lo legge.comunicati, notizie e avvisi alla cittadinanza hanno quasi sempre questo scopo.

3. Riguarda questioni di interesse pubblico: rilevante per la collettività e meritevole di dibattito pubblico. la *chiusura delle scuole per allerta meteo o le nuove regole della raccolta differenziata*.

Etichetta

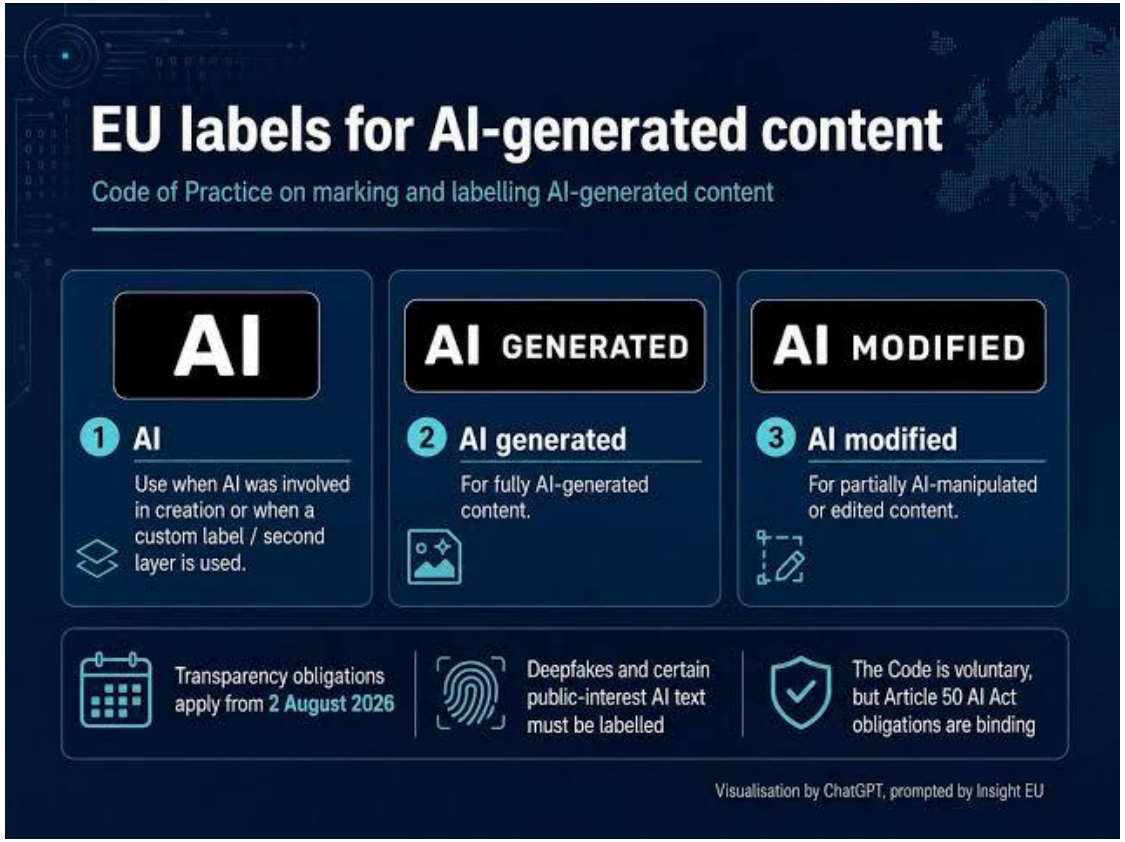


La Commissione mette a disposizione icone ufficiali, utilizzabili liberamente:

1. **quella di base, "Fully AI-Generated" per i testi interamente generati**

2. **"Partially AI-Modified" per quelli scritti da una persona e modificati in parte con l'IA.**

3. **Le icone portano la sigla inglese "AI", perciò conviene affiancarle sempre una frase in italiano, *per esempio "Testo generato con l'intelligenza artificiale" oppure "Testo redatto da [ufficio] e in parte rielaborato con l'intelligenza artificiale".***



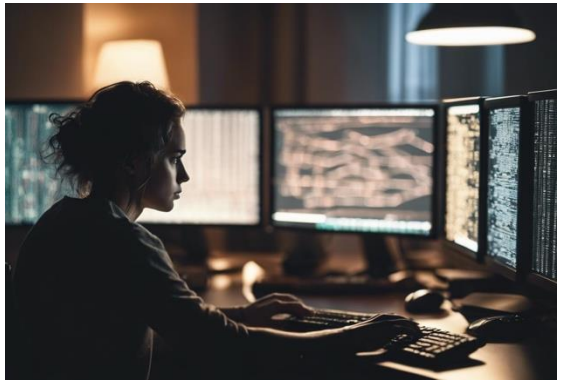
L'etichetta va messa vicino al titolo o all'inizio del testo, deve vedersi subito, senza cliccare nulla, e deve restare visibile anche se il contenuto viene scaricato o condiviso. Per chi usa un lettore di schermo serve anche il testo alternativo

Revisione umana.



- L’obbligo di etichetta non si applica se il testo è stato sottoposto a revisione umana o a controllo editoriale e una persona ne assume la responsabilità.
- Nella Pubblica Amministrazione la persona «resta l’unica responsabile dei provvedimenti e dei procedimenti» in cui è stata utilizzata l’IA (art. 14, comma 2, L. 132/2025).
- L’asticella della revisione e vale per gli atti come per i comunicati.

L'ABC DELLA REVISIONE



- **Verifica i fatti**. Il requisito minimo è il controllo del contenuto: correggere i refusi, dare una scorsa veloce o approvare con un clic non basta.
- **Metti un nome.** Chi ha la responsabilità va indicato per un atto, di norma, è chi lo firma; per il sito, chi ne cura i contenuti, con un recapito nelle note legali o nella pagina della redazione.
- **Scrivi la regola**. Il Codice chiede adottare e pubblicare regole interne chiare su chi ha la responsabilità e su come avviene la revisione..
- Non ripassare dall'IA. Se, dopo la revisione, il testo viene di nuovo modificato in modo sostanziale con l'IA, l'eccezione cade.
- **Perché conta: l'eccezione premia un controllo AUTENTICO**. Il passaggio umano non si deve ridurre a un'approvazione formale, altrimenti l'etichetta torna obbligatoria.

Revisione con IA

Ti incollo un testo che l’ente intende pubblicare su [CANALE].

È stato preparato [MODALITÀ: interamente con l’IA / scritto da un operatore e rielaborato in parte con l’IA] e [REVISIONE: è stato / non è stato] verificato nei fatti da [RUOLO DI CHI LO HA RIVISTO].

Valuta soltanto se ricorrono i tre requisiti dell’obbligo di trasparenza previsto per i testi dall’articolo 50 dell’AI Act: pubblicazione, scopo di informare il pubblico, questioni di interesse pubblico. Rispondi con una tabella di tre righe: requisito, presente o assente, motivo in una frase. Poi proponi una sola dicitura di trasparenza, di non più di due righe, e indica dove collocarla. Se dalle informazioni che ti ho dato non risulta chi ha rivisto il testo, scrivi [DA VERIFICARE] e non considerare avvenuta la revisione. Non citare altre norme e non riscrivere il testo.

A Visual Guide to Prompt Engineering

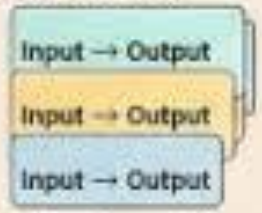
CORE PROMPTING METHODS

Zero-Shot Prompting

Asking the model a direct question without providing any examples.



Few-Shot Prompting



Including a few input/output examples to teach the model the desired pattern.



Chain of Thought (CoT) Prompting

Instructing the model to explain its reasoning step-by-step before giving an answer.



ADVANCED REASONING FRAMEWORKS

Retrieval-Augmented Generation (RAG)

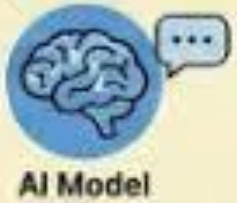
The model fetches external data before answering, ensuring up-to-date information.





ReAct (Reason + Action)

The model reasons through a problem and takes actions, such as using tools.





Tree of Thoughts

The model explores and evaluates multiple reasoning paths to find the best solution.



Grazie per l'attenzione

fratonifabrizio@gmail.com

Colonnello dei Carabinieri e Criminologo Senior certificato norma UNI 11783/2020

