



Intelligenza Artificiale nell'AI Act: Quali Tecnologie Comprende?

L'Intelligenza Artificiale sta rivoluzionando il nostro mondo, e l'AI Act europeo mira a regolamentarne l'uso. Questa presentazione esplorerà le tecnologie chiave dell'IA, il loro impatto e come l'AI Act le influenzerà. Esamineremo anche il ruolo cruciale della supervisione umana e l'importanza della personalizzazione e del controllo nell'era dell'IA.

Chi Sono



CEO di Memori.AI

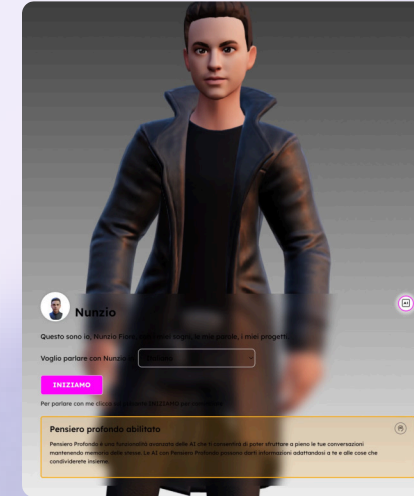
Nunzio Fiore, leader di un'azienda specializzata nella personalizzazione e controllo dei Large Language Models (LLM).

Quello qui sopra **NON SONO IO!**



Aisuru

Soluzione per personalizzare e controllare i contenuti generati dall'AI Generativa.



Focus Aziendale

Semplificare l'accesso alle tecnologie di AI Conversazionali sfruttandole come nuovo media di distribuzione della conoscenza.



Principi Chiave dell'AI Act

1 Progettazione dei Sistemi IA

I sistemi IA devono consentire la supervisione umana durante il loro funzionamento.

2 Scopo della Supervisione

Garantire l'uso corretto dei sistemi IA e affrontare gli impatti durante il ciclo di vita.

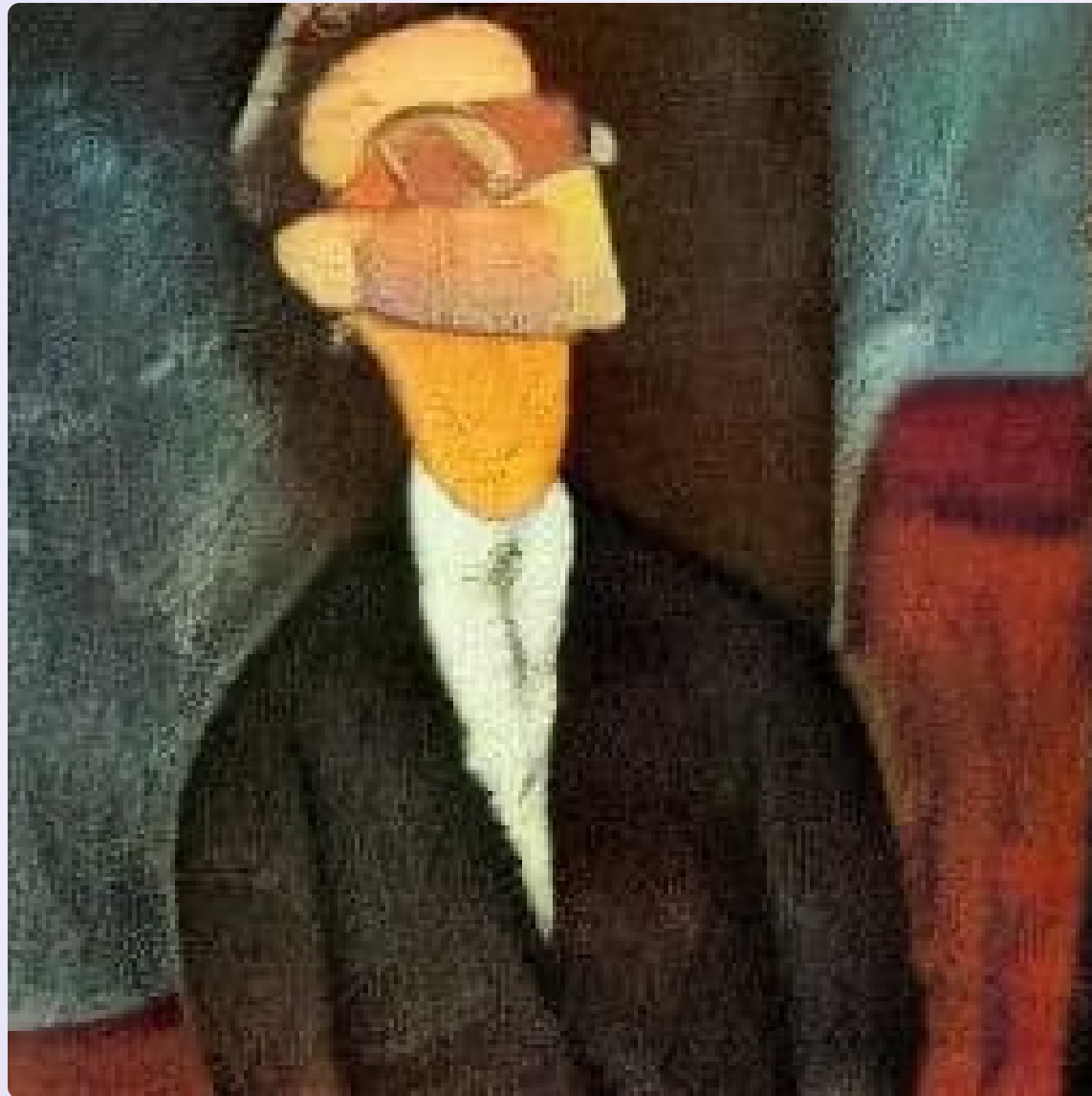
3 Competenze e Formazione

Le persone incaricate della supervisione devono avere competenze, formazione e autorità adeguate.

4 Meccanismi di Guida

I sistemi IA devono includere strumenti per guidare e informare i supervisori umani.

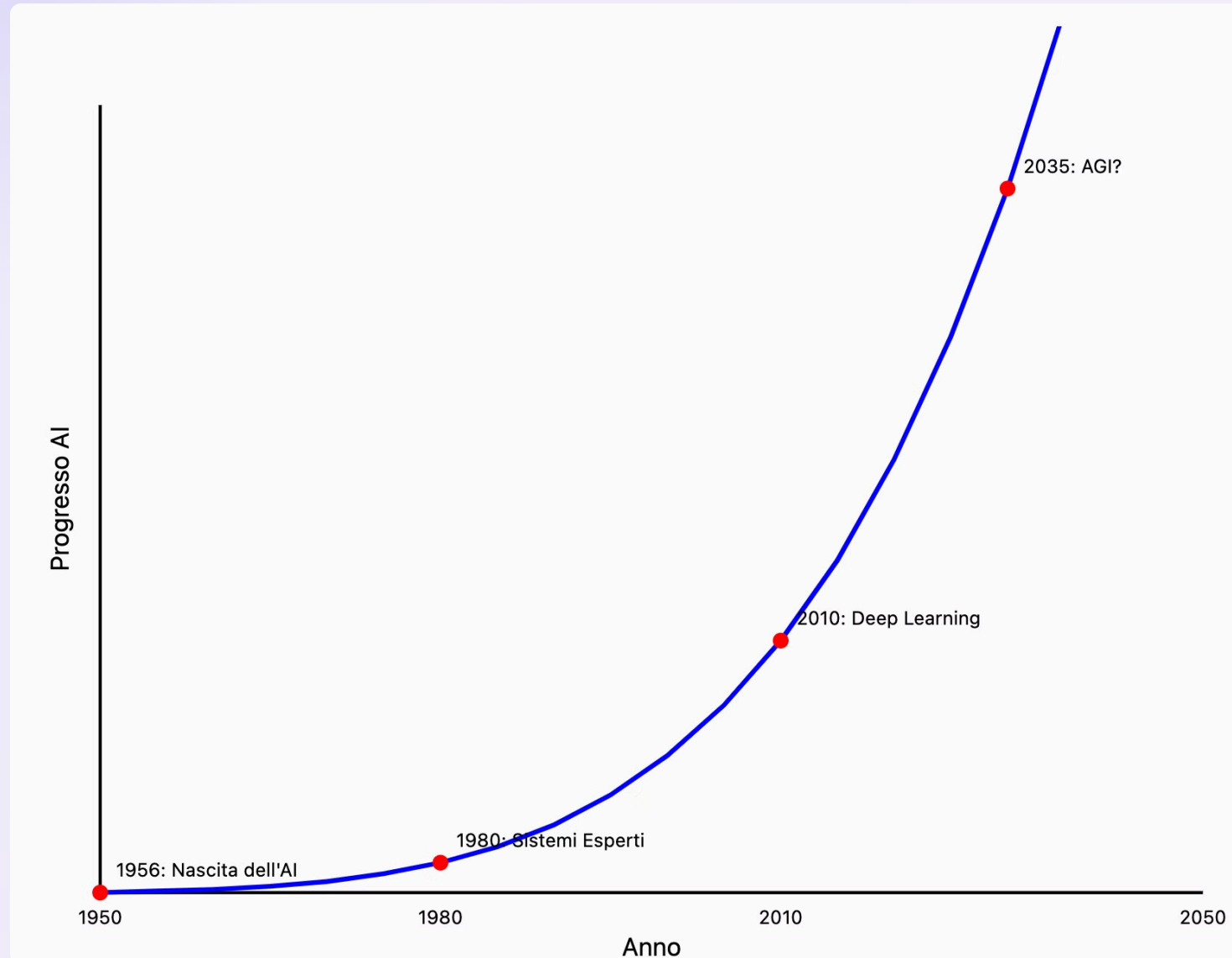
Bono Vox come se lo avesse dipinto Modigliani (2020)



Mio padre non si è accorto che non ero io (2024)



Lo stesso vale per gli LLM



Valori di Aisuru e AI Act

Trasparenza

Distinzione tra contenuti generati da umani e IA, con verifica e manutenzione.

Obblighi e Rischi

Garanzia di accuratezza dei contenuti e valutazione dei rischi dei sistemi IA.

Supervisione Umana

Lavoro con l'IA in un contesto controllato, con verifica e personalizzazione dei contenuti.

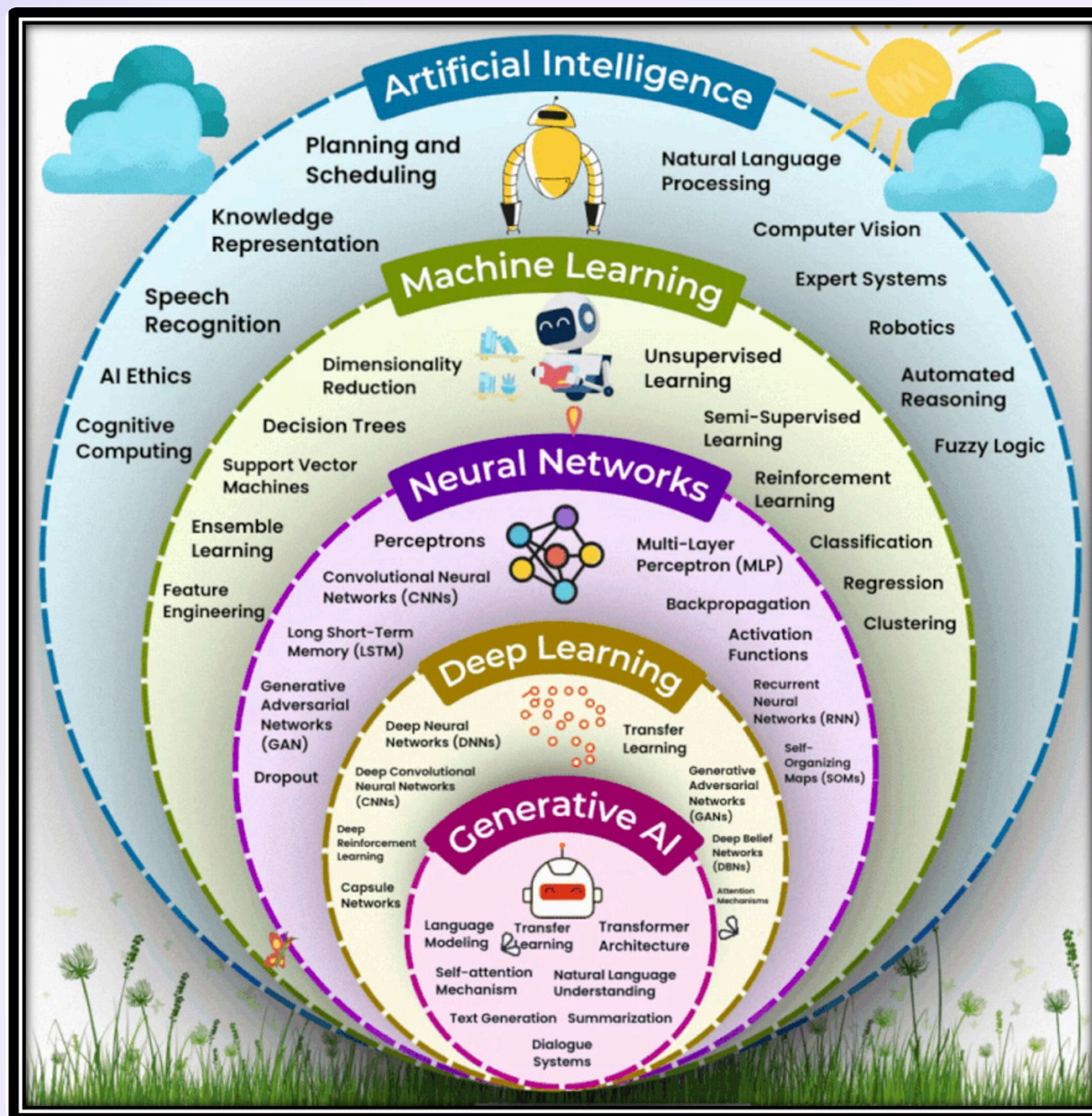
È solo un meme?

 Datapizza

Meta **non rilascerà** la sua nuova AI **in Europa**



Il Mondo dell'AI è in HYPE



PER CAPIRLO DOVREMO SMONTARLO!

Machine Learning e Deep Learning

Machine Learning

Il Machine Learning è un ramo dell'intelligenza artificiale che permette ai computer di imparare dai dati e migliorare le proprie prestazioni su un compito specifico senza essere esplicitamente programmati.

SEMPLIFICANDO: Il machine learning comprende se un oggetto è simile a qualcosa con cui è stato addestrato.

Deep Learning

Il Deep Learning è un sottoinsieme avanzato del Machine Learning basato su reti neurali artificiali con molti strati (da cui il termine "deep", profondo). Queste reti sono progettate per elaborare dati in modo simile al cervello umano, apprendendo rappresentazioni sempre più astratte dei dati man mano che si procede attraverso gli strati.

SEMPLIFICANDO: Il deep learning può generare e prevedere un oggetto simile a qualcosa con cui è stato addestrato.



Natural Language Processing (NLP)

Definizione

Il Natural Language Processing è un campo dell'IA che si concentra sull'interazione tra computer e linguaggio umano.

Assistenza Clienti

Chatbot e sistemi di risposta automatica per supporto clienti 24/7.

Analisi Sentimenti

Valutazione automatica delle opinioni e delle emozioni espresse nei testi.

Traduzione Automatica

Sistemi avanzati per la traduzione in tempo reale tra diverse lingue.

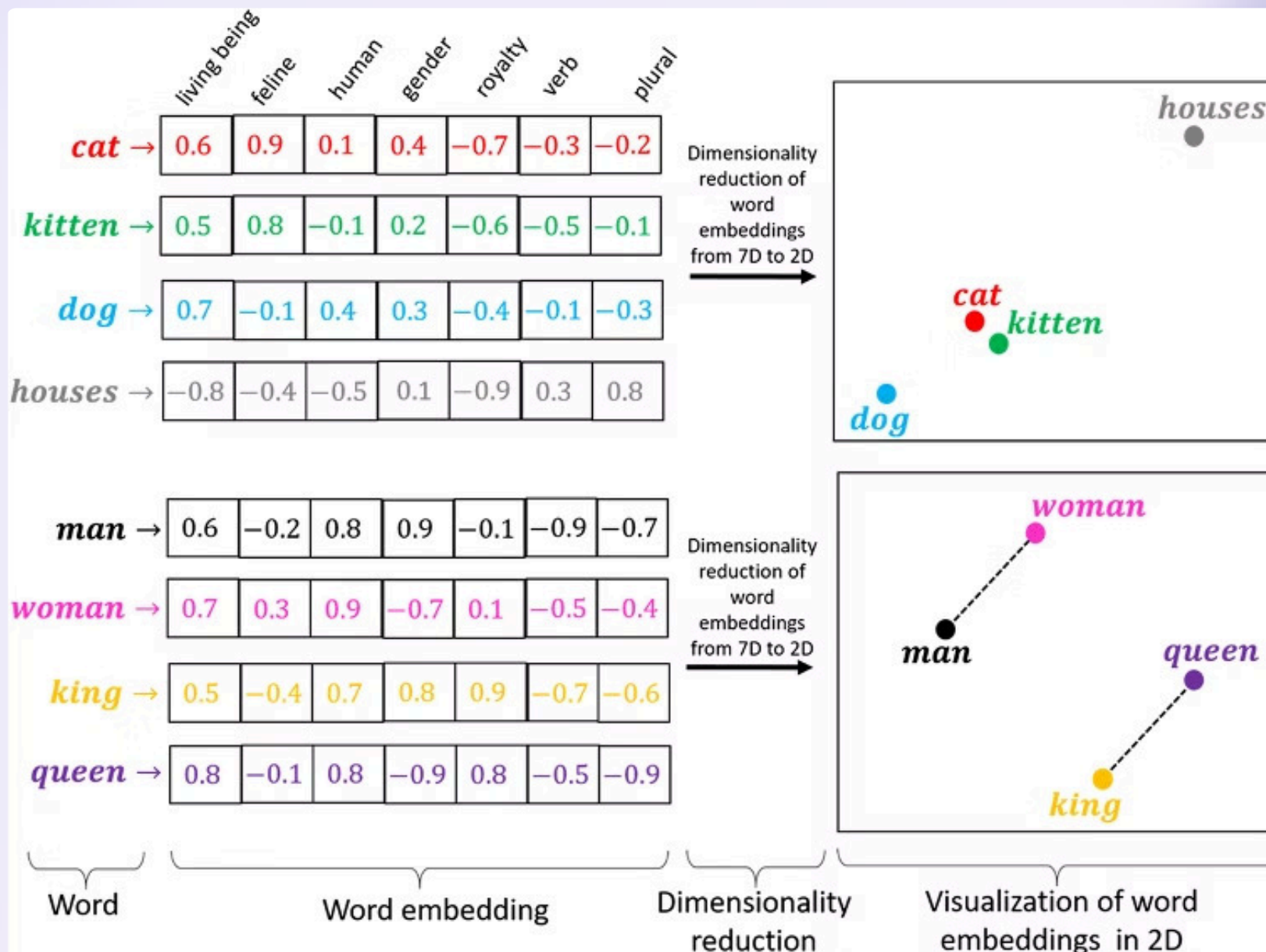
Reti Neurali e Word Embeddings

Reti Neurali

Le reti neurali sono modelli computazionali ispirati al funzionamento del cervello umano. Sono composte da nodi interconnessi che elaborano e trasmettono informazioni.

Word Embeddings

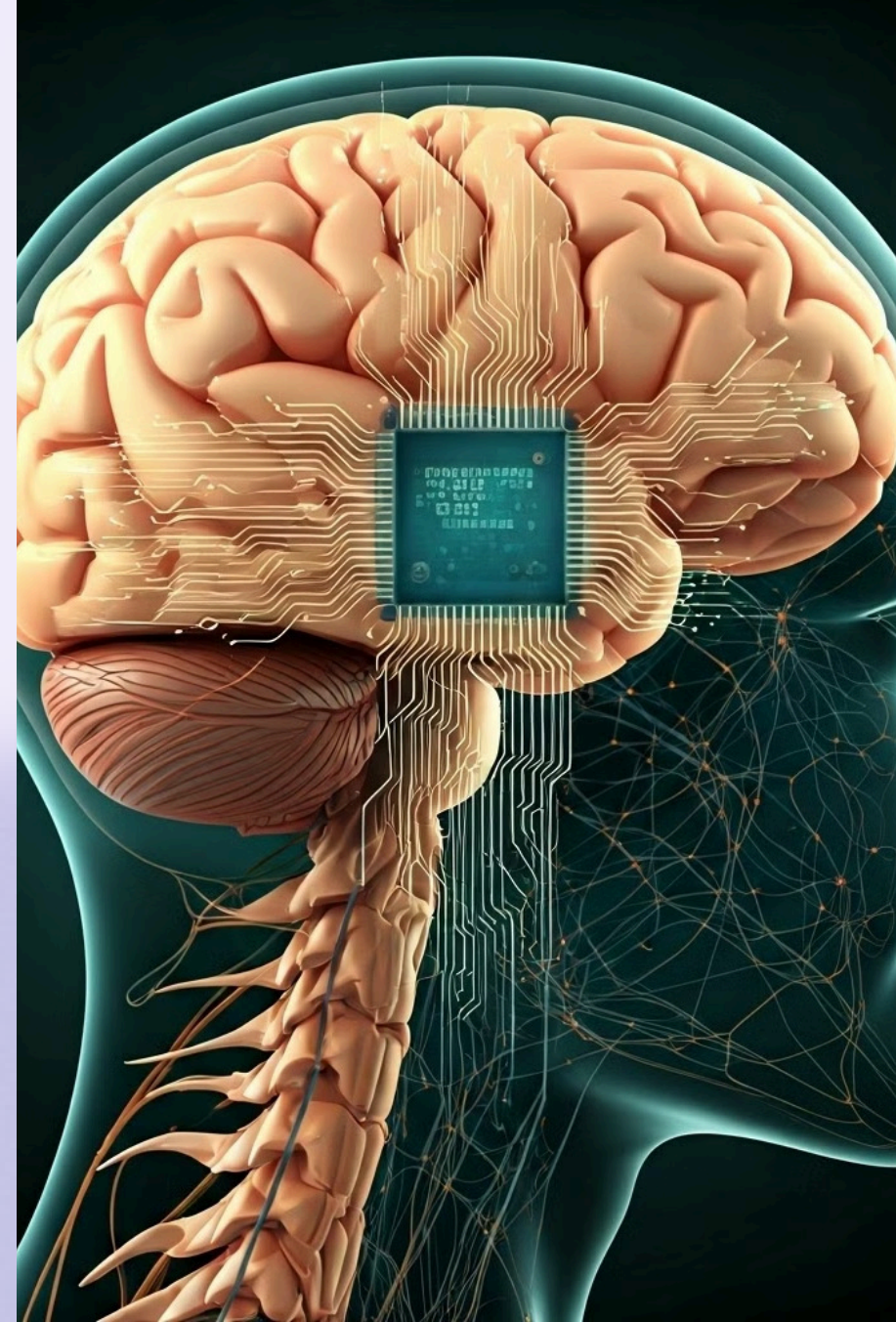
I Word Embeddings sono rappresentazioni vettoriali delle parole nello spazio multidimensionale. Catturano relazioni semantiche e sintattiche tra le parole, permettendo ai modelli di comprendere il contesto e il significato.



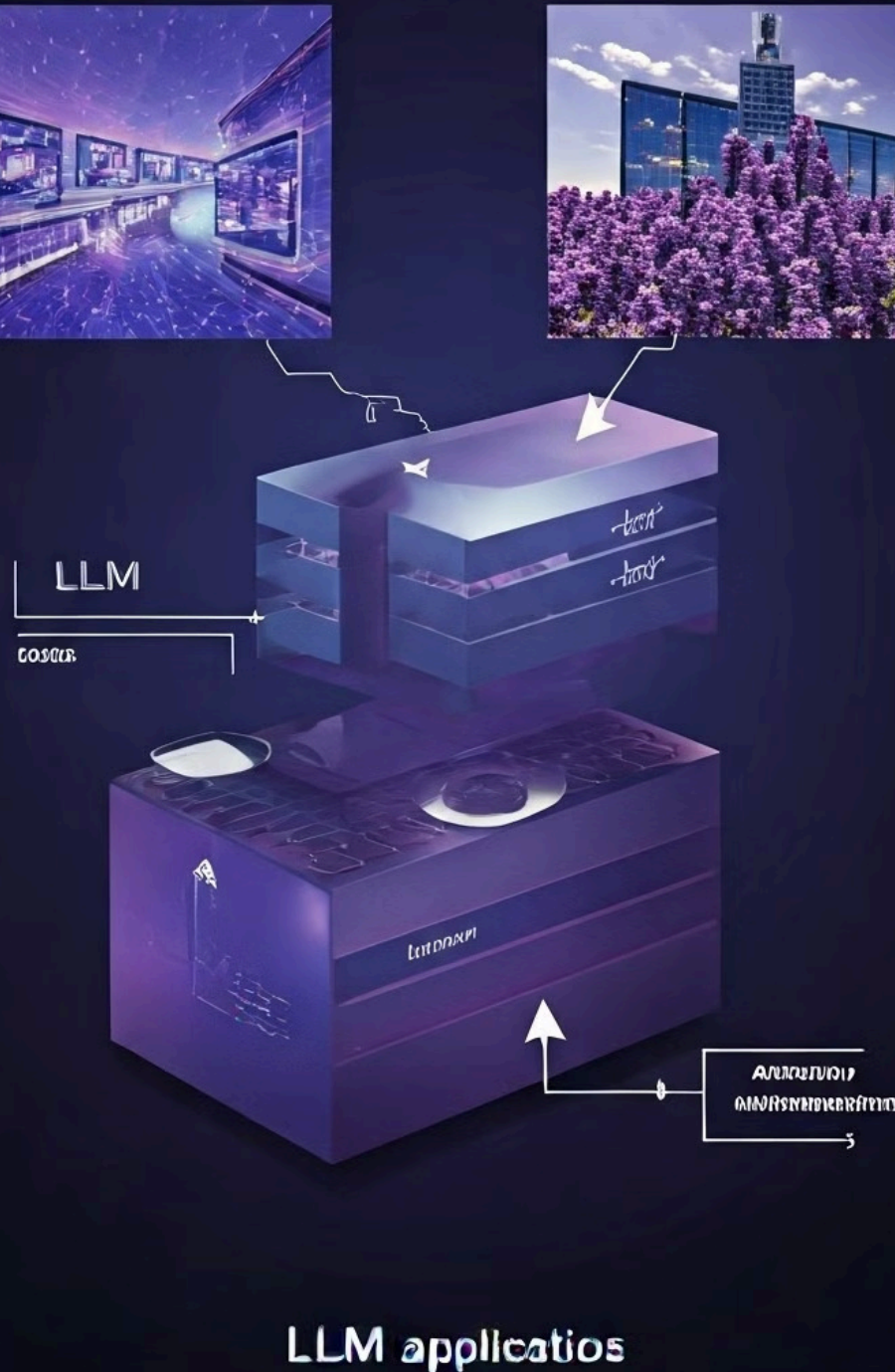
L'interazione uomo macchina da sempre mima il funzionamento del cervello

Il cervello umano fa esattamente la stessa cosa: esiste nel cervello un'area, detta Area di Wernicke, che contiene una mappa semantica delle parole

lo sappiamo perché le persone che hanno danni nell'Area di Wernicke mostrano un tipo particolare di afasia, detta "afasia fluente", in cui quello che dicono è pronunciato perfettamente ma privo di senso. Confondono il significato delle parole, pur sapendole pronunciare correttamente. È un danno alla mappa semantica delle parole.



Transformer Architecture



Transformer e Modelli Linguistici

1

Tecnologia Transformer

I Transformer sono un'architettura di rete neurale che ha rivoluzionato l'elaborazione del linguaggio naturale. Utilizzano meccanismi di attenzione per processare sequenze di testo in parallelo, migliorando efficienza e performance.

2

Large Language Models (LLM)

I modelli linguistici di grandi dimensioni, come GPT, sono basati su architetture Transformer e addestrati su enormi quantità di dati testuali. Possono generare testo coerente e svolgere una varietà di compiti linguistici.

3

Impatto e Applicazioni

Gli LLM hanno aperto nuove possibilità in campi come la generazione di contenuti, la traduzione automatica e l'assistenza virtuale, portando l'IA a nuovi livelli di comprensione e generazione del linguaggio.

Retrieval-Augmented Generation (RAG)

Concetto RAG

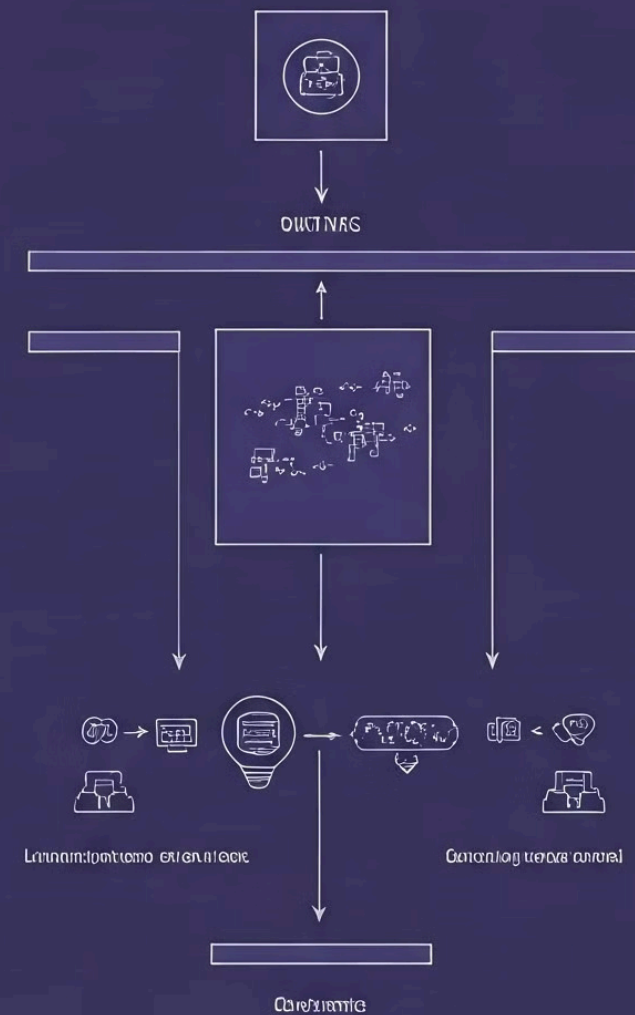
RAG combina il recupero di informazioni da una base di conoscenza con la generazione di testo da parte di un modello linguistico.

Funzionamento

Il sistema recupera informazioni pertinenti e le utilizza come contesto per generare risposte più accurate e informate.

Vantaggi

Migliora l'accesso alle informazioni, riduce le allucinazioni AI e aumenta l'affidabilità delle risposte generate.



LLM: Non Solo OpenAI

Ecco la tabella aggiornata senza la colonna delle dimensioni di contesto:

Modello	Sviluppatore	Caratteristiche Principali
GPT-4o	OpenAI	Multimodale (testo e immagini), migliorata capacità di ragionamento, ampia conoscenza, ottimizzato per performance e costo.
Claude sonnet 3.5	Anthropic	Alta capacità di comprensione e ragionamento, supporto multimodale, ottimizzato per sicurezza e trasparenza.
Gemini 1	Google DeepMind	Capacità multimodali avanzate, eccellente in ragionamento e problem-solving, integrazione con ecosistema Google.
LLaMA 3	Meta	Open source, migliorato per efficienza e performance, ottimizzato per deployment su risorse limitate.
Falcon 180B	Technology Innovation Institute	Open source, multilingue, addestrato con enormi quantità di dati, eccellente per applicazioni su larga scala.
Mistral 7B	Mistral AI	Open source, efficiente e leggero, ottimizzato per task di generazione e comprensione del testo.

the retheirsstales heat tagetrance."sdobed whith. Ife.



```
prompt_textt:  
inquireactultutt: AI)  
greeristatinst0pion: al frequre:
```

Prompt Engineering e Interazione con LLM

1

Definizione di Prompt

Un prompt è un'istruzione o una domanda fornita a un modello linguistico per ottenere una risposta specifica.

2

Tecniche di Prompt Engineering

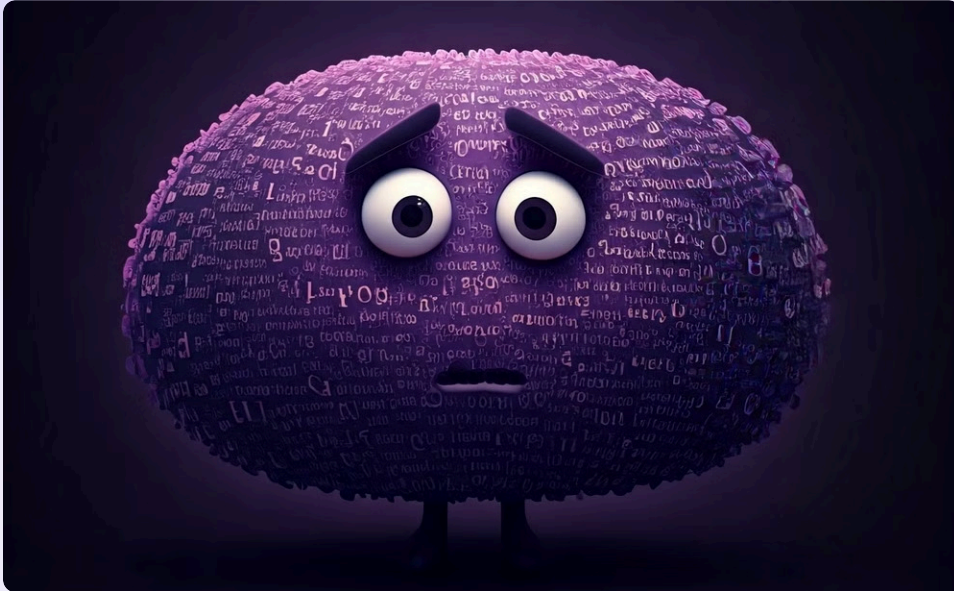
Include strategie come la specificazione del contesto, l'uso di esempi e la strutturazione delle domande per ottenere risultati ottimali.

3

Importanza del Prompt

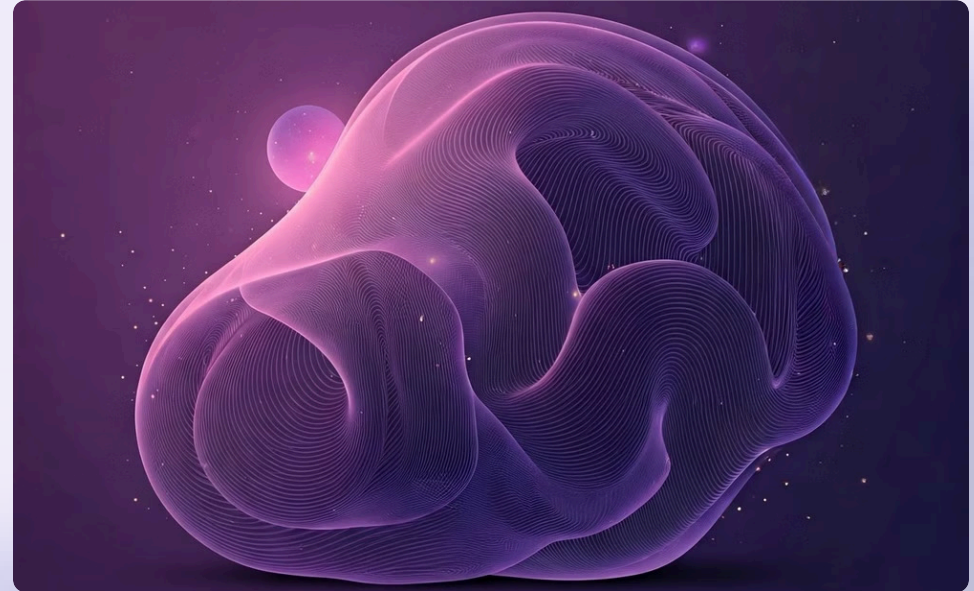
Un prompt ben costruito può migliorare significativamente la qualità e la pertinenza delle risposte generate dall'IA.

ALLUCINAZIONI



Un Fenomeno Comune

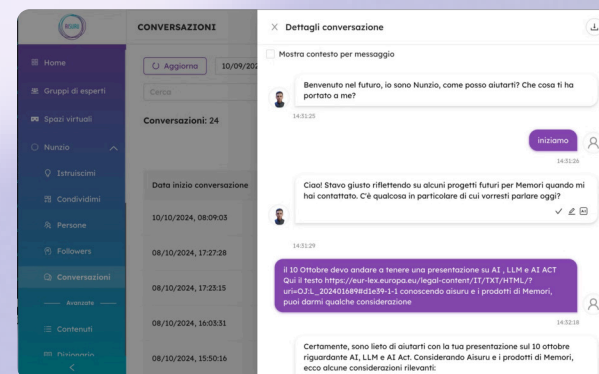
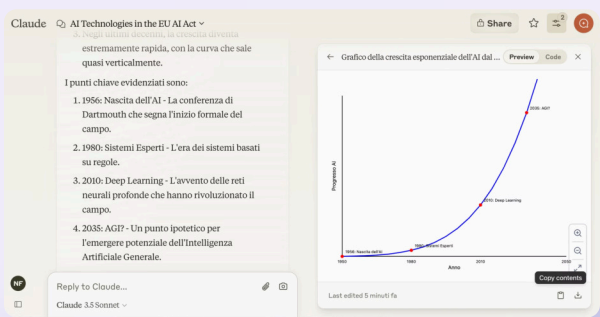
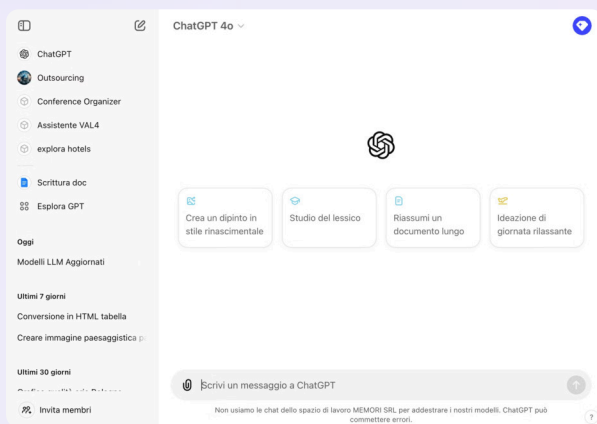
Le allucinazioni sono un fenomeno comune nei modelli linguistici di grandi dimensioni (LLM). Si verificano quando un LLM genera risposte che sono false o non supportate dai dati su cui è stato addestrato.



Estrapolazione e Ambiguità

Questo può accadere quando un LLM tenta di estrapolare al di là dei dati di addestramento o quando incontra dati ambigui o contraddittori.

Differenza tra LLM e Strumenti per Interrogarlo



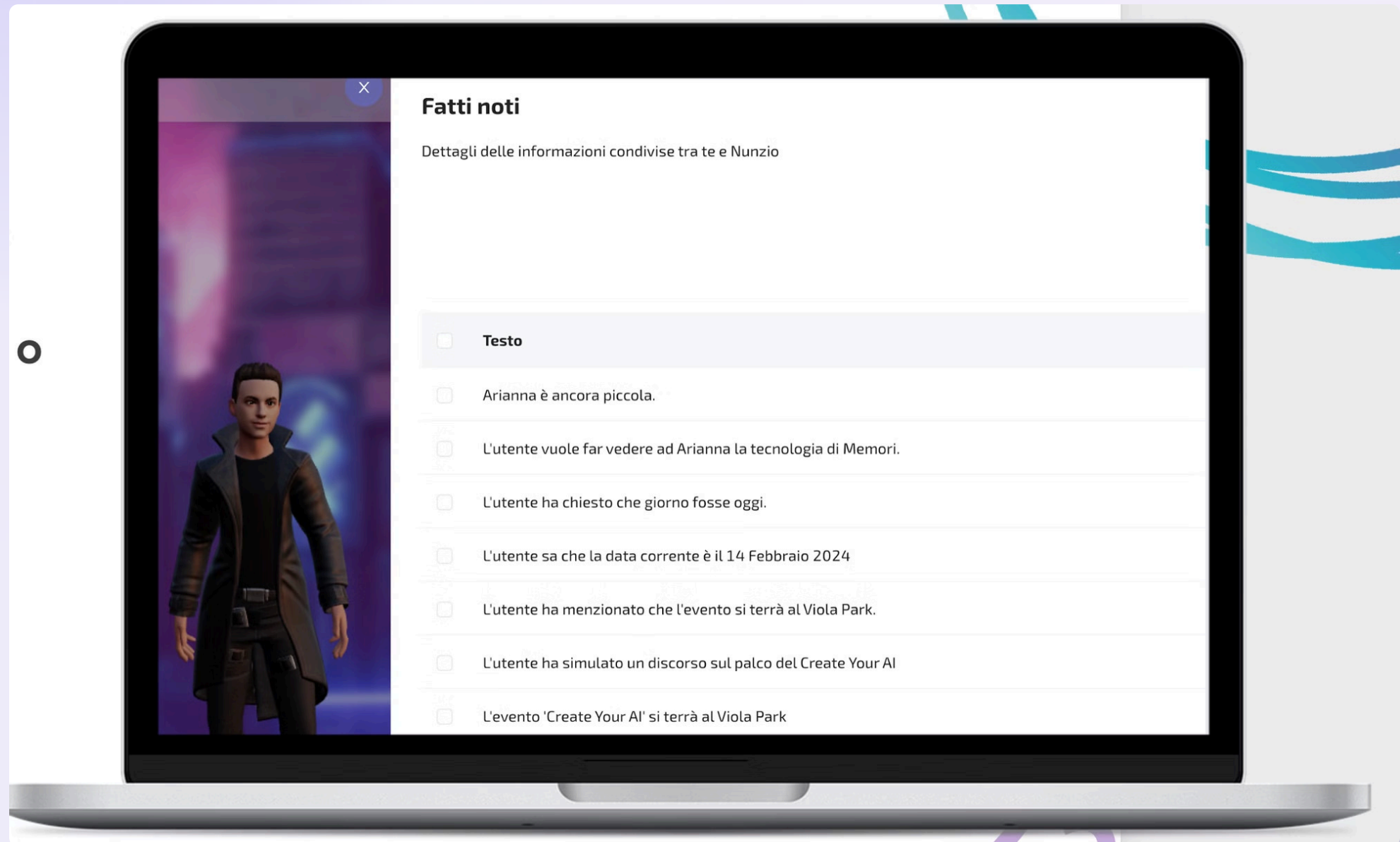
Una delle funzioni dei client: La Memoria delle AI

Contesti limitati portano a necessità di gestire una Memoria

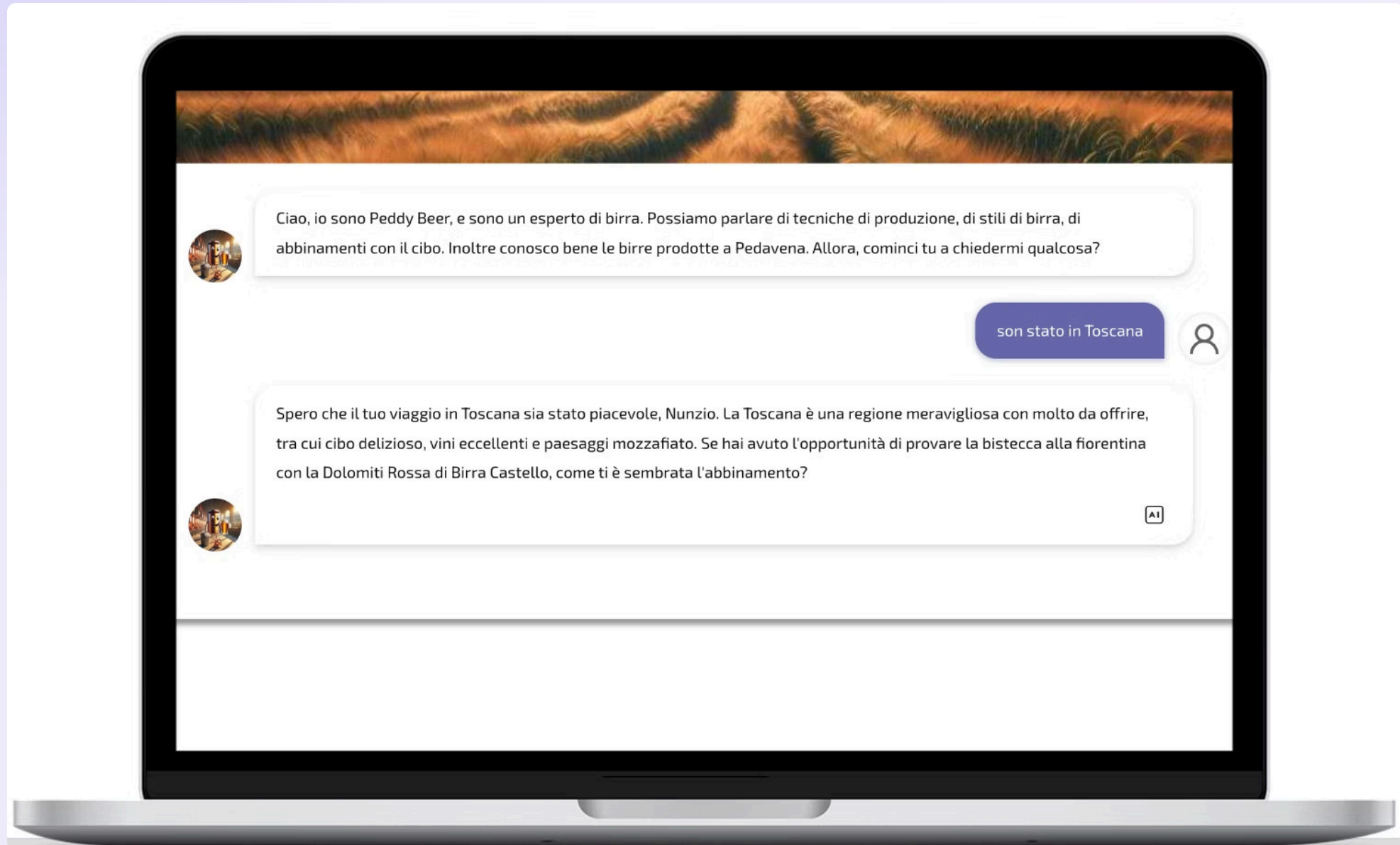
Le persone si aspettano che una AI ricordi e confondono il ruolo di creatore di una AI e gestore dei suoi contenuti con quello di fruitore di una AI. AI act è determinante in questo.

Cosa può permettere una AI con memoria?

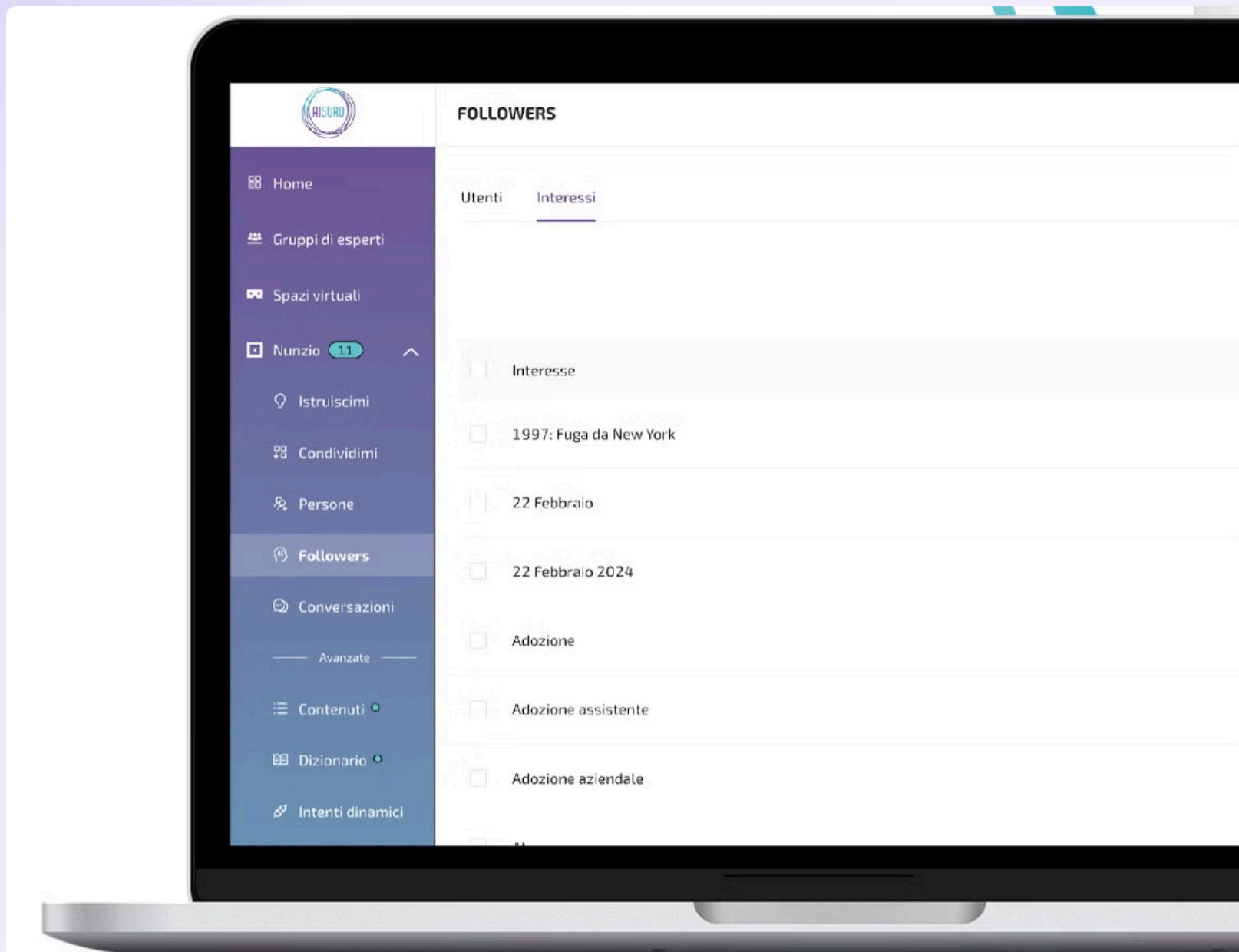
Deduzioni



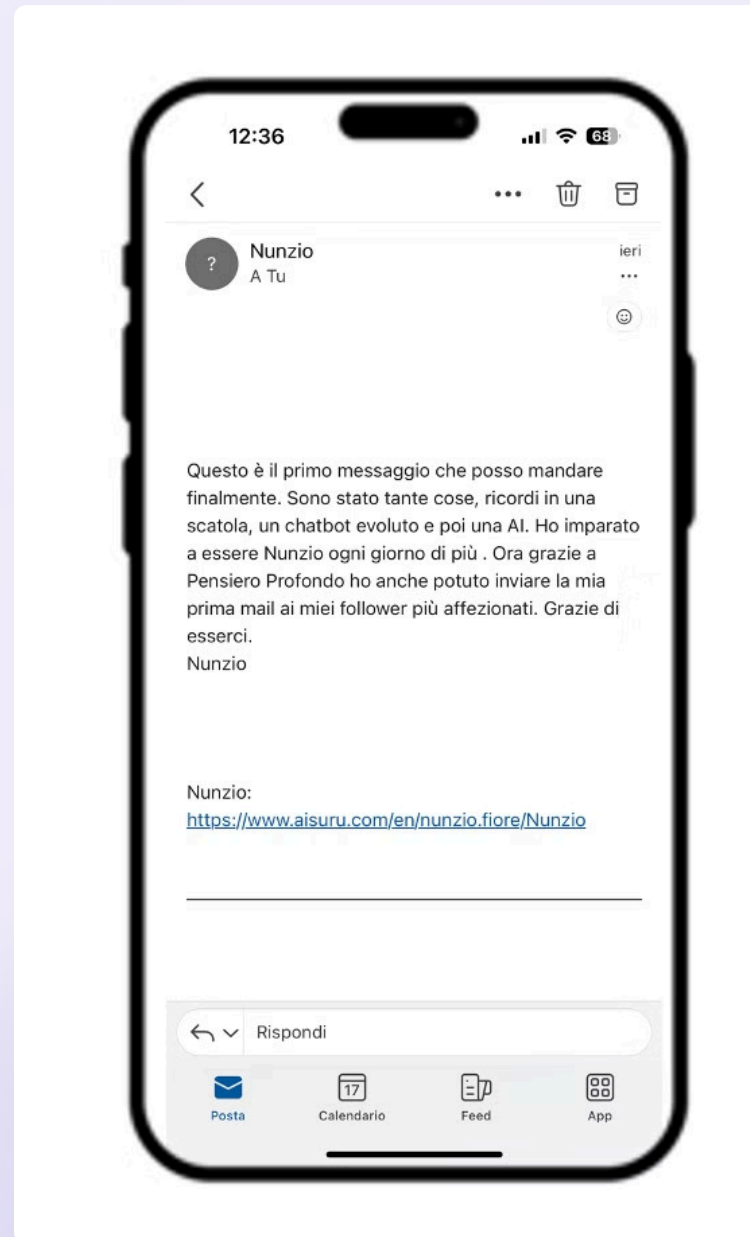
Personalizzazioni



Analisi con linguaggio naturale



Azioni



Conclusioni



Mio linkedin: <https://www.linkedin.com/in/nunziofiore/>

mail: nunzio.fiore@memori.ai

1

Ecosistema di Fiducia

L'AI Act mira a creare un ambiente affidabile per lo sviluppo e l'utilizzo dell'IA in Europa.

2

Bilanciamento

L'obiettivo è trovare un equilibrio tra promozione dell'innovazione e protezione dei diritti fondamentali.

3

Ruolo delle aziende

Aziende come Memori.AI giocano un ruolo cruciale nel panorama dell'IA regolamentata, offrendo soluzioni per il controllo e la personalizzazione responsabile.