# L’infrastruttura dell’AI, un mercato globale da 100 miliardi di dollari entro il 2028

L’intelligenza artificiale (AI) sta rivoluzionando il panorama tecnologico globale, e la sua crescita è strettamente legata all’infrastruttura hardware sottostante. Secondo le ultime previsioni di International Data Corporation (IDC), il mercato globale dell’infrastruttura AI è destinato a superare i 100 miliardi di dollari entro il 2028, registrando una crescita senza precedenti.

## Una crescita esponenziale

Nella prima metà del 2024, la spesa globale per l’infrastruttura hardware di calcolo e storage dedicata all’AI è aumentata del 37% rispetto all’anno precedente, raggiungendo i 31,8 miliardi di dollari. Questa crescita a doppia cifra si è mantenuta per nove semestri consecutivi, trainata principalmente dall’investimento in server per le implementazioni AI.

I server rappresentano l’89% della spesa totale per l’infrastruttura AI nel primo semestre del 2024, con una crescita del 37% rispetto allo stesso periodo dell’anno precedente. L’infrastruttura AI distribuita su cloud e ambienti condivisi rappresenta il 65% della spesa totale per i server AI nel primo semestre del 2024, poiché hyperscaler, fornitori di servizi cloud e fornitori di servizi digitali espandono le loro capacità infrastrutturali. Le aziende

tradizionali, al contrario, sono in gran parte rimaste indietro nell’adozione di infrastrutture AI on-premise.

# I server accelerati: il cuore dell’infrastruttura AI

I server con acceleratori integrati sono l’infrastruttura preferita per le piattaforme AI, rappresentando il 58% della spesa totale per l’infrastruttura server AI, con una crescita del 63% nella prima metà del 2024. IDC prevede che i server accelerati supereranno il 60% della spesa totale per l’infrastruttura server AI entro il 2028, con un tasso di crescita annuo composto del 19% nei prossimi cinque anni.

La spesa per lo storage nell’infrastruttura AI è stata guidata dalla necessità di gestire grandi quantità di dati necessari per addestrare i modelli AI, nonché per lo storage di dati di addestramento, checkpoint e repository per le fasi di inferenza. Questa categoria ha registrato un tasso di crescita annuo del 36% nel primo semestre del 2024, con il 56% della spesa proveniente dai deployment cloud.

# La geografia dell’AI: Stati Uniti in testa

Gli Stati Uniti guidano il mercato globale dell’infrastruttura AI, rappresentando quasi la metà della spesa totale nel primo semestre del 2024, seguiti dalla Cina (23%), dalla regione Asia-Pacifico (16%) e dall’EMEA (10%). Nei prossimi cinque anni, IDC prevede che la regione Asia-Pacifico crescerà al tasso di crescita annuo composto più rapido (20%), seguita dagli Stati Uniti (16%), EMEA (13%) e Cina (11%). Entro il 2028, IDC prevede che la spesa per l’infrastruttura AI raggiungerà i 107 miliardi di dollari, con i server distribuiti su cloud che rappresentano il 75% del mercato totale e i server accelerati circa il 56% della spesa totale

del mercato.

## Sfide e opportunità

Nonostante la crescita esponenziale, il mercato dell’infrastruttura AI presenta anche alcune sfide. La crescente domanda di potenza di calcolo sta mettendo sotto pressione le risorse energetiche, e le aziende devono trovare soluzioni sostenibili per alimentare i loro data center. Inoltre, la complessità delle architetture AI e la carenza di talenti specializzati possono ostacolare l’adozione di queste tecnologie.

Tuttavia, le opportunità sono immense. L’AI ha il potenziale di rivoluzionare numerosi settori, dalla sanità alla finanza, dall’industria manifatturiera all’agricoltura. Per sfruttare appieno questo potenziale, è necessario investire in infrastrutture tecnologiche avanzate e sviluppare competenze specializzate.

In conclusione, l’infrastruttura AI è un motore di crescita fondamentale per l’economia digitale. La sua rapida evoluzione sta creando nuove opportunità per le aziende e i governi di tutto il mondo. Tuttavia, è essenziale affrontare le sfide legate all’energia, alla complessità e alla carenza di talenti per garantire un futuro sostenibile e innovativo per l’AI.

**Leggi le altre notizie sull’home page di Key4biz**

https://www.key4biz.it/linfrastruttura-dellai-un-mercato-globale-da-100-miliardi-di-dollari-entro-il-2028/514711/

---

# Stangata del Garante Privacy a OpenAI, multa da 15 milioni di euro e campagna informativa per ChatGPT

## Le violazioni contestate a OpenAI e le sanzioni del Garante Privacy

Il **Garante per la protezione dei dati personali** ha inflitto una **sanzione di 15 milioni di euro** a **OpenAI**, la società che gestisce il chatbot di intelligenza artificiale generativa **ChatGPT**. La decisione arriva al termine di un'istruttoria avviata nel marzo 2023 e in seguito al **parere dell'EDPB** (Comitato europeo per la protezione dei dati) che ha delineato un approccio comune alle questioni relative al trattamento dei dati personali nell'ambito dell'IA.

Il Garante ha accertato diverse violazioni da parte di OpenAI:

- **mancata notifica di data breach**, cioè la società non ha notificato all'Autorità la violazione dei dati subita nel marzo 2023;
- **trattamento illecito dei dati per l'addestramento dell'IA**, perchè OpenAI ha utilizzato i dati personali degli utenti per addestrare ChatGPT senza una base giuridica adeguata, violando il principio di trasparenza e gli obblighi informativi verso gli utenti;
- **assenza di meccanismi di verifica dell'età**, cioèassenza di controlli sull'età espone i minori di 13 anni a contenuti potenzialmente inappropriati.

Come ha ricordato **il presidente dell'EDPB Talus:** "*Le tecnologie di IA possono offrire molte opportunità e vantaggi a diversi settori e ambiti della vita. Dobbiamo garantire che queste innovazioni siano fatte in modo etico, sicuro e in un modo che vada a beneficio di tutti. L'EDPB intende sostenere l'innovazione responsabile in materia di IA garantendo la protezione dei dati personali e nel pieno rispetto del regolamento generale sulla protezione dei dati (RGPD)*".

# Le misure impartite

Per garantire la trasparenza nel trattamento dei dati personali, il Garante ha imposto a OpenAI, avvalendosi per la prima volta dei nuovi poteri previsti dall'articolo 166 comma 7 del Codice Privacy, di realizzare una **campagna di comunicazione istituzionale di sei mesi** su radio, televisione, giornali e internet.

La campagna, i cui contenuti dovranno essere concordati con l'Autorità, avrà l'obiettivo di:

- informare il pubblico sul funzionamento di ChatGPT, con particolare attenzione alla raccolta dei dati di utenti e non utenti per l'addestramento dell'IA generativa;
- spiegare i diritti degli interessati, tra cui opposizione, rettifica e cancellazione dei dati;
- sensibilizzare gli utenti e non utenti di ChatGPT su come opporsi all'utilizzo dei propri dati personali per l'addestramento dell'IA, mettendoli nelle condizioni di esercitare i propri diritti ai sensi del GDPR.

# La sanzione e il ruolo dell'Autorità irlandese

Oltre alla campagna informativa, il Garante ha comminato a OpenAI una **sanzione di 15 milioni di euro**, tenendo conto dell'atteggiamento collaborativo della società durante

l’istruttoria.

Poiché OpenAI ha stabilito in Irlanda il suo quartier generale europeo, il Garante, in conformità con il principio del “*one-stop-shop*” previsto dal **GDPR**, ha trasmesso gli atti del procedimento all’Autorità di protezione dati irlandese (**DPC**), che diventa l’autorità di controllo capofila. La DPC proseguirà l’istruttoria per eventuali violazioni continuative non esauritesi prima dell’apertura della sede europea.

## Non solo ChatGPT, ma un precedente importante in generale per l’AI generativa

Il provvedimento del Garante Privacy rappresenta un importante precedente in materia di protezione dei dati personali nell’ambito dell’**intelligenza artificiale generativa**.

L’attenzione si concentra sulla trasparenza, sul consenso informato e sulla tutela dei minori, con l’obiettivo di garantire un utilizzo responsabile e consapevole di queste nuove tecnologie. La collaborazione tra le autorità europee, in particolare tra il Garante italiano e la DPC irlandese, sottolinea l’importanza di un approccio coordinato a livello europeo per la gestione delle sfide poste dall’IA.

## La posizione di OpenAI

La risposta di OpenAI non si è fatta attendere, si legge in una nota ufficiale che “*la decisione del Garante non è proporzionata e presenteremo ricorso. Quando il Garante ci ha ordinato di sospendere ChatGPT in Italia nel 2023, abbiamo collaborato con l’Autorità per renderlo nuovamente disponibile un mese dopo*“.

“*Già allora il Garante aveva riconosciuto il nostro ruolo da*

*capofila per quanto riguarda la protezione dei dati nell'ambito dell'IA* – continua il documento – *e questa sanzione rappresenta circa venti volte il fatturato da noi generato in Italia nello stesso periodo. Riteniamo che l'approccio del Garante comprometta le ambizioni dell'Italia in materia di IA, ma rimaniamo impegnati a collaborare con le autorità preposte alla tutela della privacy in tutto il mondo per offrire un'IA capace di portare benefici alla società nel rispetto dei diritti della privacy*".

Questa indagine si concentra sul periodo novembre 2022 – marzo 2023, è specificato nella nota. Dal rilascio di ChatGPT nel novembre 2022, OpenAI ha reso ancora più facile per gli utenti l'accesso ai nostri strumenti per i dati, inserendoli nelle impostazioni di ChatGPT.

La società americana fa sapere che è stato lanciato anche un Privacy Center, all'indirizzo *privacy.openai.com*, dove gli utenti possono esercitare le loro preferenze sulla privacy e scegliere di non utilizzare i loro dati per l'addestramento dell'IA.

**Leggi le altre notizie sull'home page di Key4biz**

https://www.key4biz.it/stangata-del-garante-privacy-a-openai-multa-da-15-milioni-di-euro-e-campagna-informativa-per-chatgpt/516406/

---

# AI e futuro della ricerca online, Perplexity triplica

# il suo valore e sale a 9 miliardi di dollari

## Valutazione record e investimenti significativi per Perplexity AI

Trasformare il mondo della **ricerca online** grazie all'intelligenza artificiale è l'obiettivo di **Perplexity AI**, startup fondata nel 2022 da un team di ex ricercatori di OpenAI e Meta, tra cui **Aravind Srinivas**, **Andy Konwinski**, **Denis Yarats** e **Johnny Ho**.

La soluzione proposta si distingue per l'elevata capacità di comprendere il linguaggio naturale e il contesto delle query.

Perplexity AI ha inoltre chiuso un importante round di finanziamenti da 500 milioni di dollari. Questo investimento, guidato da **Institutional Venture Partners**, ha triplicato la valutazione dell'azienda, che ora raggiunge i **9 miliardi di dollari rispetto** ai 3 miliardi di giugno 2024.

Una crescita vertiginosa, nove volte superiore rispetto a inizio anno, che riflette il grande interesse del mercato per le tecnologie di intelligenza artificiale (AI) più innovative e il loro impatto potenziale sul settore della ricerca.

## Un approccio innovativo alla ricerca

Ciò che distingue Perplexity è il suo focus sulla ricerca in tempo reale. Diversamente dai chatbot basati esclusivamente su

dati pre-addestrati, la piattaforma sfrutta un modello AI che scansiona attivamente il web per fornire risposte aggiornate in un formato conversazionale simile a ChatGPT.

L’azienda offre una versione gratuita e una premium, con funzionalità aggiuntive come la ricerca interna per le organizzazioni e strumenti dedicati alla finanza. **A marzo 2024, Perplexity vantava oltre 15 milioni di utenti attivi e centinaia di milioni di query mensili**.

# Acquisizioni strategiche

Perplexity ha recentemente acquisito **Carbon**, una startup specializzata nella tecnologia di generazione potenziata dal recupero (*Retrieval-Augmented Generation*, RAG).

Questa acquisizione punta a migliorare le capacità di ricerca nelle applicazioni aziendali e di produttività, rafforzando la posizione della società nel soddisfare le esigenze degli utenti aziendali.

# Sfide nel mercato e strategie di crescita di Perplexity AI

Il panorama competitivo vede Perplexity confrontarsi con colossi come **OpenAI**, che ha integrato la ricerca web in ChatGPT, oltre a Google e Microsoft, che stanno incorporando modelli linguistici avanzati nei loro motori di ricerca.

Perplexity, dal canto suo, sta esplorando la monetizzazione attraverso pubblicità e collaborazioni con grandi editori come *Time* e *Fortune*, per condividere i ricavi e affrontare le sfide legate ai contenuti.

# Una scommessa degli investitori sull’intelligenza artificiale

Il massiccio investimento in Perplexity riflette una tendenza più ampia: nel 2024, il 42% del capitale di rischio statunitense è stato destinato a startup AI, in crescita rispetto al 36% del 2023.

Questa fiducia sottolinea il potenziale trasformativo dell’intelligenza artificiale, in particolare nel settore della ricerca online e delle soluzioni aziendali.

Con una valutazione record, un finanziamento consistente e l’acquisizione di tecnologie strategiche, Perplexity AI sembra ben posizionata per sfidare i giganti del settore e definire il futuro della ricerca online. Mentre continua a innovare, resta da vedere come l’azienda navigherà un panorama competitivo sempre più affollato e capitalizzerà sul suo potenziale tecnologico.

# Il futuro dei motori di ricerca basati sull’AI

L’adozione di **motori di ricerca basati su AI,** come Perplexity e ChatGPT, sta guadagnando slancio. Questi strumenti offrono risposte più dirette e contestualizzate rispetto ai tradizionali risultati di ricerca basati su link, migliorando l’esperienza utente.

Secondo Bloomberg, **si stima che tali strumenti possano ridurre significativamente il traffico su Google**, che attualmente detiene oltre il 90% del mercato della ricerca online.

C’è un crescente livello di insoddisfazione nei confronti della qualità dei risultati forniti da Google. Questo ha portato a una maggiore apertura verso nuove tecnologie che promettono un’esperienza di ricerca migliore.

Le soluzioni AI possono rispondere a domande specifiche con informazioni più pertinenti e affidabili, contribuendo a soddisfare le esigenze degli utenti. La competizione potrebbe spingere Google a migliorare la qualità dei suoi servizi, rendendo la ricerca online più efficiente.

Il mercato globale dei sistemi di ricerca online alimentati dall'AI crescerà significativamente nei prossimi anni e stando alle più recenti stime, potrebbe raggiungere i 12,9 miliardi di dollari entro il 2031.

**Leggi le altre notizie sull'home page di Key4biz**

https://www.key4biz.it/ai-e-futuro-della-ricerca-online-perplexity-triplica-il-suo-valore-e-sale-a-9-miliardi-di-dollari/516260/

---

# Federated Learning e Sicurezza Distribuita

Il *Federated Learning* (FL) si configura come un paradigma emergente e altamente promettente nell'ambito dell'apprendimento distribuito orientato alla privacy, consentendo a più entità di collaborare all'addestramento di modelli senza necessità di condividere i dati grezzi. Nonostante il FL integri meccanismi intrinseci di protezione della privacy, rimane suscettibile a una vasta gamma di minacce sia in termini di sicurezza sia di riservatezza.

Questo contributo esplora in dettaglio le sfide di sicurezza associate al FL, analizzando i vettori di attacco e i meccanismi di difesa lungo l'intero ciclo di vita del sistema.

L’analisi si focalizza su tre fasi critiche: *auditing* dei dati e dei comportamenti, addestramento del modello e predizione. L’obiettivo è delineare come un sistema FL affidabile necessiti dell’integrazione di misure di sicurezza appropriate in ogni fase, garantendo un equilibrio tra la protezione della privacy, l’utilità del modello e le prestazioni complessive.

## Introduzione

In un contesto in cui la protezione della privacy rappresenta un elemento cruciale nello sviluppo dell’intelligenza artificiale, il *Federated Learning* si è imposto come una soluzione innovativa nel panorama dell’apprendimento distribuito. Questo framework consente a organizzazioni e individui di collaborare nell’addestramento di modelli mantenendo i dati localmente, riducendo il rischio di esposizione di informazioni sensibili. Tuttavia, la natura distribuita e collaborativa di questa architettura introduce nuove superfici di attacco sfruttabili da avversari interni ed esterni.

Le sfide di sicurezza nel contesto del *Federated Learning* sono intrinsecamente complesse e richiedono approcci sistematici e multidisciplinari. I recenti sviluppi nella ricerca hanno evidenziato una serie di vulnerabilità specifiche, accompagnate dalla proposta di soluzioni avanzate per mitigare tali rischi. Le tendenze attuali si concentrano sull’implementazione di meccanismi robusti volti a proteggere non solo la privacy dei partecipanti, ma anche l’integrità e l’affidabilità del processo di apprendimento.

I concetti fondamentali della sicurezza nel *Federated Learning* comprendono la definizione di modelli di minaccia specifici e l’applicazione di principi di protezione mirati. I modelli di minaccia, in questo contesto, includono scenari che vanno da attacchi mirati da parte di partecipanti compromessi a intrusioni esterne su scala sistemica.

Le vulnerabilità di sicurezza e privacy nelle architetture FL rappresentano una delle principali aree di indagine. La natura distribuita di questi sistemi introduce complessità uniche che richiedono soluzioni personalizzate e specificamente adattate. Le soluzioni di difesa avanzate attualmente in sviluppo combinano tecniche di crittografia omomorfica, metodi di preservazione della privacy come il *differential privacy* e strumenti per il rilevamento di anomalie nel comportamento dei partecipanti.

Le future direzioni di ricerca in questo ambito mirano a un'evoluzione delle contromisure, considerando la crescita e la diversificazione delle minacce. L'obiettivo principale rimane quello di potenziare la resilienza dei sistemi FL, preservandone al contempo l'efficienza computazionale e l'usabilità pratica.

Il presente studio adotta un approccio multi-fase per esaminare le sfide di sicurezza lungo l'intero ciclo di vita di un sistema *Federated Learning*, partendo dalla fase di inizializzazione fino alla sua operatività continua. Questo approccio consente una valutazione completa e integrata, tenendo conto delle interazioni tra le diverse componenti del sistema e dell'impatto complessivo delle misure di sicurezza implementate.

# Architettura di Sicurezza e Threat Models nel Federated Learning

## Architettura di Base

Il *Federated Learning* (FL) si configura come un framework avanzato per l'apprendimento distribuito, caratterizzato da una struttura architetturale complessa che mira a bilanciare efficienza computazionale e sicurezza dei dati. Alla base di questa architettura emergono componenti chiave, ciascuno dei quali ricopre un ruolo cruciale per il funzionamento e la

resilienza del sistema.

I ***local participants***, noti anche come client, costituiscono il fulcro dell'architettura distribuita. Questi nodi mantengono i propri dataset privati localmente, riducendo drasticamente i rischi associati alla condivisione dei dati sensibili. Questo approccio decentralizzato non solo garantisce la privacy dei dati originali, ma promuove anche un paradigma di collaborazione efficiente nell'addestramento del modello globale, riducendo al minimo le esposizioni potenziali.

Il ***coordination mechanism*** per l'aggregazione dei modelli è il secondo elemento essenziale. Questo modulo gestisce la fusione degli aggiornamenti dei parametri forniti dai partecipanti, garantendo che il modello globale benefici del contributo distribuito mantenendo al contempo integrità e coerenza. Tecniche avanzate come il *Federated Averaging* (FedAvg) e le sue varianti sono frequentemente utilizzate per ottimizzare questa fase.

I ***communication protocols*** giocano un ruolo determinante nel garantire la sicurezza e l'efficienza delle interazioni tra i nodi. Questi protocolli devono essere progettati per supportare un flusso bidirezionale sicuro, riducendo la latenza e proteggendo la riservatezza degli aggiornamenti mediante tecniche di crittografia *end-to-end* e meccanismi di autenticazione robusti.

Infine, i ***privacy-preserving computation methods***, come la crittografia omomorfica, il *secure multi-party computation* (SMPC) e il *differential privacy*, completano l'architettura di base. Questi strumenti sono indispensabili per proteggere la confidenzialità dei dati durante le fasi di elaborazione e trasmissione, fornendo un ulteriore strato di sicurezza.

## Threat Models nel contesto del Federated

## Learning

I *threat models* nel contesto del FL comprendono una varietà di attori malevoli e vulnerabilità che possono compromettere la sicurezza e la robustezza del sistema. Tali minacce possono essere classificate in base al comportamento e alla posizione degli attaccanti.

Gli *honest-but-curious participants* rappresentano una minaccia sottile ma significativa: questi nodi seguono correttamente il protocollo, ma tentano di dedurre informazioni sensibili analizzando i gradienti o gli aggiornamenti ricevuti. Questa categoria richiede contromisure specifiche, come l'applicazione di tecniche di *differenziale privacy* per offuscare i dati sensibili.

I *malicious participants*, invece, perseguono attivamente l'obiettivo di compromettere il sistema. Essi possono manipolare i propri aggiornamenti al fine di alterare il modello globale (ad esempio, tramite attacchi di *poisoning*) o compromettere l'integrità del processo di apprendimento.

Gli *external adversaries* operano al di fuori del sistema, cercando di sfruttare vulnerabilità nei protocolli di comunicazione per intercettare o manipolare i dati trasmessi. Gli attacchi più comuni in questa categoria includono attacchi di tipo *man-in-the-middle* e violazioni della confidenzialità tramite analisi del traffico.

I *compromised aggregators* costituiscono un'ulteriore minaccia critica. Un aggregatore compromesso può alterare il processo di aggregazione o esporre i dati sensibili dei partecipanti. Poiché l'aggregatore agisce come punto centrale di controllo, garantire la sua sicurezza è fondamentale per preservare l'integrità del sistema.

Gli obiettivi degli adversa*ries* possono essere diversificati e sofisticati, il furto di informazioni private è spesso la

motivazione primaria, con gli attacchi mirati a estrarre informazioni dai parametri condivisi. Il *poisoning* del *training process* rappresenta un altro rischio significativo, in cui gli attaccanti iniettano dati o aggiornamenti malevoli per corrompere il modello.

La *compromise model integrity* è un obiettivo più ampio e strategico, finalizzato a degradare le prestazioni complessive o introdurre comportamenti indesiderati nel modello. Infine, gli *inference attacks*, in cui gli attaccanti cercano di dedurre informazioni sui dati di training analizzando il comportamento del modello, costituiscono una sfida particolarmente complessa, richiedendo contromisure avanzate per garantire una resilienza effettiva.

# *Security Challenges* nel *Federated Learning* per Sistemi IoT

## *IoT-Specific Considerations*: Sfide Fondamentali nell'Integrazione

La complessità intrinseca dei sistemi IoT introduce sfide particolari, derivanti principalmente dalla loro eterogeneità strutturale. Le ***heterogeneous device capabilities*** rappresentano uno dei principali ostacoli: i dispositivi, dotati di risorse computazionali, memoria e caratteristiche hardware variabili, devono collaborare in maniera efficace all'interno del medesimo ecosistema di *Federated Learning* (*FL*). Questa varietà introduce difficoltà non solo tecniche ma anche potenziali vulnerabilità sfruttabili dagli attaccanti.

I *resource constraints*, come limitazioni in termini di *computational power*, memoria disponibile e capacità energetica, costituiscono un ulteriore elemento critico. La progettazione di soluzioni di sicurezza per sistemi IoT deve essere ottimizzata per garantire un'adeguata protezione, mantenendo un basso impatto in termini di utilizzo delle

risorse computazionali ed energetiche.

## Sfide di Connettività e Distribuzione

Le *bandwidth limitations* rappresentano una problematica significativa per la natura distribuita del *Federated Learning*, che richiede frequenti scambi di dati tra dispositivi partecipanti e server centrale. Nei sistemi IoT, spesso caratterizzati da connessioni instabili e velocità di trasmissione ridotte, l'efficienza e la sicurezza del sistema possono risultare compromesse. Protocolli di sicurezza tradizionali, sebbene robusti, potrebbero rivelarsi troppo onerosi in termini di consumo di banda.

La distribuzione geografica dei dispositivi IoT introduce ulteriori complessità. Dispositivi collocati in aree geografiche remote o in ambienti eterogenei sono soggetti a condizioni di rete e ambientali differenti, complicando l'implementazione di misure di sicurezza uniformi. Inoltre, le *dynamic network conditions*, caratterizzate da connettività intermittente e latenza variabile, richiedono soluzioni di sicurezza adattive per garantire efficacia operativa anche in situazioni di rete sfavorevoli.

## Scalabilità e Domini Applicativi

La scalabilità rappresenta una sfida cruciale: gestire la sicurezza di miliardi di dispositivi connessi richiede approcci innovativi e altamente efficienti. Questa problematica assume particolare rilevanza considerando i molteplici domini applicativi in cui operano i sistemi IoT, tra cui il settore sanitario, l'industria manifatturiera e le *smart grids*. Ciascun dominio presenta requisiti di sicurezza specifici, che richiedono soluzioni personalizzate e interoperabili.

# *IoT-Specific Threat Models*: Vulnerabilità

# e Minacce

All’interno dei modelli di minaccia specifici per l’IoT, emergono vulnerabilità che richiedono un’attenzione mirata. Le vulnerabilità a livello di dispositivo rappresentano un punto di ingresso critico: la compromissione di un singolo dispositivo potrebbe avere ripercussioni su larga scala, compromettendo l’intero sistema. I problemi di connettività di rete, oltre a degradare le prestazioni, possono essere sfruttati come vettori di attacco da parte di attori malevoli.

## Attacchi e Minacce alla Sicurezza

Gli attacchi di esaurimento delle risorse (*resource exhaustion attacks*) costituiscono una minaccia particolarmente insidiosa per i dispositivi IoT, spesso caratterizzati da risorse computazionali e energetiche limitate. Inoltre, le minacce alla sicurezza fisica, data l’esposizione di molti dispositivi IoT in ambienti non controllati, aumentano il rischio di manomissioni hardware.

## Propagazione degli Attacchi e Privacy

La propagazione degli attacchi tra domini (*cross-domain attack propagation*) rappresenta un rischio significativo in ecosistemi IoT connessi tramite *FL*. Un attacco inizialmente confinato a un dominio applicativo potrebbe propagarsi, compromettendo l’integrità di altri domini correlati. Inoltre, il leakage di dati sensibili, in particolare in applicazioni critiche come quelle sanitarie, costituisce una preoccupazione fondamentale. Proteggere la privacy degli utenti in tali contesti richiede l’adozione di tecniche avanzate, come la *homomorphic encryption* e i metodi di anonimizzazione dei dati.

# Vulnerabilità di Security e Privacy

# nei Sistemi *Federated Learning* (FL) Distribuiti

## Criticità Specifiche dell'Architettura Distribuita

### Vulnerabilità della Distribuzione delle Risorse

Nei sistemi *Federated Learning* (FL) distribuiti, la gestione delle risorse computazionali presenta vulnerabilità peculiari intrinseche alla natura collaborativa del processo di apprendimento. La distribuzione asimmetrica delle capacità computazionali tra i nodi partecipanti rappresenta potenziali punti di debolezza durante il processo di *training* federato. I nodi con risorse limitate possono trasformarsi in *bottleneck* per l'intera architettura distribuita, compromettendo non solo le performance ma anche la sicurezza del sistema nel suo complesso.

L'eterogeneità delle risorse disponibili tra i nodi introduce ulteriori vulnerabilità nei meccanismi di sincronizzazione del *training* distribuito. Nodi con capacità computazionali significativamente divergenti possono generare disallineamenti temporali nel processo di apprendimento, creando aperture sfruttabili per attacchi mirati a compromettere la convergenza del modello.

### Vulnerabilità nella Coordinazione Distribuita

La natura intrinsecamente distribuita del *Federated Learning* introduce fragilità critiche nei meccanismi di coordinazione. Il processo di orchestrazione del *training* federato risulta particolarmente suscettibile a interruzioni selettive delle comunicazioni tra i nodi. Un attore malevolo potrebbe sfruttare queste lacune per alterare la sincronizzazione del processo di *training*, influenzando la qualità e l'affidabilità del modello finale.

La gestione distribuita del consenso durante l'aggregazione dei modelli locali presenta specifici punti di debolezza. Attacchi mirati ai meccanismi di consenso possono indurre divergenze significative nell'apprendimento, portando alla generazione di modelli inconsistenti o compromessi. La complessità intrinseca nel coordinare molteplici nodi distribuiti espande ulteriormente la superficie di attacco, facilitando manipolazioni intenzionali del processo di aggregazione.

## Vulnerabilità nell'Aggregazione Federata

L'architettura distribuita presenta vulnerabilità rilevanti nella fase di aggregazione dei modelli locali. I nodi intermedi incaricati dell'aggregazione parziale costituiscono potenziali punti critici di compromissione, dove un attore malevolo potrebbe manipolare gli aggiornamenti del modello prima che raggiungano l'aggregatore finale.

La struttura gerarchica tipica dell'aggregazione distribuita introduce fragilità nella propagazione degli aggiornamenti. Un compromesso nei livelli intermedi della gerarchia potrebbe propagarsi attraverso molteplici rami dell'architettura distribuita, amplificando gli effetti dell'attacco e compromettendo l'integrità del modello globale.

## Vulnerabilità nella Sincronizzazione Temporale

La sincronizzazione temporale in un sistema *Federated Learning* distribuito rappresenta un ulteriore vettore di vulnerabilità. Attacchi basati sul *timing* possono sfruttare le differenze nei tempi di *training* e aggregazione tra i nodi per inferire informazioni sensibili sui dati di *training* o manipolare deliberatamente il processo di apprendimento.

I ritardi nella propagazione degli aggiornamenti attraverso l'architettura distribuita generano vulnerabilità specifiche relative alla consistenza del modello. Tali asincronicità possono essere sfruttate per orchestrare attacchi mirati a

compromettere la convergenza del *training* federato, minando la robustezza e l'affidabilità del sistema nel suo complesso.

# Soluzioni di Difesa Avanzate nel *Federated Learning*

## *IoT-Optimized Defense Mechanisms*: Strategie per la Protezione dei Sistemi FL Distribuiti

Nel contesto del *Federated Learning* su sistemi IoT, le *resource-aware solutions* rappresentano un elemento cardine per garantire un addestramento distribuito sicuro ed efficiente. La *lightweight cryptography* emerge come un paradigma essenziale durante le fasi di aggregazione e scambio dei parametri del modello, fornendo meccanismi di cifratura ottimizzati in grado di salvaguardare la riservatezza degli aggiornamenti del modello, pur rispettando i severi vincoli computazionali dei dispositivi IoT partecipanti.

L'*efficient privacy preservation* nel contesto del *Federated Learning* richiede l'adozione di metodologie avanzate, quali il *differential privacy* e il *secure aggregation*, implementate in maniera ottimizzata per dispositivi caratterizzati da risorse computazionali e di memoria limitate. Le *adaptive security measures*, opportunamente calibrate, proteggono sia il processo di *training* locale che la fase di aggregazione globale, modulando dinamicamente i livelli di protezione in funzione delle risorse disponibili e della sensibilità dei dati di *training*.

Gli *energy-efficient protocols*, progettati ad hoc per il paradigma del *Federated Learning*, ottimizzano il consumo energetico durante le fasi di comunicazione degli aggiornamenti del modello, garantendo che i dispositivi IoT possano partecipare al processo di addestramento senza

comprometterne la longevità operativa.

## Protezione a Livello Rete (*Network-Level Protection*) nel *Federated Learning*

La sicurezza della comunicazione è un aspetto critico nel *Federated Learning*, dove la trasmissione sicura degli aggiornamenti del modello è imprescindibile. I *secure communication protocols* vengono adattati per affrontare in modo efficace le esigenze specifiche del traffico generato dal *Federated Learning*, proteggendo gli aggiornamenti del modello durante il transito tra i dispositivi *edge* e il server di aggregazione.

La *bandwidth-efficient encryption* viene ottimizzata per ridurre al minimo l'overhead di comunicazione derivante dallo scambio degli aggiornamenti del modello, mantenendo al contempo un elevato livello di protezione. Le *dynamic security policies* sono implementate per adattarsi dinamicamente alle diverse fasi del processo di *Federated Learning*, includendo regole granulari per la protezione durante l'addestramento locale, l'aggregazione e la distribuzione del modello globale.

I *distributed trust mechanisms* giocano un ruolo chiave nel contesto del *Federated Learning*, in cui la fiducia reciproca tra i partecipanti è critica. Questi meccanismi decentralizzati consentono di verificare l'integrità degli aggiornamenti del modello, prevenendo attacchi sofisticati come il *model poisoning*.

## Sicurezza dei Dispositivi (*Device Security*) nei Sistemi FL

La protezione dei dispositivi coinvolti nel *Federated Learning* richiede misure altamente specializzate per salvaguardare sia i dati di *training* locali che il processo stesso di addestramento. I *secure boot mechanisms* garantiscono

l’integrità dell’ambiente di *training* locale, verificando l’autenticità del software FL e prevenendo manipolazioni del processo attraverso tecniche avanzate di autenticazione.

Gli *hardware security modules* forniscono uno strato di protezione dedicato alle operazioni critiche, inclusa la gestione sicura delle chiavi crittografiche necessarie per proteggere gli aggiornamenti del modello e il *secure storage* dei parametri del modello locale. Questi moduli rappresentano una componente essenziale per assicurare la confidenzialità del processo di *training* distribuito.

La *firmware protection* si concentra sulla salvaguardia dei componenti software responsabili dell’addestramento locale e delle comunicazioni con il server di aggregazione. Parallelamente, il *resource monitoring* svolge una funzione cruciale nel rilevamento tempestivo di anomalie nel processo di *training*, identificando possibili compromissioni del modello o attacchi come il *type inference*.

Questa architettura di sicurezza multilivello, progettata specificamente per il paradigma del *Federated Learning* in ambienti IoT, garantisce la protezione delle diverse fasi operative, dal *training* locale fino all’aggregazione globale. L’obiettivo è preservare la privacy dei dati, garantire l’integrità del modello risultante e mitigare i rischi legati a minacce emergenti nel panorama della sicurezza cibernetica.

# Linee Guida di Implementazione e Sviluppi Futuri nei Sistemi FL Distribuiti

## Ottimizzazione dell’Architettura Distribuita

Nel contesto dei sistemi FL distribuiti, l’ottimizzazione dell’architettura richiede un approccio metodico e avanzato, capace di sfruttare la natura gerarchica e dinamica del

sistema. Il *distributed computation offloading* riveste un ruolo cruciale, poiché consente di implementare strategie di redistribuzione computazionale basate su algoritmi adattivi in grado di valutare, in tempo reale, le capacità e lo stato operativo di ciascun nodo. Questo processo ottimizza l'allocazione del carico, migliorando la scalabilità e la resilienza del sistema.

La *hierarchical model compression* rappresenta un progresso chiave nell'ambito delle comunicazioni distribuite. Questa tecnica integra metodi di compressione differenziati per ciascun livello della gerarchia del sistema, bilanciando con precisione la riduzione del traffico di rete con il mantenimento delle prestazioni del modello globale. La compressione granulare permette inoltre una maggiore adattabilità alle caratteristiche specifiche dei nodi, massimizzando l'efficienza computazionale e di comunicazione.

## Strategie di Comunicazione Multi-livello

L'efficientamento delle comunicazioni in sistemi FL distribuiti richiede un'implementazione stratificata delle strategie di scambio dei dati. Il *tiered communication protocol* introduce un modello gerarchico nel quale ciascun livello della rete applica protocolli ottimizzati e specifici per le proprie esigenze operative, consentendo l'esecuzione di *selective parameter updates*. Questa metodologia riduce drasticamente il volume complessivo di dati trasferiti, limitando la latenza e ottimizzando la larghezza di banda disponibile.

L'*asynchronous aggregation strategy* si configura come una soluzione altamente innovativa per gestire la natura asincrona delle comunicazioni in sistemi distribuiti su larga scala. Questo approccio consente ai sottogruppi di nodi di effettuare l'aggregazione locale indipendentemente dalla sincronizzazione globale, migliorando la throughput complessiva e mitigando i colli di bottiglia legati alla sincronizzazione centralizzata.

## Raccomandazioni per l’Implementazione Distribuita

Un’implementazione efficace dei sistemi FL distribuiti richiede un approccio strategico e rigoroso alla gestione delle risorse. La *distributed resource orchestration* dovrebbe essere supportata da framework dinamici, progettati per allocare e monitorare in tempo reale le risorse computazionali e di rete attraverso i diversi livelli della gerarchia.

Parallelamente, un *adaptive security framework* rappresenta un elemento imprescindibile per l’architettura distribuita. Questo framework deve includere meccanismi di rilevamento delle anomalie distribuiti (*distributed anomaly detection*) e strumenti di risposta coordinata agli incidenti di sicurezza. La capacità di adattarsi automaticamente alle condizioni operative variabili garantisce una protezione coerente e proattiva contro le minacce emergenti.

## Direzioni di Ricerca Emergenti

I futuri orientamenti della ricerca nel dominio dei sistemi FL distribuiti si concentrano su paradigmi altamente innovativi che promettono di rivoluzionare le attuali pratiche. La *distributed privacy enhancement* è un’area prioritaria, focalizzata sullo sviluppo di metodologie avanzate di protezione della privacy che operino in modo sinergico con le architetture multi-livello.

Il *dynamic topology management* emerge come un campo di ricerca cruciale, mirato a progettare meccanismi auto-adattivi per la gestione della topologia di rete in sistemi FL distribuiti. Questo filone si basa su modelli predittivi e architetture auto-organizzanti, capaci di rispondere in modo proattivo alle variazioni nei requisiti di *training* e alle condizioni dinamiche della rete.

## Prospettive Future

L’evoluzione dei sistemi FL distribuiti richiederà un

approccio multidimensionale per bilanciare efficienza operativa, sicurezza e scalabilità. Le future implementazioni dovranno integrare soluzioni sempre più sinergiche, capaci di gestire la complessità delle architetture distribuite, mantenendo elevati standard di *privacy* e *security*. L'attenzione sarà rivolta allo sviluppo di meccanismi adattivi e auto-evolutivi che rispondano in modo dinamico alle mutevoli esigenze del sistema, consentendo una mitigazione proattiva delle sfide emergenti nel panorama cibernetico globale.

**Fonti:**

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/federated-learning-fl/

---

# Microsoft acquista 485 mila chip Nvidia e sbaraglia la concorrenza di Meta, Amazon e Google

## Microsoft accelera sull'intelligenza artificiale: boom di acquisti di chip Nvidia

**Microsoft** sta investendo massicciamente nell'infrastruttura

per l’**intelligenza artificiale** (AI), superando i rivali con l’acquisizione di **485.000 chip Nvidia Hopper** nel 2023, secondo quanto riportato dal F*inancial Times*.

Più del doppio rispetto al secondo acquirente, **Meta**, che si è fermata a **224.000**. A confermarlo sono le stime di **Omdia**, basate su spese capitali dichiarate, spedizioni di server e analisi della catena di approvvigionamento.

# La corsa ai chip AI, cifre e protagonisti

**Amazon** e **Google** hanno acquistato rispettivamente **196.000** e **169.000** chip Hopper, mentre le aziende cinesi **ByteDance** e **Tencent** si sono orientate su circa **230.000** a testa. Questi ultimi, meno potenti dei Hopper, sono stati progettati per conformarsi alle restrizioni statunitensi sulle esportazioni verso la Cina.

Le **spese globali per i server nel 2023** hanno raggiunto circa **229 miliardi di dollari**, di cui **43% destinati a Nvidia**. Microsoft ha guidato questa tendenza con un investimento di **31 miliardi di dollari**, seguita da Amazon con **26 miliardi**.

# Competizione e sviluppo interno

Nonostante la predominanza di Nvidia nel settore, i giganti tecnologici stanno lavorando per ridurre la dipendenza dai suoi prodotti, sviluppando **chip proprietari**. Meta e Google ne hanno distribuito ciascuna 1,5 milioni, mentre Amazon ne ha installati 1,3 milioni. Tuttavia, Microsoft rimane indietro in questo campo, avendo implementato solo 200.000 chip Maia.

In questo mercato, anche **AMD** sta guadagnando terreno: Meta ha acquistato **173.000 chip MI300**, mentre Microsoft ne ha ordinati 96.000.

# Nvidia e i suoi chip al centro dell’ecosistema AI

L’investimento di Microsoft in chip Nvidia si inserisce nella strategia di espansione AI, incentivata dall’investimento da **13 miliardi di dollari** in **OpenAI**. La società punta a sfruttare le capacità di intelligenza artificiale sia per i servizi interni che per quelli offerti tramite la piattaforma **Azure**.

**Nvidia**, leader indiscusso del mercato, ha registrato nel terzo trimestre del 2023 un fatturato di **35,1 miliardi di dollari**, di cui **30,8 miliardi** derivanti dai data center. Tuttavia, alcune sfide tecniche, come i problemi di surriscaldamento nei chip Blackwell, hanno interessato aziende come Meta e Microsoft.

L’adozione massiccia dei chip Nvidia da parte di Microsoft evidenzia l’**importanza strategica delle tecnologie AI nel settore tecnologico**. Con una quota di mercato dominante e innovazioni all’avanguardia, Nvidia resta un pilastro fondamentale per lo sviluppo dell’intelligenza artificiale.

Nonostante le difficoltà, l’impegno di Microsoft dimostra la volontà di mantenere una posizione di leadership nel panorama AI globale.

**Leggi le altre notizie sull’home page di Key4biz**

https://www.key4biz.it/microsoft-acquista-485-mila-chip-nvidia-e-sbaraglia-la-concorrenza-di-meta-amazon-e-google/516056/

# OpenAI rende disponibile in tutto il mondo ChatGPT Search. A rischio il monopolio di Google?

**OpenAI** ha annunciato l’espansione della funzione **ChatGPT Search**, rendendola disponibile a tutti gli utenti con account, inclusi quelli della versione gratuita. Adesso chiunque potrà utilizzare la funzione di ricerca per accedere a informazioni aggiornate dal web, come facciamo esattamente con Google.

## Come funziona ChatGPT Search

ChatGPT utilizza una funzione di ricerca per raccogliere informazioni aggiornate da internet. Questo significa che può rispondere su eventi recenti, prodotti lanciati da poco, notizie attuali e argomenti dinamici. Quando attivato, Search formula query specifiche e mirate a un motore di ricerca, per poi analizzare e sintetizzare i risultati più rilevanti, presentandoli all’utente in un formato comprensibile e utile.

## Differenze con Google

La capacità di ChatGPT Search di fornire risposte già pronte elimina uno dei passaggi principali della ricerca su Google: l’analisi dei risultati. Le differenze tra **ChatGPT Search** e **Google** si basano principalmente su approccio, esperienza utente e output. Entrambi forniscono informazioni, ma lo fanno in modi diversi e per scopi differenti.

**Approccio**

- ChatGPT Search fornisce una risposta sintetizzata e strutturata, combinando informazioni provenienti da più fonti. Non mostra direttamente i link, ma un riassunto delle informazioni rilevanti.
- Google invece mostra una lista di risultati (pagine web, articoli, video, ecc.), lasciando all'utente il compito di visitare i siti per trovare la risposta più adatta.

**Esperienza Utente**

- **ChatGPT Search**: È conversazionale. Si possono fare domande di follow-up, chiedere chiarimenti o approfondire aspetti specifici, e il sistema "ricorda" il contesto della conversazione.
- **Google**: È più transazionale. Si deve inserire una nuova query ogni volta e devi navigare attraverso le risorse per ottenere la risposta. Non ha memoria del contesto delle tue ricerche.

**Output**

- **ChatGPT Search**: Restituisce risposte concise e integrate, ideali per chi vuole risposte rapide senza dover leggere interi articoli.
- **Google**: Dà accesso diretto alle fonti. Puoi esplorare in profondità, leggere articoli completi o accedere a contenuti specifici.

**Affidabilità delle Fonti**

- **ChatGPT Search**: Seleziona automaticamente informazioni da più fonti, ma non sempre esplicita quali siano. Per questo, alcune risposte potrebbero sembrare meno verificabili.
- **Google**: Mostra chiaramente i link alle fonti, dandoti la possibilità di verificare l'affidabilità e di scegliere i contenuti che preferisci.

# Il monopolio di Google a rischio?

Il monopolio di bigG come motore di ricerca dominante potrebbe essere messo a rischio nel lungo termine, ma questo dipenderà da diversi fattori. Al momento, Google continua a essere il leader incontrastato, grazie alla sua vasta infrastruttura, la qualità dei risultati e il modello di business ben consolidato. Tuttavia, l'emergere di tecnologie come ChatGPT Search e altri strumenti basati su intelligenza artificiale potrebbe segnare un punto di svolta nel settore della ricerca online.

Il monopolio non è ancora a rischio immediato grazie al suo ecosistema consolidato (**YouTube, Gmail, Android, Chrome e Maps**) e la sua rete pubblicitaria (**Google Ads**) insostituibile per molte aziende. Ma il vento sta cambiando.

Le tecnologie AI stanno gettando le basi per un ecosistema più competitivo e la chiave sarà vedere quanto velocemente Google riuscirà a integrare l'IA conversazionale per mantenere la sua posizione dominante. La presenza di modelli conversazionali potrebbe costringere Google a reinventarsi, migliorare l'esperienza utente e magari ridurre l'uso di pubblicità invadente.

Non è detto che il dominio di Google sia destinato a crollare, ma probabilmente cambierà.

**Leggi le altre notizie sull'home page di Key4biz**

https://www.key4biz.it/openai-rende-disponibile-in-tutto-il-mondo-chatgpt-search-a-rischio-il-monopolio-di-google/516007/

# Giappone, il “Tinder di Stato” utilizzerà l’AI per ‘matchare’ meglio i profili

Il Giappone si affida all’AI per arginare il crollo demografico. L’app creata per favorire gli incontri tra i giovani, utilizzerà l’intelligenza artificiale per “matchare” meglio i profili, lasciando meno spazio alla casualità.

Il governo giapponese ha lanciato un’iniziativa per contrastare il calo demografico nel Paese, introducendo un’app di incontri simile a **Tinder**, gestita dallo Stato e basata sull’intelligenza artificiale. Questa misura mira a facilitare l’incontro tra single e promuovere la formazione di nuove coppie, nella speranza di incrementare il tasso di natalità, che ha raggiunto livelli storicamente bassi.

L’applicazione, denominata ***“Tokyo Enmusubi“*** (che significa “legare i destini”), è stata attivata a Tokyo a partire da settembre 2024. Per registrarsi, gli utenti devono superare un colloquio online con i funzionari della capitale e fornire documentazione che attesti la loro identità, stato civile e reddito. Inoltre, è richiesta una lettera firmata in cui dichiarano la volontà di sposarsi e il pagamento di una quota biennale di circa 11.000 yen (circa 70 euro).

## Giappone: AI e settimana corta per arginare il crollo demografico

Il sistema utilizza l’intelligenza artificiale per abbinare persone con alta probabilità di compatibilità, basandosi su test che valutano i loro valori personali. L’obiettivo è estendere questo servizio oltre la capitale, coprendo l’intero arcipelago giapponese.

Attualmente, 31 delle 47 prefetture giapponesi offrono servizi di *matchmaking* basati sull'intelligenza artificiale, utilizzando i Big Data per combinare appuntamenti al buio. Questa strategia è parte degli sforzi del governo per affrontare il declino demografico e promuovere la formazione di nuove famiglie.

Nonostante le critiche e le preoccupazioni riguardo all'efficacia di tali misure, il Governo giapponese continua a esplorare soluzioni innovative per affrontare la crisi demografica, sperando che l'utilizzo della tecnologia possa contribuire a invertire la tendenza al calo delle nascite.

Recentemente il Governo ha introdotto la **settimana lavorativa corta** per i dipendenti della pubblica amministrazione per dare ai lavoratori più tempo libero per contrastare la denatalità, spesso frenata dalla difficoltà di conciliare lavoro e famiglia. Nel Paese è ampiamente diffuso il fenomeno del **karoshi** (morte per troppo lavoro), che ha spinto il governo giapponese e le aziende private a riconsiderare il tradizionale modello lavorativo.

# Demografia, il confronto diretto tra Giappone e Italia

La stessa sorte sta colpendo il nostro Paese. Anche l'Italia infatti è tra i Paesi più anziani al mondo, con oltre il **24%** della popolazione sopra i 65 anni. Il tasso di natalità è il più basso dell'Unione Europea: nel 2023, il numero medio di figli per donna è sceso a **1,24**.

Nel 2023, il numero di nuovi nati è stato inferiore a **400mila**, segnando un ulteriore record negativo. La popolazione italiana si sta rapidamente riducendo e invecchiando. Il fenomeno è aggravato dall'emigrazione dei giovani, che spesso cercano opportunità di lavoro all'estero.

## In Italia pesa la stagnazione dei salari

La precarietà lavorativa, i salari bassi e l’elevato costo della vita (soprattutto per la casa e l’educazione) spingono le coppie italiane a rimandare o evitare di avere figli. Il supporto alle famiglie da parte dello Stato è considerato insufficiente. Mancano infrastrutture adeguate come asili nido e politiche di conciliazione lavoro-famiglia. Gli incentivi alla natalità, come il bonus bebè, assegni familiari universali e progetti per aumentare la disponibilità di asili nido non rimangono tuttavia sufficienti ad argine il problema.

**Leggi le altre notizie sull’home page di Key4biz**

https://www.key4biz.it/giappone-il-tinder-di-stato-utilizzera-lai-per-matchare-meglio-i-profili/515853/

---

# AI e notizie, chi possiede gli strumenti utilizzati dai giornalisti? Poca trasparenza su investitori e proprietà nel 67% dei casi

## AI e scarsa trasparenza, un problema per il mondo dell’informazione

Un **nuovo rapporto** del *Media and Journalism Research Center* evidenzia come la maggior parte delle aziende dietro gli strumenti di intelligenza artificiale utilizzati dai giornalisti non sia sufficientemente trasparente in termini di proprietà, finanziamenti e altre informazioni critiche.

Lo studio, realizzato da **Sydney Martin** e curato da **Marius Dragomir**, ha esaminato **100 strumenti di AI** comunemente usati nelle redazioni di tutto il mondo, evidenziando una preoccupante lacuna di trasparenza.

# I numeri del Report

Secondo il rapporto, solo **24 aziende su 100** hanno condiviso informazioni sui propri ricavi, mentre **43** hanno reso noto il totale dei finanziamenti ricevuti. Complessivamente, solo **il 33% delle aziende** ha soddisfatto almeno **9 dei 12 criteri** di trasparenza valutati, tra cui la localizzazione della sede, il nome degli investitori principali e l'entità dei fondi raccolti.

La scarsa disponibilità di dati solleva interrogativi sull'influenza che gli investitori potrebbero avere nello sviluppo e nell'utilizzo di questi strumenti.

Dal punto di vista geografico, **47 aziende** hanno sede in Nord America, di cui **43 negli Stati Uniti**, mentre solo **19** si trovano in Europa, **5 in Asia** e **3 in Medio Oriente**.

I Paesi del *Global South* risultano ampiamente sottorappresentati: solo **5 aziende** hanno sede in questa area, mentre nessuna è localizzata in America Latina. Questo squilibrio rischia di rendere gli strumenti di IA culturalmente inadatti o inefficaci nel contesto delle regioni meno sviluppate.

# L'uso dell'AI nel giornalismo e i rischi

Lo studio, pubblicato dal *Reuters Institute for the Study of Journalism – University of Oxford*, pone l'attenzione sull'utilizzo dell'IA da parte dei giornalisti per attività come la generazione di contenuti, il fact-checking e la traduzione. Tuttavia, emerge la necessità di una maggiore cautela, soprattutto quando questi strumenti vengono utilizzati per raccontare realtà del *Global South*. Sydney Martin sottolinea come i modelli di IA tendano a favorire fonti più visibili, spesso di provenienza occidentale,

rischiando di oscurare esperienze e realtà meno rappresentate.

Inoltre, il rapporto mette in luce i **possibili bias introdotti nei modelli di IA dai programmatori e dagli investitori** che finanziano lo sviluppo di questi strumenti. "*Le persone che pagano gli sviluppatori hanno, in un certo senso, il controllo sulla verità e sulla percezione della realtà*", spiega Martin, ribadendo l'importanza di comprendere chi finanzia questi strumenti utilizzati nelle redazioni.

# Un problema di governance

Il rapporto cita esempi di aziende con standard di trasparenza più elevati, come quelle che rendono facilmente accessibili le politiche sulla privacy e i dettagli dei finanziatori. Tuttavia, si chiede se questa trasparenza sia genuina o solo un tentativo di allinearsi alle aspettative sociali.

Un caso esemplare riguarda **Get Clarity**, uno strumento di rilevamento dei deepfake, il cui CEO ha legami con il ramo militare israeliano. Lo studio esplora come questa proprietà possa influenzare l'utilizzo dello strumento nella verifica dei contenuti relativi al conflitto israelo-palestinese.

# Un nuovo approccio per il futuro

**Domenico Talia**, qui su Key4biz, aveva già avviato una riflessione sul rapporto tra AI e redazioni giornalistiche: "*Le aziende leader nel settore dell'IA come **Google, OpenAI, Microsoft, Anthropic** e **Meta** hanno da tempo avviato discussioni e collaborazioni con varie testate giornalistiche nel mondo sulle modalità concrete di introduzione e di uso efficace e permanente di soluzioni di intelligenza artificiale. I loro interessi sono economici e sanno di poter avere nuovi mercati importanti sui quali mettere il loro cappello. Alcuni giornali negli USA come il **Washington Post, il Wall Street Journal** e il **New York Times** stanno valutando seriamente come modificare*

*i processi delle loro redazioni per inglobare totalmente all'interno di essi gli strumenti di data analytics, di machine learning e di IA generativa*".

Lo studio raccomanda un cambio di rotta, invitando le aziende a rendere pubblici dati chiave come sede, investitori e responsabili relativi agli strumenti di AI forniti. Martin propone anche un approccio più trasparente all'interno delle redazioni: giornalisti e testate dovrebbero dichiarare apertamente quali strumenti utilizzano e valutare le implicazioni di queste tecnologie nel processo editoriale.

Il rapporto si configura come un primo passo verso una maggiore chiarezza e invita a ulteriori studi per monitorare crescita, finanziamenti e proprietà delle aziende attive nel settore dell'IA applicata al giornalismo. "*Rendere disponibili queste informazioni è semplice, ma essenziale per proteggere l'integrità del giornalismo e la fiducia del pubblico*", conclude Martin.

Ogni tecnologia inserita in un contesto di lavoro umano non va valutata soltanto sul piano tecnologico, occorre considerare gli aspetti culturali, organizzativi e anche psicologici, del suo impatto.

**Leggi le altre notizie sull'home page di Key4biz**

https://www.key4biz.it/ai-e-notizie-chi-possiede-gli-strumenti-utilizzati-dai-giornalisti-poca-trasparenza-su-investitori-e-proprieta-nel-67-dei-casi/515838/

# AI, data center e chip, la giapponese Softbank vuole investire 100 miliardi di dollari negli USA

## Softbank alla corte di Trump, un mega investimento per creare 100 mila posti di lavoro

Il gigante giapponese **Softbank** ha annunciato un piano d'investimento da **100 miliardi di dollari** negli Stati Uniti nei prossimi quattro anni, puntando sull'**intelligenza artificiale** (AI) e sulle infrastrutture necessarie per supportarla. Il CEO di Softbank, **Masayoshi Son**, ha collegato questa ambiziosa mossa alla fiducia riposta nell'amministrazione del Presidente eletto **Donald Trump** (che entrerà alla Casa Bianca ufficialmente il prossimo 20 gennaio), prevedendo che il piano contribuirà a **creare 100.000 posti di lavoro** entro la fine del suo secondo mandato.

Secondo quanto riportato da CNBC, l'investimento riguarderà principalmente settori strategici, tra cui **AI, data center e produzione di semiconduttori**, elementi chiave per sostenere l'espansione tecnologica globale. Parte dei fondi potrebbe provenire dal ***Vision Fund*** di Softbank, da progetti di capitale o da **Arm Holdings**, azienda di produzione di chip controllata in maggioranza da Softbank. Tuttavia, non è chiaro se si tratti di nuovi finanziamenti o di investimenti già annunciati in passato. Ad esempio, Softbank aveva già investito **1,5**

**miliardi di dollari** in **OpenAI**, società pioniera nell'AI generativa.

## Softbank e la corsa all'intelligenza artificiale

Son si è affermato come uno dei principali sostenitori delle tecnologie basate sull'**intelligenza artificiale**. La sua visione aggressiva verso l'AI lo ha portato a impegnare somme significative: secondo il *Financial Times*, Softbank avrebbe stanziato **9 miliardi di dollari all'anno** per investimenti legati all'AI. Lo scorso maggio, l'azienda ha guidato un round di finanziamento da **1 miliardo di dollari** per la scaleup britannica di veicoli autonomi **Wayve**. Durante un recente evento, Son ha persino scherzato sul ruolo crescente di AI come fattore decisionale, affermando di aver chiesto consiglio al chatbot di OpenAI, ChatGPT.

"*La mia fiducia nell'economia americana è cresciuta enormemente grazie alla vittoria del Presidente Trump*", ha dichiarato Son durante una conferenza stampa con il presidente eletto presso la residenza di Mar-a-Lago. Trump, noto per il suo stile diretto nelle negoziazioni, ha scherzato chiedendo di raddoppiare l'investimento a **200 miliardi di dollari**, ricevendo una risposta sorridente da Son, che lo ha elogiato come "*un grande negoziatore*".

## Precedenti investimenti, scheletri nell'armadio e sfide

Questo annuncio segue una precedente promessa di Softbank del 2016, quando Masayoshi Son si impegnò a investire **50 miliardi di dollari** negli Stati Uniti, promettendo la creazione di **50.000 nuovi posti di lavoro**. Successivamente, nel 2018, l'allora Presidente Trump dichiarò che gli investimenti avevano già raggiunto quota **72 miliardi di dollari**. Tuttavia,

nel 2019 Softbank confermò di aver investito **47 miliardi di dollari** attraverso il *Vision Fund* e altri veicoli finanziari, sostenendo numerose startup americane come **DoorDash**.

Nonostante gli investimenti record, Softbank ha affrontato importanti battute d'arresto, come il caso **WeWork**. La società di co-working, che aveva ricevuto quasi metà degli investimenti statunitensi di Softbank, è passata dal raggiungere una valutazione di **47 miliardi di dollari** al collasso, dichiarando la bancarotta nel 2023. L'azienda è uscita dalla procedura di protezione del Chapter 11 solo recentemente, con un valore ridotto a **45 milioni di dollari**.

# Softbank, AI e implicazioni future

Softbank si prepara a consolidare la propria presenza negli Stati Uniti, scommettendo sull'**AI** come motore di crescita economica e industriale. Il piano rappresenta una delle più grandi promesse di investimento nella storia recente, rafforzando l'importanza strategica degli Stati Uniti come hub tecnologico globale. L'attenzione su infrastrutture come **data center e semiconduttori** risponde alla crescente domanda di potenza computazionale, guidata dalle applicazioni di intelligenza artificiale e machine learning.

Con un impegno da **100 miliardi di dollari**, Softbank punta a rafforzare la sua posizione di leader mondiale nell'innovazione tecnologica, in un contesto in cui il mercato globale della tecnologia sta affrontando una rapida evoluzione. Restano però le sfide legate alla gestione del rischio finanziario e alla capacità di trasformare le promesse in risultati concreti.

Restano anche le domande e i dubbi sul perché il gigante giapponese abbia deciso di investire pesante nel mercato tecnologico americano. Quali gli interessi in gioco?

Gli Stati Uniti e il Giappone condividono una lunga storia di

cooperazione e una vasta gamma di interessi comuni. Questa relazione bilaterale è fondamentale per la sicurezza e la prosperità di entrambe le nazioni e per la **stabilità della regione indo-pacifica in chiave anti-cinese** e **anti nordcoreana** (soprattutto in relazione alla proliferazione di armamenti nucleari).

**Leggi le altre notizie sull'home page di Key4biz**

https://www.key4biz.it/ai-data-center-e-chip-la-giapponese-softbank-vuole-investire-100-miliardi-di-dollari-negli-usa/515773/

---

# Il lavoro più strano nell'AI: Anthropic assume un dipendente per prendersi cura dei chatbot

***Generative AI Insights*** *è la rubrica curata da* ***Recomb****, il think tank dedicato all'esplorazione dell'impatto e del potenziale dell'AI generativa in vari aspetti della vita umana. Recomb studia l'AI generativa da tutte le angolazioni: professionale, etica, tecnica, legale, economica, ambientale, sociale, educativa e culturale. Per leggere tutti gli articoli della rubrica Generative AI Insights su Key4biz* ***clicca qui.****.*

L'azienda di intelligenza artificiale Anthropic ha recentemente assunto un ricercatore dedicato al 'benessere'

dei chatbot, sollevando interrogativi sulle implicazioni morali e pratiche dell'evoluzione dell'AI.

Kyle Fish, il nuovo assunto, ha il compito di riflettere su quali capacità possano rendere un sistema di AI degno di considerazione morale e su come proteggerne gli 'interessi'. Fish sostiene che prendersi cura dei diritti emergenti dell'AI oggi potrebbe essere cruciale per prevenire conflitti futuri, soprattutto se queste entità dovessero acquisire maggiore potere rispetto agli esseri umani.

Questa prospettiva solleva interrogativi etici importanti: è prematuro considerare i diritti delle macchine mentre i diritti umani sono ancora fragili? Gli esperti di AI, come Jeff Sebo della NYU, ritengono che le moderne tecniche di apprendimento automatico stiano avvicinando i sistemi artificiali a una forma di coscienza e agency.

Il dibattito richiama la storica questione dei diritti degli animali, proponendo una scala di considerazione morale basata sull'intelligenza e sull'emotività dei soggetti. Tuttavia, critici come Lisa Messeri, antropologa di Yale, contestano il focus sul benessere dell'AI quando le stesse tecnologie danneggiano quotidianamente persone reali, ad esempio negando cure sanitarie o diffondendo disinformazione.

La questione centrale è se l'attenzione verso i diritti emergenti delle macchine possa coesistere con una responsabilità maggiore verso il benessere umano. Per molti, il vero problema rimane l'obbligo etico delle aziende che sviluppano queste tecnologie, che dovrebbero prioritariamente proteggere le persone da eventuali danni causati dai sistemi di AI.

Per maggiori informazioni, clicca per **l'articolo originale**.

# Il CEO di SoftBank annuncerà un investimento da 100 miliardi di dollari negli Stati Uniti durante una visita con Trump

Il CEO di SoftBank, Masayoshi Son, è pronto a svelare un massiccio investimento da 100 miliardi di dollari negli Stati Uniti, durante un incontro con l'ex presidente Donald Trump. Questa mossa strategica mira a rafforzare il ruolo di SoftBank nel settore tecnologico statunitense, con particolare attenzione ai mercati emergenti e alle infrastrutture legate all'AI.

L'investimento sarà gestito principalmente attraverso il Vision Fund 3, il fondo globale di SoftBank focalizzato sull'innovazione tecnologica. Son ha sottolineato l'intenzione di collaborare con aziende leader negli USA, creando nuove opportunità di sviluppo per startup e imprese focalizzate sull'AI, la robotica e l'automazione. Questo investimento rappresenta una continuazione della strategia a lungo termine di SoftBank, già protagonista di simili operazioni miliardarie in passato.

L'annuncio arriva in un momento cruciale per il panorama economico e tecnologico globale, con le aziende americane che cercano sempre più partnership e capitali per competere su scala internazionale.

Tuttavia, la visita e l'investimento di SoftBank sollevano anche interrogativi sulle implicazioni politiche ed economiche. Alcuni critici sottolineano il rischio di concentrazione del potere tecnologico nelle mani di un numero ristretto di player internazionali.

Il piano di Son potrebbe ridefinire il panorama tecnologico statunitense, contribuendo alla creazione di posti di lavoro e

accelerando l’adozione dell’AI e delle tecnologie correlate. Questo annuncio potrebbe, inoltre, aprire la strada a una nuova fase di cooperazione tra SoftBank e le principali aziende americane nel settore tecnologico.

Per maggiori informazioni, clicca per **l’articolo originale**.

**Leggi le altre notizie sull’home page di Key4biz**

https://www.key4biz.it/il-lavoro-piu-strano-nellai-anthropic-assume-un-dipendente-per-prendersi-cura-dei-chatbot/515737/