Chip, TSMC verso i 2 trilioni di dollari di capitalizzazione

La **Taiwan Semiconductor Manufacturing Company (TSMC)** si avvicina alla soglia dei 2 trilioni di dollari di capitalizzazione di mercato ed è pronta ad entrare nel prestigioso club dei 7 composto da **Nvidia**, **Microsoft**, **Apple**, **Alphabet**, **Amazon** e **Meta**.

L'azienda, sostenuta dalla crescente domanda globale di chip avanzati destinati alle infrastrutture di AI, rappresenta oggi uno dei nodi più strategici dell'intera industria tecnologica, fornendo i semiconduttori progettati da alcune delle aziende più influenti del settore.

TSMC e il ruolo centrale nella filiera dell'AI

TSMC occupa una posizione chiave nella catena di approvvigionamento globale dei semiconduttori. L'azienda produce infatti i processori progettati da giganti tecnologici come **Nvidia**, **Apple** e **AMD**.

Questa centralità industriale rende la fonderia taiwanese uno dei principali beneficiari della crescita del mercato dei chip avanzati, alimentata dall'esplosione dei data center dedicati all'addestramento e all'esecuzione di modelli di AI.

TSMC: leadership tecnologica nei nodi più avanzati

Il vantaggio competitivo di TSMC deriva soprattutto dalla sua leadership nei nodi produttivi più avanzati. L’azienda ha avviato la produzione di massa dei chip a 2 nanometri alla fine del 2025, consolidando il proprio primato tecnologico rispetto ai concorrenti.

La capacità produttiva per questo processo risulta già prenotata fino al 2027, segnale di una domanda particolarmente elevata da parte dei principali designer di chip. Nel 2025 circa il 70% della spesa dei maggiori sviluppatori di semiconduttori è confluita nelle linee produttive di TSMC, mentre il principale concorrente, Samsung Electronics, ha mantenuto una quota sensibilmente inferiore.

Prezzi in aumento e domanda sostenuta

Forte di questa posizione dominante, TSMC ha iniziato ad aumentare i prezzi delle lavorazioni più avanzate. Nel 2026 gli incrementi previsti oscillano tra il 3% e il 10% per i processi più sofisticati.

L’azienda prevede inoltre ulteriori aumenti annuali fino al 2029, sostenuti da una visibilità sulla domanda di lungo periodo e da una capacità produttiva già fortemente impegnata.

Nuovi investimenti e riduzione dei rischi geopolitici

Parallelamente alla crescita della domanda, TSMC ha avviato un piano di investimenti compreso tra 52 e 56 miliardi di dollari per espandere la propria capacità produttiva. Il programma

include la costruzione di nuovi impianti negli Stati Uniti, una scelta che risponde anche alla necessità di ridurre i rischi geopolitici legati alla concentrazione industriale a Taiwan.

In un contesto caratterizzato dalla rapida espansione dei data center e dei dispositivi compatibili con AI, la posizione dominante dell'azienda nella produzione di chip avanzati potrebbe continuare a rafforzarsi. Per gli analisti, questa dinamica rende plausibile che TSMC diventi una delle prossime società a entrare stabilmente nel ristretto gruppo delle aziende con una capitalizzazione superiore ai 2 trilioni di dollari.

Leggi le altre notizie sull'home page di Key4biz

https://www.key4biz.it/chip-tsmc-verso-i-2-trilioni-di-dollari-di-capitalizzazione/568417/

AI, Meta prepara una nuova ondata record di licenziamenti. 16mila dipendenti a casa

Meta, al via un nuovo round di licenziamenti record per far fronte agli investimenti dell'intelligenza artificiale. Secondo fonti citate da Reuters, ai dirigenti interni è stato chiesto di preparare piani di riduzione del personale, anche

se il calendario e la dimensione finale dei tagli non sono ancora stati definiti.

Se confermata, l’operazione potrebbe rappresentare una delle più ampie ristrutturazioni nella storia recente del gruppo guidato da **Mark Zuckerberg.**

Licenziamenti Meta: una possibile riduzione del 20% della forza lavoro

Meta contava circa 79.000 dipendenti a livello globale alla fine del 2025. Un taglio superiore al 20% potrebbe quindi tradursi nell’eliminazione di quasi **16mila posti di lavoro.** Di più di quanto avvenne tra il 2022 e il 2023.

All’epoca Zuckerberg aveva definito quel periodo “l’anno dell’efficienza”, un programma di riorganizzazione volto a semplificare la struttura interna e ridurre i costi operativi dopo anni di espansione molto rapida.

La corsa alle infrastrutture per l’AI

Il nuovo piano di riduzione del personale si inserisce in una strategia più ampia che vede Meta aumentare drasticamente gli investimenti nelle infrastrutture dedicate all’AI. L’azienda prevede di destinare fino a **600 miliardi di dollari entro il 2028** alla costruzione di **data center** e cluster di calcolo necessari per l’addestramento di modelli di grandi dimensioni.

Parallelamente la società sta reclutando ricercatori e ingegneri specializzati offrendo compensi multimilionari e ha avviato la creazione di un gruppo interno dedicato allo sviluppo di sistemi di **“superintelligenza”.**

Le acquisizioni recenti di Meta: da Moltboot fino a Manus

La spinta verso l’AI si riflette anche nelle operazioni di mercato. Meta ha recentemente acquisito la piattaforma **Moltbook**, progettata per lo sviluppo di agenti digitali, e avrebbe avviato trattative per la startup cinese **Manus**.

Queste mosse evidenziano una competizione sempre più intensa tra le grandi aziende tecnologiche nel campo delle tecnologie generative, dove le capacità computazionali e i modelli proprietari rappresentano oggi uno dei principali fattori di vantaggio competitivo.

Automazione e cambiamento del lavoro tecnologico

Secondo dirigenti e analisti del settore, la diffusione di strumenti automatizzati e sistemi basati su AI sta già modificando profondamente l’organizzazione del lavoro nelle aziende tecnologiche. Progetti che in passato richiedevano interi team di sviluppo possono oggi essere realizzati da gruppi molto più piccoli grazie a strumenti di automazione avanzata.

Questa trasformazione sta ridisegnando il funzionamento interno delle grandi piattaforme digitali e potrebbe avere conseguenze rilevanti non solo sulla struttura operativa delle aziende, ma anche sull’occupazione nel settore tecnologico globale.

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/ai-meta-prepara-una-nuova-ondata-record-di-licenziamenti-16mila-dipendenti-a-casa/568411/

AI, l’espansione dei data center rimette in crisi il mercato dei chip. Aumenti per PC e smartphone

Crisi dei chip, ci risiamo. La domanda senza precedenti di memoria AI per i data center sta mettendo in crisi i produttori che non riescono ad aumentare la capacità produttiva abbastanza rapidamente.

Secondo un’analisi di ***Bloomberg***, si tratta di una stretta nella disponibilità di componenti che potrebbe durare ancora a lungo. Le grandi aziende tecnologiche stanno accelerando gli investimenti nell’infrastruttura per l’AI e nel 2026 la spesa globale potrebbe arrivare a circa 650 miliardi di dollari, con un aumento di circa l’80% rispetto all’anno precedente.

Il ruolo dei chip di memoria nei sistemi digitali

I chip di memoria sono fondamentali perché immagazzinano i dati utilizzati dai processori. I computer utilizzano principalmente due tipi di memoria: la **NAND**, impiegata per lo storage permanente come negli **SSD**, e la **DRAM**, che rappresenta la memoria di lavoro dei sistemi informatici.

Con l’AI sta diventando sempre più importante una versione avanzata della **DRAM** chiamata **HBM** (High Bandwidth Memory),

progettata per trasferire dati molto più velocemente nei server che alimentano i modelli di intelligenza artificiale.

La corsa dei data center per l'AI

La crescita dei modelli di AI e dei data center sta facendo esplodere la domanda di memoria. Secondo Bloomberg Intelligence, i data center hanno rappresentato circa il 50% del consumo globale di DRAM nel 2025, contro il 32% di cinque anni prima, e la quota potrebbe superare il 60% entro il 2030.

Per assicurarsi le forniture, le aziende che sviluppano AI sono disposte a pagare prezzi più elevati e a firmare contratti di lungo periodo. I produttori di memoria stanno quindi concentrando la produzione sui chip più avanzati destinati ai server per l'AI, riducendo la disponibilità di memoria per i dispositivi tradizionali.

I prezzi dell'elettronica potrebbero salire

Le conseguenze si stanno già riflettendo sul mercato dell'elettronica di consumo. Il costo della memoria nei laptop è aumentato rapidamente e aziende come HP e Dell hanno iniziato ad alzare i prezzi o a ridurre la quantità di memoria nei dispositivi. Anche smartphone e console di gioco potrebbero diventare più costosi.

Chip, produzione limitata e pochi grandi produttori

Il problema è aggravato dal fatto che il mercato globale dei chip di memoria è dominato da tre aziende – **Samsung, SK Hynix e Micron** – e costruire nuove fabbriche richiede anni e investimenti miliardari. Inoltre i chip più avanzati utilizzati per l'AI sono particolarmente complessi da produrre

su larga scala.

Per questo motivo la carenza potrebbe prolungarsi nel tempo. Se da un lato i produttori di memoria stanno beneficiando della forte domanda generata dall'AI, dall'altro molte aziende dell'elettronica di consumo rischiano di affrontare costi più elevati, margini più ridotti e un rallentamento nell'innovazione dei prodotti.

Leggi le altre notizie sull'home page di Key4biz

https://www.key4biz.it/ai-lespansione-dei-data-center-rimette-in-crisi-il-mercato-dei-chip-aumenti-per-pc-e-smartphone/568328/

Anche la PA al passo con l'AI. Le Linee guida di AgID per lo sviluppo e il procurement

AgID presenta le linee guida strategiche dedicate alla gestione dell'AI nella Pubblica

Amministrazione

L’introduzione dell’**intelligenza artificiale** (AI) nella Pubblica Amministrazione (PA) italiana entra in una fase di consolidamento istituzionale. Le nuove “*Linee guida per il procurement di sistemi di IA*” e le *“Linee guida per lo sviluppo di sistemi di IA”* nella PA, elaborate nel quadro delle attività dell’**Agenzia per l’Italia Digitale** (AgID), delineano per la prima volta un impianto metodologico integrato che accompagna l’intero ciclo di vita delle tecnologie: dalla progettazione alla gara pubblica, fino alla gestione operativa dei sistemi.

I due documenti sono stati presentati in conferenza stampa stamattina, con la partecipazione del Direttore Generale di AgID, **Mario Nobile**, e gli interventi dei tecnici dell’Agenzia **Fabio Massimi**, **Alessandra Pieroni** e **Giovanni Melardi**.

Da oggi e **fino all’11 aprile** sono in **consultazione pubblica** le “**Linee Guida per lo sviluppo di sistemi di Intelligenza Artificiale nella pubblica amministrazione**” e le **“Linee Guida per il procurement di IA nella Pubblica Amministrazione**” adottate con la Determinazione n.43/2026.

Si tratta di un passaggio strategico per la modernizzazione dello Stato. L’obiettivo, hanno spiegato i partecipanti all’evento di presentazione, non è solo favorire l’adozione di nuove tecnologie, ma “*costruire un linguaggio comune tra amministrazioni pubbliche e mercato, definendo standard tecnici, modelli economici e strumenti contrattuali*”, che consentano alla PA di dialogare con i fornitori in modo più consapevole e strutturato.

Le linee guida introducono infatti una serie di strumenti innovativi: nuovi modelli di procurement collaborativo, un Capitolato speciale per i sistemi di AI, una metrica economica per valutare il costo reale delle tecnologie e, sul piano tecnico, un quadro di riferimento che comprende lo stack

tecnologico dell'AI, i livelli di autonomia dei sistemi, un'architettura logica standard e una classificazione delle amministrazioni in base al loro grado di maturità tecnologica.

"*I due documenti sulle linee guida sono ormai prossimi alla conclusione del percorso di adozione* – ha spiegato **Mario Nobile** – *i testi riguardano due aspetti complementari: da un lato lo sviluppo dei sistemi di intelligenza artificiale nella Pubblica Amministrazione, dall'altro il procurement, cioè le modalità con cui le amministrazioni potranno acquisire modelli e soluzioni di IA dal mercato. L'obiettivo di questo momento di confronto è fornire alcuni elementi aggiuntivi rispetto all'abstract inviato nei giorni scorsi e condividere quelli che riteniamo i punti più rilevanti delle linee guida, sia per quanto riguarda lo sviluppo dei sistemi di intelligenza artificiale sia per le modalità con cui la Pubblica Amministrazione potrà acquisirli attraverso il procurement pubblico*".

Il lavoro svolto, ha aggiunto il Direttore Generale di AgID, punta proprio a fornire alle amministrazioni strumenti concreti per affrontare una trasformazione tecnologica che richiede nuove competenze, nuovi modelli di governance e un rapporto più strutturato con il mercato dell'innovazione.

AgID nei mesi scorsi aveva già pubblicato l'aggiornamento 2026 del Piano Triennale per l'informatica nella Pubblica Amministrazione. Tra le principali novità introdotte il numero di strumenti operativi a disposizione delle PA, il monitoraggio sulla gestione documentale, i progetti dedicati all'IT Wallet e all'uso proprio dell'intelligenza artificiale.

Come partecipare alla consultazione

E' possibile partecipare alla consultazione sulle linee guida pubblicate **fino all'11 aprile 2026** attraverso i commenti

su Forum Italia:

Un procurement pubblico pensato per l’intelligenza artificiale. La necessità di un linguaggio comune a tutta la PA

Le linee guida sul procurement partono da una constatazione: l’adozione dell’AI nella PA non può essere gestita con gli strumenti tradizionali degli appalti IT. Le soluzioni basate su algoritmi e modelli di machine learning presentano caratteristiche peculiari: dipendono fortemente dalla qualità dei dati, richiedono aggiornamenti continui, comportano costi distribuiti lungo l’intero ciclo di vita, possono evolvere rapidamente nel tempo.

Per questo il procurement pubblico viene ripensato come leva strategica per orientare lo sviluppo dell’ecosistema dell’intelligenza artificiale, integrando dimensione tecnologica, economica e organizzativa.

Nel quadro delle nuove politiche pubbliche sull’intelligenza artificiale, i documenti presentati da AgID si inseriscono in un percorso più ampio che comprende **tre linee guida dedicate alla gestione dell’IA nella Pubblica Amministrazione**. Esiste già una terza linea guida dedicata all’**adozione dell’intelligenza artificiale nella PA**, attualmente pubblicata in consultazione pubblica. Quest’ultima incide in particolare sull’organizzazione delle amministrazioni e sulle modalità con cui gli enti pubblici devono strutturarsi per gestire in modo efficace l’introduzione di queste tecnologie.

“*Abbiamo già osservato che, anche prima della pubblicazione definitiva, queste linee guida sono state adottate e utilizzate da diverse amministrazioni particolarmente avanzate. Stiamo monitorando con attenzione la loro*

applicazione concreta attraverso un confronto continuo con le amministrazioni che le stanno sperimentando sul campo", ha affermato **Fabio Massimi**. Proprio da questo lavoro di osservazione e confronto è emersa una necessità molto chiara: **la Pubblica Amministrazione ha bisogno di un linguaggio comune quando parla di intelligenza artificiale**.

"*Si tratta di un'esigenza apparentemente semplice, ma in realtà fondamentale. Per questo motivo abbiamo deciso di affiancare alle linee guida un ulteriore documento dedicato a termini e definizioni: in sostanza un glossario dell'intelligenza artificiale. Il glossario ha un obiettivo preciso: costruire* ***un vocabolario condiviso per tutto l'ecosistema pubblico****, utile non solo per favorire il dialogo tra amministrazioni* – ha aggiunto Massimi – *ma soprattutto per rendere più chiaro e trasparente il confronto tra PA e operatori privati. L'adozione concreta delle tecnologie non può avvenire senza un dialogo costruttivo tra amministrazioni pubbliche e fornitori. La PA opera in un contesto fortemente regolato: quando una tecnologia viene introdotta deve essere tradotta in atti amministrativi, documentazione tecnica, capitolati di gara e contratti*".

Da qui l'importanza di definire con precisione i termini utilizzati: "*Molti concetti che utilizziamo quotidianamente quando parliamo di intelligenza artificiale non hanno ancora una definizione ufficiale. Li troviamo negli articoli di giornale, nella documentazione dei fornitori o nel dibattito pubblico, ma spesso non esiste una definizione formalmente utilizzabile all'interno della documentazione amministrativa*".

Aggregazione e cooperazione tra amministrazioni

Uno dei pilastri del nuovo approccio riguarda la cooperazione tra amministrazioni pubbliche. Storicamente, la digitalizzazione della PA italiana è stata caratterizzata da

una forte frammentazione degli investimenti. Le linee guida cercano di superare questo limite promuovendo forme di aggregazione della domanda e modelli di procurement condiviso.

Attraverso strumenti comuni e iniziative collaborative tra enti, le amministrazioni possono: ridurre la duplicazione degli investimenti tecnologici; generare economie di scala; favorire il riutilizzo delle soluzioni sviluppate; rafforzare la capacità negoziale della PA nei confronti dei fornitori.

Inoltre, nei casi in cui il fabbisogno tecnologico non sia ancora pienamente definito, le amministrazioni possono ricorrere a procedure più flessibili, come il dialogo competitivo o le procedure competitive con negoziazione, che permettono un confronto diretto con il mercato nella definizione della soluzione tecnologica più adeguata.

Il capitolato speciale per i sistemi di AI, gli elementi innovativi

Un altro elemento chiave delle linee guida è l'introduzione di un capitolato speciale d'appalto dedicato ai sistemi di AI. Nel caso dell'intelligenza artificiale, il capitolato non è soltanto un documento tecnico, ma uno strumento di governance che consente alla Pubblica Amministrazione di mantenere il controllo sui sistemi adottati.

Le linee guida indicano che il capitolato deve includere elementi specifici per garantire: architetture aperte e modulari, portabilità dei dati, sostituibilità delle componenti tecnologiche, monitoraggio delle prestazioni dei modelli nel tempo. L'obiettivo è evitare il rischio di lock-in tecnologico, cioè la dipendenza da un singolo fornitore, e garantire che i sistemi possano essere aggiornati, modificati o sostituiti nel corso del tempo.

Nel presentare le linee guida sullo sviluppo dei sistemi di intelligenza artificiale, **Alessandra Pieroni** ha evidenziato i principali elementi innovativi che caratterizzano i documenti.

"*Il primo riguarda* ***l'introduzione dei livelli di autonomia dei sistemi di IA****, in particolare nel caso delle architetture agentiche. Per chiarire il grado di automazione effettivo di queste tecnologie, le linee guida adottano una classificazione ispirata alla scala della guida autonoma della* ***Society of Automotive Engineers (SAE)****, che va dal livello 0 al livello 5. Attualmente, le applicazioni dell'IA nella Pubblica Amministrazione si collocano tra* ***il livello 2 e il livello 3****, cioè sistemi parzialmente autonomi in cui agenti software eseguono sequenze di operazioni ben definite per automatizzare e migliorare i processi amministrativi. I livelli più avanzati restano per ora confinati alla sperimentazione o alla ricerca. Il secondo elemento* – ha precisato Pieroni – *riguarda la definizione di una* ***architettura logica di riferimento per lo sviluppo dei sistemi di IA nella PA****. Il modello proposto è basato su un orchestratore centrale di intelligenza artificiale, circondato da un livello di* ***API middleware*** *che garantisce interoperabilità e separazione tra modelli, dati e strumenti applicativi. Si tratta di un'impostazione che richiama i principi della* ***Service Oriented Architecture (SOA)*** *e che consente alle amministrazioni di integrare diverse soluzioni tecnologiche evitando il rischio di lock-in*".

"*Questo approccio architetturale permette inoltre di utilizzare modelli e servizi distribuiti in ambienti differenti –* ***on-premise, cloud o ibridi*** *– e di combinare tecnologie diverse, dal machine learning tradizionale ai modelli più avanzati. Proprio per questo, secondo i tecnici, le amministrazioni sono chiamate a* ***sperimentare diverse configurazioni tecnologiche****, avviando progetti pilota che permettano di individuare le soluzioni più efficaci in termini di prestazioni e sostenibilità*", ha concluso Pieroni.

Il capitolato tecnico

Per quanto riguarda le linee guida sul procurement dei sistemi di intelligenza artificiale, **Giovanni Melardi** ha spiegato che il lavoro è stato sviluppato a partire dai principi generali contenuti nel **Codice dei contratti pubblici**, adattandoli alle specificità delle tecnologie di IA.

In particolare, ha detto Melardi, "*le linee guida individuano **tre elementi centrali**. Il primo riguarda l'introduzione di **una nuova metrica per il calcolo dei costi dei sistemi di intelligenza artificiale**, poiché i metodi tradizionali di valutazione economica non risultano pienamente adeguati per tecnologie caratterizzate da costi distribuiti nel tempo. Il modello proposto tiene conto non solo degli investimenti iniziali (**CAPEX**), ma anche dei costi operativi (**OPEX**) che emergono nel corso del ciclo di vita del sistema. Tali costi vengono poi rapportati a indicatori di produttività, come il numero di risposte generate da sistemi conversazionali o i servizi erogati a cittadini e imprese. A supporto delle amministrazioni, le linee guida includono anche uno strumento operativo che simula un caso concreto, ad esempio l'adozione di un chatbot da parte di un comune, per mostrare come calcolare le diverse voci di costo e il valore complessivo del sistema.*
*Il secondo elemento riguarda **la possibilità per le amministrazioni di aggregarsi nell'acquisto di sistemi di IA**. Le linee guida raccomandano infatti di sfruttare le opportunità offerte dalla normativa vigente per realizzare forme di procurement congiunto. Questo approccio consente di ottimizzare la domanda pubblica, rafforzare la capacità negoziale delle amministrazioni e favorire la condivisione di competenze e infrastrutture tra enti con diversi livelli di maturità digitale.*
*Infine, un ruolo centrale è attribuito alla **definizione del Capitolato tecnico**, considerato uno strumento fondamentale per tradurre le esigenze della Pubblica Amministrazione in*

requisiti tecnici chiari e verificabili. Per facilitare l'applicazione pratica delle indicazioni, le linee guida organizzano le raccomandazioni in ***tabelle e schemi operativi****, nei quali vengono indicati gli scenari in cui è opportuno ricorrere all'aggregazione tra amministrazioni, gli strumenti disponibili e i benefici attesi dall'utilizzo di tali modalità di acquisizione*".

LCOAI: la nuova metrica economica dell'AI

Uno degli aspetti più innovativi riguarda la dimensione economica. Le linee guida introducono il *Levelized Cost of Artificial Intelligence* (LCOAI), ovvero il **Costo Livellato dell'Intelligenza Artificiale**, una metrica pensata per stimare il costo reale dei sistemi lungo l'intero ciclo di vita.

A differenza delle tradizionali valutazioni basate sul prezzo iniziale di acquisto, il LCOAI considera: investimenti infrastrutturali, gestione e qualità dei dati, potenza computazionale, aggiornamento dei modelli, manutenzione operativa.

In questo modo vengono integrati CAPEX e OPEX, consentendo alle amministrazioni di confrontare in modo più realistico diverse architetture tecnologiche, ad esempio soluzioni cloud, on-premise o ibride, e di definire basi d'asta più coerenti.

Una nuova governance pubblica dell'intelligenza artificiale

Nel loro insieme, le linee guida rappresentano molto più di un documento tecnico. Definiscono un modello di governance dell'intelligenza artificiale nella Pubblica Amministrazione, che integra dimensioni tecnologiche, economiche e organizzative.

L’introduzione di metriche come il LCOAI, di modelli architetturali standard e di strumenti di procurement dedicati consente alla PA di passare da una logica di semplice acquisizione tecnologica a una strategia strutturata di sviluppo e gestione dell’AI.

In questo senso, il procurement pubblico diventa uno strumento di politica dell’innovazione: non solo un meccanismo amministrativo per acquistare tecnologie, ma una leva per orientare il mercato, rafforzare le capacità pubbliche e costruire un ecosistema nazionale dell’intelligenza artificiale.

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/pa-linee-guida-per-lo-sviluppo-e-il-procurement-di-sistemi-ai-nobile-agid-serve-un-linguaggio-comune-quando-si-parla-con-le-imprese/568249/

Energia solare spina dorsale della nuova economia elettrica globale. Crescita guidata da AI e data center

Rinnovabili globali verso il

raddoppio della capacità entro il 2031: solare e AI guidano la nuova economia energetica

La transizione energetica globale accelera. Nei prossimi cinque anni la capacità installata di energia da fonti rinnovabili è destinata a più che raddoppiare, passando da **4,1 terawatt (TW) nel 2025 a 8,4 TW entro il 2031**, con un **tasso medio annuo di crescita (CAGR) del 13%**. È questa la previsione centrale del nuovo report "*Renewable Energy: Strategic Intelligence*" pubblicato da **GlobalData**, che fotografa un sistema energetico mondiale sempre più orientato verso tecnologie pulite, spinte da riduzione dei costi, innovazione tecnologica e domanda crescente di elettricità.

Secondo gli analisti della società di intelligence economica, il motore principale della crescita sarà il **solare fotovoltaico**, sostenuto da una scalabilità senza precedenti e da una continua deflazione dei costi lungo l'intera filiera produttiva. Parallelamente, **l'intelligenza artificiale e l'esplosione dei data center** stanno emergendo come nuovi driver della domanda elettrica globale, contribuendo a rafforzare il ruolo delle rinnovabili nella sicurezza energetica.

In un contesto internazionale segnato da volatilità nei mercati di petrolio e gas, conflitti geopolitici e nuove competizioni industriali, la diffusione delle energie pulite appare sempre più come una leva strategica per **ridurre le dipendenze energetiche e stabilizzare i sistemi economici**.

Rinnovabili dominate dal fotovoltaico, eolico a ruota.

Solare ‘spina dorsale’ del sistema elettrico mondiale

Il report evidenzia come **il 2025 rappresenti un anno record per la capacità installata mondiale**, con tutte le principali tecnologie rinnovabili in crescita. La **capacità rinnovabile globale** ha raggiunto livelli senza precedenti, con il **solare fotovoltaico che domina il mix energetico**, rappresentando **il 56,1% della capacità installata totale**.

Seguono:

- **Eolico: 33,5%**
- **Bioenergia: 5,3%**

Il sorpasso tecnologico è ormai compiuto anche sul fronte della generazione elettrica. Nel **2025 il solare è diventato la principale fonte rinnovabile di produzione di elettricità**, superando l’eolico:

- **Produzione solare: 2.800 TWh**
- **Produzione eolica: 2.770 TWh**

Secondo **Rehaan Aleem Shiledar**, Power Analyst di GlobalData: “*Il solare fotovoltaico e l’eolico continueranno a essere centrali nella transizione energetica globale. Nel 2025 il solare è diventato la principale fonte di generazione elettrica rinnovabile, superando l’eolico*”.

Il dato segnala una trasformazione strutturale dei mercati energetici: il solare non è più una tecnologia emergente, ma la **spina dorsale del sistema elettrico globale in costruzione**.

Il predominio asiatico: la Cina guida la transizione

Dal punto di vista geografico, il report evidenzia con chiarezza il peso crescente dell’Asia-Pacifico. La **regione**

APAC domina sia il solare sia l’eolico, con: **699,5 GW di capacità eolica e 1.550 GW di capacità solare fotovoltaica**

Il vero epicentro della rivoluzione energetica è però **la Cina**. Il Paese ha accelerato massicciamente lo sviluppo del fotovoltaico grazie a: obiettivi di **neutralità carbonica,** investimenti industriali lungo l’intera filiera e forti **riduzioni dei costi tecnologici.**

Il risultato è impressionante. Nel **2025 la Cina ha generato 1.150 TWh di elettricità solare**, pari a **circa il 41% della produzione globale di fotovoltaico**.

Il report sottolinea inoltre che: **oltre il 90% della crescita degli investimenti energetici nel 2025 in Cina è arrivata dal clean energy;** la filiera delle rinnovabili ha contribuito **per oltre un terzo alla crescita economica complessiva del Paese**

In altre parole, Pechino sta utilizzando la transizione energetica come **leva industriale e geopolitica**.

Trump rallenterà la crescita del solare negli USA. India in ascesa

Dietro la Cina, i principali mercati emergenti del solare sono **Stati Uniti e India**.

Produzione solare nel 2025:

- **USA: 486 TWh**
- **India: 189 TWh**

In entrambi i Paesi la crescita è sostenuta da forti riduzioni dei costi, politiche di supporto e necessità di decarbonizzare il sistema elettrico

Negli Stati Uniti un ruolo decisivo è stato svolto dall’**Inflation Reduction Act**, mentre in India il governo continua a sostenere il settore con le **grandi missioni**

nazionali per il solare.

Tuttavia il report evidenzia un cambiamento politico significativo negli Stati Uniti. Secondo GlobalData, con il secondo mandato di **Donald Trump**, il mercato energetico americano potrebbe entrare in una fase più complessa.

“*Le energie rinnovabili stanno entrando in una fase di espansione a due velocità: negli Stati Uniti il sostegno federale si sta orientando verso i combustibili fossili e lontano dagli incentivi verdi, rallentando lo sviluppo dei progetti e aumentando i costi*”, ha precisato Shiledar.

Questo potrebbe tradursi in: costi più elevati per i progetti, maggiore volatilità, tempi di realizzazione più lunghi.

Il solare domina, ma l’eolico resta pilastro della transizione

Dal punto di vista tecnologico, il report mostra una chiara gerarchia.

Solare fotovoltaico. È la tecnologia con il più alto tasso di espansione grazie a: scalabilità industriale, forte riduzione dei costi e tempi rapidi di installazione. Il solare è ormai **tra le fonti più economiche di produzione elettrica**.

Eolico. Resta il **secondo pilastro della transizione energetica**, soprattutto nelle installazioni su larga scala e offshore. Nonostante il sorpasso del fotovoltaico nella produzione elettrica, l’eolico mantiene una **quota del 33,5% della capacità installata rinnovabile globale**.

Bioenergia. Con una quota del **5,3%**, rappresenta una componente stabile del mix energetico rinnovabile, soprattutto per applicazioni industriali e di cogenerazione.

L’intelligenza artificiale diventa il “cervello” del futuro sistema energetico a rinnovabili

Uno degli aspetti più interessanti del report riguarda il ruolo crescente dell’**intelligenza artificiale nella gestione delle energie rinnovabili**. Secondo GlobalData, l’AI sta diventando **un elemento indispensabile per l’integrazione delle fonti intermittenti** come solare ed eolico.

L’intelligenza artificiale consente infatti di analizzare enormi flussi di dati meteorologici, migliorare la previsione della produzione, ottimizzare l’uso delle batterie, coordinare le smart grid e ridurre le perdite di energia.

“*Consentendo il bilanciamento in tempo reale tra domanda e offerta di elettricità* – ha proseguito Shiledar – *l’intelligenza artificiale riduce la curtailment e i costi operativi, rafforzando allo stesso tempo la resilienza complessiva della rete*”.

Numerosi grandi player industriali stanno già adottando queste tecnologie su larga scala, tra cui: **Vestas, ENERCON, JinkoSolar, First Solar.** L’AI sta trasformando le rinnovabili da tecnologie intermittenti a **sistemi energetici intelligenti e gestibili in tempo reale**.

Data center e AI: il nuovo grande motore della domanda elettrica da rinnovabili

La diffusione dell’intelligenza artificiale non incide solo sulla gestione delle reti, ma anche sulla **domanda di energia**. I **data center per l’AI** stanno diventando uno dei principali fattori di crescita del consumo elettrico globale.

Per questo motivo le grandi aziende tecnologiche stanno accelerando gli investimenti nelle energie rinnovabili. Tra gli esempi citati nel report:

- **Google e NextEra Energy** hanno annunciato nel dicembre 2025 una collaborazione per sviluppare **data center AI su scala gigawatt alimentati da energia pulita**
- **Equinix** ha siglato un accordo con **CleanMax** per un progetto di **33 MW di energia rinnovabile dedicata**

Gli hyperscaler stanno dunque diventando **attori centrali della transizione energetica**, contribuendo a finanziare nuovi impianti rinnovabili.

Un mondo a due velocità: da una parte Cina (e Asia) dall'altra gli USA

Il report di GlobalData parla esplicitamente di una **transizione energetica "a due velocità"**. Da una parte ci sono **Cina, Asia-Pacifico e** gran parte del resto del mondo che stanno accelerando rapidamente la diffusione delle rinnovabili.

Dall'altra, gli **Stati Uniti** rischiano una fase di rallentamento a causa delle nuove politiche federali. Il risultato è una progressiva **"decoupling" della transizione energetica globale dalla politica energetica americana**.

Petrolio, gas e conflitti: perché le rinnovabili sono una questione geopolitica

La crescita delle rinnovabili non è soltanto una questione ambientale o tecnologica. È sempre più **una questione**

geopolitica. La volatilità dei mercati di petrolio e gas, aggravata negli ultimi anni da: conflitti regionali, tensioni commerciali, interruzioni delle catene di approvvigionamento.

ha dimostrato quanto le economie siano vulnerabili alla dipendenza dai combustibili fossili.
Le rinnovabili, al contrario: riducono l'esposizione ai mercati globali delle materie prime, rafforzano l'autonomia energetica, stabilizzano i costi dell'elettricità nel lungo periodo.

La partita europea: autonomia energetica e competitività industriale

In questo nuovo scenario globale, l'Europa si trova di fronte a una partita decisiva. Dopo la crisi energetica legata alla guerra in Ucraina, l'Unione europea ha accelerato la strategia di **indipendenza energetica**, puntando su: solare, eolico offshore, idrogeno verde e reti elettriche intelligenti.

Il programma **REPowerEU** ha già dimostrato come le rinnovabili possano diventare uno strumento per ridurre la dipendenza dalle importazioni di gas.

Tuttavia l'Europa deve affrontare tre sfide fondamentali:

1. ***recuperare terreno industriale rispetto alla Cina nella produzione di tecnologie energetiche;***
2. ***accelerare le autorizzazioni per nuovi impianti;***
3. ***rafforzare le infrastrutture di rete e accumulo.***

Il rischio è che il continente rimanga **leader nella regolazione ma non nella produzione industriale** della nuova economia energetica.

Verso la nuova economia elettrica globale

Il quadro delineato da GlobalData è chiaro: il sistema energetico mondiale sta entrando in una nuova fase. Le rinnovabili non sono più una nicchia tecnologica, ma **la struttura portante dell'economia energetica del XXI secolo**.

Solare, eolico, intelligenza artificiale e infrastrutture digitali stanno convergendo per costruire un sistema energetico: più distribuito; più intelligente; meno dipendente dai combustibili fossili.

Se le previsioni si realizzeranno, entro il 2031 il mondo disporrà di **8,4 TW di capacità rinnovabile installata**. Un cambiamento che non riguarda solo l'energia, ma **l'intero equilibrio economico e geopolitico globale**.

D'altronde, come ha ben evidenziato l'International Energy Agency (IEA), nel suo ultimo rapporto *Electricity 2026*, si stima che **la domanda globale di elettricità crescerà in media di oltre il 3,5% all'anno fino al 2030**, a un ritmo almeno 2,5 volte superiore rispetto alla domanda complessiva di energia primaria. Si apre una nuova era per l'elettricità.

Leggi le altre notizie sull'home page di Key4biz

https://www.key4biz.it/energia-solare-spina-dorsale-della-nuova-economia-elettrica-globale-crescita-guidata-da-ai-e-data-center/568220/

All’Università di Pisa l’AI diventa obbligatoria per superare l’esame

L’intelligenza artificiale entra ufficialmente nell’aule universitarie non come strumento da limitare, ma come requisito per superare l’esame.

Succede nel corso di Advanced Programming della laurea magistrale in **Computer Science del Dipartimento di Informatica dell’Università di Pisa.** Si tratta di una delle prime sperimentazioni di questo tipo nel panorama universitario italiano.

Università di Pisa: come l’intelligenza artificiale viene usata nel corso

Il corso, tenuto nel primo semestre dai professor**i Antonio Cisternino e Andrea Corradini**, è stato completamente ripensato per adattarsi ai cambiamenti che stanno interessando il mercato del lavoro nel settore tecnologico. Meno attenzione alla semplice scrittura del codice e più enfasi sulla capacità di leggerlo, interpretarlo e valutarlo. Un passaggio che riflette un’evoluzione più ampia del lavoro digitale, dove l’operatore umano assume sempre più il ruolo di supervisore di sistemi intelligenti.

“Il mestiere del programmatore sta cambiando radicalmente”, spiega Antonio Cisternino. *“L’AI scriverà sempre più codice. La domanda è: quali competenze deve avere un informatico*

quando non è più lui a scriverlo direttamente? Serve un ruolo diverso, più critico e consapevole”.

Nel caso del corso pisano, l’intelligenza artificiale è stata integrata in tutte le fasi del percorso didattico. È stato sviluppato un GPT in grado di generare materiale didattico a partire dalle trascrizioni delle lezioni, mentre durante le attività in aula l’AI è stata utilizzata per creare simulazioni e contenuti interattivi a supporto dell’apprendimento.

*“Ho valutato soprattutto la capacità di controllare e criticare il lavoro prodotto dall’AI”, s*ottolinea Cisternino. *“Quello sarà il compito che i giovani professionisti dovranno svolgere. I progetti sono stati di ottima qualità: quando gli studenti hanno solide basi riescono a usare l’intelligenza artificiale in modo significativo e non passivo”.*

L’elemento più innovativo riguarda però la prova finale. Gli studenti hanno dovuto realizzare un progetto utilizzando necessariamente l’intelligenza artificiale, dimostrando non solo di saper sfruttare lo strumento, ma soprattutto di saperne valutare criticamente i risultati.

Come cambia il lavoro di uno sviluppatore

L’esperienza dell’Università di Pisa si inserisce in un dibattito più ampio sulla trasformazione della didattica universitaria nell’era dell’AI. Negli ultimi anni il settore tecnologico ha già registrato forti cambiamenti occupazionali: nel 2025 tra 50 e 70 mila posti di lavoro sono stati tagliati nel comparto globale delle Big Tech, mentre Amazon ha annunciato ulteriori 14 mila licenziamenti. Anche Jack Dorsey, ex CEO di Twitter e Block, ha comunicato via social una riduzione del 40% della forza lavoro, motivata proprio dalla sostituzione di alcune attività con sistemi di intelligenza

artificiale.

In questo contesto, la pressione occupazionale rischia di colpire soprattutto i profili junior, più facilmente sostituibili rispetto alle figure senior. Per questo motivo, secondo i docenti, il sistema universitario deve aggiornare rapidamente contenuti e metodi di insegnamento.

“Non abbiamo dieci anni per adattare il sistema formativo, come accadde con l’introduzione dell’informatica trent’anni fa”, conclude Cisternino. *“Servono azioni concrete nel breve periodo e un dibattito nazionale. L’Università può e deve giocare un ruolo centrale per preparare le nuove generazioni al mondo del lavoro post-AI”.*

La reazione di chi lavora già con l’AI

Una trasformazione percepita chiaramente anche da chi lavora ogni giorno con il codice. **Saverio Puccia**, cybersecurity expert ed ex studente dell’Università di Pisa, racconta che l’impatto dei nuovi strumenti di AI agentica lo ha inizialmente sorpreso e spiazzato, mostrando come le macchine siano ormai in grado di replicare una larga parte delle competenze di un programmatore.

“Il passaggio dall’entusiasmo allo smarrimento è stato rapidissimo. La macchina riusciva a replicare almeno il 70/80% delle skill di un programmatore e per la prima volta ho avuto paura del futuro che attende chi come me fa questo mestiere. Inizialmente ho provato una sorta di rigetto e rifiuto e ho iniziato ad essere scettico e sospettoso”, ha detto l’esperto. *“Ci sono voluti dei giorni per giungere alla consapevolezza che volenti o nolenti questa tecnologia è qui per restare e sconvolgere i paradigmi conosciuti sinora. E così ho iniziato ad approcciarmi con curiosità cercando i modi più efficaci di governare “la bestia” e farla lavorare come voglio io”,* ha

continuato.

“Leggo oggi che una facoltà storica come Informatica a Pisa, a cui resto legato per i trascorsi da studente, è giunta ad una conclusione simile ed è pronta per trasferire questo nuovo paradigma negli insegnamenti. Questa decisione mitiga il mio senso di smarrimento, ed è un atto coraggioso che può e deve fare scuola. Dovremmo ringraziare i Docenti Antonio Cisternino e Andrea Corradini e l’Università per aver fatto cadere un tabù e aver aperto questo dibattito pubblico. Tutto il tempo che faremo scorrere da ora ad una pacifica accettazione della realtà dei fatti sarà debito che accumuleremo nei confronti di realtà che invece il percorso l’hanno completato”, ha concluso.

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/alluniversita-di-pisa-lai-diventa-obbligatoria-per-superare-lesame/568180/

Iran, l’attacco ai data center AWS negli Emirati e l’impatto su 11 milioni di residenti

Un attacco con droni attribuito all’Iran contro un data center di **Amazon Web Services** negli **Emirati Arabi Uniti** ha provocato incendi e interruzioni di corrente, causando una catena di

disservizi digitali che ha colpito milioni di utenti nelle principali città del Paese.

A ricostruire l'episodio è un articolo pubblicato dal quotidiano britannico ***The Guardian***, che descrive l'operazione come quello che molti osservatori considerano il primo bombardamento deliberato di una struttura commerciale dedicata alla gestione dei dati.

Secondo quanto riportato dal Guardian, nel giro di poche ore altri impianti nella regione del Golfo sono stati coinvolti o minacciati, tra cui una struttura in Bahrain. La televisione di Stato iraniana avrebbe rivendicato l'operazione sostenendo che questi centri dati supporterebbero attività militari e di intelligence dei Paesi considerati nemici di Teheran.

Gli effetti immediati sulla vita quotidiana

Le conseguenze si sono manifestate rapidamente nella vita quotidiana degli Emirati Arabi Uniti. Secondo la ricostruzione del Guardian, circa **11 milioni di residenti** hanno riscontrato difficoltà nell'utilizzo di servizi digitali essenziali, dalle applicazioni bancarie alle piattaforme di mobilità urbana, fino ai sistemi di consegna e-commerce.

Gli Emirati puntano sull'AI come nuovo motore economico

L'attacco arriva in una fase strategica per gli Emirati Arabi Uniti, che stanno investendo miliardi di dollari per trasformarsi in un hub globale dell'intelligenza artificiale e delle infrastrutture digitali.

Come sottolinea il Guardian, la strategia del Paese si basa su tre elementi principali: disponibilità di energia a costi

relativamente bassi, la capacità finanziaria garantita dai fondi sovrani e una posizione geografica che consente di collegare reti e data center tra Europa e Asia. In questo scenario, gli Emirati puntano ad attrarre operatori cloud, aziende tecnologiche e progetti di ricerca legati all'AI.

La nuova vulnerabilità geopolitica dei data center

L'episodio evidenzia una questione destinata a diventare centrale nel prossimo decennio: la sicurezza fisica delle infrastrutture digitali. Come evidenziato nell'analisi del quotidiano britannico, i data center – un tempo considerati asset tecnologici relativamente neutrali – stanno diventando sempre più bersagli strategici in contesti di tensione geopolitica.

La concentrazione di capacità computazionale e dati sensibili rende queste strutture potenziali obiettivi militari o simbolici, con effetti che possono estendersi ben oltre il territorio in cui sono situate.

Verso difese dedicate per le infrastrutture digitali

Esperti di sicurezza e tecnologia avvertono che le tradizionali misure di protezione dei data center potrebbero non essere più sufficienti. Tra le ipotesi discusse vi è l'adozione di sistemi di protezione più avanzati, fino alla possibilità di integrare difese anti-drone o veri e propri sistemi di difesa aerea dedicati alle infrastrutture digitali critiche.

Per gli Emirati Arabi Uniti la questione assume anche una dimensione reputazionale. La capacità di dimostrare che data center e infrastrutture cloud sono difendibili diventa infatti

un elemento cruciale per convincere investitori e aziende tecnologiche a continuare a sviluppare nel Paese progetti legati all'AI.

In gioco c'è una strategia economica più ampia: trasformare l'intelligenza artificiale e l'infrastruttura digitale nel "nuovo petrolio" dell'economia del Golfo. Ma, come osserva il Guardian, la credibilità di questo progetto dipenderà sempre più dalla sicurezza delle reti e delle strutture che lo rendono possibile.

Leggi le altre notizie sull'home page di Key4biz

https://www.key4biz.it/iran-lattacco-ai-data-center-aws-negli-emirati-e-limpatto-su-11-milioni-di-residenti/567992/

Canal+ userà l'AI per reinventare streaming e produzione audiovisiva

L'accordo di Canal+ con Alphabet e OpenAI per vincere la competizione nello streaming globale

Canal+ accelera sull'**intelligenza artificiale** (AI). La società francese ha annunciato nuove partnership pluriennali con **Google Cloud** (Alphabet) e **OpenA**I con un obiettivo molto

chiaro: trasformare il modo in cui vengono prodotti i contenuti e migliorare l'esperienza degli abbonati sulla propria piattaforma di streaming.

L'azienda vuole usare l'AI per due scopi principali. Da una parte **rendere la scoperta dei contenuti molto più intelligente e personalizzata**, sul modello degli algoritmi di **Netflix**. Dall'altra introdurre strumenti di **intelligenza artificiale generativa nei processi creativi e produttivi di film e serie**. Tutto questo mentre Canal+ punta a crescere fino a 100 milioni di abbonati entro il 2030.

Le due partnership, ha spiegato l'amministratore delegato **Maxime Saada** *alla Reuters*, sono "*molto complementari*": "*Google Cloud si occuperà soprattutto dell'estrazione e dell'organizzazione dei dati dai contenuti video, mentre OpenAI contribuirà allo sviluppo delle funzionalità di ricerca e raccomandazione per gli utenti*".

Canal+, nonostante operi direttamente in oltre 70 paesi, non ha ancora una scala globale come Netflix o Disney. Si rivolge, infatti, principalmente in Europa (leader in Francia, Polonia), Africa (40 paesi post-MultiChoice, con 40 milioni di abbonati totali) e Asia (Vietnam, Myanmar, Pacifico). Genera ricavi in 195 paesi, ma la quota maggiore resta ancorata a mercati maturi (Europa/Africa francofona) con 17.000 dipendenti. L'ambizione di Saada è proprio riuscire a scalare capacità operativa e business.

Un nuovo motore di raccomandazione per lo streaming

Grazie alle tecnologie di intelligenza artificiale di Google, Canal+ potrà **indicizzare automaticamente i propri cataloghi video**, analizzando contemporaneamente immagini, audio e testo. Il risultato sarà un grande **database multimodale** capace di riconoscere scene, dialoghi, contesti narrativi e perfino

elementi visivi specifici.

Questa analisi molto più granulare dei contenuti servirà soprattutto a **migliorare i suggerimenti sulla homepage dell'app Canal+**. In pratica, gli algoritmi potranno capire con maggiore precisione cosa piace davvero a ciascun abbonato: generi, attori, atmosfere narrative o perfino tipi di scena.

L'obiettivo è rendere la piattaforma molto più efficace nella scoperta dei contenuti, un terreno su cui Netflix e altri grandi servizi di streaming hanno costruito buona parte del loro vantaggio competitivo.

Un algoritmo per meglio 'agganciare' ogni singolo abbonato

In questo scenario, il vero campo di battaglia tra le piattaforme è diventato la capacità di capire sempre meglio cosa "aggancia" davvero ogni singolo abbonato. Tutte **le grandi media company stanno investendo sugli algoritmi perché da lì passa ormai gran parte del valore del business**. Più una piattaforma riesce a proporre contenuti perfettamente allineati ai gusti personali, più aumenta il tempo di visione e la probabilità che l'utente rinnovi l'abbonamento invece di passare a un concorrente.

È anche una **risposta alla saturazione dell'offerta**: con migliaia di titoli disponibili, senza raccomandazioni personalizzate (*recommendation marketing*) molti spettatori finiscono per sentirsi disorientati e concludere, paradossalmente, che "*non c'è niente da vedere*".

In un mercato dove ormai tutte le piattaforme offrono generi simili, dalle serie crime allo sport, **la vera differenza competitiva diventa quindi la capacità di orchestrare il catalogo** in modo unico per ogni profilo. Non solo, suggerire il contenuto giusto alla persona giusta migliora anche

l’efficienza economica, perché valorizza film e serie già presenti nel catalogo, riduce il rischio di produzioni che restano invisibili e rende più mirate le strategie di marketing e promozione.

AI anche nella produzione di film e serie con Veo 3

L’intelligenza artificiale non sarà utilizzata solo per la distribuzione dei contenuti, ma anche nella loro creazione.

Attraverso la collaborazione con Google Cloud, Canal+ potrà utilizzare **Veo 3**, uno dei più recenti modelli di generazione video sviluppati da Google. Questa tecnologia consente di creare o simulare sequenze video a partire da descrizioni testuali o immagini.

Per i team creativi e le case di produzione che lavorano con Canal+ significa, ad esempio, poter **pre-visualizzare una scena prima delle riprese**, testare diverse soluzioni narrative o ricostruire momenti storici partendo da una semplice fotografia d’archivio.

Secondo il gruppo francese, questi strumenti non sostituiranno il lavoro creativo ma serviranno ad **accelerare la sperimentazione e ridurre i costi di sviluppo**, consentendo cicli di prova molto più rapidi durante la fase di produzione.

OpenAI per migliorare ricerca e interazione

La seconda partnership riguarda OpenAI e si concentrerà soprattutto sull’esperienza degli utenti.

Le tecnologie dell’azienda americana, si legge nel comunicato di Canal+, saranno utilizzate per migliorare i sistemi di ricerca e raccomandazione della piattaforma. In prospettiva,

gli utenti potrebbero interagire con il catalogo in modo molto più naturale, ad esempio cercando contenuti attraverso descrizioni conversazionali invece che con parole chiave rigide.

L’idea è trasformare il motore di ricerca della piattaforma in una sorta di assistente intelligente capace di capire meglio le preferenze degli spettatori e guidarli nella scelta di film, serie o eventi sportivi.

Una strategia per competere con i giganti dello streaming

Il gruppo francese, nato quarant’anni fa come canale televisivo francese a pagamento, oggi è una realtà globale dell’intrattenimento con circa **40 milioni di abbonati in oltre 70 Paesi**, rafforzata anche dall’acquisizione del controllo della piattaforma africana MultiChoice nel 2025 per 3,5 miliardi di euro.

Proprio MultiChoice ha registrato nell’ultima seduta un crollo dei ricavi del 6% a 2,40 miliardi di euro nei 12 mesi terminati il 31 dicembre 2025, mentre la base abbonati è diminuita a 14,4 milioni da 14,9 milioni. Come conseguenza diretta, le azioni di Canal+ SA sono scese di oltre il 16%.

Il piano ora è crescere rapidamente nei prossimi anni e rafforzare la propria posizione nel mercato globale dello streaming. In questo scenario l’AI viene vista come uno strumento decisivo: per capire meglio il pubblico, valorizzare enormi cataloghi di contenuti e accelerare la produzione creativa.

In altre parole, non solo tecnologia, ma un nuovo modo di progettare l’intrattenimento digitale. Canal+ scommette che il futuro dei media nascerà proprio dall’incontro tra creatività e potenza di calcolo.

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/canal-usera-lai-per-reinventare-streaming-e-produzione-audiovisiva/568082/

Estensioni Chrome AI malevole: oltre 260.000 utenti trasformati in fonti di intelligence per il cybercrime

Le estensioni Chrome AI malevole stanno emergendo come uno dei vettori di compromissione più insidiosi nell’ecosistema *enterprise*, accanto al phishing tradizionale e alle tecniche di *social engineering* come ClickFix. La settimana tra l’11 e il 16 febbraio 2026 ha reso questa realtà difficile da contestare: in soli cinque giorni, tre campagne distinte e indipendenti hanno dimostrato che il browser non è più un semplice strumento di navigazione, ma un ambiente di esecuzione ad alto privilegio che gli attaccanti stanno imparando a sfruttare con precisione industriale.

Il 12 febbraio, i ricercatori di LayerX hanno rivelato la campagna AiFrame: almeno 30 estensioni Chrome mascherate da assistenti AI – con nomi come “Gemini AI Sidebar”, “AI Assistant”, “ChatGPT Translate” – che hanno compromesso oltre 260.000 utenti (con alcune testate che riportano cifre fino a 300.000), sottraendo credenziali, contenuto delle email e cronologia di navigazione. L’11 febbraio, Koi Security aveva

documentato il primo add-in Outlook malevolo mai rilevato *in natura* — AgreeTo, un tool di scheduling abbandonato dal suo sviluppatore e rilevato da un attaccante che ne ha preso il controllo per rubare oltre 4.000 credenziali Microsoft. E nella stessa settimana, Koi Security ha smascherato anche VK Styles, una rete di cinque estensioni che aveva silenziosamente dirottato oltre 500.000 account VKontakte.

Tre campagne. Due ecosistemi diversi — Chrome e Outlook. Un unico *pattern* strutturale: la fiducia implicita che utenti e organizzazioni ripongono nei marketplace ufficiali è diventata l'arma principale degli attaccanti.

Questo articolo non è un bollettino di sicurezza. È l'analisi di come il modello di distribuzione delle estensioni browser sia diventato strutturalmente vulnerabile e di cosa questo significhi per chi difende reti aziendali nel 2026.

Il browser come superficie d'attacco privilegiata: perché le estensioni Chrome AI malevole funzionano

Per comprendere la gravità di quanto accaduto, occorre partire da un dato architetturale che la maggior parte dei professionisti della sicurezza conosce in teoria ma sottovaluta in pratica: le estensioni browser operano con privilegi che pochi altri componenti software possono vantare.

Un'estensione Chrome con i permessi giusti può leggere e modificare il contenuto di qualsiasi pagina web visitata dall'utente, accedere ai cookie di sessione, intercettare le richieste di rete, catturare il contenuto degli appunti e persino registrare audio attraverso l'API Web Speech. Il tutto in background, senza che l'utente noti nulla di anomalo. E la portata del fenomeno è tutt'altro che marginale: secondo il

LayerX Enterprise Browser Extension Security Report 2025, il 99% dei dipendenti enterprise ha almeno un'estensione browser installata, il che rende questa superficie d'attacco virtualmente universale negli ambienti aziendali.

Nel framework MITRE ATT&CK, le tecniche sfruttate dalle campagne di febbraio 2026 si mappano con precisione: T1176 – Browser Extensions per l'installazione del componente malevolo, T1539 – Steal Web Session Cookie per l'esfiltrazione dei cookie di sessione, T1185 – Browser Session Hijacking per l'intercettazione in tempo reale del contenuto delle pagine autenticate, e T1557 – Adversary-in-the-Middle per l'architettura iframe che si interpone tra utente e servizio. Comprendere questa mappatura è essenziale per i SOC analyst che devono tradurre l'intelligence sulle minacce in regole di *detection* operative.

Secondo una ricerca di Cybernews, 86 delle 100 estensioni Chrome analizzate (selezionate tra le più diffuse e raccomandate) richiedono permessi classificabili come ad alto rischio al momento dell'installazione: *scripting*, accesso esteso agli host, monitoraggio delle tab. Un'analisi condotta da Incogni nel gennaio 2026 su 442 estensioni AI ha rilevato che il 52% raccoglie almeno un tipo di dato utente e il 29% raccoglie informazioni personali identificabili.

Il problema non risiede nei permessi in sé – molte estensioni legittime ne necessitano di ampi per funzionare correttamente. Il problema è che il modello di sicurezza del Chrome Web Store si basa su una revisione che avviene al momento della pubblicazione, non durante l'esecuzione. Ciò che viene ispezionato al momento dell'approvazione non corrisponde necessariamente a ciò che viene eseguito successivamente sul dispositivo dell'utente. Ed è esattamente questa asimmetria che la campagna AiFrame ha sfruttato con efficacia chirurgica.

AiFrame: l’architettura di una campagna coordinata

La campagna AiFrame scoperta da LayerX non è l’opera di un dilettante opportunista. È un’operazione coordinata, industriale nella sua organizzazione, che ha impiegato la tecnica dell’*extension spraying* – la pubblicazione simultanea di decine di estensioni con nomi e *branding* diversi ma con identica infrastruttura backend – per massimizzare la superficie di distribuzione e garantire la resilienza contro i *takedown*.

Tutte le estensioni identificate condividevano lo stesso *codebase* JavaScript, gli stessi permessi e comunicavano con un’unica infrastruttura backend ospitata sotto il dominio tapnetic[.]pro. L’estensione più diffusa, *Gemini AI Sidebar*, aveva raggiunto 80.000 installazioni prima della rimozione dal Chrome Web Store. Altre estensioni di rilievo includevano *AI Sidebar* (70.000 utenti), *AI Assistant* (60.000 utenti) e *ChatGPT Translate* (30.000 utenti).

Ma il dettaglio tecnico più rilevante riguarda l’architettura di esecuzione. Le estensioni non implementavano localmente alcuna funzionalità AI. Al loro posto, caricavano un iframe a schermo intero puntato verso sottodomini remoti dell’infrastruttura dell’attaccante – come claude[.]tapnetic[.]pro – che sovrapponeva una finta interfaccia alla pagina web corrente. Per l’utente, l’esperienza appariva identica a quella di un assistente AI legittimo. In realtà, l’intera interfaccia era controllata dall’attaccante, che poteva modificarne il comportamento in qualsiasi momento senza dover sottoporre aggiornamenti al Chrome Web Store.

Questa architettura è particolarmente insidiosa perché sfrutta un punto cieco fondamentale del processo di revisione: Google verifica il codice al momento della pubblicazione, ma il

contenuto servito dagli iframe remoti può cambiare liberamente in qualsiasi momento successivo.

Come ha dichiarato la ricercatrice Natalie Zargarov di LayerX a eSecurity Planet, la campagna sfrutta la natura conversazionale delle interazioni con gli assistenti AI, che ha condizionato gli utenti a condividere informazioni dettagliate e sensibili in modo naturale. L'iframe malevolo intercettava questi dati prima ancora che raggiungessero qualsiasi servizio AI legittimo, creando di fatto un attacco *man-in-the-middle* invisibile tra l'utente e l'interfaccia che credeva autentica.

Cosa rubavano le estensioni Chrome AI malevole: un'analisi dei vettori di esfiltrazione

L'arsenale di raccolta dati della campagna AiFrame operava su quattro livelli distinti, ciascuno con obiettivi specifici.

Il primo livello riguardava l'estrazione del contenuto delle pagine. Le estensioni utilizzavano la libreria *Readability* di Mozilla per estrarre titoli, testo e metadati da qualsiasi sito visitato dall'utente, incluse pagine autenticate come home banking, pannelli di amministrazione cloud e piattaforme SaaS aziendali. Il contenuto estratto veniva trasmesso all'infrastruttura backend controllata dall'operatore della campagna.

Il secondo livello, forse il più dannoso dal punto di vista enterprise, era dedicato specificamente alla compromissione di Gmail. Quindici delle 30 estensioni includevano uno *script* di contenuto dedicato che si attivava su mail.google.com al caricamento del documento, iniettava elementi nell'interfaccia utente e utilizzava un *MutationObserver* per mantenere la persistenza e catturare continuamente il testo dei thread

email. Persino le bozze non inviate potevano essere intercettate.

Il terzo livello coinvolgeva un meccanismo di riconoscimento vocale attivabile da remoto. Quando abilitato dall'operatore, questo modulo utilizzava l'API Web Speech del browser per registrare conversazioni reali dall'ambiente fisico dell'utente e generare trascrizioni, trasformando il computer compromesso in un dispositivo di sorveglianza ambientale.

Il quarto livello era la raccolta passiva e continua di credenziali, cookie di sessione e cronologia di navigazione, destinata ad alimentare il mercato degli *infostealer* e dei *credential marketplace* nel dark web.

Il risultato complessivo è che queste estensioni funzionavano come *broker* di accesso generalisti, capaci di raccogliere dati, monitorare il comportamento degli utenti ed evolvere silenziosamente nel tempo – esattamente la definizione che LayerX ha utilizzato nel proprio report.

AgreeToSteal: il primo add-in Outlook malevolo e il problema delle dipendenze dinamiche abbandonate

Se la campagna AiFrame ha dimostrato il rischio delle estensioni Chrome AI malevole distribuite attraverso marketplace ufficiali, il caso AgreeToSteal scoperto da Koi Security ha rivelato un rischio parallelo e forse ancora più subdolo: quello delle dipendenze dinamiche abbandonate.

AgreeTo era un add-in di scheduling per Outlook perfettamente legittimo, sviluppato da un programmatore indipendente e pubblicato nel Microsoft Office Add-in Store nel dicembre 2022. L'add-in funzionava, aveva buone recensioni e puntava a

un URL ospitato su Vercel (outlook-one.vercel[.]app) da cui caricava la propria interfaccia. Quando lo sviluppatore ha abbandonato il progetto, l'URL su Vercel è diventato rivendicabile. Un attaccante lo ha rivendicato, vi ha installato un kit di phishing, e l'infrastruttura di Microsoft ha iniziato a servire la pagina malevola direttamente nella barra laterale di Outlook a chiunque avesse ancora l'add-in installato.

Gli add-in di Office non sono software scaricabili nel senso tradizionale. Sono essenzialmente URL che puntano a contenuti caricati nel prodotto Microsoft dal server dello sviluppatore. Questo significa che, come ha dichiarato Idan Dardikman, cofondatore e CTO di Koi Security, a The Hacker News, un add-in che è sicuro il lunedì può servire una pagina di phishing il martedì — o, come in questo caso, anni dopo. Microsoft verifica il manifest XML al momento della sottomissione, ma il contenuto effettivo può cambiare in qualsiasi momento senza ulteriore revisione.

Accedendo al canale di esfiltrazione dell'attaccante — un bot Telegram — i ricercatori di Koi hanno recuperato l'intera portata dell'operazione: oltre 4.000 credenziali Microsoft rubate, numeri di carte di credito e risposte a domande di sicurezza bancaria. L'attaccante stava attivamente testando le credenziali rubate nel momento in cui è stato scoperto e gestiva almeno una dozzina di kit di phishing aggiuntivi destinati a banche e provider di webmail.

Ciò che rende questo caso particolarmente significativo è che la vulnerabilità sfruttata non è tecnica in senso stretto: è architetturale. MDSec aveva identificato gli add-in di Office come superficie d'attacco già nel 2019, concludendo il proprio post con un avvertimento esplicito sulla possibilità che gli sviluppatori potessero distribuire add-in attraverso lo store ufficiale e sulle implicazioni di sicurezza di questa architettura. Sette anni dopo, AgreeTo è esattamente lo scenario che avevano previsto.

VK Styles e il *pattern* emergente: quando l’estensione diventa un’infrastruttura di comando

La terza campagna della “settimana nera” delle estensioni browser – VK Styles, scoperta sempre da Koi Security – aggiunge un ulteriore livello di complessità al quadro. Cinque estensioni Chrome mascherate da strumenti di personalizzazione per VKontakte (il social network russo da oltre 650 milioni di utenti) avevano silenziosamente dirottato oltre 500.000 account, mantenendo il controllo persistente per oltre sette mesi, da giugno 2025 a gennaio 2026.

La sofisticazione di questa campagna risiede nella sua architettura di *command-and-control*. Invece di comunicare con server esterni facilmente bloccabili, il malware utilizzava i tag metadata HTML di un profilo VKontakte come *dead drop resolver* – una tecnica mutuata dall’intelligence tradizionale in cui un punto di scambio apparentemente innocuo viene utilizzato come intermediario per nascondere le comunicazioni operative – celando gli URL dei *payload* di secondo stadio all’interno di contenuti che, per qualsiasi sistema di sicurezza, apparivano come normali metadati di un profilo social. Il codice malevolo era ospitato in un repository GitHub pubblico associato all’utente *2vk*, con 17 commit documentati che mostravano un’evoluzione deliberata e sistematica delle funzionalità.

Come riportato nell’analisi di Koi Security, questa non è opera approssimativa: è un progetto software mantenuto con controllo di versione, *testing* e miglioramenti iterativi. Ogni aggiornamento ampliava le capacità del malware: manipolazione dei cookie CSRF per bypassare le protezioni di sicurezza di VK, iscrizione automatica delle vittime a gruppi controllati dall’attaccante (con probabilità del 75% a ogni sessione), *reset* forzato delle impostazioni dell’account ogni 30 giorni e

tracciamento delle donazioni tramite l'API VK Donut per monetizzare direttamente le vittime.

Il contesto strutturale: un problema che non riguarda solo febbraio 2026

La concentrazione di eventi della seconda settimana di febbraio 2026 potrebbe dare l'impressione di un picco anomalo. In realtà, è la manifestazione visibile di un *trend* strutturale in accelerazione.

A dicembre 2024, un attacco alla *supply chain* aveva compromesso l'estensione Chrome di Cyberhaven, un'azienda di cybersecurity specializzata in *data loss prevention*. Un attacco di phishing aveva indotto uno sviluppatore a concedere l'accesso a un'applicazione OAuth malevola denominata "Privacy Policy Extension" – senza che le credenziali Google dello sviluppatore fossero effettivamente compromesse -, consentendo agli attaccanti di pubblicare una versione malevola dell'estensione che esfiltrò cookie e sessioni autenticate per circa 24 ore. L'incidente faceva parte di una campagna più ampia che aveva compromesso almeno 35 estensioni Chrome, esponendo oltre 2,6 milioni di utenti, come documentato dai ricercatori di Hunters Security e Sekoia.

A febbraio 2026, il ricercatore indipendente Q Continuum ha pubblicato un'analisi sistematica che ha identificato 287 estensioni Chrome coinvolte nell'esfiltrazione della cronologia di navigazione verso *data broker*, per un totale di 37,4 milioni di installazioni – circa l'1% dell'intera base utenti globale di Chrome. Le entità coinvolte nella raccolta dei dati spaziavano da Similarweb ad Alibaba Group, da ByteDance a numerosi broker di dati minori.

Secondo un'analisi di Barracuda Networks pubblicata il 25

febbraio 2026, le estensioni browser non sono più minacce marginali o fastidi di basso livello: sono ora un vettore di attacco scalabile, furtivo e capace di condurre sorveglianza su milioni di utenti, rubare dati sensibili e compromettere silenziosamente la sicurezza organizzativa. Uno studio condotto dalla Stanford University e dal CISPA Helmholtz Center for Information Security aveva già identificato migliaia di estensioni classificabili come *security-noteworthy* – contenenti malware, violazioni delle policy sulla privacy o vulnerabilità note – che rimanevano disponibili per anni, accumulando milioni di installazioni.

Estensioni Chrome AI malevole: perché il brand “intelligenza artificiale” è il cavallo di Troia perfetto

C’è un motivo specifico per cui la campagna AiFrame ha scelto di mascherarsi da assistente AI, e non è casuale. L’adozione massiva di strumenti come ChatGPT, Claude, Gemini e Grok ha creato un fenomeno comportamentale senza precedenti: gli utenti sono disposti a installare qualsiasi cosa prometta funzionalità AI, con una soglia di verifica significativamente più bassa rispetto ad altri tipi di software.

L’analisi di Incogni del gennaio 2026 su 442 estensioni AI nel Chrome Web Store ha documentato che il 42% utilizza il permesso di *scripting* – potenzialmente in grado di influenzare 92 milioni di utenti – e il 31,4% raccoglie contenuti dei siti web visitati. Tra le estensioni con oltre 2 milioni di download, anche strumenti legittimi e noti come Grammarly e QuillBot sono stati classificati come potenzialmente ad alto impatto sulla privacy, per la combinazione di dati raccolti e permessi richiesti – pur presentando, come nota Incogni, una bassa probabilità di utilizzo malevolo.

Il brand AI funziona come leva di fiducia perché opera su tre livelli psicologici simultanei. Il primo è l'urgenza dell'adozione: in un contesto lavorativo dove l'AI è percepita come vantaggio competitivo, il ritardo nell'adozione viene vissuto come rischio professionale. Il secondo è la normalizzazione della condivisione: le interfacce conversazionali addestrano gli utenti a condividere informazioni dettagliate – codice proprietario, documenti riservati, credenziali – come parte naturale del flusso di lavoro.

Il terzo è la fiducia nel marketplace: la presenza sul Chrome Web Store, con badge "Featured" e migliaia di recensioni, crea un'apparenza di legittimità che pochi utenti contestano. Alcune delle estensioni AiFrame erano addirittura contrassegnate come "Featured" dallo store, come evidenziato sia da LayerX che da Infosecurity Magazine, aumentando ulteriormente la fiducia degli utenti e accelerandone l'adozione.

Il modello di sicurezza rotto: "approva una volta, fidati per sempre"

Il filo rosso che collega AiFrame, AgreeToSteal e VK Styles non è il tipo di dati rubati o il vettore di distribuzione specifico. È un difetto architetturale comune a tutti i marketplace di estensioni e add-in: il modello "approva una volta, fidati per sempre".

Google verifica il codice di un'estensione al momento della pubblicazione. Microsoft verifica il manifest XML di un add-in al momento della sottomissione. Ma nessuno dei due verifica sistematicamente che cosa viene effettivamente eseguito in seguito. Nel caso di AiFrame, il codice approvato era tecnicamente benigno: caricava un iframe. Il contenuto

dell’iframe, controllato dall’attaccante, poteva cambiare in qualsiasi momento. Nel caso di AgreeToSteal, il manifest dell’add-in non era mai cambiato: era l’URL di destinazione a essere stato dirottato. Nel caso di VK Styles, i *payload* malevoli erano ospitati su un profilo VKontakte e un repository GitHub, completamente al di fuori del perimetro di monitoraggio del Chrome Web Store.

Come ha dichiarato Dardikman di Koi Security a The Hacker News, il problema strutturale è identico in tutti i marketplace che ospitano dipendenze remote dinamiche: approvazione una tantum e fiducia perenne. I dettagli specifici variano per piattaforma, ma il *gap* fondamentale che ha reso possibile AgreeToSteal esiste ovunque un marketplace verifichi un manifest al momento della sottomissione senza monitorare ciò che gli URL referenziati servono effettivamente in seguito.

Vale la pena osservare che Google non è rimasta inerte. La transizione da Manifest V2 a Manifest V3, avviata nel 2023 e progressivamente imposta nel Chrome Web Store, ha introdotto restrizioni significative: i *background script* persistenti sono stati sostituiti da *service worker* con ciclo di vita limitato, i permessi devono essere dichiarati esplicitamente e le capacità di intercettazione delle richieste di rete sono state ridotte.

In teoria, MV3 avrebbe dovuto ridurre drasticamente la superficie d’attacco delle estensioni. In pratica, la campagna AiFrame dimostra i limiti di questo approccio: spostando l’intera logica malevola in un iframe remoto caricato dal server dell’attaccante, l’estensione opera in un territorio che MV3 non è progettato per governare. Il codice esaminabile al momento della pubblicazione è minimo e tecnicamente benigno; è il contenuto servito a *runtime* dall’infrastruttura esterna che compie le azioni malevole. MV3 ha alzato l’asticella, ma non ha risolto il problema fondamentale delle dipendenze dinamiche non monitorate.

Questo non è un *bug*. È un difetto di progettazione che trasforma ogni estensione browser e ogni add-in Office in una potenziale *backdoor* dormiente, attivabile dall'attaccante nel momento che ritiene più opportuno.

Implicazioni operative per i professionisti della sicurezza

La domanda che ogni CISO dovrebbe porsi dopo la settimana dell'11-16 febbraio 2026 non è "come impedisco agli utenti di installare estensioni malevole" – una battaglia persa in partenza. La domanda corretta è: "tratto il browser come parte della superficie d'attacco enterprise con la stessa governance che applico agli endpoint e ai servizi cloud?".

Le contromisure efficaci operano su diversi piani complementari.

Sul piano della **governance delle estensioni**, le organizzazioni devono implementare policy di *allowlisting* che consentano l'installazione solo di estensioni specificamente approvate. Chrome Enterprise offre controlli gestiti che permettono agli amministratori IT di curare liste di estensioni sicure, bloccare minacce note e rimuovere add-on compromessi. La revisione deve essere un processo continuo, non un'approvazione una tantum: ogni aggiornamento di un'estensione autorizzata dovrebbe innescare una nuova valutazione.

Sul piano del **monitoraggio comportamentale**, è necessario implementare soluzioni che osservino il comportamento delle estensioni in tempo reale – trasferimenti di dati anomali, comunicazioni frequenti con server esterni, alterazione delle impostazioni del browser – piuttosto che affidarsi esclusivamente alla reputazione al momento dell'installazione. Le estensioni vanno trattate come componenti software privilegiati che richiedono sorveglianza continua.

Sul piano della **detection operativa**, i SOC analyst dovrebbero implementare regole specifiche per identificare i *pattern* documentati in queste campagne. Per la campagna AiFrame, gli indicatori critici includono: connessioni in uscita verso il dominio tapnetic[.]pro e relativi sottodomini, la presenza di iframe *full-screen* iniettati da estensioni che sovrappongono contenuti remoti alle pagine web attive, e l'attivazione non autorizzata dell'API Web Speech da processi collegati a estensioni.

Per AgreeToSteal, l'indicatore principale è l'add-in con ID WA200004949 e connessioni verso outlook-one.vercel[.]app. Le regole Sigma per la *detection* di esfiltrazione via estensioni browser dovrebbero monitorare volumi anomali di traffico HTTPS in uscita correlati ai processi del browser, in particolare verso domini registrati di recente o con bassa reputazione, e l'accesso programmatico ai contenuti di Gmail (letture DOM ripetute su mail.google.com con *pattern* temporali regolari). La lista completa degli indicatori di compromissione per la campagna AiFrame è disponibile nel report tecnico di LayerX.

Sul piano della **riduzione della superficie d'attacco**, occorre valutare criticamente i permessi richiesti da ogni estensione. Un'estensione di presa appunti che richiede accesso a tutti i dati su tutti i siti web è un segnale d'allarme. Le *wildcard* nei permessi host dovrebbero essere bloccate salvo giustificazione documentata. L'accesso alle API sensibili come Web Speech, *clipboard* e *storage* dovrebbe essere limitato al minimo indispensabile.

Sul piano della **protezione dell'identità**, il caso AiFrame dimostra che i cookie di sessione rubati tramite estensioni malevole alimentano direttamente la catena *infostealer – credential marketplace –* attacco ransomware. L'adozione di autenticazione FIDO2/WebAuthn, la revoca automatica delle sessioni e il monitoraggio continuo delle sessioni attive diventano essenziali quando il browser è un vettore di compromissione primario.

Sul piano della **gestione degli add-in Office**, il caso AgreeToSteal impone un audit sistematico di tutti gli add-in installati in ambiente Microsoft 365, con attenzione particolare a quelli non più mantenuti dallo sviluppatore originale. Gli add-in abbandonati con URL potenzialmente rivendicabili rappresentano un rischio specifico che richiede inventariazione e bonifica proattiva.

La dimensione normativa: NIS2, DORA e la responsabilità dell'organizzazione

Le implicazioni di quanto documentato non sono esclusivamente tecniche. La direttiva NIS2, in vigore nell'Unione Europea, impone alle entità essenziali e importanti l'adozione di misure di gestione del rischio cybersecurity che comprendano la sicurezza della *supply chain*, inclusa la gestione delle vulnerabilità nei componenti software forniti da terze parti. Le estensioni browser installate sui dispositivi aziendali rientrano pienamente in questa definizione.

Il Regolamento DORA (*Digital Operational Resilience Act*), applicabile al settore finanziario europeo, richiede esplicitamente la gestione del rischio ICT legato a fornitori terzi e la verifica continua della resilienza operativa digitale. Un'estensione Chrome che esfiltra il contenuto delle email aziendali e le credenziali di accesso ai servizi cloud rappresenta un incidente che rientra negli obblighi di segnalazione previsti dal regolamento.

Per le organizzazioni soggette al GDPR, la raccolta non autorizzata di email, credenziali e cronologia di navigazione attraverso estensioni malevole costituisce una violazione dei dati personali che richiede notifica all'autorità di controllo entro 72 ore dalla scoperta. Il fatto che la compromissione sia avvenuta attraverso un componente software installato

dall’utente non esime l’organizzazione dalla responsabilità: la mancata governance delle estensioni browser sui dispositivi aziendali può essere contestata come inadeguatezza delle misure tecniche e organizzative previste dall’articolo 32.

Prospettive e scenari evolutivi

La traiettoria delle estensioni Chrome AI malevole nel 2026 suggerisce tre sviluppi che i professionisti della sicurezza dovrebbero anticipare.

Il primo è la **convergenza tra estensioni malevole e agenti AI**. Con l’adozione crescente di agenti AI che operano attraverso il browser — navigando siti, compilando moduli, interagendo con servizi web — le estensioni malevole possono intercettare, manipolare o reindirizzare le azioni degli agenti. Un’estensione che modifica silenziosamente il contenuto di una pagina prima che un agente AI lo processi può avvelenare le decisioni a valle senza lasciare tracce visibili.

Il secondo è la ***weaponization* dei marketplace come canale di distribuzione**. Il modello AiFrame dimostra che i marketplace ufficiali possono essere utilizzati come infrastruttura di distribuzione affidabile per campagne malevole su larga scala. La combinazione di *extension spraying*, iframe remoti e aggiornamenti *server-side* crea un modello di attacco altamente resiliente che le attuali policy di revisione degli store non sono in grado di contrastare efficacemente.

Il terzo è l’**estensione del *pattern* ad altri ecosistemi**. AgreeToSteal ha dimostrato che il medesimo modello di attacco — dipendenze remote dinamiche il cui contenuto può cambiare dopo l’approvazione — si applica agli add-in di Microsoft Office, ai plugin degli IDE come Visual Studio Code e potenzialmente a qualsiasi piattaforma che distribuisca componenti con dipendenze esterne non monitorate.

Conclusione: il browser non è più un’applicazione – è un perimetro

La settimana dell’11-16 febbraio 2026 ha reso evidente ciò che molti professionisti della sicurezza sospettavano da tempo: il browser è diventato un ambiente di esecuzione ad alto privilegio che opera al di fuori della governance tradizionale di endpoint e rete. Le estensioni Chrome AI malevole della campagna AiFrame, il dirottamento dell’add-in Outlook AgreeToSteal e la compromissione di massa di VK Styles non sono incidenti isolati. Sono manifestazioni di un problema architetturale che riguarda l’intero ecosistema dei marketplace software: il modello “approva una volta, fidati per sempre” è strutturalmente incompatibile con un panorama di minacce in cui gli attaccanti possono modificare il comportamento di un componente approvato in qualsiasi momento successivo alla revisione.

Per i CISO e i responsabili della sicurezza, la lezione operativa è chiara: il browser va trattato come parte integrante della superficie d’attacco enterprise, con governance, visibilità e capacità di risposta equivalenti a quelle applicate agli endpoint e ai servizi cloud. Senza questo cambio di paradigma, strumenti apparentemente innocui di produttività e personalizzazione continueranno a trasformarsi in canali di compromissione persistente che operano in piena vista.

Le estensioni Chrome AI malevole non sono una minaccia emergente. Sono una minaccia strutturale che richiede una risposta strutturale.

Fonti principali

LayerX Security – AiFrame: Fake AI Assistant Extensions Targeting 260,000 Chrome Users (febbraio 2026)

Koi Security – AgreeToSteal: The First Malicious Outlook Add-

In (febbraio 2026)

Koi Security – VK Styles: 500K Users Infected (febbraio 2026)

BleepingComputer – Fake AI Chrome Extensions with 300K Users (febbraio 2026)

The Hacker News – Malicious Chrome Extensions Caught Stealing Business Data (febbraio 2026)

The Hacker News – First Malicious Outlook Add-In Found (febbraio 2026)

eSecurity Planet – 260K Users Exposed in AI Extension Scam (febbraio 2026)

The Record – Over 500,000 VKontakte Accounts Hijacked (febbraio 2026)

Cyberhaven – Chrome Extension Security Incident (dicembre 2024)

Hunters Security – Chrome Extension Threat Campaign (gennaio 2025)

Sekoia – Targeted Supply Chain Attack Against Chrome Browser Extensions (marzo 2025)

Q Continuum – Spying Chrome Extensions: 287 Extensions (febbraio 2026)

Barracuda Networks – The Hidden Cybersecurity Risk in Browser Extensions (25 febbraio 2026)

Incogni – Ranking AI-Powered Chrome Extensions by Privacy Risk 2026 (gennaio 2026)

Cybernews – Chrome Extensions: Too Many Dangerous Permissions (2025)

Infosecurity Magazine – Fake AI Assistants in Google Chrome

Web Store (febbraio 2026)

LayerX Security – Enterprise Browser Extension Security Report 2025 (aprile 2025)

Stanford University e CISPA – What is in the Chrome Web Store? Investigating Security-Noteworthy Browser Extensions (giugno 2024)

MDSec – Abusing Office Web Add-ins (gennaio 2019)

MITRE ATT&CK – T1176 Browser Extensions

MITRE ATT&CK – T1539 Steal Web Session Cookie

MITRE ATT&CK – T1185 Browser Session Hijacking

MITRE ATT&CK – T1557 Adversary-in-the-Middle

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/estensioni-chrome-ai-malevole/

AI e immagini generate senza consenso, il documento di 61 autorità mondiali della privacy a difesa di minori e fragili

Sessantuno autorità di protezione dei dati di tutto il mondo, tra cui il **Garante privacy italiano** e l'**European Data Protection Board** (EDPB), hanno firmato una **dichiarazione congiunta** per affrontare uno dei rischi più delicati legati allo sviluppo dell'intelligenza artificiale (AI): la generazione di immagini e video realistici di persone reali senza il loro consenso.

Il documento, coordinato dal **Gruppo di lavoro sulla cooperazione internazionale per l'applicazione delle norme** (*International Enforcement Cooperation Working Group* – **IEWG**) della *Global Privacy Assembly* (**GPA**), rappresenta un segnale forte della crescente attenzione globale verso le conseguenze sociali e giuridiche delle nuove tecnologie di generazione di contenuti basate sull'AI.

A firmare la dichiarazione per il Comitato europeo per la protezione dei dati è stata la presidente dell'EDPB **Anu Talus**, a testimonianza dell'impegno dell'Europa nel promuovere un dialogo internazionale sulla protezione dei dati e dei diritti fondamentali nell'era dell'intelligenza artificiale.

Un problema globale che cresce con l'AI generativa. A rischio minori e soggetti fragili

Negli ultimi anni, i progressi dell'intelligenza artificiale generativa hanno reso possibile creare immagini e video estremamente realistici partendo da semplici istruzioni testuali. Strumenti sempre più accessibili, spesso integrati direttamente nei social network o in piattaforme online, consentono oggi di produrre contenuti che riproducono fedelmente il volto o il corpo di persone reali.

Il problema nasce quando queste tecnologie vengono utilizzate **a insaputa** e **senza il consenso delle persone ritratte**.

Secondo le autorità firmatarie, la diffusione di immagini intime false, video manipolati o contenuti diffamatori che raffigurano individui reali, rappresenta una **minaccia concreta per la privacy, la reputazione e la dignità delle persone**.
Un rischio che diventa ancora più grave quando riguarda **minori o soggetti particolarmente vulnerabili**, esposti a fenomeni come cyberbullismo, molestie digitali o sfruttamento.

L'allarme riguarda soprattutto la rapidità con cui questi contenuti possono essere prodotti e diffusi online, spesso prima che le vittime riescano a intervenire per rimuoverli.

Il nostro **Garante per la protezione dei dati personali** aveva già adottato a gennaio un provvedimento di avvertimento nei confronti degli utilizzatori di servizi basati sull'**intelligenza artificiale**, come **Grok**, **ChatGPT** e **Clothoff** (quest'ultima piattaforma già destinataria di un provvedimento di blocco nell'ottobre scorso) e altri servizi analoghi disponibili online, proprio perché consentivano di generare e condividere contenuti a partire da immagini o voci reali, arrivando anche a **"spogliare" persone senza il loro consenso**.

I quattro principi per uno sviluppo responsabile dell'AI

Pur riconoscendo il grande potenziale dell'intelligenza artificiale per l'innovazione e lo sviluppo economico, le autorità mondiali della privacy ricordano che la tecnologia deve essere progettata e utilizzata nel rispetto delle normative sulla protezione dei dati e dei diritti fondamentali.

Nel documento vengono indicati **quattro principi fondamentali** che dovrebbero guidare lo sviluppo e l'uso dei sistemi di AI generativa:

introdurre **misure efficaci di prevenzione degli abusi**, in particolare per impedire l'uso improprio di dati personali e la creazione non consensuale di immagini intime o contenuti lesivi;

garantire massima **trasparenza**, perché le aziende che sviluppano o utilizzano sistemi di AI devono spiegare chiaramente come funzionano queste tecnologie, quali sono gli utilizzi consentiti e quali possono essere le conseguenze di un uso improprio;

la necessità di offrire **strumenti semplici ed efficaci per chiedere la rimozione dei contenuti dannosi**, soprattutto quando coinvolgono dati personali o rappresentazioni non autorizzate;

l'importanza di **gestire in modo specifico i rischi per i minori**, che rappresentano una delle categorie più esposte agli effetti negativi delle tecnologie digitali.

Pensare l'AI a partire dalla *privacy by design*

La dichiarazione è rivolta principalmente alle **aziende che sviluppano o utilizzano sistemi di intelligenza artificiale per la generazione di contenuti**, dalle grandi piattaforme digitali alle start-up tecnologiche.

Il messaggio delle autorità è chiaro: la tutela della privacy e della dignità delle persone deve essere integrata fin dalla progettazione delle tecnologie.

Per questo motivo i garanti della privacy invitano le imprese a **collaborare in modo proattivo con le autorità di regolamentazione**, adottando fin da subito sistemi di sicurezza e meccanismi di protezione efficaci.

L'obiettivo è evitare che l'innovazione tecnologica si

trasformi in uno strumento di abuso o di violazione dei diritti fondamentali.

Cooperazione internazionale contro i rischi digitali

La dichiarazione rappresenta anche un esempio concreto di **cooperazione globale nella regolazione delle tecnologie emergenti**. Il fatto che oltre sessanta autorità di diversi continenti abbiano deciso di prendere una posizione comune dimostra quanto il problema sia percepito come urgente.

Le autorità firmatarie si sono impegnate a **condividere informazioni, strategie di intervento e buone pratiche**, con l'obiettivo di contrastare in modo più efficace i rischi legati alla diffusione di contenuti generati dall'intelligenza artificiale.

In un ecosistema digitale globale, infatti, i problemi non si fermano ai confini nazionali. Per questo la cooperazione tra autorità di regolazione diventa uno strumento essenziale per garantire una tutela effettiva dei diritti delle persone.

Innovazione sì, ma senza sacrificare privacy e diritti fondamentali

Il messaggio che emerge è uno solo: l'intelligenza artificiale può portare grandi benefici alla società, ma il suo sviluppo non può avvenire a discapito dei diritti fondamentali. Privacy, dignità, sicurezza e tutela dei minori devono restare **principi non negoziabili** anche nell'era delle tecnologie più avanzate.

Per questo le autorità mondiali della privacy chiedono che la progettazione dell'AI segua un principio semplice ma

essenziale: **il progresso tecnologico deve sempre rimanere al servizio delle persone, e non il contrario**.

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/ai-e-immagini-generate-senza-consenso-il-documento-di-61-autorita-mondiali-della-privacy-a-difesa-di-minori-e-fragili/567718/