Anthropic Claude gratuito e open source per gli avvocati italiani

20 agenti AI specializzati per il diritto italiano, gratuiti e open-source su Anthropic Claude Cowork

Nel giorno dell'inaugurazione dei **primi uffici italiani di Anthropic a Milano**, un team di sviluppatori di Zurigo lancia **BetterCallClaude**, la prima **piattaforma di intelligenza artificiale (AI) legale** gratuita e *open-source* dedicata al mercato italiano.

La piattaforma dispone di **20 agenti AI specializzati**, 19 comandi ottimizzati, 14 skill integrate e 7 server MCP. BetterCallClaude non è un chatbot generico ma un **sistema di agenti intelligenti** progettato per chi lavora quotidianamente con Cassazione, Corte Costituzionale e normativa italiana. La soluzione copre tutte le **20 regioni italiane**.

Sette aree di applicazione dell'AI legale

BetterCallClaude, si legge sul sito stesso del servizio, copre sette aree specializzate che includono la ricerca sui precedenti della Cassazione, la strategia processuale, l'analisi avversariale (l'analisi strategica delle mosse, delle argomentazioni e delle prove della parte avversa), la redazione legale, la verifica delle citazioni, l'intelligenza documentale e l'arbitrato sportivo CAS/TAS. Queste funzionalità sono state sviluppate per rispondere alle

esigenze concrete degli avvocati italiani nella gestione quotidiana dei casi.

La piattaforma è distribuita con licenza **Apache 2.0**, che consente utilizzo gratuito senza costi di licenza, modifica del codice sorgente, redistribuzione delle versioni personalizzate, utilizzo commerciale da parte di studi legali e integrazione con software gestionali esistenti. Questa trasparenza è cruciale per il settore legale, dove la **privacy dei dati sensibili** dei clienti è prioritaria e gli avvocati possono verificare direttamente come vengono trattate le informazioni.

Le barriere all'AI legale in Italia

L'arrivo di BetterCallClaude in Italia coincide, come anticipato, con l'annuncio odierno di **Anthropic che apre il suo primo ufficio a Milano**, la prima grande azienda di AI a stabilire una presenza fisica nel paese. Il mercato AI italiano, che vale un terzo di quello tedesco, registra però un utilizzo di Claude **il doppio del peso demografico nazionale**, segnalando forte interesse tra i professionisti per soluzioni tecnologiche avanzate.

L'iniziativa potrebbe certamente ridurre le barriere all'adozione dell'AI legale, rappresentate soprattutto dal costo e dalla mancanza di specializzazione. Rimangono però dei nodi da sciogliere e anche rilevanti.

Open-source e gratuito cosa? E i dati dove vanno?

Ciò che è open-source sono i 20 agenti, le 14 skill, i 19 comandi e i 7 server MCP. Il "cervello" che esegue tutto è Claude di Anthropic: un modello proprietario, closed-source, che richiede un abbonamento Cowork a pagamento. Senza Claude, il repository non funziona, come ha spiegato su LinkedIn Marco

Graziano commentando la notizia: “*è gratuita la “colla”, non lo stack completo*”.

Sul fronte della sovranità dei dati, per uno strumento che processa query legali italiane e che pubblicizza la protezione del segreto professionale, si legge sempre nel commento, “*vale la pena segnalare che le query passano attraverso infrastruttura USA, prima ancora di arrivare a Claude (anch’esso servito da Anthropic negli Stati Uniti)*”.

Nulla toglie al valore tecnico del progetto, che rimane un ottimo esempio di plugin open-source costruito attorno a un modello proprietario. Tuttavia, c’è chi ancora nutre qualche dubio sulla compliance al Regolamento europeo sulla protezione dei dati (GDPR).

Novità su Google, per aggiungere Key4Biz tra le tue fonti preferite, clicca qui



Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/anthropic-claude-gratuito-e-open-source-per-gli-avvocati-italiani/573754/

Bernini annuncia “Lisa”, il primo sistema Ue per

applicazioni AI che potenzia il supercomputer Leonardo. L’11 giugno l’inaugurazione

L’Italia candida Bologna a nodo di punta della rete “Frontier AI” e a giugno arriva Lisa a potenziare il supercomputer Leonardo

L’Italia accelera sulla frontiera europea dell’**intelligenza artificiale** (AI) e sceglie Bologna come epicentro della propria strategia tecnologica. Il Tecnopolo del capoluogo emiliano ospiterà infatti **LISA**, acronimo di “*Leonardo Improved Supercomputing Architecture*”, la nuova infrastruttura progettata per potenziare il **supercomputer Leonardo** nelle applicazioni di AI generativa e nei **modelli linguistici di grandi dimensioni**.

Secondo un’agenzia *Radiocor* del Sole 24 Ore, l’annuncio è arrivato dalla ministra dell’Università e della Ricerca **Anna Maria Bernini** e da **Antonio Zoccoli**, presidente della Fondazione Icsc – Centro Nazionale di Ricerca in High-Performance Computing, Big Data e Quantum Computing, durante il convegno “*L’Italia del Pnrr: creare il modello, fare sistema, orientare il futuro*”, in corso a Milano. L’inaugurazione ufficiale è prevista l’**11 giugno** al Tecnopolo di Bologna.

Contestualmente, **il Governo italiano ha candidato Bologna a diventare uno dei nodi principali di “*Frontier AI*”**, la futura infrastruttura europea dedicata alla ricerca avanzata sull’intelligenza artificiale. Una scelta che rafforza il

posizionamento internazionale del polo emiliano come uno dei più importanti ecosistemi europei nel supercalcolo, nei big data e nell'AI.

Che cos'è Lisa e perché è importante

La nuova architettura LISA rappresenta un passaggio strategico nell'evoluzione di Leonardo, oggi già considerato tra i supercomputer più potenti al mondo e stabilmente inserito nella top ten della classifica internazionale TOP500. La macchina, installata al Tecnopolo DAMA di Bologna e gestita dal Cineca nell'ambito dell'iniziativa europea EuroHPC, è in grado di eseguire 240 milioni di miliardi di operazioni al secondo ed è utilizzata per attività scientifiche di altissima complessità: dalla modellazione climatica alla ricerca farmaceutica, dalla fisica delle particelle ai materiali avanzati, fino alle applicazioni industriali e aerospaziali.

Con LISA, però, il paradigma cambia. Leonardo nasce come infrastruttura general purpose destinata al calcolo scientifico avanzato; **il nuovo modulo è invece concepito specificamente per l'intelligenza artificiale**. Si tratta del primo sistema europeo di questo tipo realizzato nell'ambito dell'ecosistema EuroHPC e rappresenta un salto tecnologico cruciale per l'Europa nella competizione globale sull'AI.

Il cuore della nuova infrastruttura sarà costituito da 166 server GPU ad altissime prestazioni, interconnessi attraverso una rete a bassissima latenza e progettati per sostenere l'addestramento di modelli linguistici di grandi dimensioni e applicazioni multimodali capaci di elaborare simultaneamente testo, immagini, video e dati complessi. In altre parole, **LISA consentirà di sviluppare in Europa tecnologie comparabili ai sistemi di AI generativa oggi dominati** dai grandi operatori statunitensi e cinesi.

L’investimento complessivo per LISA ammonta a 28,2 milioni di euro. Il 35% sarà finanziato da EuroHPC JU, il partenariato europeo dedicato ai supercomputer strategici dell’Unione, mentre il restante 65% arriverà dal Ministero dell’Università e della Ricerca attraverso il Centro Nazionale HPC, Big Data e Quantum Computing nato con il Pnrr.

Il valore economico e industriale di questa operazione è potenzialmente enorme. **L’accesso a capacità di calcolo avanzate rappresenta infatti uno dei principali fattori abilitanti della nuova economia dell’intelligenza artificiale**: permette di accelerare la ricerca scientifica, sviluppare farmaci, ottimizzare reti energetiche, simulare materiali innovativi, migliorare i sistemi manifatturieri e creare nuovi servizi digitali ad alto valore aggiunto.

Un’AI più europea per rafforzare l’autonomia tecnologica

La posta in gioco va ben oltre il semplice incremento di potenza di calcolo. LISA rafforza infatti il tema dell’**autonomia tecnologica europea**, diventato centrale dopo la corsa globale all’intelligenza artificiale generativa. Disporre di **infrastrutture proprietarie per addestrare modelli avanzati** significa poter sviluppare capacità strategiche senza dipendere integralmente dalle piattaforme extraeuropee, preservando sovranità tecnologica, sicurezza dei dati e competitività industriale.

In questo scenario l’Italia parte da una posizione particolarmente favorevole. Il Paese dispone già di uno dei sistemi HPC più articolati d’Europa e Bologna si sta progressivamente consolidando come capitale continentale del supercalcolo. Attorno al Tecnopolo convivono infatti il supercomputer Leonardo, il Centro europeo per le previsioni meteorologiche a medio termine (ECMWF), infrastrutture scientifiche internazionali, centri di ricerca e la **AI Factory**

italiana IT4LIA, selezionata dalla Commissione europea tra le prime sette del continente.

Bologna nodo strategico per il supercalcolo europeo

Secondo i dati illustrati dalla ministra Bernini durante l'incontro tenuto qualche giorno fa a Bologna con la commissaria europea per le Start-up, la Ricerca e l'Innovazione, **Ekaterina Zaharieva**, Cineca è oggi il secondo centro HPC europeo per volume di produzione scientifica. Nel 2024 il 15% delle pubblicazioni realizzate attraverso le sue infrastrutture è già rientrato nel top 10% mondiale per citazioni scientifiche. Solo nel 2025 sono state messe gratuitamente a disposizione di università ed enti di ricerca oltre 550 milioni di ore di calcolo, per un valore stimato superiore ai 130 milioni di euro.

Anche IT4LIA mostra già numeri rilevanti: quasi 500 progetti avviati in appena un anno di attività operativa. Un dato che evidenzia come l'ecosistema bolognese stia rapidamente trasformando la potenza computazionale in innovazione concreta per imprese, ricerca e pubblica amministrazione.

Per questo **Bologna non viene più considerata soltanto un polo scientifico nazionale, ma un'infrastruttura strategica europea**. La candidatura italiana a "*Frontier AI*" punta proprio a consolidare questo ruolo: fare del Tecnopolo il luogo in cui ricerca, supercalcolo e intelligenza artificiale convergono per costruire la prossima generazione di tecnologie europee.

Con LISA, l'Italia prova dunque a entrare stabilmente nel gruppo ristretto dei Paesi capaci non solo di utilizzare l'intelligenza artificiale, ma anche di costruirne l'infrastruttura industriale e scientifica di base. Un passaggio decisivo in una competizione globale in cui la disponibilità di potenza computazionale sta diventando un

fattore geopolitico oltre che economico.

Novità su Google, per aggiungere Key4Biz tra le tue fonti preferite, clicca qui



Leggi le altre notizie sull'home page di Key4biz

https://www.key4biz.it/bernini-annuncia-lisa-il-primo-sistema-ue-per-applicazioni-ai-che-sara-inaugurato-a-bologna-l11-giugno/573740/

L'AI al centro della prima enciclica di Papa Leone per fine maggio

Entro fine maggio la prima enciclica firmata da Papa Leone XIV, l'annuncio il 22. Al centro ci sarà il ruolo dell'AI nel nostro mondo

C'è grande attesa in Vaticano per quella che potrebbe diventare la **prima enciclica di Papa Leone XIV**, un testo che secondo indiscrezioni e anticipazioni della stampa internazionale dovrebbe affrontare il tema dell'**intelligenza**

artificiale (AI) inserendolo dentro una riflessione più ampia sulla crisi dell'ordine globale, sul lavoro, sulla pace e sul futuro della persona umana nell'era digitale.

Diverse fonti avevano indicato che il documento sarebbe stato firmato questo 15 maggio, coincidendo con l'anniversario della pubblicazione di *Rerum novarum*, la grande enciclica sociale di Leone XIII. Tuttavia, il direttore dell'Ufficio Stampa della Santa Sede, **Matteo Bruni**, ha informato i giornalisti che l**'annuncio ufficiale del documento si terrà il prossimo 22 maggio**.

Il titolo provvisorio dovrebbe essere "*Magnifica Humanitas*" e la scelta simbolica di uscire a maggio riporta all'anniversario della storica *Rerum Novarum* di Leone XIII (15 maggio 1891). Una scelta che suggerisce già la direzione culturale e politica del documento: **proporre una nuova dottrina sociale per il tempo dell'intelligenza artificiale,** così come alla fine dell'Ottocento la Chiesa intervenne davanti agli effetti della rivoluzione industriale.

Il parallelismo non è casuale. Allora il problema era la macchina industriale che trasformava il lavoro e ridefiniva i rapporti sociali, **oggi il nodo è l'algoritmo** che entra nei processi decisionali, nell'economia, nella comunicazione, nella sicurezza e perfino nella produzione culturale.

Secondo quanto riportato da *Axios*, *Le Monde* e da diverse testate vicine al Vaticano, in particolare *Infovaticana*, Leone XIV considera l'AI non semplicemente come una nuova tecnologia, ma come "*una forza storica destinata a incidere profondamente sugli equilibri politici, economici e antropologici del XXI secolo*".

Un'etica per l'AI e il digitale,

con l’uomo sempre al centro

La posizione della Santa Sede, almeno stando alle anticipazioni, appare lontana sia dagli entusiasmi tecnocratici sia dalle visioni apocalittiche. Il Vaticano non demonizza l’intelligenza artificiale e non propone una lettura anti-scientifica dell’innovazione.

Negli ultimi anni, grazie a **Papa Francesco**, la Chiesa ha cercato di costruire un rapporto sempre più strutturato con il mondo tecnologico, sostenendo iniziative come il “*Rome Call for AI Ethics*”, aprendo tavoli di confronto con aziende e centri di ricerca e sviluppando linee guida interne sui temi dell’etica digitale e della cybersicurezza.

L’idea di fondo è che l’innovazione rappresenti una straordinaria opportunità per la medicina, l’educazione, l’organizzazione sociale e la diffusione della conoscenza, ma che debba restare governata da criteri umani, politici ed etici.

È qui che emerge il cuore della riflessione cattolica sull’AI. Il timore del Vaticano non riguarda la tecnologia in sé, bensì il rischio che l’uomo venga progressivamente subordinato ai sistemi tecnologici, trasformato in dato, funzione produttiva o profilo algoritmico.

Papa Francesco aveva già denunciato il pericolo di una società dominata dalla sorveglianza digitale, dall’automazione della guerra e da modelli economici capaci di aumentare disuguaglianze e marginalizzazione. Leone XIV sembra intenzionato a sistematizzare ulteriormente questo approccio, portandolo dentro una vera enciclica sociale.

Difendere il lavoro umano

Particolare attenzione sarebbe riservata al tema del lavoro. Come la *Rerum Novarum* affrontò gli effetti sociali del

capitalismo industriale, così *Magnifica Humanitas* potrebbe interrogarsi sull'impatto dell'automazione intelligente sulle professioni, sulla redistribuzione della ricchezza e sulla dignità del lavoro umano.

Non è un caso che molti osservatori leggano nella scelta del nome Leone XIV un richiamo esplicito a Leone XIII e alla stagione storica in cui la Chiesa decise di intervenire direttamente nella questione sociale. Secondo diversi studiosi cattolici citati dalla stampa americana, **il nuovo Papa vede nell'intelligenza artificiale una trasformazione comparabile a quella della rivoluzione industriale**, con il rischio concreto di una **sostituzione accelerata del lavoro umano** e di una **concentrazione senza precedenti del potere economico e informativo nelle mani di pochi soggetti globali**.

La Chiesa, naturalmente, non pretende di sostituirsi alle istituzioni democratiche nella regolazione dell'intelligenza artificiale. In uno Stato laico spetta ai governi, ai parlamenti e agli organismi internazionali definire norme, limiti e sistemi di controllo per tecnologie che avranno un impatto enorme sull'economia, sulla sicurezza e sui diritti individuali.
Tuttavia, sarebbe ingenuo sottovalutare il peso culturale e politico della voce del Vaticano su temi di questa portata.

La Santa Sede continua a rappresentare uno dei principali attori morali globali e mantiene una forte capacità di influenza nel dibattito pubblico internazionale, soprattutto su questioni che riguardano il rapporto tra sviluppo tecnologico, dignità della persona e giustizia sociale.

L'AI trasformerà il nostro mondo, non lasciamo tutto in mano al

mercato e alle superpotenze

In questo senso l’intervento di Leone XIV arriva in una fase storica particolarmente instabile, segnata da tensioni geopolitiche, crisi della governance internazionale, guerre ibride, trasformazioni del mercato del lavoro e accelerazione tecnologica.

L’intelligenza artificiale viene ormai percepita non soltanto come un fattore economico, ma come un elemento capace di ridefinire gli equilibri di potere globali. Il Vaticano sembra voler affermare che una trasformazione di questa portata non possa essere lasciata esclusivamente alle **logiche del mercato** o alla **competizione strategica tra grandi potenze**.

Il messaggio che emerge dalle anticipazioni è chiaro: la tecnologia deve restare uno strumento al servizio dell’uomo e non diventare il principio che organizza la società. È una posizione che unisce etica, politica e visione antropologica e che punta a riportare al centro del dibattito il tema della **responsabilità umana nell’epoca dell’automazione intelligente.**

Novità su Google, per aggiungere Key4Biz tra le tue fonti preferite, clicca qui



Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/ai-al-centro-della-prima-enciclica-di-papa-leone-per-fine-maggio/572793/

In Cina Trump non riesce a “piazzare” le aziende USA, neanche i chip di Nvidia. Ma gli affari di famiglia sì

Trump lascia Pechino elogiando Xi, ma a mani vuote?

Poche ore fa l’Air Force One è decollato dall’aeroporto di Pechino per riportare a casa il Presidente degli Stati Uniti, **Donald Trump**, e il suo numeroso equipaggio fatto di funzionari statali e alcuni tra gli imprenditori più ricchi e potenti del mondo. La visita di Stato di Trump in Cina si è conclusa, questa l’unica certezza, molto meno però si sa su eventuali accordi commerciali e soprattutto tecnologici tra le due superpotenze in competizione per la leadership globale digitale.

Il Presidente americano ha avuto parole di elogio per il suo omologo cinese, **Xi Jinping**, definendolo “un grande leader”, addirittura “un amico”. Al centro dei tre giorni di incontri e tavole imbandite, certamente ci sono state le questioni politiche più scottanti, Taiwan e Iran in testa, la Russia anche, le tensioni commerciali che interessano i rapporti tra le due grandi economie, la necessità di un migliore coordinamento sui temi internazionali e il rafforzamento della comunicazione tra le due principali sponde del Pacifico.

Mosca, nel frattempo, ha seguito tutto con grande attenzione, come ha riferito il portavoce del Presidente russo. Anche **Vladimir Putin**, infatti, volerà in Cina nei prossimi giorni: “*speriamo di avere informazioni di prima mano su quanto si*

sono detti (Trump e Xi, ndr).*Quando saremo in Cina, ci sarà una buona opportunità per scambiare opinioni sui contatti che i cinesi hanno avuto con gli americani*", ha commentato il portavoce Dmitry Peskov, citato dall'agenzia *Interfax*.

Erano tante le attese, a dire il vero, in particolare quelle relative ad eventuali accordi sui chip AI e gli hardware necessari allo sviluppo delle infrastrutture digitali, ma in base a quanto riportato dalla stampa americana ed internazionale Trump è ripartito a mani vuote.



Perché Trump si è portato un codazzo di super CEO in Cina? Soft power? Marketing di Stato? O puro business?

Pensando al gran numero di super CEO delle più grandi imprese americane, che per capitalizzazione di mercato rappresentavano

tutte assieme decine di trilioni di dollari di valore, ci si aspettava un risultato rilevante in termini di strategie industriali e tecnologiche, in particolare per i chip AI.

Sull'aereo presidenziale sedevano **Jensen Huang** di **Nvidia**, **Elon Musk** di Tesla e SpaceX, **Tim Cook** di Apple, più alti dirigenti di Meta e Qualcomm, solo per citare le aziende pi conosciute al grande pubblico.

Secondo quanto riferito dal rappresentante commerciale degli Stati Uniti, **Jamieson Greer**, le società americane hanno avuto modo di presentare proposte e piani industriali ai corrispettivi cinesi, ricevendo rassicurazioni sulla volontà del gigante asiatico di aprire, ancora di più, il proprio mercato alle imprese americane.

La partita chiave dei chip AI e delle terre rare

Greer ha però anche confermato che non si è parlato di "accordi o controlli" sulle esportazioni di chip durante il bilaterale Trump-Xi.

Al momento, secondo quanto riportato dalla *Reuters*, si sa solo che, già prima del volo verso Pechino di Trump, gli Stati Uniti avevano autorizzato la vendita di **chip H200 per l'intelligenza artificiale** di Nvidia a diverse società tecnologiche cinesi.

In cambio, i cinesi hanno promesso di allentare la stretta sul flusso di **terre rare e minerali critici** verso gli stati Uniti. Questo è un settore che la Cina controlla rigidamente e che però è fondamentale per la transizione digitale ed energetica di tutti i mercati occidentali, compreso quello americano.
Si attendeva qualche indiscrezione sulla proroga dell'accordo in vigore tra USA e Cina e anche qui Greer è stato molto sibillino: "*Ci sono buone probabilità…vedremo, c'è la volontà*

di entrambe le parti di continuare e anzi estendere la capacità di approvvigionamento, ma sono processi lenti”.

Vanno a gonfie vele, invece, gli affari della famiglia Trump sulle criptovalute e l’AI. Accordi con i vertici del Partito comunista cinese?

In compenso, **Eric Trump**, terzogenito del presidente degli Stati Uniti e top manager della ***Trump Organization*** (la grande cassaforte della famiglia Trump), sembrerebbe aver chiuso affari d’oro in Cina. Accompagnando il padre nel viaggio di Stato, Eric avrebbe perfezionato accordi (di cui al momento non si sa molto) con un’azienda cinese attiva nel settore dell’AI, la **Nano Labs**.

Accordi relativi alla costruzione di data center AI negli Stati Uniti e che vedono della partita anche un’azienda americana delle criptovalute, **Alt5Sigma**.



Da destra Donald Trump e i figli Donald Jr., Ivanka e Eric

Nella Alt5Sigma sarebbero stati investiti milioni di dollari direttamente dalla **World Liberty Financial** (piattaforma di **trading in criptovalute** fondata nel 2024 dalla famiglia Trump), racconta Marco Contini su *La Repubblica*, nel cui board siedono **Zach Witkoff** come presidente (fidato mediatore del Presidente Trump nelle principali crisi internazionali), e Eric Trump come osservatore.
Anche i figli di Witkoff sono presenti nella World Liberty Financial.

Un intreccio di affari e famiglie di potere, dunque, che però ha messo in allarme il Congresso degli Stati Uniti perché, secondo quanto riportato dal *Financial Times*, la Nano Labs è una società che vede impegnati i vertici del Partito comunista cinese e probabilmente delle stesse forze armate cinesi.

Le criptovalute della famiglia Trump hanno generato oltre 1 miliardo di dollari di profitti dai progetti crypto, secondo un'analisi *Reuters*, con World Liberty Financial come impresa più redditizia. Il progetto è stato anche al centro di

controversie legali, tra cui una causa per diffamazione contro l'imprenditore crypto Justin Sun, accusato di aver condotto una campagna di diffamazione pubblica e di aver corteggiato il progetto per poi *fare shorting* del token.

La combinazione tra affari privati della famiglia Trump e il progetto crypto World Liberty Financial solleva notevoli questioni di conflitto di interesse, trasparenza e possibile influenza su regolamenti e politiche pubbliche, soprattutto in un contesto in cui il presidente americano controlla direttamente o indirettamente progetti finanziari ad alto rischio e ad alta esposizione mediatica.

Quegli strani investimenti di Trump in Apple, Tesla e Nvidia

Appena conclusa la visita ufficiale di Donald Trump in Cina, sono emersi nuovi dettagli sulle operazioni finanziarie del presidente americano legate ad alcune delle aziende presenti nella delegazione che lo ha accompagnato nel viaggio.

Secondo i dati dell'Ufficio per l'etica governativa degli Stati Uniti, ripresi dalla stampa economica americana e riportati da Sandra Riccio su *La Stampa*, nei primi mesi del 2026 **Trump avrebbe incrementato in modo rilevante i propri investimenti in Apple**, arrivando a destinare fino a 7,2 milioni di dollari al gruppo guidato da Tim Cook.

Al fianco del presidente, durante la missione in Cina, c'erano anche Elon Musk, Jensen Huang di Nvidia e Kelly Ortberg di Boeing. Le analisi finanziarie statunitensi sottolineano inoltre come, nei mesi precedenti alla visita, Trump abbia effettuato diverse operazioni di acquisto e vendita sui titoli proprio di queste aziende. C'è da chiedersi fino a che punto tutto questo sia normale e fino a che punto tutto questo non abbia ricadute serie sullo stato di salute della democrazia americana e non solo.

Novità su Google, per aggiungere Key4Biz tra le tue fonti preferite, clicca qui

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/in-cina-trump-non-riesce-a-piazzare-le-aziende-usa-neanche-i-chip-di-nvidia-ma-gli-affari-di-famiglia-si/572687/

Palantir passa all’ICE una lista di 20 milioni di americani da sorvegliare

Palantir usato per la sorveglianza di massa ‘data driven’ dell’ICE

Negli Stati Uniti l’Immigration and Customs Enforcement (**ICE**), la potente agenzia federale incaricata del controllo dell’immigrazione e delle espulsioni, sta ampliando la propria capacità operativa grazie ai sistemi sviluppati da **Palantir**, la società americana specializzata nell’analisi massiva dei

dati fondata dal controverso imprenditore, ‘oscuro profeta’ del digitale apocalittico, **Peter Thiel**.

Durante il *Border Security Expo* (la fiera delle tecnologie più avanzate per “difendere i confini da ogni minaccia”, in particolare, sembra, quella dei migranti), tenutosi nei giorni scorsi a Phoenix, un alto funzionario dell’ICE ha descritto con sorprendente franchezza la portata di questa trasformazione. Secondo quanto riportato dalla piattaforma media indipendente *404*, proprio grazie a Palantir, gli **agenti ICE** avrebbero oggi accesso direttamente dai loro iPhone a un archivio di circa **20 milioni di persone** potenzialmente **individuabili, localizzabili e tracciabili**.

Questo è un punto cruciale su cui soffermarsi, non solo per la gravità dell’informazione, ma anche perchè, come hanno scritto Betty Gedlu e Cindy Cohn sul sito di Electronic Frontier Foundation, Palantir su questo è ambigua, afferma spesso il contrario, ma sono gli stessi agenti e funzionari ICE che più volte hanno confermato questa collaborazione.

Al di là della retorica securitaria e delle cifre che meritano cautela, il punto centrale è un altro: l’uso delle piattaforme Palantir sta rendendo l’apparato di controllo migratorio statunitense molto più rapido, capillare e invasivo. Non si tratta soltanto di software amministrativi o di strumenti investigativi tradizionali. Siamo di fronte a un modello tecnologico che cambia la natura stessa dell’enforcement migratorio, trasformandolo in **un sistema di sorveglianza data-driven** capace di aggregare, in maniera opaca, enormi quantità di informazioni personali e convertirle in obiettivi operativi.
Attenzione, però, perché tale sistema non riguarda o riguarderà solo una fascia sfortunata di persone, ma tutti i cittadini americani.

Gli algoritmi che aiutano gli agenti ICE a profilare esseri umani, con un tasso di successo dell’80%

Palantir non produce direttamente banche dati. **La sua forza consiste nel mettere in relazione archivi pubblici e privati che normalmente rimarrebbero separati**: dati amministrativi, registri telefonici, informazioni sanitarie, indirizzi, precedenti giudiziari, movimenti finanziari, profili sociali, documenti governativi e database commerciali.

Attraverso **algoritmi di correlazione e sistemi di visualizzazione avanzata**, queste informazioni vengono fuse in un’unica interfaccia interrogabile dagli operatori. In pratica, **la piattaforma costruisce profili dettagliati delle persone**, individua connessioni, suggerisce indirizzi probabili e attribuisce livelli di “affidabilità” o “rischio” alle informazioni raccolte.

Secondo quanto riportato da *404*, l’ICE avrebbe dichiarato che grazie a Palantir **il tasso di successo nell’individuazione delle persone da arrestare sarebbe passato da circa il 27% a quasi l’80%**. Un’indagine che prima richiedeva ore, sostengono i funzionari, oggi può essere completata in pochi minuti.

Questo salto di efficienza è reso possibile dall’**accesso simultaneo a decine di database differenti** e dalla capacità della piattaforma di trasformare dati dispersi in mappe operative immediatamente utilizzabili sul campo.

Con il sistema ELITE gli agenti ICE hanno sempre una mappa aggiornata

delle persone da ‘colpire’ e deportare

Tra gli strumenti sviluppati per l’ICE c’è anche **ELITE**, acronimo di *Enhanced Leads Identification & Targeting for Enforcement*, già rivelato nei mesi scorsi da alcune inchieste giornalistiche americane.

Il sistema consente agli agenti di **visualizzare su una mappa le persone considerate potenziali target** di deportazione, accedere a dossier individuali e ottenere un “*confidence score*”, cioè una valutazione automatica sulla probabilità che una persona si trovi realmente a un determinato indirizzo.

Le informazioni proverrebbero da fonti molto diverse, incluse banche dati sanitarie e prodotti commerciali di data brokerage, come CLEAR di Thomson Reuters.

È qui che il problema smette di essere soltanto tecnologico e diventa profondamente politico e democratico. L’uso di Palantir da parte dell’ICE non rappresenta semplicemente un aumento dell’efficienza amministrativa: segna **un salto di qualità nella capacità dello Stato di vedere, correlare e colpire**. Quando un’agenzia di questo livello dispone di strumenti che aggregano dati eterogenei e trasformano individui in “bersagli operativi” (come accade tragicamente in Ucraina e in Iran, o a Gaza), **il confine tra investigazione e sorveglianza di massa diventa estremamente fragile**.

Privacy vittima del data repurposing, quando i dati raccolti per un motivo vengono poi usati per altri scopi. E tu non lo sai

Il primo rischio riguarda la privacy. In un ecosistema di

questo tipo, informazioni raccolte originariamente per finalità completamente diverse possono essere riutilizzate per operazioni di enforcement. Dati sanitari, amministrativi o commerciali finiscono così dentro un'infrastruttura di controllo senza che le persone coinvolte abbiano reale consapevolezza del processo.

La logica è quella del ***data repurposing***: ciò che era stato fornito per ottenere assistenza medica, registrarsi a un servizio o completare una pratica burocratica viene trasformato in uno strumento di identificazione e localizzazione.
In questo modo sempre l'ICE, grazie ad un accordo di condivisione dei dati tra il Dipartimento della Sicurezza Interna e i Centri per i Servizi Medicare e Medicaid, ha **passato al setaccio i dati personali di quasi 80 milioni di cittadini americani**.

Il secondo nodo riguarda il ***due process*** e le **garanzie democratiche**. Sistemi di questo tipo funzionano attraverso correlazioni probabilistiche e inferenze algoritmiche, non attraverso certezze assolute.

Anche quando vengono presentati come strumenti "oggettivi", **possono produrre errori, falsi positivi e decisioni opache difficili da contestare.** Una persona può essere identificata erroneamente come target sulla base di dati incompleti, obsoleti o associati in modo scorretto.
Eppure, nel momento in cui l'algoritmo accelera **le operazioni sul campo, il tempo per verificare e correggere gli errori si riduce drasticamente**.

Questo problema è aggravato dalla **scarsissima trasparenza che circonda tali sistemi**. Le agenzie federali raramente spiegano nel dettaglio quali dataset vengano utilizzati, come funzionino i modelli di correlazione o quali meccanismi di supervisione indipendente esistano realmente.

Il risultato è uno **spostamento del potere decisionale verso infrastrutture tecnologiche difficili da scrutinare da parte dei giudici, dei parlamenti e dell'opinione pubblica**. La promessa dell'efficienza investigativa rischia così di prevalere sul principio fondamentale della contestabilità delle decisioni pubbliche.

Ambienti sorvegliati che producono paura e insicurezza, come cambiano i nostri comportamenti

Esiste poi un ulteriore effetto, meno visibile ma forse ancora più profondo: il cosiddetto ***chilling effect***. Quando comunità migranti, attivisti o semplici cittadini percepiscono di vivere dentro un ambiente di monitoraggio permanente, **cambiano i comportamenti sociali e politici**.

Le persone evitano proteste, riducono la partecipazione pubblica, limitano gli spostamenti o interrompono relazioni considerate rischiose. **La sorveglianza non agisce soltanto attraverso l'arresto o la deportazione: produce conformismo, paura e autocensura**.

Il caso dell'ICE mostra con chiarezza una tendenza ormai globale. Le tecnologie di analisi predittiva e integrazione massiva dei dati stanno ridefinendo il rapporto tra cittadini e istituzioni. Sistemi nati per migliorare l'efficienza amministrativa vengono progressivamente trasformati in **infrastrutture permanenti di controllo**. E quando queste capacità si concentrano nelle mani di apparati securitari con ampi margini operativi e limitati obblighi di trasparenza (quello che Trump ha voluto per l'ICE)**, il rischio non riguarda più soltanto i migranti. Riguarda l'equilibrio stesso tra sicurezza, libertà e democrazia**.

La questione Palantir-ICE è di fatto un precedente che

interroga direttamente il futuro delle società democratiche: fino a che punto siamo disposti ad accettare che lo Stato utilizzi infrastrutture digitali capaci di trasformare ogni traccia informativa in uno strumento di sorveglianza?
Dove finiscono e come vengono utilizzati i nostri dati?
Noi, oggi, siamo ormai (diventati) anche un *cluster* di dati. Trovare queste risposte equivale a garantirci sicurezza e libertà personali. E soprattutto, è necessario capire chi davvero raccoglie, usa e controlla i nostri dati? Chi realmente (lo Stato o le grandi corporation del settore tecnologico?) stabilisce le regole di questa sorveglianza di massa e con quali scopi?

Novità su Google, per aggiungere Key4Biz tra le tue fonti preferite, clicca qui

Leggi le altre notizie sull'home page di Key4biz

https://www.key4biz.it/palantir-passa-allice-una-lista-di-20-milioni-di-americani-da-sorvegliare/572655/

Per Draghi e Lagarde la

transizione green non è un lusso

Rallentare il green deal dell’Ue aggrava le vulnerabilità energetiche, tecnologiche, geopolitiche e climatiche

L’Europa ha scoperto che la **transizione energetica** non è una questione ambientale separata dalla politica industriale, dalla sicurezza e dalla stabilità economica. È diventata, al contrario, il punto di intersezione tra tutte le grandi fragilità strategiche del continente: la **dipendenza energetica dall’estero**, il **ritardo tecnologico** rispetto a Stati Uniti e Cina, l’esposizione alle **crisi geopolitiche** e la crescente **vulnerabilità climatica.** Per questo motivo, nel dibattito europeo sta emergendo una consapevolezza nuova: rallentare il **Green Deal** non significherebbe proteggere l’economia europea, ma indebolirla ulteriormente.

Gli ultimi mesi hanno accelerato questa presa di coscienza, secondo l’analisi di Antonio Pollio Salimbeni, corrispondente a Bruxelles per Il Sole 24 Ore Radiocor ed esperto di economia internazionale, su *La Matinale Européenne*. Lo shock geopolitico legato allo **Stretto di Hormuz**, tornato al centro delle tensioni internazionali dopo i bombardamenti di USA e Israele in Iran, ha ricordato quanto l’Europa resti esposta alle crisi dei combustibili fossili. Negli ultimi anni, una parte significativa del dibattito politico europeo aveva attribuito proprio alla transizione verde l’aumento dei costi energetici e la perdita di competitività industriale.
Molti governi, tra cui il nostro, avevano chiesto apertamente di rallentare o ridimensionare il Green Deal. Ma la nuova

instabilità mediorientale ha riportato al centro una realtà spesso rimossa: l'Unione europea (Ue) importa ancora circa il 60% della propria energia e continua a dipendere quasi integralmente da fonti fossili provenienti da aree geopoliticamente instabili.

Per la Presidente della Bce Christine Lagarde il vero costo della transizione è nei suoi ritardi

È in questo contesto che la **Banca centrale europea** (Bce) ha scelto di intervenire con un messaggio politico ed economico piuttosto orientato inaspettatamente alla transizione green. La presidente della Bce, **Christine Lagarde**, e il capo economista **Philip Lane** hanno rilanciato a Francoforte un paradigma strategico europeo caratterizzato non più una contrapposizione tra sostenibilità e crescita, ma dalla convinzione che **sicurezza energetica, stabilità dei prezzi, innovazione industriale e autonomia geopolitica** siano ormai elementi inseparabili.

"*Gli ultimi dieci anni hanno messo in luce un paradosso preoccupante* – ha affermato Lagarde – ***ogni nuovo dato sottolinea la necessità di accelerare la transizione verde, eppure questa sta perdendo slancio****. L'anno scorso, le emissioni globali di carbonio derivanti dai combustibili fossili hanno raggiunto livelli record e ora stiamo assistendo a un'inversione di tendenza in alcune giurisdizioni*". Il riferimento agli Stati Uniti è evidente, soprattutto dopo il progressivo smantellamento di alcune politiche climatiche federali, ma Lagarde guarda anche alle resistenze interne all'Europa.

La presidente della Bce ha infatti affrontato direttamente il cuore della polemica politica europea: "*Negli ultimi anni,*

abbiamo persino assistito a dibattiti in Europa sull'eventualità che la transizione verde abbia reso il continente più vulnerabile in un mondo geopoliticamente instabile, aumentando le bollette energetiche. Eppure, lo status quo è chiaramente insostenibile, dato che l'Europa importa circa il 60% della sua energia, quasi interamente da combustibili fossili. L'attuale impennata dei prezzi dell'energia ci ricorda il costo di questa dipendenza".

È un passaggio cruciale perché ribalta completamente la narrativa dominante di una parte del dibattito pubblico europeo. Secondo la Bce, **il vero fattore di vulnerabilità non è la transizione energetica**, **ma il ritardo della transizione stessa**. Più l'Europa rimane ancorata ai combustibili fossili, più resta esposta alla volatilità dei prezzi internazionali, alle crisi geopolitiche e alle pressioni strategiche dei grandi esportatori di energia.

Per Mario Draghi le sfide decisive si giocano sulla sicurezza energetica e l'AI

Dal 2020 l'Europa è stata colpita da una pesante sequenza di shock (pandemie, tensioni commerciali, guerre e crisi energetiche) che hanno messo in luce una fragilità strutturale: la dipendenza strategica dall'esterno. **Mario Draghi**, ospite ieri nel municipio di Aquisgrana, dove è stato insignito del *Premio Carlo Magno*, di fronte a vari capi di Stato europei, alla Presidente della Commissione europea, **Ursula von der Leyen** e la stessa Lagarde, ha spiecato che la crescita economica è oggi la condizione indispensabile per finanziare la transizione energetica, rafforzare la difesa, sostenere l'invecchiamento della popolazione e costruire le industrie digitali del futuro.

Uno dei punti centrali del discorso dell'ex presidente della

Banca centrale europea ed ex premier italiano riguarda proprio l'energia. L'Europa continua a dipendere in modo eccessivo dalle importazioni, in particolare dal gas naturale liquefatto americano e dalle catene di approvvigionamento cinesi per le tecnologie verdi. Questa vulnerabilità rende il continente più esposto agli shock geopolitici e all'aumento dei prezzi. Draghi sostiene che un mercato energetico europeo davvero integrato, con reti, interconnessioni e capacità di stoccaggio condivise, permetterebbe una **maggiore sicurezza energetica** e accelererebbe la **decarbonizzazione**. I paesi con una quota più alta di **energia pulita**, osserva, stanno già pagando prezzi dell'elettricità significativamente più bassi.

Il secondo tema è quello dell'indipendenza economica e strategica. Secondo Draghi, l'Europa non ha ancora costruito un sistema capace di trattenere e investire i propri risparmi nell'economia reale europea. Una parte consistente del capitale europeo continua infatti a finanziare innovazione e crescita negli Stati Uniti, dove il mercato dei capitali è più integrato e dinamico. Questa situazione aumenta la dipendenza europea dall'esterno e limita la capacità del continente di reagire rapidamente alle crisi.

La sfida decisiva riguarda però le tecnologie digitali e l'intelligenza artificiale. Draghi sottolinea come il divario di produttività tra Europa e Stati Uniti si stia ampliando, trainato soprattutto dalla maggiore digitalizzazione dell'economia americana. L'AI rappresenta una svolta storica: secondo le stime OCSE, potrebbe generare circa metà della crescita della produttività del prossimo decennio. Ma per competere servono investimenti enormi in energia, semiconduttori, infrastrutture di calcolo e data center.

Qui l'Europa rischia di restare indietro rispetto a Stati Uniti e Cina, che stanno investendo su scala molto più ampia. Draghi avverte che l'intelligenza artificiale non è una tecnologia come le altre: migliora con l'uso e crea vantaggi cumulativi permanenti per chi parte prima. Per questo il

ritardo europeo non è solo economico, ma strategico.

Il messaggio finale è chiaro: autonomia tecnologica e energetica sono due facce della stessa sfida. Senza integrazione economica, investimenti comuni e capacità industriale, l'Europa rischia di perdere sovranità, competitività e peso geopolitico nel mondo del prossimo decennio.

Fonti rinnovabili per affrontare crisi energetica e climatica

Lagarde, che nel suo discorso ad Aquisgrana per celebrare Draghi ha rilanciato il dovere dell'Europa di "*rimanere padrona del proprio destino*", iniziando proprio da "*mercati energetici troppo frammentati*", ha anche sottolineato come i Paesi maggiormente avanzati nella produzione elettrica da fonti non fossili abbiano mostrato una maggiore resilienza agli shock energetici. "*I Paesi in cui una quota maggiore di elettricità è generata da **fonti non fossili**, come Spagna e Portogallo, sono stati meglio protetti dall'aumento dei prezzi del gas*", ha spiegato. Non è solo un argomento ambientale: è una questione di autonomia energetica, competitività economica e stabilità macroeconomica.

Philip Lane ha rafforzato questa analisi con un messaggio altrettanto netto. "*Sebbene vi siano costi a breve termine, ad esempio a causa delle tasse sul carbonio, **il passaggio alle energie rinnovabili renderà l'area dell'euro più resiliente** riducendo la dipendenza dalle importazioni di combustibili fossili e dovrebbe anche ridurre la volatilità dell'inflazione*", ha dichiarato il capo economista della BCE. È un cambio di prospettiva importante anche per una banca centrale tradizionalmente concentrata esclusivamente sulla stabilità monetaria. **Oggi Francoforte considera il cambiamento climatico e la dipendenza energetica fattori diretti di instabilità inflazionistica**.

La questione climatica non viene più interpretata come un rischio futuro, ma come una variabile economica già pienamente operativa. Secondo le stime dell'Organizzazione meteorologica mondiale riportate da **Shiv Yucel**, Dottoranda in Geografia e Ambiente presso l'Università di Oxford, in un articolo pubblicato su *The Conversation*, **l'ondata di calore dell'estate 2025 ha contribuito a un aumento annuo dei prezzi dei prodotti alimentari non trasformati nell'Eurozona compreso tra lo 0,4% e lo 0,7**%. Non solo, si è scoperto che quattro anni dopo una siccità, o un'alluvione, la produzione regionale resta mediamente inferiore di tre punti percentuali rispetto ai livelli precedenti.

L'impatto umano è altrettanto drammatico. Nell'estate del 2025, **dieci giorni di caldo estremo hanno provocato 2.300 morti in dodici grandi città europee**, di cui 1.500 attribuibili direttamente ai cambiamenti climatici che hanno amplificato le temperature tra uno e quattro gradi. Le ondate di calore, secondo i dati internazionali, sono state responsabili di quasi mezzo milione di morti l'anno nel mondo tra il 2000 e il 2019. A ciò si aggiungono lo scioglimento accelerato dei ghiacciai europei e un'estensione senza precedenti degli incendi boschivi.

Lane ha insistito anche su un elemento spesso sottovalutato nelle dinamiche monetarie: "*L'inflazione nel settore alimentare gioca un ruolo significativo nel determinare la percezione delle famiglie sul tasso di inflazione prevalente e le loro aspettative di inflazione a breve termine*". In altre parole, la crisi climatica non colpisce soltanto la produzione agricola, ma influenza direttamente la fiducia sociale e la stabilità delle aspettative economiche.

Come si legge nel **bollettino economico** pubblicato oggi dalla Bce: l'inflazione dei beni energetici è balzata al 10,9% dopo il 5,1% di marzo, mentre per quanto concerne i beni alimentari, ha registrato un lieve aumento, al 2,5%, "*i rischi al rialzo per l'inflazione e quelli al ribasso per la crescita*

si sono intensificati”.

La transizione green è sempre più una strategia industriale e geopolitica per l’Europa, che qui si gioca un pezzo di sovranità

Il punto centrale, tuttavia, è che la transizione energetica europea non può essere ridotta a una semplice politica climatica. È ormai una strategia industriale e geopolitica. L’Europa si trova stretta tra due modelli di capitalismo industriale aggressivo: quello americano, sostenuto da enormi incentivi pubblici e dal protezionismo tecnologico dell’*Inflation Reduction Act*, e quello cinese, basato sul controllo delle catene globali delle materie prime critiche, delle batterie, dei pannelli solari e delle tecnologie verdi.

L’Unione europea rischia di trovarsi contemporaneamente dipendente dall’estero per l’energia e **subordinata tecnologicamente nelle filiere strategiche della transizione**. È questo il vero nodo politico del Green Deal nella sua nuova fase: non solo decarbonizzare, ma costruire una capacità industriale europea autonoma nelle reti elettriche, nell’idrogeno, nelle batterie, nei semiconduttori, nei materiali critici e nelle tecnologie pulite.

Anche per questo la Commissione europea ha progressivamente modificato il proprio approccio. Se nella prima fase del Green Deal il focus era prevalentemente regolatorio, oggi Bruxelles guarda sempre più agli aspetti strutturali del sistema energetico europeo: interconnessione delle reti, accumulo energetico, infrastrutture comuni, diversificazione delle fonti di approvvigionamento e politica industriale continentale. L’obiettivo non è soltanto ridurre le emissioni, ma costruire una vera **sovranità energetica europea**.

In questo quadro assume particolare rilievo la posizione di Olli Rehn, governatore della banca centrale finlandese ed ex commissario europeo all'Economia. Rehn, in passato associato alle teorie dell'"austerità espansiva", oggi sostiene che l'Europa debba affrontare simultaneamente tre grandi sfide strategiche: la sicurezza continentale, la transizione energetica e climatica e la crescita economica fondata sugli investimenti.

Il messaggio è chiaro: senza investimenti massicci nella trasformazione energetica e tecnologica, l'Europa rischia di perdere definitivamente peso economico e politico nello scenario globale. La transizione green non è più un capitolo separato delle politiche pubbliche europee. È diventata il terreno decisivo su cui si giocheranno la competitività industriale, la stabilità economica e l'autonomia strategica del continente nei prossimi decenni.

Il ritorno (inevitabile) del green

Oggi Draghi e Lagarde presentano la transizione energetica come la risposta quasi naturale alla fragilità europea: meno dipendenza dai fossili importati, più resilienza agli shock, più autonomia strategica. Ma questa lettura arriva dopo anni in cui le istituzioni europee hanno trattato il clima soprattutto come un dossier tecnico, da integrare con prudenza nei modelli macroeconomici e nei bilanci delle banche centrali, non come una questione di potere, sicurezza e sovranità industriale.

Chi la pensava diversamente finiva spesso per essere etichettato come "complottista", ingenuo o legato a impostazioni ideologiche dannose per l'Europa.

Il risultato di questo 'ripensamento' generale è una narrazione molto più ambiziosa sul piano politico, ma anche più comoda: attribuisce alla transizione green un ruolo risolutivo, proprio mentre l'Europa paga il prezzo di ritardi,

scelte sbagliate (queste sì legate a ideologie retrograde), contraddizioni e dipendenze costruite nel tempo.

Novità su Google, per aggiungere Key4Biz tra le tue fonti preferite, clicca qui

Leggi le altre notizie sull'home page di Key4biz

https://www.key4biz.it/per-draghi-e-lagarde-la-transizione-green-non-e-un-lusso/572641/

OSINT Offensivo: l'arma invisibile che precede ogni attacco

Nella cybersecurity esiste una contraddizione che viene sistematicamente sottovalutata: quanto più un'organizzazione comunica, si promuove e si digitalizza, tanto più amplia involontariamente la propria superficie di attacco. Non attraverso falle nel codice o configurazioni errate, ma attraverso qualcosa di molto più ordinario: le informazioni pubblicamente disponibili su se stessa.

OSINT offensivo: la ricognizione invisibile che precede ogni attacco

L'***Open Source Intelligence*** offensiva, nota come *offensive OSINT*, è la pratica con cui attori malevoli raccolgono, correlano e trasformano in arma questi dati pubblici, tutto senza mai toccare un sistema target, senza inviare un pacchetto sospetto, senza lasciare traccia nei log. Come documenta ShadowDragon nel suo riferimento 2026 sull'argomento, la *ricognizione passiva* non interagisce con la presenza online del bersaglio e rimane non rilevabile, non lasciando alcuna traccia dell'attività di raccolta informazioni. È invisibile per definizione.

Questa invisibilità è la prima ragione per cui l'*offensive OSINT* è tanto pericolosa quanto sottostimata.

La guerra inizia prima dell'attacco: la fase di ricognizione

La ricognizione precede ogni intrusione. Nel framework MITRE ATT&CK, la tattica **TA0043** cataloga formalmente le tecniche con cui gli avversari raccolgono informazioni utili a pianificare operazioni future, distinguendo tra raccolta attiva e passiva. La distinzione non è accademica: determina il profilo di rischio dell'attaccante e la tracciabilità dell'operazione.

La **ricognizione passiva** si alimenta di tutto ciò che è già pubblico: record *DNS*, certificati digitali, metadati nei documenti, profili *LinkedIn*, offerte di lavoro, repository *GitHub*, comunicati stampa. Nulla di illegale, nulla di tecnico nel senso tradizionale del termine. Eppure questi dati, correlati con metodo, costruiscono un profilo operativo estremamente preciso di qualsiasi organizzazione.

La ricognizione attiva, invece, prevede un’interazione diretta con i sistemi del bersaglio, come la scansione delle porte o l’enumerazione dei servizi, e per questa ragione genera tracce rilevabili. Gli attaccanti sofisticati tendono a restare nella fase passiva il più a lungo possibile, spostandosi all’attivo solo quando hanno già un quadro sufficientemente dettagliato per operare in modo chirurgico.

Come osserva Vectra AI nel suo approfondimento del marzo 2026 sulla ricognizione, la profilazione *OSINT* include la mappatura dei ruoli dei dipendenti, dei fornitori e delle tecnologie a partire da fonti pubbliche come *LinkedIn*, le offerte di lavoro e i *repository* di codice. Queste attività non generano telemetria difensiva: compaiono nel *log* solo dopo, come precisione inaspettata nelle fasi successive dell’attacco.

Che cosa cercano davvero gli attaccanti: non vulnerabilità ma contesto

L’errore più comune nel ragionare sull’*offensive OSINT* è pensare che gli attaccanti cerchino vulnerabilità tecniche. In realtà, nella fase di ricognizione cercano soprattutto **contesto**: chi prende le decisioni, quali fornitori si utilizzano, quale stack tecnologico è in produzione, quale ufficio gestisce i bonifici, chi ha appena cambiato ruolo, chi è in trasferta.

Questi dati, individualmente irrilevanti, diventano letali una volta aggregati. SecurityScorecard evidenzia nel suo aggiornamento del 2026 che la raccolta passiva permette ai *threat actor* di costruire profili completi delle organizzazioni target prima ancora di passare a metodi di raccolta attiva come la scansione delle porte o le verifiche sulle applicazioni *web*. Questa ricognizione rivela spesso vettori d’attacco che i team di sicurezza trascurano.

Le fonti preferite degli attaccanti includono: offerte di lavoro (che rivelano stack tecnologici e strumenti di sicurezza adottati); profili sui *social network* professionali (che espongono organigrammi, riporti diretti e responsabilità operative); *repository* pubblici di codice (dove credenziali hardcoded e configurazioni sensibili compaiono con frequenza sorprendente); *certificate transparency log* (che rivelano sottodomini e infrastruttura interna); e *breach database* pubblicamente accessibili (che contengono credenziali riutilizzate o pattern di password aziendali).

Il ruolo abilitante dell'intelligenza artificiale

Se la *reconnaissance* manuale richiedeva tempo e competenze, l'integrazione dell'intelligenza artificiale nei flussi di lavoro offensivi ha abbattuto entrambe le barriere. Il Google Threat Intelligence Group documenta nel suo report del febbraio 2026 che gli *APT actor* hanno usato strumenti di *AI* a supporto di diverse fasi del ciclo di vita dell'attacco, con un focus specifico sulla ricognizione e sullo sviluppo dei target per facilitare il compromesso iniziale.

I casi documentati dal *GTIG* sono precisi e verificati. **APT42**, il gruppo iraniano noto anche come *Charming Kitten* o *Mint Sandstorm*, ha impiegato modelli *AI* per cercare indirizzi email ufficiali di specifiche entità, condurre ricognizioni su potenziali partner commerciali e costruire *persona* credibili a partire dalla biografia dei target. **UNC2970**, il gruppo nordcoreano collegato a *Lazarus Group*, ha sintetizzato intelligence *open source* per profilare figure di alto valore nel settore della difesa e della cybersecurity, mappando ruoli tecnici specifici e informazioni salariali per affinare le campagne di *spear phishing*.

La portata di questa accelerazione diventa concreta guardando i dati operativi. Il *Palo Alto Networks Unit 42 Global*

Incident Response Report 2026, basato su oltre 750 indagini in più di 50 paesi, certifica che nel 2025 gli attacchi più veloci hanno raggiunto l'esfiltrazione dei dati in soli **72 minuti** dall'accesso iniziale, rispetto ai 285 minuti dell'anno precedente: una riduzione quadrupla del tempo che i difensori hanno a disposizione per rilevare e contenere una minaccia.

Questo è il paradosso che l'AI introduce nell'equazione: mentre velocizza e personalizza la ricognizione sul lato offensivo, comprime drammaticamente la finestra di risposta disponibile sul lato difensivo.

La supply chain come bersaglio strategico: l'anello debole è il tuo fornitore

L'*offensive OSINT* non si limita al perimetro diretto dell'organizzazione target. Uno dei suoi utilizzi più efficaci è la mappatura della catena di fornitura: identificare i fornitori critici, le loro integrazioni tecniche, i contratti pubblici, le partnership dichiarate. Una volta individuato l'anello più debole dell'ecosistema, l'attaccante non ha bisogno di affrontare le difese del bersaglio principale.

I dati del *Unit 42 Report 2026* certificano che nel 2025 le applicazioni *SaaS* di terze parti sono state rilevanti nel **23% dei casi** analizzati. In un'indagine documentata nel report, gli attaccanti hanno sfruttato *token OAuth* validi di una piattaforma commerciale compromessa per accedere agli ambienti *Salesforce* dell'organizzazione target. La revisione post-incidente ha rivelato quasi 100 integrazioni di terze parti collegate all'istanza, molte delle quali inattive, non monitorate o associate a ex dipendenti.

Per un *threat actor* che ha condotto una ricognizione *OSINT* accurata, l'identificazione di questa rete di trust è

tutt’altro che casuale: è il risultato di settimane di analisi pubblica delle relazioni tra fornitori, dei contratti pubblicati, degli annunci di partnership. Informazioni che esistono nel dominio pubblico e che nessuno, nel frattempo, stava aggregando e interpretando con intento offensivo.

Il tema è strettamente collegato alle pratiche di *threat intelligence* e gestione del rischio di terze parti, su cui ICT Security Magazine ha già pubblicato approfondimenti specifici nel contesto della conformità NIS2.

La velocità come elemento sistemico

Un dato del *Unit 42 Report 2026* richiede una riflessione separata: gli attaccanti cominciano a scansionare nuove vulnerabilità entro **15 minuti** dall’annuncio pubblico di un *CVE*. In molti casi, i tentativi di *exploit* iniziano prima che i team di sicurezza abbiano terminato di leggere l’*advisory*.

Questo dato ridefinisce il problema. L’*OSINT* offensiva non è soltanto uno strumento per la fase preparatoria degli attacchi mirati: è anche un meccanismo di monitoraggio continuo che consente agli attaccanti di identificare opportunità in tempo reale. La stessa logica con cui un analista difensivo monitora le fonti pubbliche per anticipare le mosse degli avversari viene applicata specularmente da chi vuole sfruttarle.

Le strutture di identità digitale delle organizzazioni sono l’altra faccia del problema. Sempre secondo il *Unit 42 Report 2026*, **le debolezze nell’identità hanno giocato un ruolo materiale in circa il 90% delle indagini condotte**. Non perché le credenziali siano state rubate attraverso attacchi tecnici sofisticati, ma perché informazioni pubblicamente disponibili, abbinate a tecniche di *social engineering* alimentate da ricognizione *OSINT*, hanno reso i tentativi di compromissione dell’identità estremamente efficaci.

Questo legame diretto tra *offensive OSINT* e attacchi di *social*

engineering è uno degli aspetti più critici e meno presidiati del panorama attuale.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/osint-offensivo/

L’AI svuota il mercato degli hard disk rendendo impossibile archiviare su Internet

L’esplosione della domanda di infrastrutture AI sta producendo un effetto collaterale inatteso: hard disk e sistemi di storage stanno diventando sempre più costosi e difficili da reperire, mettendo in difficoltà **archivisti digitali**, **università**, **Wikimedia** e persino **Internet Archive.**

Secondo un’inchiesta pubblicata da 404 Media, la corsa globale ai data center per l’intelligenza artificiale ha generato un’impennata dei prezzi di **SSD**, **RAM** e dischi ad alta capacità, con aumenti che in alcuni casi superano il 150%. Alcuni modelli sono completamente esauriti, mentre sul mercato secondario iniziano a comparire fenomeni di bagarinaggio digitale e rivendita a prezzi gonfiati.

Hard disk: Prezzi fuori controllo

Negli ultimi mesi i prezzi dello storage sono aumentati in modo significativo sia nel segmento consumer sia enterprise. 404 Media cita il caso di un SSD esterno **Samsung** da 2TB acquistato lo scorso autunno per 159 dollari e oggi venduto a

oltre 575 dollari.

Anche PC Part Picker, piattaforma che monitora l’andamento dei prezzi hardware, mostra un incremento costante dei costi a partire dalla fine del 2025. In molti negozi SSD e hard disk risultano esauriti, soprattutto quelli ad alta capacità utilizzati nei data center AI.

Internet Archive: “Problema reale che ci costa tempo e denaro”

Tra le realtà più colpite c’è Internet Archive, il progetto che gestisce la Wayback Machine e uno dei più importanti archivi della storia del web.

Brewster Kahle, fondatore dell’organizzazione, ha spiegato a 404 Media che la situazione sta creando difficoltà operative concrete.

“Abbiamo scoperto che i dischi da 28-30TB che preferiamo usare semplicemente non sono disponibili o hanno prezzi molto elevati”, ha dichiarato.

Internet Archive raccoglie oltre 100 terabyte di nuovi materiali ogni giorno e conserva già più di 210 petabyte di dati archiviati. Un’infrastruttura di questo tipo richiede aggiornamenti continui e un flusso costante di nuovi hard disk.

“È un problema molto reale che ci costa tempo e denaro”, ha aggiunto Kahle, spiegando che l’organizzazione sta cercando supporto anche direttamente dai produttori di hard disk.

Anche Wikipedia teme l’impatto

Le difficoltà riguardano anche Wikimedia Foundation, che gestisce Wikipedia e Wikimedia Commons.

“Con oltre 65 milioni di articoli solo su Wikipedia, l’accesso a server e capacità di storage è vitale per noi”, ha spiegato un portavoce della fondazione a 404 Media.

Secondo Wikimedia, gli aumenti dei prezzi riguardano non solo hard disk e memoria, ma anche i tempi di consegna dei server e la possibilità di pianificare nuovi ordini.

Essendo una no profit, Wikimedia deve valutare attentamente ogni investimento hardware. Per questo la fondazione sta cercando di estendere la vita utile dei sistemi esistenti e rendere più flessibile la gestione delle infrastrutture.

I produttori privilegiano i data center AI

Dietro la crisi dello storage c’è la priorità data ai grandi clienti AI. Western Digital avrebbe già praticamente venduto tutta la propria capacità produttiva 2026 a clienti enterprise, molti dei quali legati ai data center AI.

Micron, invece, ha annunciato l’uscita dal mercato consumer Crucial, spiegando che la domanda generata dall’AI nei data center ha reso necessario concentrare produzione e supporto sui clienti strategici.

Il risultato è che progetti di archiviazione digitale, università, ricercatori e piccoli operatori stanno faticando a trovare componenti disponibili.

I data hoarder rinunciano ad archiviare

Il tema domina anche le discussioni nella community Reddit r/DataHoarder, dove archivisti amatoriali e appassionati di backup condividono frustrazione e strategie di sopravvivenza.

Molti utenti dichiarano di aver sospeso l’acquisto di nuovi dischi o di aver ridotto drasticamente i propri progetti di archiviazione. Alcuni cercano modi per riutilizzare vecchi hard disk di piccola capacità, altri parlano apertamente di “aspettare il 2029” sperando in una normalizzazione del mercato.

In diversi commenti emerge la convinzione che le grandi aziende AI e i data center abbiano già preacquistato gran parte della produzione disponibile per gli anni futuri.

Il costo nascosto della corsa all’AI

La crisi dello storage mostra uno degli effetti meno visibili della corsa globale all’intelligenza artificiale. L’AI non sta solo consumando enormi quantità di energia e potenza computazionale: sta anche drenando componenti hardware fondamentali per altri settori.

Il rischio è che archivi storici, progetti culturali, ricerca accademica e iniziative di conservazione digitale inizino a rallentare proprio mentre la rete produce quantità sempre maggiori di dati.

Novità su Google, per aggiungere Key4Biz tra le tue fonti preferite, clicca qui

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/lai-svuota-il-mercato-degli-hard-disk-rendendo-impossibile-archiviare-su-internet/572092/

AI-OSINT: quando l’intelligenza artificiale ridefinisce i confini dell’intelligence aperta

L’*Open Source Intelligence* non è mai stata soltanto una questione di strumenti. È sempre stata, prima di tutto, una questione di metodo: la capacità di trasformare frammenti di informazione pubblica in conoscenza operativa, passando attraverso raccolta, correlazione, verifica e interpretazione. Per decenni, questo processo ha richiesto pazienza, rigore analitico e una buona dose di creatività umana. Oggi, l’intelligenza artificiale sta comprimendo in minuti ciò che richiedeva giorni, e sta aprendo possibilità analitiche che fino a poco tempo fa appartenevano alla fantascienza. Ma sta anche consegnando le stesse capacità a chi ha interesse a fare danno.

Questo è il doppio binario su cui si muove l’AI-OSINT nel 2026: uno strumento di straordinaria utilità difensiva e, al tempo stesso, un moltiplicatore di forza per gli avversari. Capire entrambe le facce non è un esercizio teorico, è una necessità pratica per chiunque lavori nel campo della sicurezza.

Il problema del volume: quando i dati superano la capacità umana

Al cuore dell'OSINT è sempre stata la capacità di usare dati pubblici per risolvere un'indagine, ma oggi il volume ha superato di gran lunga ciò che qualsiasi analista umano può realisticamente gestire. Il web indicizzato, il *dark web*, i social media, i registri pubblici, le immagini satellitari commerciali, le *blockchain*, i *repository* di codice aperti: la superficie informativa disponibile cresce in modo esponenziale, e con essa il rischio che segnali rilevanti si perdano nel rumore.

Secondo un'analisi peer-reviewed condotta da Riccardo Ghioni, Mariarosaria Taddeo e Luciano Floridi dell'Oxford Internet Institute, pubblicata sulla rivista *AI & Society* nel 2023, l'OSINT costituisce oggi tra l'80 e il 90 per cento di tutte le attività di *intelligence* condotte dalle forze dell'ordine e dai servizi di sicurezza in Occidente. Questo dato, già significativo, diventa ancora più rilevante se si considera che la mole di dati pubblicamente accessibili continua ad aumentare. L'analista umano, per quanto esperto, incontra un limite fisico invalicabile.

Il mercato globale dell'OSINT riflette questa centralità crescente: secondo Global Market Insights, il settore era valutato 12,7 miliardi di dollari nel 2025 e si prevede raggiunga i 133,6 miliardi entro il 2035, con un tasso di crescita annuo composto del 26,7%. Una traiettoria che segnala un'adozione sistematica, non più sperimentale, in governi, aziende e organizzazioni di sicurezza di tutto il mondo.

Con il calo del costo della potenza di calcolo e la sofisticazione crescente degli algoritmi, quantità sempre maggiori di dati possono essere acquisiti ed elaborati in tempo quasi reale. L'AI non sostituisce il ragionamento dell'analista: abbatte il collo di bottiglia che precede quel

ragionamento, liberando risorse cognitive per le fasi a più alto valore aggiunto.

Cosa cambia con i modelli linguistici di grandi dimensioni

L'introduzione dei *Large Language Model* (LLM) nella *toolchain* OSINT ha segnato un salto qualitativo rispetto alle generazioni precedenti di automazione. Non si tratta più soltanto di *parser* e *crawler*: i modelli linguistici possono leggere, riassumere, tradurre, correlare e suggerire percorsi di indagine su testi non strutturati provenienti da fonti eterogenee.

Lo Stimson Center, nel webinar del 26 marzo 2026 organizzato congiuntamente dallo *Strategic Foresight Hub* e dall'*Energy, Water, and Sustainability Program*, ha esaminato come i sistemi guidati dall'AI stiano trasformando la pratica OSINT allargandone le applicazioni attraverso sicurezza, *governance* e sviluppo sostenibile, analizzando in particolare le *pipeline* che alimentano modelli di analisi con dati da social media e immagini satellitari, e i sistemi di *machine learning* che classificano e mappano eventi globali in tempo reale.

Il contributo dei modelli linguistici si articola su più livelli. In fase di raccolta, automatizzano la strutturazione di dati grezzi eterogenei rendendoli immediatamente utilizzabili per analisi successive. In fase di verifica, permettono di confrontare più fonti simultaneamente, incrociare affermazioni e segnalare contraddizioni: un analista che indaga su un profilo sospetto può usare strumenti AI per confrontare nomi utente, biografie e attività in tempo reale, identificando istantaneamente le discrepanze. In fase di esplorazione, suggeriscono nuovi percorsi investigativi quando le piste sembrano esaurite.

La capacità multilingue merita un cenno a parte. L'OSINT

operata su scala globale si scontra sistematicamente con la barriera linguistica: la maggior parte dei segnali di interesse non è in inglese. I modelli linguistici attuali trattano questa barriera come una variabile secondaria, non come un ostacolo strutturale. Per approfondire il ruolo dell'AI nella cybersecurity difensiva si rimanda agli approfondimenti della redazione.

Il lato oscuro: i *threat actor* e l'OSINT potenziata dall'AI

Ogni capacità difensiva ha la sua controparte offensiva. L'AI applicata all'OSINT non fa eccezione, e i dati disponibili nel 2026 disegnano un quadro preoccupante ma anche, almeno per ora, parzialmente rassicurante nelle sue proporzioni effettive.

Per gli attori sostenuti da governi, i modelli linguistici di grandi dimensioni sono diventati strumenti essenziali per la ricerca tecnica, la definizione dei *target* e la rapida generazione di contenuti di *phishing* sofisticati. Il report trimestrale di Google GTIG del 12 febbraio 2026 documenta come gruppi legati a Corea del Nord, Iran, Cina e Russia abbiano operazionalizzato l'AI nella seconda metà del 2025, coprendo attività di oltre 57 gruppi APT distinti provenienti da almeno sedici paesi.

Il meccanismo è preciso: i *threat actor* usano l'AI per accelerare la *reconnaissance* e trasformare informazioni pubblicamente disponibili in piani di attacco pronti all'uso. Invece di passare manualmente in rassegna siti web, profili social, dati di *breach* e tracce tecniche, possono usare strumenti AI per sintetizzare grandi volumi di OSINT in note di *targeting* operative.

Gli LLM possono servire come moltiplicatori strategici durante la fase di *reconnaissance*, consentendo agli attori malevoli di

profilare rapidamente *target* ad alto valore, identificare i decisori chiave nei settori della difesa e mappare le gerarchie organizzative, passando dalla *reconnaissance* iniziale al *targeting* attivo con velocità e scala prima impossibili.

Una precisazione fondamentale è però indispensabile per leggere correttamente questo scenario: GTIG specifica chiaramente che i *threat actor* stanno sperimentando con l'AI ottenendo guadagni di produttività, **ma non stanno ancora sviluppando capacità genuinamente nuove** che alterino in modo fondamentale il panorama delle minacce. L'AI agisce come acceleratore della *tradecraft* esistente, non come generatore di capacità radicalmente diverse.

Il blog Microsoft Security del 6 marzo 2026 ha documentato una dinamica ulteriore: sebbene non ancora osservata su larga scala, la sperimentazione con sistemi di AI *agentici* segnala un potenziale cambiamento nella *tradecraft*, dove flussi di lavoro supportati dall'AI assistono sempre più il processo decisionale iterativo e l'esecuzione di compiti, indicando un adattamento più rapido e una maggiore resilienza nelle intrusioni future. In particolare, il gruppo nordcoreano Coral Sleet ha già sviluppato un flusso di lavoro completamente AI-assistito per la creazione di *lure*, il *provisioning* di infrastrutture e il *testing* di *payload*.

Il termine *agentico* merita una definizione precisa. A differenza dei modelli linguistici reattivi, i sistemi di AI *agentici* si basano sugli stessi modelli sottostanti ma sono integrati in flussi di lavoro che perseguono obiettivi nel tempo, pianificando passi, invocando strumenti, valutando risultati e adattando il comportamento senza continui interventi umani.

Ancora più recentemente, al RSAC 2026 di aprile, Microsoft ha presentato dati che mostrano come l'AI stia riducendo le frizioni lungo l'intero ciclo di vita dell'attacco, aiutando i

threat actor a fare ricerche più velocemente, scrivere *lure* migliori, generare o effettuare il *debug* di *malware* e triagare i dati rubati. Rimane tuttavia ancora un operatore umano nel ciclo che controlla le campagne, senza AI pienamente autonoma o *agentiva* che gestisca gli attacchi in modo indipendente.

Il paradosso della disinformazione: l'AI come problema e come soluzione

Esiste una tensione profonda al cuore dell'AI-OSINT che merita di essere nominata esplicitamente. L'AI genera contenuti sintetici in quantità e qualità crescenti, rendendo la verifica dell'informazione sempre più difficile. Al tempo stesso, l'AI è lo strumento principale che abbiamo per operare quella verifica su scala.

Secondo Blackdot Solutions, la disinformazione generata dall'AI e i *deepfake* rendono più difficile che mai fidarsi di ciò che si vede online. Nel 2026, i professionisti OSINT si trovano ad affrontare un bisogno ancora maggiore di verificare l'autenticità delle informazioni, poiché gli attori malevoli usano strumenti avanzati per manipolare i media e creare identità false convincenti. Sarà cruciale per le organizzazioni assicurarsi che i propri analisti siano addestrati a riconoscere i contenuti generati dall'AI; in caso contrario, rischiano di facilitare involontariamente attività criminali.

La conseguenza pratica è che la catena di verifica dell'OSINT non può più appoggiarsi soltanto sull'analisi semantica del contenuto: deve includere l'analisi della provenienza, della coerenza interna, della contestualizzazione storica e del confronto con fonti primarie di natura diversa. La verifica delle informazioni sulla proprietà effettiva di aziende, per esempio, richiede di confrontare quanto emerge da fonti online con registri societari di fonte ufficiale.

Questo introduce un rischio di concentrazione: chi ha accesso alle fonti migliori e agli strumenti più affidabili costruisce un vantaggio informativo strutturale rispetto a chi ne è privo. La democratizzazione dell'OSINT resa possibile dall'AI porta con sé, paradossalmente, una nuova forma di asimmetria. Il tema si intreccia strettamente con quello della threat intelligence e disinformazione già affrontato sulle pagine di questa rivista.

L'elemento umano: insostituibile, non residuale

Di fronte all'accelerazione tecnologica, si genera spesso una retorica della sostituzione che merita di essere corretta con precisione. Nonostante i progressi tecnologici, il giudizio e l'esperienza umana continueranno a definire i processi OSINT di maggior successo. La migliore difesa contro l'attività criminale guidata dall'AI sarà la combinazione di automazione intelligente e investigatori qualificati, in grado di validare i risultati e garantire gli standard etici.

Il punto non è che gli analisti umani siano superiori ai sistemi AI nei *task* di elaborazione massiva: non lo sono, e fingere il contrario sarebbe controproducente. Il punto è che l'AI tende a ottimizzare per *pattern* già noti, mentre l'analista umano è capace di riconoscere l'anomalia che non ha precedenti, di costruire contestualizzazioni che richiedono comprensione culturale profonda, di prendere decisioni in condizioni di ambiguità radicale.

Affidarsi esclusivamente all'AI per la totalità di un'indagine è rischioso a causa delle tendenze alla distorsione e alle allucinazioni. L'esperienza umana rimane cruciale per l'analisi contestualizzata, la verifica e il processo decisionale etico. Bilanciare correttamente l'efficienza dell'AI con l'intuizione umana sarà la chiave del successo nel 2026 e negli anni a venire.

La metafora più utile non è quella della sostituzione ma quella dell'amplificazione: l'AI amplifica le capacità degli analisti preparati e amplifica i limiti di quelli non preparati. Investire nella formazione degli operatori diventa, in questo contesto, una priorità tanto strategica quanto l'investimento negli strumenti.

Verso l'OSINT *agentiva*: cosa ci aspetta

Il 2026 segna un punto di transizione, non un punto di arrivo. La traiettoria tecnologica indica chiaramente la direzione: sistemi OSINT sempre più autonomi, capaci di monitorare superfici informative in continuo, aggiornare modelli di rischio in tempo reale e produrre *intelligence* azionabile senza intervento umano nelle fasi di raccolta e prima elaborazione.

Strumenti come Taranis AI navigano attraverso diverse fonti di dati per raccogliere articoli non strutturati, utilizzano il *Natural Language Processing* e l'AI per migliorare la qualità del contenuto e supportano la condivisione collaborativa di *threat intelligence* tramite integrazione con MISP. Non si tratta di prototipi di laboratorio, ma di sistemi operativi *open source* che ridisegnano già oggi il flusso di lavoro degli analisti.

La dimensione etica e di *governance* non è accessoria a questa trasformazione, ne è parte costitutiva. La convergenza tra AI e OSINT solleva importanti preoccupazioni in termini di governo, implicazioni etiche, legali e sociali, con la necessità di supervisione crescente a fronte di strumenti di analisi sempre più avanzati che richiedono poca o nessuna supervisione continua. Domande come: chi è responsabile delle conclusioni prodotte da un sistema AI-OSINT? Come si gestisce il falso positivo che innesca un'azione operativa? Come si bilancia la capacità di raccolta con il rispetto della *privacy*

degli individui non coinvolti in attività illecite? Queste domande non hanno ancora risposte consolidate, ma richiedono risposte urgenti.

Conclusione: lucidità senza ingenuità

L’AI-OSINT non è una moda tecnologica né una promessa lontana. È una realtà operativa che sta già ridisegnando le pratiche di *intelligence*, sicurezza e investigazione in tutto il mondo. La sfida per i professionisti della sicurezza non è decidere se adottarla, ma come farlo con lucidità.

Lucidità significa riconoscere le capacità reali senza sovrastimarle: l’AI non elimina l’errore, lo sposta e lo trasforma. Significa comprendere che ogni strumento che rafforza il difensore sta, potenzialmente, rafforzando anche l’offensore: la simmetria dell’accesso è una caratteristica strutturale delle tecnologie generative. Significa anche tenere a mente che, come confermano sia Google GTIG che Microsoft, l’AI agisce oggi come acceleratore della *tradecraft* esistente e non come generatore di capacità radicalmente nuove: un dato che non va sottovalutato, ma nemmeno usato per abbassare la guardia.

Chi si occupa di sicurezza sa già che il vantaggio non si costruisce su un singolo strumento, ma sulla capacità di integrare strumenti, metodi e giudizio critico in un sistema coerente. L’AI è uno strumento potente. Usarlo bene è, ancora, una questione umana.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/ai-osint/

Parigi apre un’indagine penale a carico di Elon Musk e la sua X per deepfake e interferenze politiche

Su Elon Musk e X la procura di Parigi apre un’indagine penale, violato il DSA

La Francia alza il livello dello scontro con **Elon Musk** e trasforma l’inchiesta su ***X*** in un procedimento penale. **La procura di Parigi ha confermato l’apertura di un’indagine criminale** nei confronti del proprietario della piattaforma social, della ex amministratrice delegata **Linda Yaccarino** e delle società che controllano il social network e il sistema di intelligenza artificiale ***Grok*** (X.AI Holdings Corp, X Corp e xAI).

Questa mossa si basa sul **Digital Services Act** (DSA) UE, che X è accusata di violare per rischi sistemici su **disinformazione** e **intelligenza artificiale** (AI). Una svolta che segna un salto di qualità giuridico e politico: non più soltanto verifiche amministrative o accertamenti preliminari sulle attività della piattaforma, ma **un’indagine penale vera e propria**, affidata ai giudici istruttori e potenzialmente destinata a portare a incriminazioni formali.

Musk non si è presentato in

tribunale il 20 aprile, ora scatta l’indagine giudiziaria

La decisione arriva dopo il mancato rispetto di una convocazione ufficiale da parte di Musk e di Yaccarino. Entrambi erano stati chiamati a comparire il **20 aprile** davanti alle autorità francesi per un’audizione volontaria nell’ambito dell’inchiesta aperta nei mesi scorsi. Nessuno dei due si è presentato. Secondo quanto riferito dalla procura parigina, anche diversi dirigenti della società americana erano stati convocati senza però fornire collaborazione sufficiente agli investigatori.

È proprio questo passaggio a spiegare perché il fascicolo abbia assunto ora natura penale. In Francia, quando emergono indizi ritenuti sufficientemente gravi o quando le autorità ritengono che vi sia il **rischio di ostacoli all’accertamento dei fatti**, l’indagine può essere trasferita dal piano preliminare a quello giudiziario penale. Significa che i magistrati non si limitano più a raccogliere informazioni, ma possono contestare reati, emettere mandati, disporre sequestri, ordinare perquisizioni e chiedere misure coercitive.
La procura ha infatti annunciato di aver chiesto ai giudici istruttori di procedere formalmente contro X.AI Holdings Corp, X Corp, X AI, Musk e Yaccarino, anche attraverso strumenti equivalenti a un’incriminazione qualora continuasse la mancata collaborazione.

Diverse le accuse: manipolazioni algoritmiche per influenzare il dibattito politico, nudi deepfake,

disinformazione

Le accuse sono pesanti e riguardano il cuore del funzionamento della piattaforma. L'indagine nasce da una denuncia presentata all'inizio del 2025 dal deputato francese **Éric Bothorel** e si concentra su presunte **manipolazioni algoritmiche** operate da X per influenzare il dibattito politico francese. Secondo gli investigatori, la piattaforma avrebbe alterato la visibilità dei contenuti in modo da favorire determinate narrative politiche e **amplificare campagne di disinformazione**.

Ma non è questo l'unico fronte. Al centro dell'inchiesta vi sono anche le attività di *Grok*, il chatbot sviluppato dalla società xAI di Musk e integrato all'interno dell'ecosistema di X. Le autorità francesi sospettano che il sistema sia stato utilizzato per creare e diffondere contenuti illegali, tra cui negazioni dell'Olocausto e **immagini pornografiche deepfake** generate senza il consenso delle persone coinvolte.
In alcuni casi, secondo le accuse, sarebbero stati prodotti anche materiali assimilabili ad abusi sessuali su minori creati artificialmente attraverso l'intelligenza artificiale.

Musk sapeva e non ha fatto niente?

È questo il punto più delicato dell'intera vicenda. Non si tratta soltanto di responsabilità editoriale o moderazione insufficiente dei contenuti, ma della possibile contestazione di una **tolleranza consapevole verso la produzione e la diffusione di materiale criminale**.
Le procure europee stanno infatti iniziando a considerare **le piattaforme** non più come intermediari neutrali, ma come **soggetti che possono rispondere penalmente** se i loro strumenti tecnologici facilitano reati gravi o se non intervengono pur essendo a conoscenza dei rischi.

La Francia, in questo senso, sta tentando di costruire un precedente giuridico di grande portata. Il passaggio

all’indagine penale segnala che **le autorità ritengono di avere elementi sufficienti per ipotizzare responsabilità dirette da parte del management della società**. Una linea molto più aggressiva rispetto agli approcci tradizionali adottati finora nei confronti delle grandi piattaforme digitali.

Musk aveva già definito l’inchiesta “*un attacco politico*” dopo la perquisizione degli uffici parigini di X avvenuta nei mesi scorsi e il 7 maggio ha twittato di un assalto alla libertà di parola, annunciando ricorsi. xAI ha negato responsabilità, insistendo che Grok è un tool per utenti non un generatore illegale. Anche il **Dipartimento di Giustizia americano**, secondo indiscrezioni emerse ad aprile, avrebbe rifiutato di collaborare con le autorità francesi, accusando Parigi di interferire impropriamente con un’azienda statunitense.

Dalla Francia all’Italia, al resto d’Europa, l’indagine su X potrebbe aprire un’inchiesta sull’AI molto più ampia

La vicenda però va ben oltre il conflitto diplomatico tra Francia e Stati Uniti. **In Italia, l’Agcom vigila su X per analoghi rischi pre-elezioni**, mentre l’Unione europea potrebbe estendere le indagini su Meta AI, per il suo chatbot Llama integrato in WhatsApp/Instagram, sospettato di amplificare propaganda politica e deepfake non consensuali durante le elezioni europee.

L’indagine su X rappresenta uno dei primi casi in cui un grande ecosistema basato sull’intelligenza artificiale e sui social network viene affrontato sul piano del diritto penale per presunti **effetti sistemici sulla democrazia, sull’informazione e sulla sicurezza digitale.** E potrebbe diventare un precedente destinato a ridefinire le responsabilità delle piattaforme tecnologiche nell’era dell’AI

generativa.

Novità su Google, per aggiungere Key4Biz tra le tue fonti preferite, clicca qui

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/parigi-apre-unindagine-penale-a-carico-di-elon-musk-e-la-sua-x-per-deepfake-e-interferenze-politiche/572233/