Cimiteri digitali, il Garante privacy multa Aldilapp

Il **Garante per la privacy** ha sanzionato **Stup**, società che distribuisce **Aldilapp** in Italia, i comuni di Ancona e Velletri e i rispettivi gestori dei servizi cimiteriali.

L'app consente agli utenti – previa registrazione – di individuare il luogo di sepoltura dei defunti nei cimiteri aderenti al servizio e offre anche funzionalità di tipo "social" e commerciale.

Profili digitali dei defunti

Utilizzando il database comunale Aldilapp crea di default i *"profili digitali"* dei defunti, consentendo la pubblicazione di dediche e l'accensione di ceri virtuali visibili a tutti gli utenti, nonché la fruizione di servizi commerciali (es. fornitura di fiori, pulizia delle tombe).

Servizi istituzionali e servizi social e commerciali insieme

All'esito degli accertamenti, è emerso che l'utilizzo di un'unica piattaforma per offrire sia servizi istituzionali sia servizi di tipo *"social"* e commerciale – inscindibilmente connessi tra loro – presenta diverse criticità. Comporta infatti trattamenti di dati personali eccedenti rispetto alle sole finalità istituzionali e può creare negli utenti la legittima aspettativa che tutti i trattamenti siano riconducibili ai Comuni.

Ulteriori criticità riguardano la regolamentazione dei

rapporti tra i soggetti coinvolti, la scarsa trasparenza nei confronti degli utenti, nonché l'inadeguatezza di alcune misure tecniche e organizzative.

Il Garante ha quindi disposto il rafforzamento delle misure di sicurezza, la netta separazione tra servizi istituzionali e quelli di natura *"social"* e commerciale, nonché la cancellazione dei *"profili digitali"* creati automaticamente dai database comunali e delle interazioni ad essi associate.

database dei Comuni esclusi

Tali servizi potranno essere erogati da Stup su richiesta degli utenti e senza utilizzare i database cimiteriali messi a disposizione dai Comuni esclusivamente per l'erogazione del servizio di informazione sull'ubicazione dei defunti nei propri cimiteri.

Tenuto conto della natura innovativa del servizio, dell'assenza di reclami e della collaborazione fornita nel corso dell'istruttoria, l'Autorità ha irrogato sanzioni amministrative di importo contenuto: 6mila euro a Stup; 3mila euro al Comune di Ancona, 2mila euro al Comune di Velletri e 2.500 euro ai gestori cimiteriali.

Leggi le altre notizie sull'home page di Key4biz

https://www.key4biz.it/cimiteri-digitali-il-garante-privacy-multa-aldilapp/567700/

Guerra in Iran, quali

conseguenze per il Tech europeo?

Il conflitto che coinvolge Iran, Stati Uniti e Israele, caratterizzato da attacchi aerei ad alta intensità, guerra con droni e operazioni informatiche, ha implicazioni significative e multiformi per il settore della tecnologia digitale dell'Unione Europea (UE). Sulla base dei report di inizio marzo 2026, realizzati dalla società di analisi IDC, gli impatti principali si concentrano sull'inflazione legata all'energia, sulle interruzioni della catena di approvvigionamento, sull'aumento dei rischi per la sicurezza informatica e su un potenziale rallentamento della spesa IT.

1. Inflazione e costi operativi legati all'energia

• **Costi dei data center**: poiché il conflitto interrompe la produzione di energia nella regione, l'aumento dei prezzi del petrolio e del gas in Europa (già del 40-50% in più a causa degli shock dell'offerta) sta gonfiando i costi operativi per i data center e i fornitori di servizi cloud.

• **Pressioni sulla produzione:** l'aumento dei costi energetici sta influenzando la fabbricazione di semiconduttori e la produzione di componenti IT, minacciando di aggravare le carenze esistenti.

2. Interruzioni della catena di

approvvigionamento e limitazioni hardware

• **Rischi nello Stretto di Hormuz:** l'interruzione delle rotte di navigazione nello Stretto di Hormuz sta causando ritardi nella consegna dei componenti, con ripercussioni sulla catena di approvvigionamento per la tecnologia di consumo e l'hardware aziendale.

• **Carenza di componenti:** il mercato globale delle memorie (DRAM/NAND) sta subendo una pressione crescente, con un potenziale aumento dei prezzi dello storage aziendale e delle infrastrutture di intelligenza artificiale.

• **Costi logistici:** i costi di assicurazione e trasporto per i prodotti tecnologici sono in aumento, il che potrebbe rallentare l'implementazione di nuove infrastrutture digitali.

3. Accelerazione delle minacce alla sicurezza informatica e aumento dei budget

• **Aumento dei rischi informatici:** le organizzazioni dell'UE devono far fronte a crescenti minacce da parte di gruppi di hacker affiliati all'Iran, che potrebbero prendere di mira infrastrutture critiche, inclusi, potenzialmente, data center e fornitori di servizi IT, come misure di ritorsione.

• **Riallocazione del bilancio:** in un contesto di rischi più elevati, si prevede che le aziende dell'UE accelereranno la spesa per la sicurezza, in particolare per il rilevamento e la risposta gestiti (MDR), la modernizzazione dei centri operativi di sicurezza (SOC) e le architetture zero-trust.

• **Vulnerabilità dei data center:** il conflitto ha evidenziato la vulnerabilità fisica dei data center all'instabilità

regionale, rendendo necessaria una rivalutazione delle strategie di backup multiregionale.

4. Rallentamento della spesa IT e rivalutazione strategica

• **Investimenti ritardati:** si prevede che la combinazione di incertezza economica, prezzi elevati dell'energia e pressioni inflazionistiche porterà a ritardi nei progetti IT e, in alcuni casi, a una riduzione della spesa tecnologica discrezionale.

• **Dare priorità ad AI/Cloud:** sebbene la crescita complessiva della spesa IT possa rallentare, è probabile che gli investimenti strategici nelle infrastrutture di AI e nella migrazione al cloud persistano, anche se forse con una rivalutazione delle sequenze di progetto in caso di aumento dei costi dell'hardware.

• **Focus sulla sovranità digitale:** il conflitto rafforza la spinta dell'UE verso la *"sovranità tecnologica",* rafforzando le capacità e riducendo la dipendenza da attori stranieri per le infrastrutture digitali critiche.

5. Impatto sul personale e sulle operazioni tecnologiche

• **Cambiamenti operativi:** le principali aziende tecnologiche si stanno affrettando a proteggere dipendenti e strutture nella più ampia regione del Medio Oriente, con alcune che stanno implementando protocolli di emergenza, che potrebbero avere un impatto indiretto sulle operazioni da remoto delle aziende europee collegate alla regione.

• **Attacchi alle infrastrutture digitali:** il potenziale, o l'effettivo, attacco ai data center, come si è visto con le

reti iraniane, indica una nuova fase di guerra digitale che potrebbe compromettere la continuità dei servizi per le piattaforme globali utilizzate all'interno dell'UE.

Leggi le altre notizie sull'home page di Key4biz

https://www.key4biz.it/guerra-in-iran-quali-conseguenze-per-il-tech-europeo/567684/

Data Center, l'UE prepara norme green più severe per quelli vecchi

Un nuovo pacchetto di sovranità digitale dell'UE richiede prestazioni più elevate in termini di risparmi energetici e consumi green per i data center esistenti più datati.

L'UE prevede norme più severe per l'ammodernamento dei data center obsoleti in tutta l'Unione.

Requisiti più rigorosi per i data center obsoleti

La Commissione europea sta preparando un pacchetto di requisiti più rigorosi per i data center obsoleti, perché non vuole consentire alle infrastrutture legacy di operare con norme più flessibili.

Una bozza di strategia legata al pacchetto di sovranità

tecnologica dell’UE visionata da *Euractiv* segnala che i siti più datati dovranno affrontare aspettative di efficienza più elevate e controlli di sostenibilità più rigorosi, nell’ambito di uno sforzo per modernizzare la spina dorsale digitale dell’UE in linea con il green deal.

Standard minimi di prestazione entro il 2030

La proposta definisce standard minimi di prestazione per i nuovi data center entro il 2030, con l’obiettivo di allineare l’intero settore agli obiettivi climatici e di resilienza dell’Unione. I funzionari vogliono ridurre gli sprechi energetici e migliorare il monitoraggio nelle strutture che operano da tempo senza parametri di riferimento uniformi.

In arrivo nuovi obblighi per i Cloud Provider

La bozza indica un ruolo più ampio per il Cloud and AI Development Act, che dovrebbe definire i futuri obblighi per i fornitori di servizi cloud, anziché basarsi su misure nazionali frammentate.

Bruxelles ritiene che norme coerenti e standard a livello continentale siano essenziali per supportare servizi cloud sicuri, infrastrutture di intelligenza artificiale e operazioni digitali transfrontaliere.

La strategia sottolinea che la modernizzazione è fondamentale per la visione dell’UE di sovranità tecnologica. I centri più datati necessiterebbero di aggiornamenti per mantenere la conformità, garantendo che l’infrastruttura digitale europea rimanga competitiva, efficiente e meno dipendente da fornitori esterni.

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/data-center-lue-prepara-norme-green-piu-severe-per-quelli-vecchi/567508/

Euro digitale, progetto pilota nel 2027. Al via la selezione per i fornitori di servizi di pagamento. Domande fino al 14 maggio

La Banca centrale europea apre la call per i fornitori di servizi di pagamento. Un altro passo in avanti verso il progetto pilota dell’euro digitale

La Banca centrale europea (Bce) compie un nuovo passo verso l’introduzione dell’**euro digitale**. Pubblicata la “*call for expression of interest*”, **l’invito a presentare manifestazioni di interesse** rivolto ai fornitori autorizzati di servizi di pagamento (*Payment Service Providers*, o PSP) interessati a partecipare a un **progetto pilota che si svolgerà nel 2027**.

L’iniziativa arriva dopo la decisione del Consiglio direttivo della Bce di passare alla fase successiva del progetto

sull’euro digitale. Parallelamente alla call, sono state rese disponibili informazioni tecniche, operative e procedurali per consentire agli operatori del settore di valutare concretamente la partecipazione.

Si parte nella seconda metà del 2027 e durerà 12 mesi

Il progetto pilota avrà una durata di **12 mesi e partirà nella seconda metà del 2027**. L’obiettivo è testare, in un ambiente controllato, il funzionamento delle principali caratteristiche del futuro euro digitale: dall’infrastruttura tecnica ai processi operativi, fino all’esperienza d’uso per cittadini e commercianti.

La valuta utilizzata nella sperimentazione sarà una **versione beta dell'euro digitale**, creata esclusivamente per finalità di test e **priva di valore legale**.

La sperimentazione, si legge nel comunicato che accompagna la call, coinvolgerà il personale delle banche centrali dell'Eurosistema e alcuni commercianti che operano all'interno delle sedi della Bce e delle banche centrali nazionali dell'area euro, come bar, mense e ristoranti. Saranno inoltre inclusi anche **operatori di e-commerce**.

I partecipanti potranno effettuare diverse tipologie di pagamento: **tra persone (peer-to-peer), online e offline**, e **tra persone e imprese**, sia nei punti vendita fisici sia negli acquisti online e tramite dispositivi mobili.

Il ruolo dei PSP

Per banche, istituti di pagamento e altri fornitori di servizi finanziari, spiegano da Francoforte, la partecipazione rappresenta l'occasione di **contribuire direttamente allo sviluppo dell'ecosistema dell'euro digitale**.

Secondo quanto comunicato dalla Bce, i PSP selezionati avranno il compito di fornire i servizi di pagamento durante la sperimentazione, gestendo **l'onboarding dei partecipanti al pilot – consumatori e commercianti – e supportando i test delle funzionalità chiave** della nuova infrastruttura.

Il confronto diretto con i team tecnici dell'Eurosistema permetterà inoltre di raccogliere feedback utili per affinare le specifiche tecniche del progetto. La partecipazione, precisa la BCE, **non sarà remunerata**.

Come partecipare

Le candidature saranno valutate dalla Banca centrale europea sulla base di diversi criteri: **conformità regolamentare,**

capacità tecniche e operative, presenza sul mercato e track record nella realizzazione di servizi di pagamento. L’obiettivo è selezionare un gruppo di operatori che rappresenti in modo equilibrato il mercato dell’area euro per dimensioni, copertura geografica e diffusione commerciale.

Per supportare gli operatori interessati, la Bce ha pubblicato una sezione di **domande frequenti (FAQ)** e organizzerà un **focus session online il 20 marzo 2026**, dedicata al confronto con i potenziali partecipanti.

Le manifestazioni di interesse dovranno essere inviate entro **il 14 maggio 2026** all’indirizzo email dedicato della BCE.

Il percorso verso l’euro digitale

Il progetto pilota rappresenta un tassello della più ampia strategia europea per sviluppare una **moneta digitale pubblica complementare al contante**, pensata per garantire autonomia strategica nei pagamenti e rafforzare la competitività dell’ecosistema finanziario europeo.

La decisione finale sull’emissione dell’euro digitale, tuttavia, **dipenderà dall’approvazione della normativa europea attualmente in discussione**. Fino ad allora, l’Eurosistema continuerà a prepararsi con un approccio flessibile, in coordinamento con il processo legislativo dell’Unione.

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/euro-digitale-progetto-pilota-nel-2027-al-via-la-selezione-per-i-fornitori-di-servizi-di-pagamento-domande-fino-al-14-maggio/567486/

L’analisi di ASviS. Un algoritmo può identificare le malattie rare?

“*Nel 2016 è nato mio figlio Vincent. Poche settimane dopo ha iniziato ad avere sintomi di sudorazione, tremori, pallore e cianosi alle labbra e alle mani, e aveva un pannolino che perdeva terribilmente, cosa che la sua pediatra continuava a dire essere normale (…) Un team di 15 medici è venuto a trovarci e ci ha spiegato che mio figlio aveva una malattia genetica chiamata Pompe e che esisteva un solo farmaco approvato*”. Un calvario ospedaliero, l’ansia di un genitore, la diagnosi di una malattia rara. Il piccolo Vincent è una delle **300 milioni di persone nel mondo** che affrontano una malattia rara: un insieme eterogeneo di patologie, per lo più ereditarie, ciascuna delle quali colpisce **non più di cinque persone su diecimila**. In occasione del Rare disease day del 28 febbraio, che quest’anno ha messo al centro il tema dell’equità, le storie di questi pazienti sono state presentate sul sito ufficiale della campagna, insieme a eventi, appelli e dibattiti.

In parallelo, il World economic forum (Wef) ha diffuso un rapporto che spiega come dare nuovo impulso alla ricerca e alla cura, migliorare il coordinamento tra i sistemi sanitari e lavorare in modo più efficace su raccolta e condivisione dei dati. Ad oggi, ricorda il Wef, la stragrande maggioranza delle malattie rare **non ha ancora una terapia approvata** ufficialmente dalle principali autorità del farmaco. D’altra parte, sottolinea il Rapporto, la ricerca su queste patologie è stata uno dei più potenti motori di innovazione della sanità globale. Molte delle tecnologie oggi centrali

nella **medicina di precisione**, dalla genomica all'mRNA, sono state sperimentate proprio in quest'ambito prima di diffondersi su larga scala. Le malattie rare hanno spinto nuovi modelli produttivi e approcci più flessibili agli studi clinici.

Non bisogna però abbassare la guardia. Il Wef identifica **cinque direttrici fondamentali** per dare nuovo impulso al progresso scientifico. La priorità principale riguarda la **raccolta dei dati di base**. Molti Paesi non dispongono delle informazioni minime e standardizzate sulle malattie rare. Per questo il Rapporto propone di definire un set essenziale di indicatori comuni, da monitorare in modo sistematico a livello internazionale.

Viviamo più a lungo, conviviamo con più malattie: come sta cambiando la salute

Tumori in calo, infarti meno letali, demenze in crescita per l'invecchiamento. Pesano le disuguaglianze sanitarie. Dalla diagnosi precoce dell'Alzheimer alle strategie anticancro, ecco le nuove frontiere della ricerca.

Un secondo asse è il **maggiore coinvolgimento dei pazienti**. Le loro esperienze (qualità della vita, tempi diagnostici, impatto sulle famiglie) sono spesso sottorappresentate nei sistemi informativi. Integrare in modo strutturato i dati riportati dai pazienti significa rendere le politiche più aderenti alla realtà.

Terzo nodo cruciale è la **diagnosi**: milioni di persone restano senza informazioni specifiche sulla loro condizione. Rafforzare lo screening neonatale e ampliare la capacità diagnostica, anche attraverso la genetica, è considerato un passaggio decisivo per intervenire prima e meglio.

Il quarto elemento è la **condivisione dei dati**. Oggi molte informazioni restano frammentate in silos nazionali o

istituzionali. Rendere interoperabili i sistemi sanitari e favorire uno scambio sicuro e affidabile delle informazioni può accelerare la lotta alle malattie rare.

Infine, serve una **migliore capacità di analisi**. I dati su queste patologie sono spesso complessi e dispersi. Strumenti digitali avanzati e intelligenza artificiale possono aiutare a individuare pattern nascosti e guidare lo sviluppo di nuove terapie.

Tra i progetti più innovativi citati dal World economic forum c'è **Oscar**, un algoritmo di intelligenza artificiale sviluppato dall'azienda biofarmaceutica Sanofi nell'ambito del Project Saturn. Si tratta di un modello multimodale per **analizzare dati clinici, genetici e di laboratorio** senza spostarli dai sistemi sanitari in cui sono conservati, superando così i limiti dei tradizionali database centralizzati e garantendo al tempo stesso la tutela della privacy.

Nelle prime sperimentazioni l'algoritmo ha già dimostrato di poter migliorare in modo significativo la capacità di individuare precocemente alcune patologie, aumentando di **oltre 18 volte l'efficienza nel rilevamento del diabete di tipo 1** e correggendo numerosi errori diagnostici. Ora la stessa architettura viene adattata alle malattie rare, a partire da quelle di Pompe e Fabry: l'obiettivo è ridurre drasticamente i tempi di diagnosi grazie all'identificazione di segnali precoci.

Il modello si basa su un sistema di "**apprendimento federato**": i dati restano nei singoli ospedali o istituti di ricerca, ma l'intelligenza artificiale può comunque analizzarli in modo distribuito. Questo consente di coinvolgere sistemi sanitari diversi, anche in Paesi con risorse limitate, e di costruire entro il 2030 (è la speranza) una rete globale capace di migliorare diagnosi e presa in carico.

Accanto all'innovazione tecnologica, il Project Saturn punta

anche su nuovi modelli di assistenza che **integrano strumenti digitali e supporto umano**, aiutando pazienti e famiglie a gestire le cure in modo più continuo e collaborativo. Lo scopo è creare un ecosistema in cui dati, intelligenza artificiale e reti di cura lavorino insieme per rendere più tempestiva ed efficace la risposta alle malattie rare.

Nel complesso, la tesi del Wef è che dati più solidi e meglio utilizzati siano la leva strategica per trasformare l'ecosistema delle malattie rare, abbassando i costi sanitari e rafforzando la produttività economica.

Scarica il Rapporto

Leggi le altre notizie sull'home page di Key4biz

https://www.key4biz.it/lanalisi-di-asvis-un-algoritmo-puo-identificare-le-malattie-rare/567463/

Nel mondo ci sono 12.241 testate nucleari

Truenumbers *è l'appuntamento settimanale con la rubrica curata dal portale www.truenumbers.it, il più importante sito editoriale di Data Journalism in Italia, fondato da* ***Marco Cobianchi****. Una rubrica utile per saperne di più, per approfondire, per soddisfare ogni curiosità, ma sempre con la precisione che solo i numeri sanno dare. Per leggere tutti gli articoli della rubrica Truenumbers su* ***Key4biz*** *clicca qui.*

Oltre 2.000 pronte al lancio immediato, la mappa dei Paesi con la bomba atomica

Il 28 febbraio 2026, nelle ore che hanno preceduto l’alba, il Medio Oriente è stato lo scenario della più grande concentrazione di potenza di fuoco statunitense degli ultimi trent’anni.
Sotto il nome in codice “Operation Epic Fury”, una coalizione guidata dagli Stati Uniti e Israele ha dispiegato 200 aerei da guerra per distruggere le infrastrutture nucleari iraniane. L’obiettivo primario è stato Natanz, il più vasto complesso di arricchimento dell’uranio della Repubblica Islamica, già parzialmente colpito nel giugno 2025.

Emmanuel Macron, il nuovo piano nucleare della Francia

Il riverbero di “Epic Fury” ha raggiunto l’Europa 48 ore dopo. Il 2 marzo 2026, dalla base sottomarina di Île Longue, il presidente francese Emmanuel Macron ha rotto un tabù decennale con un annuncio che segna la fine dell’era della trasparenza atomica europea. “Ho ordinato di aumentare il numero di testate nucleari del nostro arsenale. Non comunicheremo più le cifre relative alla nostra deterrenza”. È un cambio di paradigma assoluto. La Francia, unica potenza nucleare dell’Unione europea insieme al Regno Unito, sceglie l’opacità strategica come pilastro della propria sovranità. “Per essere

liberi bisogna essere temuti, e per essere temuti bisogna essere potenti", ha concluso Macron, riportando l'orologio della geopolitica continentale ai toni aspri della Guerra Fredda.

L'arsenale nucleare francese e i sottomarini sempre in pattugliamento

La forza di dissuasione nucleare francese (*force de frappe,* ossia forza di dissuasione) aveva raggiunto il suo apice negli anni Novanta con circa **540 testate nucleari**. Nei decenni successivi, in linea con i trattati internazionali e con la dottrina della "stretta sufficienza", l'arsenale era sceso progressivamente a 290 testate nucliari, secondo le ultime cifre pubblicate dal *Stockholm International Peace Research Institute* (SIPRI). Con l'annuncio di Macron, quella tendenza al ribasso è ufficialmente finita per la prima volta in oltre trent'anni.

La force de frappe si articola su due componenti principali. La componente sottomarina è affidata ai quattro sottomarini nucleari lanciamissili balistici della classe Triomphant, basati a Île Longue, che garantiscono il cosiddetto "second strike": dal 1972, almeno uno dei quattro è sempre in pattugliamento sottomarino, pronto a rispondere anche se la Francia venisse colpita per prima. È la garanzia della deterrenza. Cosa vuol dire? È il principio secondo cui la minaccia di una ritorsione nucleare è così certa, immediata e devastante da rendere qualsiasi attacco contro lo Stato (o i suoi interessi vitali) un "atto suicidia". Macron ha tradotto questa garanzia in un dato di scala brutale: "Uno solo dei nostri sottomarini in pattugliamento trasporta una potenza di fuoco equivalente alla somma di tutte le bombe cadute in Europa durante la Seconda Guerra Mondiale".

Che cos’è l’ombrello nucleare europeo

La vera novità, tuttavia, non è solo l’aumento delle testate, è la proposta di un **ombrello nucleare europeo**. Macron ha annunciato una collaborazione con otto Paesi europei per una “deterrenza nucleare avanzata”. Germania, Gran Bretagna, Polonia, Paesi Bassi, Belgio, Grecia, Svezia e Danimarca. Questi Paesi potranno ospitare “forze aeree strategiche” dell’aeronautica francese, consentendo loro di “distribuirsi sul continente europeo”. L’obiettivo è creare quello che Macron ha descritto come “un arcipelago di forze”.

Ma quali sono i numeri reali dietro questa escalation? Quali paesi possiedono oggi la bomba atomica, quante testate sono effettivamente operative nel mondo?

Cosa vuol dire “deterrenza nucleare”?

Cosa vuol dire deterrenza in ambito nucleare? La deterrenza è una strategia militare fondata su un principio di matematica del terrore: io non attacco te perché so che tu mi puoi distruggere, e viceversa. In pratica, un Paese possiede armi nucleari non per usarle per primo, ma per convincere i propri avversari che un eventuale attacco sarebbe così costoso da non valere la pena. È la logica della “distruzione mutua assicurata”. Yota con l’acronimo inglese MAD (*Mutually Assured Destruction*): se tu mi attacchi con il nucleare, io ti rispondo con il nucleare, e tutti e due perdiamo tutto.

La deterrenza funziona finché è credibile, finché l’avversario crede davvero che tu sia disposto a premere il bottone. È per questo che i Paesi con arsenali nucleari comunicano strategicamente le dimensioni dei loro arsenali. Mostrare troppo può provocare; mostrare troppo poco può invitare

all’aggressione. La scelta di Macron di non rendere più pubblici i dati sull’arsenale francese è la versione più estrema di questa logica: si chiama ambiguità strategica, e consiste nel lasciare che il nemico non sappia con precisione quante armi tu abbia. L’incertezza stessa diventa un deterrente. Non a caso, il discorso di Macron segna la prima variazione dottrinale francese in materia di trasparenza nucleare da oltre quarant’anni.

Quante bombe atomiche ci sono nel mondo

Il punto di partenza per rispondere alla domanda “quante bombe atomiche ci sono nel mondo” è il *SIPRI Yearbook 2025*, l’annuario dello *Stockholm International Peace Research Institute*. La risposta è 12.241 armi nucleari, distribuite tra nove stati.

Armi nucleari pronte all’uso: sono 2.100 quelle in stato di “elevata prontezza”

Ma il numero totale racconta solo una parte della storia. Il dato davvero rilevante per misurare il rischio è quello delle armi pronte all’uso: 9.614 testate sono considerate potenzialmente impiegabili, 3.912 sono già dispiegate su missili o basi operative, e circa 2.100 si trovano in stato di elevata prontezza, possono essere lanciate nel giro di pochi minuti, senza alcun ulteriore ordine di preparazione. Pensate a questi 2.100 ordigni come motori sempre accesi.

Il numero totale di testate nucleari nel mondo continua tecnicamente a diminuire, ma questo dato è ingannevole: la riduzione è dovuta allo smantellamento di vecchie testate dismesse durante il disgelo post-Guerra Fredda, un processo

che si sta però rallentando fino a quasi fermarsi. Il ritmo a cui vengono smantellate le testate obsolete sta diventando più lento del ritmo a cui nuove testate vengono aggiunte alle scorte globali: il saldo netto, per la prima volta in decenni, rischia di tornare positivo. Ovvero, il mondo potrebbe presto avere più bombe di quante ne abbia oggi.

La classifica dei paesi con armi nucleari

La Russia guida con 5.459 testate totali, di cui 1.718 già dispiegate. Gli Stati Uniti seguono con 5.177 testate (1.770 dispiegate). Insieme, le due superpotenze controllano quasi il 90% di tutte le armi nucleari del pianeta. Al terzo posto si colloca la Cina con 600 testate, un numero cresciuto di 100 unità nell'ultimo anno. Seguono Francia con 290, Regno Unito con 225, India con 180, Pakistan con 170, Israele con 90 (stimati) e Corea del Nord con 50 (stimati).

Armamenti nucleari della Russia: 5.459 in totale

La Russia possiede il maggior numero di testate nucleari al mondo: 5.459 in totale secondo SIPRI. L'arsenale russo è il diretto erede di quello sovietico, che negli anni Ottanta contava oltre 40.000 testate, e da allora è stato ridotto in modo sostanziale, ma il processo di riduzione ora si è fermato. Quello che avanza è invece la modernizzazione. Mosca sta sviluppando nuovi missili balistici intercontinentali (tra cui il Sarmat, in grado di trasportare 10-15 testate indipendenti), nuovi sottomarini classe Borei e sistemi ipersonici come il missile Avangard e il Kinzhal.

La strategia nucleare di Putin

Ma il dato più preoccupante non riguarda i numeri: riguarda la dottrina nucleare. Nel novembre 2024, Putin ha aggiornato ufficialmente il documento che definisce le condizioni in cui la Russia potrebbe ricorrere all'arma atomica. Il nuovo testo ha abbassato la soglia d'uso, ampliando la gamma di circostanze che potrebbero giustificare un attacco nucleare. In parallelo, a novembre 2024, la Russia ha effettuato il collaudo del nuovo missile Oreshnik. Un balistico a raggio intermedio con testate multiple indipendenti, in un attacco reale contro Dnipro, in Ucraina. Non trasportava testate nucleari, ma il messaggio era cristallino: quella tecnologia esiste, è operativa ed è stata testata in condizioni di guerra reale per la prima volta dal 1945.

L'annuario 2025 di Truenumbers

Tutti i dati che hanno segnato l'anno in un unico volume di 200 pagine. Grafici, analisi e zero opinioni. Solo fatti supportati da dati ufficiali.Scopri i contenuti

Quante bombe nucleari ha la Cina: 600 nel 2025

Se Russia e Stati Uniti dominano la scena con oltre 5.000 testate ciascuno, la vera trasformazione del panorama nucleare globale degli ultimi anni è la crescita dell'arsenale cinese. SIPRI stima che la Cina abbia raggiunto le 600 testate nel 2025, rispetto alle 500 dell'anno precedente. Il tasso di espansione è tra i più rapidi al mondo. Nell'arco di pochi anni, Pechino ha più che raddoppiato il proprio arsenale.

La Cina sta costruendo centinaia di nuovi silos per missili balistici intercontinentali nel deserto dello Xinjiang e del Gansu, visibili nelle immagini satellitari già dal 2021. Sta sviluppando sottomarini nucleari di nuova generazione e

missili a testata multipla. Fino alla metà degli anni 2000, la tecnologia MIRV (veicoli di rientro multipli indipendenti, che permettono a un singolo missile di colpire obiettivi diversi con testate separate) era appannaggio esclusivo di Francia, Russia, Regno Unito e Stati Uniti. Oggi la Cina ha sviluppato almeno due missili con questa capacità, e altri stati ci stanno lavorando.

Questo sviluppo pone gli Stati Uniti di fronte a un problema strategico senza precedenti: per la prima volta nella storia, Washington deve configurare la propria deterrenza nucleare contro due rivali nucleari di primo piano contemporaneamente. È una delle ragioni per cui il dibattito sul rinnovo del trattato *New START* (l'accordo russo-americano sulla riduzione delle armi strategiche che è scaduto nel 2026) è in stallo. Il rischio concreto, avvertono gli esperti del SIPRI, è un accumulo incontrollato di armi nucleari senza più alcun quadro negoziale di riferimento, scenario che non si vedeva dai tempi peggiori della Guerra Fredda.

L'arsenale nucleare di Israele è segreto

Israele è l'unico Paese al mondo che pratica una politica di opacità nucleare totale: non conferma né smentisce di possedere armi nucleari. Non ha mai firmato il Trattato di Non-Proliferazione Nucleare (NPT). Non partecipa alle conferenze internazionali sul disarmo come stato dotato di capacità atomiche. Eppure il SIPRI stima che Israele possegga circa 90 testate nucleari, tutte in giacenza, nessuna formalmente "dispiegata" secondo la classificazione internazionale.

La dottrina militare israeliana legata al nucleare è nota come "Opzione Sansone". Il principio per cui Israele, se messa di fronte a una minaccia, sarebbe disposta a usare l'arma atomica come ultima ratio, anche in assenza di una risposta simmetrica

da parte dell’avversario. È la forma più estrema di deterrenza, quella di chi dice: “se mi distruggi, io ti distruggo”.

La bombe atomiche non ufficiali

Oltre alle cinque potenze nucleari “ufficiali” riconosciute dal Trattato di Non-Proliferazione (NPT) (Stati Uniti, Russia, Cina, Francia e Regno Unito) esistono altri quattro paesi che possiedono armi nucleari al di fuori di questo quadro giuridico.

Quante bombe atomiche ha l’India

L’**India** ha condotto il suo primo test nucleare nel 1974 (“Pokhran-I”) e un secondo ciclo di test nel 1998. Possiede circa **180 testate** e sta sviluppando missili balistici intercontinentali e sottomarini nucleari. La situazione si complica per le tensioni simultanee su due fronti: verso il Pakistan e, sempre più, verso la Cina.

Quante bombe atomiche ha il Pakistan

Il **Pakistan** ha risposto ai test indiani del 1998 con i propri test nucleari, diventando il primo paese islamico a dotarsi di capacità atomiche. Possiede circa **170 testate** e sta sviluppando missili a duplice capacità convenzionale/nucleare. La prossimità geografica con l’India, la presenza di gruppi radicali sul territorio e la relativa instabilità politica del governo rendono questo arsenale uno dei più preoccupanti dal punto di vista del rischio di proliferazione.

Quante bombe atomiche ha la Corea del Nord

La **Corea del Nord** ha condotto il suo primo test nucleare nel 2006 e da allora ne ha effettuati altri cinque. Il SIPRI stima circa **50 testate.** Ma il numero reale è incerto data l'opacità assoluta del regime. Pyongyang produce missili balistici intercontinentali, testati più volte, con traiettorie potenzialmente in grado di raggiungere il territorio continentale americano.

Fonte: *International Institute for Strategic Studies – SIPRI Yearbook 2025*
I dati sono aggiornati al 2026

Leggi le altre notizie sull'home page di Key4biz

https://www.key4biz.it/nel-mondo-ci-sono-12-241-testate-nucleari/567384/

Instagram avviserà i genitori se i figli cercano contenuti su suicidio e autolesionismo. Come funziona

Meta corre ai ripari (mentre è sul

banco degli imputati negli USA): se un minore ricerca contenuti pericolosi su Instagram scatta l’avviso ai genitori

A fine gennaio, presso la Corte Superiore di Los Angeles, ha preso il via un processo storico portato avanti dal **Social Media Victims Law Center**, in rappresentanza di 1.600 querelanti, 350 famiglie e 250 distretti scolastici, contro alcune delle più grandi e popolari piattaforme social al mondo, come Meta, Snap, TikTok e YouTube.

L’accusa alle Big Tech è progettare intenzionalmente servizi online per **creare dipendenza**. Una volta che i **minori**, ragazzini e adolescenti in particolare, entrano su queste piattaforme, sostengono le associazioni di genitori, cadono preda di **depressione**, **disturbi alimentari**, **autolesionismo** e altri problemi di **salute mentale**, fino, in alcuni tragici casi, al **suicidio**.

Proteggere i minori dai rischi dei social network è diventata una priorità politica in mezzo mondo. L’Australia ha vietato l’accesso ai social agli under 16. In Francia è in discussione un divieto sotto i 15 anni. In Italia sono state depositate proposte simili. Nel frattempo, le piattaforme provano a correre ai ripari con nuove misure di tutela.

La vera novità in questo momento arriva proprio da Meta, che è tra i principali attori sul banco degli imputati. **Instagram** introdurrà un sistema di **notifiche ai genitori:** quando un adolescente cerca ripetutamente termini legati a **suicidio o autolesionismo** scatta l’*alert*. È la prima volta che una piattaforma sociale decide di avvisare in modo proattivo le famiglie e non solo di bloccare i contenuti o mostrare numeri utili di supporto.

Ma come funziona davvero questo sistema? E quali sono i rischi?

Come funziona il servizio di allerta per le famiglie

La novità riguarda gli account inseriti nel programma **“Teen Accounts”**, cioè i profili per adolescenti con strumenti di supervisione attivati dai genitori.

Il meccanismo è questo:

- Instagram analizza i **modelli di ricerca** degli utenti;
- se un adolescente effettua **ricerche ripetute in un breve**

lasso di tempo su termini collegati a suicidio o autolesionismo, scatta un alert;
- la notifica non parte al primo tentativo, ma solo dopo ricerche reiterate: una scelta che, secondo Meta, serve a evitare eccessi di controllo e a “bilanciare tutela e autonomia”;

L’avviso viene inviato ai genitori attraverso email, SMS, WhatsApp e una notifica diretta nell’app. Insomma, tutti i canali possibili per rendere l’allerta efficace e tempestiva (perché non una telefonata?)

Aprendo il messaggio, il genitore accede a una sezione dedicata con **linee guida e risorse elaborate con esperti**, per affrontare in modo corretto una possibile situazione di disagio.

Meta ha dichiarato che il sistema, però, potrebbe anche sbagliare “per eccesso di cautela”, cioè significa che potranno arrivare notifiche anche in assenza di un reale pericolo. L’obiettivo dichiarato è intercettare segnali di sofferenza prima che sia troppo tardi. Prevenire è meglio che curare.

Dove è attivo il servizio e quando arriverà in Italia

La funzione entrerà in vigore **a partire dalla prossima settimana** per gli utenti iscritti ai Teen Accounts negli Stati Uniti, nel Regno Unito, in Australia e Canada.

Meta ha annunciato che l’estensione al resto del mondo avverrà **entro l’anno**, includendo anche l’**Italia**.

Dunque, salvo cambiamenti, il sistema di alert dovrebbe arrivare anche nel nostro Paese nei prossimi mesi.

A chi si rivolge

Il sistema è rivolto esclusivamente:

- agli **adolescenti con account supervisionato;**
- ai **genitori che hanno attivato gli strumenti di controllo.**

Non si tratta quindi di un monitoraggio generalizzato, ma di una funzione legata alla scelta della famiglia di aderire al sistema di supervisione.

Nei prossimi mesi, Meta prevede di estendere un meccanismo simile anche alle conversazioni con **Meta AI**, il chatbot dell’azienda: se un adolescente tenterà di avviare **dialoghi legati a suicidio o autolesionismo**, i genitori potrebbero ricevere un alert analogo.

Le piattaforme stanno facendo abbastanza?

Il dibattito internazionale mostra una tendenza chiara: i governi stanno valutando restrizioni drastiche, come il divieto di accesso sotto una certa età. Le piattaforme, dal canto loro, stanno introducendo strumenti di controllo parentale sempre più sofisticati.

Ma la questione di fondo rimane: la sicurezza dei minori può essere affidata solo ai genitori e a notifiche automatiche?

Molti esperti sostengono che serva un cambio di paradigma, si deve andare nella direzione di piattaforme progettate **“by**

design” per essere sicure per i più giovani, con algoritmi che non spingano verso contenuti estremi e con sistemi di verifica dell’età realmente efficaci.

La vera prevenzione, alla fine, passa dalla fiducia, dall’ascolto e dalla capacità degli adulti di parlare apertamente di disagio, salute mentale e vita digitale. Le tecnologie possono aiutare a intercettare segnali, ma non possono sostituire la relazione.

In un’epoca in cui l’online è parte integrante della crescita, proteggere i più giovani è una responsabilità collettiva: delle famiglie, delle scuole, dei governi e delle imprese, che non possono e non devono mai mettere i profitti prima dell’essere umano, specialmente se parliamo di minori.

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/instagram-avvisera-i-genitori-se-i-figli-cercano-contenuti-su-suicidio-e-autolesionismo-come-funziona/567140/

Pensare ora a Data Center anti-missili? Quelli di Amazon colpiti negli Emirati e in Bahrain, è la prima volta in una guerra

“Oggetti” (droni bomba?) colpiscono i data center AWS negli Emirati Arabi Uniti e nel Bahrain, non era mai accaduto prima

I **data center** diventano infrastrutture strategiche in tempo di guerra. E nella nuova fase del **conflitto tra Stati Uniti, Israele e Iran**, iniziata il 28 febbraio 2026 con gli attacchi congiunti su Teheran e proseguito con le rappresaglie iraniane contro obiettivi nella regione del Golfo, anche le **infrastrutture digitali** entrano nel perimetro delle operazioni militari.

Amazon Web Services (AWS), la divisione cloud di Amazon, ha reso noto che proprie strutture negli **Emirati Arabi Uniti** e in **Bahrain** stanno registrando gravi problemi di alimentazione elettrica e connettività. Secondo quanto comunicato dalla stessa AWS sulla propria dashboard di stato, nella regione **ME-CENTRAL-1 (Emirati Arabi Uniti)** si è verificata un’interruzione significativa.

Blackout e problemi di connettività dopo raid nella regione

“*Alle 5:19 am PST (17:19 negli Emirati) del 1° marzo*”, la società ha segnalato che “*problemi di connettività e alimentazione avevano colpito API e istanze in una singola Availability Zone*”, identificata come **mec1-az2**, a causa di un problema elettrico localizzato.

In un aggiornamento successivo riportato da *Business Insider*, alle 9:41 del mattino ora del Pacifico (21:41 negli Emirati), AWS ha fornito maggiori dettagli: “*Attorno alle 4:30 del mattino ora del Pacifico (16:30 negli Emirati), una delle sue Availability Zone, identificata come mec1-az2, è stata colpita*

da oggetti che hanno impattato contro il data center”.

Il ritorno alla piena operatività della zona colpita avrebbe richiesto diverse ore, mentre le altre *Availability Zone* della regione risultavano regolarmente funzionanti.

Nei successivi aggiornamenti rilanciati dal quotidiano locale *Khaleej Times*, AWS ha precisato di essere a conoscenza del fatto che “*alcuni clienti stavano riscontrando errori nelle chiamate alle API di EC2, in particolare nelle API di rete. come l’assegnazione e l’associazione di indirizzi IP, la descrizione delle tabelle di instradamento e delle interfacce di rete*”, assicurando di essere al lavoro su più fronti per mitigare i problemi.

Difficile stabilire i tempi di ripristino

“*Alle 18:01 ora del Pacifico (6:01 del mattino negli Emirati del 2 marzo)*”, l’azienda ha dichiarato di non disporre ancora di una stima sui tempi per il ripristino dell’alimentazione, raccomandando ai clienti che ne avessero la possibilità di “*utilizzare Availability Zone alternative o altre regioni AWS*”.

Con il passare delle ore, però, come precisato da lanci di agenzia di *Al Jazeera*, AWS ha comunicato di stare indagando su “*ulteriori problemi di connettività e su un aumento del tasso di errori nella regione ME-CENTRAL-1*”.

AWS non ha specificato la natura degli “oggetti” che hanno colpito la struttura. Interpellata da Reuters sulla possibile connessione tra l’incidente e gli attacchi iraniani nella regione, la società non ha confermato né smentito un collegamento diretto.

Per la prima volta nella storia i data center sono obiettivi militari

Tutti ovviamente risponderebbero “certo”, ma questa notizia potrebbe essere la prima del suo genere nella letteratura di settore. Quando AWS parla di “oggetti” che hanno colpito un data center, usa una definizione volutamente generica, perché nei manuali di comunicazione aziendale non esiste un protocollo per uno scenario del genere.

“*È la prima volta nella storia che un data center di un grande hyperscaler viene fisicamente colpito durante una guerra. In ogni presentazione sull’architettura cloud, in ogni consiglio di amministrazione, la sicurezza fisica è sempre stata declinata in termini di recinzioni perimetrali e controlli biometrici. Non in termini di difesa antimissile,* o *di sistemi anti-drone. Non di spegnimento incendi in tempo di guerra mentre l’edificio accanto viene investito da ordigni*”, spiega in una nota social l’analista indipendente **Shanaka Anslem Perera**.

In questo scenario, anche le **infrastrutture digitali** diventano vulnerabili. Un’*Availability Zone,* come ricorda la stessa Amazon, è composta da uno o più data center fisici connessi tra loro, ma isolati rispetto alle altre zone della stessa regione cloud. Negli Emirati AWS dispone di tre Availability Zone, mentre il Bahrain ospita una delle regioni cloud strategiche per il Medio Oriente.

Il *Jerusalem Post* ha riportato che la struttura sarebbe stata utilizzata anche dalle forze armate israeliane. Se la circostanza fosse confermata, l’eventuale targeting iraniano di infrastrutture cloud a uso duale trasformerebbe ogni data center situato in aree prossime a un conflitto da asset civile a obiettivo militare. La distinzione tra infrastruttura digitale e infrastruttura della difesa si assottiglierebbe fino a scomparire.

Quanto il teatro di guerra si allarga e ‘scompiglia’ la geografia delle infrastrutture digitali

La geografia, in questo scenario, diventa decisiva. AWS aveva scelto gli Emirati Arabi Uniti per la propria regione Medio Oriente proprio per la stabilità politica, la connettività internazionale e la vicinanza ai clienti enterprise del Golfo. Una scelta strategica fondata sull’idea che Dubai e Abu Dhabi fossero hub sicuri e prevedibili. Quell’assunto è stato messo in discussione quando droni iraniani hanno colpito il Burj Al Arab, l’area portuale di Jebel Ali e una struttura che ospita carichi di lavoro per governi, banche e – potenzialmente – operazioni militari.

Il rischio di concentrazione è evidente, ha sottolineato Perera nel suo post: “*AWS, Microsoft Azure e Google Cloud operano tutte regioni Medio Oriente concentrate nello stesso corridoio geografico che ora è diventato un teatro di guerra attivo. Oracle dispone di infrastrutture a Dubai. Ogni impresa che esegue workload critici in queste regioni sta rivalutando piani di disaster recovery che fino a pochi giorni fa erano classificati come eventualità teoriche*”.

Che ne sarà dei servizi cloud nella regione? Fino a che punto le infrastrutture digitali saranno coinvolte?

AWS ha invitato i clienti a spostare i carichi di lavoro su altre Availability Zone o su altre regioni. La resilienza del cloud si fonda proprio sulla distribuzione geografica e sulla ridondanza. Tuttavia, se il conflitto dovesse estendersi o coinvolgere infrastrutture energetiche su larga scala, la

continuità operativa potrebbe diventare più complessa.

L’episodio negli Emirati segna un passaggio simbolico: la guerra tra Stati Uniti, Israele e Iran non si combatte solo nei cieli e nei siti militari, ma anche nello spazio digitale e nelle infrastrutture critiche.
Come ha spiegato ad Al Jazeera **Geist Pinfold**, docente di sicurezza internazionale al King’s College di Londra: “*I droni Shahed sono molto, molto economici e facili da produrre. Dal punto di vista degli stati del Golfo, la questione strategica centrale è capire cosa succederà quando le scorte antimissile inizieranno a diminuire*“.

Energia, telecomunicazioni, porti, aeroporti e ora data center diventano nodi sensibili di un conflitto che intreccia dimensione militare, economica e tecnologica. **La domanda non è più se le infrastrutture digitali possano essere coinvolte, ma fino a che punto lo saranno**.

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/data-center-amazon-colpiti-negli-emirati-e-in-bahrain-e-la-prima-volta-in-una-guerra/566985/

Anthropic vs Pentagono. Amodei: “Ci sono casi in cui l’AI è una minaccia per la democrazia”

Anthropic contro il Pentagono: lo scontro sull’AI tra sicurezza nazionale e democrazia

C’è uno scontro durissimo in corso tra una delle aziende di punta dell’intelligenza artificiale (AI) americana, **Anthropic**, e il **Dipartimento della Guerra** degli Stati Uniti, nello specifico il **Pentagono**. A innescarlo è stata una dichiarazione pubblica del CEO della società, **Dario Amodei**, che ha scelto di rendere trasparente un conflitto finora rimasto nei corridoi riservati della sicurezza nazionale.

Oggi scade l’ultimatum imposto dal Segretario della Guerra, **Pete Hegseth.**
Claude di Anthroopic è il modello AI disponibile nei sistemi più riservati dell’esercito con le migliori performance nelle attività di intelligence più delicate. Il Pentagono ha chiesto un accesso senza limiti ma la società di Amodei si è rifiutata di revocare completamente le sue misure di sicurezza, lasciando blindate due aree specifiche: la sorveglianza di massa degli americani e lo sviluppo di armi autonome, ovvero in grado di colpire senza l’intervento umano.

Il cuore del confronto non è se l’AI debba essere usata in ambito militare. Su questo punto, paradossalmente, le parti sono allineate. Il nodo è *come* debba essere usata – e quali limiti etici e tecnici debbano essere posti.

Dario Amodei Ceo e Co-Fondatore di Anthropic

Anthropic azienda di “Frontier AI”

Prima di tutto, va chiarito un punto: Anthropic non è un’azienda pacifista in rotta con il complesso militare-industriale. Al contrario, Amodei rivendica con forza il ruolo della sua società nella difesa americana.

Il modello AI di punta dell’azienda, ***Claude,*** è già ampiamente impiegato nelle reti classificate (cioè protette) del governo statunitense, nei laboratori nazionali e all’interno di missioni “mission-critical” del Dipartimento della Guerra (operazioni o sistemi il cui fallimento causerebbe danni irreparabili, come perdite umane, fallimenti strategici o

collassi operativi): analisi di intelligence, simulazioni strategiche, pianificazione operativa, cyber-operazioni, ma anche lancio di missili in caso.

Anthropic, secondo quanto dichiarato da Amodei, è stata la prima **azienda di *"frontier AI"*** (attiva nello sviluppo di modelli AI all'avanguardia, capaci di general intelligence su scala massiva, con capacità multimodali e agentiche vicine all'AGI) a distribuire i propri modelli in **ambienti classificati governativi**.

La società (che oggi vale 380 miliardi) ha inoltre interrotto rapporti commerciali con soggetti legati al **Partito Comunista Cinese**, rinunciando a centinaia di milioni di dollari, e sostiene controlli più stringenti sull'export dei chip per mantenere un vantaggio tecnologico delle democrazie.
Nei giorni scorsi, Anthropic ha accusato tre aziende cinesi, tra cui **DeepSeek**, di aver utilizzato ***Claude*** su scala industriale per addestrare i propri modelli di AI.

Non è quindi un conflitto tra tecnologia e sicurezza nazionale. È uno scontro *interno* alla visione di cosa significhi difendere una democrazia nell'era dell'intelligenza artificiale.

Dario Amodei Ceo Anthropic, Daniela Amodei Presidente Anthropic

I punti di rottura con il Dipartimento della Guerra

Anthropic (guidata da Dario, assieme alla *s*orella **Daniela Amodei**, oggi cofondatrice e presidente della società) si rifiuta di rimuovere due salvaguardie dai propri sistemi: il divieto di utilizzo per sorveglianza di massa domestica e il divieto di utilizzo per armi completamente autonome.
Ed è qui che si innesta lo scontro.

1. Sorveglianza di massa: il rischio di uno Stato algoritmico

Anthropic sostiene che l'uso dell'AI per missioni di intelligence estera sia legittimo e necessario. Ma traccia una linea rossa quando si parla di sorveglianza interna su larga scala. Il problema non è teorico. Negli Stati Uniti (come in molte democrazie occidentali) le agenzie governative possono acquistare legalmente grandi quantità di dati su movimenti, navigazione web, relazioni sociali dei cittadini, spesso senza mandato. Si tratta di dati apparentemente innocui, frammentati. La differenza, oggi, la fa l'AI.

Un sistema avanzato può aggregare automaticamente milioni di micro-informazioni e costruire un profilo completo, predittivo, comportamentale di qualsiasi individuo. Non è più semplice raccolta dati: è **ricostruzione algoritmica della vita privata**.

Il punto sollevato da Amodei è cruciale: **la legge è rimasta indietro rispetto alla tecnologia**. Ciò che è formalmente legale potrebbe diventare sostanzialmente incompatibile con le libertà costituzionali quando potenziato dall'AI.

Qui si intravede un'eco storica inquietante. Ogni grande salto tecnologico nella sorveglianza, dal telegrafo alle intercettazioni di massa post-11 settembre, è stato inizialmente giustificato in nome della sicurezza. Solo in seguito si sono aperti i dibattiti pubblici sui limiti.

2. Armi completamente autonome: quando l'uomo esce dal circuito

Il secondo punto riguarda le cosiddette *fully autonomous weapons*: sistemi capaci di selezionare e ingaggiare un bersaglio senza intervento umano.

Anthropic distingue tra:

- sistemi parzialmente autonomi (già usati, ad esempio nel conflitto in Ucraina),
- sistemi completamente autonomi che escludono l'essere

umano dal “loop decisionale”.

Amodei non esclude che in futuro tali sistemi possano diventare necessari per la difesa nazionale. Ma sostiene che oggi **l’AI non sia abbastanza affidabile per assumere decisioni letali in autonomia**.

Qui il problema non è solo etico, ma tecnico. I modelli di frontiera possono sbagliare, generare output imprevedibili, essere vulnerabili a manipolazioni. Delegare a queste architetture la scelta di un bersaglio significherebbe accettare margini di errore potenzialmente catastrofici.

C’è poi una questione di responsabilità: chi risponde di un errore? Il comandante? L’azienda? Il software?
Di fatto, a quanto riportato dalla *Reuters*, il Dipartimento avrebbe ventilato una controversa opzione, sulla cui legittimità diversi esperti hanno espresso perplessità: “*Se non collaborano, il Segretario alla Guerra farà in modo che venga invocato il Defense Production Act nei confronti di Anthropic*”, ha dichiarato un alto funzionario del Pentagono, “*costringendola a mettere le proprie tecnologie a disposizione del Pentagono, che lo voglia o no*”.

Pete Hegseth, Segretario della Guerra degli Stati Uniti

Le condizioni poste dai militari

Secondo la dichiarazione di Anthropic, il Dipartimento della Guerra avrebbe posto una condizione netta: collaborare solo con aziende che accettino “qualsiasi uso legale” della tecnologia e che rimuovano le salvaguardie nei casi citati.

Amodei scrive: “*Il Dipartimento della Guerra ha dichiarato che stipulerà contratti solo con aziende di intelligenza artificiale che acconsentono a “qualsiasi uso lecito” e rimuovono le misure di sicurezza nei casi sopra menzionati. Hanno minacciato di rimuoverci dai loro sistemi se mantenessimo queste misure di sicurezza; hanno anche*

minacciato di designarci come "rischio per la catena di approvvigionamento" – un'etichetta riservata agli avversari statunitensi, mai applicata prima a un'azienda americana – e di invocare il Defense Production Act per imporre la rimozione delle misure di sicurezza".

Le minacce riportate sono pesanti: rimozione dai sistemi militari, designazione come "supply chain risk" (etichetta finora riservata a entità ostili), possibile invocazione del Defense Production Act per forzare la rimozione delle protezioni.

C'è una contraddizione evidente: da un lato Anthropic verrebbe considerata un rischio per la sicurezza; dall'altro, la sua tecnologia sarebbe talmente essenziale da giustificare un intervento coercitivo dello Stato.

Questo passaggio apre una questione più ampia: quanto è diventata strategica l'AI privata per l'apparato militare americano? Siamo davanti a una nuova fase del rapporto tra Stato e industria tecnologica, simile, almeno per importanza, a quella che negli anni Quaranta del secolo scorso portò alla nascita del complesso nucleare.

La battuta d'arresto arriva in un momento cruciale per Anthropic, impegnata in una corsa serrata per assicurarsi commesse nel settore privato e soprattutto nei contratti governativi, dove la sicurezza nazionale rappresenta uno dei principali ambiti di espansione. Secondo quanto riportato mercoledì da Reuters, il Pentagono avrebbe chiesto ai propri appaltatori, tra cui colossi come Lockheed Martin, una valutazione dettagliata del loro grado di dipendenza dalle tecnologie di Anthropic, in vista di una possibile classificazione dell'azienda come soggetto a rischio. Un passaggio tutt'altro che marginale, se si considera che la base industriale della difesa statunitense comprendeva, già nel 2021, circa 60 mila contractor, incluse alcune delle maggiori società quotate del Paese.

Falsi problemi o questione etica centrale per la democrazia?

Il Pentagono, che l'amministrazione Trump ha ribattezzato "Dipartimento della Guerra", ha respinto il dilemma definendolo una falsa questione "*spinta dai media di sinistra*", si legge sulla *Reuters*.
"*Il Dipartimento della Guerra non ha alcun interesse a utilizzare l'intelligenza artificiale per condurre una sorveglianza di massa sugli americani (che è illegale), né vogliamo impiegare l'IA per sviluppare armi autonome che operino senza il coinvolgimento umano*", ha scritto su X il capo portavoce del Pentagono, **Sean Parnell**.

Sulla questione è intervenuta anche la senatrice democratica **Elissa Slotkin**: "*La persona media non pensa che dovremmo permettere a sistemi d'arma di entrare in guerra e uccidere persone senza che un essere umano eserciti in qualche modo una supervisione*". Parlando durante un'audizione di conferma per due candidati alla carica di vice segretario alla Difesa, Slotkin ha aggiunto: "*Non credo affatto che alcun americano, democratico o repubblicano, voglia una sorveglianza di massa sulla popolazione americana*".

La corsa globale all'AI militare

Lo scontro non può essere letto isolatamente. Sullo sfondo c'è la competizione con la Cina, la militarizzazione crescente delle tecnologie emergenti e la convinzione che il vantaggio nell'AI determinerà l'equilibrio strategico del XXI secolo. In questo contesto, ogni vincolo appare come un ostacolo.

Ma proprio qui emerge il paradosso: se la superiorità tecnologica è giustificata come difesa della democrazia, può essa stessa eroderne i principi fondamentali?
La storia americana offre precedenti: dal *Patriot Act* alla

sorveglianza di massa rivelata dall'ex contractor della NSA (National Security Agency) **Edward Snowden che portò al "*Datagate*"**. Ogni volta la tensione tra sicurezza e libertà si è risolta a favore della prima, salvo ripensamenti successivi.

Con l'AI, tuttavia, il salto qualitativo è enorme. Non si tratta di intercettare comunicazioni, ma di costruire sistemi predittivi capaci di anticipare comportamenti, orientare decisioni, automatizzare l'uso della forza.

Il caso Anthropic potrebbe diventare un precedente decisivo. Se l'azienda cederà, si consoliderà l'idea che le imprese di AI non possano imporre limiti etici quando operano nel perimetro della sicurezza nazionale.

Se resisterà e verrà estromessa si aprirà una frattura tra Silicon Valley e Pentagono, con possibili ricadute sull'intero ecosistema tecnologico. La questione centrale resta una: chi stabilisce i limiti dell'intelligenza artificiale in ambito militare? Il mercato? L'esecutivo? Il Congresso? Le aziende stesse?

Leggi le altre notizie sull'home page di Key4biz

https://www.key4biz.it/anthropic-vs-pentagono-amodei-ci-sono-casi-in-cui-lai-e-una-minaccia-per-la-democrazia/566913/

Stipendi nel mondo della finanza: chi guadagna di più

***Truenumbers** è l'appuntamento settimanale con la rubrica curata*

*dal portale www.truenumbers.it, il più importante sito editoriale di Data Journalism in Italia, fondato da **Marco Cobianchi**. Una rubrica utile per saperne di più, per approfondire, per soddisfare ogni curiosità, ma sempre con la precisione che solo i numeri sanno dare. Per leggere tutti gli articoli della rubrica Truenumbers su **Key4biz** clicca qui.*.

A Milano si prende di più, gli Head of Credit quelli meglio pagati (156.450 euro)

Ottenere un prestito oggi è più difficile rispetto a qualche mese fa. Secondo la Banca Centrale Europea le banche dell'area euro hanno reso più rigidi i criteri di concessione: sono diventate più selettive e più caute nell'assumere rischi. Per imprese e famiglie questo si traduce in condizioni più severe e in un accesso ai finanziamenti meno immediato. **In questo contesto il ruolo dell'Head of Credit diventa centrale: è la figura che stabilisce quanto rischio la banca può sostenere**, decide a chi concedere i fondi e a quali condizioni, e controlla l'esposizione complessiva dell'istituto per garantirne la stabilità. Una responsabilità che pesa, perché ogni scelta incide sui conti della banca. Ma proprio per questo si tratta anche di uno dei ruoli più riconosciuti e meglio remunerati nell'area credito: più oneri, dunque, ma anche più ritorni in busta paga.

Evidentemente anche per tutti questi motivi nel 2025, secondo la *Hays Italy Salary Guide 2025* – il report annuale che analizza retribuzioni e mercato del lavoro in Italia – proprio **l'Head of Credit è stata la figura che ha incassato la Ral più alta tra le professioni finanziarie censite: 156.450 euro lordi annui.** Su base mensile significa 13.037,50 euro lordi, senza bonus e senza componente variabile. Onori e oneri visto che dalle sue valutazioni dipendono milioni di euro di

credito e capitale impegnato.

Quanto si guadagna a fare il trader

Se l'Head of Credit è il "freno" della banca, l'Investment Banking è il motore. È il reparto che opera sui mercati finanziari e gestisce le grandi operazioni: fusioni tra aziende, emissioni di obbligazioni, quotazioni in Borsa. È qui che lavorano anche i trader, cioè i professionisti che comprano e vendono strumenti finanziari per conto della banca o dei clienti istituzionali, cercando di generare rendimento all'interno dei limiti di rischio stabiliti. Accanto a loro operano figure come Analyst, Associate e Vice President, che analizzano bilanci, strutturano operazioni e coordinano le strategie. In sintesi, se il credito definisce quanto si può rischiare, l'investment banking – trader compresi – decide come utilizzare quel rischio per far girare il capitale.

Il vantaggio di essere trader a Milano

A **Milano**, nel *Corporate & Investment Banking*, un Analyst con 1–3 anni di esperienza è a 52.150 euro di Ral lorda annua. Il livello successivo, Associate (4–6 anni), vale 83.440 euro. Oltre i 6 anni si entra nella fascia Vice President, e si torna al numero che fa girare la testa: 135.590 euro. È una progressione che assomiglia a una carriera "a scatti": il salto tra Analyst e Associate è di 31.290 euro, quello tra Associate e Vice President è di 52.150 euro: due gradini, due accelerazioni nette, perché cambiano responsabilità, complessità delle operazioni e pressione sui risultati.

E poi c'è l'Italia delle piazze finanziarie: stesso ruolo, città diversa, stipendio diverso. **Anche nella busta paga Milano è la capitale finanziaria d'Italia**: a parità di seniority, il mercato premia di più dove si concentra la

maggior parte delle operazioni, dei clienti e dei team specializzati. Per l'Analyst, Roma è a 46.935 euro e Torino a 41.720 euro; per l'Associate, Roma sale a 78.225 euro e Torino a 73.010 euro; per il Vice President, Roma arriva a 125.160 euro e Torino a 114.730 euro.

Ma Milano paga meno del resto d'Europa

Se Milano è la capitale finanziaria italiana, il confronto europeo ridimensiona subito le proporzioni. Secondo i dati di un'altra piataforma *(Glassdoor)* sulle retribuzioni medie base nel settore finanziario, un trader – o una figura equivalente nell'investment banking – guadagna 85.000 euro a **Londra**, 72.000 euro a **Francoforte**, 120.000 euro a **Zurigo**. La distanza riflette il peso dei diversi ecosistemi finanziari: Zurigo è un hub centrale per private banking e investment banking internazionale, Francoforte ospita la Banca Centrale Europea ed è il cuore del corporate banking tedesco, Londra resta il principale mercato europeo per volumi e capitali movimentati. Milano opera in un sistema più contenuto.

Carriera e stipendi nell'Asset Management

Non solo trader. Nella finanza c'è anche chi non compra e vende in prima persona, ma gestisce patrimoni e fondi per conto di clienti e istituzioni. Nell'Asset Management, secondo la *Hays Italy Salary Guide 2025*, a Milano un Investment Analyst con 2–3 anni di esperienza guadagna 52.150 euro di Ral lorda annua. È la figura che studia mercati, bilanci e scenari economici: in pratica prepara le mappe prima che qualcuno parta per il viaggio.

Il passo successivo è il Portfolio Manager (5–6 anni), a 73.010 euro: qui non si analizza soltanto, si decide come

distribuire i soldi tra azioni, obbligazioni e altri strumenti. Oltre i 6 anni si arriva all'Investment Manager, che tocca 125.160 euro: è il responsabile delle scelte strategiche sui capitali, spesso su masse che valgono milioni. Più cresce il livello, più aumenta il peso delle decisioni: se l'analista suggerisce, il manager firma.

Ancora una volta è Milano a pagare meglio

Anche qui la geografia conta. È la stessa logica vista nell'investment banking: dove si concentra il mercato del risparmio gestito, gli stipendi salgono. Per l'Investment Analyst, la Ral è di 41.720 euro sia a Torino sia a Bologna, mentre a Milano sale a 52.150 euro. Il Portfolio Manager raggiunge 62.580 euro a Torino contro 73.010 euro nel capoluogo lombardo. Oltre i sei anni di esperienza, l'Investment Manager è a 114.730 euro sotto la Mole e a 125.160 euro in piazza Affari. La distanza tra Milano e Torino, al livello più alto, è di 10.430 euro.

Carriera nel Private Banking: quanto paga

Non solo mercati e operazioni da milioni: c'è una finanza che vive di relazioni personali e patrimoni privati. Qui il lavoro non è "comprare e vendere" come nel trading, ma gestire patrimoni di clienti ad alta disponibilità economica, spesso imprenditori o famiglie con grandi capitali. Se l'analista studia i numeri, il private banker studia le persone: la relazione pesa quasi quanto il rendimento. Più cresce l'esperienza, più aumenta la fiducia del cliente – e con essa la responsabilità su capitali che possono valere intere aziende. **Nel Private Banking, secondo la Hays Italy Salary Guide 2025, un PB Role con 2–5 anni di esperienza vale 52.150**

euro di Ral lorda annua. Con 5–10 anni si sale a 78.225 euro, mentre oltre i 10 anni si arriva a 104.300 euro.

Nel Private Banking, la fascia oltre i 10 anni di esperienza è allineata: 104.300 euro a Milano, 104.300 euro a Roma e 104.300 euro a Torino. Le differenze emergono invece nei livelli inferiori (2–5 anni e 5–10 anni), dove le retribuzioni si collocano sotto i valori milanesi. In ogni caso, il tetto resta più basso rispetto all'Investment Banking: a Milano un Vice President arriva a 135.590 euro, contro i 104.300 euro del Private Banking oltre i 10 anni. La distanza riflette il diverso peso delle funzioni: operazioni finanziarie complesse da una parte, gestione di relazioni patrimoniali dall'altra.

Quanto si guadagna nel Credit e Risk

Non fanno notizia come i trader, ma senza di loro le banche si fermano. Nell'area Credit e Risk si controlla chi può ricevere un finanziamento, quanto è solido un bilancio, dove si nasconde il rischio. **Un Credit Analysis Role con 2–5 anni di esperienza vale 31.290 euro di RAL lorda annua; con 5–10 anni si sale a 41.720 euro; oltre i 10 anni si arriva a 52.150 euro**. Sono cifre più basse rispetto all'investment banking, ma il lavoro è centrale: è come il sistema di sicurezza di un edificio, invisibile finché tutto funziona. Al vertice c'è l'Head of Credit, che a Milano supera i dieci anni di esperienza e arriva a 156.450 euro: è la cifra più alta dell'intera area creditizia. Qui non si analizza solo un dossier, si decide l'esposizione complessiva della banca al rischio.

Finanza d'impresa quanto paga il

CFO

Non è in sala trading e non gestisce fondi: il CFO è il vertice della finanza d’impresa, il direttore finanziario che coordina bilanci, debito, investimenti e strategie industriali. E il settore in cui opera fa la differenza. Secondo la Hays Italy Salary Guide 2025, per un CFO con oltre 10 anni di esperienza le RAL lorde annue sono pari a 99.085 euro nel settore Energy, 93.870 euro nell’Engineering, 119.945 euro nella GDO/Retail, 88.655 euro nell’Industry, 76.139 euro nel Metalmeccanico e 102.214 euro nel comparto Financial Services.

Fonte: Hays Italy Salary Guide 2025, Glassdoor

Leggi le altre notizie sull’home page di Key4biz

https://www.key4biz.it/stipendi-nel-mondo-della-finanza-chi-guadagna-di-piu/566867/