TIG | THE INNOVATION GROUP

IL CAFFÈ DIGITALE

SETTEMBRE 2025

DALLA RICERCA AL MERCATO la sfida quantistica europea

© vishal-bansal-unsplash.com

QUESTO MESE ABBIAMO FATTO COLAZIONE CON...

Gian Fabio Palmerini,
Chief Information Security Officer, Webuild

PA DIGITALE

Ma questa pubblica amministrazione è sostenibile?

DIRITTO ICT IN PILLOLE

NIS2: siamo arrivati alla prima scadenze

notes

THE INNOVATION GROUP

SOMMARIO

Dalla ricerca al mercato: la sfida quantistica europea

Gianluca Dotti, *Giornalista*
TIG - The Innovation Group

La computazione quantistica, e le relative tecnologie, stanno passando dalla ricerca ai mercati reali, aprendo scenari concreti in farmaceutica, energia e logistica. L'Europa può ancora incidere sugli standard globali, a patto di trasformare competenze scientifiche in applicazioni industriali. Se ne discuterà anche nella prima edizione di un nuovo evento di TIG, a novembre.

Il passaggio al post-digitale segna l'avvio di una fase in cui il **calcolo quantistico**, insieme a **intelligenza artificiale** e high **performance computing**, non è più confinato alla ricerca ma diventa un pilastro industriale destinato a impattare mercati, supply chain e modelli di competitività. Parlare oggi di quantum computing significa già affrontare **un tema strategico, industriale e geopolitico**, non più solo scientifico.

La trasformazione che stiamo vivendo non riguarda più soltanto il software o il cloud, ma l'integrazione tra potenza di calcolo, sensori e applicazioni reali. Le tecnologie quantistiche stanno aprendo spazi concreti: da un lato la comunicazione e il sensing quantistico, con sviluppi che vanno dalla crittografia agli orologi atomici per la metrologia e la navigazione; dall'altro l'informatica quantistica, che nel medio periodo promette di integrarsi con HPC e intelligenza artificiale per affrontare problemi di ottimizzazione, chimica computazionale e ricerca di nuovi materiali. Queste applicazioni non sono più scenari futuribili ma mercati già in formazione, come dimostra la crescita degli investimenti: **nel 2024 le imprese di hardware quantistico hanno raccolto 1,59 miliardi di dollari**, mentre **quelle di software hanno superato i 600 milioni**, confermando l'urgenza per l'Europa di non restare indietro.

Le ricadute attese sono dirompenti. Nel settore **farmaceutico** e **chimico**, la simulazione di molecole complesse potrà ridurre i tempi di ricerca, mentre nell'**energia** gli algoritmi quantistici offriranno strumenti avanzati per ottimizzare reti e sistemi di accumulo. In **finanza** il quantum computing è visto come un alleato per la gestione di rischi e portafogli complessi, e nella **logistica** e nella **manifattura** avanzata potrà supportare la pianificazione di sistemi industriali articolati. Accanto a queste applicazioni, la sensoristica quantistica sembra destinata ad arrivare più rapidamente sul mercato, con impatti immediati in ambiti come **difesa**, **medicina** e **sicurezza** delle infrastrutture.

In questo scenario la competizione globale è già accesa.

Negli **Stati Uniti** la strategia è chiara: concentrare ingenti investimenti pubblici e privati su grandi progetti di scala, sostenuti da un ecosistema che integra università, colossi tecnologici e agenzie federali.

La **Cina** ha scelto un approccio centralizzato, con piani quinquennali, distretti industriali verticali e un forte coinvolgimento delle aziende di Stato, con l'obiettivo di legare sovranità tecnologica e politica estera.

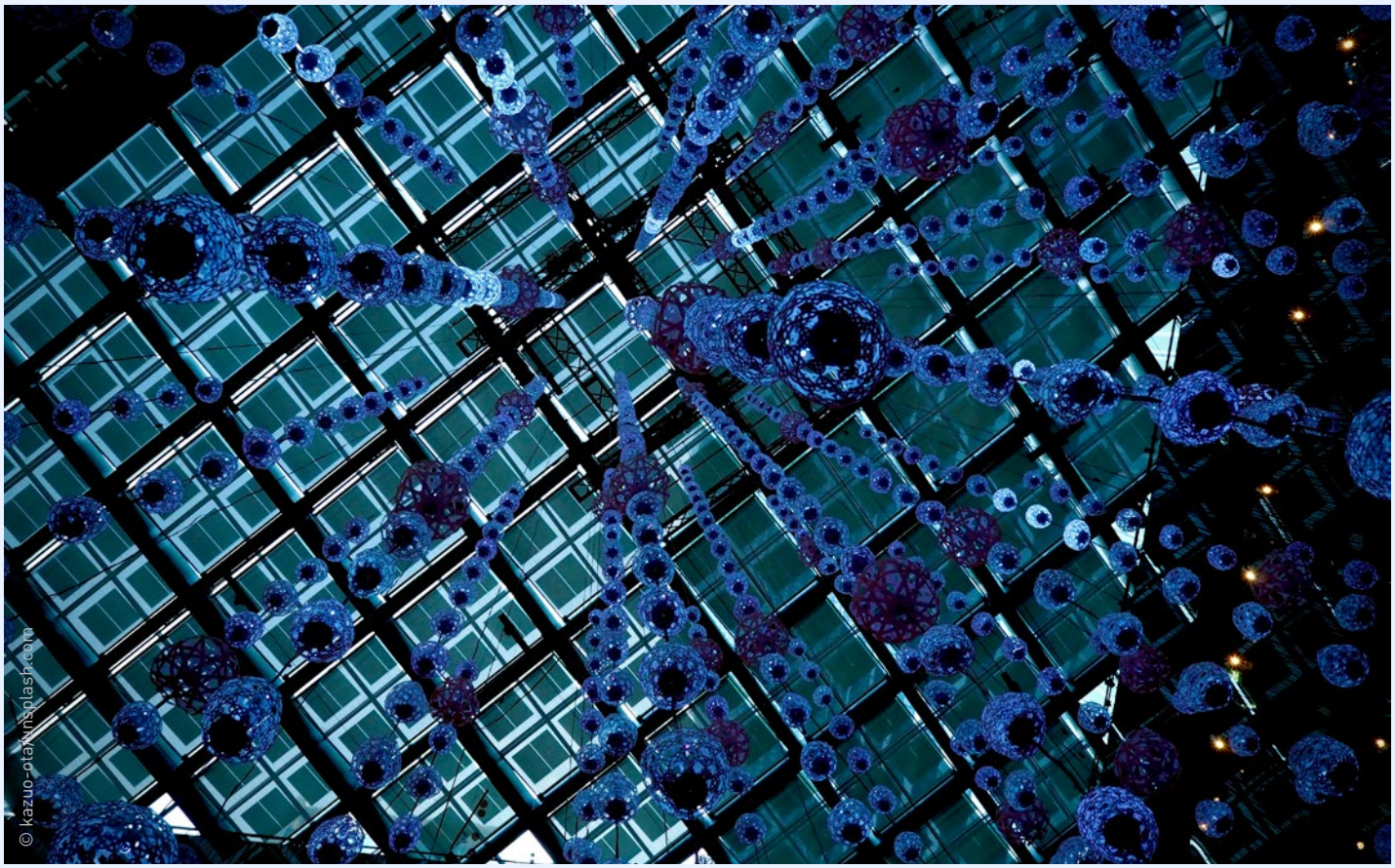
L'**Europa**, pur vantando una ricerca scientifica di eccellenza e programmi di valore come il **Quantum Flagship** o **EuroQCI,** resta penalizzata dalla frammentazione e da capitali meno consistenti rispetto ai due grandi poli globali.

Tra il 2014 e il 2024 i brevetti in tecnologie quantistiche sono quintuplicati, con Stati Uniti e Cina in forte accelerazione, mentre il continente europeo fatica a trasformare la ricerca in applicazioni commerciali scalabili.

Anche l'Italia si sta muovendo. La **Strategia Nazionale per le Tecnologie Quantistiche**, di quest'anno 2025, individua direttrici di sviluppo su ricerca, trasferimento tecnologico, formazione e industria, con un fabbisogno stimato di circa **un miliardo di euro in cinque anni**.

È un primo passo importante, ma restano da sciogliere i nodi legati alla governance e alla reale disponibilità delle risorse. Il nostro paese può contare su una solida tradizione scientifica, con eccellenze in fisica, fotonica e sensoristica atomica,

oltre a più di 4.200 pubblicazioni scientifiche sul tema. Tuttavia, il vero nodo resta **la capacità di trasformare la ricerca in impresa e di trattenere talenti**, in un contesto in cui la domanda globale di competenze quantistiche cresce a un ritmo ben superiore rispetto all'offerta.
Un ruolo decisivo è giocato anche dalle infrastrutture di calcolo. L'Italia ospita a Bologna il **supercomputer Leonardo**, tra i più avanzati al mondo, realizzato nell'ambito del programma **EuroHPC,** che costituisce un asset strategico per sviluppare scenari di calcolo ibrido in cui calcolo ad alte prestazioni e quantum computing si integrano. Questa sinergia apre la strada a nuove forme di simulazione, modellazione e ottimizzazione in settori industriali complessi, consentendo di fare dell'Europa un attore in grado di stabilire standard globali.
Le condizioni necessarie per non restare indietro sono chiare: investimenti stabili e di lungo periodo, che vadano oltre i fondi straordinari del Pnrr e garantiscano continuità; nuove competenze interdisciplinari, capaci di unire fisica, informatica e management; rafforzare il trasferimento tecnologico con strumenti finanziari adeguati per accompagnare startup e scale-up; infine, una governance coordinata che riduca frammentazioni e duplicazioni.
In questo contesto si inserisce il nuovo appuntamento di TIG - The Innovation Group: il *Quantum Computing Summit*, che si terrà il 27 novembre presso la sede di Cefriel a Milano. La giornata di lavori, intitolata ***"Tecnologie emergenti per industrie e business"***, rappresenta la prima edizione di un evento dedicato interamente al **potenziale del quantum computing per imprese e sistemi produttivi**, insieme alle aziende che stanno sviluppando le tecnologie e alle istituzioni scientifiche italiane e internazionali, oltre ai manager delle imprese su cui il quantum computing più avrà impatto.
L'iniziativa cade in un'annata dal valore anche simbolico, proclamata dalle Nazioni Unite come ***Anno internazionale della Scienza e della Tecnologia Quantistica***, e in un momento in cui il nostro Paese ha da poco varato la sua prima **strategia nazionale** in materia. L'obiettivo del Summit è fare il punto sulla frontiera della ricerca e dello sviluppo tecnologico, ma anche mettere in evidenza come i computer quantistici possano rivoluzionare settori come cybersecurity, intelligenza artificiale e ottimizzazione industriale, stimolando al contempo la crescita di infrastrutture complementari quali cloud, data center e software specializzati.
Il quadro che emerge è piuttosto chiaro: il quantum computing è già oggi **un campo di investimento e di posizionamento strategico**, non soltanto di ricerca accademica. Chi saprà muoversi rapidamente per trasformare eccellenza scientifica e infrastrutturale in ecosistemi industriali integrati, stabilirà gli standard e controllerà le piattaforme del futuro. **Per l'Italia e l'Europa la finestra di opportunità è aperta**, ma non resterà tale a lungo. Restare indietro significherebbe dipendere da soluzioni sviluppate altrove e adattarsi a regole fissate da altri. Agire subito, invece, permetterà di trasformare il quantum computing da promessa a leva concreta di sovranità tecnologica e competitività industriale.



Oltre l'Algoritmo di Shor: la minaccia quantistica alla cybersecurity

Gian Fabio Palmerini
Chief Information Security Officer, Webuild

LA CRITTOGRAFIA È OVUNQUE E PROTEGGE INFORMAZIONI E PRIVACY. CON IL QUANTUM COMPUTING, MOLTE APPLICAZIONI SONO A RISCHIO, DAI PROTOCOLLI VPN, TLS/SSL E SSH, ALLE FIRME DIGITALI E AI SISTEMI DI AUTENTICAZIONE.

Il **quantum computing**, o informatica quantistica, sta rivoluzionando il modo in cui pensiamo ai calcoli. A differenza dei nostri **computer classici** che usano bit (0 o 1), i computer quantistici impiegano i *qubit*. Questi "oggetti" speciali possono essere 0, 1, o una combinazione di entrambi contemporaneamente (*sovrapposizione*), e possono anche essere **intrecciati** (*entanglement*), influenzandosi a vicenda istantaneamente.

Gian Fabio Palmerini

Queste proprietà permettono ai computer quantistici di eseguire calcoli molto più velocemente, esplorando tantissime possibilità in parallelo. Non sono qui per rimpiazzare i nostri computer di tutti i giorni, ma per affrontare sfide immense in settori come la scoperta di farmaci, lo sviluppo di materiali innovativi, la crittografia avanzata e l'intelligenza artificiale, dove la potenza di calcolo attuale non basta.

LA RIVOLUZIONE DI SHOR E LE SUE IMPLICAZIONI

L'interesse per il calcolo quantistico è esploso nel 1994, quando il matematico Peter Shor sviluppò un algoritmo rivoluzionario. Immagina un numero enorme come una torta gigante: l'algoritmo di Shor è un coltello magico che la taglia in fette sempre più piccole, fino a trovare gli ingredienti di base (i numeri primi). Per i computer classici, trovare i fattori primi di numeri così grandi è un compito che richiede tempi proibitivi. Ma l'algoritmo di Shor, eseguito su un computer quantistico, può farlo incredibilmente più in fretta. Questo è cruciale perché la sicurezza di molti sistemi crittografici attuali, come **RSA** ed **ECC** (ampiamente usati per proteggere le nostre comunicazioni e transazioni), si basa proprio su questa difficoltà di fattorizzazione. L'algoritmo di Shor, insieme all'algoritmo di ricerca di Grover (che velocizza la ricerca in liste non ordinate), ha sollevato seri interrogativi sul futuro della crittografia.

LA CORSA ALLA CRITTOGRAFIA POST-QUANTISTICA

Con lo sviluppo sempre più rapido dei computer quantistici, organizzazioni come il **NIST (National Institute of Standards and Technology)** hanno agito. Nel 2016, il NIST ha lanciato una gara globale per identificare e selezionare **algoritmi crittografici resistenti ai computer quantistici**, noti come **crittografia post-quantistica (PQC)**. La gara si è conclusa nel 2024, con la selezione di algoritmi ritenuti sufficientemente robusti per il *futuro*.

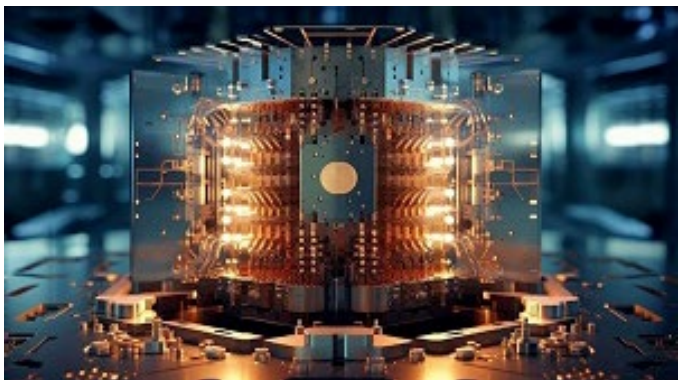
LE MINACCE QUANTISTICHE ALLA NOSTRA SICUREZZA DIGITALE

La crittografia è ovunque nella nostra vita digitale, proteggendo informazioni e privacy. Con l'avanzamento del quantum computing, molte applicazioni che usiamo quotidianamente sono a rischio:

- **VPN (Virtual Private Network)**
- **TLS/SSL (Transport Layer Security)**
- **SSH (Secure Shell)**
- **Firme digitali** e **firme dei codici** (essenziali per la sicurezza della supply chain software)
- Sistemi di **autenticazione**

Le principali minacce che dovremo affrontare includono:

- ***Harvest Now, Decrypt Later*:** criminali potrebbero già raccogliere dati criptati oggi (database, file protetti, comunicazioni) con l'intento di decifrarli in futuro, quando i computer quantistici saranno sufficientemente potenti.
- **Crittografia in transito:** protocolli come TLS e SSH, che proteggono le nostre comunicazioni online, sono a rischio. Questo è un caso d'uso molto urgente per l'implementazione della PQC.
- **Firme Firmware e Software:** la sicurezza dell'avvio dei dispositivi e l'integrità del software dipendono da firme digitali che potrebbero essere compromesse. Anche le criptovalute e le tecnologie blockchain, basate su algoritmi crittografici vulnerabili, potrebbero vedere la loro integrità e fiducia minacciate dalla possibilità di falsificare firme o manipolare le transazioni.
- **Infrastruttura a Chiave Pubblica (PKI):** la PKI, che fornisce autenticità per crittografia e identità digitali, sarà influenzata. Gli schemi PQC aumentano le dimensioni di firme e chiavi (ad esempio, una singola firma Dilithium3 può superare i 5kB), rendendo le implementazioni complesse per dispositivi con limiti di pacchetti.



- **Token:** i token basati su crittografia asimmetrica potrebbero incontrare problemi a causa di vincoli di dimensione, come nel caso dei cookie.

Il futuro della sicurezza nell'era quantistica

Abbiamo brevemente esplorato come il **quantum computing** stia ridefinendo il panorama tecnologico, offrendo capacità di calcolo senza precedenti grazie ai **qubit** e ai principi di **sovrapposizione** ed **entanglement**.

Se da un lato promette progressi rivoluzionari in settori come la medicina e l'intelligenza artificiale, dall'altro la sua abilità di **fattorizzare numeri enormi**, come dimostrato dall'algoritmo di Shor, rappresenta una seria **minaccia** per gli attuali sistemi crittografici, compresi quelli che proteggono le nostre comunicazioni, le transazioni finanziarie e le infrastrutture critiche. Dalle VPN alle firme digitali, quasi ogni aspetto della nostra vita digitale si affida a una crittografia che potrebbe diventare vulnerabile.

È per questo che la corsa alla **crittografia post-quantistica (PQC)**, con iniziative come quella del NIST, è fondamentale per garantire che la nostra sicurezza digitale rimanga robusta di fronte a queste nuove sfide. Capire queste minacce è il primo passo; il prossimo è sapere **come possiamo attivamente proteggerci e cosa devono fare le organizzazioni per implementare queste nuove difese**.

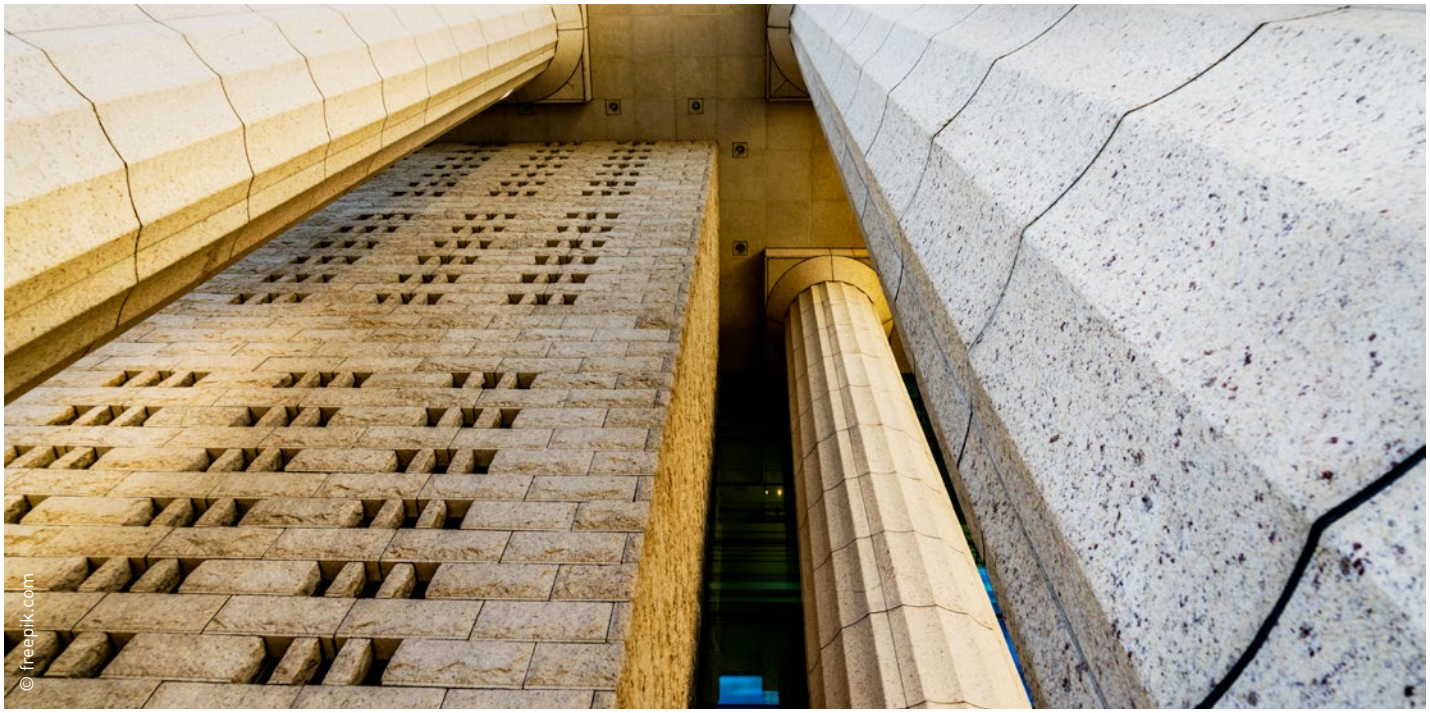
Ma questa pubblica amministrazione è sostenibile?

Roberto Masiero
Presidente, TIG - The Innovation Group

NEL SUOI ARTICOLO SUL "CORRIERE DELLA SERA DEL 27 AGOSTO INTITOLATO "LA GIUNGLA CHIAMATA BUROCRAZIA", IL PROF. SABINO CASSESE IDENTIFICA, TRA LE PRINCIPALI RADICI DELL'INEFFICIENZA DELLA PUBBLICA AMMINISTRAZIONE, L'*"ESTREMA COMPLESSITÀ DELL'ORGANISMO AMMINISTRATIVO"*: DAI VINCOLI DERIVANTI DALL'ESTERNO DALLA CONTRADDITORIA *"INTELAIATURA DELLE LEGGI"*, A *"REGOLE ISTITUZIONALI UNIFORMI PER AMMINISTRAZIONI ORMAI COMPLETAMENTE DIFFORMI"*, A *"UN PERSONALE BUROCRATICO SOTTOMESSO E SENZA VERA VOCAZIONE PER IL SERVIZIO PUBBLICO"*.

Viene quindi da chiedersi: ma questa Pubblica Amministrazione, così complessa e involuta, così "analogica" nella sua irriducibile struttura per silos, così poco capace – nonostante vari tentativi – non solo di attrare i migliori talenti, ma anche di trattenere quelli che ha già al suo interno – questa Pubblica Amministrazione è veramente sostenibile?
Per dare una risposta a questa domanda occorre affrontare i tre punti dell'analisi del Prof. Cassese (ve ne sono altri, ma li rimandiamo ad una prossima occasione).
Sul tema della **complessità** dell'organismo amministrativo: questa è il risultato di un processo "incrementale" con scelte legislative fatte spesso senza un piano organico, quando si presentava un problema da risolvere. Da una parte si legifera, dall'altra parte non si vede come questa produzione di leggi va ad impattare sulla macchina organizzativa.
E a sua volta, la vetusta organizzazione della PA per silos verticali non ha mai fatto i conti con la sostenibilità economica del sistema dei silos. Di fatto, la Pubblica Amministrazione, come è organizzata, non sembra oggi in grado di garantire la governance di tutte le piattaforme e i servizi che ne innervano la complessità. Le 11.000 pubbliche amministrazioni, piu' le 8000 scuole, non possono avere tutte le competenze per gestire le complessità crescenti; a maggior ragione come potremmo pretendere che il 70% degli 8000 comuni con meno di 5000 abitanti possano avere veramente un responsabile della transizione digitale ed occuparsi seriamente della sicurezza dei dati dei propri cittadini?
Le piattaforme al servizio dei cittadini devono vedere una progressiva convergenza sotto piattaforme comuni, senza pregiudizi nei confronti di eventuali esternalizzazioni, ma a due condizioni: che le strutture esterne forniscano soluzioni comuni per conto di tutti; e che i partner privati siano pienamente consapevoli di cosa significa esercitare un servizio pubblico, che è un servizio alla persona, alla base della democrazia.
Quanto a "**regole istituzionali uniformi per amministrazioni ormai difformi**", come si fa a pretendere che uno stsso corpus rigido di norme amministrative possa adattarsi efficacemente a realtà diverse come i Ministeri, i grandi Enti Centrali, le Regioni, le Agenzie, e i nostri 80000 Comuni? Serve centralizzare le infrastrutture, definire poche regole di alto livello e poi approfittare della flessibilità offerta dal digitale per sviluppare norme e soluzioni organizzative adatte ai diversi contesti. Ma non ci si può lamentare dell'inefficienza della Pubblica Amminsitrazione se non si aggredisce il problema istituzionale che sta alla base: se dn fatto di Sanità le Regioni non si parlano fra di loro e ancor meno con lo Stato centrale (ricordiamo per tutte la tragica pantomima dei dati delle morti per Covid), il problema è a monte.
Infine veniamo al problema del ***"personale burocratico sottomesso e senza vera vocazione per il servizio pubblico".***Se questa fosse veramente la situazione diffusa del pubblico impiego ci sarebbero pochi motivi di

speranza. Consideriamo brevemente alcuni trend:
I dipendenti pubblici in Italia sono 3.400.000 e si prevede che circa 700.000 andranno in pensione entro il 2033.
Di fatto tuttavia la tendenza prevalente è a "riempire i vuoti" lasciati nell'organizzazione, invece che a cogliere questa opportunità per un ricambio qualitativo e per una introduzione massiva di talenti. La logica inerziale delle organizzazioni prevale inesorabilmente sull'esigenza dell'innovazione tecnologica e professionale.
L'impiego pubblico offre tuttora retribuzioni più attraenti rispetto al privato al momento dell'ingresso, ma questa competitività si perde nel percorso di carriera. Ciò porta a flussi migratori da un'amministrazione all'altra in cerca di migliori condizioni, e per le professionalità migliori è quasi irresistibile l'attrazione del privato.
I recenti provvedimenti per la valorizzazione del merito possono certamente favorire la retention di alcune professionalità; abbiamo verificato anche che molti giovani – e non solo - scelgono l'impiego pubblico con uno spirito di servizio, e l'elemento valoriale non va quindi trascurato.
Rimane tuttavia che l'impatto della desertificazione demografica, unita alla scarsa competitività dell'impiego pubblico e alla mancata trasformazione delle organizzazioni rischia di ampliare il gap tra l'impiego pubblico eil settore privato.
L'introduzione delle nuove tecnologie di Intelligenza Artificiale consentirà rapidamente di ridurre le attività ripetitive e consentirà di offrire opportunità professionali assai più gratificanti anche nel settore del pubblico.
Ma per questo è necessario un massiccio investimento di formazione e re-training delle risorse esistenti per consentire loro di inserirsi in questo nuovo mondo e sviluppare le loro potenzialità per produrre nuovo valore pubblico. Altrimenti rischiamo di continuare a vivacchiare, e la Pubblica Amministrazione e ridursi a "refugium peccatorum", con un ennesimo spreco di risorse umane e finanziarie.



L'Intelligenza artificiale è ora sanzionata nei Tribunali italiani

Elena Vaciago
Research Manager, TIG - The Innovation Group

LA NUOVA LEGGE ITALIANA SULL'AI PREVEDE SANZIONI PENALI PER IL REATO DI ILLECITA DIFFUSIONE DI CONTENUTI GENERATI O MANIPOLATI CON SISTEMI DI AI, OLTRE CHE RISPETTO DEI COPYRIGHT.

Una sentenza di cui sentiremo ancora parlare.
Come *ha riportato La Stampa lo scorso 21 settembre*, il tribunale di Torino ha condannato, con una multa di 500 euro, l'uso poco accorto dell'intelligenza artificiale nelle aule di giustizia. Il condannato, che se ne era servito per un ricorso depositato lo scorso febbraio di opposizione a un'ingiunzione di pagamento, dovrà versare la multa alle controparti e alla cassa delle ammende. Aveva torto e probabilmente ne era anche consapevole, ma per mezzo dell'AI ha sostenuto la sua tesi con argomenti «astratti» e senza collegamenti con il contenuto della causa.
La giudice ha motivato così la sua scelta: «Ha agito in giudizio in malafede o quantomeno con colpa grave, dal momento che ha proposto opposizione nei confronti di avvisi di addebito che le erano stati tutti notificati in precedenza, già oggetto di plurimi atti di esecuzione».
Inoltre, per quanto riguarda l'impiego dell'AI: «... un ricorso redatto "col supporto dell'intelligenza artificiale", costituito da un coacervo di citazioni normative e giurisprudenziali astratte, prive di ordine logico e in larga parte inconferenti, senza allegazioni concretamente riferibili alla situazione oggetto del giudizio".
Del resto, la stessa recente legge italiana sull'intelligenza artificiale, il Disegno di legge 1146/2024 *approvato definitivamente dal Senato lo scorso 17 settembre 2025*, primo quadro normativo nazionale in Europa che disciplina sviluppo, adozione e governance dei sistemi AI, prevede **sanzioni penali per violazioni legate all'AI**, come l'uso dei deepfake e utilizzi malevoli dell'AI generativa. Entra infatti nel Codice penale il reato di «illecita diffusione di contenuti generati o manipolati con sistemi di IA» (punito da uno a 5 anni «se dal fatto deriva un danno ingiusto») fino al riconoscimento di "circostanza aggravante" (con aumento delle pene) per l'impiego di sistemi AI nei casi di sostituzione di persona, truffa, riciclaggio, autoriciclaggio, aggiotaggio.

COSA CAMBIA CON LA NUOVA NORMA ITALIANA SULL'AI

La legge si basa su principi di uso antropocentrico, trasparente e sicuro dell'AI, con attenzione particolare a innovazione, cybersicurezza, accessibilità e tutela della riservatezza. Integra e completa il Regolamento UE "AI Act", prevedendo garanzie di tracciabilità, responsabilità umana e centralità della decisione finale da parte di persone fisiche. Le autorità nazionali designate per la governance sono l'Agenzia per la Cybersicurezza Nazionale (ACN), con poteri ispettivi, e l'Agenzia per l'Italia Digitale (AgID), che gestisce notifiche e promuove casi d'uso sicuri. La norma poi interviene in vari settori critici (come sanità, lavoro, pubblica amministrazione, giustizia, formazione e sport), con un'attenzione particolare alle responsabilità e ai diritti fondamentali nel contesto dell'AI. Contiene 28 articoli divisi in sei capi, con uno schema programmatico e disposizioni specifiche per i settori critici, e si propone di rafforzare la tutela dai rischi legati all'impiego dell'AI nel contesto italiano, mantenendo coerenza con le disposizioni europee.
Inoltre, contiene una disposizione che autorizza l'utilizzo di una somma già a disposizione di Cdp Venture Capital (pari a 1 miliardo di euro) per l'investimento nel capitale di rischio di Pmi e grandi imprese per progetti di AI, cybersecurity e quantum computing.

I PRINCIPI GUIDA DELLA LEGGE ITALIANA SULL'AI

I principi guida ribaditi dalla nuova legge italiana sull'intelligenza artificiale sono:

- Centralità della persona umana e **antropocentrismo dell'AI**, per mettere al centro l'uso umano e responsabile della tecnologia.


Governo Italiano

Home / Notizie / Articoli / Approvata in via definitiva la...

Approvata in via definitiva la legge italiana sull'Intelligenza Artificiale

Butti: "Italia primo Paese UE con quadro nazionale allineato all'AI Act. Governance con ACN e AgID e 1 miliardo di euro per startup e PMI"

In allegato l'articolo *"Intelligenza artificiale: nella via italiana una strategia di sviluppo"* del **25 settembre 2025** de *"Il Sole 24 Ore"*.

- Trasparenza e spiegabilità dei sistemi AI, per garantire comprensione e tracciabilità delle decisioni automatizzate.
- Responsabilità degli operatori, con obblighi chiari su chi risponde degli effetti dei sistemi AI.
- Non discriminazione e inclusione, per prevenire bias e garantire pari opportunità.
- Tutela della dignità e dei diritti fondamentali delle persone.
- Protezione dei dati personali e sicurezza informatica, in coerenza con GDPR e norme privacy.

COME LA NUOVA LEGGE SI RAPPORTA CON L'AI ACT EUROPEO

La legge italiana si pone come **un'integrazione e un rafforzamento delle norme europee**, con un'attenzione più marcata su contesti sensibili e sul controllo nazionale, ma mantenendo piena coerenza con i principi dell'AI Act. Adotta un approccio precauzionale, con divieti espliciti e obblighi anche in contesti a basso rischio, mentre l'AI Act adotta un modello basato sul rischio, classificando i sistemi AI in base al livello di rischio e imponendo obblighi proporzionati solo per usi ad alto rischio. Obblighi generali e trasparenza sono temi comuni a entrambe, ma la legge italiana impone **obblighi più rigidi anche per usi a basso rischio** e rafforza il ruolo della supervisione umana.
La legge italiana è poi settoriale, con **norme dettagliate per sanità, lavoro, giustizia e pubblica amministrazione**, mentre l'AI Act ha un ambito trasversale, applicabile a tutti i settori, e stabilisce usi vietati o ad alto rischio indipendentemente dal contesto. Secondo le nuove disposizioni, ad esempio nell'ambito sanitario, l'utilizzo dell'AI è consentito a determinate condizioni (come supporto per diagnosi e cure) ma la decisione finale deve sempre rimanere ai medici e i pazienti hanno il diritto dei pazienti di essere informati. In materia di lavoro, è prevista l'attivazione di un Osservatorio nazionale: inoltre si stabilisce che è obbligatorio che il committente o lo stesso datore di lavoro informino il lavoratore dell'utilizzo dell'AI in azienda. Lo stesso obbligo di comunicazione sussiste da parte dei professionisti nei confronti dei propri clienti. Anche in ambito giudiziario la norma sancisce che ogni decisione sull'interpretazione e sull'applicazione delle leggi è sempre riservata ai magistrati (non può essere delegata all'AI).
In tema di **copyright**, una disposizione quadro prevede che anche le opere create con l'ausilio di strumenti di intelligenza artificiale siano protette dal diritto d'autore, a condizione che la loro creazione derivi del lavoro intellettuale dell'autore. La riproduzione e l'estrazione da opere o da altri materiali contenuti in rete o in banche di dati cui si ha legittimamente accesso, effettuata tramite l'utilizzo di modelli e sistemi AI, è consentita solo se non c'è copertura del copyright (o se ciò avviene fa parte di enti di ricerca e istituti culturali per scopi di ricerca scientifica).

GLI IMPATTI NELLE AZIENDE ITALIANE

La normativa italiana, nel solco dell'AI Act europeo, richiede un salto di qualità nella governance e nell'implementazione dell'intelligenza artificiale nelle

imprese, coinvolgendo tecnologie, processi e personale dedicato. È previsto quindi che influirà in modo significativo l'uso dell'AI nelle aziende, con impatti che coinvolgeranno organizzazione interna, responsabilità e compliance. Le imprese dovranno adeguare l'uso dell'AI **a standard più rigidi di trasparenza, responsabilità e sicurezza**, producendo documentazione tecnica, audit e registri delle decisioni automatizzate. Sarà necessario garantire la supervisione umana e un'accountability rafforzata oltre al rispetto di GDPR. La classificazione del rischio dei sistemi AI in base alle disposizioni (inaccettabile, alto, limitato, minimo) determina obblighi diversi, con particolare attenzione a limitare o vietare usi rischiosi come profilazioni massive, analisi biometriche e riconoscimento emotivo. Le aziende che usano software o strumenti AI, anche terzi (es. ERP, CRM, chatbot), dovranno conoscere e garantire la conformità della componente AI dei propri sistemi. Molte disposizioni sono collegate a un **uso responsabile e sicuro dei dati** collegati ai sistemi AI.

In linea con il GDPR, sono previsti rigorosi requisiti di privacy e sicurezza

- Ogni trattamento di **dati personali** da parte di sistemi AI deve avere una base legale valida (consenso, interesse legittimo con condizioni restrittive, obblighi contrattuali) e rispettare i principi di minimizzazione, liceità, trasparenza e integrità.
- Le aziende devono documentare le fonti dei dati usati per addestrare i modelli AI, assicurando che non siano impiegate informazioni ottenute illecitamente o senza consenso.
- È obbligatorio implementare **misure di sicurezza tecniche e organizzative** per proteggere i dati da accessi non autorizzati, perdite o manipolazioni, incluse misure come crittografia e controllo degli accessi.
- La normativa richiede **trasparenza** verso gli utenti, che devono essere informati del trattamento AI, della natura automatizzata delle decisioni e dei loro diritti di accesso, rettifica o opposizione.
- Per usi innovativi o a rischio elevato, occorre eseguire valutazioni d'impatto sulla protezione dei dati (DPIA) per valutare e mitigare i rischi.
- La governance dei dati dovrà essere integrata tra AI Act, GDPR e le autorità italiane competenti (Garante Privacy, AgID, Agenzia per la Cybersicurezza Nazionale), con obblighi di collaborazione e controllo.
- La legge richiede inoltre la **localizzazione dei dati critici dell'AI** (es. dati personali) in datacenter UE o italiani per tutelare la sovranità e la sicurezza dei dati sensibili dei cittadini. Il principio vale soprattutto per enti pubblici e infrastrutture strategiche, che devono riferirsi a data center nazionali anche per servizi di disaster recovery e business continuity.

In sostanza, la legge italiana sull'AI ribadisce i requisiti di sicurezza per dati e soluzioni AI, e pone una specifica enfasi sulla localizzazione dei dati per salvaguardare la sicurezza nazionale, la privacy e la governance autonoma dei dati, soprattutto per i sistemi AI usati in ambiti pubblici e strategici.

NIS2: siamo arrivati alla prima vera scadenza

Valentina Frediani
Founder and CEO, Colin & Partners

CONTO ALLA ROVESCIA PER L'ENTRATA IN VIGORE DEL MODELLO ORGANIZZATIVO IN MATERIA DI NIS2. ENTRO IL 31 DICEMBRE I DESTINATARI DELLA NORMA DOVRANNO ADOTTARE POLITICHE E PROCEDURE PER ESSERE IN GRADO DI NOTIFICARE LE PERTURBAZIONI OPERATIVE AVENDO A MONTE EFFETTUATO LA GESTIONE DEL RISCHIO.

Le recenti disposizioni dell'Autorità Nazionale in materia di cybersicurezza hanno elencato in modo molto chiaro gli ambiti di intervento sui quali ogni azienda ed ente destinatario della norma dovrà provvedere a confrontarsi a stabilire sia politiche che procedure andando poi a completare l'adeguamento entro ottobre del 2026 con l'adozione delle misure tecnologiche prescritte dal legislatore o adottate sulla base del principio di accountability.
Un primo ambito di intervento che dovrà essere affrontato dai destinatari dell'adeguamento, riguarda i ruoli e le responsabilità di coloro che si troveranno a gestire la norma all'interno della propria realtà organizzativa. Se da una parte il legislatore ha imposto l'individuazione e la nomina del punto di contatto e del suo sostituto, dall'altra appare logico come ciascuna entità giuridica debba inquadrare altri soggetti che dovranno coadiuvare tali figure sotto il profilo della gestione formativa, con riferimento alle misure di sicurezza tecnologiche e certamente sulla base delle competenze inerenti la gestione della catena di approvvigionamento con particolare riferimento ai fornitori critici.
Costruire un organigramma NIS2 deve costituire il punto di partenza pratico per andare a stabilire le competenze e le specifiche responsabilità di ciascun soggetto che debba contribuire all'attuazione della norma all'interno dell'organizzazione destinataria. Ciò consente di poter andare a stabilire anche il flusso comunicativo non solo tra il punto di contatto e il board ma anche tra questi ed ACN.
Gli altri punti della determina si concentrano sulla gestione dei rischi, degli asset, delle vulnerabilità sino a toccare tematiche come la continuità operativa, il ripristino in caso di disastro ed ovviamente il monitoraggio degli eventi di sicurezza. La gestione del rischio non può essere affrontata senza la costruzione di politiche e procedure di sicurezza informatica documentate tanto che ciascuna entità organizzativa dovrà essere in grado di dimostrare non solo di aver realizzato tali documenti ma di averli calati nella propria realtà ed averne consentito l'adozione pratica ed effettiva da parte degli operatori. Allo stato attuale nell'applicazione pratica della norma, qualche preoccupazione la destra la gestione della catena di approvvigionamento dei fornitori critici.
Nella definizione delle attività connesse alla catena di approvvigionamento, troviamo questo passaggio *"I processi di gestione del rischio di cybersecurity della catena di approvvigionamento sono identificati, stabiliti, gestiti, monitorati e migliorati dagli stakeholder dell'organizzazione."* In sostanza ogni organizzazione dovrà essere in grado di gestire i rischi connessi alla supply chain con particolare riferimento ai fornitori cosiddetti critici. Per procedere ad applicare idoneamente la norma il primo passaggio è l'identificazione dei fornitori critici che in molte realtà non è di facile rilievo perché ovviamente possono rientrare tutti i fornitori in ambito ICT ma anche quelli che collegandosi alla rete aziendale potrebbero andare a generare delle vulnerabilità.
La mappatura pertanto è un passaggio fondamentale che spesso necessita della compartecipazione non solo dei sistemi informativi ma anche dell'ufficio acquisti o delle singole direzioni laddove l'acquisizione del fornitore sia rimessa a più aree. Una volta mappati i fornitori si deve procedere alla valutazione dei rischi informatici andando ad integrare questi rischi nel proprio piano

di sicurezza. Lo strumento principale mediante il quale l'organizzazione destinataria della norma possa agire sui fornitori è ovviamente rappresentato dalle clausole contrattuali che dovranno garantire non solo la sicurezza delle informazioni e ridurre i rischi derivanti da perturbazioni operative, ma anche includere controlli e audit che dovranno essere effettuati dal soggetto che applica la NIS2. Questo implica ovviamente l'organizzazione di un sistema di monitoraggio continuo dei fornitori attivi sia attraverso procedure che garantiscano tale monitoraggio sia attraverso meccanismi contrattuali che in caso di inadeguatezza consentano di rivalutare la posizione del fornitore.
Quindi alla luce di quanto appena descritto, la *grande corsa* entro fine anno non sarà rivolta soltanto a generare documenti ragionati e realizzati sulla base dell'effettivo flusso organizzativo interno ma dovrà riguardare anche soggetti terzi.
Le azioni pertanto da porre in essere per la conformità non sono decisamente banali ma sono oggettivamente lo sviluppo inevitabile di un sistema organizzativo che debba monitorare i propri rischi rispetto alla cyber sicurezza con razioncinio e con una visione di insieme dei rischi.

Infrastruttura: una parola ambigua, ma centrale nell'era dell'AI

Valentina Bernocco
Content Manager, TIG - The Innovation Group

L'INTELLIGENZA ARTIFICIALE E IL CLOUD, CON LE LORO NECESSITÀ DI POTENZA DI CALCOLO, CAMBIANO GLI EQUILIBRI DEL MERCATO ICT. E NON SOLO.

Attenzioni, aspirazioni e investimenti si riversano su di lei: l'**infrastruttura**. Un termine lessicalmente un po' infelice, perché vago e polivalente. Anche senza sconfinare in altri campi (per esempio nei trasporti, o nella filosofia di Karl Marx) e restando nell'Ict, notiamo che la parola "infrastruttura" assume diversi significati a seconda del contesto o anche nello stesso contesto: può indicare una rete di telecomunicazione, sistemi tecnologici "fondanti" come server e appliance, oppure un intero data center. Ma sono parte dell'infrastruttura anche i chip, oggi al centro di quella corsa all'intelligenza artificiale di cui ancora si parla, carica di implicazioni geopolitiche ed economiche.
Se anche la parola non ci piace, è impossibile non usarla. E anche nell'ambiguità lessicale, il messaggio che trapela dai fatti di cronaca e dai dati degli analisti è di lampante chiarezza: senza le "basi", senza la materia, il silicio, il rame, la fibra ottica, l'ascesa del cloud e dell'intelligenza artificiale non potrebbero realizzarsi. E le fondamenta materiali di cui oggi disponiamo non sono sufficienti. Nemmeno quelle delle Big Tech, anzi soprattutto quelle delle Big Tech.

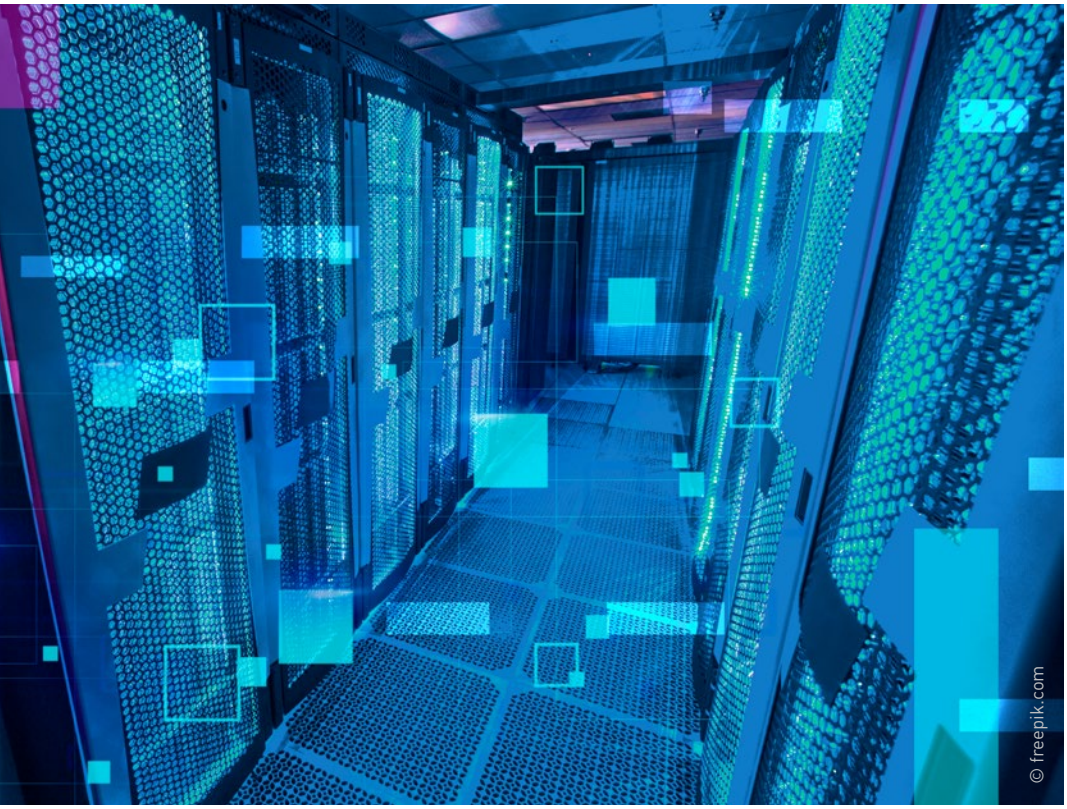
L'ASSE OPENAI-NVIDIA

Recenti dichiarazioni dell'amministratore delegato di **OpenAI**, **Sam Altman**, rendono l'idea (per quanto un po' enfatiche ed eco di una cultura molto statunitense dell'abbondanza e dell'eccesso): *"Se l'AI resterà sulla traiettoria che immaginiamo, allora cose incredibili saranno possibili. Con 10 gigawatt di potenza di calcolo magari l'AI potrebbe trovare una cura per il cancro. Oppure, con 10 gigawatt, potrebbe capire come fornire un tutoring personalizzato per ogni studente del mondo.*

Se la capacità di calcolo ci limita, dovremo scegliere a che cosa dare priorità; nessuno vorrebbe fare questa scelta, perciò costruiremo. La nostra visione è semplice: vogliamo creare una fabbrica che possa produrre gigawatt di nuova infrastruttura AI ogni settimana". Altman ha ammesso che realizzare tale visione sarà estremamente difficile: richiederà anni e sforzi di innovazione a tutti i livelli, dai chip alle forniture energetiche.
A dare concretezza a questo impegno c'è il colossale *accordo da 100 miliardi di dollari stretto con Nvidia* lo scorso settembre: a tanto ammonta l'investimento che permetterà alla società di Jensen Huang di diventare il partner strategico preferenziale di OpenAI. Parallelamente, in più fasi e a partire alla seconda metà del 2026 la società di ChatGpt comprerà da Nvidia enormi forniture di Gpu (in particolare, sistemi basati sulla nuova architettura Vera Rubin) per attività di addestramento di Large Language Model. *"L'accordo sull'investimento e sull'infrastruttura segna un nuovo passo in avanti, dislocando 10 gigawatt per alimentare la prossima era di intelligenza"*, ha dichiarato **Jensen Huang**.

LA GALOPPATA DI ORACLE

Come noto, nell'Olimpo dell'informatica Nvidia è forse l'azienda che più di tutte, finora, ha beneficiato della corsa all'adozione dell'intelligenza artificiale. Vendendo forniture di Gpu ai grandi sviluppatori di Large Language Model (come OpenAI) ai proprietari di piattaforme social (Meta, xAI) e ai cloud provider di scala mondiale (come Amazon, Microsoft e Google), la società è entrata



nell'esclusivo circolo delle *trillion dollar company,* sfondando la soglia dei mille miliardi di dollari di capitalizzazione di mercato nel giugno del 2023. Due anni dopo, il suo valore era quadruplicato. Se non ci fossero le attuali incertezze sui divieti di import/export da e verso la Cina, i numeri potrebbero lievitare ancora di più.
Ma le Gpu non sono l'unico simbolo del parallelismo tra l'ascesa dell'AI e dell'infrastruttura. Ci sono anche i sistemi hardware e i servizi cloud, due ambiti in cui negli ultimi anni **Oracle** ha visto esplodere la domanda. Nell'ultima trimestrale (quarto trimestre dell'esercizio fiscale chiuso a fine maggio) i ricavi dell'Infrastructure-as-a-Service, cioè del cloud infrastrutturale, hanno segnato una crescita del 52% anno su anno. E per l'anno fiscale 2026 l'azienda si attende per la componente IaaS un incremento del 70%. *"Oracle è sulla buona strada per diventare non solo il più grande fornitore di applicazioni aziendali cloud al mondo, ma anche una delle più grandi aziende di cloud infrastrutturale al mondo"*, ha dichiarato la Ceo, Safra Catz. Per sostenere la domanda di servizi IaaS, la Oracle Cloud Infrastructure si allargherà con ulteriori 47 data center, in via di realizzazione nei prossimi dodici mesi.
Oracle e la sua rete di data center, peraltro, sono coinvolti anche in una vicenda che ultimamente è finita in prima pagina: l'attesa, e ancora in fieri, *vendita del ramo statunitense di TikTok*. Per circa 14 miliardi di dollari, ByteDance cederà il 40% delle attività statunitensi del social network a un consorzio di investitori che include Oracle, la società di private equity Silver Lake e i miliardari Rupert Murdoch e Michael Dell. Non è solo una notizia di interesse per l'utenza del social network cinese. Sarebbe ingenuo ritenere TikTok solamente una piattaforma di intrattenimento e di advertising, e lo si capisce guardando a una delle clausole del contratto di vendita: l'algoritmo di raccomandazione dell'app di TikTok (che orienta pesantemente ciò che gli utenti visualizzano, più di quanto non accada su Facebook o su Instagram) passerà sotto al controllo dei nuovi proprietari e inoltre verrà rimaneggiato cioè ri-sviluppato sulla base dei dati degli utenti statunitensi. E con la supervisione di Oracle. Proseguirà, inoltre, l'opera di trasferimento dei dati: alla fine, tutti dovranno risiedere sui server dell'azienda fondata da Larry Ellison, in data center collocati negli States.

QUALCHE NUMERO E SPUNTI DI RIFLESSIONE...

Quelli citati sono solo esempi dei movimenti di campo, delle alleanze e interconnessioni che stanno plasmando il mercato Ict e anche i mercati finanziari mondiali. Ci sarebbero anche enormi implicazioni ambientali, ma il tema è così complesso da meritare un discorso a parte. Qualche numero ci aiuta a inquadrare meglio il fenomeno. Secondo i calcoli di *Cnbc*, basati su dichiarazioni ufficiali delle aziende in questione, nell'intero 2025 Amazon, Alphabet, Meta e Microsoft spenderanno, complessivamente, 320 miliardi di dollari in tecnologie di intelligenza artificiale e in progetti di potenziamento e costruzione di data center. Ma se le Big Tech hanno un ruolo primario in questa corsa all'infrastruttura, e con esse il modello di fruizione in cloud, non vanno dimenticate le aziende utenti finali e gli ampliamenti dei data center on-premise.
Sommando tutte le componenti del mercato, Gartner stima per i **sistemi di data center** una **spesa mondiale di 475 miliardi di dollari** nell'intero 2025. Il valore è in crescita del 42% sul 2024, quando già si era registrato per questa categoria un incremento del 40% sul 2023. *"Le aziende hanno messo in pausa le nuove spese nette per via del picco di incertezza globale"*, ha commentato **John-David Lovelock**, distinguished vice president analyst di Gartner, *"ma l'effetto è riassorbito dalle iniziative di digitalizzazione di AI e GenAI già in corso. Per esempio, pensiamo che la crescita della spesa in software e in servizi nel 2025 rallenterà a causa di questa 'pausa di incertezza', mentre continuerà l'ascesa degli investimenti in infrastrutture per l'AI, come i sistemi di data center"*. Su quest'ultimo punto, Gartner si aspetta che entro il 2027 gli acquisti di **server ottimizzati per l'AI** varranno il triplo della spesa in server tradizionali: un'ascesa mirabolante, per un categoria di prodotto che fino a quattro anni fa nemmeno esisteva.

notes

IL CAFFÈ DIGITALE

Ricevi gli articoli degli analisti
di **TIG - The Innovation Group**
e resta aggiornato sui temi
del mercato digitale in Italia!

ISCRIVITI ALLA NEWSLETTER MENSILE!

TIG | THE INNOVATION GROUP