TIG | THE INNOVATION GROUP

IL CAFFÈ DIGITALE

GIUGNO 2026

SOVRANITÀ DIGITALE EUROPEA

BISOGNA PASSARE *DALLE PAROLE AI FATTI*

Immagine generata con AI

QUESTO MESE ABBIAMO FATTO COLAZIONE CON...

Alessandro Ferrari, *Dirigente della U.O.S. Servizi Digitali presso l'Ufficio Speciale per l'Amministrazione Digitale,* Regione Campania

NUMERI E MERCATI

AI e produttività: l'Italia può crescere, ma serve una strategia coerente e sistemica

TRASFORMAZIONE DIGITALE

Cloud Repatriation: una scelta architetturale, non un ripensamento

SOMMARIO

Per la Sovranità Digitale europea bisogna passare dalle parole ai fatti

Elena Vaciago, *Research Manager*
TIG - The Innovation Group

Le crescenti tensioni geopolitiche, la concentrazione del potere tecnologico nelle mani di poche aziende globali e l'emergere dell'intelligenza artificiale come fattore strategico stanno trasformando la sovranità digitale in una questione concreta di sicurezza economica, competitività e autonomia politica. Le preoccupazioni non riguardano soltanto la protezione dei dati o la conformità normativa. In gioco c'è la capacità di governi, imprese e organizzazioni europee di mantenere il controllo delle infrastrutture digitali su cui si fondano servizi pubblici, processi industriali e attività economiche. Sempre più spesso, infatti, il tema della dipendenza tecnologica si intreccia con quello della sovranità politica.

IL RISCHIO DEL "KILL SWITCH"

Ripercorriamo alcuni fatti che hanno reso evidente questa realtà:

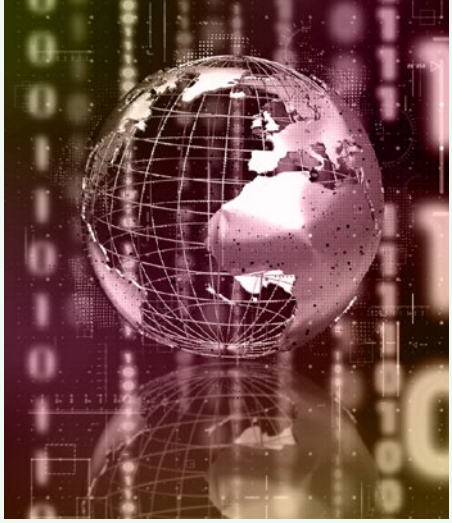
- In *un'audizione* davanti alla commissione del Senato francese il 10 giugno 2025, Microsoft ha ammesso sotto giuramento che le autorità statunitensi potrebbero accedere ai dati dell'UE. Ad Anton Carniaux, consulente legale di Microsoft Francia, è stato chiesto direttamente se potesse garantire sotto giuramento che i dati dei cittadini francesi archiviati nel cloud di Microsoft non sarebbero mai stati trasmessi alle autorità statunitensi senza l'approvazione delle autorità francesi. Carniaux ha risposto chiaramente: "Non, je ne peux pas le garantir".
- Nel maggio 2025, il Procuratore Capo della Corte Penale Internazionale (ICC), Karim Khan, ha perso l'accesso al proprio account di posta elettronica Microsoft a seguito delle sanzioni imposte dall'amministrazione USA. Il blocco dell'account è avvenuto dopo che l'amministrazione Trump ha emesso sanzioni contro i funzionari dell'ICC a seguito dei mandati di arresto per il primo ministro israeliano Benjamin Netanyahu. Il Procuratore è stato costretto a passare al provider svizzero ProtonMail. A causa di questa dipendenza tecnologica, la Corte Penale Internazionale ha avviato una transizione per *abbandonare Microsoft Office* e passare a soluzioni europee open source.
- Pochi mesi dopo, nel luglio 2025, Microsoft ha interrotto temporaneamente i servizi cloud e gli strumenti digitali di Nayara Energy (raffineria indiana parzialmente sostenuta dalla russa Rosneft) a causa delle sanzioni dell'Unione Europea. Dopo *l'azione legale* intentata da Nayara all'Alta Corte di Delhi, Microsoft ha ripristinato i servizi.
- L'inizio del 2026 ha aggiunto ulteriori elementi di riflessione. Dopo una sanzione inflitta dall'Autorità per le Garanzie nelle Comunicazioni per il mancato rispetto delle normative italiane contro la pirateria online, il CEO e co-fondatore di Cloudflare Matthew Prince ventilò pubblicamente l'ipotesi di ridurre o interrompere investimenti e servizi nel nostro Paese. Al di là dell'esito del contenzioso, il caso ha evidenziato quanto possa essere forte il potere negoziale esercitato da pochi operatori globali nei confronti dei singoli Stati.
- Ma è stato soprattutto il caso Anthropic, nel giugno 2026, a rappresentare uno spartiacque simbolico. A soli tre giorni dal lancio dei nuovi modelli di intelligenza artificiale Fable 5 e Mythos 5, l'azienda fu costretta a disabilitarli a seguito di una direttiva del Dipartimento del Commercio degli Stati Uniti relativa ai controlli sulle esportazioni. Non essendo possibile limitare l'accesso soltanto ad alcune categorie di utenti, Anthropic scelse di spegnere completamente i servizi.

Per la prima volta si è materializzato uno scenario che fino a poco tempo fa apparteneva alle analisi teoriche: il cosiddetto **"kill switch"**, ovvero la possibilità che un servizio digitale

strategico, utilizzato da imprese e istituzioni di tutto il mondo, venga sospeso unilateralmente per decisione di un'autorità straniera. Al di là delle motivazioni legate alla sicurezza nazionale americana, il messaggio percepito in Europa è stato chiaro: quando una tecnologia critica è controllata altrove, anche la continuità operativa dipende dalle decisioni prese altrove.
La domanda che oggi devono porsi aziende e istituzioni europee è semplice: possiamo permetterci che infrastrutture, dati e capacità di elaborazione essenziali dipendano interamente da soggetti esterni al nostro perimetro politico e giuridico?

I SEGNALI DEL CAMBIAMENTO CI SONO GIÀ

Nel campo dell'intelligenza artificiale cresce l'interesse verso modelli che possano essere gestiti autonomamente e distribuiti su infrastrutture controllate localmente. In questo contesto, Mistral AI rappresenta oggi il principale campione europeo dell'AI generativa: la società francese, che ha già raggiunto una valutazione miliardaria e ha ottenuto importanti contratti istituzionali, compresa la collaborazione con le forze armate francesi, dimostra che anche in Europa è possibile sviluppare tecnologie avanzate e competitive.
Anche l'Italia sta cercando di ritagliarsi un proprio spazio. Da Domyn, evoluzione di iGenius, ad Almawave con Velvet, fino ai progetti sviluppati dal mondo accademico e industriale nazionale, stanno emergendo iniziative che, pur con dimensioni inferiori rispetto ai colossi statunitensi, contribuiscono a costruire un ecosistema tecnologico europeo più autonomo.
Parallelamente, numerose organizzazioni stanno iniziando a ridurre la dipendenza dai grandi fornitori americani. Il Parlamento europeo ha adottato il motore di ricerca francese Qwant come soluzione predefinita sui propri dispositivi. In Francia migliaia di dipendenti pubblici utilizzano già LaSuite, una piattaforma open



source sviluppata dal governo. Diverse amministrazioni locali nei Paesi Bassi, in Francia e in Germania stanno progressivamente abbandonando Microsoft Office e Google Workspace. Il governo olandese sta trasferendo il proprio codice da GitHub verso repository indipendenti, mentre altre organizzazioni stanno valutando alternative europee ai grandi servizi cloud internazionali.
Si tratta probabilmente soltanto della parte visibile di un fenomeno più ampio. Le politiche sempre più aggressive dell'amministrazione Trump nei confronti delle istituzioni internazionali e dell'Unione Europea hanno accelerato una tendenza che era già presente, ma che oggi sta assumendo una rilevanza strategica.

LA VERA DOMANDA, TUTTAVIA, È SE TUTTO QUESTO SARÀ SUFFICIENTE.

Il problema dell'Europa non è la mancanza di regolamentazione: è la mancanza di scala industriale.
Il 3 giugno 2026 la Commissione Europea ha adottato una proposta di legge sullo sviluppo del cloud e dell'IA, il *Cloud and AI Development Act (CADA)*, introducendo nuovi requisiti di sovranità per i fornitori cloud destinati al settore pubblico e ponendo l'obiettivo di triplicare la capacità europea dei data center entro i prossimi anni. È un passo importante, ma nessuna normativa può sostituire la **presenza di un'industria forte, competitiva e in grado di innovare.** Il paradosso è che l'Europa avrebbe le risorse necessarie per costruirla: ogni anno il continente genera livelli di risparmio superiori a quelli statunitensi, ma una parte significativa di questi capitali continua a finanziare l'innovazione d'oltreoceano anziché sostenere la crescita di campioni tecnologici europei.

IL VERO NODO È CULTURALE PRIMA ANCORA CHE ECONOMICO

Per troppo tempo l'Europa ha interiorizzato l'idea di essere inevitabilmente in ritardo rispetto agli Stati Uniti sul fronte dell'innovazione digitale. Eppure, gli esempi che dimostrano il contrario non mancano: dall'AI al cloud, dalla data governance al platform engineering, il continente dispone di competenze, ricerca e imprese capaci di competere. Ciò che spesso manca è la capacità di scalare rapidamente e di agire come un unico ecosistema.
La frammentazione continua a rappresentare uno dei principali ostacoli. È emblematico il caso del quantum computing: secondo le analisi del Politecnico di Milano, circa il 90% dei fondi pubblici europei destinati al settore viene gestito attraverso iniziative nazionali separate, mentre solo una minima parte è coordinata a livello comunitario. Nel frattempo, le aziende americane continuano a raccogliere capitali privati in misura nettamente superiore.
La sovranità digitale, quindi, non si costruisce soltanto con nuove leggi o con dichiarazioni di principio. **Serve investire, acquistare, sviluppare e far crescere tecnologie europee.** Comprare europeo non è una scelta ideologica: è una scelta economica e industriale, significa mantenere competenze, investimenti e capacità di innovazione all'interno del continente, alimentando un circolo virtuoso che genera nuova crescita, maggiore competitività e ulteriore innovazione. Ricordandoci che la dipendenza tecnologica non è più un rischio teorico: è una vulnerabilità concreta, e la sovranità digitale europea non può più restare soltanto uno slogan. È arrivato il momento di passare dalle parole ai fatti.

Regione Campania: l'AI a supporto dei servizi digitali

Camilla Bellini, *Content & Research Manager*
TIG - The Innovation Group

NEL CORSO DELLA PRIMA EDIZIONE DEL **PAL SUMMIT** ORGANIZZATO DA **TIG-THE INNOVATION GROUP** A NAPOLI IL 19/05/2026, È INTERVENUTO L'**ING. ALESSANDRO FERRARI**, *DIRIGENTE DELLA U.O.S. SERVIZI DIGITALI PRESSO L'UFFICIO SPECIALE PER L'AMMINISTRAZIONE DIGITALE DI REGIONE CAMPANIA*, CHE HA ILLUSTRATO LE SFIDE ED I MODELLI UTILIZZATI PER DISPIEGARE APPIENO IL POTENZIALE DELL'INTELLIGENZA ARTIFICIALE ALL'INTERNO DEI SERVIZI DIGITALI PUBBLICI. PUNTO DI PARTENZA: AVERE UN RICCO PORTFOLIO DI SERVIZI DIGITALI, TERRENO FERTILE PER LE APPLICAZIONI DI AI.

Il concetto di "servizio digitale" non nasce con l'AI, che al contrario deve inserirsi in un percorso e una trasformazione più ampia. Qual è lo stato dell'arte oggi dei servizi digitali in Regione Campania?

Per comprendere il tema dell'adozione dell'AI nei servizi digitali pubblici, occorre certamente prima di tutto fare un punto sullo stato attuale di tali servizi. A riguardo, in Regione Campania abbiamo creato un *catalogo di servizi digitali*, che nei suoi primi quattro anni di vita ha già erogato un totale di 271 servizi, di cui 145 rientrano nell'ambito della digitalizzazione dei procedimenti amministrativi. Questo mostra il grande interesse dimostrato dalla Regione e dalle sue strutture per la digitalizzazione dei propri procedimenti, per ottenere una maggiore velocità, nella gestione e quindi nell'utilizzo dei fondi. Ai 145 servizi digitali si aggiungono poi tutta una serie di utility, di registri digitali e di iscrizione ai corsi che ora avvengono in maniera digitale. Per dare un'idea anche della dimensione economica dell'attività, oggi abbiamo nel complesso 102 servizi digitali che distribuiscono fondi per un valore di ben 1,65 miliardi di euro. Nell'ambito dei servizi digitali gestiamo sia la parte di back-end (con tecnologia low-code) sia quella di front-end (in linguaggio .net versione 6 e successive), creata su un framework di AgID, che ci permette di rappresentare al meglio tutte le informazioni basilari per l'erogazione di tali servizi. Inoltre, da gennaio 2024, abbiamo anche un sistema per la raccolta di questionari di gradimento per capire la qualità percepita dei servizi digitali da parte degli utenti finali e, ad oggi, abbiamo raccolto oltre 39mila questionari, volontari e anonimi, con dei valori di soddisfazione molto interessanti: il 90% degli utenti si dichiara soddisfatto, l'80% consiglierebbe il servizio ad amici e parenti, circa il 40% ammette che il servizio utilizzato ha superato le aspettative, mentre solo una piccola percentuale – il 4,6% – dichiara che ha deluso le aspettative. Questi risultati ci dicono che siamo sulla strada giusta e che certamente potremo migliorare ulteriormente con l'introduzione dell'AI.

Tra i servizi digitali "aumentati dall'AI" che la Regione Campania sta abilitando o ha già messo a terra, ce n'è qualcuno che può mostrare in modo particolare il valore aggiunto dell'AI?

Alessandro Ferrari, *Dirigente della U.O.S. Servizi Digitali presso l'Ufficio Speciale per l'Amministrazione Digitale, Regione Campania*

In questo percorso di digitalizzazione dei servizi pubblici della Regione, l'AI è entrata a partire dal 2023. Per questo motivo, abbiamo già oggi diversi esempi di progetti positivi in questo ambito. Tra questi, un esempio è quello dell'attività di matching, abilitata dall'AI, applicata a ben 2 servizi digitali, quello di adesione all'Albo dei Referee – utilizzato per selezionare revisori indipendenti (i referee appunto) che valutano bandi e progetti di ricerca e innovazione – e quello relativo alla promozione dell'imprenditorialità innovativa nella Regione "Campania Startup 2023", che prevedeva finanziamenti a fondo perduto a supporto delle startup. Grazie all'AI e agli LLM (Large Language Model), siamo riusciti a costruire nel back-office un motore in grado di facilitare e individuare il migliore abbinamento tra i progetti proposti dalle startup per ricevere i finanziamenti e le competenze dei referee, in modo che venisse selezionato, nella rosa dei revisori, quello più idoneo a valutare lo specifico progetto presentato. In questo caso, l'AI è stata applicata a posteriori: in altre parole, prima si è proceduto a svolgere l'abbinamento secondo le modalità tradizionali e solo successivamente abbiamo verificato l'efficacia dell'utilizzo di un motore di AI: ci siamo resi conto che i risultati ottenuti tramite l'AI sono stati davvero molto buoni e, in alcuni casi, ci hanno consentito di effettuare abbinamenti ancor migliori.
Un altro esempio è quello dei "Voucher asili nido", oggi alla quarta edizione. È un servizio digitale dedicato che la Regione ha pensato per le famiglie con bambini da 0 a 36 mesi iscritti in asili nido sul territorio della Campania, le quali possono fare domanda per la richiesta di voucher a rimborso delle spese sostenute. La Regione ha così modo in primis di verificare autonomamente le attestazioni ISEE della famiglia e gestire quindi digitalmente tutto il ciclo di vita delle domande, fino alla rendicontazione delle spese, per l'erogazione del rimborso, con l'intero tracking della pratica consultabile online in ogni istante dai diretti interessati.
Ogni anno, tale servizio di Regione Campania è utilizzato da circa 3mila famiglie, a cui vengono rimborsati circa 400 euro al mese per 11 mesi l'anno, anche in aggiunta al cosiddetto "Voucher asili nido statale", erogato alle famiglie dall'INPS. Anche in questo caso, l'AI ci aiuta molto. La documentazione di rendicontazione per circa 3mila famiglie genera infatti annualmente 60mila documenti contabili, che sono quelli redatti ed emessi dai diversi asili nido, pubblici, privati e parificati; si tratta quindi di documenti molto disomogenei tra loro. Grazie a un core di AI da noi addestrato, riusciamo a estrapolare dalle fatture che vengono presentate le informazioni rilevanti per lo sviluppo della pratica, verificandone la coerenza con la domanda di liquidazione, diminuendo così le tempistiche e gli errori nella gestione di ciascuna domanda.
Dopo la sperimentazione di quest'anno, intendiamo adottare questo core di AI anche per altri casi simili e altre tematiche. D'altra parte, il nostro Ufficio Speciale ha proprio tra le sue declinazioni quella di introdurre e applicare l'AI, in tutti gli ambiti gestiti e di competenza dalla Regione.

AI e produttività: l'Italia può crescere, ma serve una strategia coerente e sistemica

Sergio Patano, *Event & Research Manager*
TIG - The Innovation Group

LO STUDIO DELLA BANCA D'ITALIA MISURA L'ADOZIONE DELL'AI NELLE IMPRESE E IL SUO POTENZIALE SULLA PRODUTTIVITÀ: OPPORTUNITÀ ENORMI, BARRIERE ANCORA ALTE.

Il **32%** delle imprese italiane con almeno 20 addetti utilizzava strumenti di intelligenza artificiale all'inizio del **2026**. Un dato in crescita rispetto al **27%** del 2025 e già rispetto al 2023, ma che racconta solo una parte della storia, perché quel 32% include chi usa l'AI in modo sperimentale e occasionale. Le aziende che dichiarano un'integrazione **intensiva** nei processi aziendali sono solo il **5%** del totale. È questa la fotografia che emerge dall'indagine **Invind** della **Banca d'Italia**, presentata nel documento *L'adozione dell'intelligenza artificiale: effetti su produttività e politiche a sostegno.*
Dal confronto europeo su aziende con più di dieci addetti emerge che l'Italia è indietro di **4 punti percentuali** rispetto alla media UE e di quasi **10 punti** rispetto alla Germania.

COME E DOVE LE IMPRESE USANO L'AI

Le attività in cui l'AI è più diffusa sono quelle **commerciali**, seguite dalla produzione di beni e servizi e dalla gestione degli adempimenti amministrativi. Tra le aziende che utilizzano applicazioni di **genAI (30%)** la funzione prevalente è la generazione di testi; poco oltre la metà ricorre anche ad altre applicazioni, come chatbot per clienti o dipendenti, agenti di AI e strumenti per la generazione di codice.
Il quadro della **governance interna** è altrettanto frammentato. Nella Smart Manufacturing Survey 2026 di TIG emerge che nel **48%** dei casi l'AI viene sviluppata attraverso iniziative isolate di singole funzioni aziendali, mentre solo il **28%** delle imprese dispone di una strategia formalizzata. Oltre la metà delle aziende manifatturiere non è ancora in grado di evidenziare benefici concreti derivanti dall'adozione.

IL PARADOSSO DELLA PRODUTTIVITÀ: GIÀ VISSUTO CON L'ICT

Nel breve periodo, i dati confermano un'assenza di effetti sistemici: il **70%** delle imprese che hanno adottato l'AI dichiara che l'adozione non ha finora influenzato la produttività del lavoro. Le stime econometriche della Banca d'Italia, condotte su un panel bilanciato di circa **900 imprese** nel periodo **2022-2026**, non identificano effetti sistematici sul fatturato per addetto, sull'occupazione o sugli investimenti.
Questo è come il **Paradosso di Solow,** secondo cui l'aumento rapido degli investimenti in tecnologie ICT degli anni '80 e '90 non produsse un'immediata accelerazione della produttività aggregata. L'apparente paradosso rifletteva la necessità di ridisegni organizzativi e investimenti immateriali che solo col tempo maturarono.
Le imprese intervistate sembrano esserne consapevoli, tanto che la **metà** prevede un impatto positivo sulla produttività nel prossimo triennio, mentre il **35%** non si aspetta variazioni.

IL POTENZIALE DI LUNGO PERIODO: QUANTO VALE PER L'ITALIA

È sul medio-lungo termine che i numeri diventano significativi. Le simulazioni macroeconomiche elaborate dalla Banca d'Italia (Bertolotti et al., 2026), calibrate sulla struttura produttiva italiana, stimano che l'adozione dell'AI potrebbe generare un incremento della produttività del lavoro compreso tra **0,2 e 1,1 punti percentuali annui** su un orizzonte decennale, a seconda dello scenario di adozione (lenta, media, rapida). Nello scenario di adozione **rapida**, paragonabile a quella dei telefoni cellulari, il guadagno annuo stimato sale all'**1,1%**; nello scenario **lento**, analogo alla diffusione dell'elettricità, si ferma allo **0,2%**.
Scomponendo il contributo settoriale, il maggior apporto alla crescita del PIL verrebbe dalla **manifattura** (+2% in 10 anni), seguita dal **commercio** (+1%) e dalle **attività professionali** (+0,8%). Si stima inoltre un lieve effetto

Foto ©unsplash.com

positivo sull'occupazione, dell'ordine di circa un decimo di punto in tutti e tre gli scenari.

LE BARRIERE: NON BASTA IL SUSSIDIO

La principale ragione per cui le imprese italiane di tutte le classi dimensionali non adottano l'AI è la **carenza di competenze**. A questo si sommano la scarsa integrazione dei dati, l'incertezza normativa, i costi fissi di implementazione e i rischi percepiti in materia di privacy.

Il punto critico, sottolineato con forza dagli economisti della Banca d'Italia, è che questi ostacoli non possono essere rimossi con sussidi generici. Una politica efficace richiede una **strategia coerente e sistemica**, articolata su tre leve: stimolare la domanda di applicazioni AI (anche tramite voucher selettivi e programmi pilota); rafforzare l'offerta di soluzioni verticali per le PMI, colmando il cosiddetto "**missing middle**" tra grandi piattaforme generaliste e implementazioni su misura accessibili solo alle grandi imprese; intervenire sui fattori abilitanti, ossia certezza normativa, condivisione dei dati, accesso alle infrastrutture di calcolo avanzato.

Su quest'ultimo fronte l'Italia dispone di asset rilevanti (il supercalcolatore **Leonardo** presso **Cineca** a Bologna, integrato nella rete europea **EuroHPC JU**, e il progetto **IT4LIA**-Italy for Artificial Intelligence, con un investimento totale di circa **430 milioni di euro**) ma la sfida principale resta trasformare infrastrutture di eccellenza in risorse concretamente accessibili anche alle PMI.

UN CONFRONTO CHE NON CONSOLA

Nel 2023, secondo stime **OCSE**, l'Italia ha investito in AI pubblicamente circa **5,2 miliardi di euro**, pari allo **0,25% del PIL**: un dato inferiore alla media dei principali partner europei (Germania **0,45%**, Francia **0,30%**, Danimarca **0,59%**). Il finanziamento cumulato dei Competence Center italiani nel periodo **2019-2025** è stato pari a **186 milioni di euro**, a fronte di entrate pubbliche nel 2023 di **2,2 miliardi per la Germania** e di **320 milioni di sterline in UK**.

I numeri parlano chiaro: l'Italia ha le condizioni strutturali per beneficiare della transizione AI, un tessuto manifatturiero forte, filiere di eccellenza, competenze ingegneristiche, ma sconta un ritardo cronico negli investimenti immateriali. L'Italia è l'unico paese europeo in cui gli investimenti in beni materiali continuano tuttora a superare quelli in beni immateriali, una tendenza che altrove si è invertita già prima del **Covid**.

L'ANALISI: IL TEMPO È UNA VARIABILE CRITICA

Le imprese italiane per sfruttare il potenziale dell'AI devono investire in riorganizzazione, formazione e governance dei dati, senza i quali l'adozione tecnologica resta superficiale e i benefici non emergono.

Per l'Italia, il paradosso più pericoloso non è quello di Solow, ma quello di un paese che conosce bene le criticità (competenze, scarsa strategia, incentivi sbilanciati sul materiale) ma non agisce in modo sistemico. I prossimi due/tre anni, con la piena operatività del quadro normativo europeo (AI Act) e la maturazione delle prime AI Factory, saranno decisivi. Chi avrà già iniziato a costruire le complementarità organizzative avrà un vantaggio difficile da colmare

L'obbligo di categorizzazione, come destreggiarsi nell'ambito della prossima scadenza ACN

Valentina Frediani, *Founder & CEO*
Colin & Partners

OGNI SCADENZA SEGNA UNA TAPPA IMPORTANTE NEL PROCESSO DI CONFORMITÀ RISPETTO ALLA DIRETTIVA NIS2 E, IN SEGUITO ALLA FASE DI REGISTRAZIONE E COINVOLGIMENTO DEI SOGGETTI INTERESSATI, OGGI SIAMO DAVANTI ALL'INIZIO DI UNA NUOVA FASE CHE CONSENTIRÀ DI PIANIFICARE ATTENTAMENTE LE PROSSIME ATTIVITÀ DI MONITORAGGIO.

Attualmente molte aziende italiane si trovano davanti ad un'altra scadenza da non sottovalutare, stiamo parlando della scadenza del **30 giugno 2026** in merito alla **Categorizzazione** dei servizi NIS2. In questo caso, la finalità di ACN è ben chiara: costruire una mappa essenziale dei servizi critici.
Ciò che differenzia questa scadenza rispetto alle precedenti direttive NIS2 è l'ampliamento del bacino dei settori coinvolti. Questo è un aspetto che tende a passare inosservato, ma è il motivo per cui molte organizzazioni hanno scoperto solo recentemente di rientrare in questo perimetro e, di conseguenza, di doversi conformare alla norma. Questo le ha portate a doversi interfacciare con la normativa e gli adempimenti richiesti in tempi ridotti. Nello specifico, si fa riferimento soprattutto a enti che forniscono servizi o prodotti a strutture soggette alla disposizione, le quali, possono consolidare la loro inattaccabilità solo se anche i loro fornitori possiedono adeguati livelli di sicurezza.
Scendendo nel dettaglio, è opportuno capire cosa richiede ACN per la scadenza imminente di fine giugno. Osserviamo che, in prima battuta, l'autorità necessita di conoscere i servizi erogati dai **soggetti NIS2 e ciò significa andare** a identificare i processi aziendali che possono avere un impatto sulla continuità operativa.
A seguire, ritiene rilevante individuare le dipendenze tecnologiche e di fornitura, al fine di comprendere quanto un ipotetico incidente possa influire sull'interruzione del servizio importante o essenziale. Questo fa emergere anche la necessità di fare una stima delle possibili conseguenze in seguito al verificarsi di incidenti cyber. Infine, lo scopo sarà anche consentire una riflessione rispetto alle priorità di vigilanza e gestione del rischio. È sempre opportuno tenere presente che parlare di obbligo di categorizzazione significa parlare di una dichiarazione ufficiale verso le autorità. Si tratta quindi di un'operazione che richiede la massima attenzione da parte di tutti i soggetti NIS2 essenziali ed importanti coinvolti nel processo di compilazione.
Il **modello di Categorizzazione** è strutturato partendo dalle attività e dai servizi che un soggetto NIS2 svolge. In merito a questo, ACN ha fornito in maniera precisa e puntuale alcune macroaree di riferimento a cui dovranno essere associati attività e servizi rilevanti per il singolo soggetto e dovrà essere conferito un grado di rilevanza per ciascuna di queste macroaree. È importante tenere in considerazione che questo processo non deve avere solo uno sguardo interno all'ente, ma deve essere orientato anche verso l'esterno prendendo in considerazione l'eventuale livello d'impatto di queste attività e servizi verso i clienti.
Il template di ACN attribuisce una **categoria di rilevanza** rispetto all'eventualità in cui un'attività o un servizio possa essere al centro di una compromissione, tale da influire sulla capacità del soggetto di assicurare l'erogazione dei servizi. Per ACN esistono quattro categorie di rilevanza e l'autorità assegna preventivamente la categoria che ritiene più opportuna, ma nell'ambito di questa scadenza le organizzazioni hanno la possibilità di discostarsi dall'indirizzo iniziale fornito da ACN. In questa circostanza, sarà opportuno specificare la motivazione di tale scelta e, in caso di necessità, documentare questo tipo di valutazione.
La **mappatura** delle attività e dei servizi rappresenta un'attività articolata e si rivela un'operazione trasversale perché coinvolge più aree aziendali, ciò comporta dover avere ben chiaro chi coinvolgere in questo processo e come reperire le informazioni necessarie alla

compilazione dei campi. In quest'ottica è fondamentale munirsi di una metodologia chiara e strutturata, in modo da poter procedere con ogni step in modo coerente e lineare.
Il posizionamento all'interno di una delle categorie è il requisito essenziale per applicare un criterio di supervisione e controllo adeguato. Ovvero, più un ente è strategico per l'operatività del Paese e superiore sarà l'impegno da parte di ACN nel prevenire e fronteggiare i possibili incidenti informatici.
In conclusione, è opportuno affermare che con il tema della Categorizzazione siamo davanti ad un momento chiave in ambito della normativa NIS2 e che, come tale, richiede un elevato livello di accuratezza.

Cloud Repatriation: una scelta architetturale, non un ripensamento

Vincenzo Calabrò, *Information Security Officer*
Ministero dell'Interno

NEGLI ULTIMI ANNI HA ACQUISITO UNA RILEVANZA CRESCENTE IL TEMA DELLA CLOUD REPATRIATION, OVVERO IL TRASFERIMENTO DI DATI E APPLICAZIONI DAL CLOUD PUBBLICO VERSO AMBIENTI ON-PREMISES, CLOUD PRIVATI O SOLUZIONI DI COLOCATION. L'ARTICOLO DI VINCENZO CALABRÒ ESPLORA LE MOTIVAZIONI, I RISCHI, LE MODALITÀ OTTIMALI.

Il **rientro selettivo dal public cloud** è tornato al centro dell'agenda dei CIO e dei CISO. Proviamo a capire quali sono i fattori scatenanti e a non confondere un cambiamento di perimetro con un aumento della sicurezza. Per oltre un decennio, la migrazione verso il cloud pubblico è stata considerata la direzione naturale di qualunque strategia infrastrutturale IT. Negli ultimi anni, tuttavia, un fenomeno complementare ha acquisito una rilevanza crescente: il **cloud repatriation**, ovvero il trasferimento di dati e applicazioni dal cloud pubblico verso ambienti on-premises, cloud privati o soluzioni di colocation. È necessario chiarire subito un equivoco. Il repatriation non rappresenta un rifiuto del cloud, ma una sua maturazione: secondo le rilevazioni di settore (in particolare i report annuali come lo *State of the Cloud di Flexera*), la **quota di organizzazioni che riportano selettivamente i workload è ai massimi storici**, nonostante la spesa complessiva per il cloud sia in aumento. Si tratta, dunque, di una ricalibrazione, non di un'inversione di rotta.

I DRIVER STRATEGICI

Analizziamo i quattro principali fattori che ricorrono con regolarità nelle decisioni di repatriation. Il primo è di **natura economica**: i modelli di pricing *usage-based*, ottimali per la domanda elastica, si rivelano spesso strutturalmente più onerosi per i *workload steady-state* a utilizzo prevedibile e continuativo; a ciò si somma il peso degli *egress fees*, che incidono in modo non trascurabile sul Total Cost of Ownership (TCO) effettivo. Il secondo riguarda il **controllo delle prestazioni e della latenza**, particolarmente rilevante per le applicazioni con forte *data gravity*. Il terzo aspetto attiene alla **compliance e alla *data sovereignty***: l'esigenza di garantire che i dati restino soggetti alla giurisdizione del territorio in cui risiedono spinge verso un controllo più diretto della loro collocazione e delle architetture di riferimento adottate. Il quarto è il ***vendor lock-in***, ovvero la dipendenza da API, formati e servizi proprietari che rende oneroso, dal punto di vista tecnico e contrattuale, il cambio di provider. Questi fattori raramente agiscono in modo isolato. Un'analisi più approfondita del problema del lock-in evidenzia come la dipendenza si accentui man mano che le risorse migrano dall'on-premises al cloud, esponendo l'organizzazione a un rischio di portabilità che si manifesta nel momento in cui è necessario cambiare collocazione, spesso senza una pianificazione adeguata.

REPATRIATION E SICUREZZA: SPOSTARE IL RISCHIO, NON ELIMINARLO

Dal punto di vista della sicurezza, l'errore più comune è quello di pensare che riportare i dati "in casa" li renda automaticamente più sicuri. Il repatriation modifica la superficie d'attacco e ridistribuisce le responsabilità, ma non riduce di per sé il rischio. Nel public cloud vige uno *shared responsibility model* in cui il provider si occupa della sicurezza dell'infrastruttura sottostante. Riportando un workload on-premises, **l'organizzazione riassume integralmente gli oneri che in precedenza erano in parte delegati**: *patching* dell'hardware, sicurezza fisica, ridondanza, capacità di *detection* e response. Per un CISO, il problema principale non è dove i dati sono più sicuri, ma dove l'organizzazione è effettivamente in grado di sostenere il livello di controllo richiesto, con le competenze e i budget a disposizione. Anche dal punto di vista della data *sovereignty* il quadro è meno lineare di quanto possa sembrare. Mantenere i dati all'interno di una determinata giurisdizione può ridurre

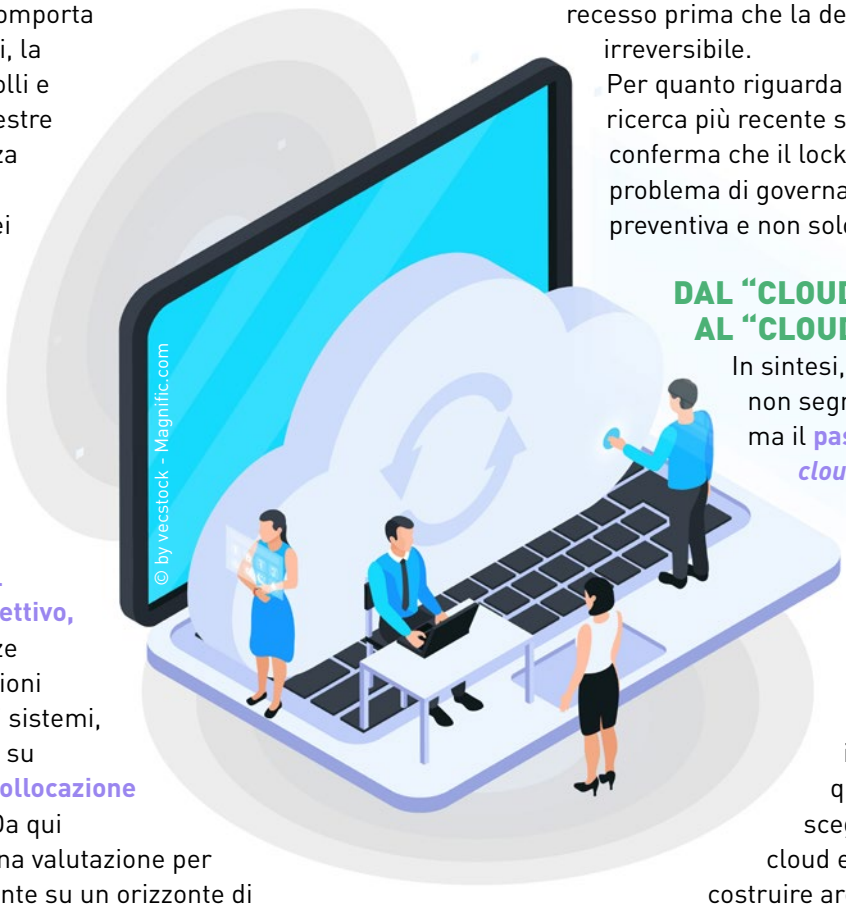
alcune esposizioni legali e regolamentari, ma le soluzioni che lo garantiscono, dalle architetture di riferimento alle misure crittografiche, impongono vincoli tecnologici ed economici, come un aumento dei costi computazionali, che devono essere presi in considerazione nella decisione finale. Va inoltre considerato che la fase di transizione è essa stessa un momento di rischio: ogni migrazione comporta la movimentazione dei dati, la riconfigurazione dei controlli e l'apertura di potenziali finestre di esposizione. La sicurezza dei workload rimpatriati deve essere reintegrata nei framework di governance esistenti e non deve essere ricostruita ex novo in modo frammentario.

UN METODO DECISIONALE

La letteratura e la prassi convergono su un punto: **il repatriation efficace è selettivo, non ideologico**. Le evidenze indicano che le organizzazioni raramente riportano interi sistemi, ma piuttosto intervengono su **workload specifici la cui collocazione non risulta più ottimale**. Da qui l'opportunità di adottare una valutazione per singolo workload, idealmente su un orizzonte di dodici-trentasei mesi, che classifichi l'elasticità effettiva del carico, modelli il TCO con sensibilità a *egress*, traffico *cross-zone*, premi sui *managed services* e quantifichi l'*effort* di uscita.

Quest'ultimo elemento è decisivo. Una ***exit strategy* andrebbe progettata fin dalla fase di adozione**, privilegiando la portabilità, la containerizzazione e gli standard aperti per limitare il rischio di lock-in. In questa direzione, i framework predittivi del rischio di lock-in forniscono un supporto concreto e quantitativo: pesando fattori quali i costi di servizio, il *data transfer*, le funzionalità di sicurezza, l'aderenza alla compliance e le integrazioni tecniche, consentono di stimare il grado di dipendenza da un provider e i costi di un eventuale recesso prima che la decisione diventi irreversibile.

Per quanto riguarda la gestione, la ricerca più recente sugli ecosistemi cloud conferma che il lock-in è prima di tutto un problema di governance e di mitigazione preventiva e non solo di natura tecnica.



DAL "CLOUD-FIRST" AL "CLOUD-APPROPRIATE"

In sintesi, il cloud repatriation non segna la fine del cloud, ma il **passaggio da una logica *cloud-first* a una logica *cloud-appropriate***, in cui ogni workload viene collocato dove si ottiene il miglior equilibrio tra costo, prestazioni, controllo e conformità. Per i CISO e i CIO la questione non è scegliere tra il public cloud e l'on-premises, ma costruire architetture *hybrid* e *multi-cloud* effettivamente governabili, dotate di *exit strategy* credibili e di una postura di sicurezza coerente, a prescindere dal perimetro. In questa prospettiva, il repatriation è uno strumento di flessibilità strategica da tenere a disposizione ed esercitare con disciplina analitica, non una correzione di rotta dettata dal pentimento.

La gestione degli incidenti nella NIS 2

Federico Lucia, *Direttore Didattico e Board Member di* ANRA,
CEO di Fortaris S.r.l.

LA NIS 2 — RECEPITA IN ITALIA CON IL D.LGS. 138/2024 — HA SPOSTATO IL BARICENTRO DELLA CYBERSECURITY DAL PIANO DELLE INTENZIONI A QUELLO DELLA RESPONSABILITÀ CONCRETA. TRA I SUOI PILASTRI, LA GESTIONE DEGLI INCIDENTI E L'OBBLIGO DI NOTIFICA RAPPRESENTANO L'AREA DI MAGGIORE IMPATTO OPERATIVO.

Non si tratta di adempiere a un form burocratico: si tratta di allertare un meccanismo di risposta nazionale e sovranazionale e di saper dimostrare — in tempo reale, sotto pressione — che l'organizzazione è pronta a riconoscere un evento avverso, contenerlo ed attivare le procedure di escalation. Questo articolo propone una lettura pratica, correlando le disposizioni NIS 2 con i framework internazionali e con i temi della cyber resilience, del GDPR e della forensics readiness.

COSA CHIEDE DAVVERO LA NIS 2 SULLA GESTIONE DEGLI INCIDENTI

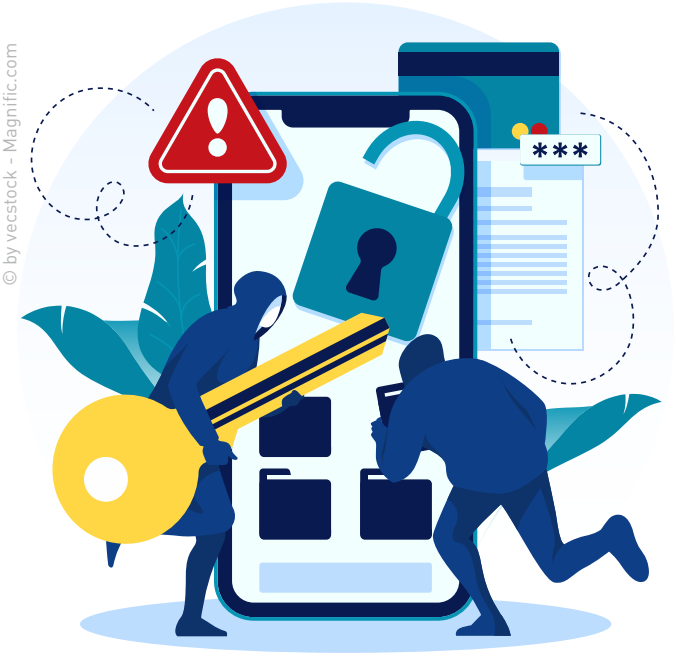
L'art. 25 del D.Lgs. 138/2024 stabilisce obblighi precisi e **tempistiche stringenti: pre-notifica entro 24 ore, notifica completa entro 72 ore** e **relazione finale entro un mese** al CSIRT Italia. Ma la norma va oltre la notifica: impone che le organizzazioni dispongano preventivamente di policies (che in italiano siamo soliti tradurre in "politiche" ma che preferisco definire "regolamenti generali e specifici", per disambiguare il termine e la reale applicazione pratica), procedure e capacità operative adeguate. È il cuore del problema: molte aziende costruiscono il processo di incident management solo quando un incidente le costringe a farlo, sulla scorta del pensiero "non capiterà mai nulla" o "sappiamo cosa fare anche senza doverlo mettere nero su bianco". La soglia di **"impatto significativo"** (art. 25, comma 4) richiede una valutazione su utenti coinvolti, durata, propagazione geografica e danno economico — da condurre nelle prime ore, quando le informazioni sono ancora incomplete. ACN fornisce linee d'indirizzo, ma spetta all'organizzazione determinare la significatività di un impatto.

ISO 27035 E NIST SP 800-61: IL PROCESSO PRIMA DELLA NORMA

La NIS 2 stabilisce **cosa** fare e **quando**; i framework internazionali dicono **come**. La **ISO/IEC 27035** descrive un ciclo di vita in cinque fasi — pianificazione, rilevamento, valutazione, risposta e lesson learned — che, oltre a definire la migliore pratica per la gestione degli incidenti e per la tutela dell'organizzazione, costituisce la spina dorsale su cui innestare gli obblighi normativi. Il **NIST SP 800-61 Rev. 2** offre un approccio complementare, più operativo, organizzato in preparazione, rilevamento e analisi, contenimento-eradicazione-ripristino e attività post-incidente; è particolarmente utile per strutturare **playbook di risposta** per tipologia di evento: ransomware, data breach, DDoS, compromissione di account privilegiati. La sintesi operativa: adottare uno di questi framework (o, meglio ancora, integrarli), documentarlo coerentemente con ISO/IEC 27001 (contromisure dell'Annex A da 5.24 a 5.28 e 6.8) e mapparlo sulle scadenze di notifica NIS 2 (e non solo), ottenendo un impianto capace di tutelare l'organizzazione da impatti economici, operativi, reputazionali e strategici e che, al contempo, dimostra la propria capacità di soddisfare autorità, enti regolatori e stakeholder.

INCIDENTI E DATA BREACH: LA DOPPIA NOTIFICA

La sovrapposizione tra incidente NIS 2 e violazione di dati personali ai sensi del GDPR è un aspetto che management e CISO non possono sottovalutare. Un attacco ransomware o un accesso non autorizzato coinvolgono spesso informazioni personali, attivando contestualmente la notifica all'ACN e al Garante Privacy (GDPR, art. 33) — quest'ultima con finestra di 72 ore, ma destinatari, contenuti e valutazioni diverse. Questo



impone un **processo integrato**: Titolare del trattamento, DPO (ove presente) e CISO devono condividere la stessa catena di escalation e un linguaggio comune di classificazione della gravità. La valutazione NIS 2 guarda all'impatto sul servizio; quella GDPR al rischio per i diritti degli interessati: due lenti diverse sullo stesso evento. Il Piano di Risposta agli Incidenti deve prevedere un capitolo dedicato alla **doppia notifica** (tripla, se consideriamo anche gli stakeholders interessati dalla violazione), con template predisposti e una matrice di escalation che coinvolga CISO, DPO, Legal, Comunicazione e Top Management.

DALLA RISPOSTA ALL'INCIDENTE ALLA GESTIONE DELLE CRISI E ALLA CYBER RESILIENCE

Non tutti gli eventi diventano incidenti e non tutti gli incidenti diventano crisi: tuttavia, ogni crisi ha avuto il suo incidente iniziale. La differenza non è solo di scala: è **organizzativa**. Un incidente viene gestito dai team tecnici; una crisi coinvolge il vertice aziendale, impatta la reputazione e richiede capacità decisionali ben oltre il SOC: è in gioco la sopravvivenza dell'organizzazione. Il concetto chiave è la **cyber resilience**: la capacità di anticipare, resistere, assorbire e adattarsi garantendo la continuità delle funzioni critiche. La gestione degli incidenti NIS 2 si connette con il **Business Continuity Management** (la cui massima espressione è rappresentata dalla ISO 22301 e dal framework del Disaster Recovery Institute) e con i piani di disaster recovery, che devono essere attivabili in tempi certi. La soglia di escalation al Crisis Management Team va definita in anticipo — in termini di impatto sui servizi critici, durata e coinvolgimento di terze parti — e non rimessa alla valutazione del momento, spesso soggettiva e condizionata da fattori fortemente emotivi. Le organizzazioni mature integrano già la risposta agli incidenti cyber nella gestione delle crisi, con scenari definiti ed esercitazioni tabletop, simulati o effettivi. Questo è lo spirito della NIS 2: un **sistema di gestione continuo e testato**, non un adempimento spot. Il rischio cyber non è soltanto cyber ma ha impatti trasversali, operativi, strategici: questa è la grande sfida – anzitutto culturale – delle organizzazioni.

LA FORENSICS READINESS: L'INVESTIMENTO CHE FA LA DIFFERENZA

C'è un tema che rimane spesso in secondo piano ma risulta determinante nella pratica: la **forensics readiness**. Per forensics readiness si intende la capacità di raccogliere, preservare e rendere disponibile la prova digitale in modo tempestivo e giuridicamente utilizzabile — prima che un incidente si verifichi. Dal regolatore al Legal, talvolta alla magistratura, le domande arrivano sempre immediatamente: cosa è successo, da quando, chi ha avuto accesso, quali dati sono stati coinvolti. Rispondere con evidenze affidabili richiede la ricostruzione della timeline, log completi, SIEM configurati per la retention adeguata e chain of custody documentata. I riferimenti tecnici — **ISO/IEC 27037** (raccolta e preservazione delle prove digitali) e **NIST SP 800-86** (integrazione delle tecniche forensi nella risposta agli incidenti) — forniscono le linee guida per costruire questa capacità. Per le organizzazioni soggette a NIS 2, non è più opzionale: è la condizione che rende possibile una notifica accurata, una risposta GDPR fondata e una difesa legale credibile.

SIETE PRONTI? LE DOMANDE CHE OGNI CISO DOVREBBE SAPER RISPONDERE

Prima di ritenersi conformi, Management e CISO dovrebbero verificare di poter rispondere positivamente a queste domande:

- Esiste un Piano di Risposta agli Incidenti approvato, con ruoli, responsabilità e procedure definite per i principali scenari di minaccia?
- Le tempistiche NIS 2 (pre-notifica 24h, notifica 72h, relazione finale 1 mese) sono tradotte in procedure operative con trigger chiari e template predisposti?
- Il processo di escalation da incidente a crisi è formalizzato, con soglie di attivazione del Crisis Management Team condivise con il Top Management?
- Esiste un protocollo integrato per la doppia notifica (NIS 2 verso ACN + GDPR verso il Garante) che coinvolge Titolare, DPO ove presente, CISO, Legal e Comunicazione?
- I piani di Business Continuity e Disaster Recovery sono collegati agli scenari di incidente cyber e testati periodicamente?
- L'infrastruttura di log management garantisce retention adeguata e integrità delle evidenze a fini forensi?
- Il personale coinvolto nella risposta — tecnico, operativo, manageriale e legale — ha partecipato ad almeno un esercizio tabletop nell'ultimo anno?
- Esiste un registro degli incidenti aggiornato, che documenti anche gli eventi sotto soglia, a supporto del miglioramento continuo?

Quantum computing, meno hype e più costruzione: il vantaggio vero sarà industriale

Gianluca Dotti, *Giornalista*
TIG - The Innovation Group

TRA SPINTA GEOPOLITICA, RICERCA APPLICATA E PRIMI CASI D'USO, IL QUANTUM COMPUTING ENTRA NELLA FASE IN CUI CONTANO LE FILIERE, LE COMPETENZE E LA CONTINUITÀ – POLITICA, DI INVESTIMENTI E DI VISIONE – PIÙ CHE LA CORSA ALL'ANNUNCIO MEDIATICO. NE PARLIAMO ANCHE L'8 LUGLIO AL QUANTUM COMPUTING SUMMIT DI MILANO.

Per il **quantum computing** il momento della svolta definitiva non è ancora in vista, ma prosegue con grande dinamismo la fase di costruzione. È questa una possibile chiave per leggere una fase in cui il settore si avvicina all'agognato **vantaggio quantistico** – ossia il momento in cui, per almeno alcune applicazioni, il quantum risulterà conveniente rispetto alla computazione tradizionale – ma non può prescindere da tutti i passaggi che separano la dimostrazione di laboratorio dall'utilità industriale.
Negli Stati Uniti la cornice è ormai chiara. Con il recente *editto* di Donald Trump, la Casa Bianca ha scelto di **trattare il quantum come una priorità strategica**, industriale e di sicurezza nazionale. Il testo parla esplicitamente di una mobilitazione di governo per sostenere commercializzazione, manifattura, ricerca e applicazioni, insieme alla transizione verso la crittografia post-quantistica. Il messaggio è politico: la computazione quantistica non è più soltanto una promessa scientifica, ma **un terreno di competizione tecnologica e industriale.**
In Europa il quadro appare più lento e meno definito. Il settore avrebbe bisogno di un riferimento comune più rapido, capace di sostenere ricerca, trasferimento tecnologico, infrastrutture e investimenti in modo più coerente. Proprio per questo il confronto su scala europea non può più limitarsi alla dimensione scientifica e alle fasi iniziali del trasferimento tecnologico: **serve una visione industriale condivisa**, se si vuole evitare che il continente resti spettatore nella fase in cui il quantum comincia a tradursi in capacità applicativa reale.

UNA DISCUSSIONE ECOSISTEMICA, LUNGO TUTTA LA FILIERA

In questo scenario si inserisce il **Quantum Computing Summit 2026**, in programma l'8 luglio a Milano, a Palazzo Gio Ponti, sede di Assolombarda. L'evento, organizzato da TIG – The Innovation Group in collaborazione con Cefriel, riunirà ospiti nazionali e internazionali tra imprese, istituzioni, provider tecnologici, centri di ricerca e attori dell'innovazione, con l'obiettivo di fare il punto sullo stato dell'arte del quantum computing e sulle sue prospettive di sviluppo in Italia e in Europa. Più che una celebrazione di una tecnologia affascinante dal punto di vista concettuale ma ancora al suo stato primitivo di sviluppo effettivo, un'analisi multi-stakeholder delle condizioni necessarie per trasformarla in valore per le imprese.
Il programma del summit conferma questa impostazione: il quantum non è più soltanto un tema da laboratorio, ma una questione di ecosistema – un ecosistema, per funzionare, richiede continuità, visione e coordinamento. Parlare oggi di *quantum advantage* ha senso solo se si evita l'idea di una soglia magica e imminente. Il vantaggio quantistico non arriverà come un interruttore acceso all'improvviso, ma come **una sequenza di avanzamenti progressivi**, diversi a seconda del problema affrontato. In alcune aree come finanza, chimica computazionale e ottimizzazione, i primi risultati concreti stanno emergendo con forza; in altri ambiti, come la crittografia e le applicazioni a cascata verso le PMI, serve ancora sviluppo e consolidamento tecnologico.
È proprio per questo che la narrativa dell'*ora o mai più* rischia di essere fuorviante, a meno che non si intenda che **per guadagnare una posizione da protagonista non si può indugiare oltre.** In senso applicativo, invece,

il quantum computing non chiede hype ma pazienza strategica. Oggi la vera partita si gioca sulla capacità di costruire piattaforme hardware più affidabili, software più maturi, modelli di accesso più aperti e competenze diffuse in grado di collegare ricerca, impresa e industria.

LA CORSA ALLA SCALATA DEI QUBIT

Un aspetto cruciale riguarda la **qualità delle macchine**, non solo il numero di qubit. Due processori con numeri simili possono avere capacità molto diverse in funzione della **qualità delle operazioni**, della **connettività interna**, del **tempo di coerenza**, della **profondità dei circuiti eseguibili** e delle **tecniche di controllo del rumore**, tutti fattori che incidono sulla quantità di computazione utile ottenibile prima che gli errori rendano il risultato inutilizzabile. Questo spiega anche perché la questione della correzione degli errori sia così importante. Oggi gran parte del lavoro più promettente si muove ancora su sistemi rumorosi, nei quali si tenta di estrarre valore attraverso tecniche di mitigazione degli errori e algoritmi ibridi. Il salto vero arriverà quando le **architetture fault tolerant** permetteranno di eseguire calcoli molto più lunghi, affidabili e ripetibili, aprendo la strada a **un utilizzo meno sperimentale e più industriale della tecnologia.**

Il settore è oggi chiamato a dimostrare il principio della scalabilità e la promessa alla ripetibilità: questo significa lavorare su supply chain, standard, formazione, cloud, integrazione con l'HPC e capacità di attrarre investimenti di lungo periodo. E anche riconoscere che la tecnologia quantistica non sostituirà in blocco i sistemi tradizionali, ma si affiancherà a essi in architetture ibride, dove computer classici, acceleratori e **Quantum Processing Unit** (QPU) saranno chiamati a collaborare in funzione del problema, **senza che il quantum scalzi i processori tradizionali CPU e GPU**.

Le prime applicazioni realistiche, infatti, sembrano muoversi proprio in questa direzione. I casi più interessanti riguardano anche segmenti dell'analisi dati e scenari in cui il quantum può operare in tandem con l'HPC e l'intelligenza artificiale. Il futuro del calcolo non sarà una sostituzione secca, ma una composizione di strumenti diversi, ciascuno con il proprio ruolo.

UNA QUESTIONE DI POLITICHE, ANCHE INDUSTRIALI

Sul piano industriale, poi, il quantum sta costringendo il settore a ragionare in termini di filiera. Non bastano i processori: servono componentistica, elettronica di controllo, software di orchestrazione, servizi cloud e competenze di integrazione. È qui che la tecnologia esce dalla retorica del "computer del futuro" e comincia a somigliare a un'industria vera, con esigenze produttive, standard e capacità di distribuzione. E, anche se con un orizzonte di medio-lungo periodo, inizia a rendersi necessaria una politica industriale nazionale e continentale, fatta di **scelte su dove puntare** e di indispensabili **rinunce laddove non si può davvero riuscire a competere.**

Per l'Italia, il punto non è soltanto partecipare a questa corsa, ma farlo con una linea coerente nel tempo. Il Paese dispone di competenze scientifiche, centri di ricerca, università e attori industriali di livello, ma il rischio di frammentazione è sempre dietro l'angolo, accentuato peraltro dal proliferare incontrollato di Centri, Alleanze, Cluster, Poli, e via dicendo. Per questo sarebbe auspicabile che la traiettoria avviata oggi non venisse frenata da oscillazioni di breve periodo. L'avvicinarsi della **prossima stagione elettorale italiana** dovrebbe semmai rafforzare, non indebolire, la consapevolezza che il quantum è una scommessa di sistema e non un tema da slogan. E, a maggior ragione, l'attuale mancanza di un **Quantum Act** europeo si fa sempre più problematica. Il messaggio più solido, oggi, potrebbe essere questo: il quantum computing non va raccontato come una scorciatoia, ma come un percorso lungo e necessario. Il suo valore non dipenderà solo dalla potenza delle macchine, ma dalla capacità di trasformare ricerca, competenze e infrastrutture in una filiera industriale credibile.

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