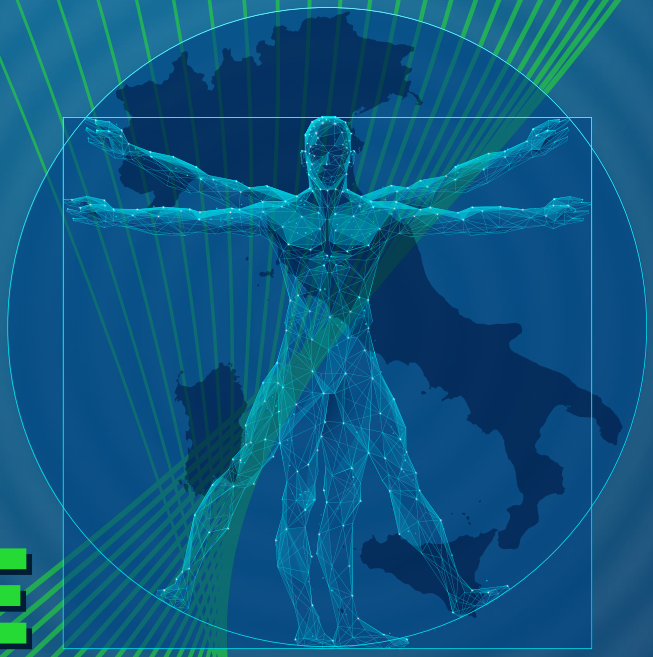
TIG | THE INNOVATION GROUP

IL CAFFÈ DIGITALE

OTTOBRE 2025



LIBERARE IL POTENZIALE DELL'INNOVAZIONE

Il ruolo del digitale e dell'AI

QUESTO MESE ABBIAMO FATTO COLAZIONE CON...

John Halamka, *medico, imprenditore e presidente Mayo Clinic Platform*

NUMERI E MERCATI

Managed Service Provider al bivio: la strada dell'AI è quella giusta

CYBERSEC E DINTRONI

Sovereign AI: la nuova corsa per l'indipendenza tecnologica

SOMMARIO

LIBERARE IL POTENZIALE DELL'INNOVAZIONE: IL RUOLO DEL DIGITALE E DELL'AI

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

Giunto alla decima edizione, il rapporto annuale di TIG – The Innovation Group offre uno spaccato dei diversi fronti attualmente coinvolti nell'evoluzione del digitale nel nostro Paese e su scala europea. Crisi demografica e della competitività, trasformazione del lavoro, tecnologie dual-use, prospettive "post-digitali", infrastrutture digitali materiali e immateriali sono solo alcune delle key word al centro dello studio.
Oggi le tecnologie ICT sono elemento fondamentale per la crescita e la competitività di Stati e territori. Lo evidenziano anche le tensioni geopolitiche e commerciali tra grandi potenze, come Stati Uniti e Cina, in cui il digitale assume un ruolo chiave. Inoltre, i Paesi europei, inclusa l'Italia, stanno affrontando "nuove" sfide legate ai cambiamenti demografici, alla trasformazione del mercato del lavoro e dell'impiego pubblico. In questo contesto, il digitale e l'intelligenza artificiale diventano strumenti centrali per gestire questi cambiamenti, che richiedono però un ripensamento complessivo di modelli e organizzazione. È questo, in estrema sintesi, il focus della decima edizione del rapporto annuale Digital Italy 2025 di TIG – The Innovation Group, dal titolo "Liberare il potenziale dell'innovazione - Il ruolo delle tecnologie digitali e dell'intelligenza artificiale", che verrà pubblicato a novembre da Maggioli Editore e presentato durante il *Digital Italy Summit 2025* in programma a Roma il 19-20 novembre 2025. Di seguito sono riportati alcuni dei principali temi affrontati.

INNOVAZIONE E COMPETITIVITÀ IN EUROPA E IN ITALIA

In un contesto geopolitico ed economico sempre più complesso, due rapporti presentati alla Commissione Europea – quello di Mario Draghi sulla *competitività e innovazione* e quello di Enrico Letta sul *futuro del mercato unico* – hanno evidenziato le vulnerabilità dell'Unione, in primis nella capacità di innovare e competere.
In entrambi questi documenti, il digitale è indicato come elemento centrale della strategia europea di rilancio, una visione che trova poi conferma nella *"Bussola per la competitività"* presentata a gennaio 2025 dalla Presidente Ursula von der Leyen.
Questa strategia pone le tecnologie digitali al centro dell'azione per colmare il gap d'innovazione e per recuperare competitività, ponendo particolare attenzione a settori emergenti come quelli dell'intelligenza artificiale e del quantum computing, cruciali per rafforzare il ruolo dell'Europa nello scenario globale.

DIGITALE E TECNOLOGIE *DUAL-USE*

La sicurezza e la difesa, nazionali e sovranazionali, dipendono sempre più dalle tecnologie digitali: l'uso di droni, l'intelligenza artificiale, i big data e la cybersicurezza sono ormai centrali nelle strategie militari e negli scontri tra Stati.
In Europa, cresce di conseguenza l'attenzione sulle tecnologie cosiddette dual-use, ossia in grado di coniugare applicazioni civili e militari, un'occasione per rafforzare allo stesso tempo infrastrutture di sicurezza e la competitività industriale del Vecchio Continente.
Lo sviluppo di un sistema di difesa europeo richiede d'altra parte investimenti coordinati e soluzioni interoperabili, che garantiscano la sovranità tecnologica, e una valutazione attenta dell'impatto di tali investimenti sul bilancio del welfare, assicurando ad esempio che lo sviluppo digitale in quest'ambito non comprometta risorse fondamentali per sanità e educazione.

LAVORO E DEMOGRAFIA: LE SFIDE DEL MILLENNIO

I Paesi dell'Unione Europea devono affrontare non solo una complessa situazione geopolitica, ma anche sfide interne di grande rilievo, il cui impatto sarà visibile nel lungo periodo.
Tra queste, la trasformazione demografica rappresenta un tema cardine, in particolare per l'Italia: l'aumento della popolazione anziana a discapito delle fasce dei giovani trasforma dinamiche ed equilibri nella società e nel mercato del lavoro: da un lato, si accentua la domanda di assistenza sanitaria e long term care a discapito di scuole e servizi educativi; dall'altro si comprime la forza lavoro attiva con conseguenti rischi per produttività e competitività. La complessità di queste sfide richiede una visione integrata che valorizzi il contributo di tutte le componenti sociali: è ad esempio essenziale promuovere l'occupazione femminile, l'inserimento dei NEET e sostenere la natalità per compensare i cali demografici e favorire uno sviluppo sostenibile del Paese.

"POST-DIGITALE": AI E QUANTUM COMPUTING

Il cambiamento riguarda non solo aspetti economici e sociali, ma anche l'evoluzione stessa della tecnologia digitale: negli ultimi anni l'ICT ha rivoluzionato il modo di accedere alle risorse informatiche grazie a paradigmi come il cloud e il mobile computing, offrendo accesso flessibile, scalabile e in mobilità a capacità computazionale e applicativi. Questo approccio ha supportato la diffusione di nuovi modelli di lavoro e di business. Oggi l'attenzione si concentra sull'intelligenza artificiale, in termini di impatti e trasformazione dell'informazione e della conoscenza, e sul *quantum computing*, che promette di moltiplicare il potenziale computazionale. In questo contento "post-digitale", l'Europa sta investendo nelle AI gigafactory e nei supercomputer, con l'Italia che può far leva su realtà come il tecnopolo DAMA di Bologna o su aziende come ENI per guidare gli investimenti in quest'area.

INFRASTRUTTURE, GOVERNO E INNOVAZIONE

Per garantire che tutti i tasselli dello sviluppo del digitale contribuiscano in modo coerente alla crescita sostenibile della società e dell'economia in Europa e in Italia, occorre promuovere sia lo sviluppo di infrastrutture (materiali e immateriali) a supporto, sia una strategia complessiva per gestire e supportare lo sviluppo dell'innovazione digitale. Investire in connettività e data center assume quindi una rilevanza strategica per assicurare l'autonomia dei territori nell'ambito del digitale: la connettività diventa sempre più ibrida, integrando reti tradizionali e satellitari, mentre lo sviluppo sostenibile di data center richiede linee guida e orientamenti per ottimizzare gli investimenti e ridurre i rischi di sprechi di territorio e di risorse. Per quanto riguarda invece le infrastrutture immateriali, in Italia, grazie anche ai fondi del PNRR, si sono compiuti progressi significativi nel campo dell'identità e dei pagamenti digitali, dell'interoperabilità e della valorizzazione dei dati pubblici. Occorre d'altro canto che queste iniziative e grandi progetti continuino ad evolversi in modo sinergico, supportando il Paese nell'affrontare le sfide e le opportunità di un'economia e di una società digitali.

Per maggiori dettagli sui contenuti della X edizione del rapporto Digital Italy ***"Liberare il potenziale dell'innovazione – Il ruolo delle tecnologie digitali e dell'intelligenza artificiale"*** *leggi la cover story sul numero di ottobre di Technopolis*
Il rapporto sarà presentato il ***19-20 novembre*** *durante il* ***Digital Italy Summit 2025*** *a Roma, presso l'Acquario Romano. Per maggiori informazioni visita la pagina dell'evento.*

Mezzo secolo di AI per ripensare la medicina

Gianluca Dotti, *Giornalista*
TIG - The Innovation Group

L'INTELLIGENZA ARTIFICIALE STA TRASFORMANDO LA SANITÀ MOLTO PIÙ IN FRETTA DI QUANTO IL SISTEMA SANITARIO RIESCA AD ADATTARSI ALLE NOVITÀ CHE SI RINCORRONO. DALLE DIAGNOSI ASSISTITE AI MODELLI PREDITTIVI, FINO AGLI ALGORITMI CHE ANALIZZANO MILIONI DI IMMAGINI E REFERTI, L'AI PROMETTE DI ALLEGGERIRE IL CARICO DEI CLINICI E MIGLIORARE L'ASSISTENZA, MA SOLLEVA ANCHE NUOVE SFIDE CHE SPAZIANO DALLA **GESTIONE DEI DATI** ALLA **SICUREZZA** FINO ALLA **RESPONSABILITÀ** DELLE DECISIONI AUTOMATIZZATE. IN UN MOMENTO IN CUI LA CORSA GLOBALE ALLA DIGITAL HEALTH STA RIDISEGNANDO GLI EQUILIBRI TRA RICERCA, INDUSTRIA E GOVERNANCE, COMPRENDERE COME INTEGRARE LA TECNOLOGIA NELLA PRATICA QUOTIDIANA È DIVENTATO CRUCIALE.

Tra le voci più autorevoli al mondo in questo dibattito c'è **John Halamka**, **medico, imprenditore e presidente della *Mayo Clinic Platform***, che raggruppa una serie di iniziative notevoli di medicina digitale.
Da oltre trent'anni – oggi ne ha 57 – Halamka lavora all'intersezione tra medicina, informatica e policy, guidando progetti pionieristici per la condivisione sicura dei dati e l'uso etico dell'intelligenza artificiale in sanità, come ha raccontato anche nel suo recentissimo *libro Transform: Mayo Clinic Platform and the Digital Future of Health* (2025). Abbiamo incontrato Halamka a margine dell'intervista esclusiva (*qui da 1:29:00*) raccolta in occasione dell'***Healthcare Innovation Summit 2025***, l'appuntamento autunnale di TIG (The Innovation Group) e AISIS (Associazione Italiana Sistemi Informativi in Sanità) per discutere il futuro del digitale per il comparto della sanità e delle scienze della vita.

John Halamka, quali sono secondo lei le tappe fondamentali che hanno portato l'AI alle applicazioni cliniche di oggi?
Lavoro sull'intelligenza artificiale da decenni, e in questo tempo sono cambiate radicalmente sfide e opportunità. All'inizio il problema era far funzionare le macchine: le risorse di calcolo erano limitate e spesso occorreva costruirle da zero. Poi l'attenzione si è spostata sul software, sui linguaggi e sugli strumenti che permettevano di dare istruzioni ai computer e di farli *ragionare*. In quegli anni venivano sperimentati sistemi basati su regole che, con il senno di poi, anticipavano alcuni meccanismi dei chatbot moderni. Pian piano l'intelligenza artificiale ha iniziato a entrare nel mondo della sanità, grazie alla creazione delle prime cartelle cliniche elettroniche e alla raccolta di dati strutturati su problemi, farmaci e referti. Questo passaggio è stato decisivo: senza dati affidabili e comparabili non può svilupparsi un'AI clinica efficace. Da lì è emersa la necessità di far dialogare i diversi sistemi informatici, definendo standard comuni e piattaforme capaci di condividere informazioni in modo sicuro e interoperabile. Oggi, dopo decenni di evoluzione, il settore dispone finalmente di tutto ciò che serve per applicare l'intelligenza artificiale alla pratica medica quotidiana: potenza di calcolo, grandi quantità di dati e un linguaggio comune per interpretarli.

La disponibilità e la qualità dei dati sanitari sono un punto chiave per lo sviluppo dell'AI: quali sono le principali difficoltà nel rendere questi dati utilizzabili in modo sicuro e standardizzato a livello globale?
Il problema non è solo raccogliere dati, ma renderli davvero utilizzabili senza violare la privacy. La maggior parte delle informazioni cliniche utili — come note, referti, immagini — non è strutturata e contiene molti dettagli personali difficili da eliminare. Non basta togliere nomi o numeri di cartella: anche un ruolo, una data o un evento specifico possono rendere una persona riconoscibile. Per questo abbiamo sviluppato tecniche che modificano o

mascherano questi elementi, come lo spostamento delle date o la sostituzione di parole troppo identificabili, così da mantenere il significato clinico ma proteggere l'identità dei pazienti. Lo stesso vale per le immagini mediche: un esame del cranio, per esempio, può essere ricostruito in 3D e mostrare il volto, quindi viene leggermente sfocato. Solo dopo un lavoro di questo tipo i contenuti possono essere archiviati e analizzati in ambienti cloud sicuri, conformi alle normative internazionali come il GDPR in Europa e l'HIPAA negli Stati Uniti.

L'Europa sembra procedere più lentamente rispetto ad altre aree del mondo. Quali passi concreti servirebbero per accelerare l'adozione dell'AI in sanità senza compromettere sicurezza e regolamentazione?

Non voglio essere eccessivamente critico, ma l'Europa oggi è davvero indietro. Negli ultimi mesi ho visitato 21 paesi, e in molti ho sentito dire che si attende l'European Health Data Space. È di certo una buona iniziativa, ma se si resta fermi fino al 2028 il resto del mondo sarà già ben più avanti. Il mio consiglio è di non aspettare: in Asia, in Medio Oriente e in molte parti dell'America si stanno già adottando soluzioni di AI a scala. In Europa ci sono stati che si muovono meglio, come Danimarca o Paesi Bassi, ma manca un approccio coordinato. La chiave potrebbe essere la creazione di un modello federato: così i dati rimarrebbero nei singoli centri, e sarebbero gli algoritmi a *spostarsi*. Questo permetterebbe di sviluppare modelli condivisi riducendo rischi, costi e tempi.

Mayo Clinic Platform è spesso citata come modello di cooperazione tra ricerca, startup e grandi aziende. Qual è la lezione più utile che può offrire a chi vuole costruire ecosistemi digitali simili?

Alla Mayo Clinic abbiamo cercato di costruire qualcosa che mettesse davvero in relazione informazioni, ricerca e innovazione. Dopo aver anonimizzato e messo in sicurezza enormi quantità di dati clinici, abbiamo aperto la piattaforma a collaborazioni con startup, aziende e istituzioni. Una sessantina di giovani imprese sono passate dal nostro acceleratore, e alcune di loro oggi sono diventate realtà globali. Anche grandi aziende e 26 case farmaceutiche hanno usato la piattaforma per validare modelli, studiare nuovi target terapeutici o analizzare coorti di pazienti. Oggi oltre 60 sistemi ospedalieri nel mondo utilizzano applicazioni nate da queste collaborazioni, integrate direttamente nelle cartelle cliniche attraverso un sidecar che le fa funzionare nel flusso di lavoro reale. È un circolo virtuoso: più attori partecipano, più valore si genera per tutti. La lezione principale è proprio questa: creare fiducia, condividere conoscenze e costruire sistemi dove ogni parte contribuisce e beneficia della presenza delle altre.

Guardando al futuro, come immagina il ruolo dell'AI nella pratica clinica quotidiana? E quanto siamo vicini da una vera intelligenza artificiale generale?

Credo che entro cinque anni ogni medico utilizzerà l'intelligenza artificiale nella propria attività quotidiana. Non per sostituirsi al giudizio clinico, ma per affrontare l'enorme quantità di dati che arrivano da pazienti, referti e letteratura scientifica. L'AI diventerà un supporto indispensabile per prendere decisioni migliori e più rapide. In un certo senso, non usarla significherà lavorare con meno strumenti di quanti se ne avrebbero a disposizione. Quanto all'intelligenza artificiale generale, sono molto più prudente: i modelli attuali sono straordinariamente utili, ma non ragionano, non hanno intenzione o consapevolezza. Aumentare la quantità di dati o la potenza di calcolo non sarà sufficiente. Servirà un cambio di paradigma, qualcosa di ancora lontano. Nel frattempo, l'obiettivo è continuare a usare l'AI come alleato dei clinici, riducendo il carico amministrativo e migliorando la cura del paziente.

John Halamka, presidente della Mayo Clinic Platform, durante il suo intervento all'Healthcare Innovation Summit 2025.

Managed Service Provider al bivio: la strada dell'AI è quella giusta

Valentina Bernocco, *Content Manager*
TIG - The Innovation Group

IL MERCATO DEI SERVIZI GESTITI È FIORENTE, MA SI IMPONE PER GLI MSP UN CAMBIAMENTO DEI MODELLI DI BUSINESS. UN CAMBIAMENTO IMPERNIATO SULL'INTELLIGENZA ARTIFICIALE.

Stanno a metà strada fra le tecnologie e le aziende utenti, e il loro ruolo è sempre più importante per la gestione dell'IT garantendo buon funzionamento, efficienza e cybersicurezza: sono gli Msp, i **Managed Service Provider**. Il loro lavoro sta cambiando sotto la spinta, sì, dell'evoluzione tecnologica ma anche di mutamenti del mercato, ovvero della sempre maggiore richiesta, da parte delle aziende, di un supporto esterno che le aiuti a sgravarsi da attività troppo gravose, complesse o specializzate.

Complici le impreviste e improvvise necessità di remotizzazione e di trasformazione digitale nelle aziende, il giro d'affari mondiale dei servizi gestiti ha vissuto un boom nell'immediato post-Covid. Non è stata, però, solo un contingenza. Secondo le stime di Grand View Research, nel 2024 il mercato ha superato i 335 miliardi di dollari di valore e si prevede oltrepasserà i 731 miliardi nel 2030, con un CAGR del 14,1%. Leggermente diversa la stima di Mordor Intelligence, che per il 2025 quantifica un giro d'affari mondiale di

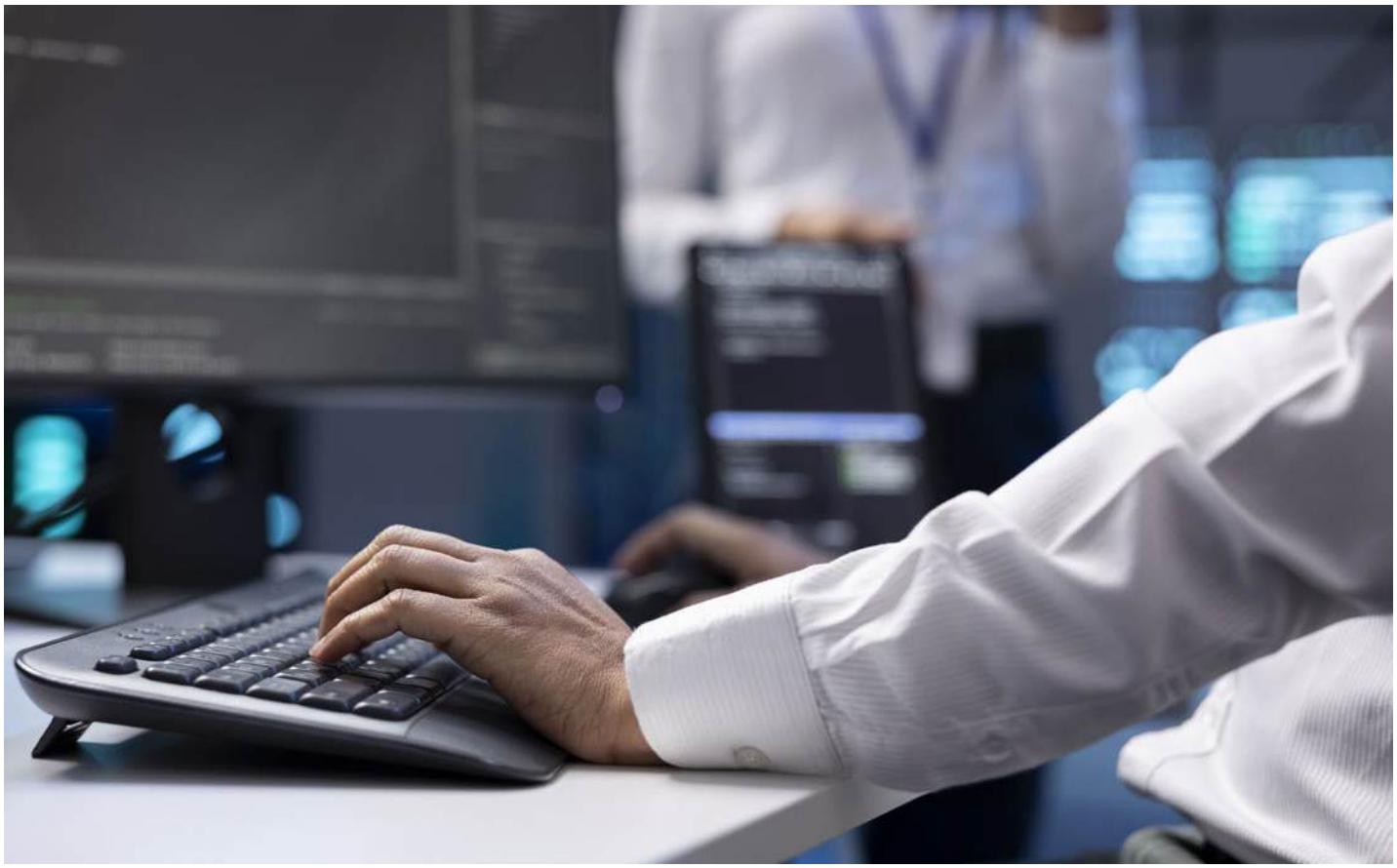


Foto ©DCstudio/freepik.com

circa 390 miliardi di dollari, destinato a crescere con un CAGR del 10,5% superando i 642,5 miliardi di dollari nel 2030. Discrepanze numeriche a parte, diversi analisti dipingono il medesimo quadro.

I MOTORI DELLA DOMANDA

Come noto, nelle aziende la **frammentazione tecnologica** è un problema endemico, risultato della stratificazione tra soluzioni legacy e standard, consolidatasi negli anni. La proliferazione di strumenti di monitoraggio, la commistione tra ambienti cloud e on-premise e la presenza di numerosi "strati" di infrastruttura, gestiti da team diversi, sono ulteriori fattori che hanno alimentato la domanda di servizi gestiti.
C'è poi la **cybersicurezza**, che si lega al buon funzionamento delle applicazioni, alla difesa di rete, al backup e al disaster recovery: in tutto questo, gli Msp sono spesso essenziali perché suppliscono alla mancanza di un Security Operations Center interno all'azienda. Garantiscono, quindi, monitoraggi continui e velocità nelle azioni di rilevamento delle minacce e risposta agli incidenti. Sebbene i servizi gestiti di infrastruttura rappresentino ancora la maggior fetta di giro d'affari (circa il 39%, in base ai dati di Mordor Intelligence riferiti al 2024), quelli di cybersicurezza sono la componente più in crescita.

LA SFIDA DELLA MARGINALITÀ

Tutti felici, in questo mercato ancora ricco di opportunità? Più o meno, perché i **margini di profitto** per gli Managed Service Provider non sono esaltanti, come sottolineato anche dal palco spagnolo dell'ultima conferenza "Msp Global". Vendor come Acronis sottolineano *l'esigenza di migliorare la produttività*, mentre società di analisti come **Idc** elencano una serie di criticità che nel prossimo futuro potrebbero limitare gli investimenti delle aziende utenti in servizi gestiti: **restrizioni di budget**, preoccupazioni dei manager sui **crescenti costi dell'IT**.

I fornitori di servizi gestiti dovranno anche aggiornare la propria offerta, per allinearla alle **nuove esigenze** dei clienti. La gestione dell'uptime, dunque la garanzia di operatività, è stata tradizionalmente la prima richiesta affidata dalle aziende agli Msp. Continuerà a essere il punto di partenza, ma da sola non basterà: sempre di più, a fronte della spesa in servizi gestiti, le aziende vorranno vedere risultati e risultati misurabili, impatti sul business come si suol dire.

VERSO UN CAMBIO DI PARADIGMA

Già oggi l'**intelligenza artificiale** viene utilizzata dagli Msp per velocizzare e automatizzare le attività quotidiane, per sopperire a eventuali carenze di personale o competenze, per offrire un servizio più tempestivo e accurato.
I casi d'uso sono molteplici: l'AI velocizza il rilevamento e la risposta agli incidenti, gli analytics, feed di threat intelligence e la reportistica, e inoltre permette di automatizzare attività quali i monitoraggi su infrastrutture e applicativi, l'installazione di aggiornamenti e patch, i controlli di compliance. Oltre all'AI generativa e agentica, il machine learning di altro tipo resta prezioso per attività di analisi e nella manutenzione predittiva, oppure per l'ottimizzazione dei costi e per il provisioning delle risorse cloud.
Non si tratta solo di un'estensione, di uno strumento tecnologico aggiuntivo e magari opzionale. A detta non solo dei vendor ma di molti osservatori, al di là dell'hype l'intelligenza artificiale rappresenta un vero cambio di paradigma, anche per gli Msp.
Come si legge in un recente *report* di **Pax8**, un marketplace per vendor tecnologici e fornitori di servizi gestiti, il cambiamento è profondo: i tradizionali modelli di business degli Msp hanno ormai raggiunto il limite e siamo a un punto di non ritorno. Solo adottando l'AI, inclusa quella generativa e agentica, i Managed Service Provider potranno prosperare, diventando *"architetti di infrastrutture intelligenti, costruttori di sistemi agentici e orchestratori di risultati di business"* per i loro clienti.

PNRR, Transizione Digitale e PA Locale: l'indagine di TIG – Gruppo Maggioli

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

L'INDAGINE ANNUALE DI TIG – THE INNOVATION GROUP E GRUPPO MAGGIOLI ANALIZZA LE EVOLUZIONI NELLA TRANSIZIONE DIGITALE DEGLI ENTI LOCALI, GUARDANDO CON UN OCCHIO DI ATTENZIONE AL RUOLO E ALL'EFFICACIA DEGLI INVESTIMENTI DEL PNRR NELL'AVVIO E NELLO SVILUPPO DEI PROGETTI DIGITALI. COSA ACCADRÀ D'ALTRA PARTE A QUESTI PROGETTI OLTRE L'ORIZZONTE DEL 2026?

Gli investimenti del PNRR hanno fornito una spinta rilevante alla transizione digitale degli enti pubblici, sia a livello centrale sia nei territori, dalle Regioni fino ai Comuni. Cloud computing, interoperabilità, valorizzazione dei dati e sicurezza informatica sono solo alcuni tra i principali ambiti su cui si è incentrata la digitalizzazione del settore. Al fine di monitorare e analizzare questa evoluzione nei percorsi di transizione digitale nelle pubbliche amministrazioni, in particolare a livello locale, TIG – The Innovation Group in collaborazione con Gruppo Maggioli promuove da alcuni anni una rilevazione annuale, l'"**Indagine sulla transizione digitale nella PA locale**". L'edizione di quest'anno, condotta tra giugno e luglio 2025 e che ha coinvolto 476 rispondenti appartenenti a Comuni, Unione di Comuni, Città Metropolitane e Province, si è incentrata in particolare sul tema della gestione dei progetti digitali post-PNRR, per comprendere come e se gli enti locali e i Comuni stanno cominciando ad affrontare questo tema, che diventerà cruciale a partire dal 2026. Di seguito alcuni dei principali risultati emersi.

IL RUOLO DEL PNRR NELLA TRANSIZIONE DIGITALE

Secondo il 90% degli intervistati i finanziamenti del PNRR hanno avuto un ruolo importante, se non fondamentale, nelle fasi di avvio e sviluppo dei progetti digitali all'interno degli enti: è una conferma del **ruolo di driver** del Piano nella digitalizzazione degli enti pubblici sul territorio. Inoltre, aumenta anno su anno la percentuale di chi considera questi finanziamenti **molto o estremamente efficaci** per la transizione digitale del proprio ente: rispetto all'edizione 2024, questo dato è passato dal 30% all'attuale 35%, con una crescita soprattutto nella quota degli intervistati che li ritiene "estremamente efficaci", dal 5% al 9%. In altre parole, si rafforza l'opinione dei partecipanti all'indagine sull'importanza e sull'efficacia di questi investimenti nei percorsi di digitalizzazione degli enti locali.

LA GESTIONE POST-PNRR DEI PROGETTI DIGITALI

Tra gli intervistati, uno su cinque ammette di non aver ancora affrontato il tema di come gestire i progetti digitali già avviati una volta conclusa l'esperienza del PNRR, oltre l'orizzonte del 2026; a questi si aggiunge circa uno su due che ammette di non essere a conoscenza dei piani del proprio ente a riguardo. L'**incertezza rispetto a questo tema**, inoltre, si conferma anche tra chi dichiara un piano di gestione post-2026: uno su quattro tra chi si è attivato non ha infatti ancora individuato azioni concrete per gestire questi progetti. Si tratta d'altra parte di un argomento complesso, che non si esaurisce con l'individuazione di risorse economiche alternative, ma tocca anche aspetti relativi alle competenze e alla **disponibilità di risorse umane** per la gestione dei progetti digitali. In questo senso, il tema della formazione emerge come un ambito su cui intervenire, sia tra i più consapevoli sia tra chi non si è attivato (o non sa). Il venir meno delle risorse economiche del PNRR rischia infatti di indebolire la capacità di compensare l'eventuale mancanza di competenze digitali interne con risorse esterne: investire in formazione significa pertanto rafforzare la capacità di governare questi progetti.
C'è d'altra parte anche una quota di chi si è attivato per gestire il post-PNRR – uno su cinque – che dichiara di

Foto ©fanjianhua/freepik.com

stare valutando un **ripensamento o una rivalutazione dei progetti digitali** in corso. Si corre pertanto il rischio di assistere a dei "passi indietro" nei percorsi di digitalizzazione degli enti locale, benché in misura minore rispetto ad iniziative più proattive, alla ricerca di risorse economiche alternative e di un rafforzamento delle competenze digitali interne.

IL FUTURO DELLA TRANSIZIONE DIGITALE DEGLI ENTI LOCALI

L'indagine di TIG -Gruppo Maggioli mette in evidenza l'importanza dei finanziamenti del PNRR nel promuovere la trasformazione digitale negli enti locali, con un ruolo rilevante e efficace nello sviluppo dei progetti individuati. Tuttavia, emergono preoccupazioni sulla **sostenibilità di queste iniziative** oltre l'orizzonte del 2026 e sulla gestione futura dei progetti digitali, senza ancora un approccio condiviso per affrontare le sfide dei prossimi anni. Si guarda in particolare ad un **rafforzamento delle competenze interne** tramite iniziative di formazione, per prepararsi anche alla gestione di nuove tecnologie, come l'intelligenza artificiale, che andranno indubbiamente a "complicare" ulteriormente il perimetro di azione degli enti.

*Per maggiori dettagli sui contenuti della X edizione del rapporto Digital Italy **"Liberare il potenziale dell'innovazione – Il ruolo delle tecnologie digitali e dell'intelligenza artificiale"** leggi la cover story sul numero di ottobre di Technopolis*
*Il rapporto sarà presentato il **19-20 novembre** durante il **Digital Italy Summit 2025** a Roma, presso l'Acquario Romano.*
Per maggiori informazioni visita la pagina dell'evento.

L'imperativo quantistico

Gianfabio Palmerini,
CISO, Webuild

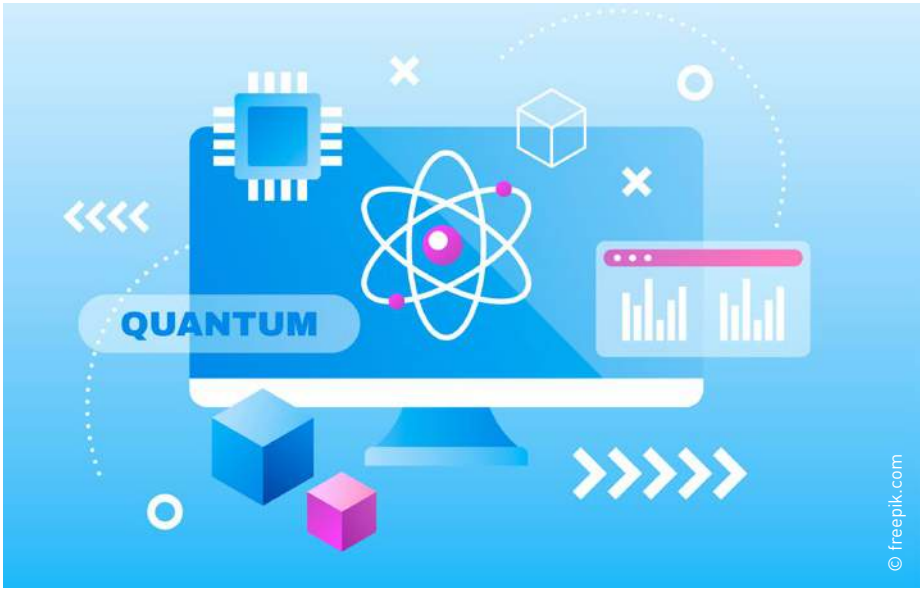
L'ASCESA DEL CALCOLO QUANTISTICO NON RAPPRESENTA UNA SEMPLICE EVOLUZIONE COMPUTAZIONALE, MA UNA MINACCIA ESISTENZIALE PER LA MAGGIOR PARTE DEI SISTEMI DI CRITTOGRAFIA A CHIAVE PUBBLICA SU CUI SI BASA LA SICUREZZA DIGITALE GLOBALE. L'IMMINENTE SVILUPPO DI UN COMPUTER QUANTISTICO CRITTOGRAFICAMENTE RILEVANTE (CRQC) CAPACE DI VIOLARE ALGORITMI STANDARD COME RSA ED ELLIPTIC CURVE CRYPTOGRAPHY (ECC) RENDE LA MIGRAZIONE A STANDARD POST-QUANTISTICI (PQC) UNA PRIORITÀ ASSOLUTA NON PIÙ RIMANDABILE. [(1)]

La problematica principale risiede nel fatto che gli avversari stanno già impiegando una strategia di "raccolta ora, decifra in futuro" (in inglese, "Harvest Now, Decrypt Later"). [(2)]
Intercettano e archiviano i dati sensibili crittografati oggi, sapendo di poterli decifrare in un futuro prossimo con un CRQC sufficientemente potente. Per i dati che richiedono una riservatezza a lungo termine, questa minaccia non è teorica, ma è già attiva e reale.
Questo rapporto delinea una roadmap strategica in tre fasi, allineata con i principali standard e direttive globali, tra cui quelle del National Institute of Standards and Technology (NIST) e del National Cyber Security Centre (NCSC) del Regno Unito, che hanno stabilito una scadenza indicativa del 2035 per una migrazione completa [(3)]. La roadmap proposta vuole offrire un percorso pratico per le organizzazioni, partendo da una fase immediata di scoperta e pianificazione, passando per la sperimentazione e la prioritizzazione, fino a una completa migrazione che assicuri una resilienza a lungo termine.
Il percorso verso la crittografia post-quantistica non è un singolo aggiornamento, ma una profonda trasformazione che richiede un'accurata pianificazione, investimenti (significativi) e un impegno a lungo termine. Le organizzazioni che fin da subito abbracciano l'agilità crittografica e aggiornano le proprie infrastrutture, saranno le uniche in grado di salvaguardare la propria integrità e il proprio patrimonio informativo nell'era quantistica che sta per arrivare.

PERCHÉ LA MIGRAZIONE QUANTISTICA È UNA NECESSITÀ IMMINENTE

I computer quantistici non sono semplicemente una versione più veloce o più potente dei supercomputer classici. Essi rappresentano un nuovo paradigma di calcolo che sfrutta i principi della meccanica quantistica, come la sovrapposizione e l'entanglement. Questa capacità intrinseca permette loro di risolvere problemi matematici che sono attualmente intrattabili per i computer classici, minando direttamente le basi della moderna crittografia.
La minaccia principale deriva dall'algoritmo di Shor, che è stato sviluppato per risolvere due problemi matematici specifici: la fattorizzazione di grandi numeri interi e il logaritmo discreto. La sicurezza di algoritmi a chiave pubblica ampiamente utilizzati, come RSA ed ECC, è interamente basata sulla difficoltà computazionale di risolvere questi problemi. L'**algoritmo di Shor** può frantumarli in tempi estremamente brevi se eseguito su un computer quantistico sufficientemente potente, compromettendo la sicurezza di una vasta gamma di applicazioni, dalle comunicazioni HTTPS alle firme digitali.
L'**algoritmo di Grover** è uno schema di ricerca che può accelerare gli attacchi a forza bruta, in particolare contro la crittografia simmetrica come AES e le funzioni hash come SHA-2/3. A differenza di Shor, che rende la crittografia asimmetrica obsoleta, l'impatto di Grover sulla crittografia simmetrica è meno distruttivo. Essenzialmente, dimezza l'efficacia della lunghezza della chiave, il che significa che un cifrario AES-256 fornisce

un livello di sicurezza equivalente a quello di una chiave a 128 bit.
La soluzione per mitigare questa minaccia è relativamente semplice: raddoppiare la lunghezza della chiave.
Una delle preoccupazioni più immediate, pressanti e in voga è la strategia di "raccogli ora, decifra in futuro" (HNDL). Questa tattica si basa sulla raccolta di dati sensibili crittografati oggi da parte di avversari, con l'intenzione di conservarli e decifrarli in futuro quando i CRQC saranno operativi. Non si tratta di una minaccia futura, ma di un problema che esiste già nel presente per qualsiasi informazione che richiede una riservatezza a lungo termine.



Dati sanitari, documenti finanziari, segreti industriali e informazioni sulla sicurezza nazionale sono tutti candidati a essere intercettati e archiviati per una successiva decifrazione. Questa minaccia, evidenziata dalla comunità della cybersecurity, sottolinea l'urgenza di agire subito per proteggere i dati in transit e at rest.
Le previsioni sull'arrivo di un CRQC variano ampiamente, con stime che vanno da "meno di 5 anni" a 15-20 anni o più. Questa incertezza deriva dalla natura del qubit, l'unità fondamentale del calcolo quantistico, che presenta significative sfide ingegneristiche come la stabilità e la fidelizzazione. Nonostante gli enormi investimenti globali e i rapidi progressi il cammino verso un CRQC su larga scala rimane imprevedibile.
A fronte di tale incertezza, i governi e gli enti di standardizzazione non stanno aspettando una data precisa. Stanno invece fissando scadenze basate sulla complessità della migrazione. La National Security Memorandum 10 (NSM-10) statunitense ha fissato una scadenza per una migrazione completa dei sistemi federali entro il 2035 *(4)*. In modo simile, il NCSC del Regno Unito ha delineato una roadmap in tre fasi che culmina con una migrazione completa entro il 2035 *(5)*; anche l'Europa ha preparato una tabella di marcia verso la transazione quantistica *(6)*. Questa tempistica non è una previsione su quando i CRQC arriveranno, ma è un riconoscimento del fatto che la transizione stessa richiederà anni, se non decenni, per organizzazioni di grandi dimensioni a causa della complessità delle loro reti e dell'enorme numero di dispositivi da aggiornare.
Il principio guida di queste tempistiche è formalizzato dal **Teorema di Mosca**, noto anche come Disuguaglianza di Mosca. Questo principio stabilisce che la migrazione deve iniziare prima che la somma degli anni in cui i dati sensibili devono rimanere sicuri (X) e il tempo stimato per completare la transizione (Y) sia superiore al tempo rimanente prima che un CRQC diventi operativo (Z). In altre parole, se X + Y > Z, allora l'organizzazione deve agire immediatamente per evitare di essere vulnerabile.
Poiché il tempo di migrazione (Y) per una grande azienda è stimato in un decennio e i dati (X) hanno spesso un ciclo di vita di molti anni, la necessità di agire ora è inequivocabile, indipendentemente dalla data esatta di arrivo del CRQC.

UN APPROFONDIMENTO SULLA CRITTOGRAFIA POST-QUANTISTICA (PQC)

La crittografia post-quantistica (PQC), nota anche come crittografia "quantum-safe" o "quantum-resistant", si riferisce a un insieme di algoritmi crittografici che possono essere eseguiti su computer classici e sono ritenuti sicuri sia contro attacchi classici che quantistici. A differenza dei sistemi di crittografia a chiave pubblica esistenti, che si basano su problemi matematici vulnerabili all'algoritmo di Shor, gli algoritmi PQC si basano su problemi diversi, come la teoria dei reticoli, i polinomi multivariati o le funzioni hash, considerati intrattabili anche per un CRQC.

Per garantire una transizione ordinata e sicura, il National Institute of Standards and Technology (NIST) degli Stati Uniti ha lanciato un processo di standardizzazione globale nel 2016 *(7)*. Questo processo ha coinvolto la comunità crittografica internazionale in un'ampia valutazione e selezione di algoritmi PQC candidati, con l'obiettivo di identificare quelli che offrono il miglior equilibrio tra sicurezza, prestazioni e caratteristiche di implementazione.

Questo processo pluriennale ha raggiunto una tappa fondamentale nell'agosto 2024, quando il NIST ha pubblicato i primi tre standard di crittografia post-quantistica. Questi standard, noti come Federal Information Processing Standards (FIPS), forniscono la base per la migrazione a livello globale:

- **FIPS 203:** Specifica il meccanismo di incapsulamento della chiave basato su reticoli modulari (ML-KEM), derivato dall'algoritmo **CRYSTALS-Kyber**. Il ML-KEM è progettato per lo scambio di chiavi segrete tra due parti e rappresenta il primo standard per la crittografia a chiave pubblica nell'era post-quantistica.
- **FIPS 204:** Specifica lo standard di firma digitale basata su reticoli modulari (ML-DSA), derivato dall'algoritmo **CRYSTALS-Dilithium**. Le firme digitali sono essenziali per l'autenticazione, la verifica dell'integrità dei dati e la non ripudiabilità delle transazioni.
- **FIPS 205:** Specifica lo standard di firma digitale basato su hash senza stato (SLH-DSA), derivato dall'algoritmo **SPHINCS+**. Questo standard fornisce un'alternativa a ML-DSA basata su una diversa famiglia di problemi matematici.

Il lavoro del NIST non si è fermato alla prima serie di standard. L'agenzia ha riconosciuto il valore strategico della diversità algoritmica, scegliendo di standardizzare più algoritmi basati su diversi problemi matematici per proteggersi dal rischio che una singola famiglia di algoritmi venga compromessa.

A questo proposito, sono in fase di standardizzazione altri algoritmi. **FALCON (FN-DSA)**, un'altra firma digitale basata su reticoli, è prevista per essere standardizzata nel FIPS 206 e si distingue per le sue firme di dimensioni più ridotte, rendendola ideale per dispositivi con risorse limitate. Inoltre, il NIST ha selezionato l'algoritmo **HQC (Hamming Quasi-Cyclic)** come meccanismo di incapsulamento della chiave di riserva (KEM) per ML-KEM. HQC è un algoritmo basato su codici, che offre una ridondanza di sicurezza nel caso in cui le assunzioni di sicurezza dei reticoli dovessero un giorno crollare.

L'approccio del NIST di standardizzare un portafoglio diversificato di algoritmi, con "backup" basati su principi matematici differenti, non è una semplice scelta tecnica, ma una strategia di mitigazione del rischio fondamentale.

Questa politica riconosce che il panorama delle minacce è in continua evoluzione e che la resilienza a lungo termine richiede un ecosistema di algoritmi che non condividano un unico punto di vulnerabilità matematica. Le organizzazioni, pertanto, dovranno sviluppare la capacità di passare da un algoritmo all'altro in modo rapido e senza interruzioni se un giorno si dovesse scoprire una nuova vulnerabilità, un concetto noto come agilità crittografica.

TestoNIS2, punto di contatto e referente CSIRT: cosa fare?

Valentina Frediani, *Founder and CEO*
Colin & Partners

LA AGENZIA PER LA CYBERSICUREZZA NAZIONALE (ACN) CON LA DETERMINAZIONE N. 333017/2025 HA INTRODOTTO LA FIGURA DEL REFERENTE CSIRT (ART. 7) PER I SOGGETTI OBBLIGATI AI SENSI DEL D.LGS. 4 SETTEMBRE 2024, N. 138 (ATTUATIVO DELLA DIRETTIVA DIRETTIVA (UE) 2022/2555 "NIS2"). LA NOMINA DOVRÀ AVVENIRE OBBLIGATORIAMENTE TRA \IL 20 NOVEMBRE 2025 ED IL 31 DICEMBRE 2025, CON CARICAMENTO DEL NOMINATIVO SULLA PIATTAFORMA A CURA DEL PUNTO DI CONTATTO. IL REFERENTE CSIRT DOVRÀ NECESSARIAMENTE ESSERE PERSONA FISICA.

Ma cosa prevede la determinazione e perché questa novità che non trae origine dalla Direttiva?
In sostanza il Referente CSIRT dovrà fare da interfaccia operativa tra il soggetto obbligato e il CSIRT stesso. Ricordiamo che il CISRT SIRT è l'acronimo di Computer Security Incident Response Team ovvero il Team che opera in risposta agli *incidenti di sicurezza informatica*. Infatti, il CISRT ha il compito di prevenire, rilevare e gestire gli incidenti informatici, coordinando le attività di risposta e mitigazione ed è di fatto, l'entità nazionale in prima linea per affrontare minacce e attacchi informatici. Proprio perché deve interfacciarsi a questa struttura, il Referente (ed il suo sostituto) debbono avere competenze di base in materia di sicurezza informatica e gestione degli incidenti informatici oltre ad una conoscenza approfondita dei sistemi informativi e delle reti dell'organizzazione per cui operano.
Si aprono ovviamente degli scenari rispetto a questa nuova figura. Innanzi tutto, si ritiene possa essere sia interna che esterna visto che nessuna precisazione sul tema è emersa in sede di pubblicazione della Determinazione da ACN. Altro aspetto riguarda la possibilità che possa coincidere con il punto di contatto o il suo sostituto: questa ipotesi è decisamente prospettabile considerato che molto spesso è proprio un soggetto con capacità tecniche, a ricoprire il ruolo di punto di contatto.
Ciò che invece rappresenta un vero e proprio cambio di rotta rispetto a quanto precedente individuato, è quanto stabilito nel seguente passaggio della determinazione: *"Il referente CSIRT ha il compito di interloquire con lo CSIRT Italia, di cui all'articolo 2, comma 1, lettera i) del decreto NIS, ed effettuare le notifiche di cui agli articoli 25 e 26 del medesimo decreto per conto del soggetto NIS."*
Pertanto, non sarà più il punto di contatto il soggetto addetto alle notifiche, ma il Referente CSIRT. Questo comporterà quindi che il punto di contatto mantenga un ruolo formale connesso all'inserimento delle informazioni in piattaforma, ma la parte operativa passa così al Referente CSIRT. Sulla base di queste considerazioni, non solo enti ed aziende dovranno rivalutare le nomine interne dei punti di contatto, andando a detrarre gli obblighi correlati alla notifica, ma dovranno anche rivalutare chi nominare. Infatti, uno dei temi cardini ad oggi è stato quello della nomina a punto di contatto del referente dei sistemi informatici aziendali. E proprio un tema piuttosto dibattuto, è stato quello correlato al dover gestire aspetti formali e connessi all'intera struttura, da parte di un soggetto con competenze appartenenti all'area della cybersicurezza. Adesso dovrà essere riragionata la nomina del punto di contatto (se inserire un soggetto fuori dall'alveo dei sistemi informatici) e riportare sugli stessi le nomine connesse al CSIRT. Aspetti che incideranno ovviamente anche sulle procedure organizzative. Dovrà sussistere la procedura interna per la nomina del referente CSIRT (e dei sostituti), che contenga i criteri di selezione e le competenze richieste oltre a consentire a questa figura, di finalizzare tutte le notifiche necessarie (quindi passando attraverso anche formazione, designazione formale e riconoscimento del ruolo anche verso gli altri attori aziendali).
Possiamo davvero dire che sulla NIS2 siamo WORK IN PROGRESS!

Sovereign AI: la nuova corsa per l'indipendenza tecnologica

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

L'INTELLIGENZA ARTIFICIALE (AI) STA RAPIDAMENTE TRASCENDENDO IL RUOLO DI MERA TECNOLOGIA DIGITALE PER DIVENTARE UNA COMPONENTE CRUCIALE DEL MONDO FISICO OLTRE CHE UN ASSET STRATEGICO E GEOPOLITICO.

In questo contesto, sta emergendo con forza una tendenza globale che prende il nome di "AI Sovrana". Questa strategia, sulla scorta della già nota (e mai raggiunta) "Sovranità Digitale", vedrebbe governi e grandi aziende **investire miliardi per sviluppare le proprie capacità di AI**, al fine di garantirsi in questo campo un'autonomia tecnologica e definire il proprio ruolo indipendente nell'ecosistema emergente dell'AI.

AI SOVRANA, UNA DEFINIZIONE

L'AI Sovrana non è un semplice trend tecnico, ma sempre più viene percepita come un imperativo strategico. Essa si riferisce alla *"creazione, implementazione e governance dei sistemi di intelligenza artificiale all'interno di framework che mettono in primo piano la sovranità dei dati, la conformità normativa e il controllo dell'infrastruttura"*. Significa che una nazione o un'organizzazione deve avere il controllo significativo su come l'AI viene costruita, utilizzata e protetta, allineata alle sue leggi, ai suoi valori e alle sue priorità strategiche. Per uno Stato, possedere, controllare e sviluppare tecnologie AI è **simbolo di autonomia strategica, potere economico e influenza diplomatica**. Per realizzare questo obiettivo bisogna però controllare ogni strato dello "stack AI", dallo storage localizzato dei dati all'orchestrazione indipendente dei modelli.

PERCHÉ I GOVERNI CERCANO L'AUTONOMIA IN CAMPO AI

Storicamente, il controllo sulle infrastrutture critiche è stato un fattore decisivo nelle dinamiche di potere globale, e l'infrastruttura di AI non fa eccezione, essendo considerata uno strumento potente di strategia nazionale e differenziazione internazionale. L'urgenza di adottare l'AI Sovrana deriva da una serie di fattori critici:

- **Geopolitica e sicurezza nazionale:** il timore principale è che le restrizioni future o le turbolenze geopolitiche possano limitare l'accesso ai sistemi di AI forniti da Big Tech statunitensi o cinesi. Per settori critici come la difesa, l'affidamento a sistemi stranieri (anche quelli statunitensi, come OpenAI) è spesso impedita dal rischio che i dati sensibili escano

dal Paese. Inoltre, i modelli addestrati all'estero possono presentare vulnerabilità o contenere distorsioni geopolitiche.

- **Allineamento culturale e linguistico:** i modelli AI più diffusi sono stati addestrati principalmente su dati in lingua inglese e presentano spesso un pregiudizio culturale anglosassone. Molti Paesi, come le "potenze medie" e i Paesi in via di sviluppo, necessitano di modelli che riflettino la loro lingua, i loro codici legali, i loro valori e le loro norme sociali.
- **Conformità normativa:** l'AI Sovrana è essenziale per imporre la conformità con i requisiti normativi locali e globali fin dall'inizio, inclusi GDPR, HIPAA e l'EU AI Act. Le grandi aziende, in particolare, considerano la costruzione della **propria piattaforma di AI sovrana** come una priorità *mission-critical* per allinearsi alle norme.

Di seguito una serie di iniziative nazionali di Sovereign AI descritte da Sean Michael Kerner su TechTarget.

COUNTRY	INITIATIVE TITLE	KEY GOALS	OFFICIAL LINK
UNITED STATES	Stargate Project	Build massive AI infrastructure, maintain global AI leadership, $500B private investment	White House AI executive order
UNITED STATES	CHIPS and Science Act	Domestic semiconductor production, AI research leadership	CHIPS Act details
EUROPEAN UNION	AI Factories Initiative	Create 13 regional AI hubs, sovereign AI capabilities, and trustworthy AI development	EU AI strategy
EUROPEAN UNION	AI Act Implementation	Comprehensive AI regulation, risk-based governance framework	EU AI Act
EUROPEAN UNION	OpenEuro LLM	Foundation model development	Open Euro LLM
CHINA	New Generation AI Development Plan	AI leadership by 2030	China AI strategy
INDIA	IndiaAI Mission	" AI for All," an inclusive development effort	India AI mission
SINGAPORE	SEA-LION (Southeast Asian Languages in One Network)	Regional LLM for Southeast Asia, cultural and linguistic representation, open source model	SEA-LION/IMDA announcement
FRANCE	National AI Strategy	European AI sovereignty, research excellence, ethical AI development	France AI strategy
UNITED KINGDOM	AI Opportunities Action Plan 2025	National AI renewal, transform public services, economic growth acceleration	UK AI's action plan 2025
SAUDI ARABIA	NEOM AI City	Futuristic AI-powered city, technological sovereignty	NEOM project

(Fonte: The future of sovereign AI and digital transformation, TechTarget, Sean Michael Kerner, 29 Jul 2025)

AI SOVRANA, REALTÀ O CHIMERA?

Nonostante l'attrattiva strategica, **l'AI Sovrana è un obiettivo difficile e costoso**. L'addestramento di un modello avanzato può costare fino a 1 miliardo di dollari, e il mantenimento richiede ingenti investimenti in infrastrutture, energia e talenti. Per le potenze minori o medie, competere con le centinaia di miliardi di dollari che Stati Uniti e Cina stanno investendo è estremamente arduo.

Di fronte a questi costi, sorge un dibattito sull'efficacia di tali investimenti. Alcuni esperti avvertono che i governi potrebbero **sprecare enormi somme di denaro pubblico** se la loro strategia di AI Sovrana non dovesse tener conto della rapidità con cui si muove la frontiera tecnologica.

Dotarsi di un'AI sovrana significa, per una nazione, avere la capacità di produrre l'AI utilizzando la propria infrastruttura, i propri dati, la propria forza lavoro e le proprie reti.

Significa avere un controllo significativo sul modo in cui l'AI è costruita, implementata, governata e protetta, allineata alle leggi, a valori e priorità strategiche della singola nazione.

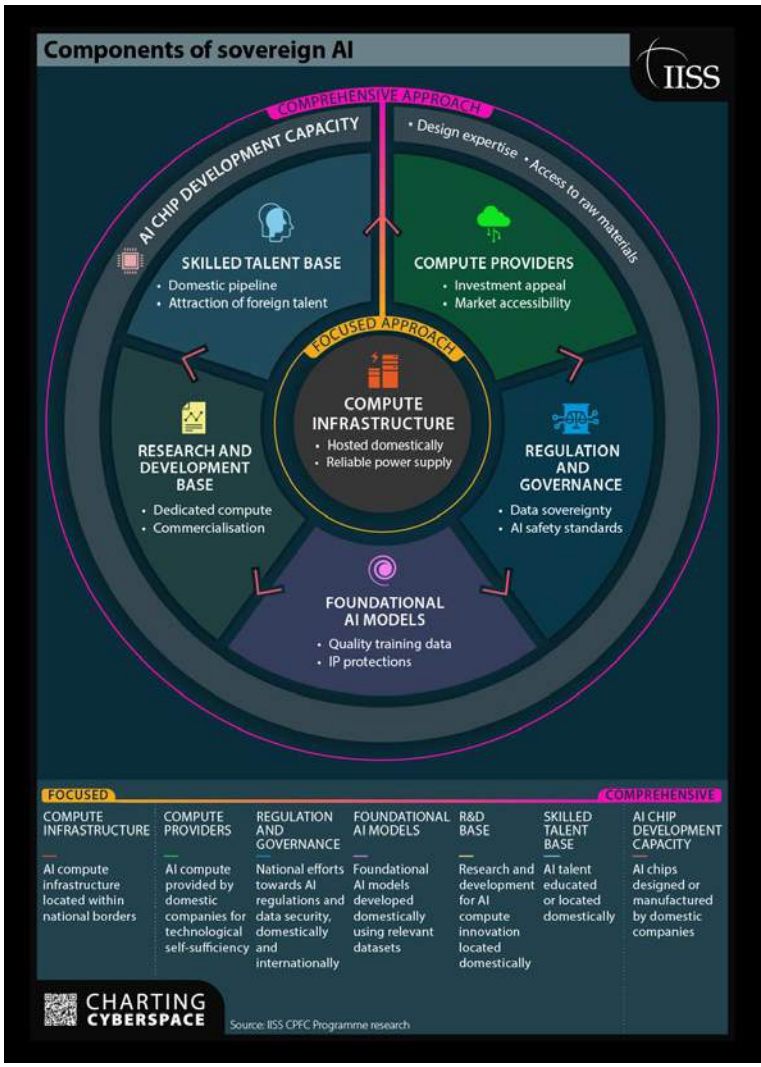
In termini tecnici, l'AI sovrana richiede il controllo dell'**intero stack di intelligenza artificiale**:

- **Dati**: dalla raccolta e archiviazione alla governance e alla residenza.
- **Computing & Network**: data center, connettività resiliente e hardware specializzato.
- **Pipeline di talenti**: sviluppo di una forza lavoro nazionale qualificata in tecnologie AI.
- **Sviluppo di modelli di intelligenza artificiale**: garantiscono la proprietà locale, la formazione e la governance dell'implementazione.
- **Sicurezza**: protezione dei sistemi, dei dati e dell'infrastruttura di intelligenza artificiale dalle minacce in evoluzione.

In altre parole, la sovranità dell'AI non è necessariamente determinata dal fatto che le nazioni possano sviluppare o meno l'AI con le tecnologie locali, ma dal fatto che l'AI possa riflettere le loro norme etiche e culturali, possa sostenerne la crescita economica e promuovere la diversità.

Lo sviluppo di un'AI sovrana comporta molteplici sforzi in almeno sette ambiti:

- infrastruttura di calcolo
- provider di calcolo



(Fonte: *Sovereign AI: pathways to strategic autonomy*, IISS, Virpratap Vikram Singh, 28th August 2025)

- regolamentazione e governance
- modelli di AI
- base di ricerca e sviluppo
- base di talenti qualificati
- capacità legati ai processori di base (chip).

Secondo alcune stime, l'AI sovrana potrebbe rappresentare circa il 15% della spesa globale annuale per le infrastrutture di AI nel prossimo futuro, traducendosi in un'opportunità di 50 miliardi di dollari all'anno.
Alla base della strategia è fondamentale dotarsi di **un'infrastruttura solida e localizzata**. La realizzazione tangibile di Sovereign AI dipende infatti dalla **robustezza e dalla sovranità della sua infrastruttura**. Reti specializzate dedicate, ad alte prestazioni e a bassissima latenza, ottimizzate esclusivamente per i carichi di lavoro di intelligenza artificiale: in sostanza, il concetto di AI Factory. Datacenter in grado di assicurare:

- Capacità **scalabili** per i carichi di lavoro AI.
- **Efficienza energetica** e **ottimizzazione dello spazio fisico**.
- Rispondenza a **una rigorosa giurisdizione nazionale,** sicurezza zero-trust.
- Distribuzione geografica per garantire un**'elevata resilienza**.

Si noti che le società di telecomunicazioni, con le loro strutture di datacenter esistenti e le robuste reti in fibra, potrebbero emergere come partner fondamentali in questa direzione.

MODELLI DI IMPLEMENTAZIONE: INVESTIMENTI IN INFRASTRUTTURA E STRETTA COOPERAZIONE

Per superare la dipendenza tecnologica e prepararsi a esigenze future di AI Sovrana, le nazioni stanno adottando diverse strategie:

- **Fondamenta infrastrutturali**: la realizzazione dell'AI Sovrana poggia su un fondamento non negoziabile, un'infrastruttura robusta e localizzata. Ciò implica la costruzione di *AI Factories* che forniscono capacità su scala *petascale* o *exascale*. Inoltre, si sta investendo in piattaforme software che integrino i dati e l'AI in un'unica architettura operativa e che siano *hybrid-by-design* (in grado di operare *on-prem*, in cloud sovrani o in ambienti ibridi).
- **Cooperazione multilaterale**: per i paesi che non possono sostenere da soli l'onere finanziario, la collaborazione è la risposta. Proposte come "An Airbus for AI" (fa riferimento al consorzio aerospaziale europeo) suggeriscono la creazione di una realtà distribuita tra un consorzio di Paesi a reddito medio (come UK, Canada, Germania, Giappone e Singapore), che uniscono le risorse per competere con i giganti statunitensi e cinesi. Consorzi internazionali come JAIS (guidato da Paesi arabi) dimostrano come la collaborazione possa aiutare a condividere costi, talenti e capacità.
- **Modelli ibridi**: pochissime nazioni possono raggiungere un'autonomia completa su ogni strato dello *stack AI.* Molti potrebbero quindi optare per un approccio ibrido, che bilanci l'impegno collaborativo con partner internazionali con il mantenimento di un controllo decisivo sui componenti e sui dati critici e sensibili.

In conclusione, l'AI Sovrana è una realtà globale in evoluzione. Non è solo una questione di se le nazioni ne abbiano bisogno, ma di quanto velocemente potranno costruirla in modo sostenibile, bilanciando il desiderio di indipendenza tecnologica con la necessità di non isolarsi dall'ecosistema globale di ricerca e innovazione.

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