TIG | THE INNOVATION GROUP

IL CAFFÈ DIGITALE

GENNAIO 2025

AI, QUANTUM E SOVRANITÀ

A **DAVOS** SI PARLA (ANCHE) DI TECNOLOGIA

damian-markut/unsplash

QUESTO MESE ABBIAMO FATTO COLAZIONE CON...

Paolo Cannistraro,
CISO, ENGIE Italia

FOCUS PA

L'utopia di città-stato autogovernate e digitali non passa di moda

INTELLIGENZA ARTIFICIALE

Dalle skill AI alla rivoluzione digitale: la competenza è il nuovo capitale

SOMMARIO

AI, QUANTUM E SOVRANITÀ: A DAVOS SI PARLA (ANCHE) DI TECNOLOGIA

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

L'EDIZIONE 2026 DELL'ANNUAL MEETING DEL WEF A DAVOS SI PROPONE DI AFFRONTARE IL TEMA DEL DIALOGO – "A SPIRIT OF DIALOG" – IN CUI LA TECNOLOGIA DIVENTA UNO DEI TERRENI E ARGOMENTI DI CONFRONTO. QUALE FUTURO IMMAGINIAMO PER L'AI E LE "SUE" INFRASTRUTTURE?

A Davos, dove come ogni inverno si svolge il *World Economic Forum Annual Meeting*, quest'anno continua il dibattito sul futuro della tecnologia, ma l'attenzione è indubbiamente rivolta anche ad altri temi. Se nella passata edizione il focus sull'intelligenza artificiale traspariva già dal titolo dell'evento – "Collaboration for the Intelligent Age" – quest'anno è un tema di cui non si può non parlare, ma che appare come parte di un sistema di ingranaggi più ampio, come una delle variabili del dibattito economico, sociale e geopolitico. All'*apertura del Forum* si parla quindi di un futuro al 2050, di libertà e risoluzione dei conflitti, di collaborazione e dialogo, di definizione di un rapporto sostenibile tra pianeta e umanità, di rispetto della biodiversità e riduzione delle ineguaglianze. Si ribadisce anche il tema della sostenibilità, in termini climatici ed energetici, come assolutamente cruciali nei prossimi venticinque anni, e di gestione e mitigazione della misinformazione e della disinformazione. L'intelligenza artificiale deve essere quindi responsabile e accessibile, per permettere alle persone di utilizzare e trarre vantaggio dalla tecnologia, evitando il rischio di rafforzare diseguaglianze e digital divide. E i social media devono essere gestiti e regolati per ridurre la diffusione di misinformazione e disinformazione, preservando e incoraggiando allo stesso tempo la libertà di espressione. Non si tratta però solo di intelligenza artificiale etica e utilizzo responsabile dei media di informazione. Nel programma ufficiale, si parla anche di tecnologie quantistiche, di sovranità e dell'evoluzione dell'infrastruttura a supporto.

Partiamo dall'intelligenza artificiale. Dai tavoli dell'incontro emerge in particolare la necessità, e la difficoltà, per imprese e organizzazioni *di affrontare la fase successiva del processo di adozione di queste tecnologie*, che richiede un passaggio da una logica di sperimentazione ad una industrializzazione dei business case e delle iniziative, per generare un valore concreto e sostenibile. Questo tema diventa

particolarmente pressante nella prospettiva evolutiva dell'AI agentica, che impone di ripensare strategie, modelli organizzativi e meccanismi di costruzione della fiducia nei confronti dei clienti. A ciò si affiancano riflessioni sempre più centrali sulle implicazioni etiche legate allo sviluppo e alla diffusione di queste tecnologie, che finiscono per catalizzare l'attenzione complessiva. Non si tratta solo di utilizzare al meglio l'innovazione per generare valore, ma di farlo in modo responsabile, con piena consapevolezza degli impatti etici e sociali che essa comporta. Su questo tema interviene *Yuval Noah Harari*, Distinguished Research Fellow del Centre for the Study of Existential Risk, che esorta a non considerare l'intelligenza artificiale come un ulteriore strumento tecnologico: è un agente, in grado di apprendere e prendere decisioni autonomamente; che può essere creativo, inventando prodotti artistici e artefatti; e può mentire e manipolare, per raggiungere gli obiettivi che si pone. Al centro del dialogo emerge il significato stesso del pensare, come chiave per comprendere da un lato la natura dell'essere umano — dal cartesiano «Cogito, ergo sum» — e dall'altro l'evoluzione dell'intelligenza artificiale. L'interrogativo riguarda il ruolo della parola nella costruzione della comprensione del mondo e della verità, un ambito in cui l'AI assume già, senza dubbio, il ruolo di autentico "master of words".

Non si parla però solo di intelligenza artificiale. Occorre affrontare anche i nodi legati allo sviluppo di un *ecosistema dell'innovazione sostenibile in Europa*, a partire dal delicato equilibrio tra innovazione e regolamentazione. Un tema cruciale per comprendere come sostenere la crescita dell'ecosistema europeo, favorendo la disponibilità di capitali, competenze e cultura imprenditoriale necessaria a far scalare start-up e iniziative tecnologiche del Vecchio Continente. Senza tralasciare il tema attuale della sovranità tecnologica, dove fondamentale diventa il bilanciamento tra la messa in sicurezza delle infrastrutture e dei dati critici di uno Stato, riducendo le dipendenze esterne, e gli indubbi vantaggi e i benefici che derivano invece dall'integrazione e dallo scambio di sistemi e tecnologie. La specializzazione necessariamente porta infatti alla creazione di dipendenze, ma occorre valutare e gestire il rischio laddove queste dipendenze rischiano di essere critiche.

Si parla anche di *tecnologie quantistiche*: appena concluso l'anno che le Nazioni Uniti hanno dichiarato l'Anno Internazionale della Scienza e della Tecnologia Quantistica, l'attenzione appare ancora alta sullo sviluppo di questa tecnologia. Fattore competitivo nel futuro prossimo (se non già oggi) e, al tempo stesso, rischio da mitigare per garantire la sicurezza di dati e sistemi in uno scenario post-quantum, la tecnologia quantistica si afferma, insieme all'intelligenza artificiale, come una delle colonne portanti dei prossimi anni. Se l'AI può essere vista come la "rete neurale" che guarda alla realtà, le tecnologie quantistiche ne amplificano la capacità computazionale, estendendone il raggio d'azione e la potenza.

Si torna così al tema dell'intelligenza artificiale, che resta in ogni caso il vero fulcro tecnologico del meeting annuale di Davos. Una sfida che oggi si fa più complessa e impegnativa: non si tratta più solo di raccontarne le potenzialità, ma di comprenderne a fondo vantaggi e criticità, di capire – se possibile – come governarne l'applicazione e di prendere coscienza del suo impatto, insieme alle implicazioni etiche, sociali ed economiche che inevitabilmente comporta.

Mettere in sicurezza le identità macchine

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

LA GESTIONE DELLE MACHINE IDENTITY RAPPRESENTA OGGI UNO DEI PILASTRI PIÙ DELICATI E STRATEGICI DEI PROGRAMMI DI IDENTITY & ACCESS MANAGEMENT. DALL'APPLICAZIONE DEL PRINCIPIO DEL LEAST PRIVILEGE ALL'INTEGRAZIONE CON I MODELLI ZERO TRUST, FINO ALLA GOVERNANCE DEI CERTIFICATI TLS, LE IDENTITÀ NON UMANE SONO DIVENTATE UN ELEMENTO CENTRALE SIA PER LA SICUREZZA SIA PER LA CONTINUITÀ OPERATIVA.

Paolo Cannistraro,
CISO di ENGIE Italia

In questa intervista con **Paolo Cannistraro, CISO di ENGIE Italia**, approfondiamo come un approccio strutturato, basato su policy chiare, automazione e responsabilità definite, consenta di ridurre i rischi cyber e operativi legati a una gestione non corretta delle identità macchina.

Quali sono le principali sfide nella gestione delle Machine Identity, o identità non umane?

Nella nostra realtà, le identità non umane sono formalmente riconosciute all'interno delle policy aziendali e rientrano pienamente nel **perimetro di governance dell'Identity & Access Management**. La principale sfida consiste nel garantire che anche queste identità siano soggette agli stessi principi di responsabilità, ownership e ciclo di vita definiti per le identità umane. Ogni identità tecnica o applicativa deve infatti avere un owner chiaro, uno scopo definito e una durata temporale limitata, evitando quindi la creazione di utenze perpetue. Un aspetto centrale è l'applicazione rigorosa del **principio del *least privilege***. Le identità macchina devono disporre esclusivamente dei permessi strettamente necessari allo svolgimento delle attività per cui sono state create. Questo vale in particolare per i cosiddetti "robot" o account automatizzati, utilizzati per eseguire operazioni ricorrenti sui sistemi applicativi e infrastrutturali.

Sarebbe importante poi utilizzare strumenti di password management per la gestione delle credenziali applicative e per l'inquadramento delle identità macchina all'interno dei processi di Privileged Access Management (PAM). In questo modello, tutte le identità tecniche con privilegi elevati sono trattate come **identità privilegiate**, sottoposte quindi a controlli più stringenti. Un'altra sfida significativa riguarda l'applicazione del **paradigma Zero Trust alle identità non umane**. A differenza delle identità umane, per le quali può esistere una certa flessibilità operativa, le identità macchina non devono beneficiare di alcuna forma di fiducia implicita. Ogni accesso deve essere rigorosamente autenticato, autorizzato e limitato nel perimetro.

Quali potrebbero essere gli impatti negativi di una cattiva gestione delle identità macchine?

La cattiva gestione delle Machine Identity è considerata oggi un rischio rilevante sia dal punto di vista cyber sia dal punto di vista operativo. Lato sicurezza, l'assegnazione di privilegi eccessivi alle identità macchina può trasformarle in un **punto di accesso estremamente critico per un attaccante**. In passato, per semplicità operativa, venivano spesso concessi permessi completi ("full access") agli account automatizzati, con la conseguenza che il furto di una singola credenziale

avrebbe potuto compromettere interi sistemi core. Oggi questo approccio è riconosciuto come **inaccettabile e incompatibile con i principi Zero Trust**. Dal lato operativo, il rischio è altrettanto significativo. Un'errata configurazione di un account automatizzato può causare danni massivi in tempi estremamente ridotti. Poiché le identità macchina eseguono automaticamente ciò che viene loro richiesto, un errore di configurazione può tradursi in cancellazioni massive di dati, modifiche non autorizzate o corruzione di processi critici di business. Il rischio – in questo caso - non è legato solo ad attacchi esterni, ma anche a errori interni, ad esempio, attività di manutenzione non correttamente testate o rilasciate in produzione senza adeguate verifiche. La **mancanza di censimento, di ownership e di documentazione** sul ruolo delle identità macchina rende inoltre estremamente complesso comprenderne la funzione durante le migrazioni di sistema, stabilire se un'utenza sia ancora necessaria, valutare l'impatto della sua dismissione.

Quale direzione avete intrapreso in modo da ottimizzare la gestione delle Machine Identities?

L'organizzazione ha adottato un modello strutturato in cui le identità macchina sono pienamente integrate nelle policy di Identity & Access Management. Le policy servono a definire le diverse tipologie di identità (umane e non umane), le responsabilità degli owner, i requisiti di ciclo di vita, le regole di gestione delle credenziali. Dal punto di vista operativo, l'ambiente è fortemente orientato al cloud, quindi la gestione degli accessi avviene prevalentemente tramite modelli basati su ruoli (RBAC), con permessi definiti in modo granulare e associati a funzioni specifiche.

All'interno del tema più ampio delle idenità macchine, un ambito che richiede particolare attenzione è la gestione dei certificati TLS: voi come approcciate questo aspetto?

La gestione dei certificati TLS è impostata su un modello ibrido che combina automazione, gestione centralizzata e governance di gruppo. Per alcune tipologie di certificati vengono adottati processi di rinnovo automatico basati su protocolli standard, mentre per altre classi è previsto l'intervento di team dedicati che supervisionano l'intero ciclo di vita.Negli ultimi anni la validità dei certificati TLS si è progressivamente ridotta, richiedendo all'organizzazione una gestione dei rinnovi più frequente. Questo ha reso necessario un ampio lavoro di censimento degli asset, mappatura delle dipendenze, definizione delle responsabilità e strutturazione di processi operativi e di controllo, al fine di garantire continuità del servizio e conformità alle policy di sicurezza.Oltre agli strumenti di emissione e rinnovo, sono attivi meccanismi di controllo periodico per individuare anomalie nella configurazione SSL o certificati in prossimità di scadenza. Questi strumenti e processi strutturati, insieme all'automazione che riduce la gestione manuale, contribuiscono a minimizzare il rischio di mancata individuazione delle scadenze, rafforzano la resilienza complessiva anche in presenza di turnover del personale e aumentano la capacità di reazione in caso di problemi o disservizi.

Mercato ICT e aspetti legali: Privacy, Sicurezza online e Intelligenza Artificiale

Valentina Frediani, *Founder & CEO*
Colin & Partners

IL SETTORE DELLE INFORMAZIONI E TECNOLOGIA È SEMPRE PIÙ GRANDE, MENTRE LE LEGGI EUROPEE DIVENTANO PIÙ COMPLESSE PER GESTIRE IL CAMBIAMENTO DIGITALE.

Quali sono gli ambiti di maggiore attenzione in Europa e nel mondo? Un breve, e non esaustivo, excursus su alcune tendenze e novità.

GDPR: CONSOLIDAMENTO E SEMPLIFICAZIONI IN ARRIVO

A sette anni dall'entrata in vigore, il GDPR rimane il pilastro della protezione dei dati personali in Europa, con sanzioni complessive che hanno superato i 6 miliardi di euro a livello continentale. L'Italia si conferma tra i paesi più attivi nell'applicazione della normativa.
Le motivazioni principali delle sanzioni riguardano l'assenza di una base giuridica valida per il trattamento, misure di sicurezza inadeguate e violazione dei diritti degli interessati. La Commissione Europea, con varie iniziative mirate, sta proponendo modifiche mirate a ridurre gli oneri amministrativi legati alla compliance al GDPR, in particolare per le piccole e medie imprese. Si tratta di operare una razionalizzazione rispetto ai temi della governance dei dati o di rendere più efficace la segnalazione degli eventuali incidenti di sicurezza riducendo la necessità di duplicare le comunicazioni, per rispondere alle diverse normative.
Grande attenzione è data al giusto equilibrio tra sviluppo dell'intelligenza artificiale e protezione e tutela dei dati. Questo implica iniziative specifiche anche rispetto ad una più efficiente e snella cooperazione tra organismi nazionali per la protezione dei dati soprattutto per quanto riguarda la gestione dei reclami transfrontalieri in materia.

NIS2: LA NUOVA FRONTIERA DELLA CYBERSICUREZZA

La Direttiva NIS2, entrata in vigore il 16 ottobre 2024, segna senza dubbio un salto di qualità negli obblighi di sicurezza informatica. Le tempistiche di adeguamento sono scaglionate: entro gennaio 2026 alle aziende era richiesto di conformarsi alle regole di notifica degli incidenti, mentre entro ottobre 2026 sarà obbligatorio implementare le misure di sicurezza tecniche e organizzative specificate dall'Agenzia per la Cybersicurezza Nazionale.
L' aspetto innovativo della NIS2, come ormai noto, è la responsabilità personale dei vertici aziendali: i membri degli organi di gestione sono esplicitamente responsabili della conformità, con possibili sanzioni che includono sospensioni temporanee o

esclusione da ruoli dirigenziali. Questo implica un forte impatto sugli aspetti di governance che, nel corso di quest'anno, certamente dovranno essere al centro delle priorità in tema di cybersicurezza.
Il report ENISA 2025, basato sull'analisi di quasi 4.900 incidenti, conferma che oltre il 53% degli attacchi informatici ha colpito proprio le entità essenziali e importanti coperte dalla direttiva. Tra l'85% e il 95% degli incidenti ha origine da comportamenti umani non corretti, rendendo fondamentale l'integrazione tra misure tecnologiche, organizzative e formazione del personale.

AI ACT: L'EUROPA GUIDA LA REGOLAMENTAZIONE DELL'INTELLIGENZA ARTIFICIALE

Il primo quadro normativo globale sull'intelligenza artificiale, noto come AI Act, è formalmente entrato in vigore nell'agosto 2024. il regolamento prevede inoltre un'implementazione graduale con un'entrata in vigore graduale. Infatti, a partire dal 2 febbraio 2025, sono entrati in vigore i divieti sui sistemi a rischio inaccettabile, quelli considerati una chiara ad una minaccia per la sicurezza e per i diritti fondamentali.
Dal 2 agosto 2025 sono ufficialmente in vigore le responsabilità per i fornitori dei sistemi. A partire dal 2 agosto 2026 sarà considerata piena l'applicabilità del regolamento per tutti i sistemi di intelligenza artificiale.
Risale invece al luglio 2025, la versione finale del Code of Practice for General Purpose AI della Commissione Europea, uno strumento di conformità volontario per i fornitori dei sistemi.
l'Italia si distingue in quanto primo stato membro dell'Unione Europea ad avere approvato, nel settembre 2025, una legge nazionale sull'Intelligenza Artificiale pienamente allineata all'AI Act europeo.
L'Italia si è aggiudicata un ruolo pionieristico essendo il primo Stato membro ad aver adottato una legislazione nazionale specifica sui sistemi AI. Con la Legge n. 132 del 23 settembre 2025 (in vigore dal 10 ottobre 2025) designa l'Agenzia per la Cybersicurezza Nazionale (ACN) e l'Agenzia per l'Italia Digitale (AgID) come autorità nazionali competenti sulla materia.
Prevede, inoltre, un programma di investimenti da 1 miliardo di euro dedicati allo sviluppo di startup e PMI nei campi delle tecnologie emergenti.
Si tratta di una norma progettata per essere e complementare al Regolamento UE 2024/1689, colmando gli spazi lasciati alla discrezionalità degli Stati membri senza imporre nuovi obblighi tecnici aggiuntivi rispetto alla norma UE.

CONVERGENZA NORMATIVA E SFIDE OPERATIVE

L'interazione tra queste normative, che hanno avuto un ruolo da protagoniste in questi ultimi anni - GDPR, NIS2 e AI Act - crea un ecosistema normativo complesso ma al tempo stesso integrato. Basti pensare ad esempi semplici come il trattamento di dati biometrici: esso deve rispettare simultaneamente i requisiti del GDPR sulla protezione dati, le disposizioni dell'AI Act sulla classificazione del rischio dei sistemi di riconoscimento, e le misure di sicurezza imposte dalla NIS2 per le entità critiche.
Una convergenza che richiede alle organizzazioni, indipendentemente dalla dimensione, un approccio olistico alla compliance, dove sicurezza informatica, protezione dei dati e governance dell'AI si fondono in un'unica strategia di risk management.
Costante fondamentale e strategica per le organizzazioni, tanto nel pubblico quanto nel privato, è includere in questo ecosistema anche la filiera dei fornitori. La Supply Chain è punto di forza o di grande debolezza a seconda di quanta attenzione e visione a lungo termine si dimostra nel gestirla.
La sfida è quindi bilanciare innovazione tecnologica e conformità normativa, trasformando gli obblighi legali in opportunità di miglioramento competitivo attraverso investimenti strutturati in sicurezza, governance dei dati e adozione responsabile dell'intelligenza artificiale.

L'utopia di città-stato autogovernate e digitali non passa di moda

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

NELL'ULTIMO DECENNIO SI SONO SUSSEGUITI ANNUNCI E INIZIATIVE ORIENTATE ALLA CREAZIONE DI UTOPIE DI GOVERNO INCENTRATE SUL MODELLO DELLA CITTÀ-STATO. GIORNALISTI E MEDIA NE MONITORANO CICLICAMENTE LE EVOLUZIONI, ANCHE SE POCHI SEMBRANO I PROGETTI IN GRADO DI CONCRETIZZARSI

Nelle scorse settimane sul Corriere della Sera *Massimo Gaggi* ha pubblicato un articolo che racconta i più recenti sviluppi dell'utopia – per lo più americana – di città- stato autogovernate, dove la tecnologia svolge un ruolo non secondario: sia perché diversi promotori e supporter di questo modello vengono proprio da questo mondo, sia perché il loro sviluppo è spesso intrecciato alle criptovalute e all'adozione di tecnologie digitali avanzate. Nell'articolo si parla soprattutto di Praxis, una start-up che promuove la creazione di una "nazione digitale" e si proporrebbe, in una location non ancora definita, di costruire una città-stato tecnologicamente avanzata libera da vincoli di governo e fiscali. Ma non è l'unico esempio di annunci e dichiarazioni di progetti simili, che in alcuni casi sembrano aver ricevuto anche supporto e investimenti concreti. Di seguito una rapida panoramica di un fenomeno che, ciclicamente, torna a destare attenzione mediatica.

PRAXIS, COSTRUIRE LA PRIMA "NAZIONE-DIGITALE"

È una start-up fondata nel 2019, inizialmente con il nome di Bluebook Cities, poi diventata "*Praxis*". Il suo obiettivo – almeno da quanto dichiara sul proprio sito – sarebbe quello di costruire la prima "nazione Digitale" al mondo, un nuovo paradigma politico globale in contrapposizione agli Stati-Nazione.

DA PUERTOPIA A SOL, UN'UTOPIA PER CRYPTO IMPRENDITORI A PORTORICO

Questo progetto prende forma in seguito all'uragano Maria, che colpisce Portorico nel 2017. A fronte degli ingenti danni e la distruzione causati dalla calamità, un gruppo di imprenditori e investitori in criptovalute si trasferisce sull'isola e propone l'idea di creare a Portorico una *città basata su blockchain e valute digitali*. Il progetto viene rinominato "Sol", ma non sembra essersi concretizzato.

PROSPERA, LA STARTUP CITY CONTROVERSA SULL'ISOLA DI ROTAN

Questo progetto vede la nascita di *una città-stato innovativa* sull'Isola di Rotan, all'interno di una delle zone economiche speciali, le cosiddette Zones for

Employment and Economic Development (ZEDEs), in Honduras. Lo sviluppo di questa città, gestita da un'azienda privata e la cui cittadinanza ha un costo annuo, ha suscitato anche diverse controversie in ambito ambientale e sociale.

UNA CITTÀ PER LE CRIPTOVALUTE A LA UNION, IN EL SALVADOR

Nel 2021 il presidente di El Salvador annuncia *il progetto "Bitcoin City"*, che prevede la creazione, lungo il golfo di Fonseca, di una città interamente vocata e finanziata dalle criptovalute. Anche la scelta del sito è strettamente connessa al mining di valute digitali: dovrebbe venir costruita ai piedi di un vulcano, insieme ad una centrale geo-termica che genererà energia per alimentare il processo di creazione di criptovalute, notoriamente energivoro. Ad oggi l'unico segnale di concretizzazione di questo progetto sembra essere la costruzione di un aeroporto nell'area, che pare tra l'altro aver generato *preoccupazione in termini ambientali*.

IL PROGETTO SENEGALESE FALLITO DI AKON CITY

Quello di Akon City è un progetto annunciato per la prima volta nel 2018 dal cantante e produttore discografico statunitense (di origine senegalese) Akon. Attualmente però, *riporta la BBC*, pare che a Mbodiène, il sito di 800 ettari identificato per la costruzione della città a circa cento chilometri dalla capitale senegalese, non presenti particolari segni di sviluppo e si valutano utilizzi più realistici di questo terreno, dal significativo valore turistico.

© freepik.com

Dalle skill AI alla rivoluzione digitale: la competenza è il nuovo capitale

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

L'INTELLIGENZA ARTIFICIALE AMPLIFICA IL VALORE DEL TALENTO UMANO E IMPONE A IMPRESE E SISTEMI FORMATIVI UN RIPENSAMENTO PROFONDO.

Per anni è stata chiamata trasformazione digitale ciò che oggi si presenta come una vera e propria rivoluzione digitale: non un progetto, ma un nuovo regime operativo dell'economia. Una recente ricerca del World Economic Forum (WEF)1[1] chiarisce la posta in gioco: senza persone in grado di capire, governare e applicare l'intelligenza artificiale, la promessa della tecnologia resta incompiuta. L'intelligenza artificiale generativa, o GenAI, può essere un moltiplicatore di crescita, ma solo se sostenuta da una base ampia di skill digitali e da un'avanguardia di competenze avanzate su AI e dati.

UNA TRASFORMAZIONE CHE CAMBIA LE COMPETENZE ALLA RADICE

Quella in corso è una trasformazione che modifica il modo in cui pensiamo, interpretiamo e utilizziamo le nostre competenze. Secondo il WEF, infatti, quasi il 70% delle skill digitali vedrà cambiare in modo sostanziale le proprie modalità d'uso: AI e big data sono i domini più esposti alla trasformazione, mentre le abilità umano-centriche, come collaborazione ed empatia, risultano meno impattate. Anche nei settori maggiormente coinvolti, tuttavia, non si parla di sostituzione lineare delle persone, ma di una ridefinizione delle competenze, che devono includere capacità di progettazione, integrazione e supervisione di sistemi potenziati dall'intelligenza artificiale.

IL MERCATO PREMIA CHI HA COMPETENZE RARE, MENTRE CRESCE IL BISOGNO DI SKILL DIGITALI DIFFUSE

Allo stato attuale, le figure davvero capaci di lavorare con l'AI ed estrarre reale valore da progetti che prevedono un suo utilizzo esteso sono significativamente inferiori rispetto alle richieste del mercato. Questo squilibrio è tanto evidente che i profili con competenze solide in AI e machine learning ottengono retribuzioni più elevate e più opportunità, pur rappresentando ancora una quota minoritaria dell'occupazione digitale complessiva. È la dimostrazione che l'AI non sostituirà il talento, ma ne accrescerà il valore nei contesti in cui le competenze sono rare e capaci di sfruttare gli strumenti emergenti. Parallelamente, cresce l'esigenza di competenze digitali di base a tutti i livelli organizzativi, anche per gestire attività quotidiane, dalla produttività personale alle decisioni data-driven.
Nonostante ciò, l'ecosistema formativo e professionale procede più lentamente rispetto alla velocità della trasformazione. Solo una minoranza dei leader d'impresa ritiene che la scuola prepari adeguatamente sui big dati e, ancor meno, sull'intelligenza artificiale. A questo quadro, si aggiunge la situazione ormai strutturale di un'Europa in cui oltre metà delle aziende fatica a reperire figure ICT.

SVILUPPO, VALUTAZIONE E ACCREDITAMENTO COME ARCHITETTURA DI UN NUOVO SISTEMA

Per affrontare questa sfida, il WEF propone una bussola operativa basata su tre direttrici: sviluppo, valutazione e accreditamento delle competenze. Navigare la prima direttrice – lo "sviluppo" – significa riportare le competenze di questa nuova economia al centro dei percorsi formativi e di upskilling, creando ambienti sicuri in cui sperimentare, sbagliare e imparare attraverso simulazioni, laboratori di AI e casi d'uso realistici.
La seconda direttrice – la "valutazione" – implica un cambio di paradigma: non è più sufficiente verificare le conoscenze tramite esami tradizionali o certificazioni vendor-specific, ma occorre misurare la reale capacità di applicare le competenze attraverso progetti concreti, portfolio, hackathon e prove autentiche che valutino non solo l'esito, ma il processo decisionale, il ragionamento e la collaborazione. Infine, l'"accreditamento" richiede credenziali realmente modulari, trasferibili e verificabili, che devono includere metadati dettagliati per rendere trasparente il contesto in cui la competenza è stata acquisita, il percorso seguito e le evidenze prodotte. Solo così le competenze possono essere riconosciute nel mercato del lavoro.

I TEMPI DELL'APPRENDIMENTO E L'INTEGRAZIONE DELLE COMPETENZE

Lo studio evidenzia anche un punto spesso trascurato: i tempi di apprendimento. La soglia d'ingresso su AI e dati è più accessibile di quanto si pensi, con poche decine di ore necessarie per acquisire un livello base di alfabetizzazione digitale e di AI; ma la padronanza avanzata richiede investimenti ben più consistenti, nell'ordine delle centinaia di ore, soprattutto perché deve includere competenze relative a reti, cybersecurity e architetture complesse. L'aspetto strategico è che queste traiettorie di sviluppo sono integrabili: programmazione, intelligenza artificiale, user experience e sicurezza informatica si rafforzano reciprocamente e si innestano su solide competenze analitiche e di system thinking, contribuendo a costruire profili professionali completi e capaci di sostenere la trasformazione digitale.

I SETTORI CHE TRAINANO LA DOMANDA E L'ITALIA

A trainare la domanda di competenze avanzate sono soprattutto i settori ad alta intensità tecnologica come l'ICT, l'automotive, l'aerospace, i servizi finanziari e i capital market, che più di altri considerano skill su AI, programmazione, cybersecurity e design dei sistemi digitali come competenze "core" per la forza lavoro. L'adozione di tecnologie emergenti come advanced analytics e machine learning, in questi ambiti, procede rapidamente e genera una pressione crescente sulla disponibilità di talenti qualificati. Pur in assenza di dati specifici nel report WEF, gli indicatori europei presenti nel documento del WEF fanno desumere abbastanza chiaramente che anche l'Italia affronta difficoltà rilevanti nel reperimento di professionisti ICT e nella diffusione omogenea delle competenze digitali.

TRE SCELTE STRATEGICHE PER COSTRUIRE COMPETENZE SOLIDE E DURATURE

In sintesi, il passaggio dalla trasformazione alla rivoluzione digitale richiede l'evoluzione simultanea dei modelli operativi, del ruolo delle persone e delle infrastrutture formative. Per prosperare, le organizzazioni devono adottare un approccio più maturo allo sviluppo delle competenze: investire in profondità nelle competenze legate all'AI e ai dati (MLOps, governance, prompt/agent engineering, data stewardship, etc.), alzare la soglia minima di skill digitali e AI literacy per tutti i ruoli e rendere le competenze visibili e trasferibili attraverso metriche e sistemi di riconoscimento basati sulla reale applicazione e sull'impatto generato.

1 Fonte: "New Economy Skills: Building AI, Data and Digital Capabilities for Growth", World Economic Forum, Dicembre 2025

Threat Hunting e Threat Intelligence: verso una catena integrata

Enrico Frumento, *Cybersecurity Research Lead*
Cefriel

DURANTE L'EVENTO "*SOVRANITÀ DIGITALE E CYBERSECURITY*" DELLO SCORSO DICEMBRE 2025, È STATO SOTTOLINEATO COME THREAT HUNTING, THREAT INTELLIGENCE E AI DEBBANO ESSERE INTEGRATI IN UNA CATENA INFORMATIVA CONTINUA, PIUTTOSTO CHE OPERARE COME FUNZIONI ISOLATE.

Storicamente, il threat hunting è nato come attività operativa per individuare minacce nascoste nei sistemi, mentre la threat intelligence è una funzione strategica di analisi del panorama delle minacce. La separazione di queste funzioni ha creato un gap: i segnali tecnici prodotti dai threat hunter non raggiungono chi deve prendere decisioni, mentre le informazioni strategiche restano scollegate dall'operatività.
La maturazione del settore ha mostrato che l'efficacia dipende dalla capacità di collegare queste fasi in un processo strutturato, che trasforma dati grezzi in intelligence azionabile. **L'AI ha accelerato questa integrazione**, permettendo di processare volumi di dati altrimenti ingestibili, ma introduce anche nuove criticità che richiedono competenze umane per essere gestite correttamente.
Le organizzazioni raccolgono enormi quantità di dati di sicurezza, generando *data lake* che, senza governance costante, degenerano rapidamente in *data swamp*, archivi inutilizzabili. L'errore comune è pensare che l'AI possa correggere autonomamente questi dati: in realtà, amplifica i difetti strutturali. Il principio "*garbage in, garbage out*" è più insidioso con l'AI, perché i modelli producono output coerenti apparentemente validi anche se basati su dati compromessi, propagando **bias, correlazioni spurie e allucinazioni**. La gestione della qualità dei dati è quindi cruciale per l'affidabilità dell'intera pipeline.
I sistemi di AI presentano tassi di errore intrinseci: bias statistico, correlazioni spurie, allucinazioni dei modelli

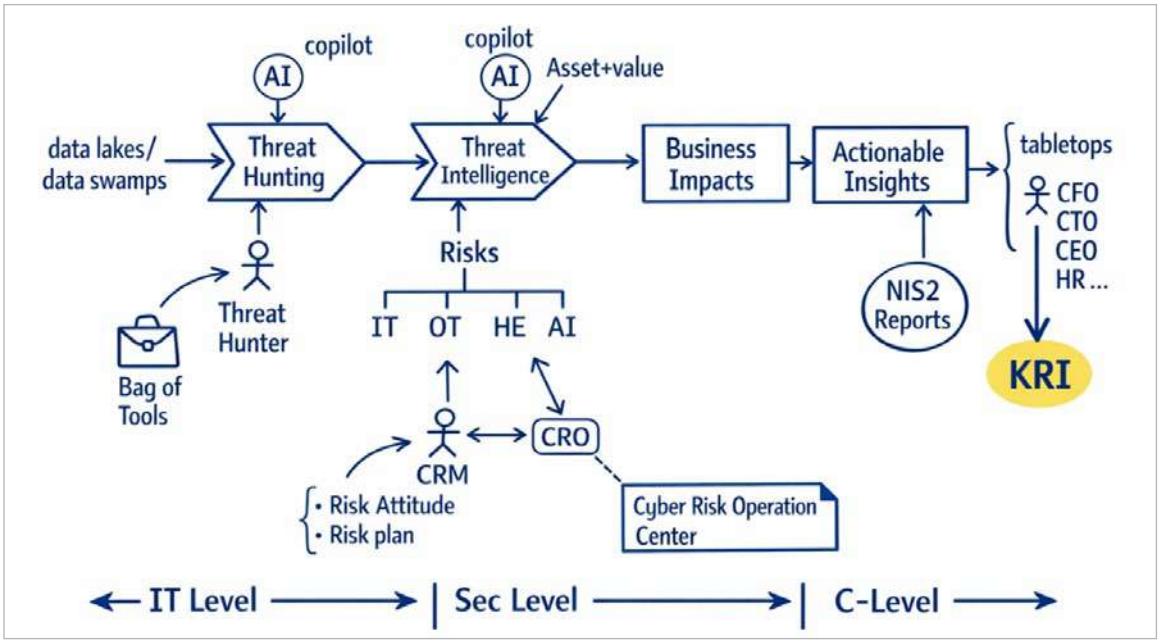
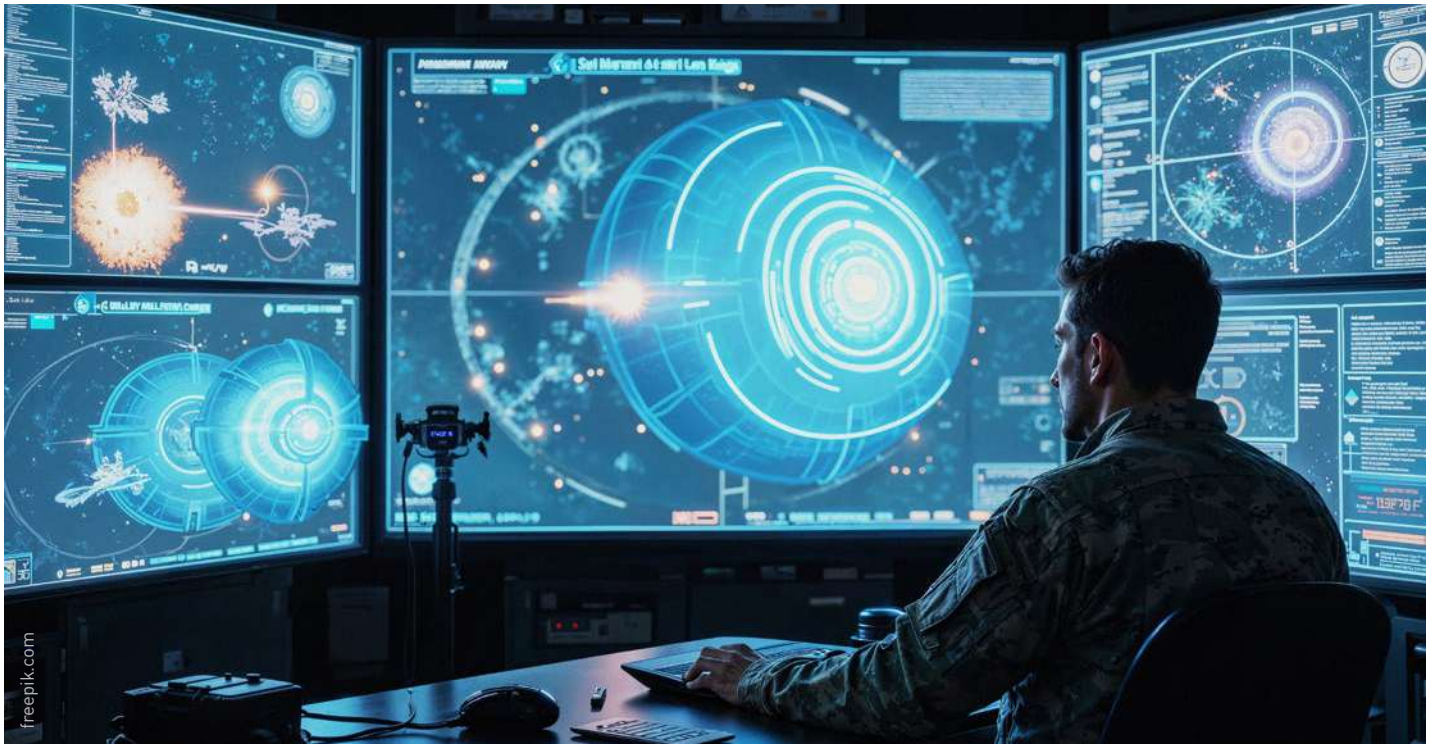


Figura 1 – La figura mostra come si collegano tre livelli operativi: Threat Hunting, Threat Intelligence e Business Impact per produrre Actionable Insights



generativi e incertezza statistica. Questi limiti non sono difetti temporanei, ma proprietà strutturali che devono essere comprese per utilizzare efficacemente l'AI in cybersecurity.

La catena operativa nella gestione delle informazioni sulle minacce collega tre livelli organizzativi (come mostra la figura successiva): IT Level, Sec Level e C-Level.

Al livello IT, i **threat hunter** analizzano log, eventi di rete e comportamenti di sistema per individuare anomalie, ora supportati dall'analisi comportamentale dell'AI, che riduce il *dwell time* delle minacce avanzate. L'AI filtra il rumore, ma la verifica umana resta indispensabile per distinguere tra falsi positivi e minacce reali.

Questi segnali alimentano la **threat intelligence**, trasformando dati tecnici in informazioni contestualizzate. L'AI automatizza la classificazione dei dati e l'estrazione di TTP (Tactics, Techniques, Procedures) dai report usando framework standardizzati come MITRE ATT&CK, permettendo agli analisti di concentrarsi sulle valutazioni prioritarie. Tuttavia, i modelli presentano limiti semantici: senza supervisione umana, possono produrre classificazioni errate che contaminano le basi informative.

Il livello strategico richiede la traduzione dei dati tecnici in **Business Impact e Actionable Insights**: quali minacce hanno effetti reali sull'operatività, la reputazione o la compliance aziendale? Queste informazioni guidano decisioni concrete su investimenti, policy, formazione e audit, producendo **Key Risk Indicators comprensibili al management**. La funzione del **Chief Risk Officer** è critica per collegare intelligence tecnica e decisioni strategiche, garantendo che il C-Level operi su basi analitiche piuttosto che percezioni.

L'AI amplifica capacità umane in ogni fase della catena, ma non elimina la necessità di **competenze qualificate**. Tre limiti operativi chiave devono essere sempre considerati: la **manutenzione continua** dei modelli e delle mappature, il **rischio di dequalificazione** degli analisti se si affidano ciecamente all'AI, e **l'alert fatigue**, che richiede calibrazione accurata per evitare che gli allarmi critici vengano ignorati. La sostenibilità della catena operativa richiede impegno costante in budget, formazione e governance.

In conclusione, la catena *Threat Hunting → Threat Intelligence → Business Impact → Actionable Insights* non è una sequenza tecnologica ma un processo organizzativo che unisce competenze tecniche, di sicurezza e strategiche. L'AI è uno strumento potente, ma va **usata con giudizio e supervisionata**, all'interno di flussi informativi definiti. La direzione evolutiva non è l'automazione totale, ma l'amplificazione intelligente delle capacità umane: le organizzazioni che investono solo in tecnologia senza sviluppare competenze falliscono, mentre quelle che integrano AI in processi strutturati trasformano i dati in intelligence reale.

La vera domanda non è se adottare l'AI, ma come mantenere l'intelligenza umana necessaria a guidarla.

*Un articolo più esteso in cui **Enrico Frumento, Cybersecurity Research Lead di Cefriel** approfondisce le relazioni che intercorrono tra i diversi ambiti del Threat hunting e della Threat intelligence, la necessità di collegarle tra loro in una catena informativa e decisionale integrata, l'apporto corretto fornito dall'AI in questo contesto, è disponibile sul canale cybersecurity di TIG: Threat hunting e threat intelligence: la catena che trasforma i dati in decisioni.*

Dall'AI alle biotecnologie, il progresso bussa alla porta

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

CODING TOTALMENTE AUTOMATIZZATO. DATA CENTER GIGANTI. CHATBOT CHE SOSTITUISCONO UNA RELAZIONE. GENETICA DI PRECISIONE E GENETICA OLTRE L'ETICA. SONO ALCUNE DELLE TECNOLOGIE PROTAGONISTE DEL 2026.

Quali saranno le tecnologie protagoniste del 2026? Bolle in pentola qualcosa di davvero dirompente, anzi di più, qualcosa di rivoluzionario? A leggere le previsioni di molti accreditati osservatori (dovremmo citarne decine), si direbbe che l'intelligenza artificiale sarà ancora il perno di molte discussioni e promesse. Ma allargando lo sguardo fuori dall'ambito dell'informatica, come fa ogni anno nelle sue previsioni *MIT Technology Review,* vedremo innovazioni o forse rivoluzioni anche nel campo delle biotecnologie, dell'energia e dell'economia dello spazio.

L'ESERCITO DEI GIGANTI

Tra gli *"avanzamenti che, crediamo, quest'anno muoveranno il progresso o stimoleranno maggiori cambiamenti, nel bene e nel male",* scrivono i redattori di *MIT Technology Review,* c'è prevedibilmente l'AI. Tra i protagonisti del 2026 ci sono innanzitutto i **data center hyperscale** (anche detti cloud data center o AI Factory), cioè enormi infrastrutture di calcolo in cui decine o centinaia di migliaia di Gpu sorreggono applicazioni di addestramento e inferenza.
Il loro numero, la capacità di calcolo e il fabbisogno energetico inevitabilmente cresceranno, considerando che aziende come Amazon, Google, Meta, Microsoft e OpenAI vi stanno investendo cifre nell'ordine delle centinaia di miliardi di dollari. Nella gara a fare di più, Elon Musk ha da poco annunciato l'operatività di Colossus 2, il nuovo gigantesco data center di xAI, con prestazioni e consumi energetici da record. Con circa 550.000 acceleratori Nvidia già in funzione, Colossus 2 sfonda la soglia di 1 GW di potenza dedicata all'addestramento di modelli (al servizio del discusso Grok) in un singolo data center, ma ancora non basta: xAI vuole arrivare a 1,5 GW entro il prossimo aprile, salendo poi a 2 GW in future configurazioni.

L'AI PRENDE IL SOPRAVVENTO NEL CODING

Nell'oroscopo tecnologico del 2026 c'è anche il ***generative coding***, cioè la scrittura di codice automatizzata o assistita dall'intelligenza artificiale, che altri chiamano *vibe coding* (espressione che però indica non tanto la tecnica ma l'approccio, l'attitudine a scrivere codice seguendo la "vibrazione"). Se ne è parlato fin dal lancio di ChatGPT e dei suoi emuli, ma se inizialmente i Large Language Model già funzionavano bene nell'analisi di grandi volumi di dati e nella generazione di contenuti, non erano altrettanto performanti nel coding.
Fino a poco tempo fa l'AI veniva usata un po' con la mano sinistra, soprattutto per il *debugging* (correzione dei problemi) o come supporto per la scrittura di funzioni. Oggi, invece, strumenti come GitHub Copilot, Cursor, Lovable o Replit permettono anche ai profani di creare interamente app per smartphone, giochi, siti Web o altri prodotti digitali in poche mosse, in pochi *prompt*. E anche le Big Tech, a cui certo non mancano gli sviluppatori esperti, sfruttano l'AI per velocizzare i progetti e per tagliare i costi. Circa il 30% del codice creato all'interno di Microsoft è opera dell'intelligenza artificiale, a detta dell'azienda di Redmond, mentre Google è arrivata al 25%.

RELAZIONI ARTIFICIALI

L'intelligenza artificiale torna una terza volta nelle previsioni di *MIT Technology Review,* in forma di **AI companion** (o social companion): chatbot progettati per dialogare simulando empatia e mostrando di avere una personalità. Sebbene sia possibilissimo, in teoria, usarli solo per fare conversazione in leggerezza, per diatribe filosofiche o per allenarsi nella pratica di una lingua straniera, spesso questi strumenti vengono utilizzati per trovare supporto psicologico o finiscono per diventare il

sostituto di un'amicizia, un partner, una figura parentale. Servizi come Replika, il pioniere del settore, permettono anche di creare un avatar e di fare videochiamate con l'interlocutore artificiale.
La frequentazione degli AI companion riguarda soprattutto i più giovani, con tutti i rischi che ne derivano. Secondo un recente studio di Common Sense Media, negli Stati Uniti il 72% degli adolescenti ha almeno una volta dialogato con un chatbot "compagno". Tra costoro, uno su tre si è sentito a disagio per qualcosa che il programma ha detto o ha fatto; uno su tre, inoltre, ha preferito il chatbot a una persona reale per discutere di questioni importanti o gravi.

APRIRE LA "SCATOLA NERA"

Di fatto, ogni giorno centinaia di migliaia di persone interrogano strumenti come ChatGPT, Gemini o Claude senza chiedersi come sia stato prodotto un contenuto o una risposta, in base a quali dati e criteri. Il problema però è reale, specie se pensiamo ai potenziali abusi di queste tecnologie per scopi di disinformazione o propaganda, oppure ad attacchi informatici che alterano il modello sottostante e, a cascata, i suoi output. In un ambito come la sanità, per esempio, la trasparenza dell'intelligenza artificiale non è un optional.
Tuttavia non dobbiamo per forza arrenderci al fatto che l'intelligenza artificiale sia una *black box*. Per "smontare" la scatola nera esistono metodi e tecniche di *reverse engineering* e di *explainable AI* (intelligenza artificiale "spiegabile") e nei prossimi mesi è probabile che sentiremo parlare anche di **interpretabilità meccanicistica**. Si tratta allo stesso tempo una tecnica di ingegneria inversa e di un campo di ricerca che esamina i meccanismi di calcolo delle reti neurali artificiali. La Mechanistic Interpretability può mettere a nudo i modelli di AI per trovare eventuali difetti o pregiudizi (*bias*), ampliando il margine di controllo dell'uomo su una tecnologia sempre più potente e complessa.

DALLA RESURREZIONE GENETICA AL TURISMO SPAZIALE

Fuori dai confini dell'informatica, la "top 10" di quest'anno è dominata dalle biotecnologie e dalle tecnologie per l'energia, con un'incursione nella space economy. Crescerà, nel mondo, il ricorso al **nucleare** come alternativa ai combustibili fossili o alle rinnovabili intermittenti, non sempre adatte o sufficienti laddove sia richiesta una continuità certa. L'avanzamento del nucleare è legato ai piccoli reattori modulari, che presentano vantaggi di costi ridotti, tempi di realizzazione più brevi e maggiore flessibilità per diverse applicazioni.
L'elenco dà spazio anche alle **batterie agli ioni di sodio,** che potrebbero gradualmente sostituirsi alle tecnologie basate su litio. Adatte a sistemi di accumulo e auto elettriche, presentano diversi vantaggi, tra cui la buona potenza in uscita, le ottime prestazioni a basse temperature, la resistenza agli incendi e costi di produzione che, a tendere, saranno inferiori a quelli delle batterie al litio.
Ci sono altri tre fenomeni da tenere d'occhio nel campo delle biotecnologie: uno è l'**editing genomico**

personalizzato. Tecniche di ingegneria genetica di precisione come il CRISPR (Clustered Regularly Interspaced Short Palindromic Repeats, anche detta "forbici molecolari"), che permettono di correggere errori genetici, inserire, rimuovere o sostituire sequenze di DNA, hanno alle spalle più di un decennio di sperimentazioni. Ma solo nel febbraio del 2025 per la prima volta dell'Ospedale Infantile di Philadelphia è stato realizzato un intervento di editing genomico ad personam e fuori dal laboratorio, su un bimbo di sette mesi affetto da una grave malattia metabolica.
Più controversa è un'altra biotecnologia che sta movimentando investimenti: la **"resurrezione genetica"** o "de-estinzione", ovvero l'impiego di tecniche di editing del DNA per riportare in vita specie estinte. Il pensiero va automaticamente a *Jurassic Park* o alla povera pecora Dolly, "generata" in Scozia nel 1996, primo mammifero clonato con successo a partire da una cellula mammaria. Se Dolly visse per sette anni, esperimenti fallimentari (come quello dello stambecco dei Pirenei clonato nel 2003, vissuto solo per pochi minuti) evidenziano i rischi di queste manipolazioni della biologia. Auguriamo più fortuna al futuro mammut, o meglio all'ibrido elefante-mammut a cui sta lavorando la società biotech texana Colossal Biosciences: dopo aver raccolto 200 milioni di dollari di finanziamenti, ha promesso di riportare sulla Terra il pachiderma del Cenozoico nel 2028. In wishlist ci sono anche il dodo e la tigre della Tasmania.
Quest'anno proseguirà anche il dibattito sull'**embryo scoring,** cioè sulle tecniche di valutazione degli embrioni prima della fecondazione in vitro. Con un'analisi delle caratteristiche morfologiche e con algoritmi di intelligenza artificiale viene determinato un punteggio che misura la probabilità di gravidanze senza complicazioni e il rischio di malattie genetiche. Fin qui niente di nuovo, sono tecniche impiegate fin dagli anni Novanta. Oggi, però, esistono startup come le statunitensi Genomic Prediction, Heliospect Genomics e Orchid, che aiutano a predire non solo il rischio di patologie come diabete o cancro ma anche l'altezza e le capacità cognitive del nascituro. Selezionare un embrione in base alla presunta intelligenza sottesa nel DNA assomiglia a una forma di eugenetica senza etica, che non a caso in Italia e in molti Paesi è vietata (ma non negli Stati Uniti, dove comunque non è chiaramente regolamentata).
L'unica tecnologia, fra le dieci selezionate, che ci consente di alzare gli occhi al cielo sono le stazioni spaziali commerciali, destinate non solo a supportare missioni scientifiche ma anche a facoltosi "turisti". Aziende come la Blue Origin di Jeff Bezos (che ha già fatto discutere lo scorso aprile, tra critiche e meme, per il volo da 11 minuti di un gruppo di ricchissime), Axiom Space, Vast Space, Virgin Galactic e Voyager Space permetteranno a selezionati passeggeri di sperimentare la microgravità e spettacolari visioni della Terra.

I "FLOP" DA DIMENTICARE

Imparare dagli errori del passato è sempre utile, anche nell'ambito del digitale. E nel 2025 non sono mancati i lanci fallimentari, le idee strampalate o semplicemente stupide. Secondo *MIT Technology Review,* il peggio si è visto con **$TRUMP**, la criptovaluta di tipo *meme coin* (token digitali legati a immagini umoristiche che circolano sui social) che richiamava l'immagine e il branding di Donald Trump, lanciata nel gennaio 2025 sulla blockchain di Solana. Oltre a presentare un rischio di altissima volatilità, come tipico dei meme coin, $TRUMP ha attirato critiche per via del conflitto di interesse tra il ruolo istituzionale e politico del presidente Usa e l'attività commerciale e finanziaria di una criptovaluta.
Altra disastrosa commistione fra politica e potere economico e imprenditoriale è stata l'iniziativa **DOGE** (Department of Government Efficiency) di **Elon Musk**, lanciata a inizio 2025 per aiutare la Casa Bianca a ridurre la spesa pubblica. Spregiudicati tagli di posti di lavoro e mancato raggiungimento degli obiettivi hanno alimentato il malcontento e spinto a chiudere il progetto dopo soli quattro mesi. Intanto, però, le vendite di auto

elettriche e le azioni Tesla erano già crollate.
Ha la firma di Elon Musk un altro flop del 2025, un disastro commerciale più che tecnologico: il Cybertruck di **Tesla**. Dopo anni di temporeggiamento, è stato lanciato nel 2024 con un buon riscontro di quasi 39mila veicoli venduti. L'anno seguente, però, le immatricolazioni sono crollate a poco più di 20mila, risultato lontanissimo dalle centinaia di migliaia a cui puntava Musk.
Può almeno suscitare simpatia **NEO, un "robot domestico" umanoide** che aiuta nelle faccende domestiche, progettato dalla startup 1X e attualmente in preordine. L'idea è valida, ma NEO ha due grossi problemi. Il primo è il prezzo: 499 dollari per il noleggio mensile, 20.000 per l'acquisto. L'altro problema sono la scarsa efficienza del robot e la sua lentezza: secondo il Wall Street Journal, impiega più di due minuti per piegare una maglietta e non riesce a svolgere azioni semplici come aprire una noce. Inoltre, pur pubblicizzato come "autonomo di default", spesso il robot necessita di essere comandato da remoto, da una persona che indossa visori.
Pioggia di critiche, da utenti e da addetti ai lavori, anche per l'**AI sicofantica** (Sycophantic AI), cioè per la tendenza di programmi come ChatGPT ad adulare l'utente o ad assecondarlo quando ha torto, pur di non restare senza qualcosa da dire. Può dipendere dal tipo di addestramento e anche dai prompt ricevuti, fatto sta che l'adulazione non è così semplice da estirpare, sebbene gli sviluppatori di Large Language Model ci stiano lavorando (principalmente con tecniche di Addestramento con feedback umano e strumenti di supervisione).
Tra i flop del 2025 c'è anche la già citata **Colossal Biosciences**, che pure compare anche tra le promesse di rivoluzione futura. L'azienda ha annunciato di aver fatto nascere tre esemplari di **enocione**, o lupo terribile, una specie scomparsa da almeno 10mila anni.
Dopo il clamore mediatico, con tanto di copertina del *Time* dedicata, la comunità scientifica ha ridimensionato il tutto, sottolineando che si trattava di canidi geneticamente modificati e solo in parte simili alla specie estinta.
Il 2025 è stato anche l'anno in cui l'**Apple Watch a "emissioni zero**", così descritto da Cupertino al suo lancio nel 2023, è stato decretato come tutt'altro che ecologico. Apple aveva dichiarato la neutralità carbonica dei modelli Series 9, SE e Ultra 2, in virtù dell'energia rinnovabile usata e dei progetti di compensazione delle emissioni di gas serra prodotte. Lo scorso agosto, però, un tribunale di Francoforte ha bollato l'operazione come *greenwashing*, dato che molte delle attività di compensazione realizzate da Apple non avrebbero effetti certi e duraturi.
Bocciatura sonora anche per le **azioni antivax** del Segretario della salute e dei servizi umani degli Stati Uniti d'America, Robert Francis Kennedy Jr., che ha cancellato mezzo miliardo di dollari di fondi destinati a progetti di ricerca su vaccini a mRNA. Un fallimento di altro tipo è stata la chiusura della **sezione di Wikipedia in lingua groenlandese**: da strumento di preservazione linguistica per un idioma parlato da meno di 60mila persone, purtroppo era diventata una collezione di articoli frutto di traduzioni automatiche e pieni di errori. Un segno nel fatto che in certi casi, ancora, dell'intelligenza artificiale è meglio fare a meno.

La sovranità digitale che vorrei

Alessia Valentini, *Advisory Board Member*
Osservatorio sulla Sicurezza Nazionale (OSSN) Unipegaso

LA TRASFORMAZIONE DIGITALE HA DATO ORIGINE ALLA NECESSITÀ DI AVERE UNA COMPLETA CAPACITÀ DI CONTROLLO SULLA COMPONENTE DIGITALE ED IN PARTICOLARE SUI DATI GESTITI.

È nato quindi il termine di **sovranità digitale** che indipendentemente dall'entità che deve esercitarla (azienda grande o piccola o organizzazione pubblica), si riferisce alla capacità di poter essere **autonomi e liberi sulle decisioni** legate al destino della propria organizzazione, senza subire nessun potenziale condizionamento dato dalle dipendenze tecnologiche.
Le leve di autonomia strategica nel contesto digitale richiedono la capacità di controllare chi elabora i dati di interesse e dove lo fa; il che significa avere consapevolezza delle partnership e delle catene di fornitura per le scelte di tecnologie abilitanti così da non rischiare una sorta di "ricattabilità digitale".
La sovranità digitale è dunque un concetto che pesa sempre di più sulle organizzazioni di ogni ordine e grado e si inserisce nel più ampio tema della **sostenibilità del business**, tipicamente legata a fattori variabili come i trend di mercato, la concorrenza e le competenze/formazione della forza lavoro. Per consolidare la sostenibilità del business a lungo termine si rende quindi necessario indirizzare e realizzare una piena sovranità tecnologica, mediante scelte strategiche ponderate e tese a valutare la "convenienza" non solo in chiave economica di spesa, ma anche in **ottica geopolitica**.

SOVRANITÀ DIGITALE IN PILLOLE

Una definizione completa di Sovranità Digitale è stata fornita da **Roberto Baldoni**, primo Direttore Generale dell'Agenzia Nazionale per la Sicurezza Cibernetica e Professore Onorario di Informatica presso l'Università di Roma La Sapienza, nel suo libro *"Charting Digital Sovereignty: A Survival Playbook"* secondo cui la piena sovranità digitale di una nazione sta ne *"l'esercizio dell'autorità su tutti i dati generati dai cittadini e dalle imprese; la capacità di utilizzare tecnologie sicure e affidabili per l'elaborazione di questi dati, supportata da una forza lavoro sufficiente e fidata; la creazione e mantenimento continuo di una collaborazione internazionale per affrontare in modo proattivo le minacce, unitamente ad un contesto sociale pienamente consapevole ed educata sui rischi nel cyberspazio"*.
Per realizzare la Sovranità Digitale è necessario agire su 4 pilastri equivalenti ad una rotta prestabilita: il **controllo dei dati**, le **capacità tecnologiche e quelle professionali**, **consapevolezza delle persone**, la capacità di creare **alleanze internazionali**.
Questi elementi sono fondanti e abilitanti per ogni soggetto che voglia raggiungere l'autonomia sui propri dati: che sia una piccola, media o grande impresa privata, un ente pubblico o uno Stato sovrano.
Per raggiungerli, qualsiasi tipo di entità, dovrebbe strutturare un piano strategico che li preveda considerandoli però 'mobili nel tempo' a causa di eventi scientifici, tecnologici, o geopolitici che modificano le condizioni per la sovranità digitale, rendendo necessaria una rivalutazione periodica delle vulnerabilità (tecniche, organizzative, formative, procedurali, di processo o normative) e introdurre correttivi e miglioramenti adeguativi appropriati. Cruciale anche l'introduzione di metriche e KPI per valutare i progressi e i necessari aggiustamenti. Quindi per acquisire una postura appropriata alla Sovranità Digitale è strettamente necessario organizzarsi, e in una parola, governare il processo. La governance si realizza in modo strutturato, preferibilmente non in balia di uno stato di emergenza e mai e poi mai per improvvisazione.

LA SOSTENIBILITÀ DEL BUSINESS TRASFORMATO DIGITALMENTE

Quando si guarda alle misure di sostenibilità del business, **la sovranità digitale ne è un abilitante** perché consente di realizzare il **controllo strategico su dati e infrastrutture, riducendo dipendenze esterne, rischi**

di sicurezza (cybersecurity), legali (normative estere) e di fatto porta alla resilienza operativa. Resilienza che è condizione necessaria per una competitività a lungo termine e che, insieme alla indipendenza tecnologica, conferisce alle organizzazioni la capacità di innovare in modo autonomo e conforme a valori e leggi locali. Poiché oggigiorno la maggior parte dei prodotti digitali afferisce alle big tech americane o ai colossi cinesi, una vera indipendenza tecnologica è complessa, a meno di ingenti investimenti, non sempre accessibili e sostenibili nel tempo. Per riprendere in mano le sorti dei dati di interesse e delle tecnologie che li elaborano, la scelta di **software Open Source** (a patto di saperlo personalizzare e gestire secondo i criteri di Cybersecurity) può costituire una valida alternativa. In effetti l'Open Source Software (OSS) potrebbe costituire un elemento chiave o anche un prerequisito per il rafforzamento della sovranità digitale, per lavorare in modo indipendente e autonomo alle soluzioni applicative necessarie ad una organizzazione. Ciò **evita effetti di lock-in e amplia il know-how tecnico** dell'azienda.

LA SOVRANITÀ DIGITALE A LIVELLO DI STATO E NELL'ASSETTO EUROPEO

Nel paper pubblicato dall'Osservatorio Sulla Sicurezza Nazionale (OSSN) dal titolo *"Sicurezza europea: evoluzione della NATO, scenari, interessi nazionali e alternative"* in cui si tratta la condizione europea rispetto alla NATO dal punto di vista della sicurezza nella sua accezione più ampia (fisica e digitale, civile e militare), un intero paragrafo è dedicato alla Sovranità Digitale e Tecnologica che ha un peso significativo sull'autonomia Europea, (specie se confrontata con i servizi digitali delle BIG tech, oggi tenute a briglia dall'amministrazione Trump) e che quindi sembra di particolare urgenza a fronte degli sviluppi geopolitici e delle frammentazioni a valle della guerra dei dazi. In questo scenario, il paper sottolinea come "*l'ultimo miglio che sembra mancare alla roadmap europea già tracciata è quello di 'imboccarla' con decisione avviando progettualità specifiche e risultati concreti. I*


©Adobe Stock

progetti potrebbero essere il risultato di una prioritizzazione delle tecnologie di interesse, scelte da tutti i paesi UE o un sottogruppo rappresentativo, accomunato dalle stesse esigenze e requisiti. Un ulteriore auspicio abilitante potrebbe arrivare dallo sviluppo di strumenti di politiche di defiscalizzazione per gli investimenti e da politiche atte a favorire partenariati pubblico privati (PPP) per alcuni tipi di tecnologie dirompenti emergenti".
In particolare, nelle conclusioni si esplicita come la superiorità tecnologica costituisca un vantaggio multidimensionale sia a livello civile che militare e il dominio dell'informazione e di quella digitalizzata si fa fondante. Pertanto, l'obiettivo di Sovranità Tecnologia e Digitale si conferma come un tema regolatorio ma anche materialmente operativo sia a livello di politica che di politica industriale, a livello nazionale, Europeo e sovranazionale Europeo.

L'articolo completo "**La sovranità digitale che vorrei**" di **Alessia Valentini**, è disponibile sul canale cybersecurity di TIG a questo indirizzo: *https://channels.theinnovationgroup.it/cybersecurity/la-sovranita-digitale-che-vorrei/*

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