TIG THE INNOVATION GROUP

IL CAFFÈ DIGITALE

FEBBRAIO 2026

Sovranità digitale europea

LE NOVITA DEL 2026

QUESTO MESE ABBIAMO FATTO COLAZIONE CON...

Giulia Ajmone Marsan,
economista, Global Foresight Network del World Economic Forum, Economic Research Institute for ASEAN and East Asia

LA TRASFORMAZIONE DIGITALE

Data Management 2026: l'AI accelera, ma vince chi ha le fondamenta solide

NUMERI E MERCATI

Il rinascimento del deep tech italiano

notes

THE INNOVATION GROUP

SOMMARIO

Sovranità digitale europea: le novità del 2026

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

Sotto il cappello della sovranità europea si stanno radunando di mese in mese nuove iniziative e annunci, che delineano e arricchiscono sempre più il dibattito sul tema. Da metodi per valutare il livello di sovranità dei servizi cloud, a dichiarazioni politiche e risoluzioni del Parlamento a Strasburgo, gli ultimi mesi tra il 2025 e il 2026 si sono dimostrati particolarmente ricchi di novità.
Il tema della sovranità digitale è ormai al centro del dibattito sul futuro e sulla sostenibilità dell'Unione Europea. In un contesto economico e geopolitico sempre più instabile e ostile, crescono le preoccupazioni per le dipendenze strategiche del Continente in settori chiave per il funzionamento e la sicurezza dei sistemi nazionali. A ribadire questo rischio è anche una recente risoluzione del Parlamento Europeo, che evidenzia come oggi l'Unione dipenda per oltre l'80% da prodotti, servizi, infrastrutture e proprietà intellettuale digitali provenienti da Paesi extraeuropei. Un dato che mette in luce la vulnerabilità del sistema europeo in ambiti cruciali come il cloud, i semiconduttori, la cybersecurity e le piattaforme digitali. In questo scenario, diventa quindi rilevante interrogarsi sul chiaro significato dello sviluppo di una sovranità tecnologica europea, che indubbiamente deve essere in grado di raccogliere e valorizzare iniziative e interventi lungo tutta la catena del valore dell'innovazione e del digitale.

LA SOVRANITÀ DIGITALE EUROPEA A FINE 2025

Già il 2025 si è dimostrato un anno ricco a livello europeo in termini di iniziative e annunci sul tema della sovranità digitale. A fine ottobre la Commissione ha pubblicato il Cloud Sovereignty Framework (CSF), con cui vengono definiti gli obiettivi, i livelli di garanzia (i cosiddetti Sovereignty Effectiveness Assurance Level - SEAL) e la metodologia di

punteggio (il "Sovereignty Score") da utilizzare per valutare la sovranità dei servizi cloud lungo diverse dimensioni, strategiche, legali, operative e tecnologiche. Questo framework si aggiunge ad un altro annuncio della Commissione, che risale a qualche settimana prima: il 10 ottobre era stato infatti lanciato il Sovereign Cloud Tender (SCT), una gara del valore di 180 milioni di euro volta a supportare nei prossimi sei anni enti e istituzioni pubbliche europee a dotarsi di soluzioni cloud sovrane.
Le iniziative non si fermano però a questo. Un mese più tardi, il 18 novembre, a Berlino, i Governi tedesco e francese hanno organizzato il Summit on European Digital Sovereignty, con l'obiettivo di discutere con gli altri Stati membri il futuro digitale dell'Europa. Durante il summit, i 27 Paesi europei, tra cui l'Italia, hanno firmato la Dichiarazione per la Sovranità Digitale Europea, per sottolineare la necessità per l'Unione di agire in modo autonomo nell'economia e nella società digitali.
A dicembre, infine, viene ufficialmente lanciato all'Aia il Consorzio per l'Infrastruttura Digitale Europea per i beni comuni digitali (il Digital Commons EDIC - European Digital Infrastructure Consortium), dopo che a fine ottobre era già stata annunciata la sua creazione dalla stessa Commissione Europea. L'obiettivo di questo consorzio – che riunisce comunità open source, aziende private e pubbliche amministrazioni – è quello di rafforzare la sovranità europea coordinando gli sforzi dei Paesi membri nello sviluppo di soluzioni aperte, interoperabili e riutilizzabili, grazie alla definizione di un framework legale di riferimento a cui aderire.

IL 2026 INIZIA CON DIVERSE NOVITÀ

Il nuovo anno si apre, il 22 gennaio, con l'approvazione da parte del Parlamento Europeo della risoluzione "European technological sovereignty and digital infrastructure", che individua e propone alla Commissione aree di intervento nell'ambito della sovranità tecnologica. In particolare, all'interno del documento viene riconosciuta la necessità di sviluppare delle Digital Public Infrastructure (DPI) che supportino il Vecchio Continente nello sviluppo di una società ed economia digitali, che siano sostenibili e coerenti ai principi e agli obiettivi dell'Unione. Il concetto delle DPI, come chiarisce lo stesso ITU, fa riferimento all'insieme di tecnologie e sistemi ritenuti fondamentali per l'erogazione di servizi pubblici e privati a individui e organizzazioni, come ad esempio i sistemi per l'identità digitale, i pagamenti digitali o le reti di comunicazione. Nella visione del Parlamento, questi devono basarsi su standard aperti ed interoperabili, per assicurare la sicurezza e la sostenibilità dell'ecosistema europeo. Non solo però infrastrutture pubbliche: si sottolinea anche il ruolo del procurement pubblico come leva per indirizzare gli acquisti e la spesa in una logica di riduzione e contenimento delle dipendenze critiche, a favore di soluzioni, ancora una volta, aperte e interoperabili: a ribadirlo il richiamo allo slogan della campagna della Free Software Foundation Europe (FSFE) "public money, public code".

SOVRANITÀ MONETARIA E EURO DIGITALE

Il tema delle sovranità europea non ha solo una valenza tecnologica. In un recente intervento di Pietro Cipollone della BCE dinanzi alla Commissione parlamentare di inchiesta sul sistema bancario, finanziario e assicurativo, il membro della Banca Centrale Europea ricorda il ruolo della sovranità monetaria nel dibattito più ampio della sovranità e della sovranità europea. In uno scenario, infatti, di instabilità geopolitica e di crescenti dipendenze, anche l'esternalizzazione di funzioni critiche, come quelle legate ai pagamenti e alla finanza, assume un ruolo non irrilevante per il futuro economico dell'Unione.
D'altra parte, il digitale è centrale anche nel dibattito sulla sovranità monetaria e, in particolare, dei pagamenti al dettaglio, con il ruolo dell'Euro digitale nell'assicurare l'indipendenza del Continente in questo ambito. A questo riguardo, lo stesso Parlamento Europeo lo scorso 10 febbraio ha approvato due emendamenti contenuti nella risoluzione sull'attività della BCE, che ribadiscono il ruolo dell'Euro digitale nei pagamenti sia online sia offline per assicurare la sovranità monetaria dell'Unione e l'indipendenza da provider di circuiti di pagamento non europei.

L'EUROPA ALLA PROVA DEL 2026

Oltre alle iniziative già avviate, cresce l'attesa per nuovi interventi e annunci che andranno ad aggiungere ulteriori tasselli al percorso verso la sovranità digitale europea. Al prossimo Mobile World Congress, che si terrà a Barcellona dal 2 al 5 marzo, è atteso il debutto su scala industriale dell'European Edge Continuum, un'iniziativa promossa grazie al supporto del progetto IPCEI-CIS e con i fondi del Next Generation EU, che mette in un sistema federato le infrastrutture edge dei principali operatori di telefonia europei: l'italiana TIM, Deutsche Telekom, Orange, Telefónica e Vodafone.
Sempre in tema di infrastrutture abilitante, per settembre 2026 è attesa revisione del Chips Act, dopo che lo scorso anno si erano già sollevate richieste di intervento verso un'evoluzione della normativa nell'ambito dei semiconduttori, per un riconoscimento della loro rilevanza nel contesto dello sviluppo della sovranità tecnologica europea.
A questo si aggiunge poi l'attesa per il Cloud and AI Development Act, per rafforzare la leadership europea nell'ambito del cloud e dell'intelligenza artificiale il Quantum Act, focalizzato sullo sviluppo dell'ecosistema delle tecnologie quantistiche, che andranno a completare ulteriormente il quadro complessivo dello sviluppo tecnologico del continente.

Fintech e inclusione: i game changer digitali delle economie emergenti

Gianluca Dotti, *Giornalista*
TIG - The Innovation Group

DA UN LATO I MODELLI FINTECH E L'OPEN BANKING, E DALL'ALTRO LA RIVOLUZIONE ENERGETICA – SOSTENIBILE E DIGITALE – STANNO FORMALIZZANDO ECONOMIE INFORMALI E ALIMENTANDO IL FENOMENO STARTUP NEI PAESI DEL GLOBAL SOUTH, DAL KENIA AL BRASILE E FINO ALL'INDIA. TRA I PAESI MENO CHIACCHIERATI QUANDO SI TRATTA DI DIGITALE, MA INVECE DALLE GRANDI POTENZIALITÀ, CI SONO RUANDA, GIORDANIA E SOPRATTUTTO NIGERIA.

Tra geopolitica del digitale, potenzialità dell'intelligenza artificiale e attenzione all'inclusione femminile, a margine della quinta assemblea generale della Digital Cooperation Organization (DCO) abbiamo fatto a colazione a Kuwait City con **Giulia Ajmone Marsan**. Economista di fama internazionale con un passato all'OECD, fa parte del Global Foresight Network del World Economic Forum e oggi guida la divisione Startups and Digital Inclusion di ERIA (Economic Research Institute for ASEAN and East Asia) e lavora presso il Digital Innovation and Sustainable Economy Center (E-DISC), con sede a Jakarta in Indonesia.

Giulia Ajmone Marsan, con ERIA avete analizzato i modelli di innovazione fintech emergenti: quali sembrano più efficaci e promettenti?

In uno studio pubblicato a fine gennaio, abbiamo analizzato percorsi diversi, ma che nella sostanza appaiono piuttosto comparabili e sovrapponibili tra loro, accomunati dal **connubio tra fintech e inclusione**. Il **Brasile** ha catalizzato le startup grazie alla regolamentazione open banking del Banco Central e al sistema PIX per pagamenti istantanei, sicuri ed economici, che è riuscito a coinvolgere nel circuito anche commercianti e utenti che prima restavano esclusi. L'**India** ha creato la Digital Public Infrastructure (DPI), con identificativo digitale universale e la Unified Payment Interface (UPI), formalizzando l'economia informale e abilitando l'e-commerce, i sistemi per la delivery del cibo e per lo sharing dei mezzi di trasporto. Nel sudest asiatico, molti paesi a partire da **Singapore**, **Indonesia** e **Malesia** hanno sviluppato app per servire le cosiddette persone 'unbanked' – con profili economici troppo incerti per i canoni delle banche tradizionali, perché non hanno un indirizzo stabile oppure un lavoro adeguatamente formalizzato – combinando wallet digitali e analisi dati per offrire credito e polizze assicurative, determinando così un cambiamento sociale significativo. Tra queste app possiamo citare Grab, che è stata realizzata tra Singapore e Malesia e ha messo fuori mercato Uber grazie alla migliore conoscenza delle realta e dei mercati locali, e l'indonesiana GoJek, ora nota come GoTo.

Oltre a Sudamerica e Asia, questi modelli sono applicabili anche all'Africa?

Gli African Big Four – Nigeria, Egitto, Sudafrica e Kenya – attirano il 50% del venture capital di tutto il continente. Il **Kenya** è un paese che si può defiire *telco-driven*: a guidare la trasformazione è il sistema di pagamento M-Pesa, che usa la rete mobile per le

Giulia Ajmone Marsan, economista, Global Foresight Network del World Economic Forum, Economic Research Institute for ASEAN and East Asia.

Lo skyline di Singapore dove ha sede ERIA (Economic Research Institute for ASEAN and East Asia)

transazioni digitali e ha ampliato di molto l'accesso. In **Egitto**, il fintech unicorn C6 Bank è riuscito a scalare grazie a partnership con banche locali. E in **Nigeria** c'è un fermento enorme, anzitutto perché è un paese con una crescita demografica esplosiva: potrebbe arrivare a rappresentare, da solo, il 25% delle nuove nascite globali. Pochi giorni fa Briter ha pubblicato l'Africa Investment Report 2025, in cui si mostra come per la prima volta gli investimenti venture capital in Africa su **solare** ed **energia green** abbiano superato il comparto fintech. Il solare può fare da vero game changer per il continente, con pannelli solari nel deserto, senza cavi e con uno storage che diventa sempre più economico. Come titolava *The Economist*, *"Solar power: new revolution for Africa"*: nei paesi tropicali, peraltro, la rivoluzione energetica ha un potenziale ancora maggiore rispetto al Golfo.

Quali temi stanno dominando la digitalizzazione dei paesi del Global South? E quale ruolo può avere la leadership politica?

Come emerso anche nelle riunioni della Digital Cooperation Organization (che a oggi riunisce 16 paesi tra Golfo, Medio Oriente, Asia e Africa, più Cipro e Grecia), l'attività riguarda lo sviluppo delle economie digitali secondo principi di **accessibilità** e **sostenibilità**, intrecciati alla trasformazione digitale. Sono gli stessi temi caldi anche in Europa – basti pensare alla twin transition, discussa da anni a Bruxelles – ma con un forte accento sull'**inclusione digitale** e una particolare attenzione al **ruolo delle donne**, dall'occupazione femminile nelle aziende tech alla partecipazione all'economia digitale. Molti stati hanno attivato azioni concrete, come il training per donne e ragazze dalla Giordania al Ruanda.

Ci sono altri trend che ritiene rilevanti?

Grande spazio nelle agende politiche è dedicato alla governance dell'intelligenza artificiale (dal contrasto alla disinformazione all'impatto trasformativo sul mondo del lavoro, ndr), consapevoli che i rischi delle tecnologie digitali sono globali, non solo africani o europei. Molti stati tra Asia e Golfo, per esempio, stanno limitando l'accesso ai social per i minori di 16 anni. Un ulteriore trend che mi ha colpito è quello della *Technology for Peace*: si cita esplicitamente il nesso tra pace e digital come asse strategico futuro, in assonanza con il Global Digital Compact dell'ONU.

Che tipo di interesse, o di attenzione, può avere un paese come l'Italia rispetto a queste dinamiche di digitalizzazione?

La stampa italiana che si occupa di digitale si concentra perlopiù su Stati Uniti e Cina, ma spesso restano fuori dai radar altre realtà con opportunità eccellenti. Posizionarsi presto su Africa, Asia e altri paesi emergenti con mercati in forte espansione è strategico. Per le imprese italiane ed europee, guardare al Global South e al Medio Oriente non significa solo Dubai, ma anche realtà come **Nigeria**, **Ruanda**, **Oman** e **Marocco**, che in questo momento offrono opportunità sorprendenti.

Data Management 2026: l'AI accelera, ma vince chi ha le fondamenta solide

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

LAKEHOUSE, DATI COME PRODOTTO E GOVERNANCE INTELLIGENTE STANNO RIDEFINENDO COME LE AZIENDE GESTISCONO IL LORO ASSET PIÙ PREZIOSO. NON SI TRATTA DI QUALE TECNOLOGIA ADOTTARE, MA DA DOVE INIZIARE.

La maggior parte delle società di ricerca concorda nel dire che il 2026 segnerà una netta discontinuità nel modo in cui le organizzazioni gestiscono i dati. Il cambiamento seguirà cinque grandi convergenze che ridisegneranno il data management.

INTELLIGENZA ARTIFICIALE COME MOTORE CENTRALE

L'AI è ormai parte integrante della gestione dei dati, non più una tecnologia da sperimentare. Entro i prossimi due anni la maggior parte delle attività di **data management** sarà **automatizzata**. Il rilevamento di **anomalie**, la **classificazione**, il **data lineage** e la gestione dei **metadati** sono già in larga parte automatizzati. Eppure, il fattore umano resta centrale. L'AI potenzia le capacità dell'uomo creando una sinergia che va nella direzione di **un'alleanza**, non una sostituzione.

CONSOLIDAMENTO DELLE PIATTAFORME E ARCHITETTURA LAKEHOUSE

La frammentazione degli stack è diventata insostenibile, a tal punto che molti provider di piattaforme stanno convergendo verso ambienti unificati. Il **lakehouse**, che combina flessibilità di un data lake e performance di un warehouse, è diventata l'architettura di riferimento, tanto che da un lato i principali **cloud** provider lo **supportano nativamente** e dall'altro è diventato il punto di partenza naturale per la **modernizzazione** degli ambienti **legacy**.

I dati come prodotto

Il concetto di "**data as a product**" è un concetto ormai consolidato e diffuso. Un dato-prodotto non è un semplice dataset: è un'unità curata, documentata, con owner definiti, SLA chiari e certificazioni di qualità. Gartner stima che nel 2026 gli utenti non tecnici genereranno il 75% dei nuovi flussi di integrazione, grazie a strumenti AI che traducono il linguaggio naturale in query SQL. In questo contesto il modello **data mesh** si consolida integrandosi con il **data fabric** per garantire governance federata senza nuovi silos.

GOVERNANCE AUTOMATIZZATA E PRIVACY BY DESIGN

Con oltre 140 Paesi che applicano leggi sulla privacy, la conformità è una pressione strutturale. Nuove versioni di

GDPR, assieme a normative globali sull'AI, intensificano lo scrutinio su decisioni automatizzate e l'**explainability**. La risposta è la "**declarative governance**": le policy vengono definite una volta sola e l'agentic AI le applica continuamente su tutto il patrimonio dati, generando prove di conformità in tempo reale. La governance cessa di essere un freno e diventa abilitatore.

OSSERVABILITÀ E REAL-TIME COME STANDARD.

Il passaggio dai processi batch ai flussi in tempo reale è ineludibile. Finanza, eCommerce e processi manifatturieri richiedono insight in secondi, non ore. La data **observability**, ovvero la capacità di monitorare in tempo reale la salute dei sistemi e delle pipeline, è classificata dalla maggior parte delle organizzazioni come **mission-critical**. Le piattaforme usano AI per rilevare anomalie e prevedere guasti, spostando i team dalla modalità reattiva a quella proattiva, abilitando l'innovazione continua.
Le organizzazioni che investono in infrastrutture AI-ready, piattaforme consolidate e governance integrata stanno definendo il baseline competitivo del prossimo decennio. Chi rimanda, rischia di rincorrere per anni.

Il rinascimento del deep tech italiano

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

UNA RECENTE ANALISI DI CDP VENTURE CAPITAL IN COLLABORAZIONE CON AIFI – ITALIAN PRIVATE EQUITY, VENTURE CAPITAL AND PRIVATE DEBT ASSOCIATION E PITCHBOOK RACCONTA LO SCENARIO DEL VENTURE CAPITAL IN ITALIA E LA CRESCENTE RILEVANZA DEL PANORAMA DEEP TECH NEL PAESE.

L'ultima edizione dell'Italy VC Monitor di CDP Venture Capital, pubblicato ad inizio anno, mostra un mercato del venture capital in Italia in espansione, con diversi elementi positivi. Nella prima metà del 2025 le startup italiane hanno raccolto più di 630 milioni di euro, con una crescita di oltre un terzo del valore raggiunto nello stesso periodo nel 2024; allo stesso tempo, il volume dei deal è rimasto stabile, con una crescita del numero di round di medie dimensioni tra i 10 e i 25 milioni di euro – che passa da 9 a 15 – ad evidenza di una maggiore attenzione verso aziende con modelli già comprovati.

LA DIMENSIONE INTERNAZIONALE E LE "DUAL COMPANY"

È forte anche la capacità di attrazione di capitali esteri, con più del 40% dei deal di venture capital italiani che lo scorso anno ha coinvolto investitori stranieri. La dimensione internazionale del venture capital italiano si ritrova anche nelle crescenti iniziative nell'ambito delle cosiddette "dual company", ossia aziende che mantengono una forte presenza in Italia, con fondatori spesso italiani, ma che hanno la propria sede legale o commerciale in un altro Paese.
Lo stesso portfolio di CDP Venture Capital include diverse aziende in ambito AI in questo senso, come le citate Nozomi Networks, attiva nell'ambito della cybersecurity OT e IoT per le infrastrutture critiche, con due italiani (i varesini Andrea Carcano e Moreno Carullo) tra i fondatori e ora sede negli Stati Uniti; o Axelera AI, che offre soluzioni di AI "at the edge", con un italiano (Fabrizio del Maffeo) alla leadership ma con sede nei Paesi Bassi.

© freepik.com

AI E CYBERSECURITY ATTIRANO INVESTIMENTI

L'ambito dell'intelligenza artificiale, così come quello della cybersecurity, è uno dei temi dominanti nei mercati del venture capital, nel mondo così come in Italia. Come riporta il monitor di CDP, nel 2024 in Italia i deal di venture capital legati a tecnologie e soluzioni di AI hanno raggiunto un valore di 851,5 milioni di euro, per 98 transazioni, pari al 46,8% del totale dei deal di VC nel Paese e al 26,3% del conteggio totale dei deal.

Nella prima metà del 2025, questo valore ha raggiunto già i 189,7 milioni di euro, contro i 107,8 milioni raccolti nello stesso periodo nel 2024; anche in termini di deal il numero è in crescita nel confronto anno su anno: nella prima metà del 2024 erano 45 i deal di VC all'attivo nell'ambito dell'AI, contro i 51 registrati nella prima parte del 2025.

Anche l'ambito della cybersecurity attira l'attenzione e gli investimenti da parte dei VC: nel 2024 sono infatti stati investiti 51,4 milioni di euro, per un totale di 7 deal, arrivando a coprire circa l'1,9% del valore complessivo dei deal di VC in Italia.

Nella prima metà del 2025 si registrano inoltre già 5 deal per un ammontare totale di 6,2 milioni di euro.

I SETTORI STRATEGICI DELL'INNOVAZIONE

Gli investimenti in tecnologie di intelligenza artificiale e in sicurezza informatica si intersecano anche con l'interesse verso settori e ambiti strategici, come le energie pulite, l'ambito industriale, le infrastrutture e la mobilità, la sanità, l'ambito dello spazio e dell'agrifood. Interessanti gli use case che si generano da questo incontro: dall'ottimizzazioni delle reti e al modelling nell'ambito delle rinnovabili (per quanto riguarda il cleantech), all'analisi dei dati satellitari e ai sistemi autonomi per l'aerospazio (lo spacetech), ai sensori real-time con l'analisi delle immagini e alle soluzioni di computer vision per i veicoli autonomi (l'Infratech & Mobility). In termini di numero di deal, nella prima metà del 2025 è soprattutto il settore della sanità quello che risulta più attivo, seguito dal settore delle Cleantech (benché in calo rispetto allo stesso periodo dell'anno precedente) e dalle Infratech (in aumento).

Intelligenza artificiale: per evitare costosi errori servono tecnologie ad hoc

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

GLI ANALISTI PREVEDONO PER I PROSSIMI ANNI UN'ASCESA DELLE PIATTAFORME DI GOVERNANCE AI. UNO STRUMENTO NECESSARIO, DA SCEGLIERE CON CURA.

L'intelligenza artificiale non può essere solo gestita: va governata. Bisogna, cioè, controllarla dall'alto, definire il raggio d'azione e i suoi limiti, valutare il rapporto tra costi e benefici e definire misure di contenimento dei rischi. E tutto questo va continuamente verificato e monitorato in tempo reale, mentre i sistemi di AI consumano e producono dati, artefatti o azioni. Poiché i regolamenti sull'intelligenza artificiale nazionali, internazionali e di settore sono in continua evoluzione, è anche necessario verificare continuamente la compliance, onde evitare multe e danni di reputazione. Per fare tutto ciò non bastano le strategie definite su carta, non basta un lavoro di controllo "analogico" (che sarebbe immane, dispersivo, poco accurato) e secondo diversi analisti non bastano nemmeno le tradizionali tecnologie di governance, risk management and compliance (Grc). Come sottolinea Gartner, i tradizionali strumenti Grc non sono equipaggiati per gestire le peculiarità dell'AI, come il rischio di *bias* e di abusi o come l'automazione in tempo reale di decisioni, processi e azioni. Inoltre molti strumenti non riescono a eseguire verifiche di compliance continue ed estese all'intero "ecosistema" del software, fornitori inclusi.

© freepik.com

A colmare queste lacune arrivano le piattaforme di governance dell'AI, la cui adozione è destinata a crescere. Con funzionalità di supervisione centralizzata, gestione del rischio e continui controlli di compliance, queste soluzioni aiutano a garantire la conformità in modo continuativo, seguendo l'evoluzione delle regole e monitorando in tempo reale le interazioni tra dati, software e persone.

SBAGLIANDO SI PAGA

L'entrata in vigore del GDPR, il regolamento europeo sulla protezione dei dati, nel 2018 ha alzato la posta in gioco nell'ambito della compliance a obblighi che riguardano (anche, ma non solo) l'utilizzo di tecnologie informatiche. L'AI Act europeo prevede un sistema sanzionatorio a scaglioni simile a quello del GDPR, con multe calibrate in base alla gravità della violazione e alla dimensione dell'azienda, ma con massimali ancor più elevati.

In caso di informazioni false, incomplete o fuorvianti riferite durante un audit o in fase di notifica alle autorità, possono scattare multe fino a 7,5 milioni di euro o pari all'1% del fatturato mondiale annuo dell'azienda (si applica il valore più alto). Si arriva, invece, fino a 15 milioni di euro o al 3% del giro d'affari in caso di mancata conformità nei sistemi di intelligenza artificiale catalogati come ad alto rischio, come quelli impiegati nella sanità, nelle infrastrutture critiche dell'energia e dei trasporti, nella valutazione dei diritti di welfare o nella selezione del personale.

L'ultimo scaglione è quello delle violazioni gravi, commesse da chi usa o vende sistemi di AI che realizzano manipolazioni, social scoring, analisi biometriche o riconoscimento delle emozioni su filmati

catturati in luoghi pubblici o scuole: il massimo della pena è 35 milioni di euro o fino al 7 % del fatturato mondiale annuo dell'azienda, a seconda di quale tra i due sia il valore più alto.

UNA CRESCITA ATTESA

Le piattaforme di governance dell'AI per ora stanno prendendo piede soprattutto nelle grandi aziende, che sull'AI hanno una strategia e investimenti più strutturati. L'adozione è però destinata a crescere: Gartner prevede che da qui al 2030 i regolamenti sull'AI si applicheranno al 75% delle nazioni, cioè a tre quarti dell'economia mondiale. Nello stesso periodo, le organizzazioni pubbliche e private affronteranno spese di AI compliance per un miliardo di dollari.
Oggi, secondo Gartner, in media le grandi aziende impiegano otto diverse soluzioni Grc in uso, ma da qui alla fine del 2028 il numero medio salirà a dieci. La stima emerge da un sondaggio condotto nella seconda metà dello scorso anno su 360 grandi aziende. Chi si affida a vere piattaforme di AI governance ha, rispetto a chi usa semplici soluzioni Grc, tre volte e mezzo più probabilità di riuscire a controllare efficacemente l'intelligenza artificiale. Secondo le stime di Gartner, i costi legati a multe e altre conseguenze di mancata compliance possono essere ridotti del 20%.
"Passando dalla sperimentazione alla distribuzione su larga scala, il rischio di modelli distorti, opachi o inaffidabili si intensifica", scrive la società di ricerca MarketsandMarkets. "Mantenere equità, capacità di auditing e coerenza lungo le pipeline di intelligenza artificiale mondiali sta diventando una sfida di governance per le aziende. La necessità di monitoraggio continuo, framework di spiegabilità e strumenti per un'AI responsabile sta ridefinendo i criteri di selezione dei fornitori, mentre la governance emerge come fattore decisivo nella strategia di intelligenza artificiale a lungo termine".

FARE LA SCELTA GIUSTA

Come scegliere una buona piattaforma di AI governance? Gartner consiglia di verificare che siano supportati tutti i principali regolamenti e le principali linee guida sull'intelligenza artificiale , come ovviamente lo European AI Act, ma anche la norma ISO 42001 e il framework di gestione del rischio AI del National Institute of Standards and Technology (Nist AI Rmf). Inoltre vanno considerate le specifiche necessità di utilizzo dell'AI in azienda, pensando sia alle esigenze immediate sia agli obiettivi di lungo termine. Terzo punto, l'interoperabilità: la piattaforma di AI governance deve integrarsi senza attrito con le tecnologie già presenti. Aziende come Ibm, Securiti, Fldder e 2021.AI (è la selezione citata da MarketsandMarkets in un suo report sul tema) si distinguono per la scalabilità delle rispettive piattaforme, per l'integrazione di framework di gestione del rischio e per le alleanze strategiche con fornitori cloud.
Per un investimento "a prova di futuro", gli analisti consigliano di orientarsi su prodotti aperti ai casi d'uso emergenti, per esempio oggi gli agenti AI, anche se l'azienda ancora non ha considerato la loro adozione. Le proposte delle startup potrebbero essere più innovative o presentare funzionalità specifiche per determinati target di utenza, ma d'altro canto un vendor consolidato offre maggiori garanzie sul fatto che la soluzione continuerà a esistere e a essere supportata in futuro.

CISO 2025–2030, dalla compliance alla governance strategica

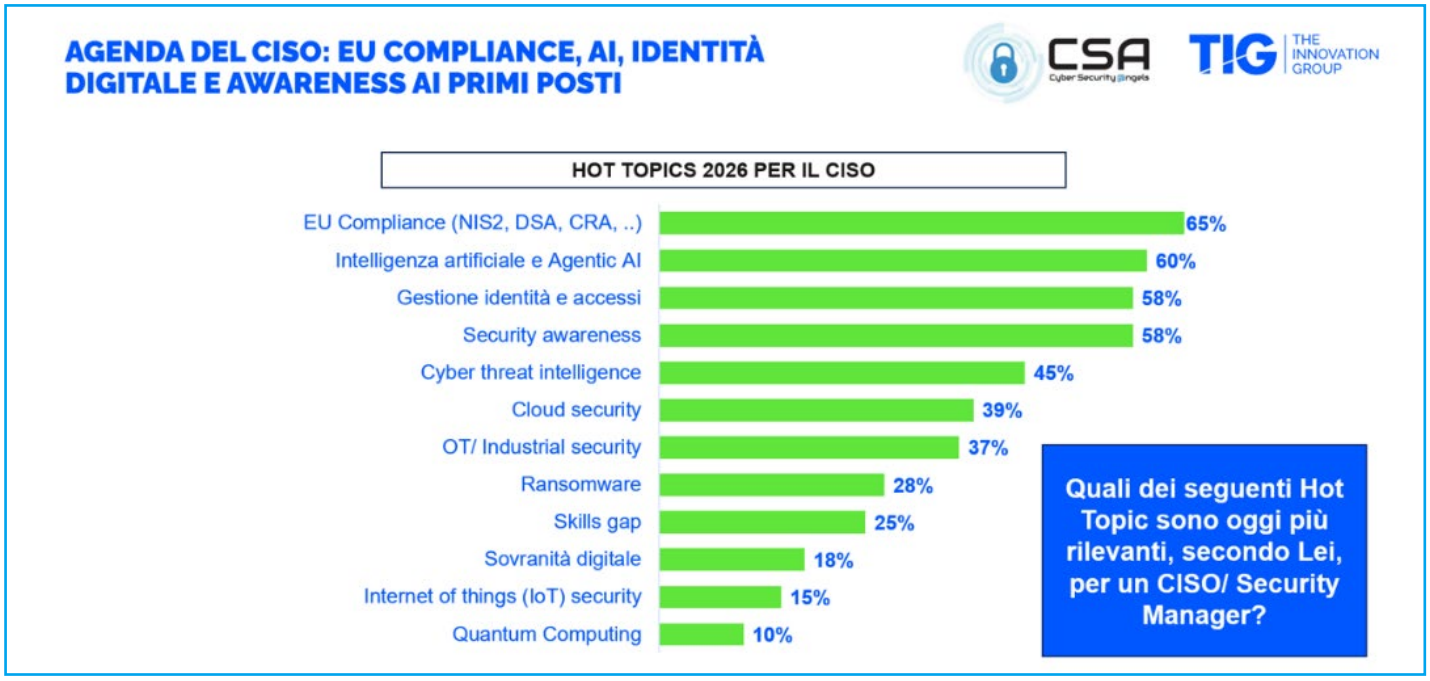
Elena Vaciago, *Content Manager*
TIG - The Innovation Group

L'INDAGINE "CYBER RISK MANAGEMENT" DI TIG – THE INNOVATION GROUP E CSA – CYBER SECURITY ANGELS MOSTRA COME LE PRIORITÀ DEI CISO STIANO EVOLVENDO, CON UNA TRAIETTORIA CHE NEI PROSSIMI CINQUE ANNI PORTERÀ IL RUOLO BEN OLTRE IL PERIMETRO TECNICO.

Il ruolo del Chief Information Security Officer sta attraversando una trasformazione profonda. I risultati dell'indagine "**Cyber Risk Management**" di TIG – The Innovation Group e CSA – Cyber Security Angels, realizzata tra dicembre 2025 e gennaio 2026 con la partecipazione di 187 professionisti della sicurezza (CISO, CIO, Security e IT Manager), mostrano con chiarezza come le priorità percepite dai CISO e dai Security Manager stiano evolvendo, disegnando una traiettoria che nei prossimi cinque anni porterà il ruolo ben oltre il perimetro tecnico tradizionale. Nel 2025 la compliance europea era la principale priorità (come dalla figura successiva), indicata dal 65% degli intervistati. Questo dato non sorprende: la crescente pressione regolatoria ha trasformato la cybersecurity in una responsabilità formalizzata, misurabile e direttamente collegata alla governance aziendale. Il CISO è oggi chiamato a garantire accountability, tracciabilità delle decisioni, adeguatezza dei controlli e reporting strutturato verso il board. In questa fase il rischio è però che la sicurezza sia interpretata prevalentemente come esercizio di conformità, con un'attenzione concentrata sul "dimostrare di essere compliant".

IN REALTÀ, COME SI LEGGE ANCHE DAI RISULTATI DELLA SURVEY, SIAMO GIÀ NEL PIENO DI UN CAMBIO DI PARADIGMA

Quando si chiede quali attività siano più efficaci per incrementare la cyber resilienza, le prime posizioni (riportate nella figura successiva) non sono occupate da



tecnologie bensì da elementi organizzativi: formazione diffusa (69%) e simulazioni periodiche di incidente (63%). Questo orientamento indica che la resilienza è già oggi considerata una capacità sistemica dell'organizzazione. La preparazione preventiva – sapere in anticipo come reagire – appare più rilevante della sola implementazione di nuove tecnologie. Anche il rilevamento tempestivo delle minacce (57%) e la threat intelligence (49%) si confermano pilastri fondamentali.
È interessante notare come l'utilizzo di Managed Security Service venga indicato solo dal 22% del campione: pur essendo ampiamente adottati sul piano operativo, i servizi gestiti non sono percepiti come un fattore differenziante della resilienza. Il quadro che emerge è quello di organizzazioni consapevoli che la capacità di assorbire e superare una crisi cyber dipende prima di tutto da **cultura, governance, allenamento e coordinamento interni,** più che dalla sola sofisticazione degli strumenti tecnologici o dall'apporto delle terze parti.

PROBLEMI INCONTRATI NELLE ATTIVITÀ DI RILEVAMENTO E RISPOSTA A INCIDENTI DI SICUREZZA

Un ulteriore elemento di riflessione emerge analizzando le difficoltà che le organizzazioni incontrano nelle attività di rilevamento e risposta agli incidenti. Il problema più citato (47%) riguarda la **difficoltà di controllare un'intera superficie d'attacco in continua espansione**, tra nuovi asset, utenti, sostituzioni tecnologiche e ambienti ibridi. Subito dopo, il 45% segnala la necessità di garantire **remediation rapide, efficaci e soprattutto prioritizzate** in base alla criticità del servizio, mentre il 43% evidenzia l'incremento costante delle vulnerabilità e i tempi lunghi nell'applicazione delle patch.
Il quadro che emerge è quello di una sicurezza costantemente in rincorsa. Non si tratta soltanto di intercettare le minacce, ma di riuscire a **intervenire con velocità e coerenza operativa** in un contesto dinamico. La mancanza di una visibilità centralizzata e completa sulle infrastrutture (36%) e la difficoltà di trovare un

DETECTION E RISPOSTA: IL PROBLEMA NON È ESCLUSIVAMENTE TECNICO, MA DI GOVERNANCE E COORDINAMENTO

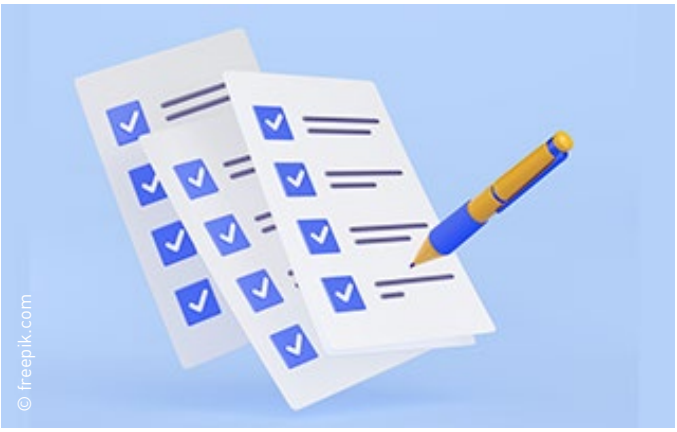
Quali problemi incontrate nelle attività di rilevamento e risposta a incidenti di sicurezza?

Difficoltà legate a controllare tutta la **superficie d'attacco**, rincorrere modifiche o sostituzioni	47%
Remediation veloce, efficace, prioritizzata in base alla criticità del servizio	45%
Incremento costante delle **vulnerabilità**, tempi lunghi nell'applicare le patch	43%
Mancanza di **visibilità centralizzata e completa** su tutte le infrastrutture	36%
Difficile trovare giusto **trade off** tra esigenza di business e di sicurezza	34%

equilibrio tra esigenze di business e sicurezza (34%) confermano che il problema non è esclusivamente tecnico, bensì di governance e coordinamento.
In sintesi, la survey conferma che la sfida della detection e response non è tanto l'assenza di strumenti, quanto la **gestione della complessità**. L'aumento della superficie d'attacco, la moltiplicazione delle vulnerabilità e la pressione sui tempi di remediation stanno trasformando il ruolo del CISO in quello di un "direttore operativo del rischio", chiamato non solo a individuare le minacce, ma a **governare processi, priorità e decisioni in tempo reale**. È proprio in questa capacità di orchestrare visibilità, rapidità e coordinamento che si gioca oggi la vera maturità della cyber resilienza.

IL CISO È DESTINATO QUINDI A EVOLVERE DA GARANTE NORMATIVO A ORCHESTRATORE DELLA RESILIENZA

Dai risultati dell'indagine emerge quindi un ruolo del CISO sempre più al centro dei percorsi di trasformazione digitale dell'azienda. Il suo compito non sarà solo assicurare l'adeguatezza dei controlli, ma costruire una cultura della sicurezza, promuovere esercitazioni realistiche, coordinare funzioni diverse – IT, legale, HR, operations, comunicazione – e garantire che l'organizzazione sappia reagire in modo coeso e tempestivo. La cybersecurity diventa così un tema di preparazione collettiva e maturità organizzativa.
Un'ulteriore evoluzione riguarda l'estensione del perimetro di responsabilità. I dati sull'utilizzo dei Managed Security Service mostrano un'adozione già consolidata in ambiti come endpoint, network e cloud, ma soprattutto una crescita prevista in settori come supply chain risk management, OT security, intelligenza artificiale e persino quantum computing. Questo indica che la sicurezza non è più confinata all'interno dei sistemi aziendali, ma si distribuisce lungo **l'intero ecosistema digitale**. Il CISO dovrà quindi sempre di più governare fornitori critici, valutare la resilienza della filiera, integrare servizi gestiti in una strategia coerente e mantenere visibilità su ambienti sempre più eterogenei. Da difensore del perimetro interno, il CISO diventa orchestratore di un ecosistema di sicurezza distribuita.
Non dimentichiamoci che, parallelamente, sta crescendo l'attenzione verso l'intelligenza artificiale, indicata dal 60% come hot topic prioritario nella prima immagine. L'AI non è solo un'opportunità di automazione, ma un **nuovo dominio di rischio** che richiede protezione dei dati di training, integrità dei modelli, utilizzo responsabile degli algoritmi, gestione di agenti autonomi. Il CISO sarà quindi chiamato in futuro a sviluppare competenze di AI governance, pianificazione post-quantum e gestione del rischio tecnologico emergente. In questo scenario, il CISO del 2030 non sarà semplicemente il responsabile della sicurezza IT, ma piuttosto una figura strategica, capace di dialogare con il board in termini di rischio sistemico, continuità operativa e sostenibilità digitale. Dovrà integrare competenze normative, organizzative e tecnologiche, governando un equilibrio complesso tra innovazione e protezione. In futuro, la maturità della cybersecurity non si misurerà più solo dal numero di controlli implementati, ma dalla capacità dell'organizzazione di anticipare, assorbire e superare le crisi.



Digital Omnibus, tra obiettivi di semplificazione e perplessità

Valentina Frediani, *Founder & CEO*
Colin & Partners

L'INTRODUZIONE DEL "DIGITAL OMNIBUS" RIGUARDA UN INSIEME DI PROVVEDIMENTI LEGISLATIVI CHE HANNO LA FINALITÀ DI SNELLIRE IL PACCHETTO NORMATIVO NELL'AMBITO DIGITALE IN UE. OSSERVIAMO CHE TRA I REGOLAMENTI INTERESSATI DA QUESTA PROPOSTA FIGURANO ANCHE: IL GDPR, LA NIS2, L'EUDPR E LA DIRETTIVA EPRIVACY.

Prendendo in esame gli ultimi dieci anni, possiamo affermare che si tratta del più importante intervento di revisione, rafforzamento e snellimento del piano normativo in merito alle tecnologie digitali. A tal proposito, la Commissione Europea esprime delle intenzioni lodevoli con la presentazione del "Digital Omnibus", puntando soprattutto su stabilità e chiarezza normativa, riduzione degli oneri amministrativi, assicurazione della piena tutela dei diritti individuali e infine l'obiettivo di portare l'UE ad una maggiore competitività.
Passando ad una valutazione esterna, il Garante europeo (EDPS) e la Presidente del Comitato europeo per la protezione dei dati (EDPB) considerano positivamente vari aspetti della proposta, tra cui possiamo citare: modifiche riguardo le notifiche per eventi di Data Breach, la volontà di innalzare la soglia per l'obbligo di notifica e la proroga del termine.
Tuttavia, è apparso evidente fin da subito un timore condiviso da EDPS e EDPB. Questo nasce in relazione ai possibili rischi che la suddetta semplificazione potrebbe produrre, ad esempio la perdita di efficacia del GDPR e dell'AI Act. Le perplessità si concentrano sul tema della tutela dei diritti e delle libertà fondamentali, i quali, si sottolinea, non devono venir meno a fronte di queste razionalizzazioni.
La preoccupazione è rivolta all'evenienza che tali alleggerimenti normativi possano avere ripercussioni sul grado di tutela di cui beneficiano le persone fisiche,

andando di conseguenza ad indebolire la tutela dei dati personali. In concreto, le criticità espresse hanno sede anche nell'ipotesi che si riscontrino difficoltà nell'attuare corrette misure in un contesto di ambiguità dei testi normativi.
Gli organi di garanzia del GDPR, assieme al nostro Garante privacy, si sono espressi appoggiando quello che è lo scopo del "Digital Omnibus" così come molti elementi della proposta, ritengono altresì opportuno concentrarsi

su alcuni perfezionamenti necessari su varie tematiche. Puntano, ad esempio, l'attenzione sulla necessità di maggiore trasparenza e di una tutela che copra ogni fase dei processi che riguardano l'adozione dell'intelligenza artificiale, dalla sua nascita alla cessazione del sistema. Nello specifico, nella creazione dei modelli di AI gli organi auspicano l'inserimento di una disciplina riguardo il trattamento minimo di alcune tipologie di dati, per assicurarne una salvaguardia maggiore durante tutta la durata dell'impiego del sistema fin dal suo avvio. Mentre, maggiore trasparenza è fortemente caldeggiata in merito alla riduzione efficace degli oneri e alla certezza che le persone siano in grado di ottenere informazioni sui propri dati.
Soffermandoci brevemente sul nucleo dell'AI, risulta appropriato menzionare anche la recente introduzione, da parte del Ministero del Lavoro, delle linee guida sull'utilizzo dell'AI in ambito lavorativo. L'utilizzo di strumenti di intelligenza artificiale nel mondo del lavoro comporta naturalmente una serie di vantaggi, ma al tempo stesso è fondamentale garantirne un uso sicuro e consapevole tramite una regolamentazione adeguata. Per questo, all'interno di queste direttive, viene evidenziata anche la necessità di una formazione di base per i lavoratori e la supervisione umana nell'utilizzo di modelli di AI, con un focus particolare riguardo l'importanza della protezione dei dati personali.
Un'altra specifica che si può trovare all'interno della proposta di "Digital Omnibus" riguarda la revisione della Direttiva ePrivacy; quest'ultima si concentra prevalentemente sulla gestione dei "cookies" ossia uno strumento di profilazione digitale. La proposta riguarda lo spostamento del regolamento relativo ai "cookies" all'interno del GDPR, con la conseguente introduzione di nuovi articoli e la soppressione di direttive che ormai si ritengono obsolete.
La privacy rimane quindi una questione di massima priorità, assieme anche allo scopo di offrire disposizioni che risultino facilmente comprensibili e che siano in grado di garantire un'adeguata protezione dei dati.
Possiamo quindi riassumere le richieste dell'EDPB, dell'EDPS e del nostro Garante Privacy nei confronti della Commissione Europea con due concetti chiave: maggiore accessibilità e maggiore protezione.

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