TIG | THE INNOVATION GROUP

IL CAFFÈ DIGITALE

APRILE 2026

L'EPOCA DELLA DISRUPTION CRONICA E INEVITABILE

QUESTO MESE ABBIAMO FATTO COLAZIONE CON...

Marcello Spagnulo,
Consigliere Scientifico, Limes

NUMERI E MERCATI

Più spesa IT, meno visione: il paradosso dei CIO italiani

LA TRASFORMAZIONE DIGITALE

Sovranità Cloud: aggiudicati i contratti delle istituzioni europee

SOMMARIO

L'epoca della "disruption" cronica e inevitabile

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

Anche i puristi della lingua italiana forse devono arrendersi a non tradurre il termine ***disruption***, da qualche anno entrato nel lessico del settore informatico e non solo. C'è una polisemia racchiusa nel sostantivo e nel suo corrispondente aggettivo disruptive: c'è l'idea di una forza distruttiva ma anche radicalmente rinnovatrice o rivoluzionaria.
Se questo tipo di narrazione ha raggiunto la popolarità mediatica in anni recenti, già nel 2015 un saggio del **McKinsey Global Institute,** *No Ordinary Disruption: The Four Forces Breaking All the Trends*, usava lo stesso lessico identificando quattro fattori di discontinuità destinati a plasmare il futuro: l'emergere di nuovi mercati energetici, l'invecchiamento della popolazione mondiale, l'accelerazione dei flussi di commercio, capitale, persone e dati, e non da ultimo l'impatto della tecnologia digitale sull'economia. Non semplici tendenze o fenomeni stagionali, ma mutazioni strutturali.

Se non è una "nuova era" (espressione che ricorre forse con un po' troppa frequenza dei titoli giornalistici e nei report delle società di consulenza), siamo senz'altro in un'epoca peculiare, in cui l'informatica in tutte le sue forme, ormai anche miste alla dimensione fisica, non è più confinata o confinabile in alcun perimetro. La "disruption tecnologica" non è solo tecnologica, ma economica, sociale, sociologica, filosofica e addirittura identitaria (se pensiamo a come i social media hanno cambiato le nostre vite e la percezione del sé).

L'AI IN UNO SCENARIO INSTABILE

Non è un mistero quale sia oggi la nuova grande disruption globale in corso, dopo quelle scatenate dall'avvento di Internet, dal cloud computing e dalla pandemia di covid (con la conseguente, obbligata accelerazione digitale di porzioni della società). Il nuovo disruptor – distruttore e costruttore di futuro – è l'**intelligenza artificiale**: fulcro e motore di investimenti, ma anche pilastro della plutotecnocrazia dei grandi governi e dei colossi tecnologici come Alphabet, Amazon, Microsoft, Meta, Oracle. E nuovamente, più ancora dei social network, **un *disruptor* identitario**, che altera le relazioni sociali e il rapporto tra esseri umani e conoscenza.
Inevitabilmente, la società di consulenza **AlixPartners** ha inserito l'intelligenza artificiale nella settima edizione del suo studio *"Disruption Index"*, basato su 3.200 interviste ad amministratori delegati e dirigenti di aziende di 11 Paesi, Italia inclusa. C'è un dato schiacciante, che smentisce un po' la favola in cui ci siamo cullati per qualche tempo: tra gli intervistati, il **95%** ha detto di **prevedere entro cinque anni riduzioni della forza lavoro** legate all'adozione dell'AI. L'orizzonte temporale, se non altro, è parecchio ampio e nel frattempo altre forze distruttrici, al momento non immaginabili, potrebbero entrare in gioco. Ovviamente l'intelligenza artificiale potrà anche creare nuove opportunità e ruoli lavorativi, ma questa è un'altra storia. Tra i **dirigenti italiani** inclusi nel campione la quota di chi immagina riduzioni di organico è pari al **75%**, segno del fatto che le nostre aziende sull'AI sono un po' in ritardo rispetto allo scenario globale. A conferma di ciò, solo per il 36% dei dirigenti italiani (contro il 52% di media globale) questa tecnologia ha già avuto un "forte impatto" sulla propria organizzazione.
Ci sono, certo, anche i grandi ottimisti, che prevedono non distruzioni ma costruzioni di valore. Citiamo, tra gli studi recenti, *quello condotto da Teha Group per Microsoft Italia,* in cui si stima che un'adozione pervasiva dell'AI possa aggiungere fino a 336 miliardi di euro all'anno al nostro PIL nazionale da qui al al 2040.
L'intelligenza artificiale, comunque, non è certo l'unica perturbazione con cui le aziende si confrontano. Ci sono le guerre, e in particolare i **fronti aperti in Medio Oriente**,

tra Palestina, Israele, Iran e Libano. Come sottolineato anche da AlixPartners, ne derivano incertezze e impatti sull'economia, trasversalmente ai settori: probabili conseguenze sono aumento dei costi, inflazione, rialzo dei prezzi, ostacoli all'export e riduzione dei consumi. In particolare, secondo la società di consulenza, i settori più a rischio di impatti drammatici sono quello automobilistico, il retail, l'aerospaziale e la difesa. Ma con la recente escalation bellica in Medio Oriente ora è probabile ci saranno impatti rilevanti anche per energia e beni di consumo, settori che fino a qualche mese registravano un *"basso livello di disruption"*, scrive AlixPartners.

ADATTARSI ALLA "PRESSIONE STRUTTURALE"

Viviamo, secondo gli autori dell'indice, in una **continua e persistente *disruption*,** che è diventata allo stesso tempo la principale sfida affrontata dalle aziende e il primario motore (nel bene e nel male) dell'economia mondiale. Chi sta alla guida delle aziende è sotto pressione: il **40% dei Ceo** delle grandi imprese ha detto di **sentirsi "più ansioso nel proprio ruolo" r**ispetto a quanto non fosse un anno prima. Per il **72%** degli amministratori delegati (il dato si fermava al 67% nella precedente edizione dell'indice) è **sempre più difficile capire a quali forze dirompenti dare priorità**, mentre il 51% dubita la che la propria azienda sappia reagire al contesto abbastanza rapidamente.

La pressione è strutturale e generalizzata anche perché le ondate di *disruption* sono frequenti e non permettono alle supply chain, ai prezzi, ai modelli di business di tornare alla normalità tra un evento dirompente e il successivo. Esistono, comunque, aziende capaci di una maggiore proattività e che hanno imparato a *"gestire ordinariamente situazioni straordinarie"*, scrive AlixPartners.

"Le ondate di disruption si susseguono ormai con frequenza e magnitudine tali da sovrapporsi: quelle nuove arrivano prima che l'incertezza derivante dalle precedenti sia normalizzata", ha commentato **Dario Duse**, Italy country leader di AlixPartners. *"L'imperativo per il business è quindi quello di cavalcare un mondo dove i cicli economici, l'influenza delle policies e la volatilità dei mercati sono disaccoppiate, e conta sempre di più la capacità di gestire ordinariamente lo straordinario. Agilità e capacità di discernimento sono essenziali. Per sostenere la crescita e imparare a gestire le ondate di disruption, serve creare anche allineamento nei team più senior. Le aziende che sapranno continuare a trasformare rapidamente modelli di business e supply chain, e padroneggiare l'utilizzo dell'AI non si limiteranno a difendere la propria posizione, ma potranno costruire un vantaggio competitivo duraturo in un contesto globale in continua evoluzione, sui fronti non prevedibili e coordinati".*

Spazio, la nuova frontiera cyber

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

*LA SPACE CYBERSECURITY STA ASSUMENDO UN RUOLO SEMPRE PIÙ STRATEGICO NELLO SCENARIO ECONOMICO E GEOPOLITICO GLOBALE, POICHÉ I SISTEMI SATELLITARI RAPPRESENTANO OGGI UN'INFRASTRUTTURA CRITICA ESSENZIALE PER SERVIZI FONDAMENTALI COME NAVIGAZIONE, COMUNICAZIONI, ENERGIA E FINANZA. LA SICUREZZA PERÒ DEVE ESTENDERSI ALL'INTERA FILIERA, INCLUDENDO INFRASTRUTTURE DI TERRA, RETI E TERMINALI, ATTRAVERSO UN APPROCCIO END-TO-END BASATO SU CRITTOGRAFIA, AUTENTICAZIONE E SEGMENTAZIONE DELLE RETI. ABBIAMO APPROFONDITO L'ARGOMENTO DELLA SPACE CYBERSECURITY CON L'INGEGNERE **MARCELLO SPAGNULO, CONSIGLIERE SCIENTIFICO DI LIMES**, CHE SUL TEMA INTERVERRÀ NEL CORSO DEL **CISO PANEL DI TIG**, IL PROSSIMO 7 MAGGIO A ROMA.*

Perché nell'attuale scenario economico e geopolitico è sempre più importante parlare di "cybersecurity dello spazio"?

La cybersecurity dello spazio è stato un problema rilevante sin dall'inizio delle attività spaziali, ma negli ultimi anni è diventata una questione cruciale perché gli **assetti spaziali sono ormai un'infrastruttura critica globale**. Questi sistemi sono infatti un pilastro dell'economia moderna, della sicurezza e della geopolitica. Oggi i satelliti sono fondamentali per la **geolocalizzazione e la navigazione** (pensiamo al GPS, al sistema globale di navigazione satellitare Galileo della UE o al cinese BeiDou) e senza di essi le applicazioni sui nostri cellulari non funzionerebbero. Inoltre, questi sistemi garantiscono la **sincronizzazione delle reti energetiche, delle transazioni finanziarie, della logistica e dei trasporti**, oltre a gestire comunicazioni, internet e TV. Un attacco informatico ai sistemi satellitari potrebbe quindi bloccare servizi bancari ed energetici, causando perdite economiche enormi. La loro vulnerabilità deriva dal fatto che utilizzano software digitali per comunicare con le reti terrestri: basta questo ad esporli a diverse forme di attacco.

Quali sono le principali minacce e tipologie di attacco che si osservano?

Spesso si pensa solo al "sistema satellite", mentre i sistemi spaziali sono fortemente dipendenti dalle **infrastrutture di terra,** che li controllano e ne gestiscono il flusso dei dati. Gli attacchi possono colpire direttamente queste basi terrestri o essere di tipo **elettromagnetico**. In questo secondo caso, possono avvenire dalla terra verso lo spazio o tra satelliti stessi, attraverso tecniche di **jamming** (disturbo delle comunicazioni) o **spoofing** (falsificazione del segnale). È dunque fondamentale proteggere l'intera catena.
Un esempio inquietante è avvenuto lo scorso dicembre a ***Nanchino*,** nella Cina orientale, dove un potente sistema di jamming ha paralizzato per ore i servizi civili ed essenziali della metropoli da 10 milioni di abitanti interferendo con le frequenze GPS e BeiDou. Le app di navigazione per auto e di consegna di cibo a domicilio,

Marcello Spagnulo, Consigliere Scientifico di LIMES

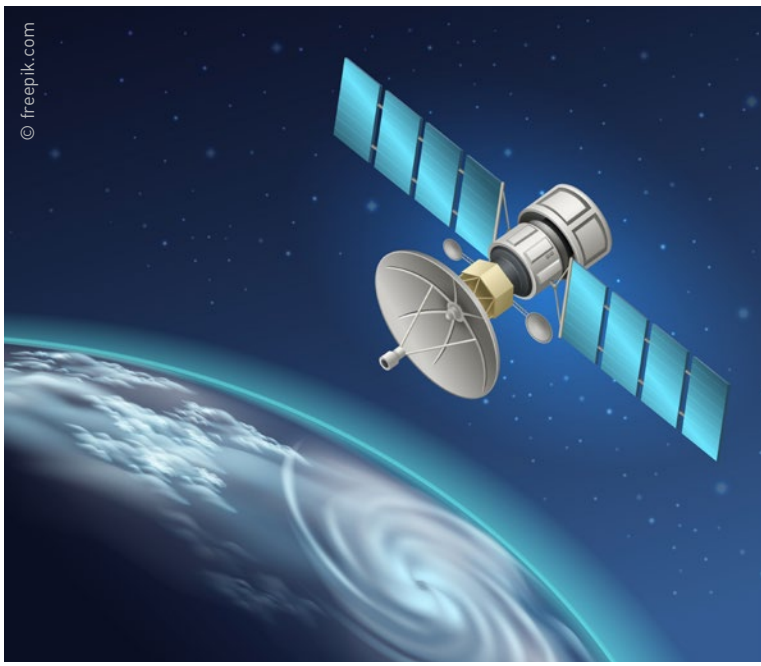
i servizi di trasporto privato e di controllo droni, che si basano sul posizionamento satellitare, hanno riscontrato un'"anomalia sistemica" per questo lasso di tempo. Sebbene la notizia sia passata quasi inosservata sui media occidentali, ha avuto una grande eco su quelli asiatici, poiché ha rappresentato una dimostrazione concreta di ciò che potrebbe accadere in caso di attacco ai satelliti, ha fornito indicazioni sula nostra attuale capacità di affrontare tali situazioni.

Di quali misure, tecnologie e servizi si devono dotare oggi le imprese e gli operatori pubblici per preservare la sicurezza e la continuità delle comunicazioni satellitari?

È necessaria una sicurezza **"end-to-end"**, il che significa che non basta proteggere il satellite, bisogna mettere in sicurezza tutta la catena: rete di comunicazione, centri di controllo, satelliti e terminali di terra (antenne, modem). Ricordiamo l'**attacco a Viasat** nel febbraio 2022, poco prima dell'invasione dell'Ucraina: un virus introdotto su un satellite commerciale è stato trasmesso a tutti i terminali di terra, rendendoli inservibili. In quel caso, l'obiettivo non era disattivare il satellite, ma colpire i **terminali terrestri** attraverso di esso, bloccando di fatto le comunicazioni. Le misure chiave da adottare includono una **crittografia forte dei dati** (sia in transito che a riposo), sistemi di **autenticazione robusta** tra satellite e terminali e la **segmentazione delle reti** per aumentare la resilienza del sistema.

Considerando questi rischi, come si sta orientando il quadro normativo europeo e italiano per la space cybersecurity?

Attualmente non esiste ancora un corpus giuridico o tecnico unico per la cybersecurity dello spazio, ma la situazione sta evolvendo rapidamente. Un vero punto di svolta è stata la **direttiva NIS2**, che include le infrastrutture spaziali tra i settori critici. Questo significa che un operatore satellitare oggi è trattato con la stessa importanza di un operatore energetico o bancario.



L'Italia ha recepito la NIS2 con un decreto legislativo del 2024, rafforzando il ruolo dell'**ACN (Agenzia per la Cybersicurezza Nazionale)** e introducendo obblighi specifici per le imprese. Inoltre, l'ACN ha siglato un accordo con l'**Agenzia Spaziale Italiana (ASI)**: la collaborazione tra ACN e ASI serve a garantire che l'industria spaziale italiana si adegui ai nuovi e più stringenti requisiti di cybersecurity imposti dalla legge, proteggendo un settore ormai considerato vitale per l'economia e la sicurezza del Paese.
A livello europeo, si discute dell'**EU Space Act**, presentato dalla Commissione Europea a giugno dello scorso anno. Questa proposta mira ad armonizzare le regole tra gli stati membri, prevedendo un registro europeo degli oggetti e un ruolo rafforzato per l'Agenzia dell'Unione Europea per il Programma Spaziale. Tuttavia, essendo un tema sensibile che tocca la sicurezza nazionale, l'EU Space Act è attualmente sotto revisione a causa di questioni di legittimità sollevate da diversi stati membri.

Imprese e digitale: la sfida di non restare indietro

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

LA DIGITAL ENTERPRISE SURVEY 2026 DI TIG – THE INNOVATION GROUP RESTITUISCE IL RITRATTO DI UN SISTEMA IMPRENDITORIALE CHE PROCEDE CON CAUTELA: L'AI È PRESENTE NELLE DICHIARAZIONI DI INTENTO, MA L'APPROCCIO RESTA ANCORA PER LO PIÙ SPERIMENTALE; LA TRASFORMAZIONE DIGITALE È PERCEPITA COME INEVITABILE, MA CON LA POSSIBILITÀ CHE VENGA PERCEPITA E ATTUATA IN MODO DIVERSO TRA GRANDI IMPRESE E PMI; E LO SKILL GAP RISCHIA DI INFLUENZARE LE STRATEGIE E IL RICORSO A PARTNER ESTERNI PER INNOVARE.

Il 2026 si apre per le aziende italiane all'insegna dell'incertezza. L'aumento dei costi – energia, materie prime, fattori produttivi – è la principale preoccupazione dichiarata dal 43% delle 105 organizzazioni coinvolte nella Digital Enterprise Survey 2026 di TIG – The Innovation Group, subito seguita dall'instabilità economica (42%) e dalla difficoltà nel reperire e trattenere talenti (37%). Da notare che l'indagine, condotta tra febbraio e marzo 2026, subisce indubbiamente gli effetti dello scoppio del conflitto in Iran nel periodo, ancora nell'incertezza relativa alla durata e agli effetti del conflitto. In questo scenario, il saldo tra aspettative positive e negative sull'andamento dell'economia italiana per l'anno in corso emerge come negativo di 19 punti, a dimostrazione un clima nel complesso cauto, difensivo e poco propenso all'accelerazione.
In questo scenario, l'innovazione digitale non smette di essere rilevante – con l'Innovazione digitale e la cybersecurity che vengono citate rispettivamente dal 26% degli intervistati – ma "scivola" in secondo piano, lasciando il passo a valutazioni e interventi più di contesto e di gestione di dinamiche di incertezza complessiva, con cui le aziende devono imparare a convivere

AI E AUTOMAZIONE: LA PRIORITÀ STRATEGICA DEL 2026

Nonostante il contesto prudente, l'adozione di soluzioni di automazione avanzata e AI resta la priorità strategica più citata (54%) tra gli intervistati, mentre – a livello di investimenti – l'AI generativa si posiziona al secondo posto (30%), preceduta solo dalla cybersecurity (39%). L'intelligenza artificiale comincia così ad essere presente sia nelle priorità strategiche sia nei budget, a mostrare un passaggio – almeno nelle intenzioni dichiarate – dalla fase esplorativa e di sperimentazione a una più orientata all'impatto concreto e industrializzato.
D'altra parte, se si guarda allo stato effettivo dell'adozione, il divario tra aspirazioni e realtà emerge ancora con evidenza. Oltre la metà delle aziende intervistate si trova ancora in una fase sperimentale: il 35% ha avviato progetti pilota o proof of concept sull'AI generativa, il 27% si limita alla fruizione gratuita di strumenti disponibili sul mercato; solo il 19% dichiara invece di avere approvato progetti avanzati. La fruizione gratuita è d'altra parte particolarmente marcata proprio nel comparto dell'AI generativa, che per molti rimane ancora un terreno di esplorazione individuale per la produttività, più che di strategia complessiva e strutturata.

DOVE L'AI LASCIA IL SEGNO (E DOVE NON ANCORA)

Tra le aree più impattate dall'adozione dell'AI i rispondenti citano il marketing e le vendite (49%), il customer service (46%) e, con una quota significativa per un campione in cui il settore manifatturiero pesa per il 29%, la produzione (37%). Sono ambiti in cui il valore è probabilmente più immediato e facilmente visibile: velocità di risposta al mercato, miglioramento dell'esperienza del cliente, supporto alla pianificazione o alla manutenzione predittiva in fabbrica. Molto meno

coinvolte risultano invece le funzioni di back office: finanza e contabilità (29%), supply chain e logistica (19%) e risorse umane (17%). L'adozione dell'AI sembra quindi fare più fatica a scalare nei processi interni più complessi, dove i casi d'uso a valore – al di là di quelli che possono essere "facili" utilizzi – sono più difficili da identificare e dove la trasformazione richiede una revisione più profonda di processi e competenze.
Un altro tema centrale, e collegato alle riflessioni appena riportate, riguarda il ritorno degli investimenti in AI. Nel 2026 la spesa in AI è prevista in crescita o stabile per la maggior parte delle aziende rispondenti, ma circa quattro su dieci non stanno ancora valutando il ritorno dei propri investimenti in quest'area. Dove presente, la misurazione si basa soprattutto su analisi costi-benefici e valutazioni qualitative. Un gap che d'altra parte oscilla tra due opposti: un'assenza che rischia di frenare il passaggio della tecnologia da sperimentazione a produzione, o una presenza che potrebbe imbrigliare e vincolare troppo presto il potenziale di una tecnologia in fondo ancora emergente.

LA TRASFORMAZIONE DIGITALE È NECESSARIA, MA ANCORA DISOMOGENEA

La trasformazione digitale è ormai percepita come un processo strutturale e permanente, almeno nelle grandi imprese. Sono queste ultime a cogliere con maggiore consapevolezza la dimensione culturale del cambiamento, che non è solo tecnologico, e a respingere l'idea che la "digital transformation" sia un termine ormai abusato o superato. Per le grandi organizzazioni è, al contrario, una necessità competitiva sempre più urgente, anche su scala internazionale. Le PMI mostrano invece un atteggiamento diverso, con la tendenza spesso a ridurre questo concetto a un tema di efficienza operativa, considerandolo probabilmente meno prioritario rispetto ad urgenze di breve periodo. Il rischio però è che si crei (o si accentui) un divario di maturità digitale, che si traduca poi in un differenziale competitivo crescente e sempre più difficile da colmare.

FORNITORI LOCALI, SODDISFAZIONE DISCRETA

Sul fronte delle strategie di sourcing, le aziende intervistate confermano una preferenza strutturale per partner vicini al proprio contesto di business: software vendor e system integrator locali vengono privilegiati rispetto ai grandi player internazionali. I criteri di selezione – la conoscenza del settore specifico (43%), il rapporto qualità/prezzo (39%), l'affidabilità e il rispetto delle tempistiche (35%) – e rispecchiano in parte questa logica. Il livello medio di soddisfazione nei confronti dei partner tecnologici si attesta a 6,6 su 10, un risultato sufficiente ma con margini di miglioramento evidenti.
Il ricorso a partner esterni è d'altra parte destinato a rimanere stabile o crescere: non è una scelta di convenienza contingente, ma probabilmente una risposta strutturale alla carenza di competenze interne e alla rapidità dell'evoluzione tecnologica. Parallelamente, il 24% delle aziende dichiara di valutare iniziative di insourcing IT, motivate principalmente dalla riduzione dei costi (30%), dal miglioramento delle performance (26%) e dalla necessità di maggiore controllo su sistemi e applicativi critici. Non sembra quindi essere un'alternativa al modello di sourcing esterno, ma una leva selettiva, attivata su ambiti strategici o sensibili.

COMPETENZE: IL COLLO DI BOTTIGLIA PERMANENTE

Tra le aziende intervistate, gli investimenti in competenze interne si concentrano su cybersecurity (39%), project management (39%), business intelligence e analytice (37%) e sviluppo software (26%). Profili quindi prevalentemente "tecnici", che confermano l'approccio, soprattutto delle PMI, alla trasformazione digitale ancora orientato all'esecuzione più che alla strategia. Le competenze più avanzate – dal change management al prompt engineering – risultano invece poco citate, il che potrebbe parzialmente spiegare la crescente dipendenza da partner esterni e lo skill gap che le aziende stesse indicano come uno dei principali ostacoli alla trasformazione.

L'Europa accelera: cosa devono aspettarsi le aziende nei prossimi mesi?

Valentina Frediani, *Founder & CEO*
Colin & Partners

LA ROADMAP DEI DIVERSI IMPIANTI NORMATIVI PROCEDE A TAPPE SERRATE E NEL CORSO DEL 2026 LE IMPRESE AFFRONTERANNO CHIAMATE SU VARI FRONTI PER IMPLEMENTARE E RENDERE OPERATIVI I VARI OBBLIGHI PREVISTI.

Nei prossimi mesi, normative come **NIS2, Cyber Resilience Act, Data Act e AI Act** entreranno nella fase pienamente operativa, confermando il ruolo sempre più centrale della gestione del rischio e della protezione dei dati nell'agenda delle autorità. Un'azione sinergica resa necessaria dal contesto europeo ed internazionale che pone i dati al centro della trasformazione digitale rendendo prioritaria una strategia integrata in cui privacy e sicurezza informatica divengono i pilastri essenziali per la gestione responsabile dei dati.

Queste normative, rivolte al mondo delle imprese, rappresentano i capisaldi attorno ai quali prende forma il programma di digitalizzazione europeo, con ambiti di intervento che interessano l'intero ciclo di vita aziendale lungo tutta la filiera, dai produttori ai fornitori, fino ai dipendenti, ai clienti e ai consumatori finali.

Partendo dalla **NIS2**, la cui applicazione a tappe è stata inaugurata nel corso dello scorso anno con la registrazione alla piattaforma digitale di ACN, dopo l'obbligo di notifica degli incidenti significativi dello scorso gennaio 2026, vedrà la prossima deadline rilevante il **prossimo ottobre**. In quella data le imprese soggette alla normativa dovranno completare l'adozione delle misure di sicurezza tecniche e organizzative. Queste ultime definite nell'articolo 21 richiedono un approccio multidisciplinare dal momento che coinvolgono vari ambiti a partire dalla sicurezza dei sistemi informativi e di rete, fino alle politiche di analisi dei rischi, gestione degli incidenti, e pratiche per la continuità operativa (backup, disaster recovery). Da non trascurare poi il tema della formazione delle policy sulla crittografia, e della sicurezza delle autenticazioni.

Dopo, quindi, una fase formale di iscrizione/registrazione/comunicazione dei referenti si passerà ad una pienamente operativa per le imprese che dovranno agire sul piano pratico non solo per raggiungere la piena compliance, ma anche per essere pronte in caso di eventuali controlli da parte dell'autorità. Merita ricordare che in caso di mancata conformità sono previste sanzioni fino a 10 milioni di euro o al 2% del fatturato annuo globale per i soggetti essenziali e la responsabilità personale per gli amministratori, con conseguenze non trascurabili sia sul piano dell'esclusione da appalti pubblici che della brand reputation.

La sicurezza informatica è il cuore pulsante anche del **Cyber Resilience Act** focalizzato sui prodotti che incorporano elementi digitali, quali ad esempio dispositivi IoT, software, elettronica di consumo e device intelligenti. Sono inclusi nel suo raggio d'azione anche i fornitori di servizi cloud, i data center e le soluzioni software-as-a-service.

Emanato nel dicembre 2024 pur divenendo pienamente operativo nel dicembre 2027 prevede alcuni adempimenti anche per il **prossimo settembre 2026**, ovvero l'obbligo per i produttori di notificare al CSIRT le vulnerabilità sfruttate, utilizzando la piattaforma Enisa, ovvero l'agenzia UE per la cybersicurezza. Dovranno essere segnalati anche incidenti gravi: entro 24 ore attraverso un early warning, seguito entro 72 ore da notifica completa.

Il **Data Act** pone, invece, al centro l'accesso e la gestione dei dati industriali generati dai prodotti connessi, stabilendo disposizioni precise su condivisione dei dati IoT, clausole contrattuali, portabilità tra servizi cloud, interoperabilità e salvaguardia contro accessi indebiti. Ne deriva la necessità, per imprese e fornitori, di aggiornare

prodotti, contratti e processi. La cornice normativa chiama in causa molteplici attori dai produttori di prodotti connessi ai fornitori di servizi digitali correlati fino agli utenti professionali e consumatori, importatori, distributori e terze parti. Entrato in vigore nel settembre 2025 vedrà scattare alcuni obblighi nei prossimi mesi. Nello specifico, dal **prossimo settembre** non sarà consentita l'immissione sul mercato di prodotti che, per impostazione predefinita, non assicurino un accesso ai dati facile e gratuito.
Ultimo della nostra rassegna, non certo per importanza, l'**AI ACT** che fissa per **agosto 2026** il termine entro cui i fornitori di sistemi classificati ad alto rischio dovranno adempiere ad una serie di disposizioni, tra cui la valutazione di conformità, monitoraggio, registrazione nella banca dati europea. Per i sistemi ad alto rischio certificati CE gli obblighi scatteranno nel 2027.

Come abbiamo visto alla crescente emanazione di specifiche normative che vedranno le imprese impegnate in prima linea nei prossimi mesi corrispondo obblighi che costituiscono al tempo stesso una preziosa occasione per sfruttare appieno le opportunità offerte dalla digitalizzazione.

Più spesa IT, meno visione: il paradosso dei CIO italiani

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

CYBERSECURITY E GESTIONALI DOMINANO I BUDGET. L'AI È PRESENTE MA NELLE RETROVIE. LA TRASFORMAZIONE DIGITALE SEMBRA CRESCERE PIÙ PER INERZIA CONTRATTUALE CHE NON PER VISIONE STRATEGICA.

C'è un dato che fotografa meglio di ogni altro lo stato dell'IT nelle grandi aziende italiane nel 2026: tutti dichiarano che i dati sono centrali, quasi nessuno li governa davvero.
I CIO assegnano alla centralità dei dati per la competitività un punteggio medio di 4,22 su 5. Ma la readiness delle data platform per sviluppare AI si ferma a 3,02. Ancora più significativo: solo il 10% inserisce la data governance tra le priorità di investimento. È il paradosso più eloquente della CIO Leaders Survey 2026, condotta a febbraio da TIG-The Innovation Group e CEFRIEL su 50 CIO di grandi aziende.

L'AI È IL GRANDE ASSENTE

Nel 2026, anno in cui l'Intelligenza Artificiale agentica domina ogni agenda tecnologica, l'AI generativa è area di investimento prioritaria per appena il 22% dei rispondenti, alla pari con l'ammodernamento infrastrutturale. È citata da un esiguo 10% come fattore che influenza la spesa IT. Sul podio si trovano cybersecurity (44%) ed ERP e modernizzazione dei gestionali (40%): voci storicamente difensive, tutt'altro che disruptive. Il messaggio è eloquente: i CIO italiani sono pragmatici. Pragmatismo o paura di sbagliare?

SI SPENDE DI PIÙ, MA NON PER VISIONE

Il 64% delle aziende aumenta la spesa digitale nel 2026. Sembra una buona notizia, fino a quando non si legge che per il 50% dei rispondenti la crescita non nasce da una scelta strategica, ma dall'aumento di canoni, licenze e costi di aggiornamento. Prima ancora dell'AI come driver di spesa compaiono le tariffe dei fornitori in aumento (26%). I budget crescono perché i contratti costano di più, non perché si è deciso di innovare. Un'inflazione IT silenziosa, che pesa sui conti ma non genera valore proporzionale.

LEGACY, GOVERNANCE E KPI MANCANTI

I sistemi legacy restano uno dei freni principali: il 47% dei CIO dichiara che incidono in modo rilevante sulla capacità di innovare.
A questo si aggiunge una governance debole: solo il 16% considera la gestione della trasformazione digitale un vero vantaggio competitivo. E se non si governa, non si misura: l'11% delle aziende non utilizza KPI per valutare l'efficacia degli investimenti IT.

IL CIO VUOLE FARE IL MANAGER, MA RESTA INTRAPPOLATO TRA IT E BUSINESS

Il coinvolgimento del CIO nelle decisioni di business si attesta a 7,07 su 10. Il 67% concorda che le competenze di business siano oggi importanti quanto quelle tecniche. Eppure, la sfida numero uno dichiarata rimane l'allineamento IT-business (40%). L'AI come area di intervento del CIO raccoglie appena il 9%, meno del vendor management.

UN SISTEMA IN TRANSIZIONE, NON ANCORA IN ACCELERAZIONE

Il CIO è consapevole delle proprie lacune ma è ancora frenato da inerzie organizzative, tecnologiche e contrattuali. Dichiarare i dati fondamentali senza governarli, aumentare la spesa senza sceglierla davvero, aspirare all'allineamento con il business senza raggiungerlo: sono segnali che il sistema sa dove vuole arrivare, ma che il percorso è più lungo del previsto. Finché AI e data strategy resteranno in fondo all'agenda operativa, il divario con chi ha già fatto scelte radicali rischia di diventare strutturale.

Sovranità Cloud: aggiudicati i contratti delle istituzioni europee

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

QUATTRO AZIENDE EUROPEE, DAL LUSSEMBURGO AL BELGIO, DALLA FRANCIA ALLA GERMANIA, SI AGGIUDICANO L'APPALTO DA 180 MILIONI DI EURO LANCIATO NELL'AMBITO DEL CLOUD III DPS. AL CENTRO DELLA SELEZIONE, IL CLOUD SOVEREIGNTY FRAMEWORK. NEL FRATTEMPO CRESCE L'ATTESA PER IL TECH SOVEREIGNTY PACKAGE.

Nel *numero di febbraio di questa newsletter*, in un articolo in cui parlavo degli annunci e delle novità sul tema della sovranità digitale in Europa per il 2026, tra le diverse iniziative promosse dall'Unione Europea era citato anche il lancio dello scorso ottobre del **Sovereign Cloud Tender**, una gara del valore di 180 milioni di euro per supportare enti e istituzioni pubbliche europee a dotarsi di soluzioni cloud sovrane nell'arco di sei anni. Questo appalto, lanciato nell'ambito del Cloud III Dynamic Purchasing System (Cloud III DPS), è stato nelle scorse settimane aggiudicato a quattro aziende europee, dal Lussemburgo al Belgio, dalla Francia alla Germania. Nello specifico, *come riporta la stessa Commissione Europea sul suo sito*, le aziende aggiudicatarie – con i loro partner – risultano le seguenti:

- l'operatore di rete mobile lussemburghese **Post Telecom**, con partner quali le francesi CleverCloud e OVHcloud;
- **STACKIT**, il cloud provider di Schwarz Digits, la divisione IT e digitale del gruppo tedesco Schwarz, uno dei grandi player della GDO in Europa che comprende marchi come Lidl e Kaufland;
- **Scaleway**, controllata del Gruppo Iliad che attualmente – così dichiara sul proprio sito – opera in Francia, Polonia, Italia e Paesi Bassi, con prossime attivazioni in Svezia e Germania;
- La società di telecomunicazioni belga **Proximus**, che collabora con Clarence, joint venture nata dalla collaborazione tra LuxConnect e Proximus, la francese Mistral e S3NS, la joint venture tra Thales e Google Cloud.

La scelta di puntare su quattro fornitori – dichiarata sempre dalla stessa Commissione Europea – è ricondotta alla volontà di assicurare la diversificazione e la resilienza nel supporto allo sviluppo del settore del cloud sovrano in Europa, evitando di creare dipendenze eccessive da un unico fornitore. Il criterio di selezione dei fornitori aggiudicatari ha visto inoltre al centro il ricorso al Cloud Sovereignty Framework (CSF) – citato anch'esso già nell'articolo della *newsletter di febbraio*– che definisce dallo scorso ottobre gli obiettivi, i livelli di garanzia e la metodologia di punteggio da utilizzare per la valutazione di soluzioni e servizi di cloud sovrano europeo. Tra gli obiettivi che vengono presi in considerazione da questo modello emergono sia aspetti di natura strategica, legale, operativa e ambientale, sia temi legati alla trasparenza, sicurezza e conformità della catena di approvvigionamento. Alla luce di questi sviluppi, la Commissione ha dichiarato inoltre di volere aggiornare lo stesso Cloud Sovereignty Framework, per includere ulteriori criteri specifici di valutazione della sovranità in chiave europea.
Non è d'altra parte l'unico punto su cui sta lavorando al Commissione per rafforzare il proprio posizionamento in termini di sovranità tecnologica. È atteso infatti il lancio del pacchetto "Tech Sovereignty" – già rinviato due volte, prima al 15 aprile e ora a fine maggio – che dovrà comprendere sia l'atteso Cloud and AI Development Act (CADA), il Chips Act 2, la strategia per l'open source e una roadmap strategica per la digitalizzazione e l'AI nel settore energetico.

I dati sanitari stanno diventando il motore della ricerca clinica

Gianluca Dotti, *Giornalista*
TIG - The Innovation Group

LE INFORMAZIONI SANITARIE DIGITALI (DI REAL WORLD) SONO SEMPRE PIÙ RICONOSCIUTE COME UNA RISORSA UTILISSIMA PER FARE RICERCA SCIENTIFICA, MA SOLO QUANDO VENGONO INTEGRATE, STANDARDIZZATE E INSERITE IN ARCHITETTURE ORGANIZZATIVE COERENTI.
LA SFIDA NON RIGUARDA LA DISPONIBILITÀ TECNOLOGICA,
MA LA CAPACITÀ DI COSTRUIRE FLUSSI COORDINATI E BEN GOVERNATI.

L'attività di ricerca scientifica in ambito clinico si sta spostando verso sistemi che registrano ogni giorno l'attività sanitaria. Una quota crescente di conoscenza giace tra **cartelle cliniche elettroniche**, **registri** e **piattaforme ospedaliere**, che generano flussi informativi continui, ma spesso eterogenei e non allineati tra loro. Queste informazioni stanno venendo progressivamente riorganizzate e trattate come una base strutturata su cui sviluppare nuove forme di ricerca, capaci di seguire i fenomeni clinici nella loro evoluzione reale. Si tratta dei cosiddetti **dati secondari**, ossia del riuso a fini di ricerca delle informazioni raccolte attraverso la pratica clinica. Questo patrimonio informativo deriva da un processo articolato che richiede costruzione, pulizia, standardizzazione e integrazione, e solo attraversando questi passaggi diventa davvero utilizzabile in modo confrontabile. E scalabile. La difficoltà si concentra qui: trasformare flussi disomogenei in strutture leggibili, mantenendo continuità nel tempo e coerenza tra contesti diversi. Quando questo lavoro riesce, i dati diventano strumenti operativi per studiare fenomeni clinici su larga scala.
Su questi temi che si è concentrata la sessione di sguardo prospettico della ***Healthcare Innovation Executive Conference 2026***, organizzata da TIG insieme ad AISIS (Associazione Italiana Sistemi Informativi in Sanità) e tenutasi a Roma lo scorso 23 aprile, dedicata al ruolo del digitale nella ricerca clinica. Uno degli elementi più evidenti riguarda il passaggio da una logica centrata sulla raccolta dei dati a una logica di ingegneria del dato. **Matteo Gabetta**, responsabile della sicerca e sviluppo di Biomeris, caso italiano d'eccellenza a livello europeo, ha tracciato il lavoro necessario per trasformare dati eterogenei in sistemi interrogabili: lo standard internazionale per organizzare e analizzare dati sanitari OMOP (Observational Medical Outcomes Partnership) rappresenta una delle architetture più avanzate, perché consente di integrare informazioni provenienti da fonti diverse e di renderle confrontabili secondo standard condivisi. Questo non elimina la complessità, ma la sposta a monte, nel processo di mappatura e normalizzazione.

IL PARADIGMA FEDERATO APPLICATO ALLA RICERCA CLINICA

Nel **modello federato** ogni ospedale o centro di ricerca conserva i propri dati nei sistemi in cui vengono prodotti, senza spostarli o centralizzarli. Quando si vuole condurre uno studio, non si raccolgono le informazioni in un unico database: si utilizza invece lo stesso algoritmo, che **viene eseguito separatamente all'interno di ciascun sistema**. Ogni nodo elabora i propri dati e restituisce risultati già aggregati, che possono essere messi insieme per ottenere un quadro complessivo. In questo modo le organizzazioni mantengono il controllo delle informazioni e si riducono i passaggi più critici legati alla gestione della privacy, mentre diventa possibile lavorare su basi ampie e distribuite senza dover costruire archivi centralizzati.
Applicazioni di questo tipo sono già presenti in ambito europeo, soprattutto nei **registri di patologia** e nelle reti dedicate alle **malattie rare**, dove la distribuzione dei dati rende necessario un approccio di questo tipo.
Infatti, le tecnologie necessarie sono già disponibili e continuano a evolvere rapidamente, anche se la loro

presenza non basta di per sé a rendere i dati realmente utilizzabili. **Alfredo Cesario**, CEO di Gemelli Digital Medicine & Health, ha descritto un percorso in cui l'integrazione tra attività clinica e infrastrutture digitali si costruisce nel tempo, attraverso passaggi progressivi che coinvolgono organizzazione, processi e competenze. Il dato entra in tutte le fasi del lavoro, dalla raccolta alla gestione fino all'analisi, ma produce valore solo quando questi livelli riescono a funzionare insieme. La difficoltà si concentra proprio qui: mettere in relazione sistemi diversi, allineare le competenze e definire modalità operative condivise che permettano al dato di circolare senza perdere coerenza.

Questa trasformazione ha ricadute dirette anche sul lavoro clinico. **Diana Ferro**, attiva tra SIIAM (Società Italiana Intelligenza Artificiale in Medicina) e Ospedale Bambino Gesù di Roma, ha portato l'esperienza di utilizzo di sistemi avanzati di intelligenza artificiale a supporto della ricerca, a partire dal co-scientist di Google di cui è una delle prime utilizzatrici in Italia. L'introduzione di questi strumenti non comporta una sostituzione delle competenze, ma una loro ridefinizione: cambia il modo in cui si formulano le domande, si analizzano i dati e si interpretano i risultati. La rapidità con cui queste tecnologie evolvono, anche a livello internazionale, rende necessario un aggiornamento continuo delle pratiche e dei modelli formativi, e le potenzialità già effettive di questi strumenti sono impressionanti.

IL QUADRO NORMATIVO E L'ECONOMIA SEGUONO L'EVOLUZIONE TECNOLOGICA

Un altro elemento riguarda il modo in cui i dati entrano nei processi di sviluppo e valutazione. **Giuseppe Seghi Recli**, componente della Giunta di Farmindustria, ha evidenziato il ruolo crescente dei dati secondari in affiancamento agli studi clinici tradizionali, contribuendo a costruire **modelli basati sugli outcome del mondo reale** e a rafforzare l'approccio della **value-based medicine**. Tuttavia, la possibilità di utilizzare questi dati dipende da condizioni ancora non pienamente soddisfatte, come l'accesso, l'interoperabilità e l'allineamento dei diversi sistemi informativi. Su questo piano si inserisce anche il tema normativo. **Erica Molinari**, Data Protection Officer dell'Azienda USL di Modena, ha sottolineato l'importanza di integrare gli aspetti regolatori fin dalle prime fasi di progettazione. L'**approccio *by design*** rappresenta una condizione necessaria per rendere sostenibili i processi nel tempo, ma incontra difficoltà operative legate alla struttura delle organizzazioni e alla **mancanza diffusa di unità dedicate alla gestione del dato**. Il quadro normativo, dal Regolamento generale sulla protezione dei dati (GDPR) alle iniziative europee come lo European Health Data Space, continua a cambiare per adattarsi a modelli che non erano stati previsti in origine. Insomma, le tecnologie sono disponibili e in rapido sviluppo, mentre la loro integrazione richiede un lavoro più lento e stratificato.

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