

MARZO 2024

011
111
11 101
100 110
11



IL CAFFÈ DIGITALE



LA NUOVA SFIDA DEI CIO SI CHIAMA COMUNICAZIONE

**QUESTO MESE ABBIAMO
FATTO COLAZIONE CON...**

**FOCUS
PA**

**CIO
SUMMIT**

**Daniele Catteddu
CLOUD SECURITY ALLIANCE**

**AI, le potenzialità per la
Pubblica Amministrazione**

**Dall'innovazione di frontiera
alle fondamenta dell'IT**

IL TEAM DEL CAFFÈ DIGITALE



Roberto MASIERO
Presidente
The Innovation Group



Ezio VIOLA
Co-founder
The Innovation Group



Emilio MANGO
General Manager
The Innovation Group



Elena VACIAGO
Associate Research Manager
The Innovation Group



Roberto BONINO
Giornalista, Research and
Content Manager
The Innovation Group



Valentina BERNOCCO
Web and Content Editor
The Innovation Group



Arianna PERRI
Research Analyst
The Innovation Group

3

L'EDITORIALE

**La nuova sfida dei CIO
si chiama comunicazione**

Roberto Bonino

4

**QUESTO MESE ABBIAMO
FATTO COLAZIONE CON...**



Daniele Catteddu
***Chief Technology
Officer, Cloud
Security Alliance***

Elena Vaciago

7

**PREDICTIVE
ANALYTICS**

FOCUS PA

**AI, le potenzialità per la
Pubblica Amministrazione**

Arianna Perri

9

GDPR
GENERAL
DATA PROTECTION
REGULATION

DIRITTO ICT IN PILLOLE

**Ruolo del DPO: la
relazione del Comitato
europeo per la
protezione dei dati**

Valentina Frediani



11

CIO SUMMIT

**Dall'innovazione di frontiera
alle fondamenta dell'IT**

Valentina Bernocco



14

**INTELLIGENZA
ARTIFICIALE**

**Generative AI tra le
priorità per le aziende
italiane**

Arianna Perri



16

LA TRASFORMAZIONE DIGITALE

**Lavoro 5.0, un'opportunità da sfruttare
per i CIO**

Roberto Bonino

La nuova sfida dei CIO si chiama comunicazione

Roberto Bonino, Research and Content Manager

TIG



Siamo già andati oltre, per certi versi, all'era della digital transformation. Sia chiaro, ci sono parecchie aziende tuttora nel pieno del processo evolutivo e altre che addirittura lo stanno iniziando ora. Ma l'onda montante dell'intelligenza artificiale sta di nuovo mutando lo scenario di riferimento e portando i percorsi di evoluzione strategica verso quella che potremmo definire la "generative transformation".

Lo spunto è stato insinuato nella mente dei CIO da Carlo Alberto Carnevale Maffé, Associate Professor of Practice di Strategy and Entrepreneurship presso SDA Bocconi

School of Management, in chiusura del Summit che TIG – The Innovation Group ha organizzato dal 14 al 16 marzo scorsi a Baveno. In un mondo che agisce sempre più in tempo reale e dove, di conseguenza, non ha più senso dettare regole cristallizzate, i CIO hanno l'opportunità di distogliere l'attenzione dalla codifica dei processi per provare a gestire organizzazioni giocoforza sempre più liquide, sfruttando una visibilità a 360° che non ha pari in altre funzioni aziendali.

Tanto dagli interventi degli esperti che hanno introdotto e concluso i lavori del Summit quanto dalle discussioni che hanno animato i vari tavoli di lavoro dell'evento, è emerso un tratto comune, a volte strisciante e, in altri casi, esplicitato in modo chiaro: per il CIO non è più il tempo di occuparsi di tecnologia fine a sé stessa e nemmeno dei dati in quanto tali, bensì di concentrarsi sul linguaggio e sulla comunicazione.

Acquisire peso e generare valore in azienda, oggi, significa padroneggiare uno scenario che l'intelligenza artificiale generativa sta rimodellando in direzione del rapporto fra base di conoscenza e capacità di fornire rapide risposte. Organizzare correttamente il patrimonio informativo delle aziende, costruire i modelli dai quali far discendere gli input richiesti dal business e dare evidenza della propria centralità sono le sfide che attendono l'IT nell'era della generative transformation. I CIO sono pronti a raccoglierle? Da Baveno qualche indicazione positiva è arrivata, in mezzo alle classiche preoccupazioni sui budget raramente adeguati, il dialogo faticoso con le Line of Business, le richieste destrutturate da gestire e le difficoltà ad attrarre e trattenere i talenti. La strada dell'evoluzione appare segnata e deve portare a quello che, presto o tardi, dovrà chiamarsi "Chief Language Officer".

Daniele Catteddu, Chief Technology Officer, Cloud Security Alliance

Zero Trust, tendenza chiave per la cybersecurity

Elena Vaciago, Research Manager

TIG



L'approccio Zero Trust è oggi un tema scottante. È noto, infatti, un certo scetticismo su questa strategia, anche per l'equivoco su quello che rappresenta: va detto che non si tratta di una tecnologia. Si tratta infatti di un approccio strategico, una vera e propria filosofia

Zero Trust è un approccio strategico moderno alla gestione della cybersecurity, i cui capisaldi sono l'attribuzione di fiducia sulla base delle evidenze, il privilegio minimo, il "need to know".

Durante il suo intervento, nel corso del Cybersecurity Summit 2024, lo scorso 29 febbraio a Milano, Daniele Catteddu, Chief Technology Officer di Cloud Security Alliance, si è concentrato sugli aspetti fondamentali della filosofia zero trust.

CHI È CLOUD SECURITY ALLIANCE E QUAL È IL SIGNIFICATO DI "ZERO TRUST"?

Cloud Security Alliance (CSA) è una no-profit che fa ricerca e formazione. In Italia siamo conosciuti soprattutto perché l'ACN, l'Agenzia di Cybersicurezza Nazionale, ha selezionato il nostro programma "Star" di certificazione e di governance di sicurezza per Cloud service provider, come sistema di requisiti per il PSN, il Polo Strategico Nazionale.

Parlando dell'approccio Zero Trust (ZT), sappiamo che è oggi un tema scottante. È noto, infatti, un certo scetticismo su questa strategia, anche per l'equivoco su quello che rappresenta: va detto da subito che non si tratta di una tecnologia. Questa ha sì un valore fondamentale, ma non deve essere considerata un punto di partenza. Si tratta infatti di un approccio strategico, una vera e propria filosofia. Il nome stesso paga lo scotto di essere in parte un nome improprio: non si tratta tanto di avere "fiducia zero", ma piuttosto, di dotarsi di un processo di costruzione della fiducia, ossia capire su quali elementi fondare una fiducia che renda possibile l'accesso alle risorse da parte di chiunque debba farlo.

PUNTO FONDAMENTALE DELL'APPROCCIO ZT È IL CAMBIO DI PARADIGMA

Fino ad ora, anche per una cattiva gestione corrente del rischio, ci si trova a dover fare delle analisi riguardo al livello di "trustworthiness" (affidabilità) sulla base di



considerazioni soggettive, poco razionali. Questo non è il presupposto ideale. ZT ci dice che dovremmo invece basarci su un concetto di “evidence-based trust”, ossia su prove e fatti da analizzare in modo da accordare il corretto livello di fiducia.

In termini di definizioni di ZT, ce ne sono diverse. CSA, che ha cominciato a lavorare su ZT nel 2014 (quando il mio team ha creato il software defined perimeter), utilizza come working definition quella del report NSTAC rivolto al Presidente USA. È una definizione che scaturisce da una spinta politica forte, ossia dall’Executive Order di Biden di due anni fa, che ha richiesto a tutta la PA americana di adottare questo approccio. In particolare, il DOD (Department of Defense) USA,

analogo del nostro Ministero della Difesa, per primo ha richiesto che entro il 2025 tutto sia adeguato a ZT. Questo ha dato una spinta molto forte al mercato.



ZT È UN VIAGGIO, UN PERCORSO E UN PROCESSO DA COMPLETARE NEL TEMPO

Non è pensabile che un’organizzazione possa implementare ZT dall’oggi al domani. Può farlo Google, che lo ha applicato in 2 anni, nel 2013 e 2014, per tutta la società (con il modello denominato BeyondCorp), ma si è trattato di un caso unico. Non ci sono molte organizzazioni con risorse e competenze per un deploy su tutta la scala.

Quello che serve è dotarsi di un approccio consapevole e seguire vari passaggi, seguendo l’intero ciclo di vita. Oggi abbiamo numerose complessità nella cybersecurity, dovute a tecnologie che vanno convergendo: il cloud che deve parlare con l’Industrial OT, l’arrivo

AI, le potenzialità per la Pubblica Amministrazione

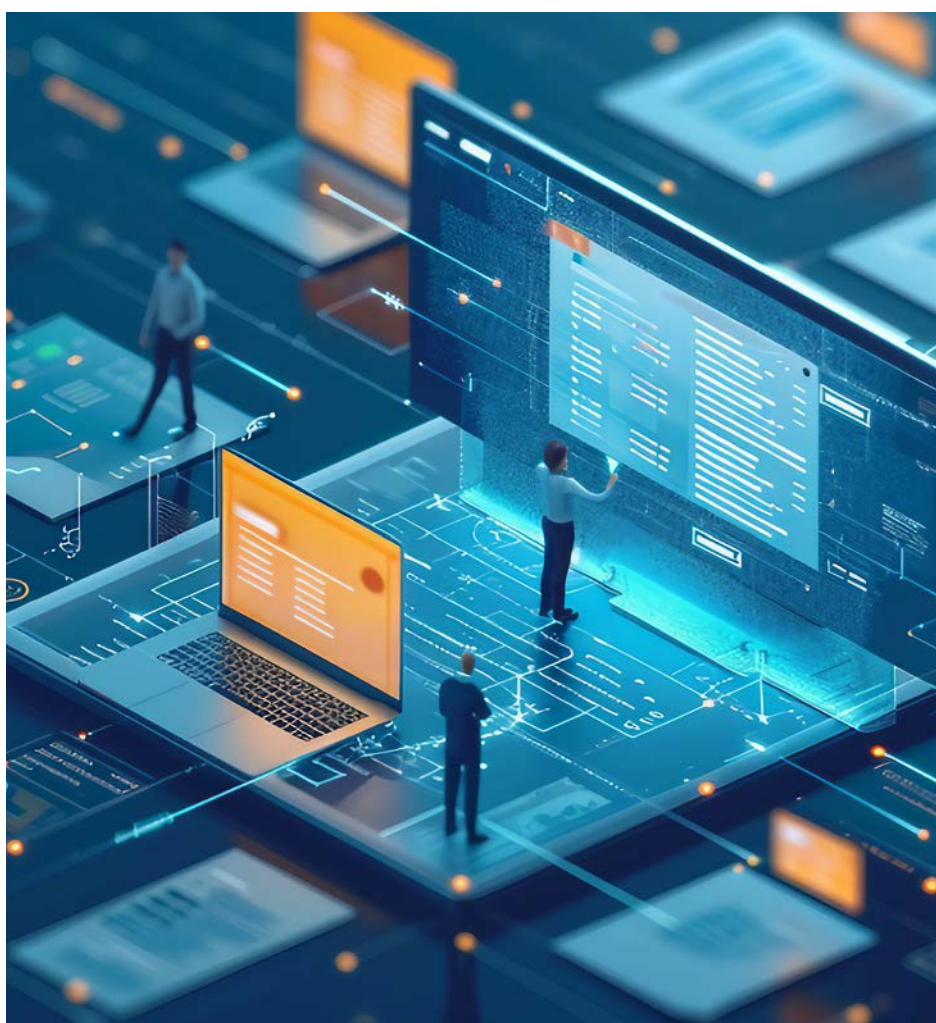
Arianna Perri, Research Analyst

TIG

Lo scorso 12 febbraio è stato pubblicato il Piano Triennale 2024-2026 per l'informatica nella Pubblica Amministrazione di AgID. Il Piano rappresenta uno strumento fondamentale per stimolare la trasformazione digitale della Pubblica Amministrazione (PA) e si traduce nella definizione di una strategia di digitalizzazione, fornendo indicazioni operative sotto forma di obiettivi e risultati attesi.

Come sottolineato da Mario Nobile, Direttore Generale di AgID durante l'evento di presentazione, tre sono i punti chiave che caratterizzano la nuova edizione del Piano Triennale:

1. **Partecipazione attiva:** assumendo un ruolo altamente strategico, il Piano necessita di un coinvolgimento da parte di tutti gli attori, ossia la partecipazione attiva non solo della PA centrale, ma anche dei comuni.
2. **Dinamismo:** la consapevolezza circa la rapidità dei cambiamenti nel mondo digitale e la conseguente necessità di adattarsi in modo flessibile, rendono evidente quanto non ci si possa più permettere di affidarsi esclusivamente a pianificazioni a lungo termine. Per questo motivo, sono stati previsti due aggiornamenti intermedi del Piano: il primo programmato per settembre 2024 e il secondo nel corso del 2025.



3. **Strumenti abilitanti e inclusività:** fornire strumenti abilitanti che agevolino la pianificazione strategica è di fondamentale importanza. L'accento è posto sulla necessità di ridurre il digital divide: le fasce della popolazione che sono in ritardo nell'adozione o, nel peggiore dei

casi, ne sono escluse, rischiano di rallentare l'intero sistema paese. Nonostante le numerose iniziative di formazione avviate, permangono difficoltà nella diffusione di competenze.

Ma la vera novità di questa edizione del Piano è l'inclusione di un capitolo dedicato all'intelligenza



artificiale. Gli obiettivi che il Piano si propone di raggiungere tramite l'adozione dei sistemi di AI sono legati all'automatizzazione delle attività di ricerca e analisi delle informazioni semplici e ripetitive; all'aumento delle capacità predittive, migliorando il processo decisionale basato sui dati; alla personalizzazione dei servizi incentrata sull'utente, aumentando l'efficacia dell'erogazione dei servizi pubblici.

Partendo dalle norme di affidabilità, sicurezza, protezione dei diritti fondamentali ed eticità definite dall'AI Act, il Piano riporta dieci principi generali che dovranno essere adottati dalle PA:

1. Miglioramento dei servizi e riduzione dei costi tramite l'automazione dei compiti ripetitivi
2. Analisi del rischio per garantire che i sistemi non provochino violazioni dei diritti fondamentali della persona
3. Trasparenza, responsabilità e informazione riguardo all'utilizzo dei servizi che sfruttano l'AI
4. Inclusività e accessibilità, assicurando equità, trasparenza e non discriminazione

5. Privacy e sicurezza, conformandosi alla normativa vigente in materia di protezione dei dati personali e di sicurezza cibernetica
6. Formazione e sviluppo delle competenze necessarie per gestire e applicare l'AI in modo efficace
7. Standardizzazione, tenendo in considerazione la normazione tecnica in corso a livello internazionale ed europeo da CEN e CENELEC, con particolare riferimento all'AI Act
8. Sostenibilità, valutando gli impatti ambientali ed energetici legati all'adozione di queste tecnologie
9. Foundation Models (sistemi AI "ad alto impatto"), assicurandosi che adottino adeguate misure di trasparenza prima di introdurle nei processi
10. Modalità e condizioni dei fornitori nella gestione dei dati forniti dall'amministrazione.

Affinché l'introduzione dell'AI nella Pubblica Amministrazione possa dirsi completa ed efficace, bisogna prima valorizzare il patrimonio informativo pubblico e affrontare le nuove

sfide della data economy. Infatti, se l'ingente quantità di dati prodotti dalle PA fosse ben valorizzata e di alta qualità, potrebbe costituire una solida base per l'implementazione efficace dei sistemi di AI. In particolare, l'affermarsi dei foundation models, importante fattore di accelerazione per l'adozione di soluzioni di AI, rende ancor più necessaria la creazione di dataset di elevata qualità, rappresentativi della realtà della PA, con un'attenzione diretta alle norme, nazionali e comunitarie e ai procedimenti amministrativi.

I target definiti nel Piano per la creazione di basi di dati nazionali strategiche sono:

- Target 2024: Ricognizione delle basi di dati strategiche
- Target 2025: Digitalizzazione delle basi di dati strategiche
- Target 2026: Promozione delle basi di dati strategiche

Nel Piano, infine, vengono citate le esperienze di alcune PA centrali che hanno già iniziato a utilizzare soluzioni di AI: Agenzia delle entrate, con l'utilizzo di algoritmi di machine learning in grado di prevenire e rilevare le frodi; INPS, con l'adozione di chatbot che semplificano e personalizzano l'interazione con l'utente; ISTAT, con l'utilizzo di GenAI per creare query tramite il linguaggio naturale, migliorando l'accessibilità ai dati statistici.

Ruolo del DPO: la relazione del Comitato europeo per la protezione dei dati a sei anni dall'entrata in vigore del GDPR



Valentina Frediani, General Manager
Colin & Partners

Un primo dato significativo riguarda proprio il numero delle risposte raccolte: rispetto ai 60.000 soggetti coinvolti, solo 17.490 hanno fornito una risposta e di queste solo una piccola percentuale appartiene a Responsabili della protezione dei dati, mentre la maggioranza dei riscontri proviene dalle stesse organizzazioni

Tenendo fede all'impegno di un'applicazione coerente della normativa in materia di protezione dei dati personali e di una cooperazione tra Autorità di controllo, in occasione dell'ultima plenaria, il Comitato europeo per la protezione dei dati ha reso noto l'esito di un'indagine condotta da 25 autorità di protezione dei dati dell'UE e dello Spazio economico europeo riguardo al ruolo, la designazione e la posizione dei Data Protection Officer.

La relazione, frutto di un'analisi avviata nel corso del 2023, raccoglie oltre 17.000 riscontri di titolari e responsabili per la protezione dei dati provenienti da molteplici settori, sia pubblici che privati. I dati analizzati consentono di costruire un quadro piuttosto significativo rispetto alla posizione e all'attività del DPO, senza dubbio un ruolo ancora piuttosto

giovane a livello professionale, ma che a distanza di sei anni dall'entrata in vigore del Regolamento europeo è già possibile interpretare a livello pratico.

Un primo dato significativo riguarda proprio il numero delle risposte raccolte: rispetto ai 60.000 soggetti coinvolti, solo 17.490 hanno fornito una risposta e di queste solo una piccola percentuale appartiene a Responsabili della protezione dei dati, mentre la maggioranza dei riscontri proviene dalle stesse organizzazioni. Un aspetto non certamente trascurabile, che potrebbe aver influenzato considerevolmente l'esito dell'indagine.

A dispetto della partecipazione limitata, i dati raccolti offrono una panoramica molto interessante e una chiara visione delle principali criticità riscontrate, che devono fungere da punto di partenza per rimediare ai gap.

Tra le maggiori difficoltà evidenziate dal report, emerge la mancata nomina del responsabile della protezione dei dati, anche per le società o Enti in cui tale figura risulta obbligatoria. Un dato assolutamente sconcertante se si pensa che il Regolamento è pienamente applicabile dal 2018 e che mette in luce la mancata conformità di molte realtà al quadro normativo vigente.

Se pensiamo a gran parte delle società di informatica che si occupano di cloud, di manutenzione o sviluppo e che trattano in modo diretto o incidentale dati per i quali dovrebbero essere costantemente allineate al tema privacy, nonostante quanto evidenziato da parte dal Garante italiano, una gran parte di esse non ha ancora provveduto ad alcuna nomina.

Scarsità di risorse e conoscenze sono ulteriori punti deboli rilevati che non consentono di rispondere in maniera efficace alle sfide che tale ruolo è chiamato a fronteggiare. Il contesto legal-tech, in continua evoluzione, richiede

un effort considerevole in termini di risorse e formazione e amplia in maniera significativa il campo di attività e conseguenti responsabilità del DPO. Sollecitato da incarichi sempre maggiori e gravosi, da responsabilità crescenti e non supportato da risorse affiancate alla funzione, il report descrive addirittura il “burnout” tra le potenziali conseguenze.

Proseguendo nell’analisi dei risultati dell’indagine si riscontrano segnalazioni che mettono in evidenza una scarsa chiarezza nella definizione dei compiti del DPO: se da un lato in alcune organizzazioni manca una piena consapevolezza del ruolo svolto, in altre emerge come tale funzione venga ricoperta da soggetti non adeguati, che talvolta, per i ruoli ricoperti, generano un conflitto di interessi rispetto all’incarico di Responsabile per la protezione dei dati. Il fatto che la funzione venga assunta da CEO, CFO o Responsabili di Direzioni, genera non poca preoccupazione e tale circostanza, a ben vedere, non consente di esercitare un controllo indipendente e oggettivo rispetto ai trattamenti dei dati effettuati, alle scelte organizzative in essere o pianificate e agli investimenti.

In altre situazioni, invece, la problematica riscontrata è di altra natura: è questo il caso in cui il DPO non gode della necessaria autonomia decisionale, o indipendenza che dir si voglia. Talvolta, infatti, accade che il responsabile per la protezione dei dati non possa contare su un canale di dialogo diretto con i vertici aziendali e questo è un serio ostacolo all’esercizio sia delle funzioni che della propria responsabilità.

In un momento in cui una serie di normative del settore digital si trova in una fase di sviluppo decisiva o prossima all’entrata in vigore – dalla NIS2 all’AI ACT – il DPO è soggetto ad ulteriori evoluzioni e assumerà un ruolo chiave per tradurre le nuove disposizioni nell’ecosistema aziendale. Ragione in più per cui diviene fondamentale, per imprese e PA, valutare attentamente sia i soggetti incaricati a svolgere tale funzione che le modalità con cui gli stessi sono supportati e coinvolti nei processi.

Il report non si limita ad una panoramica statica delle criticità, ma offre importanti spunti per fronteggiare concretamente le nuove sfide, suggerendo una serie di



raccomandazioni, alcune rappresentate in modo esplicito, altre deducibili dal documento stesso, prima tra tutte, la designazione del DPO per le strutture obbligate, tutt’oggi inadempienti.

Maggiori risorse in termini di budget e tempo sono altre importanti esortazioni per potenziare il ruolo del DPO, che dovrà essere sostenuto anche da un aggiornamento costante rispetto al quadro normativo di riferimento in continuo sviluppo. Parimenti, il Responsabile della protezione dei dati dovrà poter contare su maggiori margini di autonomia e sulla possibilità di svolgere la propria funzione senza interferenze e con un dialogo diretto con i vertici aziendali. I suoi compiti dovranno essere ben definiti e conosciuti anche dal resto della popolazione aziendale, in modo tale da essere coinvolto attivamente nelle attività che abbiano a che fare con il trattamento dei dati personali.

Queste sono solo alcune delle principali raccomandazioni citate nel documento dell’EDPB che, in chiusura del report, non manca di ricordare alle organizzazioni le conseguenze sanzionatorie previste per la non conformità agli articoli da 37 a 39 del GDPR (le disposizioni che disciplinano la figura e i compiti del DPO), che possono raggiungere i 10 milioni di euro o il 2% del fatturato di gruppo.

Dall'innovazione di frontiera alle fondamenta dell'IT

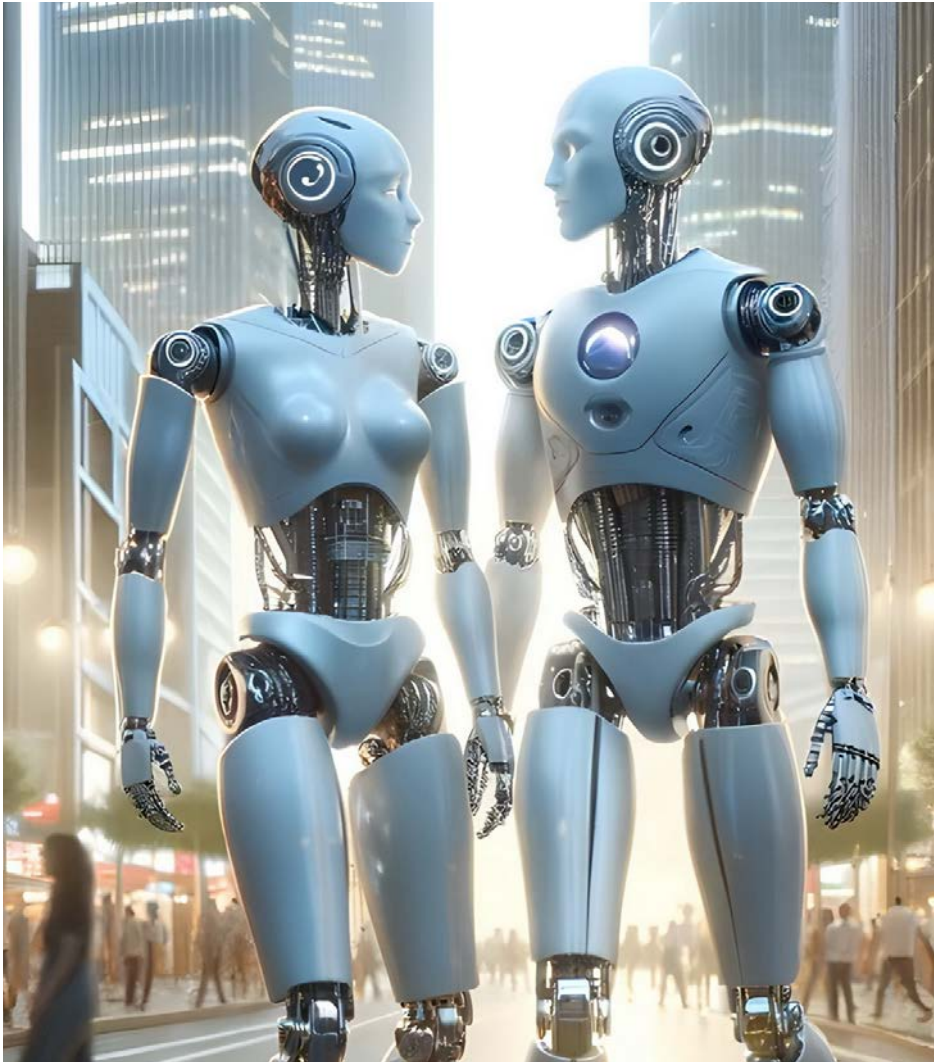
Valentina Bernocco, Web and Content Editor

TIG

Quello dei Cio è un ruolo complesso, che oscilla tra richieste di cambiamento e necessità di rendere più solida l'infrastruttura IT e le competenze esistenti.

Da un lato l'innovazione tecnologica che corre verso le nuove frontiere dell'ingegneria informatica, dove si sovrappongono intelligenza artificiale, robotica, quantum computing, droni. Dall'altro un'esigenza di consolidare le fondamenta dell'IT aziendale, un ritorno alle attività e conoscenze troppo trascurate in anni di frenetica spinta verso l'ultima novità dell'universo digitale. Questi due temi apparentemente opposti trovano un comune denominatore nella figura del chief information officer, protagonista dell'evento "Cio Leaders Summit", organizzato da TIG – The Innovation Group il 14, 15 e 16 marzo scorsi a Baveno, sul Lago Maggiore. Un'occasione per ripensare alle responsabilità di una figura professionale che spesso si relaziona direttamente con i vertici aziendali, dovendo assecondare le richieste di cambiamento dettate dal business; una figura, allo stesso tempo, responsabile della solidità e della sicurezza dell'infrastruttura





hardware e software che fa da base a tutto, a ciò che è consolidato e alle future innovazioni.

A parlare di innovazione di frontiera, dal palco del Cio Leaders Summit, è stato

Cosimo Accoto, research affiliate & fellow del Massachusetts Institute of Technology (Mit) di Boston e professore aggiunto dell'Università di Modena e Reggio Emilia (Unimore). "Siamo in un'epoca che sta muovendosi rapidamente dalla condizione di scienza a quella di ingegneria", ha esordito Accoto. "Questo significa che molte delle innovazioni tecnologiche che fino a poco tempo fa erano innovazione scientifica nata nei laboratori, oggi stanno diventando innovazioni ingegneristiche. Stiamo costruendo le nuove fondamenta ingegneristiche

per la civiltà del ventunesimo secolo".

Tra gli esempi di "ingegneria della frontiera" (così li chiama il Mit), protagonisti del prossimo decennio, ci sarà probabilmente l'intelligenza artificiale, che oggi è maturata da semplice machine learning ad AI generativa, capace di produrre testi, audio e immagini. La prossima fase teorizzata dal Mit sarà quella dell'intelligenza incorporata nella robotica (di cui peraltro già esistono esempi concreti, come le macchine umanoidi di Figure sommate alle reti neurali di OpenAI), mentre in un futuro più lontano esisterà forse una "intelligenza planetaria", cioè un'attività cognitiva che opera su scala planetaria.

L'ingegneria della frontiera oggi sperimenta in diversi ambiti, dalla scienza dei materiali all'informatica vera e propria. Si lavora, per esempio, nel calcolo quantistico con progetti di quantum sensing, quantum networking, crittografia post-quantistica, e si arriverà forse nei prossimi decenni ad avere una "quantum Internet". Secondo i ricercatori la Blockchain avrà un ruolo di peso nel nostro futuro, ma si dovrà vincere la sfida della interoperabilità creando una piattaforma di raccordo per quelle che sono, attualmente, isole tecnologiche non dialoganti tra loro (cioè, incapaci di scambiarsi dati). E che dire dell'idea, forse anche un po' inquietante, di una intelligenza collettiva governata tramite Blockchain e utilizzata per far funzionare sciami di droni? Anche questa è una prospettiva all'orizzonte.

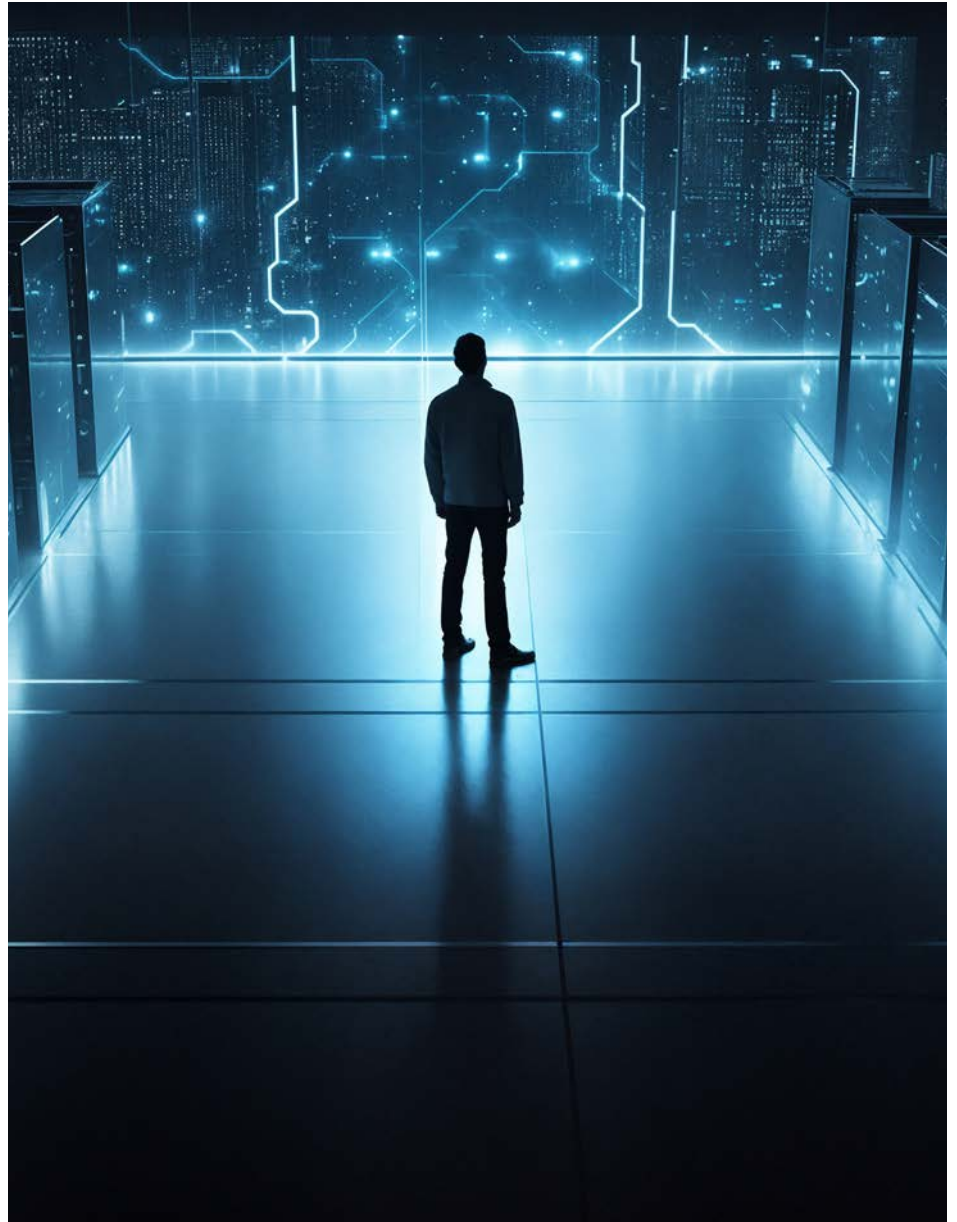
"In realtà quelle che sembrano innovazioni tecnologiche si candidano a diventare innovazioni istituzionali", ha sottolineato Accoto. "Stiamo passando dalle macchine di Turing alle istituzioni di Turing: macchine che danno vita a forme organizzative del tutto nuove". Il ricercatore ha anche sottolineato una sfida insita nell'ingegneria della

frontiera: “Dovremo capire come tenere insieme gli avanzamenti tecnologici qui descritti, molti dei quali sono energivori, con l’abitare il Pianeta in modo più sostenibile”, ha detto Accoto.

Se queste sono le nuove frontiere, le aziende di ogni dimensione e settore oggi si trovano a dover gestire questioni forse meno attraenti ma più concrete, fondamentali per la loro sicurezza e sopravvivenza nel mercato: per esempio la transizione al cloud (ancora in gran parte incompiuta), l’integrazione dell’intelligenza artificiale generativa nei processi esistenti (come quelli di CRM, Erp, o nelle risorse umane) e l’esigenza di lanciare continuamente nuovi servizi, e quindi nuove applicazioni, senza trascurare una cybersicurezza sempre più difficile da garantire.

Sul palco del “Cio Leaders Summit” diversi relatori hanno concordato sull’esigenza di rafforzare le fondamenta dell’IT aziendale, di qualsiasi azienda, prima di poter pensare a queste evoluzioni. Un back to basics, insomma. “In tante aziende c’è da lavorare per mettere a posto le fondamenta”, ha detto Alfonso Fuggetta, Ceo di Cefriel. “Un esempio: non si sa più progettare software, perché tanto lo si compra e ci si illude che non servano competenze. Non si sa progettare architetture di rete, non si sa gestire un sistema distribuito o utilizzare tecnologie come le Api, inventate vent’anni fa”.

Marco Bentivogli, economista ed esperto di politiche di innovazione dell’industria e del lavoro, ha sottolineato che all’Italia manca, attualmente, una rete di trasferimento delle competenze. “Più che pensare a fare l’OpenAI italiana, dovremmo ricostruire il nostro tessuto delle competenze del lavoro e il tessuto produttivo per rendere il sistema industriale realmente più aperto all’innovazione. Credo che la parola d’ordine sarà polarizzazione:



pochi staranno in mezzo e i più saranno agli estremi, o coinvolti o marginalizzati dall’innovazione”.

In questo scenario complesso, i Cio si trovano sulle spalle la responsabilità di orientare la trasformazione tecnologica delle aziende, su cui poggia anche la trasformazione dei modelli di business. Una responsabilità enorme, che oscilla tra i due poli opposti: richiede curiosità, apertura verso l’innovazione già consolidata o “di frontiera”, ma esige anche la capacità di restare con i piedi per terra e anzi di scavare più sotto, fino alle fondamenta dell’IT, per renderle più solide.

Generative AI tra le priorità per le aziende italiane

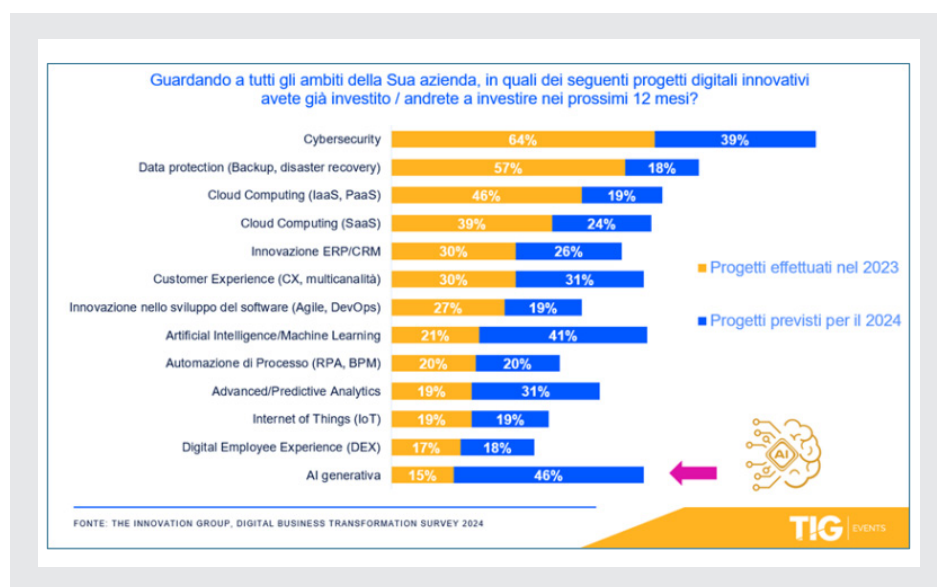
Arianna Perri, Research Analyst

TIG

Nell'ultimo anno e mezzo, l'entusiasmo per la Generative AI (GenAI) ha travolto i modelli di business delle aziende che hanno iniziato a considerarla non solo come vantaggio competitivo, ma una vera e propria questione di sopravvivenza. Superato il momento di euforia, la domanda che ora ci si pone è: come sfruttare concretamente le potenzialità di questa tecnologia? Dai risultati dell'indagine annuale "Digital Business Transformation", condotta da The Innovation Group nei mesi di gennaio e febbraio 2024, la GenAI risulta essere una priorità nelle agende delle imprese italiane per l'anno in corso. Grazie alla sua capacità di apprendimento continuo e alla facilità di accesso tramite interfacce conversazionali user-friendly, la GenAI può indurre infatti un reale cambio di passo nel percorso di trasformazione digitale delle aziende.

Attualmente, il 39% delle imprese italiane si trova in una fase di studio, mentre il 36% l'ha già introdotta in toto o in parte nei processi aziendali. Se il 2023 è stato un anno in cui le aziende si sono impegnate in prevalenza in progetti innovativi di cybersecurity, data protection e cloud, il 2024 sarà l'anno in cui le aziende investiranno di più in GenAI (46%).

Le aree di applicazione spaziano dall'automazione del customer service all'analisi di mercato, dalla personalizzazione della customer experience alla cybersicurezza. L'area meno impattata è quella delle risorse umane, con il 31% delle aziende che riferisce di non fare alcun utilizzo della GenAI in questo ambito: una possibile spiegazione potrebbe essere correlata alle crescenti preoccupazioni relative alle questioni etiche e legali come la trasparenza, la privacy e le possibili discriminazioni. Nel complesso, le aziende prevedono di utilizzare la GenAI principalmente in attività di interazione e di coinvolgimento dei propri clienti.





Applicazioni e tendenze

Lo scorso anno, al fine di introdurre la GenAI, le aziende hanno primariamente valutato le proprie esigenze aziendali, la sicurezza e le questioni legate alla privacy. Nel 2024, invece, si prevede un aumento significativo delle attività legate alle scelte tecnologiche più adatte (64%), alla gestione dei dati (54%), alla formazione e supporto (39%) e all'integrazione dei sistemi (36%).

L'uso regolare degli strumenti di GenAI è attestato dal 45% degli intervistati, dato che ne dimostra un'adozione sempre più

diffusa. L'uso nel contesto lavorativo è ampio (40%), mentre solo una quota minore afferma di non aver mai utilizzato questi strumenti. Le applicazioni dell'AI generativa sono versatili: sebbene sia attualmente prevalente nel contesto della ricerca e della raccolta di informazioni, è evidente che, nel complesso, il suo ruolo sarà semplificare sempre di più le attività lavorative.

Le aziende si affidano principalmente a società di servizi IT e consulenti per l'implementazione della GenAI, ma il 19% fa affidamento esclusivamente

su competenze interne, dato che dimostra una crescente maturità interna nel campo dell'intelligenza artificiale.

Sfide e opportunità

Nel percorso di adozione della GenAI, sebbene le aziende siano avanzate nell'identificazione dei casi d'uso e nella scelta dell'infrastruttura di riferimento, gli aspetti di governance e la costruzione di team in grado di realizzare i progetti, rappresentano ancora un ostacolo. Un cambiamento culturale profondo, l'acquisizione di competenze specializzate, rassicurazioni sugli output e una gestione attenta delle questioni legali sono considerati necessari per adottare pienamente questa tecnologia.

Le potenzialità della GenAI, secondo le aziende, sono: efficienza, automazione, semplificazione, riduzione dei costi operativi e potenziamento delle capacità predittive. Mentre gli IT manager sono particolarmente orientati verso l'automazione e la riduzione dei costi operativi, i CEO mirano, tramite l'adozione della GenAI, all'efficienza delle persone e all'aumento del valore dell'offerta.

Lavoro 5.0, un'opportunità da sfruttare per i CIO

Roberto Bonino, Research and Content Manager

TIG



L'AI è rapidamente divenuta un potente motore di trasformazione per il mondo delle imprese, anche se ancora non sembra aver dispiegato tutto il suo potenziale

Gli effetti del periodo pandemico del 2020-21 e, più di recente, quelli collegati alla pur disordinata diffusione dell'intelligenza artificiale generativa hanno contribuito a ridisegnare l'organizzazione del lavoro (o, meglio, di alcuni lavori) nelle aziende. Il concetto di ibrido si è ormai radicato e, anche se una certa tendenza al rientro in presenza si è manifestato in molte realtà, soprattutto medio-piccole, l'idea che una parte degli organici svolga le proprie mansioni professionali anche da remoto è più meno accettata ovunque. Allo stesso modo, il numero di riunioni è aumentato e anche qui lo svolgimento coinvolge persone fisicamente raccolte in un unico ambiente e altre collegate da remoto.

L'AI, dal canto proprio, è rapidamente divenuta un potente motore di trasformazione per il mondo delle imprese, anche se ancora non sembra aver dispiegato tutto il suo potenziale e siano tutt'altro che chiare le ricadute organizzative e sociali che si porta dietro.

Questi fenomeni, incrociati con la cronica carenza di competenze qualificate nei contesti a maggior tasso di innovazione e con le aspettative dei giovani che si affacciano al mondo professionale, concorrono a disegnare quella

che si può definire l'era del lavoro 5.0, caratterizzato dalla flessibilità, dalla collaborazione e dall'utilizzo spinto della tecnologia.

Per i CIO si aprono notevoli opportunità di consolidamento del proprio ruolo, ma anche di orchestratore di un cambiamento che appare più nelle loro corde rispetto ad altre figure manageriali in azienda (le Hr su tutte). A patto che, una volta per tutte, essi siano pronti a ragionare per processi, acquisiscano capacità organizzative e si facciano promotori del dialogo interno e di quello con i soggetti da integrare nella nuova dinamica del lavoro.

Nel corso del 2023, di questi temi si è discusso nei CIO Panel che The Innovation Group ha organizzato in diverse tappe, a Milano, Napoli e Roma, mettendo a confronto complessivamente quasi un centinaio di professionisti in tavoli che facessero emergere le aree aziendali nelle quali concentrare l'attenzione, capire dove ci si trova oggi e con quale metodo affrontare i cambiamenti, individuare gli interventi da mettere in atto ma anche quali interlocutori coinvolgere e quale sia l'orizzonte temporale per definire e attuare le azioni ritenute necessarie.

La diversità dei settori di appartenenza ha condizionato le discussioni nei vari tavoli costruiti in ognuno degli eventi, ma alcuni tratti comuni sono emersi. I CIO hanno evidenziato difficoltà nell'individuazione delle figure corrette con le quali interfacciarsi per condividere un percorso strategico verso il cambiamento, una cultura aziendale ampiamente da far evolvere e anche la complessità non solo di reperire, ma anche di trattenere le risorse più qualificate. Il focus sugli aspetti organizzativi è risultato ampiamente prevalente e ha coinvolto la necessità di definire modelli al momento poco presenti, di avere una flessibilità nell'adattamento degli obiettivi a evoluzioni che avvengono in tempi molto stretti e di poter ricavare valore dal consolidamento del lavoro 5.0.

Dal punto di vista di utilizzo delle tecnologie, inoltre, siamo ancora molto lontani dal capire come sfruttarle al meglio in questo contesto. L'impiego dell'AI potrebbe essere valorizzato nel mondo del lavoro, come già accade, per esempio sui social network, per costruire dei "grafi sociali" e capire, fra le altre cose, chi sono i colleghi in azienda che possono influire o incidere sui team presenti.



ISCRIVITI ALLA NEWSLETTER MENSILE!

**Ricevi gli articoli degli analisti di
The Innovation Group e resta aggiornato
sui temi del mercato digitale in Italia!**



COMPILA IL FORM DI REGISTRAZIONE SU
www.theinnovationgroup.it