

GIUGNO/LUGLIO 2024



IL CAFFÈ DIGITALE



CAVALCARE L'ONDA DELL'AI

IL "RINOCERONTE GRIGIO" NEL CORRIDOIO DELLE BANCHE

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

**Giovanni Di Stefano
Comau**

**TRASFORMAZIONE
DIGITALE**

**Customer service: l'AI è un
alleato ma deve avere un
volto umano**

FOCUS PA

**I numeri della Piattaforma
Digitale Nazionale Dati
(PDND)**

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 BERNOCCHI
Web and Content Editor
The Innovation Group



Arianna PERRI
Research Analyst
The Innovation Group

3

L'EDITORIALE

**Cavalcare l'onda dell'AI,
il "rinoceronte grigio" nel
corridoio delle Banche**

Ezio Viola

6

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



**Giovanni Di
Stefano**

*Responsabile
dell'Ingegneria
delle soluzioni
di automazione
avanzata e della
robotica*

Comau

Roberto Bonino

8

**CYBERSEC
E DINTORNI**

**Incrementi a tre cifre portano
l'Italia ai primi posti tra i Paesi
più colpiti dagli attacchi cyber**

Elena Vaciago

11

DIRITTO ICT IN PILLOLE

**Aspetti chiave per la
costruzione di una strategia
di brand protection**

Giulia Rizza





14

LA TRASFORMAZIONE DIGITALE

Edge data center, un futuro che passa per il dialogo

Luca D'Alleva



16

**FOCUS
PA**

**I numeri della
Piattaforma Digitale
Nazionale Dati (PDND)**

Arianna Perri



18

LA TRASFORMAZIONE DIGITALE

Customer service: l'AI è un alleato
ma deve avere un volto umano

Valentina Bernocco

Cavalcare l'onda dell'AI, il “rinoceronte grigio” nel corridoio delle Banche

Ezio Viola, Co-founder

TIG

I risultati di bilancio delle banche italiane mostrano che il 2023 è stato uno degli anni migliori di sempre, superando le aspettative e i risultati di molte banche straniere.

La crescita dei profitti è stata principalmente dovuta all'aumento dei tassi di interesse deciso dalla BCE. L'outlook per il 2024 rimane positivo, come dimostrato dai dati del primo trimestre, anche se il picco dei tassi nel 2023 porterà a una rimodulazione al ribasso nella seconda metà del 2024. Inoltre, dopo un 2023 in calo, si è osservata una ripresa dei ricavi commissionali, aumentati tra il 6% e il 10%.

La normalizzazione dei tassi deve incentivare le banche a prepararsi adeguatamente, affrontando le incertezze macroeconomiche e geopolitiche, la crescente pressione competitiva, e l'impatto delle nuove tecnologie digitali, come l'intelligenza artificiale e le tecnologie di GenAI basate su modelli linguistici di grandi dimensioni (LLM).

Le banche devono fare un salto ulteriore di qualità e quantità nel processo di trasformazione e innovazione digitale per essere preparate a nuovi “cigni neri” sempre in agguato, legati in primis all'instabile situazione geopolitica, ma anche ai nuovi “rinoceronti grigi”, se sottovalutati.

Un rinoceronte grigio è un evento/fenomeno/fattore altamente probabile e di forte impatto, qualcosa di cui dovremmo renderci conto, (come suo cugino l'elefante nella stanza), ed è qualcosa che dovremmo essere in grado di vedere chiaramente per via della sua portata. Infatti, qualcosa di così imponente deve pur ricevere l'attenzione che merita. Al contrario è proprio l'ovvietà di questi pachidermi a fare parte di ciò che ci rende così incapaci di agire perché a volte non siamo in grado di riconoscere ciò che è ovvio, e quindi di prevenire impatti altamente probabili sia positivi che negativi: quelli rispetto ai quali siamo in grado di fare qualcosa.

Le banche devono fare un salto ulteriore di qualità e quantità nel processo di trasformazione e innovazione digitale per essere preparate a nuovi “cigni neri” sempre in agguato



Alcuni esempi li conosciamo già come il cambiamento climatico e, appunto, la nascita e lo sviluppo di tecnologie radicali e rivoluzionarie come l'AI. Tutte queste sfide, come i rinoceronti che pascolano all'orizzonte, si delineano come minacce lontane all'inizio. Più si avvicinano più alti sono i costi da sostenere per intervenire e più ci convinciamo che sono lontani più è improbabile che faremo qualcosa, facendoci rimanere immobili mentre la minaccia viene verso di noi.

Il settore dei servizi finanziari, secondo diverse analisi, è quello che più sarà impattato dall'utilizzo di tecnologie di AI, con aumenti previsti di produttività di circa il 27% e con un incremento complessivo del valore aggiunto nel settore di circa 23 miliardi di Euro se l'adozione sarà pervasiva in tutti i processi della banca.

Occorre anche dire che nella recente relazione del Governatore della Banca d'Italia si evidenzia "come gli investimenti in tecnologie innovative realizzati dagli intermediari italiani sono quadruplicati dal 2017, ma rimangono limitati, e per le banche significative sono inferiori a quelli delle concorrenti europee. Vanno incrementati: sarebbe un grave errore accumulare ritardi su questo fronte." *

Nonostante l'aumento degli ultimi anni, in Italia gli investimenti in tecnologie innovative (come intelligenza artificiale, cloud, blockchain e big data) sono rimasti nel complesso ridotti, pari al 5% della spesa complessiva in tecnologie che facilitano l'elaborazione delle informazioni, e sono concentrati presso un numero contenuto di banche.

L'IA è già una realtà nel settore bancario. Quasi tutte le banche italiane stanno utilizzando o pianificando di utilizzare l'AI, con molti progetti di AI Generativa in fase sperimentale o di implementazione. Queste



istituzioni vedono l'AI non solo come un'opportunità di crescita, ma anche come una necessità per rimanere competitive.

Poter sfruttare appieno il potenziale dell'IA generativa, è necessario affrontare le sfide e i rischi legati all'integrazione, alla formazione, alla compliance, all'affidabilità e all'etica delle soluzioni sviluppate. Il settore finanziario è in testa nella corsa all'IA generativa, ma deve continuare a innovare, sperimentare nuovi casi d'uso e incominciare a strutturarsi per portare quelli più di valore a scala per tutta la banca

L'AI può essere un "rinoceronte grigio" per quelle banche che non si attrezzano con un approccio strategico complessivo alla sua adozione e utilizzo. La prospettiva, che è ormai una certezza, di una accelerazione dell'utilizzo esteso delle tecnologie digitali, con l'AI può avere un impatto generalizzato su prodotti e servizi, sui modelli e processi operativi



in tutti i segmenti del banking: dalla banca commerciale retail e corporate, al risparmio gestito, ai pagamenti.

Il potenziale inespresso del valore dei dati interni ed esterni della banca, che l'AI è in grado di sfruttare, continuerà a crescere. Ciò permetterà di rivedere i processi bancari per migliorarne la semplicità e la produttività, andando oltre le attività transazionali per ottimizzare le funzioni relazionali e di conoscenza nei processi di front e back office. I casi d'uso dell'AI sono trasversali a tutti i processi aziendali, consentendo di aumentare l'efficienza, migliorare la relazione con i clienti attraverso un ingaggio più personalizzato e conversazionale, e creare nuovi modelli di business monetizzando i dati.

Se l'AI, potenzialmente, possa costituire la prossima frontiera della produttività e redditività per le banche sarà al centro del prossimo "Banking Summit" di The Innovation Group.

È necessario che le banche passino velocemente dalla fase prototipale con sviluppi sui diversi use-case, in alcuni casi con troppa dispersione, alla capacità di mettere a scala progetti di impatto complessivo che generano valore. Oggi la maggior parte delle banche italiane sono ancora in una fase prototipale e alla ricerca di un posizionamento, anche interno, strategico dell'AI nel portafoglio di innovazione.

È importante saperne gestire l'impatto sia interno che esterno in modo responsabile dell'utilizzo esteso delle tecnologie di AI, poiché siamo ancora in una fase di evoluzione delle tecnologie disponibili molto veloce

Il processo di evoluzione e trasformazione delle banche è guidato parallelamente alla tecnologia, anche dalla roadmap che il regolatore sta dando su diversi segmenti cruciali dell'industria bancaria dalla gestione dei nuovi rischi operativi con DORA, alla gestione degli asset digitali con MICAR e alla tutte le normative legate alle tematiche ESG che quest'anno avranno un impulso con l'avvio della CSDR, alla nuova retail investment strategy a normative specifiche come l'AI act a livello europeo.

Occorre ad esempio che le banche siano di fianco nel processo di definizione e realizzazione del modello alla base dell'euro digitale perché costituirà un ulteriore elemento di innovazione e trasformazione tecnologica non solo nei pagamenti ma nel rapporto complessivo tra banche e clienti.

Naturalmente occorre settare realisticamente le aspettative nell'utilizzo di queste nuove tecnologie e i relativi rischi che si estendono all'impatto sul lavoro delle persone, sulla reputazione e sulla fiducia delle banche verso clienti e vari stakeholder, sulla crescita del capitale umano, senza creare un nuovo digital-divide interno alle banche e verso i clienti.

Giovanni Di Stefano, Responsabile dell'Ingegneria delle soluzioni di automazione avanzata e della robotica, Comau

Una digitalizzazione a doppio binario, interna e verso i clienti

Roberto Bonino, Research and Content Manager

TIG



Nel mondo manifatturiero, la trasformazione digitale sta viaggiando sul doppio binario dell'evoluzione dei processi aziendali e degli ambienti di fabbrica. Se nel primo blocco ritroviamo temi comuni al resto del panorama industriale (dalla collaboration alle relazioni con la clientela, per fare degli esempi), il secondo è tipico di un comparto che fonda il corpo centrale del proprio business sulla produzione e sugli stabilimenti dove si realizza. Questi ultimi ambienti sono stati per diverso tempo un terreno quasi pionieristico di innovazione, a partire dall'automazione di fabbrica introdotta in molti casi oltre trent'anni fa. Gli sviluppi tecnologici dei tempi più recenti hanno quantomeno riequilibrato (se non ribaltato) il ritmo dell'innovazione fra il mondo IT e quello OT, non riuscendo però sempre a creare l'armonizzazione necessaria fra dipartimenti con priorità spesso differenti.

In questo contesto, comunque, gli ambienti di produzione si trovano oggi ad affrontare diverse sfide, che vanno dall'efficienza operativa dei macchinari e delle persone che le controllano

all'introduzione dell'IoT industriale e dell'intelligenza artificiale. Su questi temi, ci siamo intrattenuti con Giovanni Di Stefano, Responsabile dell'Ingegneria delle soluzioni di automazione avanzata e della robotica di Comau, società del gruppo Stellantis che realizza prodotti e sistemi di produzione robotizzati, ma si occupa anche di project management, consulenza, manutenzione e formazione per una grande varietà di segmenti industriali.

Nella vostra realtà, quali sono i principali fattori che animano i progetti di trasformazione digitale, quali i processi maggiormente coinvolti e gli obiettivi che si intendono raggiungere nel breve e nel lungo termine?

Il business di Comau ha una doppia sfaccettatura. Da un lato siamo produttori di robot o altri prodotti industriali (esoscheletri o sistemi di visione, per esempio), mentre dall'altro svolgiamo un ruolo di integratori per i nostri clienti. Il percorso di digitalizzazione riguarda entrambe le anime dell'azienda e segue tragitti differenti, seppure con punti di convergenza non



trascurabili. Basti pensare alla scelta del cloud, che serve a noi direttamente tenere sotto controllo il costo capitale dell'infrastruttura, ma anche di agevolare i processi di digitalizzazione dei nostri clienti attraverso la strada della servitizzazione. Sui nostri prodotti, il peso dell'innovazione è molto elevato e parte integrante della nostra value proposition, mentre nel rapporto con la clientela dobbiamo confrontarci con ogni specifica realtà, anche se ci sono temi come la cybersecurity, l'IoT industriale o l'intelligenza artificiale, che sono comuni, pur seguendo declinazioni diverse.

Quali use case descrivono meglio l'impatto dell'innovazione sul vostro modo di lavorare e dove occorre ancora fare sforzi aggiuntivi per migliorare?

Al nostro interno, possiamo citare l'utilizzo dei digital twin, che ha introdotto la possibilità di testare a monte gli impatti di ciò che andrà poi a essere integrato nei nostri sistemi industriali, portando a una velocizzazione del time to market e a una parallela riduzione dei rischi e dei costi di produzione. Verso la clientela,

nodale è la possibilità di raccogliere ed elaborare i dati che provengono dalle macchine, soprattutto per poter fornire un servizio più efficiente e, con l'introduzione dell'intelligenza artificiale, passare dalla manutenzione preventiva a quella predittiva, che consente di intervenire, per esempio, su un componente prima di una possibile rottura già preconizzabile perché calcolata sulle serie storiche raccolte e analizzate a monte.

Visto che l'argomento è stato introdotto, quali sono gli ambiti sui quali state maggiormente studiando un'evoluzione dettata dall'introduzione dell'intelligenza artificiale?

Stiamo iniziando a introdurre queste tecnologie sui sistemi di visione e sulla gestione delle cinematiche dei robot. I nostri primi sistemi di image processing risalgono al 2017 e all'epoca era necessario scrivere algoritmi che poi diventavano resilienti in corso d'uso, monitorando tutti gli scostamenti funzionali. Ora con l'intelligenza artificiale questa resilienza può essere ottenuta automaticamente. In generale, però, ci stiamo muovendo con

prudenza perché occorre tenere sotto controllo i risultati che l'AI produce e che non sempre sono affidabili, per cui procediamo innovando piccole componenti software all'interno di sviluppi più complessi. La reportistica fatta in generative AI è un altro sviluppo certamente importante, stiamo ad esempio testando l'utilizzo di Chatbot basati su AI per agevolare l'utilizzo e la consultazione dei nostri manuali di uso e manutenzione. L'Image Processing ha fatto un notevole balzo in avanti e questo si può verificare sulle capacità di movimento efficace dei robot e sull'ispezione di qualità, In questo caso potendo insegnare all'intelligenza artificiale quando un determinato prodotto contiene le corrette caratteristiche e non presenta difettosità. On top, stiamo testando l'utilizzo dell'intelligenza artificiale sulle cinematiche dei robot per insegnare alle macchine come muoversi al meglio.

Quali sono i progetti più interessanti sui quali state lavorando per il futuro?

Stiamo cercando di andare il più possibile sul generative design, poiché una parte significativa del nostro lavoro è fatto di analisi di accessibilità e conformità sulle componenti che via via andranno a costituire il prodotto finale. L'analisi delle compenetrazioni fra solidi porta via parecchio tempo e si costruisce sulle regole che ci servono per disegnare. Riuscire a trasferire queste regole a una AI sarebbe un bel passo avanti. Stiamo però parlando di sviluppi di frontiera, sui quali non è semplice individuare i partner corretti con i quali lavorare.

Incrementi a tre cifre portano l'Italia ai primi posti tra i Paesi più colpiti dagli attacchi cyber

Elena Vaciago, Research Manager

TIG

Il panorama delle minacce cyber nel nostro Paese è sempre più complesso e minaccioso, come dimostrano i dati del nuovo documento mensile sullo stato della minaccia cyber nazionale pubblicato dall'ACN, l'“Operational Summary” di maggio 2024. Redatto dal Computer Security Incident Response Team (CSIRT Italia) dell'ACN, riporta le statistiche mensili sull'evoluzione delle minacce cyber, approfondendo quali sono le minacce più frequenti, in Italia e in Europa (in sostanza, malware, DDoS e ransomware) e quali sono i settori economici che hanno subito i maggiori impatti.

A maggio, ad esempio, c'è stato un aumento del 148% degli eventi cyber rispetto al mese di aprile, con 283 casi registrati dal CSIRT, di cui 175 con un impatto significativo su soggetti nazionali. Un incremento a tre cifre che dimostra quanto l'Italia sia oggi un obiettivo privilegiato per organizzazioni criminali e gruppi sponsorizzati dagli Stati.

l'Italia è oggi un obiettivo privilegiato per organizzazioni criminali

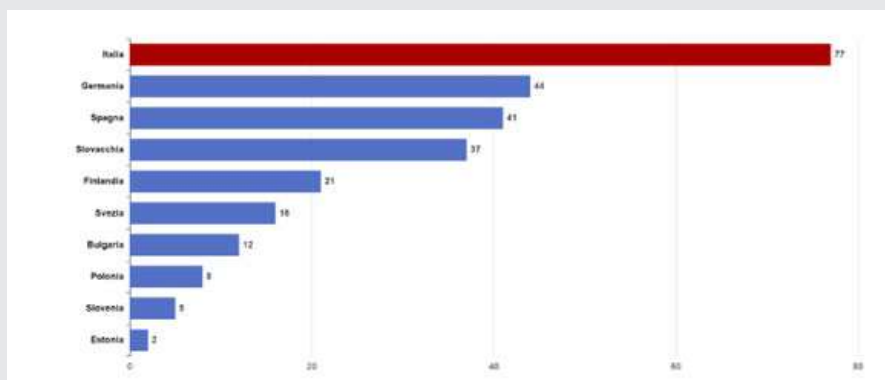


Le minacce cyber più frequenti

Con riferimento alle tipologie di minacce rilevate, si conferma la massiccia presenza di attacchi DDoS, che di solito sono accompagnati da campagne di attivismo con motivazioni ideologiche o politiche, quindi associabili al supporto a particolari parti coinvolte nei conflitti russo-ucraino e israelo-palestinese. Oltre agli attacchi DDoS, per cui è stata rilevata una crescita del 220% rispetto alla media del semestre precedente, le altre minacce rilevate (spesso più di una in contemporanea nel corso degli eventi registrati) sono state: Brand Abuse (in crescita del 94%); Information Disclosure (+125%); Spear Phishing (+38%); Esfiltrazione o data breach (+176%, a conferma delle varieguate strategie di data monetization seguite ora dagli attaccanti); Ransomware (+ 64%).

Il monitoraggio delle rivendicazioni DDoS nel mese di maggio 2024 mostra che l'Italia è stato il primo paese in Europa e il quarto al mondo per numero di rivendicazioni. I gruppi più attivi sono stati NoName057 e CyberArmyofRussia. Il grafico successivo mostra la classifica dei primi 10 Paesi in Europa per rivendicazioni di attacchi DDoS, da cui spicca il posizionamento dell'Italia.

Numero di rivendicazioni DDoS per Paese dell'UE

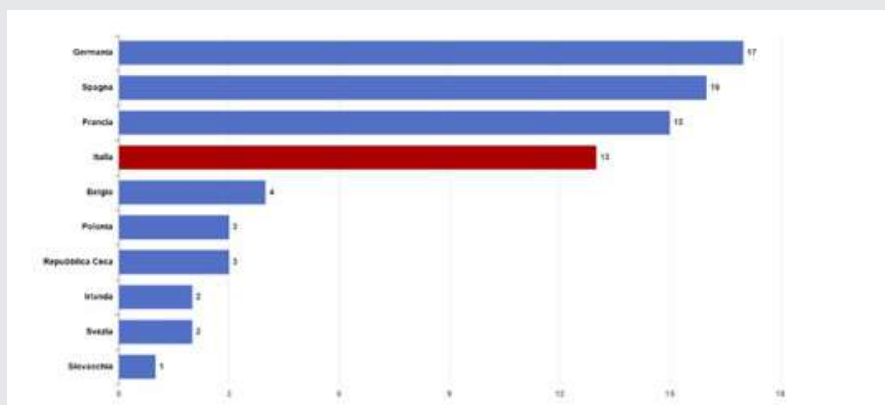


Fonte: "Operational Summary" di maggio 2024. Redatto dal Computer Security Incident Response Team (CSIRT Italia) dell'ACN

Con riferimento invece al ransomware, il monitoraggio di fonti aperte nel mese di maggio 2024 riportato dal CSIRT mostra che l'Italia è stato il quarto paese in Europa e il nono nel mondo per numero di rivendicazioni. In aprile

era stato il secondo in Europa e il sesto nel mondo. I gruppi più attivi sono stati Blackbasta e Lockbit. Il grafico successivo mostra il numero di rivendicazioni ransomware per Paese europeo.

Numero di rivendicazioni ransomware per Paese dell'UE



Fonte: "Operational Summary" di maggio 2024. Redatto dal Computer Security Incident Response Team (CSIRT Italia) dell'ACN

Purtroppo, molto preoccupante anche la situazione che emerge sulle vulnerabilità scoperte di mese in mese, con tutta una serie di indicatori negativi. A maggio scorso, la pubblicazione di 5.026 nuove CVE (Common Vulnerabilities and Exposures, errori di sicurezza già identificati presenti nel software) ha registrato una crescita notevole, del 27% (ossia, 1.355 CVE in più rispetto ad aprile). Per queste CVE il CSIRT fa riferimento naturalmente al database più noto che è quello mantenuto nel National Vulnerability Database del NIST USA (sul sito <https://nvd.nist.gov/vuln>). Di queste CVE, 831 offrono almeno un Proof of Concept (PoC), in calo (-196), e per 14 CVE l'agenzia ha rilevato lo sfruttamento già attivo da parte di attori malevoli, mentre gli exploit (programmi specializzati nello sfruttare una certa vulnerabilità) sono in aumento (+4) rispetto ad aprile.

I settori italiani più impattati secondo il CSIRT

Guardando invece ai settori più impattati dagli attacchi di cybersecurity, dall'analisi emergono la PA centrale, i Trasporti, le TLC: anche il settore ICT è colpito in modo particolare, a dimostrazione di come la catena di fornitura ICT sia oggi uno dei target preferiti dagli attori malevoli. Va detto però che in questo momento il settore pubblico e delle infrastrutture critiche sono

anche quelli sottoposti ad obblighi di notifica, mentre non lo sono al momento le PMI operanti in settori 'non critici' (la maggioranza) o la PA locale. Una situazione questa che potrebbe cambiare con l'arrivo di norme europee come DORA e NIS 2, o la stessa norma DDL Cyber di recente approvazione, che imporranno obblighi di notifica in modo molto più esteso a più operatori economici e pubbliche amministrazioni. Già da fine di quest'anno, sarà possibile quindi avere una visibilità molto più ampia su tutti gli attacchi e gli incidenti in corso che avvengono ogni giorno nel nostro Paese, almeno quelli che impatteranno su operatori pubblici e privati (non chiaramente sui singoli cittadini).

La direzione intrapresa è quella che tutti si auspicano: come emerge anche dall'indagine "Cyber Risk Management 2024" (realizzata a inizio 2024 da TIG e Cyber Security Angels – CSA su un campione di 166 aziende medio grandi) la visibilità estesa e l'accesso a threat intelligence sono considerati fattori cruciali per una strategia efficace di cyber resilienza da un'azienda su 2 (il 55% degli intervistati). Le informazioni sulle minacce in corso, unite a una visibilità estesa sui sistemi e sulle reti aziendali, sono infatti fondamentali per individuare e rispondere prontamente alle minacce informatiche.

Le attività chiave per migliorare la cyber resilienza della propria organizzazione possono garantire un'ampia formazione sui rischi nella popolazione aziendale, con l'81% degli intervistati che ritiene che la formazione sia prioritaria per aumentare la consapevolezza e la preparazione del personale di fronte alle minacce informatiche. Al secondo posto, la tempestività della risposta è cruciale: il 73% ritiene che la capacità di rispondere prontamente agli attacchi informatici sia fondamentale per limitare i danni e ripristinare rapidamente le operazioni. Aziende e pubbliche amministrazioni, operatori pubblici e privati, sono chiamati oggi a collaborare per realizzare una sicurezza di sistema basata su best practice condivise e informazioni messe a fattore comune.

Aspetti chiave per la costruzione di una strategia di brand protection



**Giulia Rizza, Consultant e PM
Colin & Partners**

In un mercato sempre più competitivo dove l'inarrestabile evoluzione tecnologica impone sfide sempre più complesse, la tutela del portafogli IP diviene un'attività centrale per qualsiasi organizzazione. L'espressione definisce il complesso di marchi, design, brevetti, opere tutelate dal diritto d'autore, segreti industriali e know-how rappresentativi del patrimonio intellettuale dell'organizzazione.

L'esperienza di chi scrive conferma che, sebbene si registri un'impennata di cyber attacchi ai danni del patrimonio intellettuale, complici sistemi di frode sempre più sofisticati e tecnologicamente avanzati, nelle organizzazioni manca spesso la consapevolezza del valore reale dei beni immateriali di cui dispone e dei rischi generati da una cattiva gestione o, addirittura, dalla mancata gestione degli stessi.

La costruzione di una strategia

di brand protection efficace parte da un'analisi del portafoglio IP dell'organizzazione: attività essenziale, questa, per raggiungere un livello adeguato di consapevolezza rispetto al valore dei beni immateriali. Alla presa di coscienza deve poi seguire, ad esempio, la corretta registrazione di marchi e domini, altrettanto importante per scongiurare casi di domain grabbing o, persino, di illegittimi usi di segni identici e/o confondibili ai propri da parte di terzi.

Ulteriore aspetto da non trascurare nell'analisi e nella pianificazione delle attività, sono le tempistiche necessarie per la costituzione di proprie privative, che variano a seconda di ciò che è interesse tutelare. L'acquisto di un nome a dominio richiede infatti tempi e costi molto inferiori rispetto a quelli previsti per la registrazione di un marchio, soprattutto laddove vi sia

interesse a ottenere tutela in più territori, e ciò deve essere tenuto in considerazione.

Costituiti i diritti sul proprio portafogli IP nel rispetto delle diverse condizioni previste dalla legge a seconda della privativa del caso, è parimenti importante vigilare sui concreti utilizzi del patrimonio di beni immateriali. Adottare validi strumenti di monitoraggio e implementare le opportune azioni di contestazione, anche giudiziale, consente di avere contezza sia degli usi che degli abusi dei propri beni immateriali e di attivare eventuali azioni cautelative con una certa prontezza, permettendo in molti casi di risolvere la questione mediante strumenti, anche stragiudiziali, che il nostro ordinamento mette a disposizione e, in ogni caso, scongiurando danni maggiori. Spesso, tuttavia, eventuali azioni sono possibili soltanto in un determinato periodo di tempo. Basti

“

I numerosi fatti di cronaca e i dati dei report in materia di sicurezza informatica registrano un significativo aumento di frodi basate sullo sfruttamento non autorizzato di marchi altrui. Si pensi ai casi di siti web che fanno uso non autorizzato di brand anche noti per la vendita di prodotti contraffatti

pensare, ad esempio, alla possibilità di opporsi alla registrazione di un marchio comunitario identico e/o confondibile col proprio marchio italiano, riconosciuta al titolare della privativa anteriore entro un termine definito dalla legge (90 gg. dalla pubblicazione della domanda di marchio contestato sul relativo bollettino EUIPO): laddove non abbia attivato strumenti tali da consentirmi di venire informato in merito a dette pubblicazioni, rischio di precludere, o comunque limitare, le possibili azioni esperibili.

Soprattutto per le aziende che godono di una consolidata presenza online, l'adeguato monitoraggio costituisce, pertanto, uno dei principali strumenti da adottare per un'adeguata strategia di difesa del patrimonio immateriale.

La creazione e il mantenimento di un efficace perimetro di protezione intorno al portafoglio IP aziendale richiede, oggi, anche l'utilizzo di strumenti tecnologici. I numerosi fatti di cronaca e i dati dei report in materia di sicurezza informatica registrano un significativo aumento di frodi basate sullo sfruttamento non autorizzato di marchi altrui. Si pensi ai casi di siti web che – sotto la parvenza di siti ufficiali – fanno uso non autorizzato di brand anche noti e/o utilizzano tali siti, confondibili con quelli ufficiali, per la vendita di prodotti contraffatti.



Non mancano nemmeno esempi di tentativi di phishing attraverso l'impiego di domini confondibili (c.d. typosquatting) con il marchio di organizzazioni ignare.

La portata delle conseguenze connesse a tali condotte illegittime risulta facilmente intuibile: non solo sul piano reputazionale, con tutti i conseguenti risvolti in tema

di fiducia dei clienti e del mercato, ma ovviamente anche in termini di investimenti fatti e sotto il profilo del rischio sanzionatorio che, merita ricordare, può coinvolgere anche la normativa in materia di trattamento di dati personali.

Ulteriore attività da attenzionare in ottica di una corretta strategia di tutela del Portafogli IP è lo

sviluppo e la gestione del sito web aziendale, che ad oggi è il "biglietto da visita" di un'azienda. Si tratta di un'attività che comprende non solo la scelta del nome a dominio e le conseguenti registrazioni, anche a scopo preventivo, ma interessa pure l'ideazione e la selezione dei contenuti del sito e/o delle applicazioni che ne determinano la funzionalità, in particolare laddove tali attività siano affidate ad un terzo. Tali valutazioni dovrebbero – nemmeno a dirlo – essere idoneamente disciplinate a livello contrattuale con tutti i fornitori coinvolti nel processo, delineando obblighi, garanzie e manleve tenuto conto della attività pattuite, nonché definendo opportunamente ruoli, ivi inclusi gli aspetti privacy.

Sebbene spesso sia trascurato o gestito con una certa superficialità, l'aspetto contrattuale non può né deve essere considerato di secondaria importanza. La definizione dei rapporti con i fornitori i cui servizi hanno direttamente a che fare o sono connessi al proprio patrimonio IP dovrebbe essere condotta con impegno e attenzione e dovrebbe essere considerata un investimento fondamentale per le organizzazioni, tenuto conto di quelli che sono i rischi connessi alle varie attività concordate.

Un'adeguata definizione dei rapporti contrattuali, pur comportando molte volte il dilungarsi delle fasi di negoziazione preliminare, consente infatti di ridurre gli impatti sull'operatività del progetto una volta avviato, in particolare laddove siano stati debitamente disciplinati i comportamenti delle parti al verificarsi di eventuali criticità che, a seconda della tipologia di servizi stabiliti, potrebbero casisticamente occorrere.



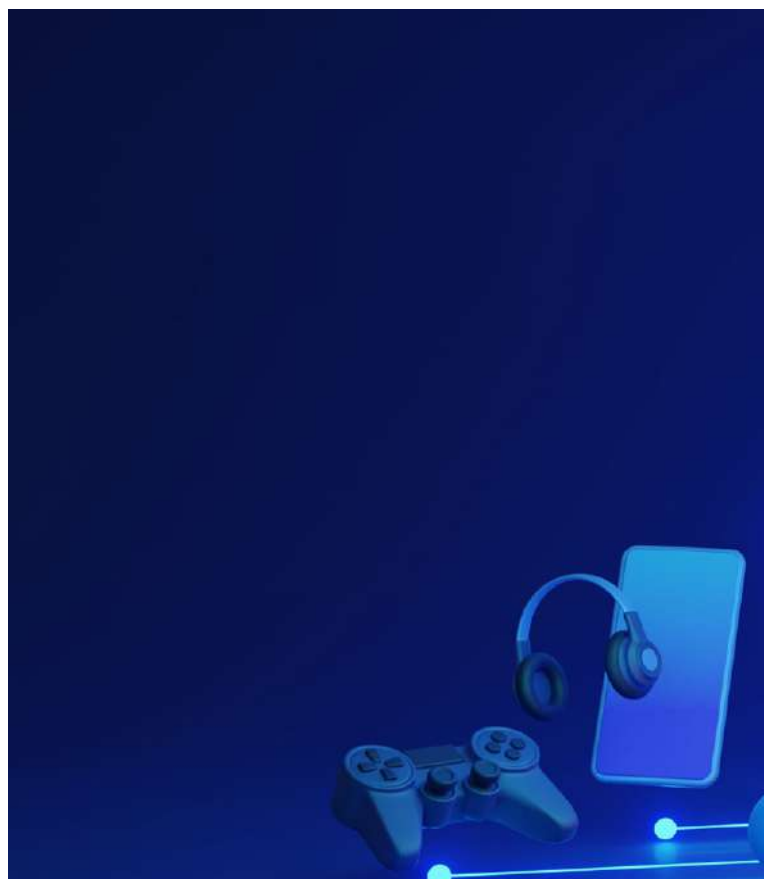
Edge data center, un futuro che passa per il dialogo



Luca D'Alleva, Senior Consultant
BCS Italia

Lo standard di comunicazione mobile 5G ha inaugurato una nuova era nella trasmissione dei dati. Offre capacità e velocità maggiori, oltre a una minore latenza per un numero più elevato di dispositivi rispetto ai suoi predecessori. Le enormi prestazioni garantite da questa tecnologia rendono apparentemente superfluo l'edge data center, uno sviluppo relativamente nuovo nel settore. Considerato che le connessioni 5G possono trasferire grandi quantità di dati a velocità così elevate e a bassa latenza, sembra inutile portare la capacità di calcolo più vicino al luogo in cui viene generata o dove si trova l'utente.

Questa impressione è, tuttavia, ingannevole. Per molte applicazioni esiste, infatti, una relazione quasi simbiotica tra il 5G e l'edge computing. Senza quest'ultimo il primo non sarebbe in grado di soddisfare le aspettative riposte in esso. I progressi di tecnologie come AI, ML, deep analytics, guida autonoma e AR/VR saranno possibili solo grazie alla connettività ad alta velocità combinata con l'elaborazione dei dati vicino all'utente finale. Consideriamo l'area critica della sicurezza della guida autonoma. Dopo tutto, i veicoli autonomi non devono solo "riconoscere" il loro ambiente, ma idealmente anche comunicare con gli altri veicoli e con i centri di controllo del traffico per essere pronti ad affrontare situazioni come code o punti pericolosi. Più brevi



sono i percorsi di trasmissione, più efficiente sarà lo scambio di dati.

L'esigenza di edge data center è inoltre rafforzata da un fenomeno noto anche nel settore della costruzione di strade con il termine "traffico indotto". Un noto professore tedesco esperto di pianificazione urbana e trasporti ha riassunto bene il concetto in poche parole: "Se si seminano strade, si raccoglie traffico". La maggior parte di noi ha familiarità con questo concetto nella vita di tutti i giorni. Se una strada viene allargata da due a quattro corsie, ad esempio, il flusso di traffico sarà inizialmente migliore, ma a medio termine aumenterà e, di conseguenza, scorrerà male come prima delle opere di allargamento. Lo stesso accadrà con il 5G. La rapida crescita del numero di utenti e applicazioni che si affidano a questa tecnologia farà sì che la larghezza di banda, che inizialmente sembra essere abbondante, diventi un bene scarso nel medio termine.

Per le applicazioni del futuro è quindi evidente la necessità di edge data center. Non tutti sono, tuttavia, entusiasti all'idea di averne un numero sempre maggiore in prossimità dei centri urbani e, per questo motivo, gli edge data center stanno cominciando a rappresentare un problema dal punto di vista della



pianificazione urbanistica. Esistono, fortunatamente, diverse possibili soluzioni.

Recupero o integrazione

Nelle città ci sono spesso spazi liberi. I grandi magazzini chiudono e i parcheggi multipiano non sono più indispensabili nei centri cittadini, a causa della riduzione del traffico a favore di un incentivo a utilizzare mezzi pubblici e biciclette. Spesso questi edifici possono essere convertiti in data center, consentendo così di non modificare il paesaggio urbano. Non sempre si tratta di edifici completi ma, poiché gli edge data center non hanno le dimensioni di quelli tradizionali, il piano di un ex edificio per uffici, ad esempio, è sufficiente in termini di spazio. Il recupero o l'integrazione in un immobile esistente presenta poi vantaggi dal punto di vista ambientale, in quanto riduce l'utilizzo di materiali ed energia.

Anche un nuovo edificio deve inserirsi in modo armonico nell'ambiente circostante. In termini di design, i data center in città non devono necessariamente basarsi sulle gigantesche strutture "greenfield". Piuttosto, possono essere progettati in modo da integrarsi nel paesaggio urbano esistente o addirittura arricchirlo.

I data center, poi, non godono della migliore reputazione, anche a causa del loro fabbisogno energetico ed è innegabile che hanno un impatto negativo sull'ambiente. Esistono diversi modi per far fronte a questa problematica, dalla fornitura di energia rinnovabile, all'utilizzo di server e sistemi di archiviazione a risparmio energetico, passando per il raffreddamento con aria esterna e l'utilizzo del calore residuo. Per progettare le parti esterne del data center in modo ecologicamente sostenibile, oltre agli interni, l'inverdimento della facciata è una componente essenziale. Questi giardini verticali contribuiscono ad abbassare la temperatura esterna – soprattutto in estate – e a ridurre la necessità di raffreddamento all'interno.

Infine, ma non meno importante, l'accettazione degli edge data center nei nostri centri urbani può essere promossa attraverso un'adeguata comunicazione che coinvolga le persone interessate. È importante spiegare i vantaggi e la necessità degli edge data center nel modo più chiaro possibile su tutti i canali e cercare il dialogo con la comunità locale. Per i cittadini sarà più semplice accettare la nuova potenza di calcolo nel loro quartiere.

I numeri della Piattaforma Digitale Nazionale Dati (PDND)

Arianna Perri, Research Analyst

TIG

La Piattaforma Digitale Nazionale Dati (PDND) è un'infrastruttura tecnologica promossa dal Dipartimento per la trasformazione digitale e realizzata da PagoPA S.p.A.. La piattaforma è attiva dal 21 ottobre 2022, con largo anticipo rispetto alle scadenze previste, e finanziata dai fondi PNRR con 556 milioni relativi alla misura 1.3.1.

Il suo obiettivo principale è facilitare lo scambio di informazioni tra le amministrazioni pubbliche italiane e tra queste e soggetti privati, utilizzando interfacce digitali chiamate e-service. La PDND è stata progettata al fine di rendere più semplici, sicuri ed efficienti i processi amministrativi, eliminando la necessità di fornire ripetutamente le stesse informazioni alla pubblica amministrazione, secondo il principio once-only. La piattaforma permette agli enti pubblici di operare sia come fornitori di servizi digitali (erogatori) sia come utenti degli stessi (fruitori).

Le prime due scadenze sono giunte al termine: entro il 30 settembre 2023 le pubbliche amministrazioni hanno dovuto accreditarsi alla PDND, sviluppato le interfacce di programmazione (API) e reso

disponibili le proprie basi dati sulla piattaforma, mentre entro il 31 marzo 2024 lo stesso hanno fatto i gestori di servizi pubblici. Prossima scadenza riguarda le società a controllo pubblico che dovranno adempiere entro il 30 settembre 2024.

Grazie al monitoraggio di PagoPA, che trasmette trimestralmente all'AgID l'elenco dei soggetti aderenti alla PDND, è possibile analizzare la crescita delle adesioni alla piattaforma. Nella pagina I numeri della PDND, in costante aggiornamento, sono contenuti tutti i progressi compiuti. Riportiamo

di seguito gli aggiornamenti al 26 giugno 2024:

- hanno aderito 6.732 enti, ossia +209 enti (+3,1%) rispetto al mese precedente;
- di questi, 6.621 sono Enti pubblici, che equivalgono a +206 Enti pubblici (+3,1%) e 111 enti privati rispetto al mese precedente;
- gli e-service pubblicati hanno raggiunto la soglia di 7.544, ossia +476 servizi (+6,7%) rispetto al mese precedente;
- sono state effettuate 8.094 connessioni totali, che



equivalgono a +620 connessioni (+8,3%) rispetto al mese precedente.

Negli ultimi 12 mesi, gli e-service più utilizzati, per enti fruitori attivi, sono stati:

- SEND – Servizio Notifiche Digitali con 3.735 richieste.
- INAD Consultazione dei Domicili Digitali con 410 richieste.

Stando sempre ai dati forniti da PagoPA, i Comuni sono gli enti erogatori che hanno pubblicato un maggior numero di e-service (7.183), seguiti dalle Pubbliche Amministrazioni Centrali (161) e dagli Enti Nazionali di Previdenza e Assistenza Sociale (127).

Fotografia 2023 dei progressi nella PA locale

Lo scorso anno, TIG – The Innovation Group ha condotto, in collaborazione con Gruppo Maggioli, l'indagine "2023, PA Digitale al punto di svolta", con lo scopo di monitorare il progresso delle iniziative digitali nella Pubblica Amministrazione locale, a cui hanno risposto 207 enti pubblici locali. Dalla ricerca è emerso che il 51% aveva già aderito alla PDND, mentre il 47% dichiarava che lo avrebbe fatto in futuro, del resto l'adesione sarebbe stata obbligatoria entro il mese di settembre 2023. Il 46% di coloro che avevano già adottato la PDND,

assumeva il ruolo sia di erogatore dei dati sia di fruitore. Nonostante la possibilità di scambiare dati con altre PA locali o centrali sia stata valutata dal 61% degli enti «molto» o «moltissimo» importante, solo il 9% affermava di essere «molto» o «moltissimo» avanzato in termini di interoperabilità.

Nell'indagine venivano poi indagati gli ostacoli e i facilitatori nell'utilizzo della PDND. Il punto di forza della piattaforma maggiormente condiviso dagli enti era la riduzione dei tempi di accesso alle informazioni, seguito dalla semplificazione dell'iter amministrativo. Il complesso processo di integrazione con altre piattaforme, invece, è risultato essere la principale criticità della piattaforma, seguito dagli eccessivi costi gestionali e di mantenimento dell'infrastruttura e le scarse linee guida sul formato dei dati da immettere.

In parte, alcuni di questi ostacoli sono stati ovviati, ma sembrano esserci nuovi impedimenti, tra cui la scarsa tempestività da parte degli enti erogatori nell'autorizzazione della richiesta di fruizione. Al fine di monitorare i progressi e le nuove sfide nel percorso verso la digitalizzazione della pubblica amministrazione, anche quest'anno TIG e Gruppo Maggioli stanno conducendo l'indagine "Transizione digitale nella PA locale 2024".

In conclusione, i dati forniti da PagoPA sono incoraggianti perché testimoniano una crescita sostenuta sia nel numero di enti aderenti sia nell'utilizzo dei servizi digitali offerti dalla PDND, a dimostrazione di un progresso costante nella digitalizzazione dei servizi pubblici in Italia.



Customer service: l'AI è un alleato ma deve avere un volto umano

Valentina Bernocco, Web and Content Editor

TIG

Nel servizio clienti è meglio trovarsi dall'altra parte dello schermo (o dell'app) un chatbot, pronto a rispondere in qualsiasi momento, oppure una persona? Le applicazioni di intelligenza artificiale nel customer service non sono qualcosa di nuovo, ma oggi si assiste a una transizione verso soluzioni più evolute, basate su large language model e su un più consapevole uso dei dati dei clienti. Le capacità linguistiche e interpretative dell'AI generativa consentono ai chatbot di nuova generazione di fornire risposte più complesse e contestualizzate, oltre che di dare supporto in più lingue (e addirittura nella lingua dei segni). E si tratta di tecnologie che possono anche notevolmente migliorare il servizio clienti, renderlo più puntuale, sempre disponibile e più personalizzato.

Tutto bello? In realtà tra i consumatori permangono scetticismi e resistenze nei confronti dell'AI utilizzata nel customer service. Uno studio di Gartner di nuova pubblicazione, condotto lo scorso dicembre su 5.728 consumatori, svela che il 64% preferisce interagire con persone reali quando richiede informazioni o supporto. Il 53% addirittura potrebbe considerare di rivolgersi alla concorrenza se scoprisse che l'azienda in questione usa l'AI per fornire assistenza.

Le aziende si ritrovano un po' schiacciate tra dinamiche opposte: da un lato, le perduranti

resistenze dei clienti nei confronti dell'AI, dall'altro la pressione ad adottare queste tecnologie per ottenere efficienze e risparmi. Citiamo per esempio l'annuale report "State of Service" di Salesforce: l'81% delle società di servizi pianifica di incrementare gli investimenti in intelligenza artificiale nel corso di quest'anno (in Italia la percentuale scende al 75%). "Il 60% dei leader del servizio e supporto clienti sentono la pressione di dover adottare l'AI nella propria funzione", ha osservato Keith McIntosh, senior principal, research della practice Customer Service & Support di Gartner. "Ma non possono ignorare le preoccupazioni circa l'uso dell'AI, specialmente quando potrebbero significare perdere clienti".

Le criticità emerse dal sondaggio di Gartner sono di vario tipo. Da un lato, molti temono che parlare con un addetto al servizio clienti sarà più difficoltoso e macchinoso se l'azienda in questione punta sulle chatbot. Inoltre, c'è una diffusa preoccupazione per i posti di lavoro che l'AI potrà "rubare" nell'ambito del servizio clienti. "Molti clienti", ha proseguito McIntosh, "temono che la GenAI diventerà semplicemente un ulteriore ostacolo tra loro e un agente. Spetta ai leader del servizio e supporto dimostrare ai clienti che l'AI può ottimizzare l'esperienza".



Le aziende, suggerisce Gartner, dovrebbero quindi lavorare per rafforzare la fiducia dei clienti nei confronti della GenAI. Come? Per esempio, tenendo sempre presente il famoso “customer journey”, cioè i percorsi e l’esperienza vissuti dal cliente. I chatbot dovrebbero dare accesso diretto agli agenti “umani”, comunicando questa possibilità agli utenti. Inoltre, gli agenti dovrebbero poter riprendere il filo del discorso direttamente da dove la conversazione tra utente e chatbot si era interrotta (senza quindi obbligare il cliente a ripetere la richiesta o a fornire dati ulteriori, perdendo tempo e pazienza).

Sarà banale sottolinearlo, perché è stato detto molte volte, ma il percorso di adozione dell’intelligenza artificiale dovrà compiersi tenendo conto delle logiche umane, relazionali, ancor prima di quelle

tecnologiche. Se questo vale per qualsiasi ambito, ancor più sarà decisivo nel servizio clienti e più in generale nelle relazioni tra aziende (o marchi) e consumatori, dove fiducia e rispecchiamento valoriale sono ancora – anzi, forse oggi più che mai – delle forze determinanti.

Le relazioni contano ancora, eccome, ma le persone pretendono anche risposte tempestive: in sintesi, un’efficienza che non deve sfociare nella spersonalizzazione. In base a una recente analisi di Infobip, pubblicata lo scorso aprile e basata su oltre 473 miliardi di interazioni digitali tra aziende e consumatori, i clienti si rivolgono sempre di più alla messaggistica per ottenere informazioni e supporto, oltre che per acquistare prodotti e servizi. Messaggistica significa innanzitutto Whatsapp,



“

L'89% degli addetti al customer service o customer support pensa che le aspettative dei clienti oggi siano più elevate che mai

strumento che nel 2023 ha registrato un incremento del 137% (rispetto al 2022) nel numero di interazioni tra consumatori e aziende. Stando ai dati di Infobip, crescono inoltre le interazioni conversazionali tramite le chat dei social media (+73% nel 2023) e di applicazioni (+63%).

“I nostri dati mostrano come le esperienze conversazionali si stiano rapidamente diffondendo in tutto il mondo con l'introduzione di casi d'uso per il marketing, le vendite e l'assistenza”, ha commentato Ivan Ostojic, chief business officer di Infobip. “Con l'emergere dell'AI interattiva, ci aspettiamo che i brand incorporino una serie di diversi chatbot e algoritmi di intelligenza artificiale che lavorano insieme per attivare azioni nei punti strategici del customer journey. Nel corso del prossimo anno, prevediamo un'adozione diffusa nel servizio clienti, nell'automazione del marketing e delle vendite e per casi d'uso operativi come la pianificazione delle consegne e la gestione dei pagamenti”.

Come emerso dal già citato report di Salesforce, l'89% degli addetti al customer service o customer support pensa che le aspettative dei clienti oggi siano più elevate che mai. Le persone si aspettano un servizio tempestivo, risolutivo e quindi efficace, ma anche personalizzato. Più di ogni altra cosa, i consumatori vorranno potersi fidare. L'intelligenza artificiale può far quadrare il cerchio per le aziende che ricercano tutto questo e contemporaneamente inseguono risparmi ed economie di scala. Tuttavia, l'AI è un oggetto da maneggiare con cura perché, come sappiamo, nel marketing la fiducia è il bene più prezioso, nonché il più facile da perdere e il più difficile da ricostruire.



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