SETTEMBRE 2022

IL CAFFÈ DIGITALE

THE INNOVATION GROUP NEWSLETTER

BLUE & GREEN: I GEMELLI DIVERSI DELLA TRASFORMAZIONE DELLE IMPRESE

QUESTO MESE ABBIAMO FATTO COLAZIONE CON...

Maria Teresa Basile, Head of IT, Telespazio

DIRITTO ICT IN PILLOLE

Cyber Resilience Act: l'Europa verso una sicurezza responsabile dei prodotti digitali

LA TRASFORMAZIONE DIGITALE

Metaverso, da buzzword a realtà concreta. Ma quando?

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

Loris FREZZATO
ICT Ecosystem

SOMMARIO

12

CYBERSEC E DINTORNI

Zero Trust, come evolve l'architettura di cybersecurity

Elena Vaciago

15

LA TRASFORMAZIONE DIGITALE

Metaverso, da buzzword a realtà concreta. Ma quando?

Roberto Bonino

17

WOMEN IN TECH

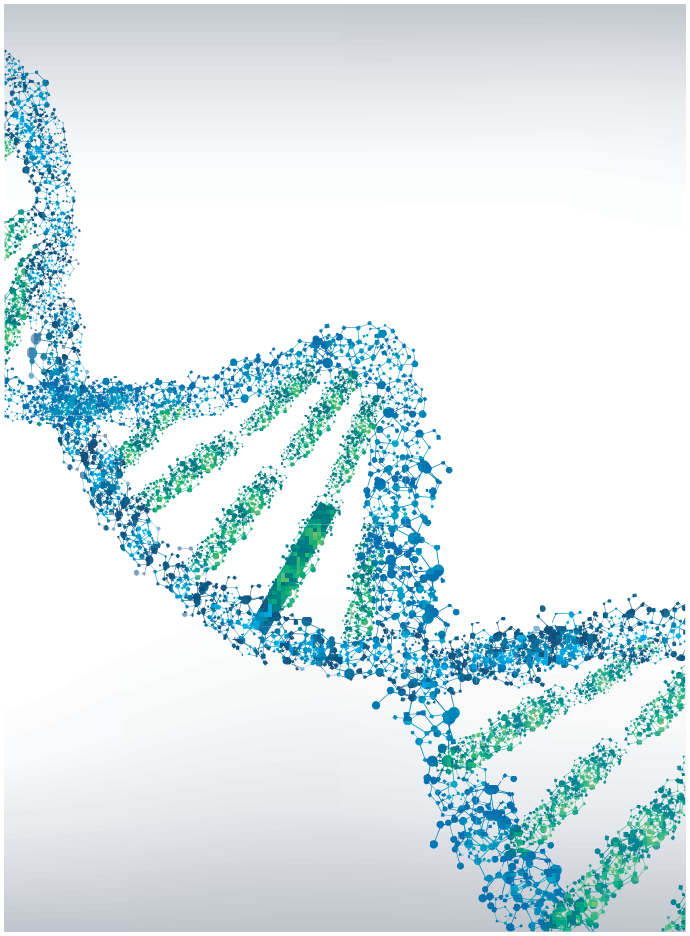
La certificazione di genere fa bene ai dipendenti e anche all'azienda

Valentina Bernocco

Blue & Green: i gemelli diversi della trasformazione delle imprese

Ezio Viola, Co-Fondatore

The Innovation Group



Stiamo vivendo come cittadini ed imprese un periodo di profonda incertezza legata a quanto potrebbero essere pesanti sulla situazione economica e sociale gli impatti di inflazione, crisi energetica e guerra in Ucraina. Ciò sta mettendo seriamente alla prova la coesione delle politiche dei vari Paesi Europei nel trovare una strategia comune ed efficace per affrontare la crisi energetica così come fatto per la Pandemia 2 anni fa. I provvedimenti adottati dall'Unione Europea nell'ambito della transizione ecologica sono numerosi e hanno finalità differenti: il principale provvedimento è il "New Green Deal" varato per fare dell'Europa il primo continente a impatto climatico zero entro il 2050, all'interno del quale è stato approvato il Piano "Fit for 55" che ha come principale finalità una riduzione delle emissioni di gas che possono alterare il clima di almeno il 55% già entro il 2030.

Sono obiettivi sfidanti che hanno già scatenato molte resistenze anche nel nostro Paese sui tempi di realizzazione e sui potenziali impatti in alcuni settori quali i trasporti e l'automotive. La situazione di crisi energetica attuale sta creando preoccupazioni e urgenze, senz'altro comprensibili, che potrebbero seriamente rallentare le tappe del percorso verso un'economia globale sostenibile: uno scenario che, qualora dovesse verificarsi, secondo l'IPCC provocherebbe danni irreversibili per la società, inclusi quelli relativi a infrastrutture e insediamenti costieri.

La Commissione Europea ha richiesto a tutti i Paesi membri dell'Unione Europea di prevedere all'interno dei singoli Piani Nazionali dei requisiti minimi di spesa per la transizione verde e per la transizione digitale (pari rispettivamente al 37% e 20% dei fondi destinati a ciascun Paese) e di realizzare progetti in aree di intervento segnalate come particolarmente importanti (per esempio, efficienza energetica degli edifici o trasporto sostenibile).

Nello specifico, la Missione 2 del PNRR in Italia ha destinato 59,46 miliardi di euro (a fronte dei 191,5 miliardi totali previsti dal Piano) per la costruzione di un'economia sostenibile dal punto di vista ambientale, distribuiti nelle quattro componenti: agricoltura sostenibile ed economia

circolare, energia rinnovabile, idrogeno, rete e mobilità sostenibile, efficienza energetica e riqualificazione degli edifici, tutela del territorio e della risorsa idrica.

Come agevolare la lotta al cambiamento climatico e velocizzare il percorso verso la Net Zero society in un momento in cui lo scenario geopolitico e le necessità dei singoli Paesi e Governi sono una minaccia per la transizione green? Alcune risposte possono arrivare sia dall'innovazione tecnologica per il settore dell'energia (in particolare per le rinnovabili e per le soluzioni di decarbonizzazione) sia dall'utilizzo innovativo delle tecnologie digitali. L'innovazione tecnologica e il digitale hanno un impatto pervasivo, cross-industry, con la capacità di efficientare i processi (sia intra-organizzativi sia inter-organizzativi) attraverso la connessione e integrazione delle filiere produttive e con la creazione di nuovi ecosistemi digitali che abilitano la sostenibilità ambientale.

Il digitale rappresenta un importante fattore critico per consentire un nuovo livello di decarbonizzazione sistemica e per accelerare il passaggio da un utilizzo lineare delle risorse a un modello circolare. Le tecnologie digitali possono giocare un ruolo chiave per il raggiungimento della neutralità climatica, la riduzione dell'inquinamento e il recupero della biodiversità. In particolare, l'utilizzo di piattaforme tecnologiche che agevolano l'utilizzo di dati e l'automazione, permettono un consumo più efficiente delle risorse e una migliore flessibilità dei sistemi e delle infrastrutture di comunicazione. L'uso dell'Intelligenza Artificiale per la misura e la riduzione delle emissioni inquinanti offre diverse opportunità per mitigare il rischio climatico, misurare l'impatto ambientale, aumentare la resilienza verso eventi catastrofici e modelli avanzati previsionali.

Quale potrebbe essere l'effettivo contributo del digitale alla realizzazione degli obiettivi climatici è ancora difficile da misurare e alcune stime indicano che il digitale sarà responsabile dell'abbattimento delle emissioni in misura pari al 53,2%: il 17,8% per effetto diretto (emissioni evitate direttamente grazie all'uso del digitale) e per il 46,8% per via indiretta, mentre il restante 46,8% di riduzione delle emissioni sarà funzione di tecnologie non digitali.

Il movimento verso la transizione net-zero è un fenomeno strutturale accelerato dalla pandemia che riflette un grande mutamento socioeconomico e culturale, che sempre più è andato affermandosi negli ultimi. Ciò si è tradotto in un cambiamento delle esigenze e degli interessi di cittadini e consumatori, a cui ci si è dovuti necessariamente adeguare e che le aziende devono tenere in considerazione costruendo una propria strategia net-zero. Da una ricerca svolta da TIG che sarà presentata nel **Rapporto annuale DIGITAL ITALY 2022** risulta che per le aziende italiane la transizione green non è più un'opzione. Essa sta diventando una necessità, non solo derivante da normative presenti o future, e sta diventando parte della loro strategia di innovazione per migliorare la reputazione del brand, per innovare o differenziare la propria offerta per l'ampiamento delle opportunità e il miglioramento dei rapporti con gli stakeholder.

Un altro aspetto importante che sarà toccato durante i lavori del Digital Italy Summit (Roma, 17 – 18 – 19 ottobre) all'interno del BLUE & GREEN TRANSITION SUMMIT (Roma 18 ottobre) dedicato a tutti questi temi, è come il digitale e in generale il settore ICT stesso devono perseguire la transizione ecologica. Le fonti di energia rinnovabili saranno importanti anche per il consumo di energia del settore digitale a partire dai data center e delle grandi infrastrutture per il cloud e delle reti di comunicazione. Questo settore è responsabile, secondo diverse stime, di una quota compresa tra il 5% e il 9% del consumo globale di elettricità e di circa il 3% o 4% delle emissioni di gas-serra. La transizione green del settore digitale deve riguardare non solo l'offerta ma anche la domanda degli utenti del digitale, su come utilizzano device e tecnologie poiché il consumo di energia legato a queste ultime dovrebbe essere improntato a pratiche di utilizzo più sostenibili, a partire dalla consapevolezza che il digitale non è energy-free. Avere un IT sostenibile dovrà diventare un obiettivo e una pratica fondamentale nelle strategie ICT di molte aziende e riguarderà le scelte tecnologiche, architetturali e processi di governance che toccano il rapporto tra IT, utenti e principali fornitori.

Oltre al digitale il fattore che sta accelerando la transizione ecologica nelle aziende è la finanza. I fattori ESG (Enviromental, Social e Governance) stanno diventando un driver per gli investimenti nel mercato dei capitali e costituiscono degli elementi discriminanti dell'attività creditizia da parte delle banche verso la maggior parte dei settori di attività economica. Le attività dell'azienda sono considerate sostenibili sempre di più non solo da un punto di vista economico, ma anche ambientale e sociale e rappresentano fattori sempre più rilevanti nelle decisioni di investimento.

Comunque la si guardi, che si tratti di un processo di trasformazione aziendale o di una forma di investimento, la sostenibilità necessita di tempo. In quanto sostenibilità e innovazione digitale portano entrambe una profonda trasformazione a livello di produzione, di innovazione nei processi e dei modelli di business nella gestione delle risorse e nella richiesta di nuove competenze.

Non è più possibile guardare "solo" all' innovazione sostenibile e /o all' innovazione digitale, ma occorre vederle come due trasformazioni "gemelle" che anche quando partono in modo indipendente sono destinate a convergere e a intrecciarsi tra loro.

Maria Teresa Basile, Head of It di Telespazio

Doveroso ma meditato il passaggio al cloud per Telespazio

Roberto Bonino, Research and Content Manager
The Innovation Group

La migrazione al cloud è da diverso tempo al centro dei processi di evoluzione tecnologica e strategica delle aziende. Infrastrutture, applicazioni e dati sono coinvolti a differente titolo e molte scelte, dalla prioritizzazione delle attività alla scelta dei provider di riferimento, possono dipendere da fattori e mindset ancora in grado di condizionarne l'attuabilità o la velocità di esecuzione.

I responsabili It devono tener conto di spinte ed esigenze non sempre allineate già all'interno dell'azienda, fra chi mette davanti a tutto la necessità della business continuity a tutti i costi e chi, proprio sul fronte tecnologico, deve far fronte anche alle problematiche di sicurezza. Il mondo sembra andare in una direzione ben definita, talvolta imponendo la propria legge a chiunque, ma non tutti i dubbi appaiono fugati e non tutti i dilemmi risolti.

Abbiamo provato ad analizzare la realtà di un soggetto molto particolare, come Telespazio, joint venture fra Leonardo e Thales, da sessant'anni impegnata nello sviluppo di soluzioni e servizi satellitari e per questo abbiamo incontrato la Head of It Maria Teresa Basile.

Quali tipologie di workload e relativi dati avete già portato in cloud e quali esigenze si celano dietro questa scelta?

Ci sono diversi elementi che concorrono a determinare le nostre scelte. Da un lato, stiamo certamente procedendo nella digitalizzazione dei processi aziendali e in vari casi le migliori soluzioni individuate sono cloud-native, quindi il passaggio diventa inevitabile. Tuttavia, tra le nostre line of business c'è la vendita di immagini satellitari che dopo il download, sottopone i dati a processi di post elaborazione anche impiegando forme di AI, come il machine learning, sulla base delle richieste dei clienti,: in questi casi vengono richieste risorse computazionali o di storage decisamente consistenti, che ha decisamente più senso gestire in una logica a consumo. Naturalmente, anche noi abbiamo l'esigenza di ottimizzare le risorse e i processi, per cui diventa conveniente centralizzare attività come backup, aggiornamenti, patching e gestione della security, in questo caso su cloud privato, ma non mancano situazioni in cui è il nostro cliente a chiederci l'erogazione di servizi in cloud, presso il suo provider di riferimento. Insomma, lo scenario è variegato, ma la direzione appare comunque ben delineata.

Come vi siete orientati per supportare da un lato l'attività di test & sviluppo e dall'altro il disaster recovery?

Già prima della pandemia abbiamo messo a fattor comune una serie di risorse aziendali, con particolare riferimento alla virtualizzazione, per cui abbiamo realizzato all'interno dell'azienda un cloud privato, destinato in modo particolare a chi si occupa di test e sviluppo di applicazioni, soprattutto

se orientate al business. Storicamente, poi, la nostra azienda si è sempre preoccupata sia della continuità del business che del disaster recovery, per cui la nostra infrastruttura è distribuita geograficamente, così come lo sono le nostre sedi sia in Italia che all'estero. La scelta del cloud privato ci ha consentito più agevolmente di aggiornare processi che esistono da oltre un decennio.

Abbiamo compreso quanto sia importante coinvolgere tutte le figure implicate in un processo, per cui vediamo dall'inizio di identificare un "cloud board" con le figure It, business, security e data protection, per analizzare ogni situazione, capire quali tipologie di dati siano coinvolte e fare una scelta orientata verso il provider più adatto

Quella del private cloud è una scelta univoca o siete flessibili rispetto ai differenti modelli disponibili oggi?

Sul cloud non si può fare una scelta unidirezionale, perché dipende dal tipo di soluzione, dai dati sottesi, dai vincoli del vendor e da altri fattori. Per questo, lavoriamo anche con infrastrutture di cloud pubblico, così come l'attenzione sul tema della protezione dei dati ci porta in alcuni ambiti a mantenere rigidamente i dati in casa, demandando al cloud solo l'implementazione delle policy. Con il tempo, abbiamo compreso quanto sia importante coinvolgere tutte le figure implicate in un processo, per cui tutte le volte che ci troviamo a dover fare una scelta non scontata vediamo dall'inizio di identificare un "cloud board" con le figure It, business, security e data protection, per analizzare ogni situazione , capire quali tipologie di dati siano coinvolte e fare una scelta orientata verso il provider più adatto anche in base alle politiche di sicurezza proposte e alla concreta possibilità di poterne verificare l'attuazione.

Al di là degli aspetti tecnologici, dove ritenete di dover lavorare per migliorare il livello di protezione dei vostri workload e dati, pensando al mindset aziendale nel suo complesso, alla sensibilizzazione delle persone o a una visione che ancora deve consolidarsi a livello It?

Dal punto di vista it, abbiamo registrato una fase di cambiamento che ci ha portati a evolvere da coloro che eseguono operativamente determinati processi a coloro che si occupano più della configurazione iniziale e del monitoraggio di quello che accade. Le professionalità su questo fronte stanno cambiando: fra qualche anno forse faremo fatica a reperire persone in grado di fare il patching, ma ce ne saranno di bravissime a interagire con i cockpit che i cloud provider mettono a disposizione per comprendere il processo di patching che saranno loro ad aver eseguito. Il mindset aziendale, invece, è certamente cresciuto anche grazie all'effetto della pandemia e alla generalizzazione di alcune prassi di accesso e utilizzo di strumenti prima meno considerati, facendo scoprire anche agli utenti meno digitalizzati modalità di utilizzo delle soluzioni in precedenza sconosciute.

Open Banking, ovvero, Open Innovation nel settore finanziario

Elena Vaciago, Associate Research Manager
The Innovation Group

Nato tre anni fa con l'entrata in vigore (il 14 settembre 2019) della PSD2, la direttiva europea che ha rivoluzionato il mondo dei pagamenti e dei servizi finanziari, l'Open Banking italiano si sviluppa grazie alla condivisione di dati tra gli attori del panorama bancario. È un cambiamento che presto ci riguarderà tutti, perché porterà a grandi novità nel gestire i risparmi, accedere a nuovi servizi finanziari, spendere i soldi. Oggi gli attori bancari sono obbligati a condividere (tramite le cosiddette API) alcune informazioni su conti e pagamenti dei propri clienti, se autorizzati dagli stessi. Questo cambia molte logiche competitive, favorisce l'innovazione collaborativa nel mondo finanziario e apre la strada alle Fintech. Come procede l'evoluzione dell'Italia verso l'Open Banking?

Lo scenario italiano ed europeo dell'Open Banking

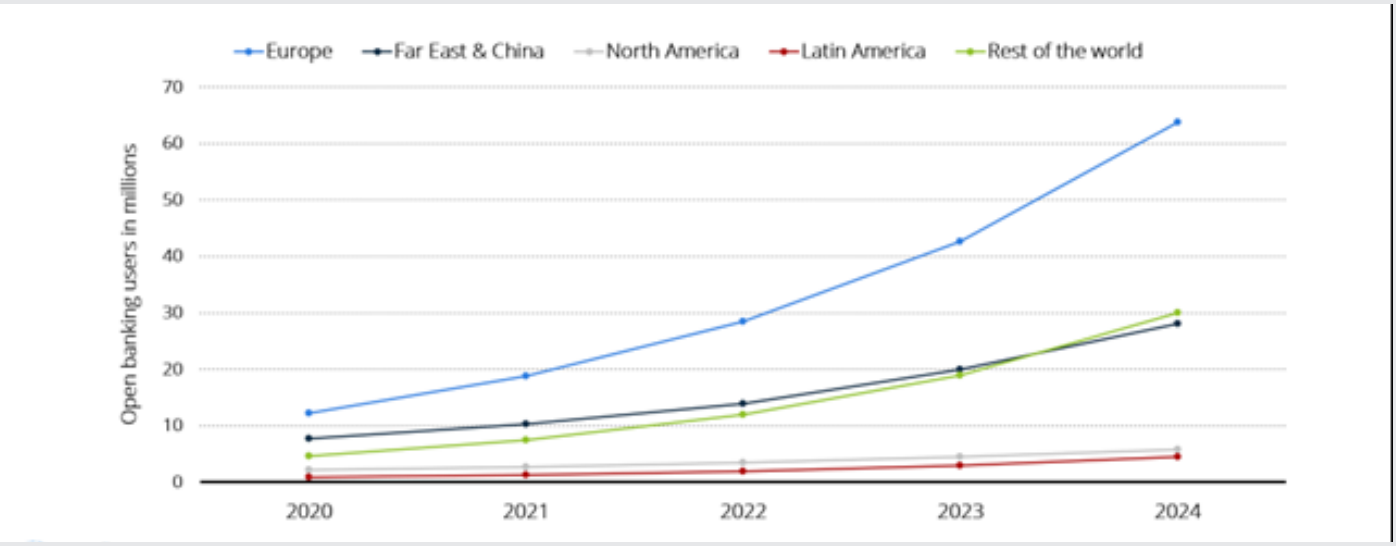
Un **report di Cbi e PwC Italia** ha descritto a inizio 2022 quali erano i livelli di diffusione raggiunti da Open Banking e Open Finance in Italia. Dall'analisi emerge una crescita in Italia, anche se l'adozione è ancora distante dai livelli di altre Paesi europei, soprattutto del Nord Europa.

Secondo il rapporto, l'Open Banking è oggi una tendenza importante: vi partecipano gli operatori bancari e finanziari di oltre 60 paesi nel mondo, che hanno dato vita a numerose iniziative. Se l'adozione della PSD2 ha dato il via al fenomeno, alimentando una maggiore competizione dei servizi finanziari e favorendo l'ingresso a nuovi player, alcuni numeri ne dimostrano oggi il dinamismo.

Abbiamo infatti a livello globale oltre ai 4.000 Accounting Servicing Payment Service Provider (ASPSP) ed anche un numero crescente di Third-Party Provider (es. IP/IMEL che offrono servizi di Account Information e Payment Initiation): se ne contano infatti circa 500 (quindi una crescita a tripla cifra rispetto al 2019, +300%). In aggiunta, le acquisizioni in ambito Open Banking (es. Mastercard-Aiia) del 2021, hanno raggiunto circa i due miliardi di euro di valore complessivo.

Anche secondo un'indagine di **Juniper Research**, l'Europa sarà il primo mercato mondiale per numero di utenti di servizi Open Banking nei prossimi anni. Gli utenti cresceranno a un tasso medio annuo di quasi il 50% tra il 2020 e il 2024, passando dai 24,7 milioni gli individui in tutto il mondo

Numero di utenti dell'Open Banking nel mondo, dal 2020 al 2024, per area geografica ***(milioni)***



Fonte: Juniper Research, marzo 2021

del 2020 a 132,2 milioni entro il 2024, con l'Europa al primo posto (passerà da 12,2 milioni di utenti a 63,8 milioni di utenti).

Con riferimento all'offerta di servizi basati su API, un'analisi specifica condotta su 41 operatori di mercato ha rilevato che, su un totale di 2.400 API, il 63% si basa su dati PSD2 relativi ad Account Information (AIS) e Payment Initiation (PIS). In misura inferiore (14%), cominciano ad emergere servizi basati su investimenti, prestiti o dati assicurativi.

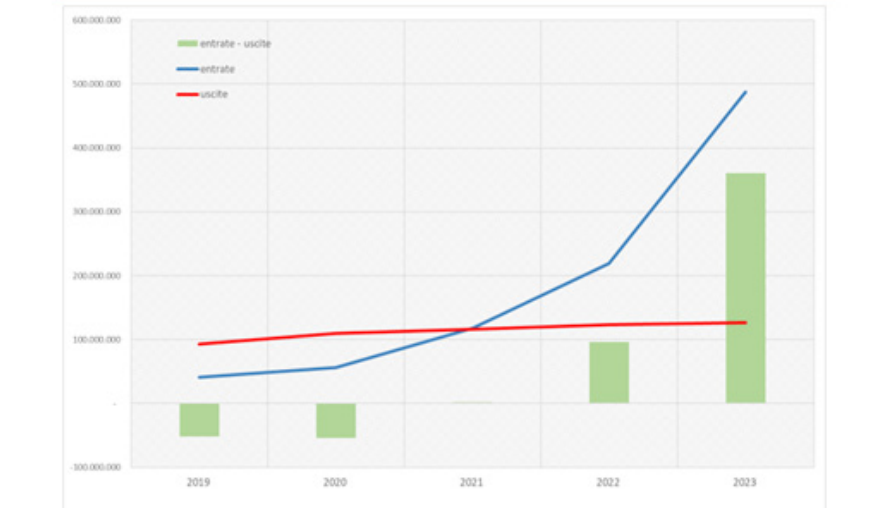
In Italia però lo sviluppo dell'Open Banking è inferiore rispetto ad altre aree europee. Analizzando le principali banche italiane, i servizi che compongono l'offerta al momento sono:

- Account Aggregation (55%),
- Check IBAN (45%),
- Personal Financial Management (36%),
- Instant Payment (27%)
- Digital Identity & Digital Onboarding (18%).

Inoltre, si contano 13 terze parti attive e gli utenti finali che utilizzano questi servizi sono meno del 5% del totale. Per il futuro, i servizi di Digital ID & Onboarding (64%) e Check IBAN (55%) sono i VAS su cui le banche dichiarano di voler puntare maggiormente. La survey ha inoltre evidenziato che nell'ultimo biennio è cresciuto il numero di istituzioni finanziare che ha investito più di 1,2M€ per lo sviluppo di servizi commerciali Open Banking (22% nel 2019 vs. 27% nel 2021): un trend che dimostra la volontà degli operatori a investire nel settore.

Secondo la terza **Indagine Fintech di Banca d'Italia** di novembre 2021, più di un quarto dei progetti Fintech delle banche italiane presuppone lo sviluppo di attività che ricadono nel perimetro dell'Open Banking. Inoltre, secondo Banca d'Italia, dal 2022 l'Open Banking porterà profitti (vedi la figura successiva). Questi progetti, nel biennio 2019-2020, hanno generato flussi di cassa in uscita e in entrata rispettivamente pari a 202 e 97 milioni; a partire dal 2021, a fronte di un profilo degli investimenti relativamente costante, è attesa una sensibile accelerazione dei flussi in entrata.

Flussi di cassa generati dai progetti di Open Banking *(euro)*



Fonte: Indagine Fintech di Banca d'Italia, novembre 2021

Open Banking e ruolo della Customer Experience

Il rapporto con gli utenti finali è indicato come una leva fondamentale per la crescita dei servizi di Open Banking. Serve incremento dell'awareness, sicuramente, ma anche una nuova Customer Experience, basata su interfacce innovative, dedicate alle terze parti e messe a disposizione dalle banche, nell'ambito di iniziative win win di collaborazione e innovazione.

L'esperienza utente dovrà quindi essere posta al centro per il successo di queste innovazioni. Se oggi i consumatori sono abituati a interagire con gli operatori bancari e finanziari attraverso una moltitudine di canali (fisici o digitali), l'obiettivo ultimo sarà quello di un'esperienza completa e continuativa, supportata da un ecosistema di player con origine e competenze diversificate.

Secondo il rapporto di Banca d'Italia, gli ambiti in cui vedremo i maggiori miglioramenti della CX saranno: l'informativa precontrattuale, contrattuale e periodica, le fasi della gestione dei reclami e della chiusura anticipata del rapporto. La dematerializzazione della documentazione consentirà alla clientela di consultare più facilmente le informazioni rilevanti relative al prodotto acquistato. L'utilizzo della firma digitale (già iniziato, sarà esteso sempre più) permetterà di velocizzare il processo di sottoscrizione dei contratti e abiliterà l'acquisto dei servizi anche in mobilità. Inoltre, sarà possibile semplificare l'acquisto dei servizi mediante strumenti di assistenza automatica durante la compilazione delle richieste di sottoscrizione. Processi di onboarding celeri e fluidi porteranno ad auspicabili miglioramenti della customer experience, senza pregiudicare l'adeguata conoscenza delle caratteristiche e delle condizioni del servizio acquistato.

Le sfide dell'Open Banking

Se da un lato le prospettive di crescita per il settore sono molto buone, non andranno sottovalutati alcuni punti critici che possono frenare questi sviluppi.

Da un lato, non va dimenticato che si tratta di gestire progetti complessi, nei quali intervengono più attori, più figure con ruoli e competenze diversificate. Progetti quindi molto delicati e difficili da portare a buon fine. Dal punto di vista tecnologico, un aiuto viene dalla capacità di garantire l'interoperabilità delle piattaforme incluse nel progetto.

La cybersecurity e la data protection saranno poi temi centrali. Sappiamo bene quanto banche e attori finanziari siano quotidianamente presi di mira dagli hacker: l'Open Finance, col passaggio di dati da un sistema ad un altro, potrebbe aprire la porta ai cyber criminali e amplificare questi rischi. Serviranno quindi solide soluzioni di cybersecurity e competenze avanzate a tutti i livelli (dal mantenimento delle infrastrutture ai nuovi sviluppi, alle stesse API) per realizzare ambienti allo stato dell'arte della sicurezza.

Andrà infine mantenuta attentamente la conformità alle norme generali che regolano questo mercato, per evitare che, se uno dei soggetti non riesce a rispettare queste norme, l'intero ecosistema collaborativo del progetto di Open Finance sia esposto al rischio di danni finanziari e reputazionali.

Cyber Resilience Act: l'Europa verso una sicurezza responsabile dei prodotti digitali

Valentina Frediani, General Manager

Colin & Partners

L'Unione Europea ha presentato nuove regole per la sicurezza di tutti i prodotti connessi a Internet che vengano prodotti e venduti all'interno dell'UE. Il Cyber Resilience Act – che attende ora di terminare l'iter di approvazione – vuole creare un equilibrio di mercato che responsabilizzi i produttori da un lato e rassicuri imprese e consumatori nei propri diritti. Un miglioramento in termini di fiducia e trasparenza, attenzione alla sicurezza, alla privacy e alla protezione dei dati è quanto auspica questo intervento regolatorio.

Il Cyber Resilience Act, che sarà vincolante entro due anni dalla sua approvazione, mira inoltre a diventare un punto di riferimento anche al di fuori dei confini europei, sui mercati globali. La cybersecurity dei prodotti a contenuto digitale, connessi direttamente o indirettamente a dispositivi o a una rete, è di fatto una priorità sentita in tutto il mondo. I costi dei cyber attacchi hanno superato, nel mondo, i 5 trilioni nel 2021.

In un presente in cui applicazioni hardware, software, prodotti wireless, sviluppo IoT e strumenti ad alto contenuto tecnologico – basati sulle reti – sono sempre più presenti, la sicurezza diviene l'unico pilastro in grado di consentire uno sviluppo futuro del mercato digitale europeo e non solo. Essa deve essere parte integrante dell'intera filiera, una "sicurezza by-design", sul modello già adottato dal GDPR per la privacy, che introduce requisiti obbligatori per i prodotti a contenuto digitale, durante l'intero ciclo di vita.

Per alcune tipologie (dispositivi medici, automobili, aviazione) esistono già norme vincolanti sotto questo profilo, per tutti gli altri produttori il primo step – a un anno dall'approvazione – sarà quello di dover segnalare vulnerabilità o incidenti, come avviene in materia di dati personali con il data breach.

Il nuovo Cyber Resilience Act si integrerà, quindi, nella più ampia visione strategica di Cyber security da tempo perseguita dall'UE, che ha portano alle direttive NIS e NIS 2.

Cosa significa per i produttori?

È indubbio che essi avranno maggiori responsabilità, sarà fatto obbligo, ad esempio, di fornire supporto sul tema sicurezza nonché provvedere agli aggiornamenti

necessari per ovviare ad eventuali vulnerabilità che vengano identificate durante l'intero ciclo di vita del prodotto. Una sorta di marchio CE sui prodotti digitali e connessi che sia a garanzia e tutela di consumatori consumer, realtà business e PA.

Torna, anche sul fronte sicurezza e non solo data protection, il tema della compliance. Anche in questo caso la linea tracciata ripercorre la medesima logica introdotta dal GDPR. Non è più sufficiente correre ai ripari in caso di attacco, quello che serve è una progettazione, a monte, che ruoti intorno ai principi di sicurezza e tutela, nel lungo periodo.

Cosa conterrà il nuovo regolamento?

La stessa Commissione europea riassume in questo modo i contenuti:

(a) norme per l'immissione sul mercato di prodotti con elementi digitali per garantirne la sicurezza informatica;
(b) i requisiti essenziali per la progettazione, lo sviluppo e la produzione di prodotti con elementi digitali e gli obblighi per gli operatori economici in relazione a tali prodotti;
(c) requisiti essenziali per i processi di gestione della vulnerabilità messi in atto dai fabbricanti per garantire la cybersicurezza dei prodotti con elementi digitali durante l'intero ciclo di vita e obblighi per gli operatori economici in relazione a tali processi. I produttori dovranno inoltre segnalare vulnerabilità e incidenti sfruttati attivamente;
(d) norme sulla vigilanza del mercato e sull'esecuzione.

Cosa accade alle aziende che non si adegueranno?

Abbiamo già visto come – a legge approvata – i tempi saranno di un anno per creare flussi organizzativi che permettano di rendere note le vulnerabilità che hanno portato a incidenti accaduti e anni per ridefinire i propri processi in ottica security by design.

L'impianto sanzionatorio per ora previsto, salvo modifiche successive, sottolinea l'urgenza che l'UE avverte sul tema sicurezza.

In caso di non conformità, le autorità di vigilanza del mercato potranno agire in modi diversi a seconda, si intuisce, della gravità dell'inadeguatezza. Si va dall'obbligo, per l'operatore, di porre fine alla non conformità eliminando quindi il rischio, alla limitazione della messa a disposizione sul mercato del prodotto / servizio, fino al suo ritiro completo. Negli ultimi due casi non occorre sottolineare il danno materiale e reputazionale al quale l'operatore andrebbe incontro.

Alle autorità nazionali spetterà, inoltre, comminare sanzioni amministrative che potranno raggiungere i 15 milioni di euro o fino al 2,5% del fatturato globale.

Si tratta di un intervento, potenzialmente dirompente che, pur introducendo nuovi obblighi restrittivi, sarà una ulteriore occasione per le imprese produttrici di ripensare i processi di filiera e di armonizzarli con altre normative (come la privacy) che già hanno dato, in molte realtà, un impulso positivo in termini di consapevolezza e crescita.

Zero Trust, come evolve l'architettura di cybersecurity

Elena Vaciago, Associate Research Manager

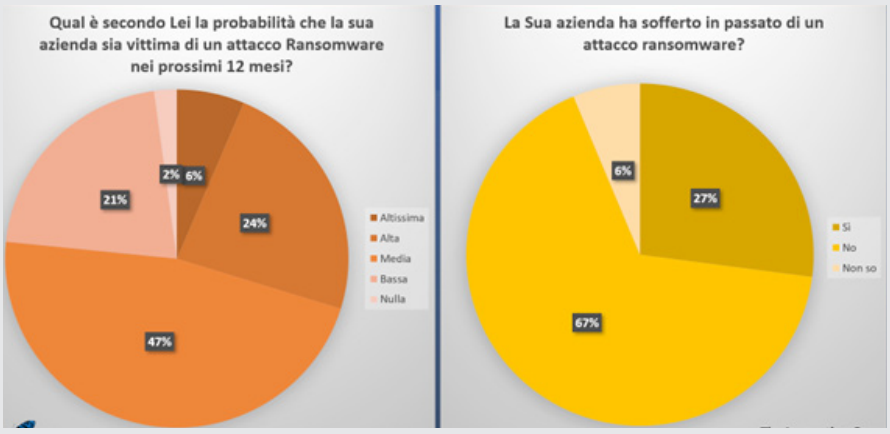
The Innovation Group

Gli attacchi informatici continuano a modificarsi e a crescere in volume. Le aziende sono impegnate nel migliorare costantemente la propria postura di sicurezza, gli investimenti in servizi e prodotti di cybersecurity crescono, ma i rischi di subire un attacco informatico grave come un ransomware rimangono.

Oggi non c'è in pratica nessuna realtà che possa dirsi del tutto immune dai rischi cyber. Durante la pandemia, il ricorso maggiore allo smart working ha ampliato la superfice d'attacco, aprendo agli hacker nuove porte per portare a termine i propri attacchi. Allo stesso tempo, gli attacchi sono aumentati numericamente, e hanno preso di mira servizi critici come quelli sanitari, che durante il periodo del Covid19 hanno dovuto sostenere gravi malfunzionamenti. Nell'ultimo periodo invece sono aumentati i tentativi contro gli operatori del mondo energy, probabilmente come conseguenza della situazione geopolitica che si è creata con il conflitto russo ucraino.

Secondo la "Cyber Risk Management 2022 survey" di TIG, dello scorso febbraio 2022, la probabilità di incorrere in un ransomware è oggi "Alta o Altissima" per il 28% delle aziende, "Media" per il 48%, "Bassa o Nulla" per il 24%. Con riferimento a chi afferma di aver già sofferto in passato per un evento di questo genere (il 26% dei rispondenti, un'azienda su 4) si tratta di realtà dei diversi settori e di diversa dimensione.

RAMSONWARE



Fonte: The innovation Group, Cyber Risk Management 2022 Survey, Febbraio 2022

Mitigare i rischi di cybersecurity significa stare continuamente al passo con i tempi e conoscere l'evoluzione delle minacce, che sono sempre più sofisticate. La pandemia ha forzato cambiamenti accelerati del modo di lavorare, la digitalizzazione è diventata più diffusa, sono aumentati gli oggetti connessi e gli attaccanti hanno naturalmente puntato a trarre vantaggio dalla nuova situazione.

Poiché oggi le infrastrutture da proteggere sono ibride e multicloud, via via che le aziende si espandono si accorciano le distanze con clienti e partner, si crea un ecosistema fluido in cui ciascuno ha il compito di contribuire a una resilienza di sistema. Sta quindi crescendo la consapevolezza che è necessario ripensare il modello utilizzato finora per la protezione di risorse e dati, visto che la sicurezza tradizionale su cui in tanto hanno investito non è risultata sufficientemente efficace.

Un tema al centro dei nuovi modelli di cybersecurity è Zero Trust. Questa metodologia, nota già da una decina d'anni, prevede che, ogni volta qualcuno o qualcosa abbia accesso a una rete, senza prova contraria e senza una verifica, non sia considerato affidabile. In un mondo in cui il perimetro di sicurezza ha perso senso, ogni transazione deve essere autenticata prima di potersi concretizzare. Per le aziende, in un contesto in cui la superfice attaccabile continua a crescere e le risorse critiche sono sempre più esposte, è fondamentale proteggersi meglio e non "accordare fiducia" (avere "Zero Fiducia") evitando di lasciare aperti gli accessi a utenti che hanno privilegi superiori a quelli richiesti, ai fornitori della supply chain, a terze parti che accedono ai sistemi aziendali, a device non gestiti che si collegano alla rete.

Il cambio di mindset porta con sé l'adozione di una serie di principi che guidano lo sviluppo dell'architettura di sicurezza (ZTA, Zero Trust Architecture). Una corretta progettazione punta quindi alla realizzazione di ambienti semplici e modulari per il controllo e la gestione degli accessi. La semplificazione dello stack di sicurezza può eliminare alcuni tradizionali problemi di gestione, ridurre significativamente il sovraccarico operativo e aiutare a scalare fino a decine di migliaia di utenti o di device che si collegano alle reti. Allo stesso modo, l'onboarding di dipendenti, terze parti, cloud provider e IT Supply chain, potrà diventare più efficiente, flessibile, reattivo e sicuro.

Come mostrano i risultati della "Zero Trust 2022 Survey" di The Innovation Group, condotta a giugno 2022 su un campione di 40 imprese italiane di grandi dimensioni (composto per l'80% da aziende con oltre 500 addetti), l'interesse per i principi Zero Trust (ZT in seguito) è costantemente cresciuto negli ultimi anni e ora si comincia a vederne l'effettiva applicazione. Secondo la survey, le aziende sono oggi in una fase di implementazione iniziale (46% delle risposte) o parziale (37% delle risposte) del modello, con un percorso di adozione che avverrà inevitabilmente per step successivi.

Nessuno ha implementato ZT in toto: il motivo è che un progetto di questo genere presenta complessità elevate. Alcuni poi rispondono che ancora non ci stanno pensando (17% delle risposte), ma nessuno ritiene che ZT non possa essere applicato alla sua realtà, confermando così l'interesse universale per questi principi.

Avanzamento della strategia Zero Trust in azienda

Fonte: The innovation Group, Zero Trusty 2022 Survey, Giugno 2022

Per rimanere competitive, le aziende sanno che padroneggiare i temi della Cybersecurity non è più un'opzione. L'adozione di ZT sta quindi crescendo, grazie a vantaggi come: la maggiore sicurezza attraverso tutta la superfice digitale attaccabile (es. cloud), l'accesso sicuro alle applicazioni fuori dal network, il maggiore controllo sugli accessi e la visibilità incrementata, la maggiore business agility e la minore complessità di gestione della sicurezza, la possibilità di assicurare una scalabilità futura dell'architettura di sicurezza. Come ultimo punto, indicato solo da pochi intervistati, ZT potrebbe servire anche a migliorare la user experience di chi si collega da remoto: un tema questo che dovrebbe nei prossimi anni ottenere sempre maggiore interesse da parte dei Responsabili della cybersecurity.

Guardando invece alle principali "difficoltà tecniche" nello sviluppo di una ZT Roadmap, al primo posto (57% delle risposte) la necessità di considerare le diverse tecnologie in uso, gli aspetti di integrazione e assessment preliminare di eventuali gap di sicurezza. In aziende in cui l'automazione è già entrata in altri ambiti (DevSecOps, NoOps), un'architettura ZT basata su capacità di automazione e orchestrazione deve essere pensata in modo accorto, per funzionare bene in sinergia con altri aspetti.

Al secondo posto, il problema legato al mantenimento di legacy e del cosiddetto "technical debt": soprattutto in grandi aziende, per ridurre la complessità di gestione si consiglia di identificare singoli blocchi più facilmente gestibili.

A livello operativo, le principali sfide legate alla transizione ZT sono invece quelle da ricondurre all'utilizzo sempre più ampio di modelli gestiti di security; a difficoltà organizzative nella gestione di ruoli, identità, permessi; alla necessità di superare i silos organizzativi e di "recuperare" le competenze corrette per questo passaggio.

Metaverso, da buzzword a realtà concreta. Ma quando?

Roberto Bonino, Research and Content Manager
The Innovation Group

Il mercato del metaverso si sta creando sulla base di una riorganizzazione di prodotti e servizi che hanno a che fare in vario modo con la realtà aumentata, gli asset digitali come gli Nft e i mondi virtuali che già esistono

Ormai da tempo si sta affermando il concetto di Web3, indicato da alcuni come il futuro dell'economia e dell'esperienza di utenti e professionisti e da altri come un incubo energivoro. probabilmente il futuro, come capita spesso, sta nel mezzo, ma studiosi e analisti concordano sul fatto che non si concretizzerà in tempi troppo brevi e ci lascerà, quindi, il tempo di prepararci.

Nel corso dell'anno e, a maggior ragione, nel tempo che verrà, dovremo aspettarci una moltiplicazione di studi, eventi e interventi sul principale oggetto di questo nuovo scenario, ovvero il metaverso. Varie realtà dell'analisi e della consulenza, da McKinsey ad Accenture, da Gartner a Deloitte, hanno già pubblicato analisi più o meno dettagliate dalle quali fare emergere una visione o le tendenze per il futuro.

Un punto di partenza comune per tutti riguarda il fatto che non stiamo parlando di qualcosa di totalmente nuovo. le tecnologie del Web3 esistono da almeno una decina di anni e in larga parte sono disponibili. il mercato del metaverso si sta creando sulla base di una riorganizzazione di prodotti e servizi che hanno a che fare in vario modo con la realtà aumentata, gli asset digitali come gli Nft e i mondi virtuali che già esistono.

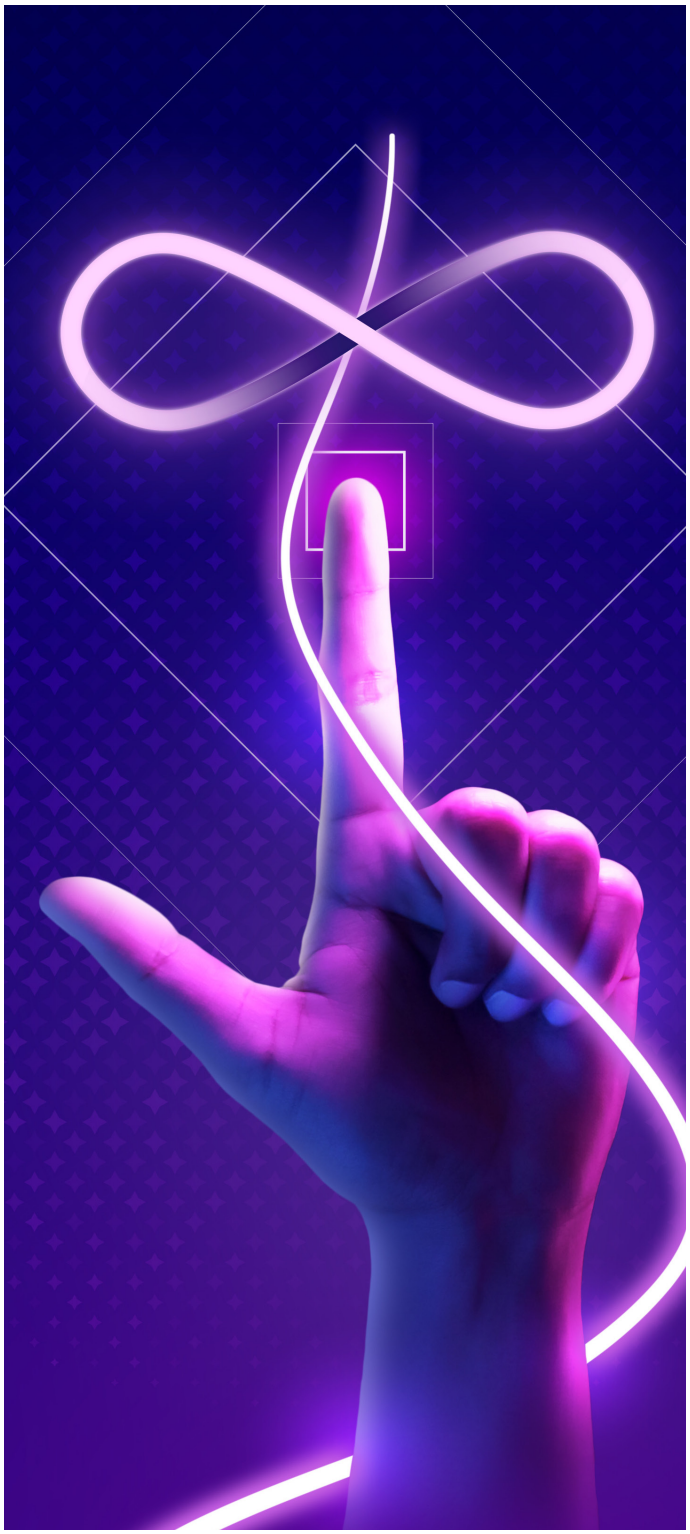
In questo senso, le analisi possono sfruttare il vantaggio di non dover partire completamente da zero ed elaborare stime basate su numeri in qualche modo già definiti. per citare un dato, Gray Investments stima il mercato dei mondi virtuali nel 2025 ha un valore di 400 miliardi di dollari, pur partendo da una cifra di 180 miliardi del 2020, che si deve all'aggregazione della componente videoludica. com'è già capitato per altre evoluzioni, non è così semplice oggi fare delle stime credibili e omogenee, perché si tende a inserire o escludere componenti fra loro diverse. il caso più tipico è quello delle criptomonete, che

certamente saranno una componente del metaverso, ma nel caso dei Bitcoin si sono sviluppate senza bisogno di un'infrastruttura virtuale ancora da costruire.

Quindi, in generale, il nuovo mercato sarà determinato da una combinazione di tecnologie, che ancora non sappiamo esattamente in quale misura andranno a pesare nella determinazione del valore complessivo. siamo ancora nella fase di incertezza determinata dalle modalità di utilizzo e dalla velocità alla quale tutto andrà ad evolvere prima di raggiungere la massa critica determinata dall'integrazione di diverse tecnologie. Per questo si rileva oggi ancora una notevole discrepanza nei tassi stimati di crescita, in alcuni casi collocati al di sotto del 20% e in altri attorno al 40% annuo almeno fino al 2030.

Se pensiamo al mondo dei videogiochi, parliamo già di una realtà immersiva, dove funzionano correttamente caschi per la realtà virtuale e strumenti di collaborazione. questo è anche il mercato di maggior attrazione oggi per Meta (ex Facebook), che ha acquisito la tecnologia Oculus, ma anche dei big player del settore, come Sony, Microsoft e Nintendo. anche il mercato degli eventi immersivi e collaborativi dovrebbe svilupparsi di pari passo, con riferimento primario a concerti e manifestazioni sportive.

Diverso e, per certi versi, più interessante è la declinazione del metaverso nel campo della trasformazione digitale delle aziende e delle riflessioni sulla customer experience. Qui già oggi ci sono settori nei quali sono stati fatti passi avanti dal punto di vista dell'utilizzo della realtà virtuale e aumentata. Chi lavora nel mondo del design, della moda o dell'arredamento anche in Italia ha già messo a punto esperienze di showroom nei quali far immergere i propri clienti e dimostrare loro il potenziale dei loro prodotti calati in un contesto virtuale, ma anche esperienziale. Magari non siamo ancora all'era nella quale si venderanno anche mobili occhiali unici secondo la logica degli Nft, ma qualche evoluzione collegata al potenziale del Web3 è già ipotizzabile nel medio termine. nulla sembra destinato ad avvenire troppo presto e forse nemmeno nella forma tecnologica immaginata da Mark Zuckerberg, che per primo ha introdotto sta cercando di cavalcare il concetto di metaverso.



La certificazione di genere fa bene ai dipendenti e anche all'azienda

Valentina Bernocco, Web and Content Editor
The Innovation Group

Che cosè la **certificazione di genere**, quali vantaggi può consentire di ottenere e come realizzarla? Si tratta di una pratica ancora poco conosciuta nelle aziende, anche perché di inclusione e parità di genere nel campo lavorativo si parla da relativamente poco tempo. Oggi, per fortuna, queste tematiche sono ben presenti non solo nel dibattito mediatico ma anche nei consigli di amministrazione e nelle discussioni dei team manageriali. Inoltre in Italia ci sono alcune interessanti novità legislative, che è bene conoscere per cogliere le opportunità collegate. Abbiamo approfondito il discorso con Alice Palumbo, socia amministratrice e fondatrice di IN-Genere, un'azienda benefit che si rivolge a Pmi, enti e associazioni, sviluppando progetti tesi alla creazione di ambienti di lavoro inclusivi.

Quanto è diffuso, tra le aziende italiane, l'interesse sulle certificazioni e i bilanci di genere?

È vero che la Legge n. 162/2021 interviene in materia di pari opportunità nel contesto lavorativo rafforzando la tutela già offerta dal D.lgs. n. 198/2006 (c.d. Codice delle Pari Opportunità), il concetto di certificazione invece è abbastanza recente. La legge n. 162/2021, in materia di parità di genere, estende ai datori di lavoro che occupano almeno cinquanta dipendenti dell'obbligo di trasmissione al Ministero del Lavoro e delle Politiche Sociali del rapporto di parità; istituisce una nuova certificazione di parità, al cui rilascio corrisponderà la possibilità di applicare un esonero dei contributi a carico dell'impresa nella misura massima dell'1% e sino all'importo di 50.000 euro su base annua da riparametrare e applicare su base mensile.

La prassi di riferimento UNI/PdR 125:2022 è la linea guida che consente la certificazione della parità di genere alle imprese. È stata attuata dal decreto del ministro Bonetti dell'1 luglio 2022. I certificatori sono stati individuati (4 luglio) dopo l'introduzione della certificazione (16 marzo).

Negli scorsi mesi i quotidiani nazionali ne hanno parlato, i più sensibili al tema hanno seguito passo passo. Ho riscontrato molto interesse da parte delle aziende, degli enti e delle associazioni di categoria, sono certa che nelle prossime settimane creeranno momenti di approfondimenti utili a conoscerne i vantaggi.

Quali vantaggi si possono ottenere attraverso una politica aziendale di parità d i genere, e quali vantaggi in particolare dalle certificazioni?

Programmi di leadership inclusiva, definizione di politiche e procedure aziendali orientate alla diversità e all'equità di genere, nonché il rafforzamento di meccanismi positivi legati al confronto costruttivo dovrebbero rappresentare la normalità. È il modo giusto per stare insieme e fare meglio. La certificazione è la validazione da parte di un esterno del fatto che un luogo di lavoro rispetta determinati standard, quindi è una garanzia per chi desidera andare a lavorarci o per le realtà che si trovano a dover scegliere tra un'azienda e un'altra in mercati ultracompetitivi.

Come è nata l'idea di IN-Genere? Quali difficoltà ha incontrato nel lancio del progetto e come è stato accolto in questi primi mesi?

Ho cominciato a fare impresa — prima generazione — nel 2012 in un settore diverso, sempre a contatto con le aziende. Credo molto nel networking e ho sempre dedicato molto tempo a progettualità all'interno di associazioni di categoria e focalizzate all'empowerment femminile, penso a LE Imprenditrici di Confindustria Brescia, a Ewmd (European Women's Management Development), e più di recente con il Lions Club Capitolium, composto da sole donne. Sono molto grata alle reti di donne proattive che ho incontrato e con le quali ho vissuto un decennio di esperienze arricchenti. L'obiettivo nelle associazioni femminili che frequento non è mai pensare o coordinare un progetto, è collaborare con altre donne con il vantaggio

di imparare l'una dall'altra nel percorso. Sono palestre di genere.

Personalmente ritengo che ogni centimetro di strada percorsa insieme fin qui abbia plasmato la mia vita e rafforzato il mio impegno verso l'inclusione. In più l'amore per l'autoimprenditorialità, la voglia di costruire team che possano fare la differenza, crescere e prosperare senza dimenticare il beneficio comune. Non è un caso che la neonata IN-Genere sia un società benefit.

Sicuramente l'attesa del decreto attuativo e della nomina dei certificatori ci ha rallentati, guardo al bicchiere mezzo pieno e penso che forse così abbiamo avuto più tempo per prepararci. Sono linee nuove per tutti, anche per chi fa già consulenza magari su altre certificazioni sarà nuovo. Noi abbiamo avuto mesi per concentrarci solo sulla ISO dedicata all'inclusione della diversità e sulla UNI per l'equità di genere. Incontriamo quotidianamente aziende interessate e cominciamo a costruire le prime proposte, per lo più sono aziende tra i cinquanta-sessanta dipendenti e i mille che hanno già politiche attive random da incrementare e trasformare in prassi da valorizzare.

Tipicamente, qual è l'iter previsto per una certificazione?

Come in tutti i progetti c'è la fase analitica (indagine sulla cultura della diversità, dell'equità e dell'inclusione nell'ambiente di lavoro con benchmark su settori analoghi), quella strategica (proposte di intervento personalizzate per colmare eventuali divari rispetto al desiderato, che possono essere attività di apprendimento e sviluppo come di revisione di interi processi interni e progettualità specifiche) e quella operativa, il momento attuativo. Non è necessario certificarsi per costruire un percorso di crescita su questi temi, qualche azienda potrebbe volersi mettere al passo senza necessariamente poi procedere con audit esterno. Coloro che invece desiderano certificarsi devono necessariamente, una volta pronti, chiamare un certificatore per essere verificati sul campo.

Quali azioni, secondo lei, sono più efficaci per promuovere nelle aziende una cultura dell'inclusione?

Credo che i processi HR e in particolare la selezione rappresentino un nodo strategico che influisce sul futuro gettando solide basi nel presente. Come identificare i migliori talenti senza discriminare alcun gruppo? Alcune ricerche spiegano ad esempio come la personalità sia un forte predittore delle prestazioni senza produrre differenze significative di sottogruppi. Ho trovato sensate le parole di Hogan in un articolo che ho letto tempo fa sulla rete, in cui si affermava che "le persone che sono ottimiste, perspicaci, calorose, coscienziose, tolleranti, di mentalità aperta, non difensive, fiduciose, modeste, umili, oneste, comprensive e preoccupate di aiutare gli altri lavoreranno per promuovere un ambiente di inclusività, indipendentemente dalla razza, dall'età, dal sesso, dal background e dalle idee.

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