MARZO 2023

IL CAFFÈ DIGITALE

THE INNOVATION GROUP NEWSLETTER

BANCHE "FRAGILI"
E FINTECH CON PIEDI PER TERRA

QUESTO MESE ABBIAMO FATTO COLAZIONE CON...

Angelo Ruggiero
Unilever

INTELLIGENZA ARTIFICIALE

La battaglia "intelligente" sui motori di ricerca

REALTÀ AUMENTATA

Google Glass addio, fine di una scommessa (perdente e vincente)

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

13

DIRITTO ICT IN PILLOLE

Semaforo giallo per l'atteso erede del Privacy Shield

Yuri Monti

15

INTELLIGENZA ARTIFICIALE

La battaglia "intelligente" sui motori di ricerca

Roberto Bonino

17

REALTÀ AUMENTATA

Google Glass addio, fine di una scommessa (perdente e vincente)

Valentina Bernocco

L'EDITORIALE

Banche "fragili" e fintech con piedi per terra

Ezio Viola, Co-Fondatore

The Innovation Group

Dopo la pandemia, la guerra, il costo dell'energia, l'inflazione, ecco l'ennesima crisi che si somma: quella delle banche. La Silicon Valley Bank in California prima, Credit Suisse in Svizzera poi e non ultimo l'attacco speculativo a Deutsche Bank.

Il sistema bancario continua a mietere vittime e da molto tempo la valutazione e la fiducia sono in calo. Le banche si stanno dimostrando organizzazioni fragili, troppo fragili e il ruolo delle Banche Centrali a volte non è sufficiente non tanto ad affrontare le crisi ma a stabilire regole e farle controllare in modo efficace. Dopo la fine della lunga stagione dei tassi a zero o addirittura negativi e il ritorno della lotta all'inflazione che era stata dimenticata, alla luce di crack bancari, già in essere e potenziali, vengono riproiettati gli spettri del 2007-2008-2009 (crisi finanziaria globale e conseguente recessione). La crisi e il salvataggio delle banche americane e di Credit Suisse sono due fenomeni diversi apparentemente disconnessi, ma che devono essere considerati due facce della stessa medaglia.

La Silicon Valley Bank storicamente si era posizionata su start-up e venture capital dove le banche tradizionali fanno più fatica ad arrivare. Questo evento sta modificando profondamente tutto il settore delle start-up perché il 50% di esse aveva un conto presso SVB e anche se i depositi sono stati salvati questo segnerà per sempre il settore. Con un mercato di tassi bassi o negativi il settore fintech è esploso. Perché il costo del capitale per le start up del credito, che si finanziavano con linee di credito era molto basso. Ad esempio, il modello BNPL (Buy Now Pay Later) è esploso come modo di fare credito al consumatore. Tutte i segmenti del Fintech sono cresciuti dalle piattaforme di trading, alle nuove banche con conti e carte a zero costi. Tutto ciò era reso possibile dalla crescita del venture capital che riceveva capitale da fondi pensione e altri investitori in cerca di rendimento. Questi fondi hanno investito milioni di dollari nelle start-up facendole crescere esponenzialmente e con tante start-up diventate unicorni.

La situazione di oggi è quasi rovesciata e il settore ha dimostrato di essere fragile e si teme che inizi una fuga generale dei consumatori che non si fidano più di istituzioni finanziarie nuove e poco regolate. Le start-up che nasceranno dovranno avere modelli di business sostenibili e prezzi più competitivi e segnano una forte discontinuità con il passato. Ciò che preoccupa non è solo la velocità con cui la crisi è arrivata anche se è evidente una incapacità manageriale di gestione di una banca che deve salvaguardare e bilanciare depositi a breve e investimenti e debiti a lungo temine, ma che ci siano già altre banche americane locali che traballano e con la fuga dei depositi verso grandi banche.

Anche la crisi del Credit Suisse, certo più grave per le dimensioni globali dell'istituto elvetico, è da tempo noto per problemi di cattiva gestione e dunque non è stata una sorpresa per nessuno.

Uno dei fattori più gravi e comune ad entrambi i casi è che, né le grandi banche centrali né tantomeno i governi abbiano calcolato, e quindi prevenuto, il rischio di crisi bancarie generate dalla brusca (per velocità e dimensione) inversione della politica monetaria da loro decisa di fronte alla crescita dell'inflazione che ha colpito il mondo a partire dal secondo semestre dell'anno scorso.

L'aumento dei tassi di interesse deciso dalle banche centrali riduce il valore dei titoli di stato nei quali le banche hanno investito depauperando l'attivo delle banche. Si era sicuri che l'inasprimento delle regole impresso (molto in Europa, meno negli Usa) dopo il 2008 potesse fare da argine. Ma qui non siamo di fronte (solo) ad un problema regolatorio. Quella che è mancata è la comprensione di ciò che avrebbe comportato mettere velocemente fine ad un regime di denaro facile, senza costo, durato 15 anni da aver ingenerato nel mondo del business come tra la gente comune l'idea che si trattasse della normalità, non di uno stato d'eccezione.

Le banche servono perché consentono di diversificare il rischio e controllano il debitore in modo efficace. I depositanti mettono sul conto i loro soldi, ritirabili in qualunque momento, la banca li presta a lungo termine a imprenditori o famiglie, lucra sul differenziale dei tassi (più alti a lungo, più bassi a breve) e controlla in modo efficace l'uso delle risorse, cosa che milioni di depositanti non potrebbero fare. Nel mondo di ieri, però, nessuno pensava a spostare i propri soldi dal conto, se succedeva perché si spargeva la voce che la banca era gestita male, poteva avvenire la "corsa agli sportelli". Oggi nessuno va più allo sportello, basta un clic dalla app del cellulare. E togliere i soldi dal conto per metterli, per esempio, in titoli di stato che rendono il 4-5 per cento a rischio quasi zero non è una scelta dettata dal panico, ma razionale, specie in tempi di alta inflazione

Naturalmente, come sempre, il detonatore è stato il panico che si è diffuso velocemente tra investitori e risparmiatori anche per la facilità con cui la tecnologia digitale oggi permette di comunicare e sollevare "panico" con e sui social media e i clienti fare transazioni bancarie da mobile. Spostando depositi su banche o investimenti alternativi.

Come è anche stato evidenziato dal governatore della FED la corsa agli sportelli di Silicon Valley Bank è stata agevolata, velocizzata dai social media ed è stato normale che investitori e risparmiatori abbiano cominciato a bussare alle porte di fondi e banche per recuperare i loro soldi.

Non si vogliono qui analizzare e valutare le cure e i metodi utilizzati da governi banche centrali sia nel caso americano che quello svizzero anche se molte critiche sono state sollevate per il trattamento speciale riservato ai depositanti del SVB e per le priorità date agli azionisti e non ai possessori di obbligazioni nel caso del salvataggio di Credit Suisse con la vendita a UBS.

Quello che sé è osservato è che tutti i più autorevoli rappresentanti di diversi Paesi europei e dei loro Regolatori si sono affrettati a dire che in Europa siamo relativamente al sicuro. Questo è vero, le banche sono maggiormente capitalizzate e il credito più regolamentato e va valutata come dimostrazione di questa consapevolezza la scelta della Bce di non interrompere il suo programma di rialzo dei tassi recente.

Se le banche perdono il senso sociale e la loro fragilità intrinseca (crediti a lungo termine, debiti a breve) diventa ingestibile, gli argomenti per aiutarle diventano più deboli. Aumentare i requisiti patrimoniali non basta. Vale la pena ricordare che 15 anni fa la crisi nacque americana e poi però finì per essere prevalentemente europea, e che molte delle ragioni della debolezza strutturale di allora del Vecchio Continente sono tuttora esistenti, a cominciare dal fatto che da noi gli strumenti di politica monetaria e quelli di politica di bilancio sono separati e l'unione bancaria è ancora un'incompiuta, con tutti i rischi che ciò comporta. La crisi di fiducia nelle banche non riguarda tanto dettagli del loro conto economico, ma la loro stessa natura e la tecnologia amplifica opportunità ma anche gli errori e le conseguenze di rischi non gestiti.

Angelo Ruggiero
CIO di Unilever

Il passaggio al cloud, fra vantaggi concreti e residue paure

Roberto Bonino, Research and Content Manager
The Innovation Group

Il percorso di migrazione al cloud riguarda, in un modo o nell'altro, la maggioranza delle aziende oggi. Modalità e scelte, tuttavia, dipendono da numerosi fattori e devono necessariamente tener conto della storia di ogni realtà, dello sviluppo tecnologico seguito nel tempo, della tipologia di processi e dati coinvolti e del mindset complessivo dell'organizzazione.

Unilever è una grande multinazionale, che opera nei mercati Nutrition and Ice Cream, Home Care, Beauty & Wellbeing and Personal Care, raggiungendo oltre 190 paesi con più di 400 brand. Fra questi, troviamo Algida, Calvé, Dove, Grom, Knorr, Mentadent e Svelto. Se nel mondo l'azienda impiega circa 149mila dipendenti, l'Italia ha comunque una dimensione rilevante in rapporto allo scenario locale, con 3.500 persone impiegate e molte attività coordinate o gestite sul territorio. Per capire le dinamiche dell'evoluzione tecnologica e il rapporto fra scelte corporate e autonomia locale, abbiamo incontrato Angelo Ruggiero, CIO di Unilever.

Qual è oggi il vostro rapporto con il cloud e quali esigenze si celano dietro le scelte fin qui effettuate?

Veniamo da un anno, a livello corporate, che ha sancito la definitiva migrazione, dapprima con le applicazioni più piccole e poi con quelle core, a partire dal gestionale. Tra i motivi che hanno convinto al passaggio, troviamo la possibilità di disporre di aggiornamenti automatici puntuali, con ovvie ricadute sulla cybersecurity, i costi e la sostenibilità, potendo progressivamente dismettere i due data center che prima agivano in parallelo. Il prossimo passo sarà probabilmente in direzione dell'edge computing, poiché l'IoT sta prendendo piede nelle fabbriche grazie ai tempi di latenza molto bassi. L'input arriva direttamente dal mondo della produzione, dove il cloud viene ancora percepito come possibile fonte di interruzione del servizio. Dal punto di vista It, vantaggi rilevanti si sono registrati con il disaster recovery, oggi fruito in gran parte as-a-service con relativo sgravio di oneri per noi,

e con lo storage, per ragioni di spazio occupato e flessibilità di gestione delle capacità.

Come avviene il processo decisionale all'interno di una multinazionale come la vostra?

La scelta dei fornitori e dei provider viene gestita a livello corporate e non ci sono margini per agire localmente. La scelta centrale si è orientata verso il cloud pubblico, ma è allo studio la possibilità di dotarsi anche di cloud privato per alcune tipologie di applicazioni e dati. Come già indicato, gran parte dell'azienda è ormai migrata, mentre la produzione progredirà in direzione dell'edge computing per ragioni di opportunità e di business. In generale, riteniamo che il cloud vada interpretato soprattutto come una soluzione, in grado di alleggerire.

Quali sono le principali preoccupazioni che avete sul fronte della sicurezza?

Poniamo un'attenzione estrema su tutto quanto si può ricondurre alle classiche minacce esterne, ma monitoriamo con precisione anche quanto accade sulla rete, per poter rilevare attività anomale anche attribuibili a specifici utenti, in modo da poter intervenire e verificare con tempestività l'accaduto. Esiste anche un crisi scorporate team, del quale faccio parte anch'io, che si riunisce periodicamente per esaminare situazioni di potenziale pericolo di vario genere (disastri naturali, ma anche guerre o altro), che possono avere ripercussioni sui nostri siti.

Come sta evolvendo il mindset aziendale alla luce della trasformazione dei processi e dei metodi di lavoro?

Gli utenti hanno capito che tutto sta andando in cloud e questo porta con sé magari anche qualche rischio, ma soprattutto benefici talvolta tangibili e talaltra senza comunque impatto sull'operatività.

Dal nostro punto di vista, poniamo molta attenzione sull'adattamento del comportamento in funzione della minimizzazione dei rischi. Ogni volta che si accende un pc, compare una maschera che ricorda i principi fondamentali da rispettare, arrivano messaggi che ricordano gli aggiornamenti frequenti da effettuare e poi si fanno anche campagne simulate di attacco. Qui si gioca la vera partita della digitalizzazione oggi e nel tempo a venire.

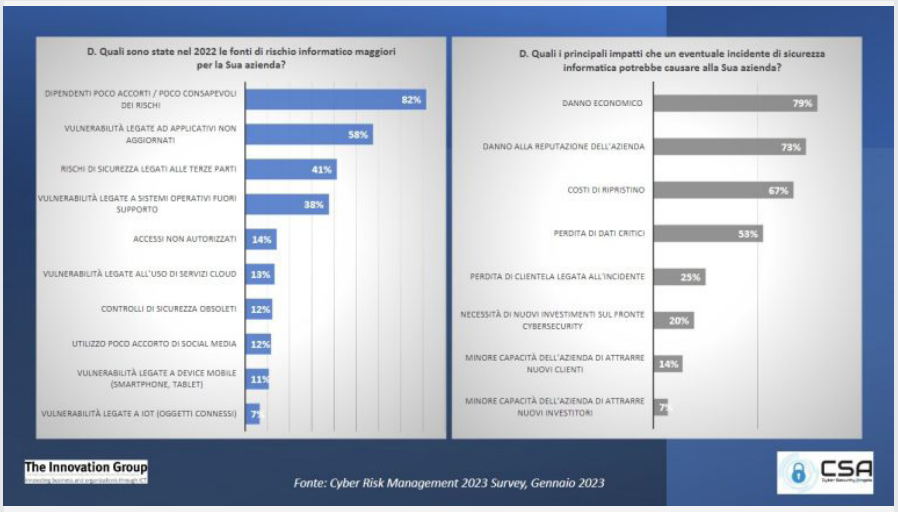
Cybersicurezza, il “fattore umano” è il primo problema

Valentina Bernocco, Web and Content Editor
The Innovation Group

La parola awareness, consapevolezza, è sempre più utilizzata dalle aziende che vendono tecnologia ma anche da quelle che la utilizzano. Non è un caso. Computer, smartphone, servizi cloud, posta elettronica, applicazioni per chat e videoconferenze sono strumenti di uso quotidiano in ambito lavorativo, a maggior ragione oggi che lo smart working ha preso piede e sembra destinato a consolidarsi.

La facilità d’uso di questi strumenti può ingannarci, spingendoci a comportamenti apparentemente senza conseguenze ma in realtà rischiosi: cliccare su un allegato di posta o su un link senza aver prima controllato il mittente, condividere un documento usando un servizio di file sharing non previsto dalle policy aziendali, usare password poco sicure o “riciclate”, accedere al cloud da qualsiasi dispositivo (incuranti della presenza di software obsoleti) e talvolta anche da reti Wi-Fi pubbliche. Sono solo esempi di leggerezze e distrazioni, a cui si sommano le infinite vie del phishing (sempre più sofisticato e ingannevole, grazie a nuove tecniche di camuffamento, al social engineering e ai deepfake creati dall’intelligenza artificiale), la crescente proliferazione dei ransomware (ormai accessibili anche a malintenzionati inesperti di codice software, grazie al modello as-a-service) e l’irrisolto problema delle vulnerabilità presenti in sistemi operativi e applicazioni (il patch management può essere complesso e l’eterogeneità degli ambienti IT crea dei “punti ciechi” in cui possono nascondersi falle).

Si tratta di problemi stratificati nel tempo e intrecciati tra loro, problemi che i vendor di sicurezza informatica affrontano sempre di più con un approccio cosiddetto Zero Trust, in cui si agisce per ridurre al minimo il rischio e prevenire gli incidenti. Per queste criticità non esiste una soluzione facile e veloce, tuttavia migliorare l’awareness sulle tematiche di sicurezza informatica sarebbe d’aiuto su tutti i fronti.



Fonte: Cyber Risk Management 2023 Survey, The Innovation Group, Gennaio 2023

Un'indagine condotta da The Innovation Group e da Cyber SecurityAngels (Csa) su un campione di duecento aziende italiane ha evidenziato che anche nel nostro Paese il "fattore umano" è l'elemento più critico per la cybersicurezza delle aziende. Tra i principali elementi di pericolo per la propria azienda nel 2022, l'82% degli intervistati ha indicato la scarsa consapevolezza e attenzione ai rischi informatici da parte dei dipendenti: si tratta della risposta più citata, prima ancora delle vulnerabilità degli applicativi (58%) e dei rischi legati alle terze parti (41%). A ulteriore conferma del fatto che il "tallone d'Achille" sono le persone, nel 55% delle aziende l'anno scorso c'è stato almeno un caso di furto o smarrimento di un dispositivo in uso ai dipendenti. Questa è stata la tipologia di incidente più diffusa, ancor prima delle infezioni da malware (47%), del furto di identità o credenziali (37%), degli accessi non autorizzati (29%) e dei data breach (18%).

"Possiamo scrivere regole di ogni genere per definire ogni processo, ma il fattore umano potrà sempre prevalere", ha commentato Stefano Lusardi, IT security manager di Feltrinelli e referente per la Lombardia di Cyber Security Angels (Csa), in occasione del recente Cybersecurity Summit organizzato a Milano da The Innovation Group. "La chiave è educare alla cybersicurezza", ha proseguito Lusardi, "non con un corso di formazione fatto una volta l'anno bensì spiegando le necessità della cybersicurezza all'utente, che si tratti di un impiegato o di un manager. Le regole vanno benissimo, ma l'educazione degli utenti è essenziale, e non bisogna pensare di essere tutti degli esperti di informatica solo perché si utilizzano determinati strumenti".

Ma su quali temi si dovrebbero focalizzare gli sforzi di formazione sulla cybersicurezza? Attraverso le riflessioni di rappresentanti di aziende vendor e utenti, dalle tavole rotonde del summit è emerso che oggi è ancora necessario far capire i rischi legati alla ormai famigerata "dissoluzione del perimetro" dell'IT aziendale. Un fenomeno iniziato da circa un decennio prima con l'apertura all'uso dei dispositivi personali (il cosiddetto bring your own device, Byod) e proseguito con la crescente adozione del cloud e con i modelli di lavoro ibrido nati sull'onda della pandemia.

Altri rischi spesso sottovalutati sono la posta elettronica (principale vettore di infezione, sia per i malware sia per i tentativi di phishing) e le interfacce API, Application Programming Interface. Oggi, in ambienti informatici sempre più eterogenei e geograficamente dispersi, per il personale IT mantenere il controllo e la visibilità è un'impresa ardua. Tutti i dipendenti di un'azienda, in ogni livello dell'organigramma, dovrebbero contribuire a tenere le minacce fuori dalla porta.

Intelligent Automation sempre più diffusa nelle aziende italiane

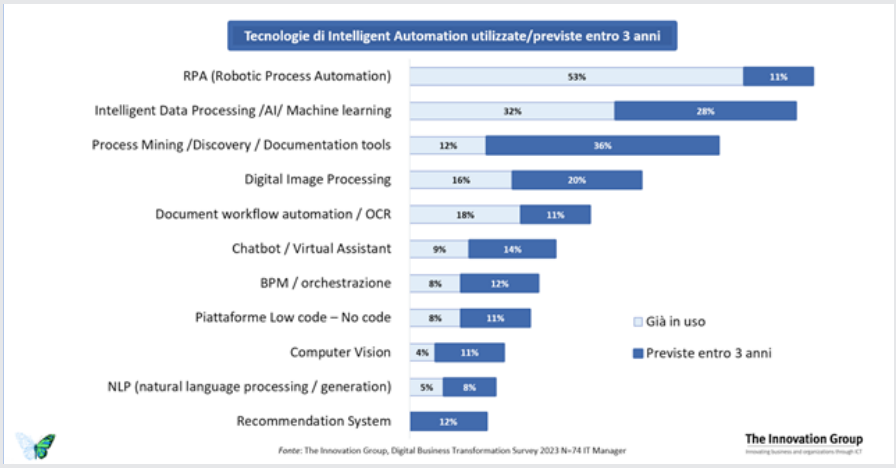
Elena Vaciago, Associate Research Manager
The Innovation Group

Il 2023 è l'anno del grandissimo interesse per le applicazioni dell'intelligenza artificiale e più in generale della crescita generale dell'uso di tecnologie di Intelligent Automation, o "automazione intelligente dei processi aziendali", oggi applicate in molteplici modi nelle aziende italiane, come emerge anche dalla survey "Digital Business Transformation 2023" di TIG.

Secondo la ricerca, infatti, realizzata a gennaio 2023 su un campione di 197 aziende medio grandi italiane, intervistando sia Manager del business sia IT Manager, si assiste oggi a un ampio ricorso all'automazione intelligente per ottimizzare i processi aziendali. Le soluzioni RPA (Robotic Process Automation) sono l'applicazione più utilizzata dalle aziende (53%), con un 11% che prevede di adottarla entro 3 anni.

Segue l'Intelligent Data Processing, categoria ampia in cui rientrano tutte quelle soluzioni che utilizzano algoritmi di intelligenza artificiale su dati strutturati e non per estrarre informazioni: ne sono esempio, i sistemi per la rilevazione delle frodi finanziarie, la ricerca di pattern, i sistemi di monitoring e controllo, l'analisi predittiva. Sono utilizzati dal 32% delle aziende, con una previsione di un ulteriore 28%.

Le soluzioni di Intelligent Automation sono sempre più diffuse nel panorama aziendale



Fonte: TIG, Digital Business Transformation Survey 2023 | N=74 IT Manager

In generale, l'Intelligent Automation è utilizzata per automatizzare i processi aziendali, migliorare l'efficienza e ridurre gli errori, aumentare la produttività e la redditività. Alcuni esempi di utilizzo sono:

- Automazione dei processi manuali: le tecnologie di IA sono utilizzate per automatizzare i processi aziendali manuali.
- Ottimizzazione della catena di approvvigionamento: l'IA è utilizzata per ottimizzare la catena di approvvigionamento, identificare i punti deboli e migliorando la pianificazione della produzione, la gestione del magazzino e la logistica.
- Gestione dei dati: l'IA è utilizzata per gestire grandi quantità di dati in modo efficiente e accurato, identificare pattern e tendenze che possono essere utilizzati per migliorare la produzione e le vendite.
- Assistenza clienti: l'IA è utilizzata per fornire assistenza ai clienti in modo automatico, attraverso chatbot e altri strumenti di comunicazione automatizzati, riducendo i tempi di attesa e migliorando la soddisfazione del cliente.
- Analisi dei dati: l'IA è utilizzata per analizzare i dati in modo automatico, identificando trend e predizioni che possono essere utilizzati per migliorare i processi aziendali e aumentare la redditività.
- Gestione dei processi finanziari: l'IA è utilizzata per gestire i processi finanziari, come la fatturazione e la gestione delle scadenze dei pagamenti, riducendo gli errori e migliorando l'efficienza.

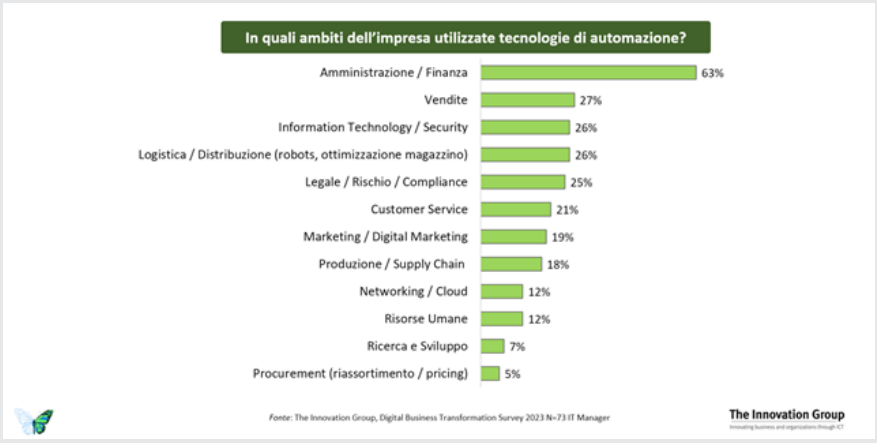
In quali ambiti dell'impresa si utilizza l'Intelligent Automation

In generale, l'IA viene utilizzata in tutti gli ambiti dell'impresa in cui ci sono processi ripetitivi e standardizzati che possono essere automatizzati.

Ciò consente di migliorare l'efficienza operativa, ridurre gli errori, migliorare la customer experience.

Dalla survey emerge che l'automazione intelligente è applicata in particolar modo nell'ambito amministrativo/ finanziario (63% delle risposte) dove aiuta ad automatizzare i processi di contabilità e finanza come la fatturazione, la gestione delle scadenze dei pagamenti, la contabilità generale e la gestione delle attività bancarie.

L'automazione intelligente dei processi trova applicazione soprattutto in ambito amministrativo, ma sono molteplici gli utilizzi in tutti gli altri ambiti dell'impresa



Fonte: TIG, Digital Business Transformation Survey 2023 | N=73 IT Manager

In generale, l'Intelligent Automation è utilizzata per automatizzare i processi aziendali, migliorare l'efficienza e ridurre gli errori, aumentare la produttività e la redditività

Altri ambiti sono:

- Vendite (27%): l'IA viene utilizzata per analizzare i dati dei clienti, ad automatizzare le attività di vendita
- Tecnologia dell'informazione (26% delle risposte): l'IA è utilizzata per automatizzare i processi di gestione dei dati, la sicurezza informatica e il monitoraggio delle reti.
- Gestione delle operazioni aziendali (26%): l'IA viene utilizzata per automatizzare i processi operativi come la gestione dei processi di produzione, la gestione del magazzino e la logistica.
- Servizio clienti (21%): l'IA viene utilizzata per fornire assistenza ai clienti attraverso chatbot e altri strumenti di comunicazione automatizzati.
- Marketing (19%): l'IA serve a migliorare la segmentazione del pubblico, creare campagne di marketing personalizzate.
- Gestione delle risorse umane (12%): l'IA viene utilizzata per automatizzare i processi di gestione delle risorse umane come la selezione del personale, la formazione e lo sviluppo, la gestione del tempo e la pianificazione delle risorse.

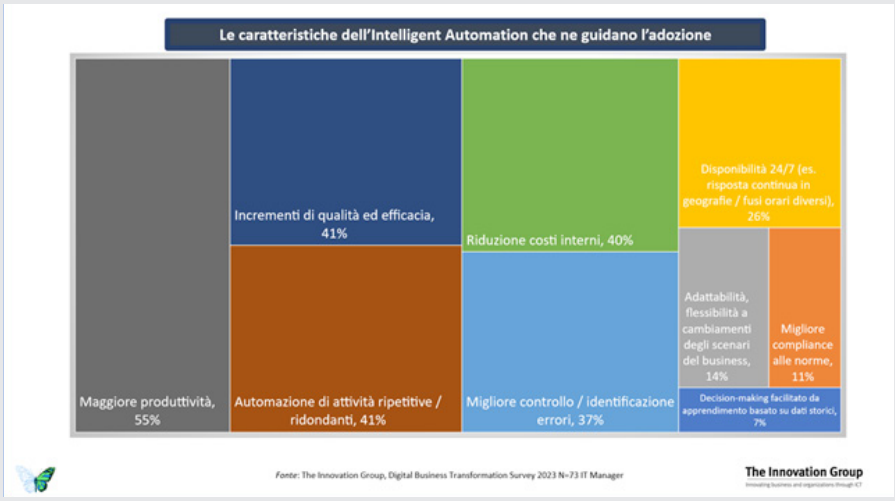
Quali sono i vantaggi per chi adotta queste tecnologie?

Il vantaggio che viene percepito dalle aziende rispetto all'adozione dell'Intelligence Automation è in primis la conseguente maggiore produttività (55%), seguito da incrementi di qualità ed efficacia (41%), automazione di attività ripetitive/ridondanti (41%) e riduzione dei costi interni (40%).

- Aumento della produttività. L'IA può automatizzare i processi aziendali, riducendo i tempi di esecuzione e aumentando la produttività dei dipendenti.
- Maggiore efficienza. L'IA può automatizzare i processi aziendali riducendo i tempi di esecuzione e migliorando l'efficienza operativa, liberando tempo e risorse per altri compiti.
- Risparmio di costi. L'IA può ridurre i costi aziendali automatizzando i processi ripetitivi e standardizzati, liberando tempo e risorse per attività ad alto valore aggiunto.

- Riduzione degli errori. L'IA può ridurre gli errori causati dall'intervento umano nei processi aziendali, migliorando la qualità dei prodotti e dei servizi e riducendo i costi per correggere gli errori.
- Miglioramento della customer experience. L'IA può fornire assistenza ai clienti in modo rapido e personalizzato attraverso chatbot e altri strumenti di comunicazione automatizzati, migliorando la customer experience.
- Maggiore agilità. L'IA può aumentare la flessibilità aziendale, consentendo alle aziende di rispondere rapidamente ai cambiamenti del mercato e alle esigenze dei clienti.
- Analisi dei dati avanzata. L'IA può analizzare grandi quantità di dati in modo rapido e preciso, fornendo informazioni utili per il miglioramento dei processi aziendali e la presa di decisioni strategiche.

Le caratteristiche dell'Intelligent Automation che ne guidano l'adozione



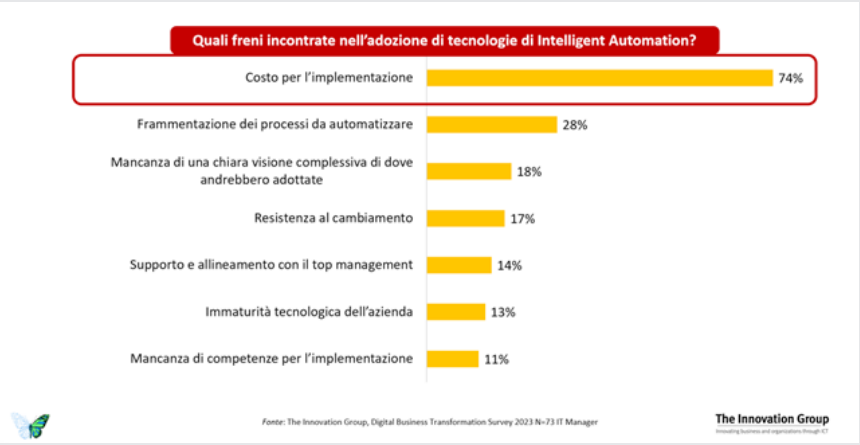
Fonte: TIG, Digital Business Transformation Survey 2023 | N=73 IT Manager

Quali sono invece gli elementi che ancora frenano questa adozione?

Nonostante i numerosi vantaggi dell'Intelligent Automation (IA) o Automazione Intelligente dei Processi Aziendali (IPA), ci sono ancora alcuni elementi che possono frenare l'adozione di queste tecnologie da parte delle aziende. Tra i principali fattori ci sono i costi elevati, citati dal 74% dei rispondenti (l'adozione dell'IA richiede spesso investimenti significativi in tecnologie, formazione e risorse umane specializzate, il che può essere proibitivo per alcune aziende); la frammentazione dei processi da automatizzare (28%); la mancanza di una chiara visione (18%) e la resistenza al cambiamento (17%).

Nonostante i numerosi vantaggi dell'IA ci sono alcuni elementi che possono frenare l'adozione di queste tecnologie. Tra i principali fattori ci sono i costi elevati, la frammentazione dei processi da automatizzare, la mancanza di una chiara visione e la resistenza al cambiamento

Il costo è visto come il limite principale all'adozione di soluzioni di automazione intelligente dei processi



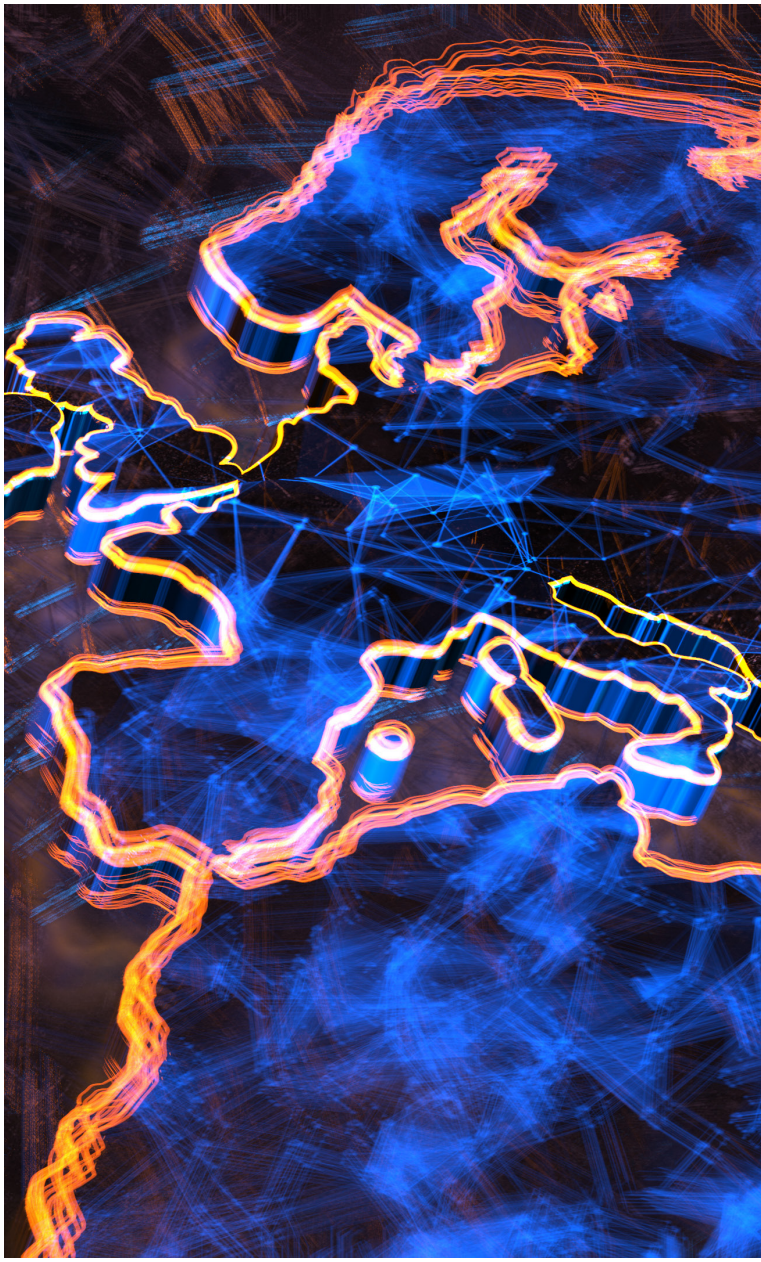
Fonte: TIG, Digital Business Transformation Survey 2023 | N=73 IT Manager

DIRITTO ICT IN PILLOLE

Semaforo giallo per l'atteso erede del Privacy Shield

Yuri Monti, Consultant

Colin & Partners



È stata approvata giovedì, dal Parlamento europeo con larga maggioranza, la direttiva NIS2 (Network and Information System Security). Si tratta di un necessario lavoro di aggiornamento di uno strumento già esistente (la direttiva NIS di prima generazione) che ha prodotto, anche in Italia, interventi normativi e, prima ancora, riflessioni strutturate sulla gestione della sicurezza in contesti digitali.

La nuova direttiva, stimolata anche dai cambiamenti prodotti dalla pandemia, viene considerata, stando alle parole del relatore Bart Groothuis, "La migliore legislazione sulla sicurezza informatica che il Continente abbia mai visto, perché offre all'Europa una gestione proattiva degli incidenti informatici e orientata al servizio".

L'accrescersi delle problematiche relative alla cybersecurity, l'aumento degli attacchi ai sistemi informativi e delle minacce alla tutela dei dati, rendono necessarie reazioni coordinate e razionali tra gli stati membri per garantirne i cittadini.

Si tratta, come sempre nel caso delle direttive europee, di un impianto che ciascuno Stato dell'UE dovrà tradurre e recepire, tenendo presente l'obiettivo, ovvero creare una uniformità e una condivisione degli strumenti e delle procedure che consentano un lavoro organico e collaborativo all'interno dell'Unione.

I destinatari

Al momento, i principali destinatari sono i cosiddetti "settori essenziali" e "settori importanti". Tra i primi rientrano senza dubbio: energia (dall'elettricità al gas, dal petrolio all'idrogeno), trasporti, banche e finanza, sanità, settore idrico, infrastrutture digitali (cloud, data center, gestione reti, ecc.), gestione servizi ICT, pubblica amministrazione e spazio. Tutti dovranno adeguarsi alle nuove disposizioni in materia di sicurezza.

Tra i settori considerati importanti sono citati i servizi postali, la gestione dei rifiuti, il settore alimentare, quello dei prodotti chimici e sanitari, la produzione di dispositivi medici, l'elettronica, la fabbricazione di macchinari e quella di veicoli a motore e, non ultimi, i fornitori di servizi digitali quali motori di ricerca o piattaforme di servizi di social network.

La difesa, stando allo spirito della normativa, non è meno importante dello stimolo che tale direttiva vuole offrire agli attori coinvolti affinché possano operare, con successo, la propria trasformazione digitale, cogliendone tutti i vantaggi economici e sociali e

garantendo ai fruitori dei servizi pari giovamento da essi.

Responsabilità condivisa all'interno della supply chain, proattività, capacità di reagire in modo efficace e rapido, monitoraggio costante e condivisione delle informazioni su vulnerabilità e incidenti, sono i cardini che ispirano l'intervento europeo.

I capisaldi

In base alla Strategia nazionale per la cyber sicurezza, richiesta a ciascuno Stato membro – che comprenda obiettivi e priorità, nonché le risorse necessarie e una valutazione dei rischi – la direttiva punta l'attenzione su alcuni aspetti:

- l'individuazione di misure volte a garantire la preparazione e la risposta agli incidenti e il successivo recupero dagli stessi, inclusa la collaborazione tra i settori pubblico e privato;
- un elenco delle diverse autorità e dei diversi portatori di interessi coinvolti nell'attuazione della strategia nazionale per la cyber sicurezza;
- un quadro strategico per il rafforzamento del coordinamento tra le autorità competenti ai fini della condivisione delle informazioni sui rischi, le minacce e gli incidenti sia informatici che non informatici e dello svolgimento di compiti di vigilanza, se del caso;
- un piano, comprendente le misure necessarie, per aumentare livello generale di consapevolezza dei cittadini in materia di cyber sicurezza.

Per le aziende e gli enti coinvolti, non solo medi e grandi, significa quindi introdurre la cyber sicurezza, a livello sistemico, nell'intera filiera dei prodotti o servizi proposti. Al di là degli obblighi normativi attuali o futuri, si tratta di un approccio corretto, utile e che non può prescindere da un aumento responsabile di consapevolezza e cultura rispetto al tema della cyber sicurezza.

La linea tracciata, che resta coerente rispetto agli interventi normativi europei degli ultimi anni, è quella di generare un ecosistema virtuoso che operi in continuità e coordinamento e che sia in grado di affrontare cambiamenti e innovazioni, non solo tecnologici ma anche inerenti modelli di business che potranno essere introdotti in futuro.

INTELLIGENZA ARTIFICIALE

La battaglia “intelligente” sui motori di ricerca

Roberto Bonino, Research and Content Manager
The Innovation Group

A stretto giro, Google e Microsoft hanno lanciato le loro soluzioni di intelligenza artificiale applicata ai rispettivi search engine. Da uno strumento di base, parte un nuovo serrato confronto, con possibili conseguenze anche sulla vita di tutti noi.

L’intelligenza artificiale appare il più recente terreno di scontro fra i big della tecnologia, con diverse implicazioni sugli strumenti con i quali affrontare la competizione e, in controluce, effetti anche sulla vita dei miliardi di utilizzatori coinvolti. A breve distanza, Google e Microsoft hanno annunciato evoluzioni sui rispettivi motori di ricerca, facendo tesoro degli ultimi sviluppi sul fronte e delle contrapposte scelte di presenza sul mercato.

L'evoluzione di Bard

Google, infatti, lavora da molto tempo sulla ricerca interna e sull'elaborazione del linguaggio naturale, per utilizzi inizialmente pensati per il mondo professionale, ma destinati a estendersi verso il grande pubblico. Microsoft non ha perso tempo, investendo in OpenAi, l'azienda che ha creato l'hype più potente del periodo con la divulgazione di ChatGpt.

Proprio il cambio di paradigma nel modo di affrontare la ricerca semantica e la relativa user experience sembra aver allarmato Google, per molto tempo leader incontrastata delle tecnologie di search engine, utilizzate come base per lo sviluppo di un ecosistema software apertamente in contrasto con il parallelo dominio di Microsoft nell'ambito della produttività individuale.

Da qui nasce la corsa all'annuncio della prossima disponibilità di Bard, un servizio di intelligenza artificiale conversazionale, fin qui sperimentale e usato soprattutto al proprio interno. L'idea è quella di aprire la tecnologia a tester ritenuti di fiducia prima di un lancio definitivo a beneficio del grande pubblico. Se ChatGpt deriva da Gpt-3 (175 miliardi di parametri), Bard è un'emanazione di LaMda, ovvero un modello di elaborazione del linguaggio naturale rilasciato nel 2021, ma che aveva avuto una prima concretizzazione l'anno precedente con Meena (2,6 miliardi di parametri).

LaMda è un modello specializzato nell'emulazione di un dialogo fra macchina ed essere umano, con un addestramento costruito su un numero di parametri elevatosi a 137 miliardi e un volume che comprende 1,56 T-words (equivalenti di 2,97 miliardi di documenti, 1,12 miliardi di dialoghi e 13,39 miliardi di enunciati. Un lavoro chiaramente ispirato a quello di OpenAi su Gpt-3.

L'addestramento è durato circa sessanta giorni sulle Tpu v3, ovvero i processori Asic di Google, per poi procedere con diversi affinamenti, legati alla definizione di dialoghi con persone reali, tenendo conto di criteri di qualità, allineamento alla realtà e sicurezza. Bard appare come una versione light di LaMda, soprattutto perché necessità di una potenza di calcolo decisamente minore.

Una risposta costruita su Bing

Senza perdere tempo, Microsoft ha risposto con il lancio di una preversione di Bing, potenziata da un modello Nlg realizzato in combinazione con OpenAi. Vengono integrati, in modo particolare, gli apprendimenti e gli sviluppi di ChatGpt e Gpt-3.5. L'addestramento è avvenuto tramite una collezione di strumenti denominata Prometheus.

Questi sviluppi saranno integrati tanto in Bing quanto nel search engine di Edge e si concretizzeranno in una barra laterale che, secondo Microsoft, sarà in grado di fornire risposte più complete, pianificazioni di viaggi o itinerari, composizione di messaggi e posta elettronica. Per il momento, l'accesso a queste evoluzioni è ancora limitato, ma si prevede di allargarlo a milioni di persone nelle prossime settimane.

Nel corso della presentazione, sono state fornite anche prove delle capacità di Prometheus, in grado di sintetizzare una ricerca a partire da una semplice domanda, restituire un riassunto delle risposte disponibili sul Web e includere link verso le pagine utilizzate come fonti. Per ora siamo fermi qui, a una sorta di rielaborazione intelligente dei risultati più pertinenti ottenuti tramite il motore di ricerca, ma un'evoluzione maggiormente orientata alle capacità generative di ChatGpt appare naturale.

I termini della contesa

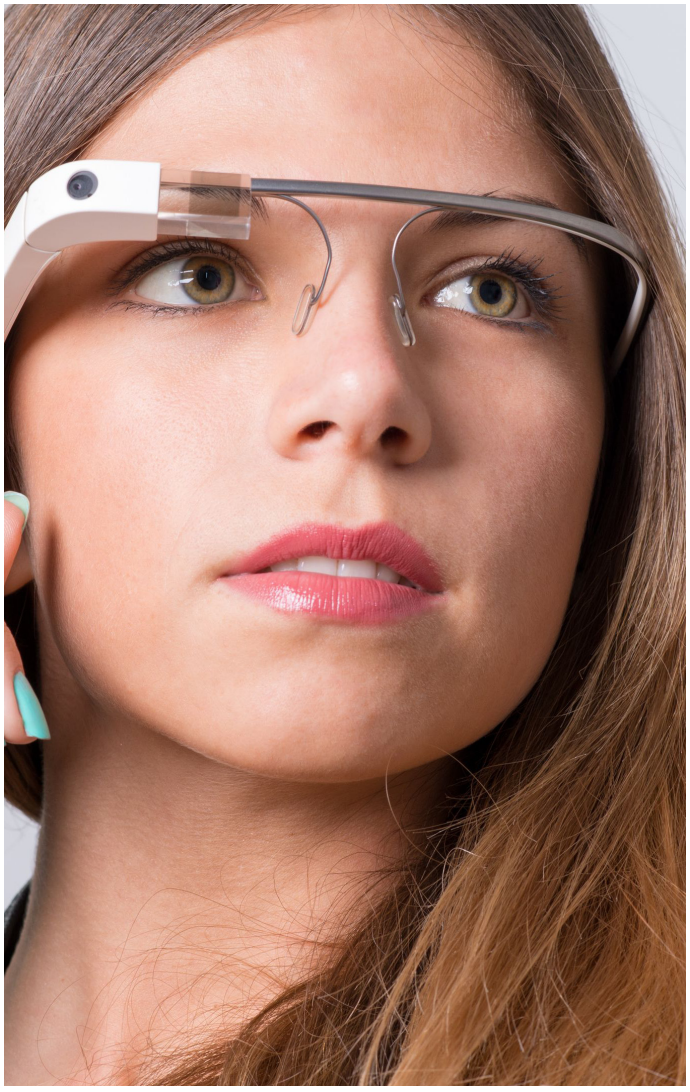
Il guanto di sfida lanciato da Microsoft lascia presagire che ci sia la volontà di estendere le tecnologie di intelligenza artificiale tanto in voga verso le applicazioni più popolari o di nuova realizzazione, ma anche di attaccare Google sul suo terreno prediletto, per rosicchiare i guadagni derivati dal mercato pubblicitario. Tutto il castello del Seo e della rivendita dei click costituisco una delle fondamenta più solide del business di Google e la minaccia può generare più di una preoccupazione.

Qui si potrebbe giocare la partita nell'immediato, mentre ancora prematuro è parlare di un'infusione di Ai generativa in ambiti come i contact center o le chatbot aziendali, poiché, almeno finora, sia ChatGpt che Bard non sembrano ancora in grado di riconoscere le specificità di ogni impresa, del loro brand o della gamma di prodotti.

REALTÀ AUMENTATA

Google Glass addio, fine di una scommessa (perdente e vincente)

Valentina Bernocco, Web and Content Editor
The Innovation Group



La società del gruppo Alphabet interrompe definitivamente la produzione e lo sviluppo degli occhiali di realtà aumentata. Ma lasciano un'eredità pesante.

L'avventura dei Google Glass è arrivata al capolinea. Gli occhiali di realtà aumentata nati a Mountain View non saranno più sviluppati né prodotti: così ha deciso l'azienda alla luce dell'insuccesso commerciale di una tecnologia che, d'altra parte, ha aperto la strada per molte evoluzioni successive. Dopo il lancio del primo prototipo, nel 2013, i "Glass" sembravano destinati a diventare nel giro di qualche anno un oggetto hi-tech che ci avrebbe accompagnati nella vita quotidiana in numerose attività, sovrapponendo immagini digitali alla realtà che vediamo: dalla navigazione Gps alle esperienze di shopping nei negozi, dalle comunicazioni alla fruizione di contenuti multimediali o social media, dall'autenticazione biometrica all'editing fotografico. Da quasi subito Google si era affidata all'opera creativa degli sviluppatori, incaricati di alimentare l'ecosistema di app fruibili, e aveva attivato una collaborazione con Luxottica per declinare la tecnologia su montature appetibili anche ai più modaioli.

L'hype, come si suol dire, al debutto dei Glass era notevole, alimentato da valanghe di articoli e recensioni della stampa di settore. Tuttavia, di fronte ai dati di vendita di questi oggetti avanguardistici e costosi, gradualmente si è capito che non sarebbero diventati un bene di massa, che non avrebbero sostituito per l'utente comune l'app Skype o di Google Maps installata su telefono. L'azienda ha allora ricalibrato le proprie ambizioni puntando sulle applicazioni verticali per ambiti come la logistica, il lavoro di magazzino, l'odontoiatria e la chirurgia. Tra aggiornamenti sempre meno frequenti e investimenti ridotti, nel 2015 il programma sperimentale Glass Explorer aveva chiuso i battenti. Dopo due anni di silenzio Google aveva rilanciato il

progetto con una Enterprise Edition dei visori e un nuovo programma di affiliazione con software house di realtà aumentata per settori verticali. Risale al 2020 L'ultimo sostanzioso aggiornamento, i Glass Enterprise Edition 2, potenziati nella caratteristiche tecniche (processore, fotocamera, display), ancor più belli e leggeri e venduti solo tramite provider autorizzati e solo alle imprese a un costo di circa mille dollari.

C'è molto di buono nell'avventura dei Google Glass, sia dal punto di vista strettamente tecnologico sia per il loro ruolo apripista in un mercato che si è poi sviluppato in direzioni diverse e ad alto potenziale di crescita. Microsoft, per esempio, ha puntato sulla realtà mista degli Hololens, più voluminosi da indossare e veicolo di esperienze immersive, dunque non pensati per un uso continuativo come invece i Google Glass. La società di Redmond un anno fa ha anche annunciato una collaborazione con Qualcomm per la messa a punto di processori pensati per le future applicazioni del metaverso.

A Menlo Park Meta, pur focalizzandosi sui visori di realtà virtuale (eredità dell'acquisita Oculus) ha anch'essa sviluppato occhiali di AR con il marchio Ray-Ban. E intanto gli ancora fantomatici Apple Glass o Apple Glasses (il nome è ipotetico) di cui si chiacchiera da anni dovrebbero debuttare, secondo le ultime indiscrezioni, forse nel 2024 o nel 2025, dopo continui slittamenti di data. Verrebbe da pensare che Apple, a differenza della concorrente di Mountain View, non voglia correre il rischio di sfornare una tecnologia ancora non perfetta. Inoltre oggi, non è un mistero, tra inflazione e paure di recessione in molti mercati tecnologici la domanda sta rallentando e potrebbe valer la pena posticipare il lancio di device particolarmente costosi.

Nel medio periodo, però, le prospettive sono ottime. Secondo le stime di Grand View Research, il mercato delle tecnologie di realtà aumentata (fruite sia tramite visori ad hoc sia tramite smartphone) valeva 38,56 miliardi di dollari nel 2022 e con un tasso composto di crescita annuale del 40,9% supererà i 597 miliardi di dollari nel 2030. MarketsAndMarkets ha invece calcolato un valore di 31,97 miliardi di dollari per il 2022 e pronostica un'ascesa fino agli 88,4 miliardi di dollari stimati per il 2026. A fare da traino alla crescita ci saranno applicazioni negli ambiti del marketing e dell'advertising (lanci di prodotto, eventi virtuali), nell'ingegneria, nell'architettura e nell'edilizia (simulazioni e test), nella formazione (esperienze di apprendimento "aumentate"), nella sanità (telemedicina e chirurgia) e utilizzi pratici come la navigazione indoor.

A meno di inaspettate (ma non del tutto improbabili) rinascite, a tutto questo Google assisterà da spettatore: a metà marzo l'azienda ha annunciato di aver interrotto la produzione dei Glass. A partire dal prossimo settembre non saranno più erogati servizi di supporto né pubblicati aggiornamenti. Sono stati un prodotto che non è stato capito, un "genio incompreso"? O forse semplicemente un progetto che Alphabet, presa tra mille iniziative, negli anni non ha saputo supportare abbastanza né con adeguati investimenti né con strumenti (Sdk, Api) destinati agli sviluppatori? Qualunque sia la risposta i Google Glass, nonostante le sconfitte, fanno ormai parte della storia della tecnologia.

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