NOVEMBRE / DICEMBRE 2023

IL CAFFÈ DIGITALE

THE INNOVATION GROUP NEWSLETTER

SIAMO THE INNOVATION GROUP

FACTORY EVENTS MEDIA

WE DRIVE TRANSFORMATION

THE INNOVATION GROUP

CRESCE PER AFFIANCARE LE AZIENDE NEL PERCORSO DI TRASFORMAZIONE DIGITALE

QUESTO MESE ABBIAMO FATTO COLAZIONE CON...

Giorgio Veronesi e Massimo Cottafavi SNAM

NUMERI E MERCATI

L'AI plasmerà i mercati tecnologici nel 2024, dal cloud ai Pc

FOCUS PA

I principi dell'Occidente una guida nell'era dell'incertezza

IL TEAM DEL CAFFÈ DIGITALE

Roberto MASIERO
Presidente
The Innovation Group

Ezio VIOLA
Co-founder
The Innovation Group

Emilio MANGO
General Manager
The Innovation Group

Elena VACIAGO
Associate Research Manager
The Innovation Group

Roberto BONINO
Giornalista, Research and Content Manager
The Innovation Group

Valentina BERNOCCO
Web and Content Editor
The Innovation Group

Arianna PERRI
Research Analyst
The Innovation Group

SOMMARIO

The Innovation Group cresce per affiancare le aziende nel percorso di trasformazione digitale

Redazione
TIG

Dall'integrazione promossa da Marketing Multimedia nasce la nuova TIG – The Innovation Group, un gruppo composto da tre aree di business diversificate che può contare da oggi su un organico di 72 persone, oltre 500 clienti attivi e una crescita media costante (CAGR) superiore al 21% negli ultimi 4 anni.

Un'evoluzione che si fonda sulle dinamiche molto positive del mercato digitale italiano, destinato ad assumere un ruolo sempre più trainante dell'economia grazie agli investimenti in continua crescita per la trasformazione digitale di imprese e enti pubblici. Per il 2023 la stima di crescita del mercato digitale è infatti pari al 2,7% a fronte di un +1,2% del PIL, e in previsione, assisteremo a un trend analogo anche nel 2024 (fonte: Rapporto Annuale Digital Italy 2023).

"L'accelerazione indotta dalle tecnologie come l'AI Generativa sta portando a un nuovo modo di vivere la quotidianità e a nuovi modelli di business. Come è accaduto con l'avvento di Internet, esattamente 30 anni fa quando è nato il nostro Gruppo, stiamo assistendo a un vero e proprio cambio di paradigma. Da qui la spinta a ridisegnare la nostra struttura, creando una nuova e più grande organizzazione, TIG – The Innovation Group, come punto di

riferimento per le imprese nella scelta delle soluzioni tecnologiche più idonee ai propri obiettivi di business" ha dichiarato Roberto Silva Coronel, CEO e maggiore azionista del Gruppo TIG.

All'interno di TIG – The Innovation Group saranno presenti tre aree di business: TIG Factory, TIG Events e TIG Media che lavoreranno in sinergia per un'offerta integrata. L'area con la quota maggiore di fatturato è quella degli Eventi (60%), seguite dalle aree Media (25%) e Factory (15%).

TIG Factory, la società in cui è confluita PrimeWeb, è specializzata nella produzione creativa e nella costruzione di progetti digitali come ad esempio LiveForum, l'innovativa piattaforma completamente customizzabile per le aziende. Dal 1996 ha realizzato più di 4.000 progetti di comunicazione integrata, disegnando e implementando nuovi format attraverso il mix di creatività, coding e dati con un approccio custom made. Tra i clienti: Università Bocconi, Manageritalia, ASK, Chantecler e BMW Group Italia.

TIG Events, con più di 45.000 partecipanti all'anno e 400 clienti attivi, si occupa della ideazione, creazione e gestione di eventi, contenuti e ricerche per l'industria digitale in Italia. In questa società confluiranno le precedenti Digital Events e The Innovation Group che a oltre quindici anni presidiano la comunità italiana del digitale, dell'ICT e del Retail con un palinsesto eventi di proprietà, in licenza e custom. Tra i più rilevanti: il NetComm Forum all'Allianz MiCo di Milano (la prossima edizione si terrà l'8-9 maggio 2024), il Cybersecurity Summit a Milano (28-29 febbraio 2024), l'AI Forum a Milano (4 aprile 2024), il Banking Summit (24-26 settembre) a Baveno, il Digital Italy Summit (12-14 novembre) a Roma.

TIG Media, società dove è confluita MediaMatic, sviluppa e gestisce campagne di comunicazione, fra le prime in Italia già dal 2016 a integrare algoritmi di AI nei processi di ottimizzazione e gestione delle strategie media multicanale. Con oltre 250 campagne gestite e 15 anni di pianificazione omnicale e full-funnel, annovera tra i clienti Agos, Norqain, SENEC, Capital.com.

All'interno di TIG – The Innovation Group è stato inoltre istituito un Comitato di Direzione presieduto dal Prof. Roberto Masiero e Roberto Silva Coronel, composto da: Pietro Cerretani, CEO e shareholder di TIG Events, Emilio Mango, General Manager e shareholder di TIG Events, Valentina Usellini, General Manager di TIG Factory e Marco Di Gioacchino, General Manager di TIG Media.

"TIG punta a una crescita organica nell'area dei servizi di content creation e ricerche di mercato, nella creazione di eventi proprietari, nello sviluppo di progetti digitali e piattaforme per la business community, ed infine nella consulenza strategica media – ha continuato Roberto Silva Coronel – "parallelamente contiamo di sviluppare nuove sinergie in ambito universitario per accelerare i processi di R&D e arricchire le nostre soluzioni e il business proposal".

In occasione del cambiamento di Marketing Multimedia in TIG – The Innovation Group, il Gruppo ha rinnovato la propria immagine coordinata, con un nuovo logo e un nuovo sito (www.tig.it).

Giorgio Veronesi, Executive Director ICT – Innovation & Digital Technologies e Massimo Cottafavi, Director Cyber Security & Resilience, SNAM

Cloud e security alla base della trasformazione digitale

Elena Vaciago, Research Manager
TIG

L'avviamento di progetti di trasformazione digitale porta con sè ricadute importanti sulle infrastrutture tecnologiche delle aziende, sotto diversi aspetti. La convivenza fra componenti on-premise e workload migrati in cloud si abbina a scelte che possono andare in direzioni come l'adozione di architetture a microservizi o di strumenti di monitoraggio più evoluti, ma anche la definizione di una strategia dy cybersecurity che tenga conto del perimetro allargato oggi da presidiare.

Di questi temi e di come sono calati in una realtà come Snam, abbiamo parlato con Giorgio Veronesi, Executive Director ICT – Innovation & Digital Technologies e Massimo Cottafavi, Director Cyber Security & Resilience.

Nell'ambito del percorso di trasformazione digitale che avete eventualmente intrapreso, quali sono gli elementi sui quali vi siete concentrati e gli ambiti aziendali maggiormente coinvolti?

Veronesi: Nel definire gli aspetti di trasformazione dobbiamo partire da una riflessione attenta su ciò che abbia più o meno senso portare in cloud e metterlo in relazione con la vicinanza a macchine e persone. Questo trade-off fra efficienza e prossimità è l'elemento cardine dei processi decisionali di aziende come la nostra che gestiscono anche infrastrutture critiche per il paese. Noi abbiamo deciso di portare avanti entrambe le linee. Il cloud è stato adottato laddove le operations e la complessità lo richiedono oppure dove sono presenti servizi adatti, come nel caso di tutti i servizi che vengono forniti agli impiegati. Molte attività però human-centric e mission critical, su tutte la manutenzione degli impianti, poggiano ancora su infrastrutture on-premise.

Il mutamento di scenario e l'adozione, ad esempio, di architetture containerizzate e a microservizi, hanno comportato una revisione delle strategie di protezione dei sistemi?

Cottafavi: Quando abbiamo deciso di adottare queste tecnologie è stato anche ribaltato il modello di verifica delle vulnerabilità. Siamo passati dal classico approccio Waterfall, in cui le verifiche arrivano ex post appena prima o addirittura durante il rilascio, a quello più tipicamente security by design. Abbiamo anticipato

con questo modello l'arrivo della containerizzazione e oggi esso viene applicato trasversalmente in tutti gli ambiti, dalle applicazioni corporate per arrivare a oggi anche a quelle OT. Questo approccio consente di mettere subito in evidenza eventuali vulnerabilità che non fossero state considerate in anticipo.

Un tema storicamente delicato per chi gestisce le infrastrutture tecnologiche riguarda l'aggiornamento degli ambienti operativi. Come avviene il processo di patching e la relativa la manutenzione per i sistemi e le applicazioni business critical?

Veronesi: Abbiamo fatto un grosso lavoro di allineamento con tutti i nostri fornitori e mettere così a punto un modello che ci consente di tenere aggiornati tutti i nostri ambienti operativi e le applicazioni. Si tratta di un percorso in essere, ancora un po' complesso per la presenza di sistemi legacy, ma stiamo lavorando per essere progressivamente sempre più puntuali. Il grosso dell'attività si basa su processi di aggiornamento che hanno una valenza periodica, integrati da interventi on call richiesti soprattutto dalla struttura di cybersecurity in presenza di vulnerabilità che non è possibile o accettabile lasciare in essere fino alla scadenza del successivo ciclo di patch.

Avete sentito l'esigenza di adottare specifiche certificazioni e relative strategie per poi rispettarle?

Cottafavi: Sicuramente uno stimolo forte deriva dai vincoli normativi negli ultimi anni. Noi ci dobbiamo confrontare con ciò che attiene al Perimetro di Sicurezza Nazionale Cibernetica e dalla metà del prossimo anno affronteremo anche la scadenza di adozione della direttiva NIS2. Tuttavia, non vediamo in queste normative particolari complessità rispetto a come ci stiamo già posizionando, ma semmai consentono di fare ordine e attribuire le corrette priorità. Di sicuro, la certificazione deve essere un volano di allineamento e non un paravento per poi non seguire un percorso virtuoso e vigile.

I principi dell'Occidente una guida nell'era dell'incertezza

Elena Vaciago, Research Manager
TIG

Ogni giorno sperimentiamo cosa vuol dire vivere in un'epoca caratterizzata da molte incertezze, e quanto possa essere complicato interpretare la realtà in cui viviamo. Nonostante mai prima di ora si abbia avuto accesso a enormi basi di conoscenza e a flussi informativi aggiornati in tempo reale, mai prima si siano palesate capacità realizzative e predittive come quelle promesse dall'intelligenza artificiale, nonostante tutto questo, mai come oggi è stato altrettanto difficile orientarsi in una situazione così complessa e incerta.

In occasione del Digital Italy Summit 2023, intervenendo sul tema "Europa e Italia: geopolitica, autonomia strategica e politiche industriali", Nathalie Tocci, Direttrice dell'IAI (Istituto Affari Internazionali), ha sottolineato come nel giro degli ultimi venti anni, si sia via via affermato un processo di chiusura che ha cancellato la precedente visione di un mondo aperto e di una globalizzazione che avrebbe abbattuto frontiere e cancellato divergenze. "Partiamo da ieri per capire dove siamo e dove stiamo andando – ha detto Nathalie Tocci -. Alla fine della guerra fredda, il commercio internazionale aumentava, la globalizzazione cresceva, e noi credevamo in

alcuni principi, come la linearità dei processi di cambiamento, il fatto che la liberalizzazione economica avrebbe comportato una liberalizzazione democratica, e il fatto che l'interdipendenza tra gli Stati sarebbe stata fonte di efficienza, prosperità e pace. Invece, dall'11 settembre 2001, abbiamo avuto una successione di crisi, abbiamo visto come la globalizzazione potesse in realtà portare disuguaglianze e problemi, abbiamo osservato chiusure e tendenze che hanno messo in dubbio i precedenti assunti".

Il nuovo millennio ci ha in realtà catapultato in un mondo che ripropone, come avveniva in passato, il sopravvento delle ideologie, che a loro volta determinano scontri non economici ma militari. Il bipolarismo è abbandonato e si cerca un nuovo equilibrio nel multipolarismo. Servono, i rapporti internazionali, a far fronte ad alcune grandi sfide globali (dal clima, al nucleare, ai rischi legati alla digitalizzazione) ma per il resto l'orientamento degli Stati va verso una minore dipendenza estera, verso politiche di incremento della produzione interna e di diversificazione dei fornitori.

Anche secondo Gregorio De Felice, Chief Economist di Intesa Sanpaolo (intervenuto sul tema "Lo scenario economico, drivers e possibili criticità della ripresa") il 2024 sarà un anno molto incerto. Non tanto per incertezze di natura economica ma piuttosto di origine geopolitica: bisognerà considerare infatti (e non sappiamo quanto sarà grave) l'impatto sull'economia della guerra in Israele. Avremo le elezioni europee al giugno del prossimo anno e la riforma del patto di stabilità. "Rispetto a queste incertezze abbiamo però alcuni punti fermi – ha detto Gregorio De Felice -: ad esempio, l'inflazione sta rallentando, il dato americano ci ha sorpreso con il ribasso dell'andamento dei prezzi, in Europa stiamo rallentando, in Italia siamo a novembre all'1,9% e questo vuol dire che il ciclo restrittivo delle banche centrali sta terminando. Altro aspetto positivo, gli USA contrariamente alle attese non sono andati in recessione. Ha deluso molto invece la Cina, che ha registrato una crescita ben inferiore al potenziale. L'Europa aveva cominciato molto bene ma poi abbiamo avuto una decelerazione della crescita (come prevedibile visto l'incremento dei tassi voluto dai banchieri centrali)".

Le prospettive economiche per l'Italia, quindi, sono oggi leggermente migliori rispetto a un anno fa: la riduzione dell'inflazione fa recuperare il potere di acquisto delle famiglie, e ci possiamo ora attendere anche benefici dall'implementazione del Pnrr. "Lo stesso governo prevede che i tre quarti della crescita del 2024 e del 2025 sarà legata all'implementazione del piano – ha aggiunto Gregorio De Felice -. C'è stato un rinvio di molte voci di spesa nel 24 e 25, dovuto a una rivisitazione complessiva del piano in condizioni di contesto diverse alla prima stesura dello stesso, quindi una grande riduzione del numero di progetti. Il nostro apparato centrale, e soprattutto quello locale, non sono infatti in grado di gestire un numero così elevato di progetti; quindi, è corretto fare una selezione dall'inizio. Il governo punta oggi di più sui contributi agli investimenti privati rispetto a quando inizialmente previsto".

Instabilità e incertezza si incontrano anche passando a considerare gli scenari legati al cyberspazio e alla situazione geopolitica, ambiti sempre più interconnessi da cui emergono rischi molto insidiosi per le economie occidentali. "Non sfugge a nessuno la situazione di estrema instabilità – ha detto Edmondo Cirielli, Viceministro degli Affari Esteri e della Cooperazione Internazionale intervenendo sul tema "Scenari di guerra: sicurezza e cooperazione internazionale" -. Abbiamo due guerre in corso, una "regionale", quella in Israele, e una in Ucraina. Oltre a rappresentare fatti gravissimi sul piano umanitario, rappresentano per noi uno scivolamento che ha molti elementi insidiosi. Sappiamo da tempo che esistono potenze ostili dal punto di vista economico e commerciale che hanno sfruttato per anni le debolezze del mondo digitale, per acquisire informazioni da utilizzare nella loro guerra commerciale, o per superare in maniera illecita e velocemente un gap tecnologico che le separava dai Paesi più avanzati. Oggi quello che dobbiamo temere più di tutto è che si ripropongano dei blocchi, che metà del Pianeta, che non condivide i valori dell'Occidente, faccia scudo contro di noi. Purtroppo, questi episodi bellici, hanno un aspetto deleterio: un coalizzarsi sempre più di questi mondi. La nostra missione è quindi rompere questa retorica dei blocchi e cercare di essere coerenti sulla nostra ideologia valoriale rispetto agli altri Paesi".

Compliance della supply chain: audit lo strumento chiave per dimostrare l'accountability

Giulia Rizza, Consultant e PM

Colin & Partners

Il tema degli approvvigionamenti e dei fornitori è un tema centrale in numerose normative europee dal GDPR alla NIS2, passando per numerosi provvedimenti e normative nazionali. Tutte le norme e le direttive citate individuano, infatti, nelle perturbazioni a cui sono soggette le filiere di fornitura, una delle maggiori minacce per la continuità operativa delle imprese e per la loro sopravvivenza

La filiera dei fornitori sempre più sofisticata e tecnologicamente avanzata gioca un ruolo chiave nella costruzione della sicurezza delle organizzazioni – siano esse imprese private o enti pubblici. L'emergenza sanitaria e l'inarrestabile aumento delle minacce informatiche – complice la crisi Russia-Ucraina – hanno evidenziato la necessità urgente di innalzare il livello di attenzione relativo alla gestione del rischio, in primis sulla idoneità, selezione e monitoraggio costante della supply chain.

Il passo decisivo che le imprese sono chiamate a compiere prevede il passaggio dalla reazione alla prevenzione, ponendo tra i temi di maggior rilievo nell'ambito dei processi decisionali il valore della business continuity che impone loro l'adozione della logica del monitoraggio e del controllo costante delle possibili minacce per approntare gli strumenti e le misure adeguate ad affrontarle.

Non è che un caso che il tema degli approvvigionamenti e dei fornitori sia un tema centrale in numerose normative europee dal GDPR – dove il concetto rappresenta uno dei pilastri portanti dell'intero impianto – alla NIS2, passando per numerosi provvedimenti e normative nazionali. Tutte le norme e le direttive citate individuano, infatti, nelle perturbazioni a cui sono soggette le filiere di fornitura, una delle maggiori minacce non solo per il patrimonio informativo delle imprese, ma addirittura per la loro continuità operativa e – estendendo la visione – per la loro sopravvivenza.

Non si tratta dunque di ridurre la questione della conformità dei fornitori ad un mero adempimento normativo o ad un passaggio obbligato da compiere per il raggiungimento della compliance. Per il titolare tale tematica assume un valore strategico che parte dalla scelta stessa del fornitore e prosegue per l'intera durata del rapporto di fornitura. Rispetto al mercato il Titolare dimostra inoltre l'attenzione posta al tema della tutela e sicurezza delle informazioni, accrescendo la fiducia dei consumatori nell'azienda e nel brand stesso.

Le responsabilità dei Titolari

Faro guida per il titolare che si trovi a selezionare il provider è l'articolo 28 del GDPR, in base al quale il titolare deve nominare responsabili del trattamento che presentino garanzie sufficienti tali da poter mettere in atto misure tecniche ed organizzative adeguate, in modo che il trattamento soddisfi i requisiti prescritti dal GDPR e garantisca la tutela dei diritti degli interessati. Tale scelta pone l'accento sul concetto di "responsabilizzazione del titolare" traducendo nella pratica il principio dell'accountability, secondo cui – ricordiamo – il titolare deve essere in grado di dimostrare di aver attuato quanto di sua competenza per valutare la conformità della filiera di fornitori; al contempo, quest'ultimi dovranno dimostrare di aver rispettato gli obblighi normativi. Ragion per cui la fase di selezione del fornitore risulta assolutamente cruciale e impone al Titolare una serie di valutazioni preliminari.

I titolari inadempienti alle prescrizioni del GDPR possono esporre l'impresa a sanzioni tutt'altro che banali, che possono raggiungere importi pari al 4% del fatturato globale dell'azienda. Oltre all'aspetto normativo è necessario considerare l'impatto reputazionale e competitivo: dotarsi di una catena di fornitori in grado di garantire misure tecniche ed organizzative adeguate sul fronte del trattamento dei dati personali favorisce l'instaurazione di un rapporto di fiducia con i propri clienti e assicura una maggiore credibilità sul mercato, in quanto denota la sensibilità e la gestione responsabile da parte del titolare degli aspetti connessi alla sicurezza, alla tutela e alla riservatezza delle informazioni.

Cosa esibire in caso di controllo dell'Autorità: l'importanza degli audit

Quanto detto rende pertanto necessaria una risposta concreta delle organizzazioni all'art.28. Una presa di coscienza che – sul piano pratico – si dovrebbe tradurre nella creazione di un processo di verifica di responsabili e sub-responsabili del trattamento che consenta all'ente o all'impresa di costruire una visione completa dell'indice di rischio di conformità rispetto ad ogni singolo fornitore e di avere una panoramica chiara per procedere – eventualmente – con valutazioni e analisi più approfondite sulle aree di maggiori criticità o sulle tematiche più sensibili.

Un sistema di gestione siffatto si rivela una dimostrazione concreta rispetto alle valutazioni condotte e alle scelte compite oltre che una memoria storica da esibire in caso di controlli da parte dell'Autorità Garante che, attraverso il nucleo dedicato della Guardia di Finanza può effettuare controlli e ispezioni in qualsiasi momento.

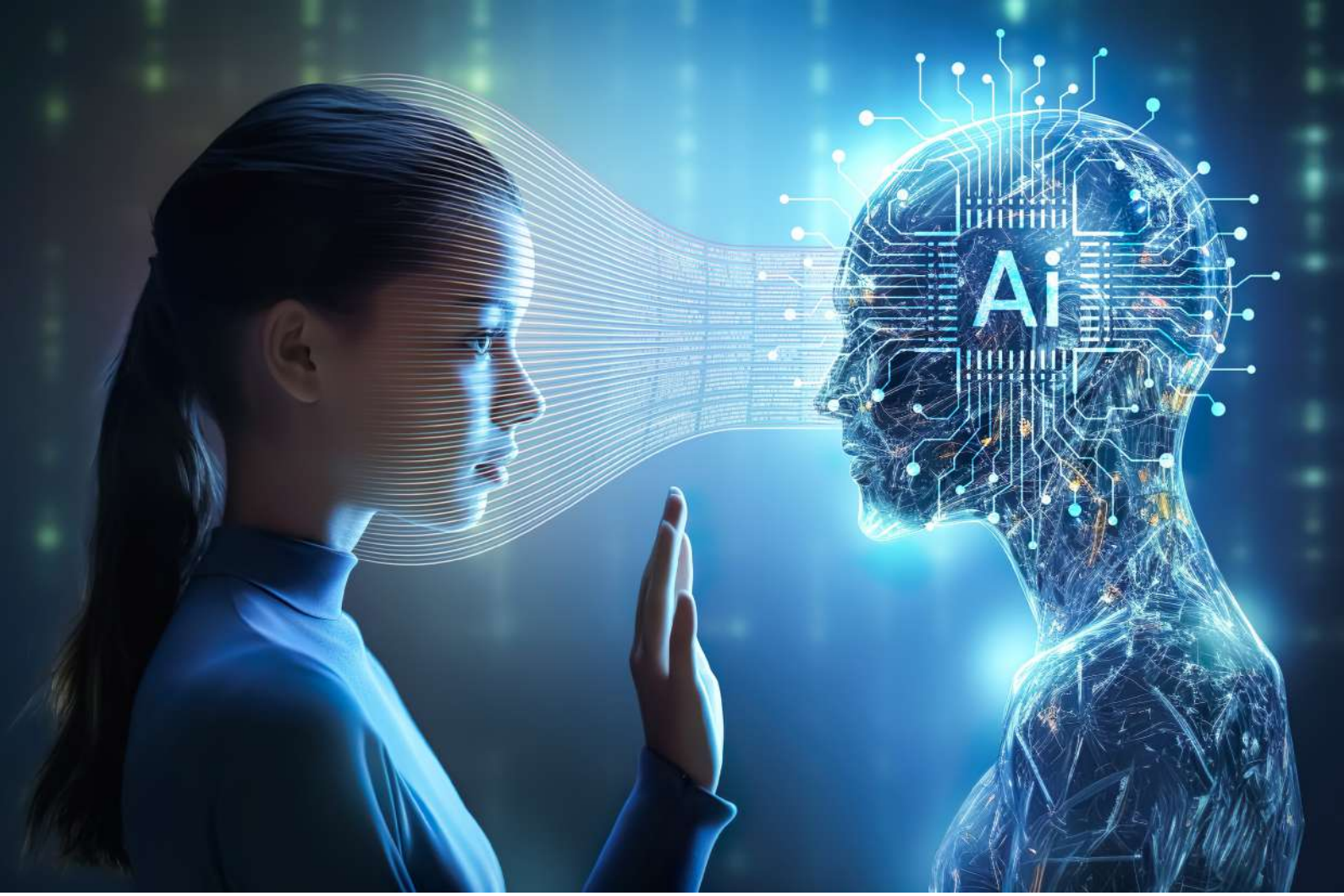
Va da sé che una volta creata la procedura per la verifica della catena di approvvigionamento, il Titolare debba – con cadenza periodica e una certa costanza – verificare attraverso audit e valutazioni specifiche le attività dei soggetti coinvolti nei processi alimentati in maniera più o meno diretta dal trattamento dati personali. Per scongiurare eventuali possibili criticità nel rapporto titolare/responsabili/sub responsabili lo strumento del contratto diviene indispensabile per andare a definire il perimetro di obblighi, responsabilità e reciprochi doveri delle parti – comprese le modalità di audit.

In riferimento a quest'ultimo aspetto merita ricordare che il Titolare può avvalersi di soggetti esterni per l'attività di audit nei confronti dei responsabili e può declinarsi in diversi modi: può infatti concentrarsi sull'intero rapporto disciplinato oppure può avere ad oggetto aspetti ritenuti particolarmente critici o rischiosi, ad esempio a seguito di un breach subito dal Responsabile su un determinato ambito di dati. L'ispezione, in linea generale, non può tuttavia prescindere dall'analisi di alcuni aspetti cruciali quali la tipologia di dati trattati, misure tecniche impostate e settabili, procedure organizzative, modalità di acquisizione e trattamento dati, amministrazione del sistema. Ulteriori scenari giuridici di gran lunga più complessi possono poi aprirsi nel caso si parli di cloud o sviluppi su commissione.

L'AI plasmerà i mercati tecnologici nel 2024, dal cloud ai Pc

Valentina Bernocco, Web and Content Editor
TIG

Non bisogna avere la sfera di cristallo per poter scommettere che il 2024 sarà, un po' come lo è stato il 2023, l'anno dell'intelligenza artificiale generativa. Ma non sarà una fotocopia. Se guardiamo a quanto si è evoluta rapidamente l'AI basata su modelli fondativi (e in particolare su large language model), è facile ipotizzare che osserveremo trasformazioni altrettanto rapide, che faranno sembrare superato ciò che solo 12 mesi prima era avanguardistico. Applicazioni come Midjourney e Dall-E, che generano immagini in base a prompt testuali, stanno facendo rapidi progressi: distinguere gli artefatti digitali dalle fotografie autentiche diventerà sempre più difficile. E non a caso nell'AI Act, il nuovo regolamento dell'Unione Europea sull'intelligenza artificiale, è ribadito il principio della trasparenza: andrà previsto un watermark o altro metodo per identificare chiaramente le immagini generate



Intelligenza artificiale e cybersicurezza saranno molto probabilmente due temi caldi nel 2024, ma altri eventi tecnologici sono all'orizzonte. Uno di questi è la ripresa delle vendite di personal computer.

dall'AI, arginando così gli abusi di proprietà intellettuale e i potenziali usi malevoli.

A tal proposito, nelle previsioni per il 2024 analisti e società di cybersicurezza indicano anche l'utilizzo dell'AI all'interno di attacchi informatici, sia per la generazione di codice malware (attività in cui, al momento, l'AI ancora non raggiunge i livelli di un bravo hacker) sia per la creazione di video deepfake, immagini e audio utili per truffe, phishing e diffamazione. Di fronte a questi rischi, le società di sicurezza informatica ribadiscono che, oggi più che mai, in azienda si deve fare opera di sensibilizzazione, aiutando i dipendenti a diventare più consapevoli e meno ingenui quando leggono una email o ricevono un messaggio sui social network. Ma molti suggeriscono anche di rafforzare le procedure e gli strumenti Zero Trust, che prevedono il controllo sistematico delle identità e dei permessi d'accesso ad applicazioni e dati.

Intelligenza artificiale e cybersicurezza saranno molto probabilmente due temi caldi nel 2024, ma altri eventi tecnologici sono all'orizzonte. Uno di questi è la ripresa delle vendite di personal computer, pronosticata da Gartner,

Idc, Canalys e da molti vendor di semiconduttori e di Pc. "Il mercato dei Pc aziendali è pronto per il prossimo ciclo di sostituzioni, spinto dagli aggiornamenti a Windows 11", ha dichiarato Mikako Kitagawa, director analyst di Gartner, ma il suo è un pensiero comune tra gli addetti ai lavori. "La domanda di Pc consumer dovrebbe ripartire anch'essa, perché i dispositivi acquistati durante la pandemia stanno entrando nelle fasi iniziali del ciclo di sostituzione". Gartner pronostica per il 2024 una crescita complessiva del mercato pari al 4,9%.

E gli smartphone? Dopo due anni di forte rallentamento delle vendite, a detta dei principali osservatori anche questo mercato dovrebbe ripartire, Canalys, per esempio, stima che nel 2024 saranno immessi in distribuzione 1,17 miliardi di telefoni cellulari, numero in crescita del 4% sul 2023. La ripresa sarà sostenuta da diversi fattori, tra cui la crescita di domanda nei mercati emergenti e il lancio di nuovi modelli di fascia alta con migliori fotocamere, processori più potenti e batterie a più lunga durata.

Per quanto riguarda il cloud computing, gli analisti scommettono che il 2024 sarà un anno di crescita alimentata dal proseguimento di progetti di "migrazione" ma anche (impossibile sfuggire all'argomento) dall'intelligenza artificiale generativa. Il cloud e in particolare l'Infrastructure as-a-Service (IaaS) permette di soddisfare i requisiti di potenza di calcolo, memoria e storage necessari sia per l'allenamento degli algoritmi sia per il funzionamento delle applicazioni di AI. Forbes prevede che l'anno prossimo la spesa mondiale in IaaS supererà per la prima volta la soglia dei mille miliardi di dollari, e che si consoliderà un fenomeno già battezzato come "AI-as-a-Service", ovvero l'acquisto di servizi di infrastruttura destinati ad attività di intelligenza artificiale. Sempre a detta di Forbes, passerà dall'attuale 76% all'85% la percentuale di grandi aziende che seguono una strategia multi-cloud, cioè mescolano servizi di differenti fornitori, selezionati a seconda del caso d'uso e della convenienza. Proseguirà, inoltre, lo spostamento sul Software as-a-Service (SaaS) anche per le applicazioni aziendali "core", come l'Erp, il Crm e le piattaforme per la gestione delle risorse umane e dei fornitori.

Solo un accenno, perché la questione è assai complessa, al mercato dei semiconduttori. Le ultime trimestrali di aziende come Samsung, Qualcomm, Tsmc indicano ancora una tendenza calante nelle vendite di componenti destinati a Pc e smartphone, e quest'anno si è anche visto un rallentamento del segmento dei server "commodity". Di contro, i colossi del cloud computing mondiale (come Amazon, Microsoft, Google, Meta) si stanno contendendo le forniture di processori destinati ad applicazioni di intelligenza artificiale, e la forte crescita del market cap di Nvidia lo dimostra. Ma sui semiconduttori per l'AI si gioca anche la competizione politica ed economica tra le grandi potenze, Stati Uniti e Cina innanzitutto, e lateralmente l'Europa. Probabilmente queste stesse dinamiche si svilupperanno anche nel corso del 2024.

In questo scenario restano, ovviamente, le incognite della geopolitica, delle supply chain e dell'inflazione, che negli ultimi anni hanno dimostrato di esercitare una pesante influenza sulla domanda di tecnologie e servizi Ict, sia tra i consumatori sia tra le aziende. Ma ci sono tutte le premesse per un nuovo anno dinamico e segnato dalla ripresa nei più importanti mercati dell'Ict.

Gli impatti di DORA nel mondo finanziario

Elena Vaciago, Research Manager
TIG

Il regolamento DORA (Digital Operational Resilience Act), entrato in vigore il 17 gennaio 2023, diventerà vincolante a decorrere dal 17 gennaio 2025, quindi gli attori del mondo finanziario hanno a disposizione poco più di un anno per adeguarsi. Il DORA si applica alla totalità delle società operanti nel settore finanziario (banche, assicurazioni, Fintech) oltre che ai relativi fornitori di servizi ICT. Pensato per elevare la cyber resilienza a livello sistemico nel mondo finanziario fissa un quadro regolamentare comune per

– Un'efficace gestione dei rischi ICT

– Il monitoraggio dei fornitori di ICT critici

– La segnalazione e la condivisione di informazioni sugli incidenti

– La verifica e l'auditing dei sistemi e dei processi ICT.

Come conformarsi agli obblighi più imminenti? Nel corso del Banking Summit 2023 di The Innovation Group, lo scorso settembre a Baveno, durante il Workshop "Il Trust come Valore: Cyber Security e Protezione dei Dati", sono stati analizzati gli impatti di DORA con un Panel di esperti del settore.

Il regolamento DORA impone a terze parti come fornitori di servizi IT di elevare processi e misure di cybersecurity. "Credo che ci fosse necessità del regolamento DORA – ha commentato Alessandro Bulgarelli, Group CISO di BPER Banca -. Il mondo della supply chain è diventato molto rischioso per la sicurezza delle grandi organizzazioni, che potrebbero scoprire il fianco alle terze parti non in linea con gli indirizzi che ci si è dati internamente. Il regolamento obbliga chi fa parte dell'ecosistema a elevare i propri presidi. Potrebbe però essere molto difficile adeguarsi ed essere conformi a questa norma in tempi così brevi, gennaio 2025 è una scadenza prossima. Chi non sarà pronto ad adottare queste logiche potrebbe rimanere escluso dagli ecosistemi digitali sempre più sfidanti. Per essere resilienti e reattivi a determinate tipologie di incidenti servirebbe però poter contare su una community più attiva dal punto di vista della cooperazione. Potrebbe servire a questo scopo un orchestratore comune".

Tra le novità di DORA, in primo piano va sottolineata l'introduzione di un nuovo mindset, in particolare il passaggio da requisiti di continuità operativa a una visione più ampia di cyber resilienza, che deve essere incorporata in tutti i processi organizzativi. "Intesa Sanpaolo ha investito molte risorse nella cybersecurity – ha detto Domenico De Angelis, Head of Cybersecurity Group Architecture and Framework di Intesa Sanpaolo -. Il regolamento non ci coglie quindi impreparati, lo consideriamo uno strumento utile e necessario per tutti gli attori che insistono nella digitalizzazione dei servizi. Il singolo operatore bancario, per portare il servizio fino alla clientela, deve utilizzare una serie di attori che concorrono a garantire la resilienza end-to-end, che ora avranno gli stessi requisiti di cybersecurity da dover soddisfare.

Per il settore finanziario questo deve essere visto come un vantaggio, considerando il passaggio che sta avvenendo verso i concetti di cyber resilienza, quindi di una sicurezza di sistema. Resta invece qualche perplessità sulla possibilità di fare sinergia e di omogeneizzare i requisiti. L'esempio classico in questo caso è quello del processo

di Incident Reporting, dove, in caso di incidente, è sempre maggiore il tempo necessario per riconciliare template di comunicazione, informazioni richieste e tempistiche di notifica da rispettare nei confronti dei regolatori, con possibili ripercussioni sulla gestione degli incidenti stessi. Servirebbe quindi un'omogeneizzazione dei requisiti di compliance, mentre la stratificazione delle normative nazionali e internazionali rende molto difficile il percorso. Inoltre, restano alcune perplessità sulla supervisione delle terze parti che dovranno adeguarsi a queste normative. Le banche sono vigilate, le terze parti invece da chi saranno supervisionate? Questo onere non dovrebbe ricadere sugli istituti, in quanto il rapporto tra cliente e fornitore potrebbe rendere poco efficace la supervisione".

Una delle sfide maggiori per le banche che puntano a un più ampio miglioramento della propria capacità di risposta a eventi cyber riguarda però la revisione della propria organizzazione. "DORA è una grande opportunità perché allinea il regolamento di tutte le banche italiane a quello delle banche europee – ha commentato Giuseppe Galati, Head of Group ICT and Security Risk di Mediobanca -. Faremo riferimento, di fatto, al regolamento europeo condividendone il piano delle regole e i requisiti di sicurezza. Affronteremo inoltre le stesse sfide, in alcune occasioni faremo altresì scelte comuni forti di esperienze identiche. Questa iniziativa rappresenta quindi un'importante occasione per gestire al meglio le situazioni di crisi aumentando al contempo il livello di scambio di informazioni e di cooperazione. Inoltre, DORA sancisce ufficialmente regole già applicate. Chi lavora nel mondo bancario sa che il 40mo aggiornamento di Banca d'Italia ha già richiesto agli istituti finanziari di adeguarsi a questi temi, di creare le unità di controllo di secondo livello per la gestione dei rischi IT oltre che di lavorare sui rischi ICT e di sicurezza dei fornitori, tutte tematiche ampliamente incluse e dettagliate ora all'interno di DORA. Oggi tutte le organizzazioni, per competere sui mercati finanziari, devono essere attrezzate per gestire rischi IT e di sicurezza supportando in modo adeguato e robusto le unità di business. I clienti retail e istituzionali sono sempre più consapevoli della necessità di lavorare con servizi bancari sicuri scambiando informazioni confidenziali in modo protetto. Siamo oramai abituati a essere attaccati sempre più frequentemente da organizzazioni criminali, negli ultimi anni spalleggiate in alcuni casi anche da agenzie governative e apparati militari, quindi sempre più forti, strutturate e con importanti risorse finanziarie e tecnologiche. Rispondere solo con il CISO è una lotta impari. Il Gruppo Mediobanca già da tempo si è ampiamente strutturato per rispondere come Organizzazione a questo genere di attacchi, continuando a rafforzare le proprie strategie di difesa grazie anche agli stimoli regolatori (vedi ad esempio il Cyber resilience stress test di ECB). Le organizzazioni che non si stanno ancora muovendo in tal senso saranno forzate a farlo dalle nuove norme, come DORA e NIS2. Chi lo ha compreso in anticipo, ha già creato al proprio interno dei centri di competenza per la gestione della crisi cyber, centri trasversali che coinvolgono il DPO, il legale, la comunicazione di gruppo, passando dal procurement e includendo chiaramente le strutture IT e le nuove unità di controllo per la gestione del rischio IT e di sicurezza. DORA non ha fatto altro che prendere atto di questa situazione e mettere ordine richiedendo alle aziende di organizzarsi per rispondere agli attacchi come un'organizzazione unita, strutturata e resiliente, altrimenti nel nuovo contesto cyber potranno avere diversi problemi e importanti impatti".

Blockchain e esperienze innovative del cliente

Elena Vaciago, Research Manager
TIG

Il principale ambito di applicazione della tecnologia Blockchain nelle aziende italiane è quello della tracciatura di informazioni riguardanti prodotti e servizi. In Italia, sperimentata oramai da diversi anni, la Blockchain comincia oggi a trovare applicazione pratica in qualche centinaio di imprese, soprattutto del settore finanziario, retail, fashion, governativo, automotive, agri-food, dei media e dell'arte. I concetti su cui si basa la tecnologia sono oramai ampiamente conosciuti: in sostanza, si tratta di un database distribuito, una struttura dati contenente i log di transazioni che sono automaticamente validate (per il fatto stesso di esservi registrate) senza la necessità di un intermediario fidato. I dati registrati nella catena sono collegati l'un all'altro e distribuiti tra tutti i partecipanti: non possono essere modificati, possono solo essere aggiunti in coda, e in questo modo sono gestite anche le modifiche e le correzioni.

Le applicazioni e i casi d'uso della tecnologia Blockchain in ambito business vanno tutti nella direzione dell'efficientamento di vari processi esistenti, come: gestione degli accessi (a cui aggiunge caratteristiche di trasparenza e tracciabilità molto fine) e immutabilità delle informazioni e affidabilità nel caso degli smart contract. I contratti "smart" sono un'importante innovazione: servono a stringere un accordo tra le parti, e lo fanno specificando ed eseguendo le condizioni dello stesso con codice eseguito in una Blockchain (anziché su un foglio di carta conservato da un notaio). In Italia la Blockchain è impiegata, ad esempio, per tracciare la provenienza di un prodotto alimentare lungo una filiera complessa, per informare tutti su processi o metodologie o riconoscimenti qualitativi associati alla produzione,

per garantire sicurezza e affidabilità dei dati. Applicazioni che ne sottolineano i vantaggi basilari, ossia: trasparenza, fiducia, accessibilità e tracciabilità.

In molti prevedono un uso sempre più ampio della Blockchain, perché in un mondo digitale così distribuito, ampio e spesso confuso, garantisce che le informazioni che vi fluiscono siano basate su dati efficaci e veritieri. Un ambito interessante da considerare è quello della Blockchain utilizzata in situazioni pensate per gestire la relazione con i clienti: quindi per gestirne con efficacia, sicurezza e trasparenza le numerose transazioni; per mantenere una storia certificata di ogni fase; per rafforzare la fidelizzazione e fornire una nuova "esperienza cliente" più avanzata e innovativa.

I benefici della tecnologia Blockchain per la gestione del cliente

Ad oggi, anche se questi utilizzi sono in gran parte ancora sperimentali, si può già affermare che i principali benefici della tecnologia Blockchain utilizzata nella gestione della relazione con i clienti sono:

- Garantire informazioni certe su provenienza, qualità, autenticità e sostenibilità green dei prodotti
- Aumentare sicurezza e trasparenza nei processi di acquisto, tramite la registrazione di tutte le operazioni
- Permettere ai clienti di avere un maggiore controllo sui propri dati, garantire una maggiore sicurezza dei dati, migliorare la privacy
- Incrementare la fiducia e la loyalty del consumatore nei confronti dell'azienda
- Abilitare un rapporto più diretto tra l'azienda e il consumatore/cliente finale
- Migliorare la reputazione, presentarsi sul mercato come azienda attenta all'innovazione.

Quali sono gli utilizzi chiave della Blockchain che possono contribuire alla soddisfazione dei clienti

Di seguito un elenco dei principali ambiti di applicazione di tecnologie Blockchain rivolte ai clienti:

- Gestione dei dati del cliente: i clienti con questa tecnologia possono avere un maggiore controllo sui propri dati personali, ad esempio, concedere l'accesso a determinate parti dei loro dati a specifici servizi o aziende, in modo sicuro e secondo i dettami della privacy.
- Tracciabilità e trasparenza: la tecnologia blockchain offre una tracciabilità completa delle transazioni e delle attività, rendendo più trasparenti ai clienti le loro operazioni.
- Programmi fedeltà e premi: token basati su blockchain possono essere utilizzati per creare programmi di fedeltà e premi più efficaci.
- Risoluzione delle controversie: utilizzata per registrare contratti e accordi tra le parti.
- Pagamenti internazionali e transfrontalieri.
- Condivisione sicura di informazioni: per condividere informazioni sensibili tra organizzazioni o partner commerciali in modo sicuro e protetto.
- Recensioni e feedback dei clienti: possono essere immutabilmente registrati sulla Blockchain, aumentando la fiducia dei clienti.

NFT (Non-Fungible Tokens) ed esperienza del cliente

Un utilizzo particolare della Blockchain poi è quello legato all'impiego di NFT (Non-Fungible Tokens): la Blockchain offre sicurezza, immutabilità e autenticità ai possessori di NFT, il che li rende particolarmente adatti per l'uso in una varietà di contesti, compresi quelli legati all'arte, ai giochi, alla musica, agli oggetti virtuali e molto altro ancora. Gli NFTs sono un tipo di token digitale, di fatto un asset unico e indivisibile. Stanno a rappresentare qualcosa di reale (come un oggetto fisico o un'esperienza da vivere come un evento o un concerto) o virtuale, come un'opera d'arte digitale, una canzone, un video, una proprietà virtuale in un gioco. La Blockchain è la tecnologia sottostante che consente di creare, gestire e autenticare questi token digitali unici, che, in quanto tali, traspongono il concetto di proprietà nel mondo virtuale, potendo essere acquistati, regalati, ceduti, venduti: la proprietà che passa è sempre quella relativa all'NFT stesso, che come smart contract, certifica cosa il suo proprietario possiede.

Gli NFT (Non-Fungible Tokens) a loro volta sono utilizzati in diversi ambiti per migliorare il customer service e la customer experience. Gli NFT sono token digitali unici che rappresentano proprietà digitale o fisica, e la loro caratteristica distintiva è l'individualità, il che li rende adatti per una serie di casi d'uso. Ecco alcuni modi in cui sono impiegati:

- Contenuti digitali autentici rilasciati direttamente ai clienti. Gli NFT vengono utilizzati per autenticare contenuti digitali, come opere d'arte digitali, video, musica e altro ancora.
- Esperienze digitali personalizzate. Le aziende possono utilizzare gli NFT per creare esperienze digitali personalizzate per i clienti. Ad esempio, un cliente che possiede un NFT potrebbe avere accesso a contenuti esclusivi, eventi virtuali o vantaggi speciali all'interno di un'applicazione o di una piattaforma.
- Programmi di fedeltà e rewards: ricompense nei programmi di fedeltà.
- Tracciabilità di beni fisici: i clienti possono verificare l'autenticità e la provenienza dei prodotti che acquistano.
- Gestione delle garanzie e della manutenzione: per tenere traccia delle garanzie dei prodotti e delle informazioni sulla manutenzione.
- Accesso a eventi e contenuti esclusivi, come concerti virtuali, conferenze o anteprime di prodotti.
- Proprietà virtuale in giochi e mondi virtuali. I giocatori possono acquistare, vendere e scambiare NFT per personalizzare le proprie esperienze di gioco.
- Accesso a contenuti giornalistici o educativi: accesso a contenuti giornalistici premium o corsi educativi online.

In conclusione, i vantaggi della tecnologia Blockchain e NPT nella relazione con i clienti

L'uso di tecnologie innovative, come Blockchain e NFT, aiuta a creare esperienze positive che possono aiutare a mantenere salda la relazione con i clienti. I vantaggi come visto nell'articolo sono molteplici, i casi d'uso già oggi sono molto articolati. Tutti sono volti a incrementare la fiducia che i consumatori ripongono in un determinato Brand. Tuttavia, è importante notare che l'adozione di queste soluzioni comporta ad oggi anche numerose sfide e complessità, legate soprattutto al fatto che in molte aziende si tratta tuttora della prima implementazione di queste soluzioni. Guardando al futuro, aspetti chiave che decreteranno il successo di questi sviluppi saranno legati alla possibilità di passare da alcune sperimentazioni a implementazioni su larga scala, di cui sarà necessario garantire la scalabilità, la sicurezza e la conformità alle norme.

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