DICEMBRE 2021

IL CAFFÈ DIGITALE

THE INNOVATION GROUP NEWSLETTER

BITCOIN&STABLECOIN, CRYPTO&TOKEN ASSET:

LA NUOVA FINANZA DIGITALE SPINGE LA NASCITA DELL'EURO DIGITALE

QUESTO MESE ABBIAMO FATTO COLAZIONE CON...

Oscar di Montigny
Banca Mediolanum

NUMERI E MERCATI

TIG Predictions: il mercato digitale nel 2021 e le attese per il 2022

CYBERSEC E DINTORNI

Otto previsioni per la Cybersecurity nel 2022

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

Carmen CAMARCA
Analyst
The Innovation Group

Roberto BONINO
Giornalista, Research and Content Manager
The Innovation Group

Valentina BERNOCCO
Web and Content Editor
The Innovation Group

Loris FREZZATO
Channel Area Manager
The Innovation Group

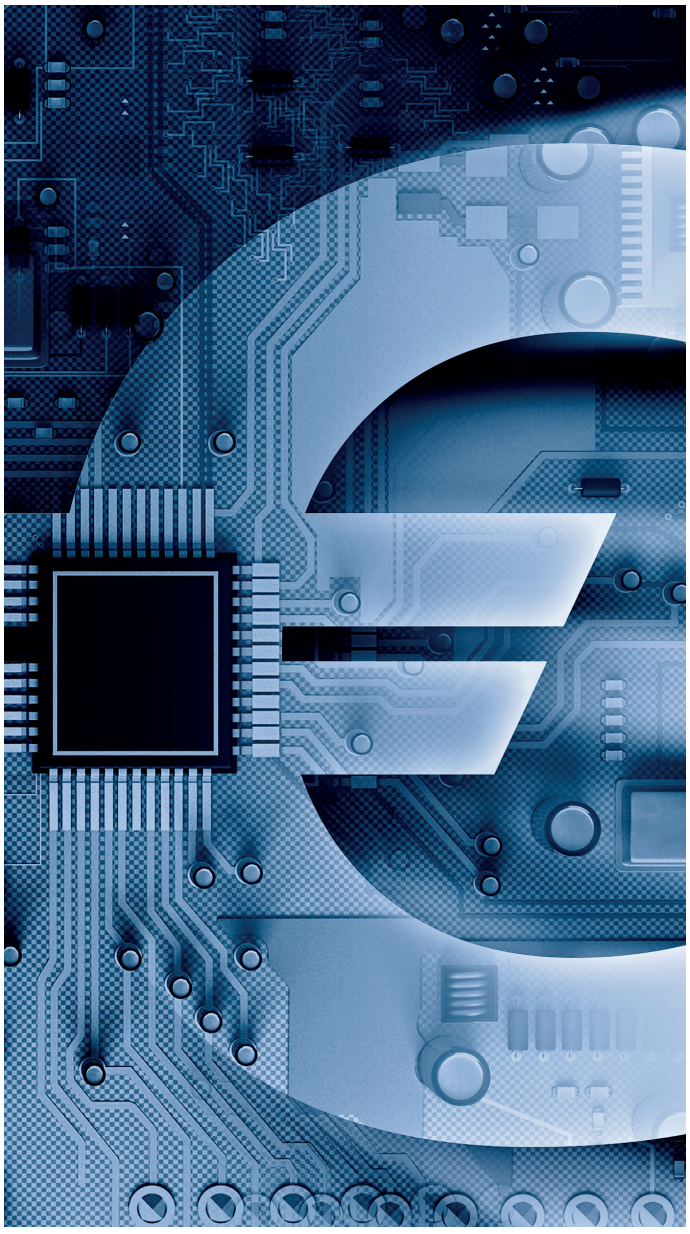
SOMMARIO

L'EDITORIALE

Bitcoin&stablecoin, crypto&token asset: la nuova finanza digitale spinge la nascita dell'euro digitale

Ezio Viola, Co-Fondatore

The Innovation Group



Stiamo vivendo una accelerazione anche nel mondo della finanza digitale (che non significa offrire i servizi finanziari attraverso i canali digitali). La nuova finanza digitale vuole ripensare completamente infrastrutture di scambio per i pagamenti anche con denaro digitale, con modelli decentrati e autogestiti senza un regolatore del traffico, con prodotti di investimento digitali di varia natura anche non solo finanziaria, con nuove monete. Il futuro stesso della moneta, il suo ruolo e la sua natura possono essere messe in discussione dalla rivoluzione digitale della finanza. Alla base, come minimo comun denominatore, della DeFi (Decentralized Finance) c'è l'ecosistema della blockchain con i limiti tecnologici che si conoscono. Quella più conosciuta tra le crypto attività è il bitcoin il cui utilizzo si sta diffondendo anche in Italia, sta crescendo la sua "credibilità" come asset digitale di investimento, più che come mezzo di pagamento, alcuni intermediari del risparmio lo stanno proponendo come asset class per diversificare i portafogli di investimento.

Il valore delle cripto-attività è in rapida crescita e attualmente supera i duemilacinquecento miliardi di dollari. Si tratta di un ammontare che le banche centrali, giudicano in grado di generare potenziali rischi per la stabilità finanziaria e da non sottovalutare (esso supera il valore dei mutui subprime cartolarizzati che nel 2007- 2008 scatenarono la crisi finanziaria globale).

Il tema della digitalizzazione della moneta e della finanza digitale è ormai nell'agenda del G 7 e del G 20, delle banche centrali, della Commissione

Europea e del Parlamento europeo per le implicazioni e gli impatti sul sistema finanziario che può avere se non gestito opportunamente. Anche la BCE ha varato recentemente una iniziativa per valutare l'introduzione di un euro digitale, cioè una moneta elettronica emessa dalla banca centrale le cosidette CBDC.

L'euro digitale può avere conseguenze rilevanti su temi di carattere economico-finanziario, sia su aspetti di ampia rilevanza come gli equilibri geopolitici globali e i diritti fondamentali degli individui, quali la riservatezza.

L'euro digitale sarà una moneta sovrana offerta dalla BCE sotto forma elettronica, utilizzabile da chiunque per effettuare o ricevere pagamenti retail ovunque nell'area dell'euro. Esso fornirebbe ai cittadini i servizi che oggi essi ottengono dalle banconote: ossia l'accesso a uno strumento di pagamento sicuro, privo di costi, di facile utilizzo e accettato da tutti. L'euro digitale si affiancherà al contante senza sostituirlo e permetterà ai cittadini un accesso più ampio e agevole ai pagamenti elettronici, promuovendo l'inclusione finanziaria quindi anche a chi non ha un conto corrente bancario e, a differenza del contante, potrà essere utilizzato anche per le spese online. Essendo una moneta emessa della banca centrale, l'euro digitale non avrebbe alcun rischio – di mercato, di credito, di liquidità – come le banconote. L'euro digitale non ha nulla a che fare con le cripto-attività quale il bitcoin o le stable-coin che non sono emesse da alcun operatore. Esse sono create con programmi informatici per essere scambiate in piattaforme digitali con valori che oscillano in modo molto sensibile come dimostra l'andamento del valore del bitcoin anche negli ultimi mesi. I rischi che gli operatori finanziari e le banche centrali evidenziano è che alcune cripto-attività sono utilizzate per attività criminali e terroristiche, per l'evasione fiscale e sono anche facili bersagli di attacchi cyber. L'euro digitale differisce anche dalle cosiddette stablecoin, il cui valore è si legato a quello di un portafoglio di attività a basso rischio, quali valute o titoli, ma poiché manca una regolamentazione anche le stablecoinrisultano inadatte a svolgere le funzioni della moneta. Infatti, molte volte le riserve accantonate dagli operatori non sono sufficienti a garantire il rischio di insolvenza nel caso di riscatto degli investitori /utilizzatori, generando rischi di instabilità sull'intero mercato dell'asset a cui la stablecoin è agganciata. Inoltre, le stablecoin non sono state poi così "stabili" poiché un terzo delle iniziative avviate sul mercato negli ultimi anni è fallito.

Alcuni strumenti della finanza digitale possono portare innovazione ed efficienza agli utilizzatori e consumatori ma la crescita ancora incontrollata della finanza digitale decentralizzata a livello globale rendono i rischi maggiori delle opportunità e sono necessari interventi coordinati a livello globale.

Nel contesto appena descritto, l'euro digitale sarebbe uno strumento di stabilità al mondo della finanza digitale senza impattare sulle innovazioni che possono essere prodotte. L'esigenza di un euro digitale nasce anche dall'evoluzione delle abitudini di pagamento dei cittadini, da un lato sempre più portati ad utilizzare strumenti digitali, carte o mobile e dall'altro la crescita degli acquisti on-line. Le banconote saranno usate maggiore come riserva e meno come mezzo di pagamento: lo stock di contante

è in aumento e la quota delle banconote detenuta a fini di mezzo di pagamento è scesa al 20 per cento, dal 35 di quindici anni fa.

Se questa tendenza proseguisse, le banconote in futuro perderebbero importanza e diverrebbero un mezzo di pagamento marginale e l'impegno delle banche centrali a offrire il contante non basterebbe a preservarne il ruolo qualora la sua domanda come mezzo di pagamento divenisse insufficiente. I cittadini potrebbero quindi ritrovarsi privi di uno strumento sicuro e affidabile, offerto senza costi dallo Stato e accettato da tutti e sarebbe necessario introdurre una moneta digitale pubblica. Inoltre, oggi in Europa, oltre due terzi dei pagamenti digitali retail sono intermediati da operatori esteri che potrebbero acquisire ulteriore importanza, fino a sostituire i mezzi di pagamento esistenti sul mercato europeo. Per la BCE e i governi europei un sistema dei pagamenti e un settore finanziario dominati da operatori esteri sarebbero inadatti a sostenere la moneta unica. Il rischio di "colonizzazione" del sistema europeo dei pagamenti non è un pericolo remoto: dall'inizio del 2020 il valore delle stablecoinin circolazione è aumentato da 5 a 120 miliardi di dollari e contemporaneamente le Big Tech hanno ampliato l'attività in campo finanziario offrendo diversi servizi finanziari sulle loro piattaforme. Una non virtuosa convergenza di queste due tendenze potrebbe impattare il funzionamento dei mercati finanziari. Per evitare questi pericoli non solo va adeguato il quadro regolamentare ma anche gli operatori devono essere spinti ad offrire servizi finanziari efficienti e innovativi, in grado di rispondere alle esigenze di semplicità, velocità e trasparenza che stanno emergendo nella nostra società. L'introduzione dell'euro digitale deve andare in questa direzione e poter anche garantire la riservatezza dei dati così come la possibilità di continuare a utilizzare il contante. La realizzazione dell'euro digitale è un cammino complesso perché impatta su molte altre problematiche, dalla politica monetaria, al ruolo delle banche che non possono essere dis-intermediate. Il modello che la BCE sta seguendo è che l'euro digitale sarà introdotto in stretto raccordo con gli intermediari cui sarà delegata la distribuzione e l'offerta di servizi al pubblico e sarà compatibile con i servizi che essi offrono. Questo si ritiene debba stimolare l'innovazione: la nuova moneta fornirebbe agli intermediari un'infrastruttura capace di connettere sistemi oggi separati, come ad esempio le diverse modalità di pagamento al dettaglio, l'identità digitale, la firma digitale, le ricevute elettroniche. La moneta digitale renderebbe disponibili modalità di pagamento avanzate quali i pagamenti programmabili, gli acquisti online condizionati alla consegna del prodotto, i pagamenti in base all'utilizzo di un dato bene o servizio, i trasferimenti automatici di denaro da e per la pubblica amministrazione. A partire da queste innovazioni nei pagamenti, l'euro digitale può rappresentare un volano per modernizzare e rendere più efficiente il sistema finanziario e l'economia nel suo complesso. L'euro digitale rappresenta quindi un obiettivo ambizioso, complesso, in grado di innalzare l'efficienza del sistema economico e finanziario ma la BCE e l'Europa devono farlo con più speditezza perché molti paese stanno correndo, in particolare i grandi, come la Cina che sperimenterà già l'anno prossimo la sua valuta digitale.

Oscar di Montigny, Presidente di Flowe, Chief Innovation, Sustainability & Value Strategy Officer di Banca Mediolanum e Amministratore Delegato di Mediolanum Comunicazione

Green and blue: l'uomo è il principio e la fine

Emilio Mango, Managing Director
The Innovation Group

Per Oscar di Montigny non esiste sostenibilità senza mettere l'uomo al centro, e sugli investimenti in innovazione servirebbe un visione a lunghissimo periodo.

"Siamo una generazione che si è ritrovata, suo malgrado, in mezzo al guado. Siamo quelli che potrebbero non avere un futuro, a meno di un'inversione di rotta". A parlare è Oscar di Montigny, Presidente di Flowe, Chief Innovation, Sustainability & Value Strategy Officer di Banca Mediolanum e Amministratore Delegato di Mediolanum Comunicazione.

Di Montigny si è speso molto spesso sui temi della sostenibilità ma ancora di più sul concetto che lui stesso ha battezzato "humanovability", quell'incrocio tra innovazione, sostenibilità e centralità dell'essere umano che condensa, in un singolo neologismo, molto del suo pensiero.

Che cosa significa esattamente humanovability?

Il significato potrebbe sembrare scontato, in un'epoca dove l'innovazione, cioè l'alterazione dell'ordine costituito per creare cose nuove sembra una costante. In realtà i processi innovativi non sono mai scontati, in un certo senso vanno contro natura, perché coloro che molto spesso sono chiamati a innovare sono proprio quelli che l'ordine costituito l'hanno creato.

E come è cambiato il modo di fare innovazione?

Alla velocità con cui il mondo sta cambiando, l'innovazione, che prima era un modo per essere e sentirsi "cool", ora è una condizione necessaria per sopravvivere.
Ma questo non deve significare che vada fatta senza criterio: il

nuovo deve essere una risposta all'ambiguità e alla complessità che attanagliano la società moderna e allo stesso tempo deve essere sostenibile.

Come possiamo essere veramente sostenibili?

Al di là della tecnologia, il primo protagonista della sostenibilità deve essere senza dubbio l'uomo. È lui da cui parte e finisce tutto ed è lui a dover essere sostenibile prima delle imprese o delle organizzazioni. L'uomo deve avere pensieri puri, innovativi e sostenibili, affidarsi a sentimenti puri (amore, coraggio) e agire di conseguenza. Chiunque abbia capacità decisionali, nel pubblico e nel privato, dovrebbe avere come scopo ultimo il benessere dei suoi simili.

Come si colloca in questo contesto il greenwashing?

È esattamente il tentativo di mantenere l'ordine costituito, provando a far sembrare nuovo qualcosa che in effetti è vecchio. Chi fa greenwashing, senza mezzi termini, per quanto mi riguarda è solo un delinquente, qualcuno che non è capace di occuparsi dell'essere umano.

E la tecnologia digitale che ruolo ha?

È un abilitatore, ma più che di digitale io parlerei di innovazione tout court. Come ho già detto, però, tutto parte dall'uomo e dalla sua capacità di mettere idee e progetti nella scala dei tempi: ci sono innovazioni che riescono a dare benefici nel breve ma poi costituiscono un'incognita nel lungo periodo, così come ci sono investimenti e progetti che devono essere pianificati in un lasso temporale che supera quella della vita umana, un esercizio che pochi riescono a fare.

TIG Predictions: il mercato digitale nel 2021 e le attese per il 2022

Carmen Camarca, Analyst
The Innovation Group

L'accelerazione digitale verificatasi nel 2020 sta proseguendo anche nel 2021. Per l'anno in corso, infatti, The Innovation Group stima una crescita del mercato digitale pari al 5%, un dato che riflette, da un lato, il prolungamento dell'applicazione delle misure restrittive (e la conseguente necessaria conferma di alcuni "comportamenti digitali") e, dall'altro, la percezione che il graduale ritorno alla normalità non stia comportando un mero ripristino allo status quo. Tali fenomeni, seppur nel complesso postivi per l'andamento generale del mercato digitale (si ricorda che nel 2020 il mercato è stato sostanzialmente stabile, a differenza di altri settori produttivi che hanno registrato significative flessioni), non hanno impatti omogenei all'interno dei diversi segmenti che lo compongono, con il rischio, dunque, di ridisegnare le sue dinamiche interne.

Le performance dei segmenti del mercato digitale nel 2021

IT Tradizionale

Per quanto riguarda il segmento IT tradizionale, nel 2021 la perdita attesa è dello 0,3%. Il mercato, già in decrescita prima della diffusione del Covid-19 (e delle sue conseguenze), ha subito ulteriormente gli impatti negativi della crisi pandemica. In particolare, a decrescere nel 2021 sarà soprattutto la componente dei Servizi in quanto relativa ad applicazioni a cui si stanno sostituendo soluzioni sempre più evolute basate sull'utilizzo delle New Digital Technologies (al riguardo si considerino, ad esempio, i segmenti dell'ERP e CRM per cui si attende un progressivo spostamento da soluzioni on premise/proprietarie a soluzioni Cloud). Sempre per l'anno in corso, un migliore andamento si rileva, invece, per la componente Hardware grazie soprattutto al mercato dei PC (PC desktop, notebook, PC portatili), delle stampanti e dei monitor, un fenomeno dovuto al forte ricorso allo smart working e alla didattica a distanza rilevato negli ultimi mesi e supportato dall'introduzione da parte del Governo dei voucher per l'acquisto di device da utilizzare per le suddette attività.

NDT – New Digital Technologies

Per quanto riguarda il mercato NDT (New Digital Technologies), l'aumento atteso per il 2021 è del 7%. Il segmento per cui si registra la crescita maggiore è quello dei Servizi, dovuto principalmente alla significativa crescita del Cloud Pubblico, da ricondurre alla necessità di disporre di soluzioni as a service in grado di garantire la continuità del business anche da remoto, non si dimentichi, del resto, che l'esperimento forzato dello smart/home working ha portato

moltissime aziende ad accelerare il proprio percorso di migrazione al cloud. Si tratta di fenomeni che si sono affermati nel 2020 (anno in cui appunto si è verificato per la prima volta l'impatto della pandemia), riconfermati nel 2021 (a causa del prolungamento della situazione di emergenza e dell'applicazione delle conseguenti misure restrittive) e che in parte si ritiene proseguiranno anche nel 2022. In particolare, ciò avverrà considerando l'incertezza che ancora caratterizza la situazione pandemica e tenendo conto che, presumibilmente, molti dei fenomeni sviluppatisi in seguito all'emergenza saranno riconfermati anche una volta che questa sarà terminata: al riguardo si pensi, ad esempio, al tema del lavoro ibrido, da molti considerato la nuova frontiera delle modalità di svolgimento ed organizzazione del lavoro e caratterizzato dalla compresenza di smart working e lavoro in sede.

Ad avere un andamento positivo sono anche i servizi professionali (in cui rientrano i servizi per Collaboration, Security ed Internet Application): anche in questo caso si tratta di segmenti in cui la situazione emergenziale ha portato ad un aumento degli investimenti. Infine, per quanto riguarda la componente Hardware, se da un lato le perdite vengono limitate grazie alla domanda di device (Tablet, Ultrabook, dispositivi ibridi) utilizzati per smart/home working e didattica a distanza, una domanda sostenuta, come anticipato in precedenza, anche dai voucher messi a disposizione dal Governo per l'acquisto di un device, dall'altro si rileva la decrescita per il mercato degli smartphone: si stima che il deployment del 5G (e la commercializzazione dei relativi nuovi servizi che indurrà un aumento degli acquisti dei dispositivi) inizierà ad avere i suoi effetti a partire dal 2022.

Tuttavia, bisogna specificare che se da un lato si attende che l'affermazione del 5G darà un forte impulso al mercato degli smartphone, dall'altro la crisi globale dei chip degli ultimi mesi che sta impattando diversi settori (l'automotive in particolare) potrebbe causare dei rallentamenti anche in questo ambito con eventuali ritardi nella produzione degli smartphone.

TLC tradizionali

Per quanto riguarda il mercato delle TLC tradizionali, per il 2021 si rileva una crescita del 2,6%, soprattutto grazie alla crescita dei Servizi: l'aumento atteso è dovuto principalmente alla crescita del segmento degli apparati carrier (che fanno aumentare il mercato totale degli apparati del 3,8%) per l'aumento degli investimenti in infrastrutture per il 5G.

Elettronica di consumo

Si stima che nel 2021 il mercato dell'elettronica di consumo crescerà del 5,6%, trend positivo da ricondurre soprattutto al mercato dei videogiochi e al segmento della riproduzione video (che comprende le TV digitali). In quest'ultimo caso, in particolare, la crescita è dovuta, oltre che all'aumento del tempo trascorso in casa (che ha comportato un maggior ricorso alla fruizione di contenuti in streaming), anche all'acquisto di device di nuova generazione in seguito all'obbligo di cambiare lo standard delle TV (a partire dal 1° settembre 2021). Tale fenomeno (che insieme all'impatto di eventi sportivi quali gli Europei di calcio e le Olimpiadi) ha impattato positivamente anche sul mercato dei decoder. Similmente al 2021, ad avere effetti positivi sul mercato delle TV nel 2022 sarà anche l'effetto di alcuni eventi sportivi e in particolare dei mondiali di calcio.

Contenuti digitali

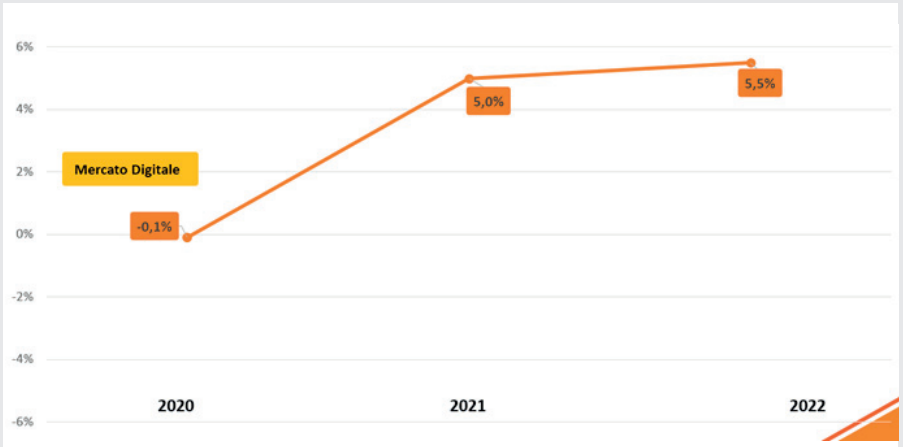
Nel 2021 per il segmento dei contenuti digitali si rileva una crescita del 6,6% (valore totale di circa 14,7 miliardi di euro) grazie soprattutto al software gaming (ciò avviene per le motivazioni analoghe al mercato dei videogiochi e impatta anche sul mercato del Cloud, soprattutto grazie alla preferenza verso le soluzioni on demand, as a service) e alla ripresa del segmento del digital advertising che nel 2020, a seguito del primo lockdown, aveva subito un arresto.

Infine, con riferimento agli altri contenuti digitali, la performance positiva per il 2021 è data in particolare dai servizi SVOD – Subscription Video on Demand, segmento che comprende aziende quali Netflix, Disney+, Amazon Prime. Per il 2021 si prevede che il mercato dei servizi SVOD subirà un'ulteriore crescita: oltre a ritenere che si tratti di servizi verso cui l'interesse proseguirà, si sta notando un innalzamento dei prezzi dei piani tariffari, fenomeno che non ha ancora colpito il mercato italiano ma che potrebbe avvenire presto.

Il rincaro potrebbe riguardare principalmente Netflix (principale player del settore) che, nonostante la "streaming war" (la forte competizione che caratterizza il mercato dello streaming), ha già applicato un aumento dei prezzi in diversi Paesi in cui è disponibile il servizio (si ritiene che ciò sia avvenuto principalmente per far fronte all'aumento delle spese che l'azienda sta sostenendo per creare nuovi contenuti di qualità).

Nel 2021 per i contenuti digitali si rileva una crescita del 6,6% grazie soprattutto al software gaming e alla ripresa del digital advertising

Andamento del mercato digitale 2020 – 2022e



Fonte: TIG, 2021

Le attese per il 2022

Nel 2022 si stima che il mercato digitale crescerà del 5,5%. La crescita sarà trainata principalmente dal segmento NDT – New Digital Technologies, una performance positiva dovuta soprattutto alla componente Software e Servizi e, in particolare, ai mercati ERP e CRM, oltre che alle soluzioni di Intelligenza Artificiale, Business Intelligence/Analytics e Cloud. Una crescita sostenuta si attende anche per i segmenti dell'elettronica di consumo e dei contenuti digitali, grazie alla conferma dell'interesse verso il mercato dei videogiochi (sia nella componente hardware sia in quella software gaming), oltre che della pubblicità e dei servizi SVOD. Proseguirà, invece, il rallentamento del segmento IT, venendo meno l'interesse verso determinati servizi o componenti hardware da ricondurre principalmente alla situazione emergenziale. Il mercato TLC, infine, limiterà le perdite grazie al deployment del 5G, i cui effetti si stima saranno visibili a partire dal 2022.

Lo scenario, seppur complessivamente positivo, rimane tuttavia incerto. Un primo aspetto che indurrebbe ad una maggiore cautela riguarda lo shortage di materie prime e in modo particolare di chip e semiconduttori che stanno provocando dei rallentamenti all'interno delle supply chain e potrebbero avere un impatto notevole su alcuni segmenti del mercato. Allo stesso tempo si rileva, all'interno del mercato del lavoro, un forte mismatch tra domanda e offerta di lavoro. È sempre più forte, infatti, la richiesta di determinate competenze (data scientist, data analyst, esperti di cybersecurity) che si ha difficoltà a reperire, correndo, da un lato, il rischio di creare un'inflazione di competenze (tale per cui si andrebbero ad offrire retribuzioni eccessivamente elevate per i profili più richiesti) e, dall'altro, di non essere in grado di cogliere a pieno il valore dello strumento digitale. Infine, la principale incognita riguarda l'applicazione degli investimenti previsti dal Piano Nazionale di Ripresa e Resilienza – PNRR (i cui primi effetti potrebbero essere visibili già a partire dalla seconda metà del 2022) e il contributo aggiuntivo che apporteranno alla crescita del mercato: molto dipenderà dall'effettiva capacità di "scaricare a terra" le risorse disponibili.

Se, dunque, il 2021 ci lascia con la consapevolezza che il digitale è destinato a ricoprire un ruolo sempre più rilevante, oltre che nella vita delle persone, anche all'interno delle dinamiche economiche del nostro Paese, il 2022 porta con sé ancora numerose incognite, oltre che il "peso" della responsabilità di applicare (e bene) le misure del PNRR.

8 Previsioni per la Cybersecurity nel 2022

Elena Vaciago, Associate Research Manager
The Innovation Group

Dopo due anni di pandemia, si chiude un 2021 piuttosto difficile per chi lavora nella cybersecurity. La situazione recente, con la scoperta a metà dicembre di una vulnerabilità zero-day del codice Log4j (una libreria presente in quasi ogni prodotto o servizio web Java), dimostra quali sono le difficoltà dei team di sicurezza, impegnati quotidianamente a chiudere falle e aggiornare sistemi.

Parlando di previsioni della cybersecurity per il prossimo anno, eviterò di ripetere banalità come "gli attacchi continueranno ad aumentare e diventeranno sempre più sofisticati" o "gli attaccanti guadagneranno milioni con il ransomware" o ancora "le aziende, procedendo nella digitalizzazione, avranno una superfice d'attacco maggiore da controllare". Questi sono fatti noti.

Mi concentrerò invece nell'indicare sia alcune tendenze evolutive (che in sostanza partono dall'attualità e la proiettano ai prossimi mesi), sia anche le novità che potrebbero verosimilmente comparire nel 2022.

Le "tendenze evolutive" nel prossimo anno saranno:

Gli attaccanti troveranno nuovi metodi per monetizzare gli attacchi

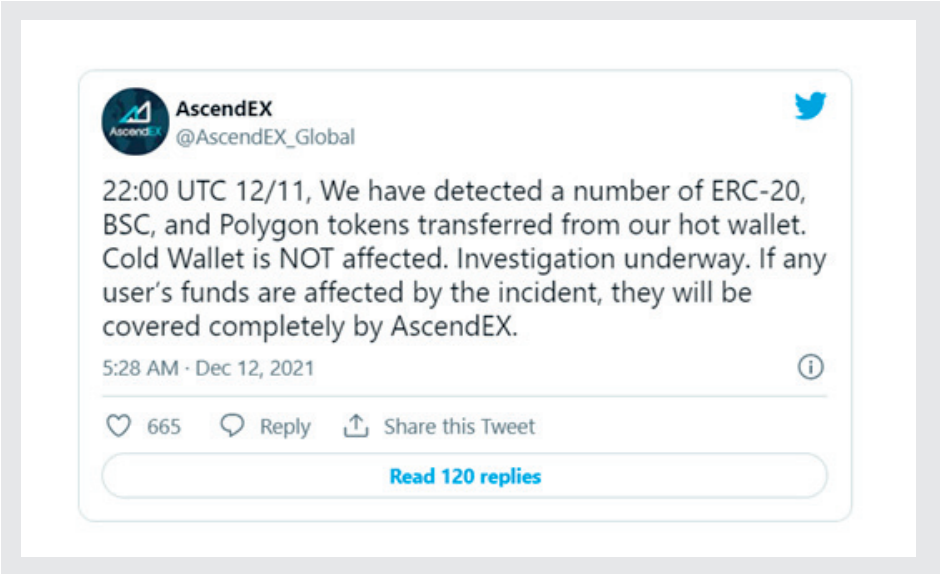
Nel 2021, la minaccia che ha raccolto maggiore interesse, perché molto visibile, è stata senza alcun dubbio il ransomware. Ha fatto vittime in tutti i settori e in qualsiasi dimensione d'azienda, e molto probabilmente rimarrà ancora per molto tempo il tema di sicurezza più temuto dalle aziende. I gruppi specializzati in questi attacchi hanno grandi capacità nel far evolvere continuamente obiettivi e tattiche, sia per quanto riguarda gli schemi di estorsione sempre

più complicati e temibili, sia per quanto riguarda l'esfiltrazione e la cifratura dei dati. Con la pandemia vettori comuni per il ransomware sono state le VPN, le porte esposte RDP e le mail di spear phishing. Nel futuro vedremo invece un incremento del ransomware indirizzato a nuove superfici di attacco, come il cloud o l'IoT.

Nei propri obiettivi di monetizzazione, gli attaccanti si spingeranno però oltre il ransomware: oggi almeno 2 altri ambiti sono fonti di grandi guadagni. Da un lato, il Malicious Cryptomining, o Cryptojacking, utilizzato dagli hacker per trasformare computer infetti in "miniere" di criptovalute.

Si stima che milioni di computer in tutto il mondo siano stati infettati da malware di cryptomining, a insaputa dei loro proprietari, con risorse di elaborazione ed energia sfruttati dal cyber crime per generare criptovaluta. Dall'altro lato, con la crescita del valore delle valute digitali, sta diventando molto comune l'hacking di portafogli di criptovalute direttamente nei marketplace e negli exchange. Si calcola che nel 2021 ci siano stati almeno 169 incidenti riguardanti il furto di criptovalute, con perdite intorno ai 7 miliardi di dollari.

Il 12 dicembre si è saputo, ad esempio, che la piattaforma di trading di criptovalute AscendEX aveva subito un furto di 77,7 milioni di dollari: sembra che gli hacker siano riusciti a compromettere l'hot wallet, potendo quindi trafugare i token ospitati sulle blockchain Ethereum, Binance Smart Chain e Polygon.



La frequenza con cui avvengono questi incidenti fa temere per la scarsa sicurezza dei wallet e delle piattaforme di trading, come se, nella velocità con cui questi marketplace sono stati realizzati, siano rimaste molte vulnerabilità dovute al processo di sviluppo applicativo troppo rapido.

Le aziende investiranno maggiormente per rendere sicuro l'uso del cloud

Negli ultimi 2 anni, la pandemia ha favorito un esteso ricorso al cloud, per supportare il lavoro ibrido e facilitare i nuovi processi di collaborazione online. Ora è però il momento di gestire con più sicurezza il cloud: alcuni provider si distingueranno nei prossimi anni dagli altri per la capacità di rispondere a questa domanda di maggiore sicurezza. Le aziende invece si rivolgeranno sempre di più ad adottare strategie multi-cloud, per rispondere ad esigenze come elevata disponibilità, prezzo, offerte commerciali e altro. Sarà fondamentale quindi poter utilizzare soluzioni di sicurezza in grado di fornire una visibilità omogenea verso un range di piattaforme e risorse in cloud.

Focus sulla sicurezza applicativa: SHIFT LEFT e SHIFT RIGHT

Oggi il tema è garantire non soltanto la sicurezza dei nuovi sviluppi ("shift left", ossia avere un security-by-design per le nuove app), ma anche, soprattutto (come ha dimostrato in questi giorni l'enorme attenzione alla vulnerabilità di Java) quella di una gran quantità di software già in produzione ("Shift right").

Crescita della rilevanza della Supply Chain Security

A partire dall'attaccoSolarWinds nel dicembre 2020, per passare poi a quelli del 2021, da Colonial Pipeline a Kaseya, sono stati osservati attacchi alle supply chain sempre più gravi. Oggi nessuno mette in discussione la necessità di controllare meglio la sicurezza lungo intere filiere: nelle aziende vedremo sempre più spesso team dedicati alla gestione delle terze parti, attivi non soltanto nel controllare (con monitoraggio e audit) la sicurezza delle transazioni con terze parti, ma di adottare

anche approcci più proattivi per elevare una resilienza di sistema in filiere sempre più interconnesse.

Maggiore adozione di norme per la Privacy a livello globale

Ci si aspetta che nel 2022 vedremo un'adozione sempre più estesa a livello globale di norme a difesa della privacy delle persone, con una migliore supervisione quindi delle modalità con cui sono trattati i dati riferiti alle persone nella nuova economia digitale. In particolare, dopo l'adozione del GDPR in Europa (nel 2018) e quindi del California Consumer Privacy Act (CCPA), e regolamenti analoghi in Cina e Brasile, il 2022 sarà l'anno per legislazioni simili in Paesi in cui non sono ancora formalizzate, come Giappone, India, altri Stati americani. Con l'arrivo di nuove norme, si alzerà il rischio per le grandi multinazionali di incorrere in multe superiori, soprattutto per data breach che vadano a impattare contemporaneamente su consumatori e clienti dislocati in più Paesi.

Parlando invece delle tendenze nuove della cybersecurity, queste potrebbero essere già nel 2022 le seguenti:

Nuove forme di attacco AI-enabled

Un primo esempio di come potrebbero essere sfruttate tecniche AI-enabled per realizzare frodi su internet è quello dei Deepfake, video modificati in cui a personaggi famosi sono messe in bocca parole in realtà mai dette. Oggi la personificazione di terzi avviene sia con video sia con audio, e ha raggiunto un livello di realismo molto elevato: mimetizzandosi dietro qualcuno, gli attaccanti riescono a perpetrare frodi del tutto nuove. L'interesse per i Deepfake registrato nei dark market è in continua crescita. Il futuro ci riserva ulteriori forme di attacco che faranno leva sempre più su tecniche importate dall'intelligenza artificiale.

Azioni più decise per contrastare il cyber crime da parte dei Governi

In molti Paesi vedremo il prossimo anno iniziative molto più decise nel contrasto al cyber crime. L'Executive Order di Biden del 2021 ha sottolineato la necessità di assumere un ruolo non solo difensivo, piuttosto anche proattivo nella prevenzione dei crimini online. In passato, le azioni di contrasto delle forze dell'ordine erano spesso limitate dalla mancanza di una normativa in materia. Con il coinvolgimento diretto dei Governi, questo passaggio sarà presto colmato. Anche in Italia, l'istituzione dell'Agenzia per la cybersicurezza nazionale (ACN) rappresenta un passo avanti importante nella capacità di rendere più efficace una risposta coordinata nel Paese.

In futuro è probabile che le azioni di Law enforcement contro i cyber criminali assumano forme più decise. Potrebbero arrivare leggi che impediscono di pagare estorsioni legate a ransomware; la chiusura di exchange di criptovalute utilizzati dai cyber criminali per raccogliere i fondi; una maggiore collaborazione tra le polizie a livello internazionale nella cattura ed estradizione delle cyber gang.

Security due diligence: diventerà centrale nelle operazioni M&A

Via via che le aziende diventano più mature nella valutazione della bontà di un programma di Cyber Risk Management, aumenta anche la comprensione sull'effettiva Security Posture di una terza parte. Ecco, quindi, che il valore di un'acquisizione societaria comincia a dipendere anche dalle misure in essere in campo cybersecurity, e per minimizzare il rischio di incorrere in futuri danni di immagine, si comincia a svolgere un'attività preliminare di Due Diligence. Questa sarà sempre più volta a verificare (ad esempio con un vulnerability scanning, o con un audit dei processi di sicurezza e compliance in atto) l'effettiva efficacia delle scelte di cybersecurity dell'organizzazione sotto scrutinio.

Privacy by design e sviluppo: l'importanza della compliance software

Valentina Frediani, General Manager

Colin & Partners

L'articolo 25 del GDPR si concentra su principi fondamentali: privacy by design e privacy by default. Essi si applicano in modo specifico al mercato delle soluzioni e applicazioni IT, coinvolgendo l'intero ciclo, dallo sviluppo all'implementazione.

Requisito e obiettivo di questa parte della normativa è rendere la responsabilità dei titolari consapevole rispetto alle scelte effettuate, coniugando la necessità di dimostrare quali misure sono state adottate a tutela dei dati.

Di questo tratta il principio di privacy by design che, operando in coerenza con quello di accountability, richiede, sul piano pratico, il coinvolgimento diretto dei titolari rispetto alle misure scelte.

Le misure tecniche

Partendo da quelle "tecniche" si può dire che esse rappresentino parametri e soluzioni di protezione che mirano a limitare e ridurre il più possibile e in modo efficace il rischio di violazione, furto o perdita, dei dati.

Non vengono definite in maniera specifica e dettagliata ma si lascia alla libera scelta del titolare attuare le azioni che ritiene più idonee, in modo da consentirne la variazione a seconda della specificità del business piuttosto che della tecnologia utilizzata, dei dati trattati, delle finalità e di tutte quelle variabili che possono intervenire.

L'articolo 32 ne richiama, tuttavia, alcune che fungono da guida di base per chi sviluppa, implementa o deve valutare, anche in fase post-sviluppo, il grado di compliance delle soluzioni realizzate.

Si parla dunque, di pseudonimizzazione e minimizzazione dei dati, per evitare l'immediata e semplice associazione del dato al soggetto fisico a cui si riferisce.

Sono citate anche cifratura, capacità di ripristino ed accesso ai dati e garanzia della riservatezza.

Le misure organizzative

Nella categoria delle misure organizzative, alle quali fa riferimento sempre l'articolo 25 GDPR, sono raggruppate tutte le misure volte a disciplinare la creazione e la gestione dei profili di autorizzazione compresi quelli degli amministratori di sistema o ancora le modalità di verifica delle misure di sicurezza da adottare in caso di implementazione.

Nel caso in cui un Fornitore voglia rilasciare un software "chiuso", non personalizzabile, la sua responsabilità rispetto ai criteri di sicurezza applicati, si accresce. Occorrerà, quindi, formalizzare tutte le ipotesi e le responsabilità a livello contrattuale, dando evidenza dell'impossibilità di intervento da parte del Cliente.

Obblighi e responsabilità di Titolari e Fornitori

Più complesso può risultare la lettura delle responsabilità giuridiche di chi realizza un software e di chi invece lo acquisisce. Si tratta, però, di un nodo fondamentale che deve sempre essere sciolto, da imprese ed enti, a tutela degli investimenti programmati, evitando i rischi di progetti che comprendano soluzioni non conformi.

In fase di acquisto o commissione di sviluppo di una soluzione, il Titolare del trattamento è obbligato a realizzare una valutazione delle misure – sia tecniche che organizzative – che prevede di adottare. Non sempre, a livello pratico, questa via è percorribile; capita, quindi, che la responsabilità del controllo venga trasferita al Fornitore. Quest'ultimo, per non entrare in contrasto con il principio di accountability, dovrà assicurare la possibilità di settare le diverse funzioni a discrezione del Titolare (si pensi, ad esempio, alla cancellazione dei dati o ai profili di autorizzazioni).

Nel caso in cui un Fornitore voglia rilasciare un software "chiuso", non personalizzabile, la sua responsabilità rispetto ai criteri di sicurezza applicati, si accresce. Occorrerà, quindi, formalizzare tutte le ipotesi e le responsabilità a livello contrattuale, dando evidenza dell'impossibilità di intervento da parte del Cliente.

Escludendo il settore di Enti e PA, che operano attraverso bandi e gare, nel privato una prassi di acquisizione della documentazione che attesti l'effettiva e comprovata conformità normativa del software viaggia ancora a rilento, esponendo le imprese a conseguenze giuridiche di non poco conto.

I comportamenti più corretti

Due sono gli step fondamentali: la verifica preliminare della soluzione da parte del Titolare rispetto ai principi e alle misure applicate alle diverse tipologie di dati di cui è Titolare e rispetto alle scelte perseguite. Il secondo riguarda il Fornitore che dovrà attuare, a sua volta, verifica di conformità del software per quanto riguarda la tipologia di dati trattati, le misure tecniche impostate ed impostabili, le procedure organizzative di rilascio, il caricamento dati e amministrazione del sistema, nonché la contrattualizzazione delle specifiche responsabilità. Si tratta di passi fondanti ma non necessariamente sufficienti per ogni casistica possibile. Per questo occorre sempre affidarsi a un'analisi accurata e centrata sulla propria realtà di business.

Luci e ombre sull'Intelligenza Artificiale applicata ai social media

Andrea Boscaro, Partner
The Vortex

> **Gli algoritmi ci osservano mentre li utilizziamo e registrano non solo i nostri comportamenti, ma anche le variazioni di questi ultimi per individuare nuove opportunità**

Gli studiosi di storia dell'arte si sono sempre interrogati sulle ragioni per le quali i mosaici bizantini siano ricchi di personaggi ritratti con fattezze non realistiche, ma soprattutto con gli occhi fissi e sgranati, rivolti verso l'osservatore: alcuni sostengono che questi sguardi vogliono trasmettere l'idea che quelle donne e quegli uomini siano già arrivati alla mèta e, da un luogo senza tempo, ci guardino. Sono loro, a ben vedere, a guardare noi e non viceversa.

Come quei nostri antenati raffigurati nelle basiliche, nei mausolei, nei battisteri di Ravenna, anche gli algoritmi ci osservano mentre li utilizziamo e registrano non solo i nostri comportamenti, ma anche le variazioni di questi ultimi per individuare nuove opportunità da cogliere così da restituire suggerimenti editoriali, commerciali e pubblicitari sempre più pertinenti e coinvolgenti.

Nel corso degli ultimi due anni, due episodi hanno dimostrato come gli algoritmi di intelligenza artificiale applicati al mondo dei social media siano stati utilizzati per adempiere ad obblighi imposti dalla legge anche se con luci e ombre.

Nel provvedimento con il quale il Garante della Privacy italiano ha imposto a TikTok lo scorso 9 febbraio il blocco dei profili degli under 13 si fa esplicito riferimento all'opportunità di avvalersi dell'IA per comprendere l'età degli iscritti e decidere di inibire loro la partecipazione al social network: ne è derivato che dal 21 aprile sono stati più di 12 milioni e mezzo gli utenti italiani ai quali è stato chiesto di confermare di avere più di 13 anni per accedere alla piattaforma e sono stati quasi 550 mila gli utenti rimossi perché probabili under 13: circa 400 mila perché lo hanno dichiarato esplicitamente e 150 mila attraverso una combinazione di moderazione umana e strumenti di segnalazione implementati all'interno dell'app che si sono avvalsi dell'intelligenza artificiale.

L'analisi degli interessi desunti dalla visualizzazione dei contenuti e della rete dei collegamenti ha consentito tale intervento e dimostra, anche in termini numerici, il peso con il quale un software è intervenuto in una scelta delicata per i minori e strategica per lo sviluppo del social network.

Ancor più interessante è come sta cambiando l'uso degli algoritmi nella moderazione dei contenuti da parte di Facebook e nell'integrazione con l'attività manuale. Oltre all'Oversight Board indipendente che dallo scorso anno opera da "giudice di ultima istanza", quindicimila sono infatti i manual checkers che, in tutto il mondo, supportano Facebook nella moderazione dei contenuti. E' un numero che appare rilevante, ma che si può ben comprendere di fronte alla valutazione che lo stesso social network ha fatto lo scorso autunno: nel 2020 sono infatti stati pubblicati 22,1 milioni di contenuti di incitamento all'odio, 19,2 milioni di immagini violente, 12,4 milioni di foto connotate da nudità infantile e 3,5 milioni di post legati al bullismo ed alle modestie. Se il 94,7% di tale materiale è stato rilevato dai software di intelligenza artificiale, l'apporto umano resta dunque determinante nel valutare il materiale e deciderne la cancellazione, ma anche nell'identificare i casi dei quali gli algoritmi non riescono ad interpretare il significato.

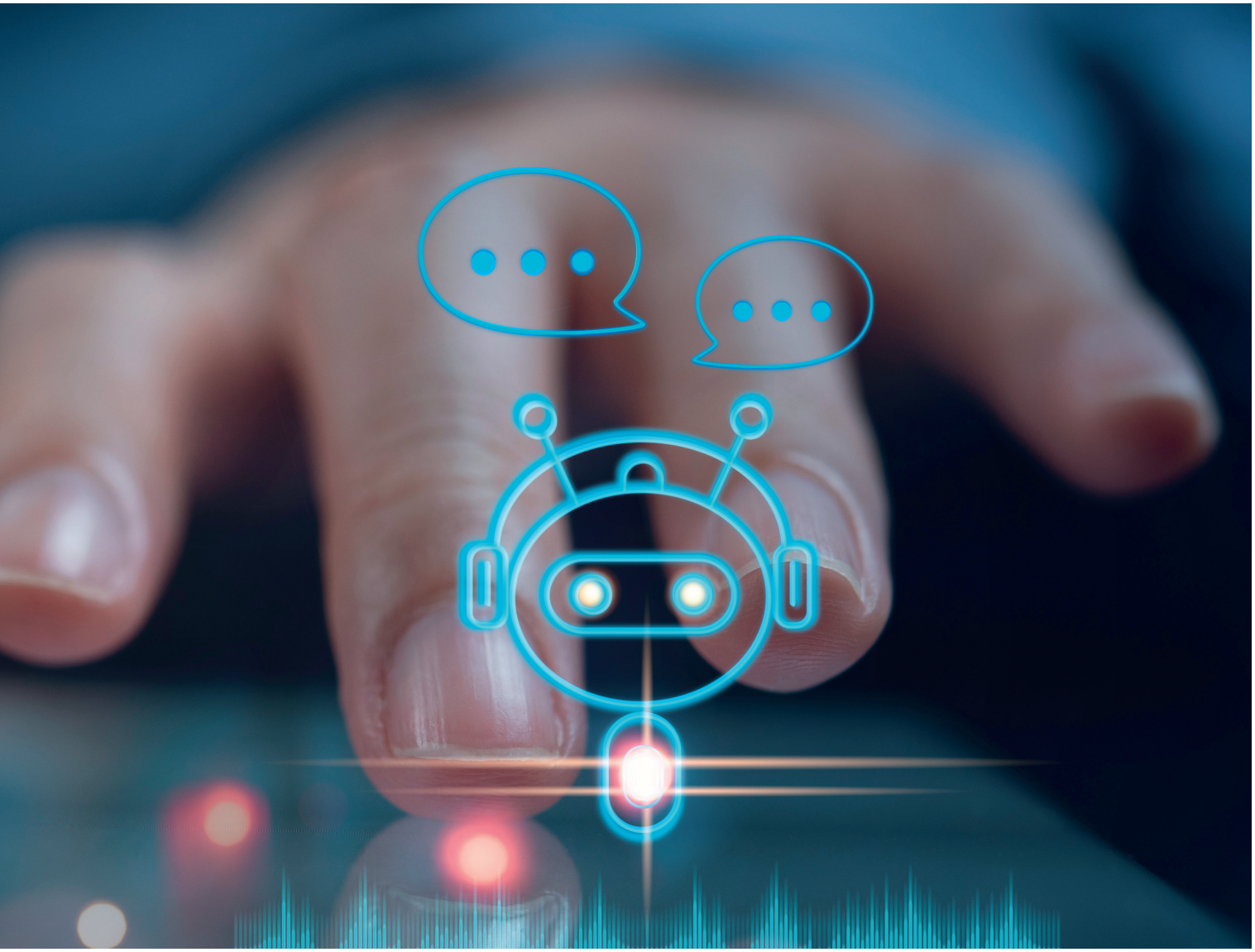
In uno scenario connotato da vere e proprie campagne organizzate ed orientate a obiettivi di propaganda sociale e politica, risulta pertanto chiaro quanto sia importante che il sistema funzioni e che, come chiede il Digital Services Act, siano trasparenti i criteri adottati e tempestivi gli interventi attuati sia nella fase di vaglio prodotta dagli algoritmi che nella fase di revisione manuale da parte dei controllori.

Il responsabile di Facebook, Chris Palow, ha ammesso infatti che la

tecnologia manca della capacità di un essere umano di giudicare il contesto di molte comunicazioni online, soprattutto con argomenti come disinformazione, bullismo e molestie per via della mancanza di informazioni precedenti o di fronte a errori di valutazione causati da pregiudizi o fraintendimenti ed ha dichiarato: "Il sistema consiste nel far sposare intelligenza artificiale e revisori umani per fare meno errori".

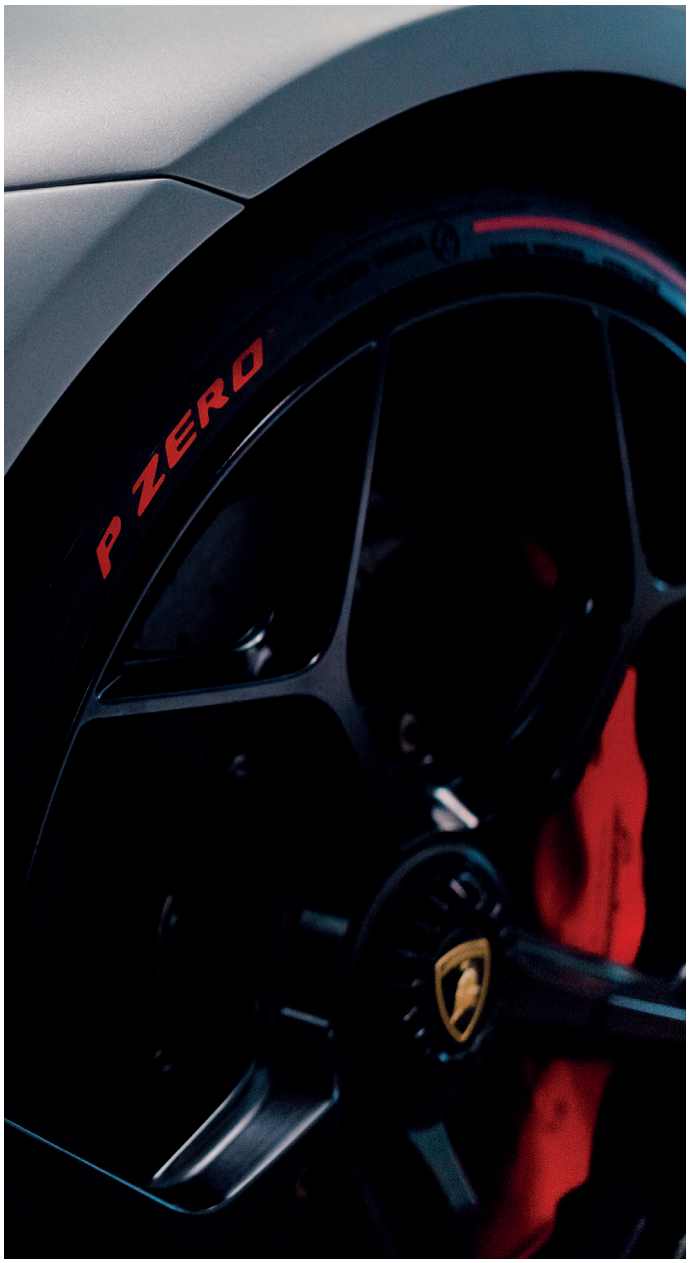
Che il futuro veda un maggiore, e non minore, ruolo dell'essere umano è evidente se si pensa all'intento, da parte di Facebook, di affidare all'IA il compito di selezionare e ordinare i contenuti che dovranno essere valutati dai revisori, dall'attuale ordine cronologico ad un diverso ordine improntato alla pericolosità, una combinazione di potenziale gravità dei messaggi in virtù del loro contenuto, di probabilità che il post infranga le regole della piattaforma e di viralità rilevata in termini di reazioni, visualizzazioni e condivisioni maggiori.

Forse anche per questa componente manuale e dunque organizzativa, lo sprone continuo da parte delle istituzioni e dell'opinione pubblica verso un maggiore investimento da parte del social network non è superfluo, ma utile e appropriato.



Pirelli sfreccia sulla strada della trasformazione digitale

Roberto Bonino
Giornalista, Research and Content Manager
The Innovation Group



Percorriamo con il senior vice-president & chief digital officer della società, Pier Paolo Tamma, le fasi di un processo evolutivo tuttora in corso e fortemente centrato sulla pianificazione.

Dopo aver attraversato diverse fasi storiche ed esplorato altri settori, Pirelli è oggi una realtà focalizzata sul core business degli pneumatici, in particolare per i modelli di fascia alta del mercato Premium e Prestige. Nel tempo, sono state definite partnership con le più importanti case automobilistiche, per la co-progettazione dei modelli specifici che andranno montati su ogni vettura.

In questa fase, l'azienda è pronta ad affrontare le nuove sfide del mercato con il supporto di una visione strategica che fa leva in modo consistente sulla tecnologia. La trasformazione si fonda sulla capacità di saper pianificare tutte le fasi che compongono il business della società. Da qui è nato ciò che è stato battezzato Integrated Operating Model, ovvero il disegno complessivo che dettaglia le fasi di un cambiamento che ha come obiettivo la fidelizzazione totale del parco di costruttori presidiato (oggi più dell'80% ricompra pneumatici Pirelli) e l'ampliamento delle quote di mercato su ogni singola casa automobilistica.

Il percorso di trasformazione digitale, iniziato circa tre anni fa, ha tratto spunto dal modello così approntato e si è dipanato su quattro stream di lavoro, destinati a ridisegnare le vendite, la pianificazione complessiva, lo sviluppo del prodotto e la produzione.

La prima componente ad aver subito un processo di trasformazione digitale è stata quella commerciale: "Grazie all'evoluzione costruita sul Crm di Salesforce",

conferma Pier Paolo Tamma, senior vice-president & chief digital officer di Pirelli, “ogni venditore è oggi in grado di mostrare ai dealer di sua competenza quale sia il parco circolante del loro territorio, nel segmento che ci interessa, in quale misura esso sia presidiato dai prodotti Pirelli e quante vetture saranno interessate da un primo o secondo ciclo di ricambio nei successivi mesi. Da questo ricaviamo quale sarà la domanda potenziale che il dealer riceverà dal mercato, riuscendo a tarare la migliore proposta commerciale, dandogli visibilità sull’approvvigionamento del quale avrà necessità”.

In questa fase, Pirelli sta lavorando sulle componenti di pianificazione strategica, facendo leva sulla conoscenza della domanda a lungo termine per bilanciare i carichi di lavoro sui 18 stabilimenti del gruppo o addirittura pensare di costruire con anticipo un nuovo impianto: “Il sistema che stiamo mettendo a punto è basato sulla tecnologia di o9 e consente anche di fare simulazioni su tutta la nostra catena”, illustra Tamma. “Ogni volta che riceviamo da una casa costruttrice la richiesta di sviluppare un nuovo pneumatico, riusciamo a proiettare l’impatto su tutto il processo a monte, arrivando a capire quanto sarà profittevole il nuovo business anche grazie alla domanda che genererà nel mercato del ricambio. Questa pianificazione consentirà di controllare meglio tutta la filiera, dalla produzione, alla logistica, fino al percorso delle materie prime”.

In prospettiva, Pirelli ha messo in cantiere altre due aree di trasformazione a forte connotazione digitale. Un primo ambito riguarda lo sviluppo dei prodotti. L’azienda sviluppa circa trecento nuovi progetti all’anno, ma ciascuno ha una durata indicativa di tre anni, quindi ce ne sono circa mille attivi in parallelo. Poter ricavare efficienza da questa complessità è un elemento di comprensibile importanza: “Abbiamo pianificato di implementare la piattaforma Plm di Dassault e stiamo realizzando algoritmi di intelligenza artificiale che consentano di riutilizzare il lavoro già fatto nel caso di sviluppi su vetture assimilabili, di stimare gli elementi che servono e di effettuare simulazioni senza dover creare prototipi fisici. L’esito finale sarà una piattaforma in grado di gestire un processo end-to-end fino al fine ciclo di vita dello pneumatico”, sottolinea Tamma

L’altra area di trasformazione di medio termine riguarda la produzione industriale, dove l’esigenza di fondo riguarda un’ottimizzazione destinata a coinvolgere un insieme di fabbriche impegnate, ognuna con complessità diverse, su un’ampia varietà di prodotti. L’evoluzione prevista si fonderà su una piattaforma di Industrial IoT (Internet of Things), che dovrà consentire di estrarre in tempo reale i dati dalle macchine e generare pattern utili per rendere più efficiente la produzione anche per singolo stabilimento, sulla base delle informazioni sulle caratteristiche dell’impianto, del prodotto e della base storica già acquisita.

Intervista a
Antonio Fumagalli, Chief Information Officer dell'Azienda Socio Sanitaria Territoriale (A.S.S.T.) Papa Giovanni XXIII di Bergamo

Sanità sotto attacco cyber: come impostare la risposta

Elena Vaciago, Associate Research Manager
The Innovation Group

Gli Enti Sanitari sono sempre più spesso presi di mira dagli hacker. Come ha rilevato un'analisi Swascan di inizio ottobre 2021, il rischio di "data breach" e di interruzione delle attività per 'ransomware' nel mondo ospedaliero è molto cresciuto negli ultimi anni. Su un campione di 20 enti sanitari italiani analizzati con il SOC del security provider, solo 4 hanno passato l'esame senza dimostrarsi vulnerabili. Per gli altri 16 ospedali sono emersi 942 problemi di natura tecnica, 239 indirizzi IP esposti su Internet, 9.355 indirizzi e-mail compromessi, 579 portali di accesso, console o servizi di database accessibili dall'esterno. Nel settore sanitario il Ransomware è oggi la minaccia più pericolosa: oltre al danno informatico immediato, procura l'arresto dei servizi, danni di reputazione ed economici, tra cui multe salate prescritte dal GDPR, il regolamento europeo per la protezione dei dati personali. È proprio il valore delle informazioni sanitarie a rendere questo settore molto appetibile, tanto che recenti indagini lo posizionano al terzo posto tra quelli più attaccati.
Come riporta lo speciale di Milena Gabanelli sul Corriere, il prezzo di una cartella clinica sul dark web tocca oggi i 1.000 dollari, mentre il prezzo di una carta di credito rubata, secondo Privacy Affairs, oscilla tra i 17 e i 65 dollari. Se poi i dati sanitari sono corredati di un "kit di identità" costruito dai cyber criminali per la singola persona, si arriva fino a 2.000 dollari.

Per comprendere quali siano le strategie da mettere in atto per mitigare il rischio informatico, aggravato dalla pandemia (dati esfiltrati, sistemi di prenotazione

bloccati), abbiamo intervistato Antonio Fumagalli, Chief Information Officer dell'Azienda Socio Sanitaria Territoriale (A.S.S.T.) Papa Giovanni XXIII di Bergamo.

Cosa è cambiato nell'ultimo periodo? Come mai le aziende ospedaliere si trovano oggi ad affrontare questa emergenza in ambito 'cybersecurity'?

L'urgenza non è dettata dal fatto che ci si accorga adesso della sicurezza, in quanto questo tema è noto da anni. Oggi però sono aumentati moltissimo gli attacchi. Il percorso per la cybersecurity era già avviato da tempo nel mondo ospedaliero italiano: oggi è però necessario rinforzare le difese, potenziarle,

essere in grado di affrontare anche le situazioni più pressanti.

Come migliorare quindi? Cosa è diventato prioritario?

Da un lato è sicuramente importante dotarsi di strumenti nuovi, più performanti nell'elevare le difese, nel ridurre i rischi e nell'aiutare ad affrontare questi problemi. Dall'altro lato, bisogna rendere sempre più consapevoli gli operatori e gli utenti di strumenti informatici, di quali sono i rischi reali che corrono. Nonostante tutta la tecnologia, se poi un operatore clicca su una mail che ha superato l'antispam, le sandbox e altro, l'attaccante entra. Quindi è soprattutto la consapevolezza dei rischi a fermare un attacco (anche se chiaramente gli strumenti devono esserci se vogliamo ridurre le vulnerabilità).

Le strategie che serviranno maggiormente in futuro saranno quelle basate su modalità di affrontare i problemi più formali, industrializzate, scientifiche. In aggiunta, serviranno sempre di più persone esperte per gestire e controllare gli strumenti di cybersecurity. Stanno arrivando gli investimenti del PNRR, aiuteranno sicuramente a individuare le misure più adatte al singolo ambito, bisognerà però implementarle, farle funzionare, dotarsi di competenze: per farlo non basteranno le poche risorse interne, bisognerà rivolgersi ad esperti e a società esterne in grado di erogare servizi gestiti.

Oggi molti attacchi arrivano con il phishing e sfruttano le debolezze degli utenti: come rafforzare la gestione delle identità? Nel mondo della sanità vale il discorso dell'autenticazione multifattore?

Noi da 10 anni abbiamo un

sistema di gestione delle identità digitali basato su smart card con certificato digitale; quindi, 'strong authentication' e 'Single-sign-on'. È importante però trovare un corretto bilanciamento: se un infermiere segue più malati un reparto, ogni paziente avrà il suo computer con cartella clinica elettronica che monitora la sua condizione clinica, l'infermiere dovrà quindi gestire con la sua tessera più procedure di autenticazione.

Serve un bilanciamento tra esigenze di sicurezza e operative.

La pandemia ha poi spinto l'Home Working, quindi, il tema della VPN e del secondo fattore di autenticazione va considerato con attenzione. Se uso le solite credenziali con utente e password, la sicurezza non è sufficiente, anche se ho la VPN.

Negli Ospedali i sistemi medicali hanno bisogno di essere gestiti dal punto di vista della sicurezza così come PC, reti e server: quali difficoltà si incontrano?

Nella pratica la situazione non è sempre ottimale: i sistemi medicali non sono computer classici, devono avere una gestione specifica. Oggi negli ospedali usiamo ancora macchine XP, che non possono essere eliminate perché collegate a una serie di altri strumenti. Sicuramente però nelle specifiche dei nuovi acquisti vanno inseriti requisiti di sicurezza, tra cui la possibilità di effettuare il 'patch' delle macchine in qualsiasi momento sia opportuno, o sia richiesto dalle norme. Così come deve essere possibile testare la resilienza e la sicurezza di questi sistemi, che svolgono operazioni critiche sulle persone.

Se possiamo eseguire un 'penetration test' più volte all'anno sui PC delle cartelle cliniche, che contengono dati sensibili, non si vede perché non sia possibile farlo sui sistemi medicali. I fornitori dovranno impegnarsi formalmente a garantire l'aggiornamento del sistema operativo di queste macchine per un numero certo di anni.

Parliamo di sicurezza applicativa, legata quindi a nuovi applicativi ospedalieri: come regolarsi?

Il 98% del nostro patrimonio applicativo (parliamo di 170 – 180 applicazioni) fa riferimento a fornitori esterni. Quello che possiamo fare di nuovo è avere requisiti nelle gare d'acquisto, ad esempio per la compliance al GDPR, o per garantire che l'applicazione continui a funzionare quando aggiorno il sistema operativo delle macchine, e così via. Su un prodotto commerciale, si potrebbe in teoria, almeno per le parti sviluppate custom, fare dei test di sicurezza sul codice con strumenti ad hoc. In pratica però è molto difficile da realizzare, e comporta investimenti che dovrebbero ricadere sul fornitore esterno.

Con riferimento all'utilizzo del cloud per le applicazioni, nelle prossime gare avremo nuovi servizi (un esempio è il trasporto di persone ed emoderivati) che saranno corredati da software specifico, software che quindi ci sarà fornito 'in cloud' come servizio realizzato esternamente. Di nuovo, la nostra risposta sarà puntare a fissare requisiti di sicurezza informatica molto stringenti.

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