

LUGLIO 2022



11  
111  
101  
100110  
11

# IL CAFFÈ DIGITALE



## CRYPTOVALUTE E MERCATI DIGITALI: LA BUFERA DI OGGI PASSERÀ

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

**Francesco Fiaschi,  
CTO di Autostrade per l'Italia**

**ICT ECOSYSTEM**

**IT Ecosystem Summit 2022,  
i nuovi ruoli dei fornitori IT  
alle prese con il PNRR**

**CONNECTED MOBILITY**

**2035, anno zero per i motori  
benzina e diesel**

## IL TEAM DEL CAFFÈ DIGITALE

---



**Roberto MASIERO**  
Presidente  
*The Innovation Group*



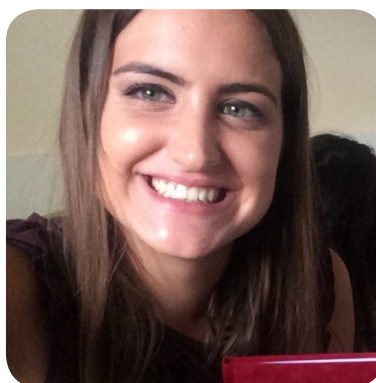
**Ezio VIOLA**  
Co-founder  
*The Innovation Group*



**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**  
*ICT Ecosystem*

**3**

**L'EDITORIALE**

**Cryptovalute e mercati digitali:  
la bufera di oggi passerà**

**Ezio Viola**

**6**

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



**Francesco  
Fiaschi**

**Autostrade  
per l'Italia**

**Roberto Bonino**

**11**

**ICT ECOSYSTEM**

**IT Ecosystem Summit  
2022, i nuovi ruoli dei  
fornitori IT alle prese con  
il PNRR**

**Loris Frezzato**

**8**

**NUMERIE MERCATI**

**Cloud Computing: iniziative,  
ostacoli, opportunità per  
aziende ed organizzazioni**

**Carmen Camarca**

15

## **DIRITTO ICT IN PILLOLE**

**Metaverso: opportunità di business nel virtuale a cui occorre una regolamentazione reale**

**Valentina Frediani**



17

## **CYBERSEC E DINTORNI**

**Come impostare l'adozione di un'architettura Zero Trust**

**Elena Vaciago**



20

## **CONNECTED MOBILITY**

**2035, anno zero per i motori benzina e diesel**

**Elena Vaciago**



# Cryptovalute e mercati digitali: la bufera di oggi passerà

---

**Ezio Viola, Co-Fondatore**

***The Innovation Group***

Da diversi giorni sui media la fanno da padrone le analisi relative all'andamento negativo delle quotazioni del Bitcoin e in generale delle principali crypto-attività, accentuate da alcuni episodi eclatanti e importanti tra cui ultimi il collasso della stablecoin Terra-Luna, il caso di Celsius che hanno causato perdite significative a investitori e messo in discussione e allarme i regolatori sui rischi dell'espandersi della finanza decentralizzata. La capitalizzazione di tutte le crypto attività è crollata dai massimi di novembre di più di 2700 miliardi di dollari e meno di 1000 Miliardi.

Queste analisi generalmente hanno 2 principali orientamenti la prima è che ci troviamo di fronte a un fisiologico ripulisti di realtà fragili e in alcuni casi anche truffaldine in un mercato quello crypto ancora in divenire e che quindi ciò che sta accadendo può avere anche effetti positivi e si fa diverse volte riferimento a quanto è accaduto più di 20 anni fa agli albori di internet e del web 2.0. La seconda valutazione invece è che quanto sta accadendo sia la ulteriore testimonianza che la finanza decentralizzata è un terreno di colture "selvaggio" e che deve essere fortemente regolamentato se non rallentato e fermato.

Come spesso capita probabilmente una analisi più accurata è necessaria per non fare di tutto un'erba un fascio e buttare via il bambino con l'acqua sporca. Occorre fare dei distinguo nel mondo della cryptoeconomia che è complesso e composito.

Riprendendo quanto dichiarato in diversi contesti da Corrado Passera per individuare una logica di intervento

dobbiamo distinguere tra piattaforme di mercato di scambio basate su infrastrutture tecnologiche su cui la finanza decentralizzata è nata basate su DLT e BLOCKCHAIN, le crypto attività e le crypto-currencies/valute digitali.

Le piattaforme digitali di scambio di nuova generazione (basate su tecnologie blockchain e DLT's sono nate con il mondo crypto, ma attraverso il meccanismo di tokenizzazione (i NFT's, i Non Fungible Token) possono diventare piattaforme in grado di scambiare praticamente qualsiasi tipologia di asset (da beni immobili, a crediti, a opere d'arte, a contratti di qualsiasi genere). Rappresentano un'opportunità straordinaria perché mettono a disposizione degli utenti funzionalità non disponibili sugli attuali sistemi di trading elettronici (come smart contract, programmabilità degli asset, ecc.). Le applicazioni che possono essere sviluppate su queste piattaforme sono sostanzialmente infinite. Molti settori, e tra questi quello bancario, saranno profondamente condizionati e si apriranno inedite nuovi spazi per l'offerta di nuovi servizi. Queste piattaforme sono ad oggi, molto energivore e ancora piuttosto complicate nel loro utilizzo (tokens, wallets, exchanges, ecc.) e, spesso, molto onerose in termini di costi di transazione per l'utilizzatore. Il più serio punto di attenzione è però un altro. C'è infatti un enorme rischio sistemico legato al fatto che queste piattaforme possono realizzare scambi in forma, di fatto, anonima. Si sa da quale nodo parte uno scambio e a quale nodo arriva, ma nel caso di piattaforme del tutto aperte, è certamente possibile celare l'identità di chi sta dietro al nodo di partenza e a

quello di arrivo. Non sfugge a nessuno l'interesse che la criminalità può avere per meccanismi di scambio e di trasferimento che evitino i controlli di Anti Money Laundering, e delle implicazioni fiscali.

Dei crypto assets, cioè gli attivi digitali di investimento (usati talvolta anche come mezzi di scambio e di pagamento) ne esistono migliaia (più di 12000 a febbraio 2022) e ne nascono ogni giorno. Il Bitcoin è la principale di queste. Esse incontrano il favore di un largo pubblico anche retail per la promessa di facili guadagni. La "mannaia" regolatoria deve essere usata però coscientemente perché non sono certamente i primi asset virtuali in circolazione, basti pensare a molti derivati, futures, ecc. In quanto tali, non c'è probabilmente ragione di limitarne la circolazione, quanto meno nel mondo degli operatori professionali. Un investitore deve essere adeguatamente informato ma deve essere libero di investire i suoi soldi in attivi di sua scelta con un chiaro livello di rischio ma occorre segnalare alcuni oggettivi rischi che questa categoria di assets porta con sé, soprattutto poiché molti di questi assets – basti pensare a talune ICO's (Initial Coin Offering) si sono dimostrate delle vere e proprie truffe. Gli investitori retail devono essere resi consapevoli del fatto che si tratta di assets virtuali (non convertibili cioè automaticamente in valute legali), estremamente volatili e certamente manipolabili (la cui proprietà spesso è concentrata in poche mani). In buona sostanza gli investitori retail devono essere messi in guardia anche dagli intermediari dal rischio di considerare questi assets come vere e proprie valute utilizzabili come mezzi di pagamento o comunque automaticamente liquidabili. Recentemente Banca D'Italia ha pubblicato una comunicazione al riguardo in cui richiama fortemente la responsabilità degli intermediari e media in tal senso.

C'è poi un aspetto che potrebbe apparire secondario, ma che secondario non è: il cosiddetto mining di Bitcoin è energivoro e sta diventando una vera industria in mano di pochi – si parla di consumi di elettricità pari a quelli di grandi paesi – e promuovere tecniche di questo genere in una fase storica come l'attuale nella quale viene richiesta a tutti maggiore responsabilità per ridurre lo spreco di energia, appare quanto meno irresponsabile.

Il terzo pilastro riguarda quello delle crypto currencies come strumento di pagamento (Digital Money). In questa categoria rientrano sia le Stable Coins che le CBDC-Central Bank Digital Currencies. In questa ultima categoria troviamo ovviamente, l'Euro Digitale.

Le Stable Coins, sono crypto assets che vengono

presentate come convertibili in monete a corso legale, Esse oggi rappresentano la componente del mondo crypto più opaca. Anche se molti emittenti dicono di essere convertibili in valute legali, è ampiamente dimostrato, come nei casi citati recentemente, le stable coins non tutte garantiscono la convertibilità in valute legali, in quanto le riserve detenute a garanzia della loro convertibilità sono ridottissime rispetto alle masse di stable coins emesse. Se fossero riconosciute come convertibili in monete legali, gli emittenti di stable coins diventerebbero di fatto delle crypto banks in un contesto di vero e proprio free banking. Si creerebbe cioè, una nuova categoria di banche in grado di produrre base monetaria, ma fuori da qualsiasi controllo delle banche centrali. Ciò farebbe perdere alle autorità il controllo della base monetaria e quindi, potenzialmente, dell'intera economia. Infine oggi le Stable Coins si qualificano come campioni della Finanza Decentralizzata (DEFI Decentralized Finance) e si vogliono costruire un'aura di democrazia in alternativa alle autorità monetarie. Esiste, invece, il grande rischio che diventino strumento di ulteriori concentrazioni di potere e potrebbero infatti diventare le Company Coins delle Big Tech (es. Diem di Facebook che però è morta di fatto). Certamente molti mega operatori che già fanno tutto



di noi (dove siamo, cosa compriamo, cosa pensiamo, ecc.) sarebbero felici di conoscere anche il contenuto del nostro portafoglio e poterne addirittura determinare il valore. Nel metaverso sicuramente si darà per scontato l'uso di monete virtuali. E' necessario quindi intervenire prima che le stable coins diventino "too big to stop." In questa categoria delle digital currencies troviamo anche l'Euro Digitale e le CBDC's – Central Bank Digital Currencies. Sono come le attuali monete a corso legale con una caratteristica in più, quella di poter "viaggiare" anche su reti digitali di nuova generazione (Blockchain e DLT) gestite dalle Autorità Monetarie. E qui sta la differenza rispetto alle stable coins: le CBDC's sono strumenti capaci di tenere il passo della modernità garantendo al contempo un quadro di legalità che altrimenti rischiamo di perdere per sempre. Avranno sostanzialmente i vantaggi prospettati da molte banche centrali e dal sistema bancario? Esse permetteranno di godere di tutte le più innovative funzionalità delle piattaforme digitali di scambio (es. smart contracts), potranno aprire spazi di innovazione nel mondo dei servizi finanziari e bancari (dal credito al wealth management alle stesse operations degli intermediari finanziari), potranno garantire tutte le tutele giuridiche delle monete a corso legale e il rispetto delle regole

dell'Anti Money Laundering in quanto tutti i nodi sarebbero parte di una rete controllata dalle Autorità e condivisa con gli intermediari regolamentati. Le autorità preposte potrebbero sempre sapere da chi partono le transazioni e a chi arrivano e verrebbe evitato il rischio di introdurre sistemi di transazioni anonime al servizio delle attività illegali. Tutte queste tematiche saranno al centro dell'agenda del prossimo Banking Summit di The Innovation group il 22-23 Settembre prossimi.

L'Euro Digitale non sarebbe solo un acceleratore di innovazione e uno strumento indispensabile per difendere la nostra sovranità monetaria, ma avrebbe anche forti e positive implicazioni geopolitiche. Non a caso la Cina lavora al Renmimbi Digitale almeno da 5 anni e lo presenterà fra pochi mesi alle Olimpiadi Invernali. Il primato della Cina, che sta già consolidandosi in molti settori dell'economia, potrebbe ricevere un ulteriore boost e la sua presa su molti paesi già ad essa legati aumenterebbe ulteriormente. Gli Stati Uniti seguiranno certamente a breve e potrebbero avvalersi della forza di talune Big Tech americane e delle enormi nuove infrastrutture digitali che si stanno costruendo nel loro Paese. L'Euro non deve rimanere indietro e deve accelerare se non vuole perdere peso nella scena globale e se vuole rimanere tra le principali valute mondiali utilizzate per transazioni e riserve. Se l'Euro rimanesse l'unica grande valuta non digitale sarebbe a rischio il suo valore e il ruolo della stessa Unione Europea"

I detrattori dell'Euro Digitale paventano il rischio di disintermediazione delle banche commerciali e una concentrazione di potere informativo eccessivo nelle mani della BCE. Il rischio di disintermediazione delle banche commerciali che taluni sollevano è del tutto gestibile perché è escluso che la banca centrale voglia mettersi a gestire in proprio i rapporti con consumatori e imprese diventando una specie di Grande Fratello della finanza. La BCE continuerebbe a regolare l'emissione dell'Euro – per via fisica, per via bancaria e per via digitale – e a garantire il rispetto delle regole da parte degli intermediari. I rapporti con consumatori e imprese rimarrebbero in capo agli intermediari che continuerebbero a farsi concorrenza sul mercato sviluppando le migliori applicazioni anche grazie alle nuove piattaforme digitali di scambio.

Il fattore tempo può essere cruciale: lasciare crescere troppo e disordinatamente il mondo crypto delle valute digitali e lasciare troppo vantaggio al renminbi e al dollaro digitale, potrebbe costare molto caro ai cittadini e alle imprese europee, oltre che all'Europa nel suo insieme.



**Francesco Fiaschi, CTO di Autostrade per l'Italia**

## Il cambiamento strutturale di Autostrade fa perno sul cloud

---

**Roberto Bonino, Research and Content Manager**

***The Innovation Group***

Si tende a identificare nel cloud uno dei principali fattori di trasformazione delle aziende in chiave digitale. Non è sempre così, in realtà, poiché la semplice migrazione in logica “lift & shift” di applicazioni o carichi di lavoro precedentemente ospitati nei data center interni cambia le modalità di fruizione, ma non agisce sui processi. Laddove alle spalle ci sia una strategia, con obiettivi ben definiti e modalità di esecuzione esplicitate, si può legittimamente parlare di digital transformation a tutti gli effetti.

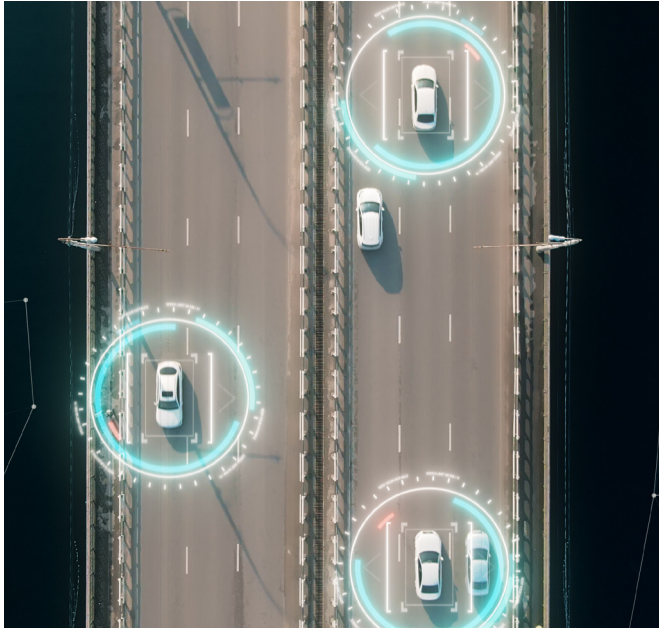


Autostrade per l'Italia ha intrapreso recentemente un percorso di cambiamento profondo, con conseguente turnover di proprietà e management. In questo contesto, ha preso forma il piano Next to Digital, che si concentra su nove aree prioritarie, spaziando dalla gestione degli asset all'ottimizzazione del controllo di viabilità e traffico, dall'evoluzione delle modalità di esazione dei pedaggi all'innovazione dell'esperienza del viaggiatore. Solo nei prossimi tre anni, sono previsti investimenti di oltre 130 milioni di euro. La revisione dell'infrastruttura tecnologica è uno degli aspetti-cardine di questo processo di trasformazione. Ne abbiamo parlato con Francesco Fiaschi, CTO della società.

### **Su quali basi avete costruito il vostro cloud journey e come sta procedendo la modernizzazione infrastrutturale?**

Siamo partiti dalla riorganizzazione e dalla digitalizzazione dei processi interni, sia di tipo core che non core. Questo progetto primario è stato accompagnato da diverse altre iniziative di trasformazione, tra le quali rientra anche il programma di ammodernamento, che va a incidere sulle architetture e le applicazioni It che non sono toccate direttamente dalla trasformazione digitale. Oggi ancora possediamo due data center interni, ma il piano prevede che nei prossimi tre anni la nostra componente architetture e applicativa sarà migrata in cloud per il 60% del totale. La percentuale salirà di un altro 10% l'anno successivo. Si tratta di un





*Il piano Next to Digital si concentra su nove aree prioritarie, spaziando dalla gestione degli asset all'ottimizzazione del controllo di viabilità e traffico, dall'evoluzione delle modalità di esazione dei pedaggi all'innovazione dell'esperienza del viaggiatore*

obiettivo sfidante, ma riteniamo che il cloud metta a disposizione strumenti di costruzione dei processi digitali che possono agire come facilitatori. Inoltre, l'ammodernamento ci serve per fare efficienza soprattutto sul fronte dei processi operativi, distogliendo investimenti dalle componenti a basso valore aggiunto dell'IT.

### **Come avete costruito il percorso di migrazione e quali logiche lo hanno presieduto?**

Nella nostra visione, oggi c'è il dato al centro dei processi e tutto ruota attorno a questo concetto. La trasformazione delle architetture e il loro conseguente passaggio nel cloud, con orientamento ai microservizi e alle architetture a eventi, serve a valorizzare i nostri asset, i dati aziendali e i processi rivisti in ottica moderna. Avendo posto il data lake al centro della nostra evoluzione e delle attività operative, concentriamo la nostra attenzione sulle informazioni che servono per prendere decisioni. A livello infrastrutturale, il nostro obiettivo di riferimento è la business continuity, estesa anche alle soluzioni di produzione, oltre che agli ambienti di test & sviluppo. Tutto questo testimonia come il cloud sia per noi un perno centrale della trasformazione e la scelta primaria per tutte le evoluzioni architetturali.

### **Privato, pubblico, ibrido: quale cloud model si adatta alla vostra realtà?**

Nel processo di decisione iniziale, la componente che ha maggiormente catalizzato la nostra attenzione riguarda la sicurezza. Abbiamo fatto le opportune

comparazioni fra i modelli proposti dal mercato e ne abbiamo concluso che non siano particolari elementi di differenziazione, poiché l'affidabilità deriva dall'utilizzo di pattern di costruzione delle architetture che siano intrinsecamente sicure e non lascino buchi o spazi pericolosi. Per questo abbiamo adottato la logica dell'infrastructure-as-a-code, che già integra modelli sicuri e in questo modo possono guadagnare in velocità dall'utilizzo del cloud pubblico.

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

Il mindset aziendale è strettamente collegato alla centralità del dato e all'importanza che si pone su questo aspetto. Le persone rappresentano sempre un potenziale veicolo di utilizzo non corretto degli strumenti aziendali, per cui poniamo attenzione a una forte cultura della sicurezza, all'accesso ai dati, all'utilizzo delle best practice. Cultura, conoscenza, attenzione all'implementazione delle architetture, test, alta affidabilità e ridondanza sono tutti elementi del mosaico di protezione di dati e workload.

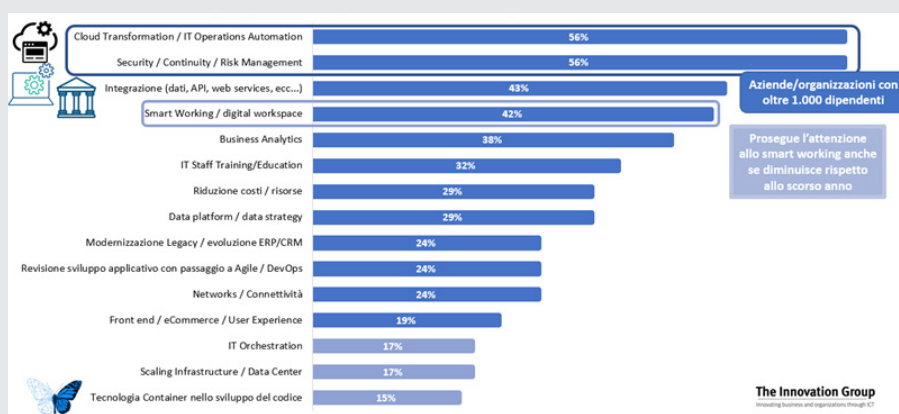
## Cloud Computing: iniziative, ostacoli, opportunità per aziende ed organizzazioni

**Carmen Camarca, Analyst**  
*The Innovation Group*

Per il 2022 si attende una sempre maggiore attenzione da parte della funzione ICT verso i progetti e le iniziative di Cloud Transformation. È quanto emerge dalla Digital Business Transformation Survey 2022, condotta da The Innovation Group tra gennaio e febbraio 2022 su un campione di 213 aziende italiane appartenenti a diversi settori e dimensioni. In particolare, dall'analisi è emerso che, nel 2022, oltre la metà del campione (56%) prevede di promuovere attività in ambito Cloud e Security (si tratta soprattutto di aziende ed organizzazioni con oltre 1.000 dipendenti), mentre nel 43% dei casi saranno sviluppate attività volte all'integrazione e all'interoperabilità dei dati e nel 42% di smart working e digital workspace (anche se rispetto agli scorsi anni diminuisce l'interesse, un aspetto da ricondurre principalmente al fatto che la maggior parte degli investimenti in quest'ambito sono stati effettuati gli anni scorsi).

In particolare, tra le iniziative Cloud che si prevede di effettuare nel 2022, la maggior parte del campione prevede di automatizzare le procedure (53% dei rispondenti, un'attività nella maggior parte dei casi già svolta nel 2021) e ottimizzare l'attuale

### Quali saranno le principali iniziative per la funzione ICT nel 2022, nello sforzo di modernizzare l'architettura IT?



Fonte: TIG, 2022

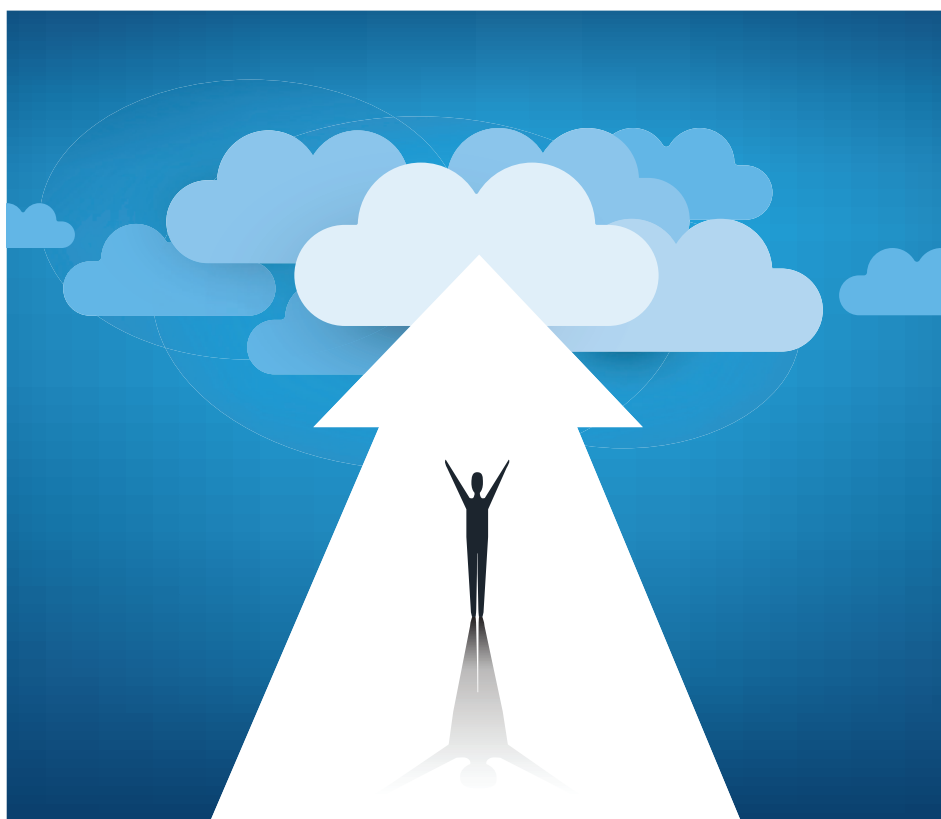
utilizzo del Cloud per risparmiare i costi (45%). Inoltre, per quest'anno, rispetto allo scorso, si attende un forte aumento nel passaggio da software on-prem a SaaS, dell'espansione dell'utilizzo del Public Cloud e del miglioramento delle attività di reporting sul Cloud.

Si tratta, tuttavia, di attività la cui realizzazione non è priva di ostacoli. In particolare, nel passaggio al Cloud, gli elementi considerati di maggiore criticità sono la necessità di preservare la sicurezza di dati, applicazioni e infrastrutture (considerato Molto o Moltissimo critico dal 73% del campione e, in particolare, da aziende con più di 2.500 dipendenti operanti

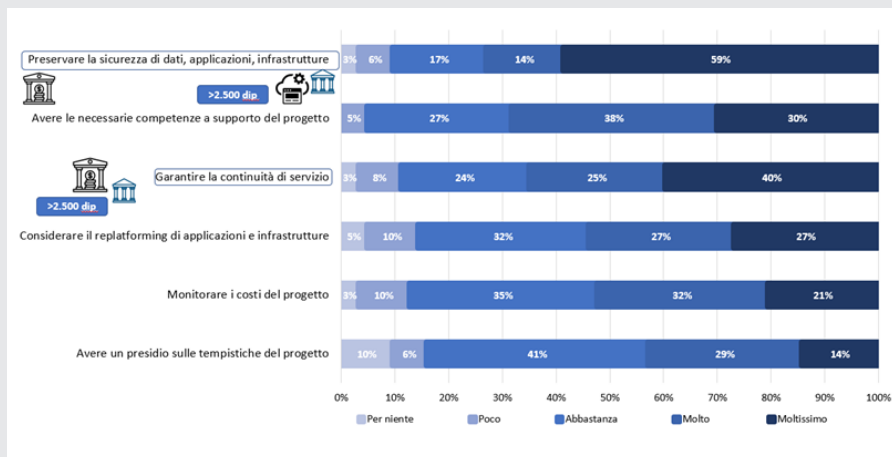
in ambito Finance e Servizi e organizzazioni pubbliche), avere competenze necessarie a supporto delle attività (considerato Molto o Moltissimo critico dal 68% dei rispondenti, un aspetto considerato come criticità in maniera diffusa da tutto il campione) e riuscire a garantire la continuità del servizio (un aspetto considerato Molto o Moltissimo critico dal 65% del campione, soprattutto organizzazioni pubbliche e istituti finanziari di grandi dimensioni). In particolare, la necessità di disporre di competenze adeguate che supportino il percorso di migrazione al Cloud è stata ben evidenziata anche da Anna Ascani, Sottosegretaria di

Stato, Ministero dello Sviluppo Economico, che, ad una recente web conference organizzata da The Innovation Group[1], ha ribadito l'importanza di «costruire elementi di consapevolezza soprattutto a partire dalle scuole». Per Ascani, inoltre, per favorire una più ampia adozione e diffusione del Cloud è importante intervenire con adeguate misure di accompagnamento e di sostegno alla domanda di connettività (al riguardo, si ricorda, il Governo sta lavorando molto con le PMI per garantire al loro interno servizi performanti di connettività, oltre che sull'erogazione dei voucher di connettività alle famiglie).

Nella migrazione al Cloud viene, altresì, posta particolare attenzione anche alla scelta dei fornitori che dovranno supportare tale attività e, in particolare, alle competenze tecnologiche (nel 74% dei casi) e alle capacità progettuali di cui dispongono (57% dei casi), aspetti indicati soprattutto da aziende di grandi dimensioni (oltre 2.500 dipendenti). Una minore attenzione (seppur comunque elevata) viene, invece, dedicata al ruolo consulenziale/di advisory svolto dai propri partner (50% dei rispondenti) e alle partnership concluse con i principali Cloud provider (43%).



### I principali elementi critici da considerare nel passaggio al Cloud



Fonte: TIG, 2022

## Le attese per il medio-lungo periodo

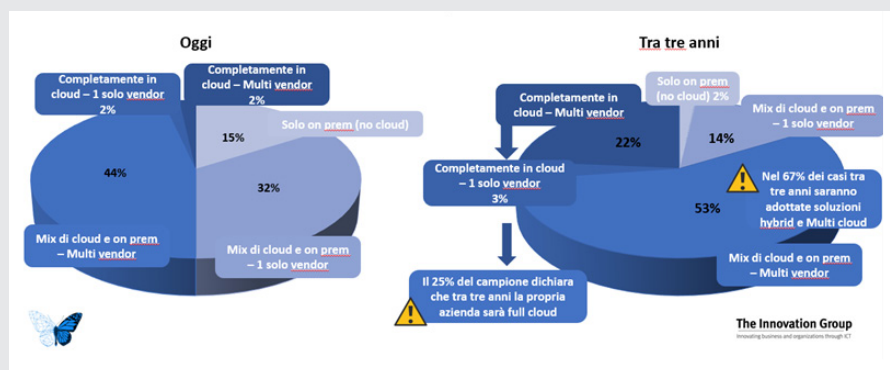
Il forte interesse (da parte di aziende ed organizzazioni pubbliche) verso le soluzioni di Cloud Computing rilevato per il 2022 proseguirà e si consoliderà anche nei prossimi anni.

Secondo l'analisi, infatti, nei prossimi tre anni tenderà a scomparire la presenza di soluzioni solo on prem (il 2% del campione si esprime in questo senso contro il 15% che dichiara di farvi ricorso allo stato attuale) a favore di soluzioni Multi e Hybrid Cloud (ad aspettarsi che tra tre anni la propria azienda/organizzazione farà ricorso a tali soluzioni è il 67% del campione, una tendenza comunque osservabile già allo stato attuale) e Pure Cloud (il 25% del campione dichiara che tra tre anni la propria azienda sarà full cloud, contro il 4% di oggi). Va, tuttavia, chiarito che anche in quest'ultimo caso si preferiranno soluzioni Multi Cloud più che affidarsi ad un solo vendor.

Per i prossimi anni si attende, dunque, una forte crescita nell'utilizzo del Cloud da parte sia di aziende sia di organizzazioni pubbliche. Se, infatti, come rilevato in precedenza, allo stato attuale la tendenza è quella di affidarsi a soluzioni Multi e Hybrid Cloud (pur essendoci una discreta presenza di soluzioni solo on prem), tra tre anni si prevede uno scenario in cui, pur essendovi sempre la compresenza di più tipologie di Cloud (e di diversi provider), le soluzioni on prem andranno a scomparire a favore di una maggiore diffusione di chi sceglierà di essere full cloud.

## Utilizzo del Cloud in azienda, oggi e tra tre anni

*D. Quali delle seguenti alternative descrive meglio l'utilizzo del Cloud nella sua azienda, ora e tra tre anni?*



Fonte: TIG, 2022

Tuttavia, la condizione abilitante perché ciò accada sarà garantire un adeguato sviluppo infrastrutturale che sia soprattutto omogeneo in tutto il territorio nazionale (si considerino in particolare le aree bianche e grigie). Senz'altro negli anni l'Italia ha accumulato gravi ritardi da questo punto di vista (secondo l'ultima edizione dell'indice DESI[2], l'Italia è al 25esimo posto – su 27 Paesi – per l'utilizzo complessivo della banda larga fissa) ma il Piano Nazionale di Ripresa e Resilienza al riguardo dedica ampio spazio e notevoli investimenti (si pensi, in particolare, all'investimento “Reti ultraveloci – Banda ultralarga e 5G” a cui vengono dedicati circa 6,7 miliardi).

In questo senso, dunque, l'auspicio è che la forte domanda di servizi Cloud a cui si sta assistendo (e a cui sempre più si assisterà nei prossimi anni) sia supportata da adeguati sviluppi infrastrutturali e servizi di connettività in grado di sostenerla, oltre che specifici

interventi (in particolare per quanto riguarda le competenze e la sicurezza delle informazioni) volti a risolvere alcune delle principali problematiche che finora ne hanno limitato una più ampia diffusione.

[1] Per maggiori informazioni: <https://www.theinnovationgroup.it/events/cloud-ultrabroadband-5g/?lang=it>

[2] Per maggiori informazioni: <https://digital-strategy.ec.europa.eu/en/policies/desi>

---

## IT Ecosystem Summit 2022, i nuovi ruoli dei fornitori IT alle prese con il PNRR

---

**Loris Frezzato, Channel Area Manager**  
*The Innovation Group*



Il Summit di TIG disegna un canale in evoluzione, obbligato alla consulenza che non può perdere le opportunità del PNRR, adattando le proprie attività sulla base delle caratteristiche dei propri, singoli, clienti

Non esistono più system integrator, se chiamate i Corporate Dealer sprecate fiato, nessuno vi risponderà.

Se poi azzardate a rapportarvi con un fornitore IT chiamandolo Rivenditore, rischiate che vi tolga il saluto. Siamo tutti consulenti. Volenti o nolenti.

Questione di nomenclatura, probabilmente, ma indice anche di un'esigenza da parte dei clienti che insiste proprio sul fatto che dal proprio fornitore di tecnologie di fiducia ci si attende una proposizione fatta per obiettivi e non per tecnologie.

Obiettivi che devono per forza rispondere a delle esigenze espresse dal cliente stesso e che puntino a una crescita e ottimizzazione del proprio business, attuale e futuro.

Sono queste, tra le altre, le indicazioni che sono state espresse dai CIO italiani sentiti in occasione della survey esclusiva "Il fornitore IT che vorrei" svolta da The Innovation Group e presentata in occasione dello scorso ICT Ecosystem Summit, l'evento annuale che TIG dedica agli operatori del canale IT italiano, quest'anno per la prima volta tenutosi in presenza, coinvolgendo analisti, giornalisti, vendor, distributori e, ovviamente, system integrator e operatori del canale, in un confronto diretto su trend di mercato e strategie di business dirette al canale.

E, finalmente, la possibilità di farlo in presenza, riattivando quel ciclo virtuoso di networking tra operatori che tanto bene fa al canale.

*Crescita del business, dell'efficienza e ottimizzazione dei costi (quest'ultima con minore priorità rispetto agli scorsi anni) tra i motivi principali per i quali un cliente attiva il proprio fornitore/consulente sulla digitalizzazione della propria azienda*

**Quale fornitore IT è adatto alle esigenze attuali dei clienti**

Una survey, dicevamo, che ha voluto mettere in luce come sia cambiato il rapporto tra clienti e fornitori di tecnologie. Un rapporto le cui regole e gli equilibri sono cambiati radicalmente e velocemente nel corso degli ultimi due anni. Anni in cui la richiesta di trasformazione digitale ha raggiunto picchi altrimenti insperati, ovviamente mossi dalle difficoltà sollevate dalla pandemia, andando a incidere sui modelli di business e sulle strategie di crescita delle aziende, prima ancora che sulle tecnologie da adottare. Crescita del business, dell'efficienza e ottimizzazione dei costi (quest'ultima con minore priorità rispetto agli scorsi anni) tra i motivi principali per i quali un cliente attiva il proprio fornitore/consulente sulla digitalizzazione della propria azienda e, per fare ciò, come anticipavamo, le qualità maggiori richieste sono la capacità consulenziale, il rigore nei termini di consegna dei progetti ma, sempre di più, la conoscenza delle dinamiche sia del settore verticale del mercato, sia della singola azienda, andando perciò nella direzione della creazione di progetti vicini alla personalizzazione.

**Un mercato IT a due velocità: cala quello a volume mentre cresce quello a valore aggiunto**

Caratteristiche necessarie per affrontare uno scenario di mercato internazionale di grande incertezza in cui si viaggia a vista, come ha ricordato e sottolineato Isabel Aranda, country manager di Context nel suo intervento al Summit:

“In tutto questo una certezza è rappresentata dalla trasformazione digitale, un processo iniziato da anni ma che ha avuto una forte spinta da parte della pandemia”. Ben il 50% degli oltre 2.700 rivenditori IT sentiti in occasione del survey “Channel Watch” che Context annualmente elabora, dichiara di avere accelerato il proprio percorso di digital transformation, superati dai loro stessi clienti, che arrivano al 67%.

“Sono i clienti che stanno segnando il passo di questo journey – osserva Aranda – soprattutto nelle aree della customer experience, della sicurezza e del passaggio verso modelli as a service. A seguire il 5G e l'AI”.

Negli ultimi sette anni la distribuzione, ossia il mercato generato dagli acquisti dei rivenditori presso i distributori (che rappresenta il mercato monitorato da Context – ndr) risulta essere in continua crescita, anche nel 2021, del 4%, generando 9,5 miliardi di euro. In rallentamento nei primi mesi di quest'anno, con un -2,5%, un calo che soffre del confronto della grandissima crescita che nello stesso periodo dello scorso anno aveva visto fino a un +43%.

Si tratta comunque di un mercato, quello italiano, che viaggia a due velocità: da un lato il mercato a volume che ha rallentato fino a quasi un -15%,



bilanciato dall'altro lato da un mercato a valore aggiunto, che corre a +17%.

**PNRR: dalla PA ai fornitori distributori e vendor. Un viaggio di andata e ritorno dove non si ammettono ritardi**

Effetti che iniziano a scaturire anche dall'accesso ai fondi messi a disposizione del PNRR, sui quali The Innovation Group tiene un costante osservatorio. Fondi che partono dalle richieste delle pubbliche amministrazioni ma che a cascata prima o poi dovranno concretizzarsi in gare e forniture di soluzioni e servizi erogati dalle aziende dell'IT, system integrator e consulenti in primis.

Progetti di migrazione al cloud e di modernizzazione che vengono rimborsati solo una volta realizzati, generando argomenti di finanziamento ai system integrator che vedono aumentare il ruolo di banche ed enti finanziatori.

**PNRR, opportunità e sfida insieme. Da affrontare insieme ai partner**

“Il PNRR rappresenta insieme una enorme opportunità, ma anche una sfida” commenta Edoardo Accenti, country manager di HPE Aruba, invitato insieme a Microsoft e a Esprinet a esprimersi sul tema, sempre nell'agenda del Summit Ecosystem, che prosegue: “Una sfida alimentata anche dallo shortage

dei componenti e prodotti che vanno a scapito di quella velocità d'azione adeguata all'innovazione, digitale. Una sfida alla quale tutti dobbiamo essere preparati. Aruba in particolare, insieme ai propri partner e distributori, si occupa di connettività che è un tema in primo piano nei progetti finanziabili dal PNRR. In questo contesto, il cloud consente di gestire l'infrastruttura in maniera più automatizzata rispetto a una gestione totalmente on prem. E il fatto che la parola cloud sia entrata nel vocabolario infrastrutturale della PA, ci apre verso opportunità importanti. Soprattutto nelle scuole. E con questi fondi, noi, insieme ai nostri partner, possiamo andare ad automatizzare la sfida della connettività, che è quanto descritto nelle linee guida del PNRR. Con la responsabilità anche di dover informare e formare chi poi dovrà gestire queste problematiche”.

**Caccia ai professionisti per fare fronte ai progetti PNRR**

“C'è una quantità tale di opportunità e di progetti che si potranno aprire grazie al PNRR che la vera difficoltà sarà poi anche trovare il numero sufficiente di professionisti con le competenze adatte a gestirli – fa eco e allerta Luca Casini, country manager business division di Esprinet -. E avere al proprio fianco un distributore che è in grado di fornire circa 200 specialisti di prodotto, permette di affrontare



la sfida con maggiore serenità. Soprattutto in un momento in cui migliaia di persone stanno cambiando posti di lavoro sulla base delle nuove esigenze che la pandemia stessa ha contribuito a sollevare, rendendo difficile più che prima garantire per le aziende una fidelizzazione della propria forza



lavoro. In Esprinet ci siamo preparati investendo in risorse umane e in competenze, oltre che aumentare lo sforzo logistico per poter sopperire alle difficoltà create dallo shortage dei prodotti. E il pericolo è di sbagliare qualcosa nella realizzazione di un progetto, che è fatto di tante variabili, e rischiare così di ricevere i fondi. Fondamentale quindi dotarsi di professionisti e consulenti, visto che non è una fase banale da poter affrontare senza le dovute e sufficienti professionalità”.

### **L'esigenza di sollevare l'esigenza. Compito arduo per vendor e partner ingaggiati nella trasformazione digitale**

Giacomo Frizzarin, direttore divisione small medium and corporate di Microsoft, anch'esso sul palco, seppur esponendolo con tono sereno, lancia un messaggio allarmante, convalidato da numeri insospettabili: “Da una nostra recente ricerca, circa il 50% delle medie imprese italiane non sa dell'esistenza del voucher dell'innovazione messo a disposizione del MISE attraverso il quale ci si può avvalere di un consulente per capire quali sono le proprie esigenze in termini di innovazione digitale. E oltre il 40% di questi ha addirittura dichiarato non esserne proprio interessati. Il 22% delle PMI italiane non ha nemmeno una persona dedicata alle tematiche del mondo digitale e il 70% non ha nessuno al proprio interno che sia in grado di pensare o ripensare alla strutturazione dei processi in ottica digitale. Perché il tema di fondo rimane la consapevolezza da parte delle aziende riguardo ai benefici che il digitale può portare. E sia sul fronte del pubblico che su quello del privato, la prima barriera da abbattere è proprio quella delle competenze e della cultura del digitale, sulle quali noi vendor possiamo e dobbiamo fare molto. La formazione, quindi, è quello che ci impegna in prima fila insieme ai nostri partner. Attraverso una serie di accordi, come quelli che abbiamo fatto con Poste e ora anche con Unicredit, stiamo cercando di portare al mondo delle imprese dei pacchetti di soluzioni all'interno dei quali è compreso un aiuto sulla definizione del fabbisogno, un aiuto sul tema dei finanziamenti, anche complementari a quelli del PNRR, e poi andiamo anche a toccare il tema della formazione, che può essere sia su tematiche tecnologiche sia sui temi finanziari, fornendo così degli strumenti per poter misurare gli effetti dell'uso della tecnologia. Un aiuto per aiutare le aziende a beneficiare in maniera corretta di tutti gli incentivi esistenti”.



# Metaverso: opportunità di business nel virtuale a cui occorre una regolamentazione reale



**Valentina Frediani, General Manager  
Colin & Partners**

“Ci vediamo nel metaverso”. Potrebbe essere questo il futuro, molto prossimo, che attende consumatori e imprese. Una vera e propria realtà, ibrida, che – dopo la denominazione Meta della holding che controlla il Gruppo Facebook, Whatsapp, Instagram e Oculus – racconta di un digitale fatto di universi reali e virtuali fortemente interconnessi. Un passo avanti rispetto alla realtà aumentata che ne è comunque il presupposto.

Qualcuno ricorderà Second Life che, nel lontano 2003, aveva rappresentato un esperimento di realtà virtuale che ha prodotto milioni di dollari di fatturato. Caduto quasi in disgrazia, forse è stato lanciato fin troppo presto, quando la tecnologia in uso alle persone non era capillarmente diffusa. Oggi il digitale ha fatto balzi enormi sia in termini di computer graphic che in capacità di gestione dei dati (si pensi al cloud computing).

Questo è il punto, ciò che di più vivo esisterà nel metaverso saranno dati e informazioni. Essi vanno a ricreare metriche che ci sono familiari, quelle spazio-tempo, che consentono di dedicarsi ad attività quotidiane senza muoversi di casa o dal proprio ufficio. Non è solo un “gioco”, si parla di sport, eventi, formazione ma anche di attività lavorative, come le riunioni, compiendo un passo ulteriore rispetto agli ormai tradizionali strumenti di web conference.

Non stupisce dunque che molte realtà produttive ne vogliano cogliere i vantaggi e le potenzialità.

Il mondo del fashion è stato tra i primi a ritagliarsi



uno spazio, quello del gaming trova nel metaverso una quasi naturale collocazione. Si sono avvicinati anche marchi Food&Beverage, così come è facile immaginare applicazioni che riguardino la didattica immersiva o iniziative culturali e dello spettacolo.

Unendo le potenzialità della rete alle applicazioni di intelligenza artificiale su dispositivi sempre più evoluti, il metaverso potrebbe riservare molte sorprese, si pensi alla geolocalizzazione o all’immobiliare (già sperimentato in Second Life, peraltro).

### **Cosa accade dal punto di vista giuridico?**

Nel metaverso non si parla solo di avatar ma di vere e proprie identità digitali che replicano quelle reali e – come ormai sappiamo – questo comporta delle responsabilità per chi opera nel virtuale e per chi gestisce questo (o questi) mondo parallelo. È difficile, ora come ora, immaginare che l’impianto normativo esistente sia pronto e preparato a regolamentare le interazioni tra reale, web e metaverso.

Quale autorità ne sarà il riferimento? Chi formulerà le leggi e chi le farà rispettare? Quali saranno i diritti e le responsabilità delle identità che ne fruiranno?

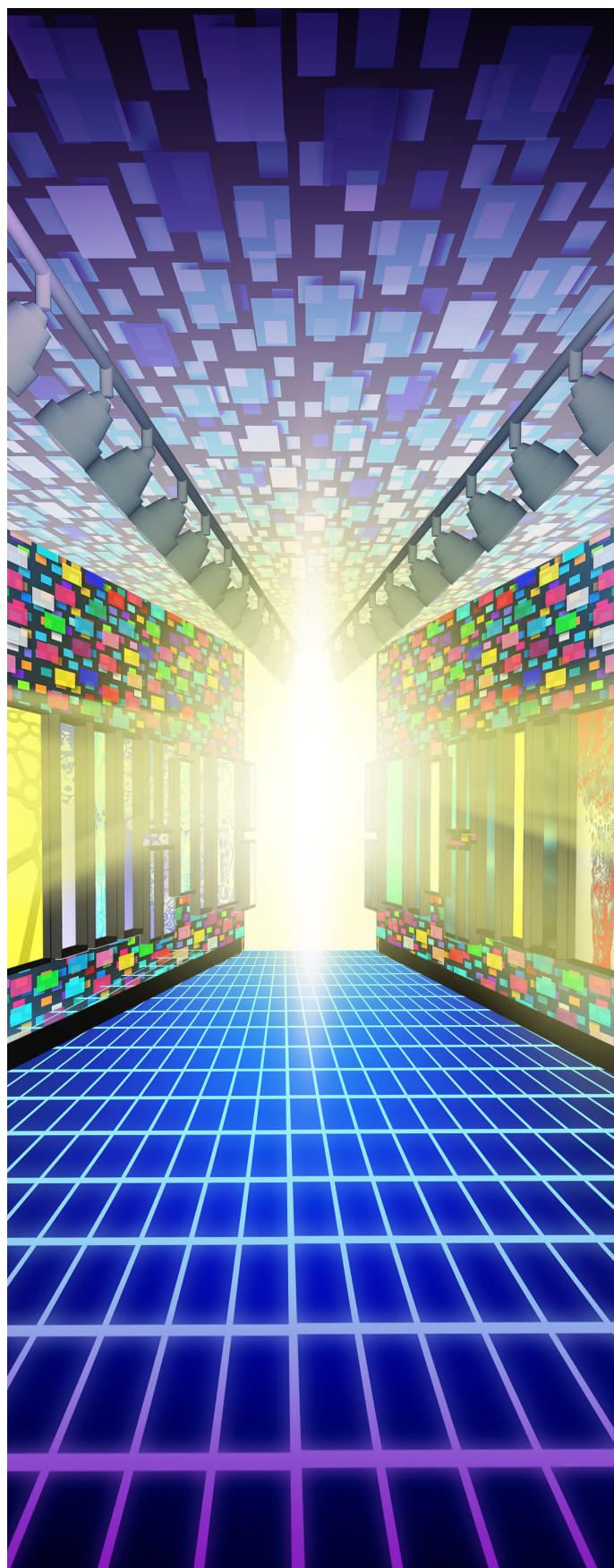
È evidente che il primo grande tema è quello della privacy. Attorno al metaverso graviterà una enorme mole di dati personali che rappresenteranno un valore sostanziale per le imprese che li raccoglieranno e li gestiranno. Non è un caso che l'Unione Europea, che sempre più si esprime su temi innovativi come quello dell'intelligenza artificiale, abbia già colto la necessità di un regolamento dedicato a questa nuova dimensione digitale.

La tutela dei dati degli utenti è oggetto di quattro diverse proposte in valutazione: il Regolamento EU 112/2018 che si focalizza sui principi di equità e trasparenza per gli utenti commerciali dei servizi di intermediazione online; la proposta di Regolamento 850/2020 relativo a un mercato unico dei servizi digitali; quella di Regolamento 842/2020 sui mercati equi e contendibili nel settore digitale e, infine, la proposta di Regolamento 106/2020 relativo a regole armonizzate sull'intelligenza artificiale (AI).

Quest'ultima è di certo quella che più si interroga sull'equilibrio tra tecnologie fortemente innovative e pervasive e sicurezza e tutela dei dati.

Il noto General Data Protection Regulation (GDPR) che ci ha accompagnati negli ultimi anni avrà di certo molto da fare per tenere fede ai suoi principi fondamentali in una realtà estremamente fluida e in divenire. Si pensi al concetto di minimizzazione dei dati, non sarà facile declinarlo rispetto alle finalità dichiarate in un potenziale infinito scenario di servizi e applicazioni virtuali.

Anche gli interlocutori potrebbero essere diversi (non è detto che vi sarà un solo metaverso o che i molti che potrebbero nascere saranno interoperabili), di certo per tutti sarà mandatorio garantire i diritti fondamentali: il consenso chiaro ed esplicito, in primis, ma anche la possibilità di revocarlo efficacemente senza che la propria identità, nel reale, resti agganciata a quella di un avatar non più desiderato. Anche altri diritti, come libertà di espressione, controllo sui comportamenti scorretti o fraudolenti e furto dell'identità assumeranno di certo un'importanza assoluta che la normativa dovrà saper gestire con chiarezza ed efficienza.



### Intervista a

**Francesco Di Maio, Head Corporate Security Department di ENAV.**

## Come impostare l'adozione di un'architettura Zero Trust

**Elena Vaciago, Associate Research Manager**

**The Innovation Group**



*“Conoscenza è potere”. Applicando alla cybersecurity questo concetto di natura baconiana, se conosciamo il comportamento atteso di una risorsa potremo limitare gli accessi indesiderati e soprattutto i movimenti laterali. Il principio si sposa perfettamente con la filosofia Zero Trust, che raccomanda un'identificazione costante dell'oggetto/soggetto che richiede l'accesso alla rete. Ne parliamo in questa intervista con Francesco Di Maio, Head Corporate Security Department di ENAV.*

**Quali sono i motivi che spingono all'adozione di una “filosofia Zero Trust” per la gestione dei rischi cyber?**

Il modello Zero Trust facilita le organizzazioni sottoposte al

Perimetro di sicurezza cibernetica nazionale, fornendo una strategia basata su principi e codifiche. È da prendere come punto di riferimento, soprattutto ora che il NIST ha codificato le attività da considerare in questa roadmap. Aiuta le aziende ad aderire ai principi fondamentali della sicurezza delle informazioni che vanno oltre il concetto tradizionale di “perimetro da difendere”.

Oggi osserviamo un incremento esponenziale delle minacce cibernetiche, non solo legate al

cyber crime: anche aspetti di guerra ibrida, temi legati alla gestione degli insider threat. È indispensabile passare ad un approccio di cybersecurity olistico e integrato, secondo cui ogni componente del sistema è da salvaguardare, con una logica di prioritizzazione valida per tutti gli asset e tutte le informazioni.

**Come si colloca il nuovo approccio Zero Trust rispetto ai framework tradizionali?**

Per chi ha iniziato a lavorare in logica di framework nazionale di



sicurezza cibernetica, il concetto Zero Trust evoca da vicino il livello “Identify” del framework, ossia, avere sottomano l’architettura dei sistemi core e non solo.

Oggi – soprattutto in organizzazioni complesse, che vanno verso il lavoro agile e richiedono un coinvolgimento pieno del personale su aspetti di sicurezza, il modello deve permeare l’intera gestione IT. In questo scenario, Zero Trust è una necessità, significa identificare e controllare ogni singola componente del nostro ambiente. Bisogna abbandonare l’assunto

secondo cui se un asset si trova all’interno del sistema è trusted, e identificare il migliore bilanciamento tra necessità e rapidità, e tipologia dati trattati, per un’identificazione costante dell’oggetto/soggetto che richiede l’accesso alla rete. In sostanza, controllare pedissequamente i comportamenti di tutto quanto si muove nel network. In questo modo applichiamo un concetto di natura baconiana, ossia, “Conoscenza è potere”: se conosci il comportamento atteso di una risorsa potrai limitare gli accessi indesiderati e soprattutto i movimenti laterali.

**Come impostare un percorso di adozione dei principi Zero Trust? Quale strategia avete delineato per questa transizione?**

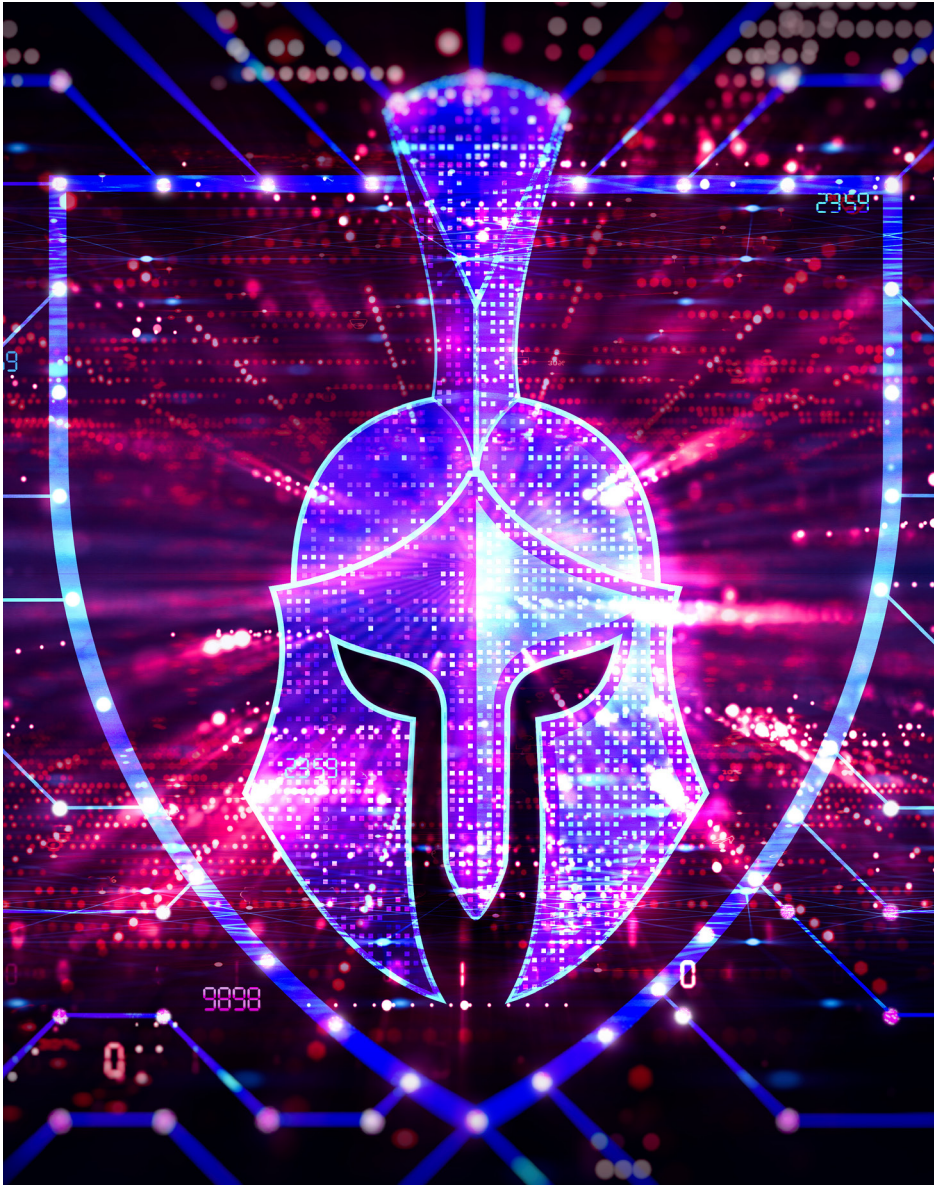
Con riferimento al mondo IT in ENAV, distinguerei tra l’IT tradizionale (Office Automation, ERP, posta) e gli ambienti core afferenti al settore dell’aviazione civile. Per questi ultimi, oggi in grande trasformazione con la remotizzazione degli strumenti a disposizione del controllore (portati dalle torri di controllo fisiche a un unico remote tower control center), si può dire che il concetto Zero Trust era presente fin dal principio. Per motivi di elevata sicurezza si è sempre avuto per gli ambienti core una segregazione delle reti, controlli quotidiani incisivi e una riduzione spinta della superficie attaccabile. Per quanto riguarda invece gli ambienti dell’IT tradizionale, siamo per un approccio graduale a Zero Trust: partendo da una preparazione degli elementi, con categorizzazione e selezione, sarà avviata una transizione a Zero Trust con logiche di web application firewall, identificazione del trust nelle attività, microsegmentazione, ampliamento della robustezza della rete per ridurre la superficie di attacco.

È poi molto importante considerare il cambiamento culturale introdotto dal nuovo approccio: serve un controllo end-to-end, tutti gli elementi del network devono essere fortemente presidati. Bisogna fare fronte a nuovi costi, all’aspetto culturale, a nuovi processi manutentivi per l’infrastruttura. E’ un passaggio importante e complicato. Non esiste poi un unico modello ZT e non si tratta di una tecnologia,



“

**Zero Trust è una necessità, significa identificare e controllare ogni singola componente del nostro ambiente**



ma piuttosto, di un'architettura che si compone anche di ciò che già abbiamo e che deve essere maggiormente valorizzato.

#### **Quanto è importante automatizzare?**

L'automazione aiuta a ridurre fortemente i tempi di identificazione dei problemi che si presentano all'interno del perimetro e a rispondere in modo immediato guardando agli aspetti di behaviour.

Con la progressiva digitalizzazione e assorbimento di tecnologie nuove e sempre più performanti, tendiamo a perdere di vista cosa abbiamo all'interno, e viene

meno il controllo rigoroso, che ora va recuperato per ogni risorsa nell'organizzazione. Il controllo però richiede un processo di automazione spinto.

Accanto a questo, bisogna adottare misure non solo tecnologiche ma anche procedurali, ad esempio, la drastica riduzione dei poteri degli amministratori di sistema e di dominio, la loro convergenza verso necessità di controllo, l'adesione a sistemi di autenticazione non generalizzati, l'utilizzo di credenziali di amministratore con OTP (one time password). Una svolta culturale che contraddistingue anche la gestione del day-by-day, il change management, il vulnerability management.

#### **In conclusione, cosa considera essenziale nell'implementazione di un'architettura Zero Trust?**

Tutto parte dalla necessità di avere una piena ed effettiva conoscenza di cosa ho in casa e di come funziona. Serve quindi un lavoro strutturato per agire con policy e controlli: solo così si garantisce anche ad altri utenti, a chiunque abbia a che fare con la tecnologica, di far parte del nuovo sistema. Zero Trust è un'innovazione che riguarda l'intera organizzazione, tutti devono parteciparvi in modo convinto. Terzo aspetto fondamentale è avere il commitment dell'alta direzione: la security non appartiene solo ai "tecnici" ma è oggi parte integrante del business, processo profondamente integrato nella consapevole catena gestionale del rischio e, per questo, è importante il flusso continuo verso il board e l'alta direzione, in quanto è elemento essenziale di governo dell'organizzazione.

# 2035, anno zero per i motori benzina e diesel

**Elena Vaciago, Associate Research Manager**

***The Innovation Group***

Per l'industria automotive europea il 2035 dovrebbe essere l'anno dell'addio alla vendita di auto nuove con motori benzina, diesel e ibride. Il 29 giugno scorso il Consiglio dei ministri dell'Ambiente dei Paesi UE ha infatti trovato l'accordo su un pacchetto di misure ("Fit for 55"), nato da una proposta del 2021 della Commissione UE. Saranno ridotte ulteriormente le emissioni di CO2 di nuove autovetture e nuovi furgoni, rispettivamente di almeno il 55% e il 50% entro il 2030 (rispetto ai livelli del 1990), con l'obiettivo di raggiungere la neutralità climatica nel 2050.

Tra le misure del pacchetto "Pronti per il 55%", oltre alle revisioni al mercato ETS (Emissions trading System), il sistema di scambio di "diritti ad inquinare" introdotto nel 2005, quella, molto dibattuta tra i diversi Paesi membri, sullo stop alla vendita delle auto endotermiche dal 2035. L'Italia, ad esempio, ha spinto molto sulla neutralità tecnologica e quindi sulla possibilità di "allungare la vita" ai motori endotermici (si puntava fino al 2040). Non è passato, ma almeno si è arrivati con la Germania a un compromesso, la possibilità di immatricolare dal 2035 ancora modelli endotermici a patto che utilizzino solamente biocarburanti o e-fuel. Un'apertura quindi a tecnologie alternative all'elettrico, e una spinta a continuare ad innovare su questi temi.

È stato deciso anche un momento di controllo intermedio, nel 2026, quando la Commissione Europea valuterà i progressi compiuti verso il raggiungimento degli obiettivi di riduzione delle emissioni del 100%. Potranno quindi essere riesaminati gli obiettivi tenendo conto di eventuali nuovi sviluppi tecnologici, perché la transizione sia anche gestibile da un punto di vista economico e sociale. Nel caso, un ricorso più prolungato all'ibrido potrebbe aiutare nella fase di passaggio.

Veicoli di lusso e produttori di nicchia (con meno di 10mila vetture prodotte all'anno) avranno una proroga di cinque anni, quindi riduzione delle emissioni di almeno il 55% entro il 2035. I testi definitivi dell'accordo dipenderanno poi dai prossimi lavori del Parlamento.

Per il settore automotive si apre quindi oggi una fase di

profonda trasformazione industriale, economica, di filiera, che andrà monitorata costantemente per verificare nel Paese se l'adeguamento avviene nei modi e con i risultati migliori per la competitività del settore. Ad esempio, c'è un tema occupazionale che non va trascurato: in Italia il settore dà lavoro a 570mila lavoratori contando l'intera filiera automotive, a oltre 1.270mila persone se si considera anche l'indotto. Secondo una recente stima dell'Anfia, l'associazione della filiera automotive italiana, ci sarebbero almeno 450 imprese a rischio (sulle 2.198 che compongono la platea della filiera automotive in Italia), pari a 70mila addetti, perché specializzate in componentistica per auto con combustione interna, quindi destinate a sparire. Se nel medio periodo, molte di queste aziende continueranno a lavorare nell'aftermarket (per assicurare i ricambi anche dopo il 2035, visto che le case auto assicurano la reperibilità dei pezzi fino a dieci anni) presto cominceranno comunque a subire impatti negativi. Infatti, secondo Anfia, già tra qualche anno le grandi case automobilistiche fermeranno o rallenteranno la produzione di auto diesel e benzina: per questi fornitori già il 2024 potrebbe essere l'anno in cui ripensarsi per il futuro. Oggi, nel mondo automotive, servono investimenti, nuove competenze, innovazione, per favorire il consolidamento di nuove linee produttive sostitutive di quelle dei motori tradizionali. Se l'Europa vuole effettivamente guidare la trasformazione verso una mobilità sostenibile e a impatto zero sull'ambiente, è chiaro che servirà un notevole sforzo e la capacità di guardare al futuro. Una nuova legislazione in materia è uno stimolo positivo, può anche aiutare all'industria automotive italiana a rimettersi in gioco, a recuperare alcune posizioni perse negli ultimi decenni. Saranno fondamentali quindi gli investimenti in ricerca, per sostenere le aziende che puntano a innovare, e la capacità di trasferimento tecnologico. Ecosistemi, competenze, filiere produttive subiranno un forte scossone nei prossimi anni: è importante cominciare da subito a investire su un gioco di squadra, riconoscendo da subito alle aziende Capo filiera un ruolo forte di trazione.





## **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](http://www.theinnovationgroup.it)