APRILE 2019

IL CAFFÈ DIGITALE

THE INNOVATION GROUP NEWSLETTER

Cybersecurity

Multilateralismo o Cyber-sovranità?

QUESTO MESE ABBIAMO FATTO COLAZIONE CON...

Fabio UGOSTE
Information Security Officer,
Intesa Sanpaolo

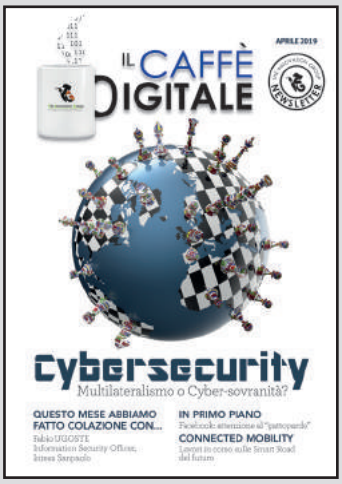
IN PRIMO PIANO

Facebook: attenzione al "gattopardo"

CONNECTED MOBILITY

Lavori in corso sulle Smart Road del futuro

Sommario



QUESTO MESE ABBIAMO FATTO COLAZIONE CON...

Fabio UGOSTE
Information Security Officer
Intesa Sanpaolo

INTESA SANPAOLO

L'EDITORIALE

MULTILATERALISMO O CYBER-SOVRANITÀ?

La dimensione geopolitica della Cybersecurity

Roberto Masiero | Presidente, The Innovation Group

La Cybersecurity non è soltanto al centro delle preoccupazioni delle aziende, ma è sempre più al centro dell'attenzione dei Governi e dei singoli cittadini.

Al recente Cybersecurity Summit di Roma, organizzato da The Innovation Group, il Sottosegretario di Stato Angelo Tofalo - Ministero della Difesa – ha affermato che "Simulazioni eseguite da specialisti hanno stimato che in caso di attacco alla rete elettrica, un black out elettrico di qualche settimana determinerebbe un collasso dell'intero Sistema Paese, producendo danni anche in termini di vite umane".

E a proposito di Active Defence ha aggiunto: "In ambito cyber, difendere è molto più impegnativo di attaccare… oggi il sistema di difesa tradizionale è stato (quindi) rivisto."

"La NATO, dopo aver riconosciuto lo spazio cibernetico quale nuovo dominio operativo da difendere alla stregua di terra, mare, aria e spazio, si prepara alla cyberwarfare… In questa direzione si sta muovendo anche l'Italia come Sistema Paese".

In questo contesto stiamo quindi assistendo al moltiplicarsi del potere di offesa nelle mani di pochi Paesi tecnologicamente avanzati, sempre più rivali tra loro.

Nel suo intervento al Cybersecurity Summit, il Pro-Rettore alle Relazioni Internazionali della Luiss, Raffaele Marchetti, ha documentato come, a partire dal 2005, 16 Paesi in più di 150 casi abbiano direttamente o indirettamente utilizzato tecniche cyber per interferire negli affari interni di altri Paesi.

La gravità di questa guerra sotterranea ha portato allo sviluppo di alcuni approcci al tema della "Cyber Governance", senza però un accordo universale.

In pratica stanno emergendo una serie di accordi a vari livelli: regolamentazioni nazionali, leggi internazionali, standard professionali, accordi politici e protocolli tecnici, in un contesto che rimane per ora dominato da aspre contrapposizioni e lontano da una visione complessiva coerente e condivisa.

In questo dibattito, secondo il Prof. Marchetti potremmo identificare due "poli": il polo ispirato al concetto di "Multilateralismo digitale", sviluppato dal Presidente di Microsoft Dan Smith - che ha proposto una "Convenzione di Ginevra Digitale" – e quello di "Cyber-sovranità", sostenuto da Natalia Karsperski.

Dan Smith invita i governi a implementare regole internazionali per proteggere l'uso civile di Internet in tempo di pace, così come la Convenzione di Ginevra li proteggeva in tempo di guerra: e questa sorveglianza dovrebbe essere garantita dall'assistenza attiva delle società ICT.

“

Natalia Karsperski non ha alcuna fiducia in un organismo transnazionale del tipo di quello proposto da Dan Smith, e vede in potenziali accordi regolamentari internazionali solo un ulteriore strumento per consolidare di fatto il dominio del club dei Paesi egemoni.

”

In questo modo si dovrebbe mirare a evitare attacchi su imprese private e su infrastrutture critiche, favorire comunque la condivisione delle informazioni su eventuali attacchi, assistere le imprese private che ne fossero comunque oggetto e lavorare a una sorta di accordo contro la proliferazione delle cyberweapons, da tutelare attraverso una istituzione internazionale del tipo dell’Agenzia per l’Energia Atomica.

Alla natura apparentemente un po’ utopica di questa posizione si contrappone quella di Natalia Karsperski, centrata sul concetto di Cyber-sovranità.

Secondo questa posizione, il mondo è diviso in due gruppi di nazioni: un primo gruppo, più ristretto, composto da Paesi tecnologicamente avanzati in grado di tutelare la propria cyber-sovranità, e una maggioranza di Paesi destinati a rimanere allo stato di cyber-colonie.

Natalia Karsperski non ha alcuna fiducia in un organismo transnazionale del tipo di quello proposto da Dan Smith, e vede in potenziali accordi regolamentari internazionali solo un ulteriore strumento per consolidare di fatto il dominio del club dei Paesi egemoni.

In questo contesto, il modo migliore per proteggere la propria sovranità nazionale sarebbe quello di “contare sulle proprie forze”.

E visto che ciò che fa gioco è la capacità di tutelare e sviluppare la propria capacità tecnologica, la strategia vincente dovrebbe mirare allo sviluppo di “National Champions” in grado di tutelare con la propria eccellenza tecnologica la sovranità digitale del proprio Paese.

Il quadro complessivo emerso dal dibattito all’interno del nostro “Cybersecurity Summit” non è quindi particolarmente ottimistico.

Alcune considerazioni:

- Di fatto esiste già una sperequazione tra la capacità tecnologica di un piccolo numero di Paesi e il resto del Mondo. Sperequazione destinata ad allargarsi con l’accelerazione del progresso tecnologico e l’allargarsi del gap tra i paesi digitalmente avanzati e gli altri.
- In un vuoto di regolamentazioni internazionali e in un contesto in cui sempre più Paesi si sentono legittimati a utilizzare attacchi cyber per interferire negli affari interni di altri Paesi, non pare ci siano validi incentivi a favore dello sviluppo di un sistema di regolamentazioni internazionali come quello proposto da Dan Smith.
- Siamo in un periodo di transizione caratterizzato a livello politico internazionale dall’onda del sovranismo che contrasta e tende a prevalere su quella della globalizzazione. Il che fa prevedere che il cyberspazio, il “quinto dominio”, vedrà nei prossimi anni un aggravarsi delle tensioni e un intensificarsi degli attacchi, rivolti sempre più alle imprese e alle infrastrutture critiche dei Paesi “nemici”.
- Secondo una logica di “corsi e ricorsi storici”, è possibile tuttavia che questa corsa all’intensificarsi dei conflitti possa trovare un argine soltanto nel momento in cui i Paesi egemoni si ritrovino reciprocamente vulnerabili, così come accadde con il processo di distensione che fece seguito all’“equilibrio del terrore” fra le potenze nucleari nel secondo dopoguerra.
- In conclusione, peccato che in Europa i “National Champions” siano spariti 30 anni fa… in che modo dunque i nostri Paesi e le nostre imprese possono attrezzarsi per giocare un ruolo non subordinato sul terreno strategico della Cybersecurity?

Continueremo questo dibattito sui nostri siti e certamente in occasione del prossimo “Cybersecurity Summit” di Milano, insieme agli Esperti e ai Rappresentanti del Governo e delle nostre Imprese.

QUESTO MESE ABBIAMO FATTO COLAZIONE CON

Le priorità 2019 per la Cybersecurity

Intervista di **Elena Vaciago** a

Fabio Ugoste

Information Security Officer, Intesa Sanpaolo

Nonostante le aziende siano sempre più attente e preparate in tema di gestione dei rischi cyber, i Responsabili della Sicurezza ICT devono confrontarsi con uno scenario ogni anno più complesso.
Quali priorità assegnare oggi alle scelte strategiche per la protezione del business e degli asset critici? Ne parliamo in questa intervista con Fabio Ugoste, Information Security Officer di Intesa Sanpaolo.

Facciamo il punto su quelle che potrebbero essere, nel corso del 2019, le sfide principali in tema di cyber risk management. Secondo Lei cosa le aziende italiane dovrebbero mettere a piano per contrastare questi rischi? Quali sono oggi azioni prioritarie su cui focalizzare gli sforzi?

È complesso oggi individuare una priorità unica in quanto gli attacchi sono sempre più ad ampio spettro.
E' quindi fondamentale tenere sotto controllo tutto l'insieme degli elementi.

Noi puntiamo ad essere sempre più bravi, anzi, ad eccellere, per quanto riguarda le misure di protezione fondamentali.

Lavoriamo per ottimizzare alcune attività che oggi vengono date quasi per scontate, come il patch management, il mantenere hardware e software costantemente aggiornati e fare in modo che tutti gestiscano al meglio le proprie credenziali di accesso ai sistemi. Questo costituisce l'ABC della sicurezza e deve essere portato a livelli di eccellenza, perché è proprio su questo fronte che viene indirizzato il 95% degli attacchi massivi (come malware, ransomware, ecc.) che nel complesso possono causare danni importanti.

Fondamentale è anche il tema legato alle nuove tecnologie, alle soluzioni innovative che aiutano a farci diventare sempre più preparati nell'intercettare eventi anomali.

Oggi la sfida è essere in grado di verificare enormi quantità di dati, usando al meglio tutte le nuove tecnologie disponibili quali Machine Learning, AI, Anomaly Detection, ecc. Queste soluzioni aiutano anche nella prevenzione da Advanced Persistent Threat (APT), gli attacchi avanzati e mirati su singoli target, che risultano essere una piccola percentuale sul totale, ma possono essere molto dannosi.

Infine, il terzo fondamentale aspetto da considerare, trasversale ad entrambe le attività, è il tema della diffusione della cultura della cybersecurity non solo all'interno dell'azienda.

Ad oggi infatti l'anello debole della catena

continua a essere il fattore umano, e non parlo solo dei dipendenti, ma considero tutti i soggetti che entrano a far parte del perimetro aziendale, come i fornitori e i clienti.

Come vede la situazione con riferimento all'attuale cultura sulla sicurezza digitale?

E' indispensabile continuare a far crescere l'awareness delle persone: è un problema che noi, con la nostra presenza diffusa in tutto il mondo, riscontriamo praticamente ovunque, anche se nel passaggio da USA a Europa a Italia il problema si aggrava. In futuro mi aspetto che il tema diventerà ancora più complesso da gestire, perché la tendenza in atto è quella di una sempre maggiore interconnessione e condivisione tra le persone di dati digitali, senza particolari remore e precauzioni nell'utilizzo dei social.

Quali sono oggi le azioni prioritarie per incrementare una cultura generale per la sicurezza?

Bisogna educare le persone a rispettare alcune prassi fondamentali, a non condividere le password, ad utilizzare schemi di password diversi sui diversi ambiti di utilizzo.

Le persone devono comprendere che ogni volta che autorizzano un provider a usare i propri dati, la proprietà delle informazioni viene sostanzialmente ceduta a terzi. In Intesa Sanpaolo abbiamo intrapreso un percorso di progressiva eliminazione delle password: come già fatto con i clienti, anche per i dipendenti avremo presto una multi factor authentication.

Non è però sufficiente individuare un processo sicuro, perché, nella nostra esperienza, se questo risulta troppo complesso, diventa difficile riuscire a farlo utilizzare.

Abbiamo quindi studiato una user experience applicata alla sicurezza e continuamente la verifichiamo per ogni nuova soluzione.

È necessario quindi che questa sia al tempo stesso molto semplice da usare ed anche molto sicura.

Diffondere cultura di sicurezza vi sta portando quindi a svolgere un ruolo sociale, laddove le istituzioni e la scuola in primis non stanno facendo abbastanza per educare maggiormente le persone su questi temi …

Nella nostra area di lavoro, puntiamo ad eccellere nei fondamentali e ad aumentare la capacità di intercettare i segnali deboli, mentre per quanto riguarda i dipendenti del Gruppo, ma anche fornitori e clienti, l'obiettivo è quello di diffondere cultura e awareness.

Oggi considerare i rischi che provengono da terzi è fondamentale: basti pensare che quasi tutte le frodi avvengono perché i clienti cedono, in buona fede, le proprie credenziali, nella convinzione di stare operando con la propria banca.

Anche negli incontri con grandi aziende internazionali vediamo che queste affrontano lo stesso problema: far crescere il livello di sicurezza lungo tutta la catena.

Parlando di cultura della cybersecurity diventa inevitabile pensare a quanto potrebbero fare la scuola di base oltre che i percorsi formativi universitari; c'è ritardo nella risposta ad un problema concreto: mancano figure professionali con competenze specifiche sulla cybersecurity, mentre, se pensiamo ad esempio al mondo anglosassone, le lauree con specializzazione di questo tipo esistono da molto più tempo.

Su questo punto noi stiamo cercando di fare la nostra parte avendo avviato importanti collaborazioni con le principali Università italiane.

Oggi si parla molto di automazione e Intelligenza Artificiale come una possibile risposta al tema dell'accresciuta complessità di gestione della cybersecurity: potrebbe essere una soluzione alla mancanza di persone e competenze?

Il problema non può essere del tutto risolto con l'Artificial Intelligence (AI): è sicuramente vero che, al momento, con questi strumenti si eliminano alcune attività di tipo più operativo, ma per sviluppare soluzioni di AI e per integrarle nei processi aziendali, servono competenze specialistiche molto difficili da reperire.

Oggi appare chiaro che se occorre gestire milioni di allarmi, sarà possibile farlo solo attraverso l'uso di strumenti informatici. Le persone dovranno invece concentrarsi maggiormente su aspetti di indagine ed approfondimento.

Con l'A.I. potenzialmente si riduce quindi la domanda di effort operativo, ma sta crescendo la domanda per altre professionalità. Da una prima indagine, effettuata immaginando una serie di possibili use cases per il machine learning, abbiamo verificato che ci sono, ad oggi, veramente poche persone nel mondo in grado di lavorare su questi temi in modo efficace.

IN PRIMO PIANO

Facebook: attenzione al "gattopardo"

Ezio Viola
Managing Director, The Innovation Group

Se c'è una cosa certa di Facebook dalla nascita della sua storia è che ha sempre privilegiato la crescita di utenti e del suo business rispetto al trattamento della privacy dei suoi utilizzatori.

Forse queste sono state le scelte di un Mark Zuckerberg giovane e sicuro di sè, confidente anche nelle magnifiche sorti e progressive di internet: sono state le scelte di chi stava costruendo un grande business sulla pubblicità e basato sulla raccolta e utilizzo di un numero infinto di dati.

Ora il CEO di FB è cresciuto, ha 34 anni, è famoso, ammirato, è anche un figura pubblica, spesso attaccata dalla stampa e dai politici in diversi paesi. Ha visto la sua azienda bruciare milardi di dollari di capitalizzazione per aver un po' "ignorato" i problemi di privacy degli utenti, ha visto la sua piattaforma digitale, che ha reso il mondo più aperto e connesso, essere usata da razzisti, violenti, terroristi e da paesi come arma anche contro la democrazia.

Così la reputazione di FB (e un po' anche la sua) è crollata, la crescita di utenti si è rallentata ed è diminuito anche il morale di chi in FB ci lavora. Insomma è arrivato il momento di cambiare qualcosa o forse di cambiare tutto.

Così Zuckerberg ha pubblicato 3000 parole sul suo blog qualche settimana fa delineando la nuova "privacy focus division" di Facebook incominciando cosi:

"Public social networks will continue to be very important in people's lives—for connecting with everyone you know, discovering new people, ideas and content, and giving people a voice more broadly. But now, with all the ways people also want to interact privately, there's also an opportunity to build a simpler platform that's focused on privacy first."

Vengono fatte molte promesse circa i miglioramenti sulle tecniche di encryption in FB e Instagram, su come spostare i server fuori dai Paesi autoritari dove possono essere spiati e su come ridurre la la memorizzazione e permanenza dei messaggi e delle storie generate dagli utenti.Viene anche descritto come si integreranno le tre piattaforme di messaggistica esistenti, (FB Messenger, Instagram Direct e Whatsapp), in modo da essere interoperabili.

Esse quindi non verranno unificate e ciò porterà alla generazione di dubbi su come potrà "facilmente" essere garantita la privacy e la sicurezza tra le tre piattaforme. Sono elencati anche i 6 Principi alla base della privacy ma non viene menzionato quale sarà l'approccio utilizzato per la condivisione dei dati e per le tecniche di "targeted adv". Questo è importante, tenendo conto che i problemi maggiori di FB sono nati proprio dal flusso di dati raccolti dalla piattaforma e ceduti a terze parti esterne come Cambridge Analytica e dalla messa a disposizione di questi flussi di dati a partner tecnologici, come costruttori di device e sviluppatori di software.

Queste cose Mark Zuckerberg le conosce molto bene e infatti scrive: "I understand that many

people don't think Facebook can or would even want to build this kind of privacy-focused platform—because frankly we don't currently have a strong reputation for building privacy protective services.." Quella prospettata sembra una rivoluzione copernicana nel social network ma sarà veramente così?

O siamo di fronte alla tecnica "gattopardesca" del cambiamo tutto affinché nulla o poco cambi?

Molti analisti e commentatori infatti si sono divisi tra chi pensa che siamo davanti ad un profondo cambiamento e chi pensa che si sia fatto troppo rumore per nulla. Probabilmente non è così perchè i cambiamenti annunciati, se realizzati, miglioreranno comunque la privacy dei più di 2 miliardi di utenti FB mensili e l'encryption end-to-end sarà cruciale anche per la loro sicurezza fisica, così come sarà meglio non avere i server di FB in Paesi pericolosi e non permettere più a FB di tenersi i nostri dati per sempre. Diamo quindi credito al CEO di FB e agli esperti che ha affermato essere già stati assunti in azienda per realizzare questi cambiamenti. L'annuncio di questi cambiamenti farà piacere ai regolatori sia europei (in attesa dopo l'avvio della GDPR) sia americani che stanno adottando misure che vanno in questa direzione.

Rimane però la domanda cruciale su quali diventeranno le priorità di FB in futuro, tenendo conto che la privacy non è gratis non solo per realizzarla ma anche per le conseguenze che su FB può avere. Infatti il news feed diventerà obsoleto, e tutto si concentrerà nelle chat private, per una comunicazione più intima e sicura. Queste chat saranno protette da crittografia end-to-end ed è difficile però "fare i poliziotti" su sistemi che sono encrypted end-to-end. Inoltre guidare le persone verso sistemi privati e intimi di messaggistica può presentare nuove sfide a chi vuole distribuire news sulla piattaforma oltre che ulteriormente "balcanizzare" il consumo di news e contenuti su FB.

Non è infatti un caso se non viene affrontata la questione più grande e cioè se questa visione e questi cambiamenti siano compatibili con l'attuale business model di FB che si fonda sull'utilizzo e la fornitura dei dati dei suoi utilizzatori.

Se questi cambiamenti saranno effettivamente realizzati, ci sarà un costo non solo per realizzarli ma anche sul business così come è oggi e bisognerà vedere fino a che punto FB sarà disposto a sopportarlo. Fino a quando non si capirà questo, non sapremo se la nuova privacy vision sia vera e realizzabile oppure solo un diversivo.

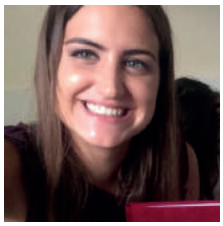
C'è comunque una parte molto interessante da considerare: se Facebook si concentrerà sempre più sui suoi sistemi di messaggistica potrebbe cercare di emulare il modello di WeChat, la superApp cinese di Tencent. Sappiamo anche che il modello di business di WeChat non si basa solo sulla pubblicità ma in gran parte sulla vendita e utilizzo di servizi come giochi, pagamenti etc.

Questo significherebbe una vera rivoluzione per FB ed è difficile oggi fare previsioni su quante possibilità ci siano per riuscirci senza compromettere crescita e profittabilità.

Una cosa è certa, quello che sta accadendo ci insegna che il flusso dell'innovazione comincia a muoversi al contrario da Est verso Ovest.

NUMERI E MERCATI

Business Intelligence, Analytics, Big Data: una triade sempre più vincente



Carmen Camarca
Analyst, The Innovation Group

Business Analytics, Data Management e Artificial Intelligence le principali iniziative della funzione ICT nel 2019 (intraprese dal 63% degli IT Manager), seguono progetti in ambito Security/Risk Management (61%) e strategie di Cloud Transformation (40%).

Lo rileva la Digital Business Transformation Survey 2019 condotta da The Innovation Group tra dicembre 2018 e febbraio 2019 e basata su un campione di 126 LoB Manager e 70 IT Manager.

Tra gli strumenti di Business Analytics e Business Intelligence maggiormente utilizzati la survey rileva che, ad oggi, le aziende prediligono Big Data Analytics (26%) e Predictive Analytics (19%), ambiti per i quali è previsto un significativo aumento nell'utilizzo anche tra tre anni, registrando una crescita pari rispettivamente al +115% e al +174%.

Aumenti rilevanti sono attesi anche per AI/ML Analytics, utilizzati oggi nel 19% dei rispondenti e tra tre anni dal 42% (+121%).

Tuttavia, sarà l'IoT Data Analytics (soluzioni analitiche generate dai dati provenienti dall'Internet delle Cose) la funzionalità di Business Intelligence a crescere di più, passando da una diffusione attuale del 9% ad una del 31%, con un incremento pari al +244%.

Analizzando, inoltre, i risultati per dimensione aziendale emerge che nei prossimi tre anni aumenterà l'utilizzo di Big Data Analytics soprattutto per le imprese piccole (51% delle risposte) e medie (63%); queste ultime, inoltre, intensificheranno anche le attività di Predictive Analysis (65,7%) e AI/ML Analytics (45,7%).

Non sono stimati, invece, cambiamenti significativi per le grandi imprese, nelle quali sin da ora viene rilevato un uso diffuso di tali strumenti.

Business Analytics sempre più indispensabile…

La survey rileva che gli ICT manager ricorrono all'utilizzo di dati e strumenti analitici per molteplici attività: dal web/market analytics (51%) al miglioramento dei processi di business (aumento efficienza/riduzione dei costi) e allo sviluppo di nuovi prodotti e servizi (46%).

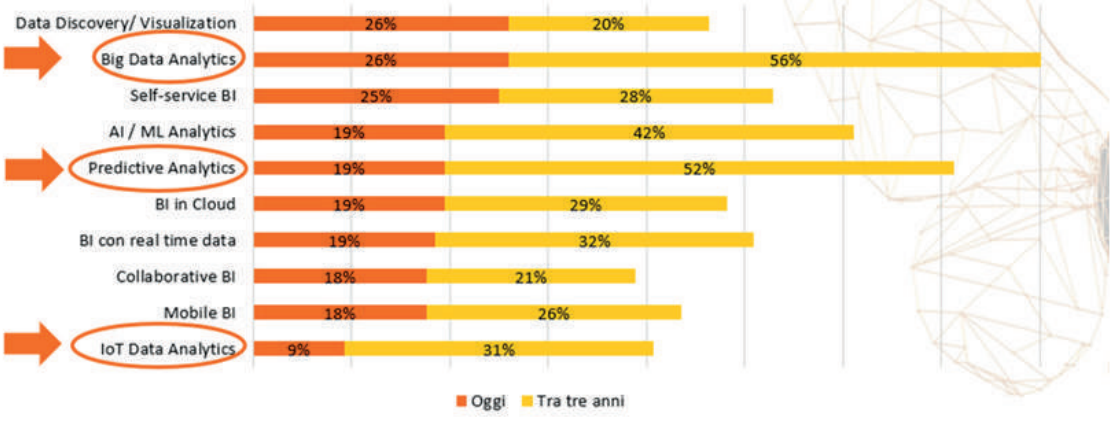
Con riferimento ai Big Data Analytics, il 64% del campione ha dichiarato di utilizzare soluzioni analitiche per costruire modelli predittivi e per poter svolgere migliori analisi sui propri clienti.

Tra le altre opportunità di utilizzo anche la possibilità di accelerare i processi di decision making in azienda (61%).

Le soluzioni volte all'analisi dei Big Data si estendono a diverse aree aziendali: se attualmente sono diffuse principalmente all'interno dei reparti Produzione/Supply chain (27%), Marketing (26%), Customer Service (23%), tra due anni ne sarà prevista la crescita soprattutto nelle divisioni Vendite (+83%) e Ricerca e Sviluppo (+217%).

BI abbastanza diffusa. Tra 3 anni previsto boom di Big Data Analytics, Predictive e IoT Analytics

Quali delle seguenti funzionalità delle piattaforme di Business Intelligence (BI) usate oggi/tra 3 anni?



Fonte: Digital Business Transformation Survey, TIG, gennaio 2019, N=78 rispondenti LoB Manager + N=30 IT Manager

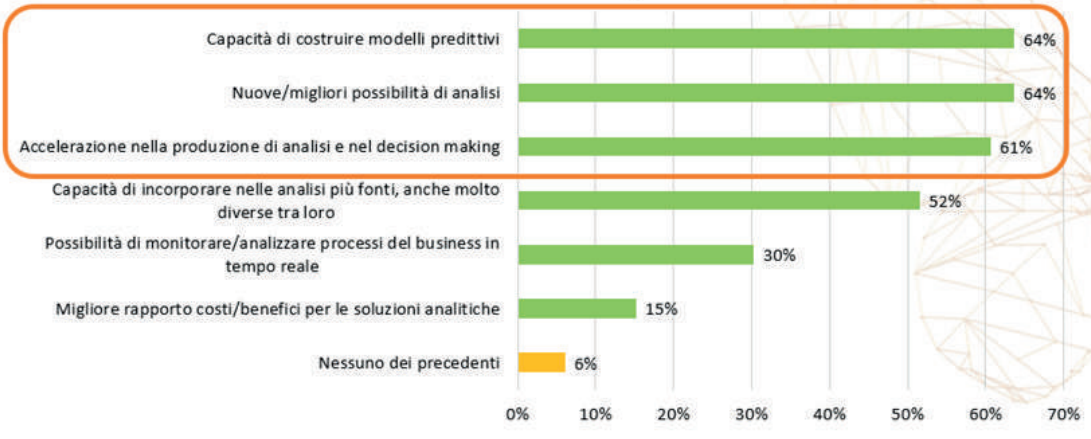
Business Analytics, molteplici utilizzi in azienda

Per quali ambiti la Sua azienda si basa sull'utilizzo di dati e strumenti analitici?

Fonte: Digital Business Transformation Survey, TIG, gennaio 2019, N= 87 rispondenti LoB Manager

Big Data Analytics: quale valore per l'azienda?

Quali delle seguenti opportunità pensate possano essere colte utilizzando soluzioni analitiche basate sui Big Data?



Fonte: Digital Business Transformation Survey, TIG, gennaio 2019, N= 33 rispondenti IT Manager

FOCUS PA

Comunicare sui social network: l'esperienza del Comune di Trieste

Intervista di **Alberico Vicinanza** a **Christian Tosolin**
Social Media Manager del Comune di Trieste

L'esperienza maturata e gli obiettivi raggiunti dall'amministrazione comunale di Trieste attraverso il percorso di attivazione e l'utilizzo dei social network. Il ruolo dell'Associazione PA Social nel miglioramento del rapporto tra cittadini e Pubblica Amministrazione.

Ne parliamo con Christian Tosolin, social media manager del Comune di Trieste.

Tosolin, il Comune di Trieste ha ormai acquisito una vasta conoscenza nell'utilizzo dei social media

Si, da cinque anni l'amministrazione comunale impiega i social media come strumento di informazione, condivisione, confronto e contatto con la cittadinanza.

Durante i primi anni la pagina Facebook e l'account Twitter sono stati gli unici canali attivi, arrivando in breve tempo ad un'ampia platea ed un coinvolgimento sempre maggiore, sia in termini di reaction che nell'utilizzo della messaggeria diretta come sportello virtuale, per fare domande e segnalazioni.

Un coinvolgimento dei cittadini, all'inizio impensabile, i quali hanno ristabilito mediante Facebook e Twitter un rapporto diretto con il loro Comune, attingendo informazioni in tempo reale e potendo inviare richieste e segnalazioni in maniera diretta, senza doversi muovere da casa, in qualsiasi ora della giornata e ricevendo una risposta nell'arco di poche ore. Ormai la strada di una comunicazione smart a quel punto era tracciata.

Poi avete attivato il canale Instagram

Con l'attivazione di Instagram, che rappresenta il canale più frequentato dai giovani, abbiamo cominciato ad interagire con la fascia della popolazione meno abituata ad entrare in contatto con il municipio.

Con Instagram oltre a postare quotidianamente delle immagini della città, abbiamo testato per il primo anno, un progetto di partecipazione civica chiedendo a chi avesse voluto di mettersi in gioco e diventare amministratore dell'account del Comune per due settimane.

Questo è stato il trampolino di lancio per far conoscere il canale e coinvolgere i cittadini.

L'utilizzo delle stories è stato il miglior sistema per attirare l'attenzione della fascia di cittadini che va dai 18 ai 25 anni, la quale è attualmente quella che segue maggiormente il canale.

Tramite le stories riusciamo a veicolare contenuti e alcune conferenze stampa, che difficilmente un giovane avrebbe intercettato mediante la comunicazione tradizionale.

Telegram e Linkedin hanno consentito, poi, l'attivazione di un sistema di comunicazione specifico per segnalare alla città le opportunità di lavoro e le emergenze del territorio

Per la comunicazione su Telegram abbiamo coinvolto la Polizia Locale che riceve questo tipo di informazioni in tempo reale e Trieste Trasporti S.p.A. la società dei trasporti pubblici di Trieste.

Con Linkedin abbiamo sentito l'esigenza di aprire un nuovo canale di informazione per i cittadini, che crediamo possa incentivare il lavoro e le relazioni interne all'Amministrazione facendo convergere tutte le notizie riguardanti i concorsi pubblici che il Comune di Trieste vuole lanciare e le informazioni riguardanti le opportunità di tirocini, in Italia o all'estero.

Il passo successivo, infine, sarà quello di attivare un gruppo Linkedin associato alla pagina, per mettere in comunicazione i dipendenti del Comune, abbattendo così i compartimenti stagni che spesso si creano all'interno delle aziende pubbliche e favorendo un confronto tra diversi ambiti e competenze.

Tosolin lei è anche membro del Comitato promotore dell'Associazione PA Social

La mia esperienza come social media manager è maturata attraverso il contatto diretto con il cittadino, imparando a conoscere il "pubblico" del Comune di Trieste, capendone sempre di più le necessità, ascoltandone le richieste, analizzando il sentiment e cercando di adeguare la comunicazione dell'amministrazione comunale a chi vive quotidianamente la città.

Un aiuto fondamentale nella mia crescita professionale è stato e lo è tutt'ora, quello di far parte dell'Associazione PA Social, che oltre ad essere una rete nazionale di comunicatori e giornalisti, rappresenta un punto di riferimento per chi vuol condividere conoscenze ed esperienze ed una casa comune per tutti coloro che vogliono migliorare, giorno per giorno, il paese.

Un progetto nato dal suo Presidente, Francesco Di Costanzo, e spinto dalla voglia di migliorare il rapporto tra cittadini e Pubblica Amministrazione, che si sta evolvendo in concrete azioni a beneficio di tutti mettendo in luce, finalmente, il lavoro di quei dipendenti pubblici mossi da un senso civico, ma che spesso non riescono a ricevere il giusto riconoscimento e una piena valorizzazione delle loro capacità.

LA TRASFORMAZIONE DIGITALE

Collaborazione ed Orchestrazione in Azienda

Vincenzo D'Appollonio
Partner, The Innovation Group

Come ho già avuto modo di scrivere, capita spesso, durante le mie attività di Management Consulting per le PMI lombarde, di constatare come lo stile di gestione aziendale, applicato 'spontaneamente' ed in modo 'non strutturato' soprattutto in quelle piccole realtà di impresa industriale di origine artigiana, con pochi soci tutti 'operativi' spesso appartenenti allo stesso nucleo famigliare, e con un numero massimo di 20-30 dipendenti, sia assimilabile a modelli organizzativi di 'Management Collaborativo', inteso come l'atto di lavorare 'insieme come una squadra' per raggiungere un obiettivo comune entro un determinato periodo di tempo, basato sul principio della partecipazione attiva di tutti i membri del team nel processo di pianificazione e controllo, nonché nella condivisione di informazione, comunicazione e esperienza di collaborazione: dove dunque la gestione dell'azienda non è considerata un'attività riservata esclusivamente ai dirigenti, ma come parte integrante del lavoro di squadra di tutti i membri del team.

Ma, attenzione, in generale un insieme di individui non diventa una squadra solo perché gli è stato imposto l'appellativo di 'squadra': ci sono molti processi culturali, psicologici e comportamentali che devono essere proposti ed assimilati affinché un gruppo di lavoro funzioni come un 'organismo aziendale'. Creare squadra non è semplice: ogni gruppo di lavoro è diverso, ma alcune 'regole metodologiche' di cui hanno bisogno le squadre per essere vincenti sono universali.

Occorre dare priorità alle abilità sociali per creare un gruppo di lavoro vincente, mettendo insieme persone che rendano bene in una dinamica sociale: chi sa ascoltare gli altri, chi sa condividere le critiche in modo costruttivo, chi ha una mente aperta. Bisogna costruire un ambiente in cui la Fiducia tra colleghi sia un fattore indispensabile: ciò permette di rendere un gruppo di lavoro pronto a superare ogni difficoltà.

Il successo del lavoro di una squadra passa necessariamente dall'individuazione di un Obiettivo, chiaro e preciso. Per lavorare in team è fondamentale identificare una Mission, in modo da aver chiara la direzione verso cui orientare l'operato e capire quali strumenti scegliere, come strutturare il gruppo e quali precisi compiti e chiari ruoli affidare. Occorre infine una Comunicazione interna Aziendale concisa, chiara e trasparente: l'obiettivo di comunicare in azienda deve essere quello di distribuire le informazioni in maniera efficace, rendendole disponibili a coloro che le utilizzano per il lavoro da svolgere.

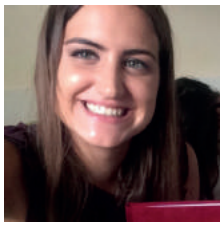
Si tratta, in estrema sintesi, di fare dell'eterogeneità un valore aggiunto, essere organizzati operativamente e focalizzati, avere un metodo condiviso, avere elasticità mentale, avere una motivazione di gruppo e non solo individuale, sostenere la crescita di squadra e

il perseguimento dell'obiettivo. Il ciclo virtuoso che ne consegue comporta coesione, relazione tra i componenti, maggiore produttività e maggior soddisfazione e senso di realizzazione. È fondamentale che ogni membro abbia bene in mente il proprio ruolo per riuscire ad operare in autonomia, evitando di interferire con l'operato altrui, in una collaborazione costruttiva.

Tutto ciò si chiama Orchestrazione Aziendale, ovvero l'arte e la tecnica di distribuire e combinare insieme gli interventi dei vari strumenti dell'orchestra (i componenti della Squadra Aziendale) nella partitura (Piano Strategico); può consistere sia nella scelta degli strumenti con cui realizzare un'idea musicale (Business Plan), sia nella trascrizione per orchestra di un brano scritto originariamente per un organico ristretto o per un solo strumento (Management Collaborativo). Se si vuole ricreare anche in azienda lo stesso clima di energia e di positività che pervade un'orchestra, è necessario dunque che siano garantiti due presupposti fondamentali: condivisione di obiettivi e definizione di una metodologia di base; in queste condizioni, ogni persona si sentirà stimolata a dare un contributo personale (Improvvisazione creativa) alla sua prestazione in Squadra.

LA TRASFORMAZIONE DIGITALE

AI: The Next Big Thing. L'evento di The Innovation Group alla Milano Digital Week



Carmen Camarca
Analyst, The Innovation Group

Lo scorso 14 marzo, presso il Palazzo dei Giureconsulti e nell'ambito della Milano Digital Week, si è tenuto l'evento "Artificial Intelligence e il futuro della nostra società – Per un approccio Human-centric all'Artificial Intelligence". Nella discussione, promossa da The Innovation Group, sono stati confrontati i diversi approcci alle sfide che il rapido sviluppo dell'Intelligenza Artificiale ha posto, così da fornire un adeguato sostegno a tutti gli stakeholder coinvolti.

Lo scorso 14 marzo, nell'ambito della Milano Digital Week, The Innovation Group ha organizzato, in collaborazione con l'Ambasciata Britannica in Italia e lo UK Government Science and Innovation Network, l'evento "Artificial Intelligence e il futuro della nostra società – Per un approccio Human-centric all'Artificial Intelligence". La discussione, a cui hanno partecipato esponenti del mondo accademico e scientifico sia nazionale che internazionale, della Pubblica Amministrazione nonché di aziende private, è stata un'occasione per creare un solido dibattito attorno ai temi dell'Artificial Intelligence, illustrare i diversi approcci e strategie sviluppati per far fronte alle sfide che il suo rapido sviluppo pone.

Ad aprire i lavori KenO'Flaherty, Vice Ambasciatore Britannico in Italia, che ha ricordato le iniziative di Artificial Intelligence promosse dal governo britannico: dagli accordi di settore tra industria e ricerca agli investimenti finora stanziati dal governo britannico (quasi un miliardo di sterline). È stata ribadita, inoltre, l'importanza di sviluppare collaborazioni internazionali volte a promuovere knowledge sharing, soprattutto con l'Italia (nono partner commerciale di Londra) per rafforzare la crescita economica, creare forme di lavoro sostenibile e accrescere il benessere dei cittadini.

Ha seguito l'intervento di Roberto Masiero, Presidente The Innovation Group, che ha sottolineato la necessità, sia per l'Italia che per l'Europa, di individuare strategie per competere con i giganti internazionali: a tal proposito è stato più volte menzionato un approccio all'AI "human centric", focalizzato sulle persone e sulle loro esperienze nonché sulle potenzialità del cervello umano.

Il Presidente ha, inoltre, posto l'accento sulle iniziative europee ed italiane in ambito AI: l'Europa, attualmente impegnata con il Piano "AI Made in Europe", lanciato nel 2018, propone, tra le altre cose, lo stanziamento di 20 miliardi di euro di investimenti pubblici e privati in AI per il periodo 2018-20 e ogni anno a partire dal 2021. Tale obiettivo, senz'altro ambizioso, fa ancora fatica a reggere il passo con l'entità dei fondi erogati dai competitor Usa e Cina.

Per quanto riguarda l'Italia, invece, la Digital Business Transformation Survey 2019 di The Innovation Group, ha rilevato, allo stato attuale,

una scarsa rilevanza dell'AI nelle strategie aziendali, uno scenario destinato a mutare in maniera significativa nei prossimi cinque anni, dove le soluzioni di Intelligenza Artificiale raggiungeranno ampia diffusione in qualsiasi strategia di business.

Il dibattito è stato, inoltre, animato da due panel. Il primo relativo allo stato attuale della ricerca AI, tenendo conto, in particolar modo, delle strategie e delle politiche messe in atto da Italia e UK: a tal proposito interessanti le testimonianze di Rita Cucchiara, Direttore Laboratorio Nazionale di Intelligenza Artificiale e Sistemi Intelligenti del CINI e Allaine Cerwonka, Direttore Area Partnership The Alan Turing Institute che hanno esposto le principali iniziative promosse dai rispettivi istituti.

In particolar modo è stata posta l'attenzione sui rischi, per l'Europa e soprattutto per l'Italia, di sviluppare progetti simili a quelli promossi da Cina e Usa: qualsiasi piano di azione deve essere creato a partire dalle peculiarità del contesto produttivo e macroeconomico del territorio di riferimento.

Nel secondo panel, invece, sono stati affrontati i potenziali cambiamenti che l'Artificial Intelligence creerebbe in qualsiasi mercato: da cosa accadrebbe alla produttività ai cambiamenti etici e sociali (quali variazioni per le dinamiche occupazionali e quali gli impatti previsti per le professioni del futuro).

A tal proposito Alberto Fioravanti, Presidente Digital Magics, ha suggerito lo sviluppo di un approccio volto all'open innovation, basato su forti collaborazioni tra aziende e startup specializzate; secondo Cristiano Radaelli, Vice Presidente Vicario, Anitec-Assinform, invece, bisognerà attendere ancora qualche anno prima di poter godere dei benefici, soprattutto in termini di produttività, dell'AI.

Infine, di spicco il tema del digital skill mismatch, affrontato da Marco Bentivogli, Segretario Generale FIM CISL, secondo cui per cogliere le sfide tecnologiche, quelle attuali, ma soprattutto quelle future, sarà necessario un nuovo approccio culturale aziendale.

Affrontare le sfide tecnologiche e cercare di cogliere quanto più possibile l'opportunità dei cambiamenti in essere saranno i primi passi per la creazione di un nuovo welfare, sociale ed aziendale, sostenibile per chiunque.

Roberta Cocco: "La Pubblica Amministrazione deve promuovere lo scambio e il dialogo tra le parti"

Al di là dell'ormai noto gap, l'Italia, soprattutto a partire dagli ultimi anni, ha fatto numerosi progressi.

Esordisce così Roberta Cocco, Assessore a Trasformazione digitale e servizi civici-Comune di Milano nel suo intervento conclusivo.

Senz'altro, continua Roberta Cocco, l'AI viene accolta con timore da parte delle persone, delle aziende e delle stesse amministrazioni pubbliche, ma non va dimenticato che essa porta con sé un'inevitabile natura umana: l'AI è frutto dell'intelligenza umana, sono gli uomini a governarla e a praticarne gli algoritmi.

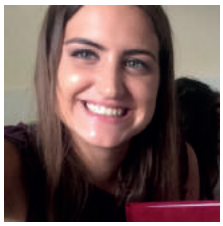
"Il nostro ruolo, dunque, in qualità di istituzione, è quello di promuovere e facilitare il dialogo tra due ecosistemi, quello pubblico e quello privato, così differenti tra di loro, promuovendone l'interazione.

Se davvero riusciremo in quest'intento allora raggiungeremo il fine ultimo, ovvero la semplificazione: semplificare la vita ai nostri cittadini, che si tratti di aziende, di studenti, di istituti di ricerca sarà sempre la nostra priorità e in questo l'Intelligenza Artificiale può davvero aiutarci."

Il Comune di Milano - ha concluso - sta lavorando molto per un piano di trasformazione digitale ampio collaborando anche con altre città italiane: è vero che l'Italia ha ancora molta strada da fare, secondo gli esperti il nostro gap digitale è di circa dieci anni ma se continueremo a lavorare come abbiamo finora lo risolveremo.

BANCHE E FINTECH

Cosa cambia con la MIFID 2 e come evolve l'industria dell'Asset & Wealth Management



Carmen Camarca
Analyst, The Innovation Group

Come già più volte affermato, la Mifid 2 è stata l'ultima di una serie di cambiamenti che negli ultimi anni hanno impattato i mercati finanziari nazionali e internazionali.

La nuova normativa sulla cost trasparency, entrata in vigore ormai un anno fa, esprime, inoltre, i suoi principali effetti in un momento non particolarmente favorevole per i mercati finanziari, soprattutto per quello italiano, caratterizzato da andamenti negativi, prospettive economiche poco favorevoli e crescita lenta.

Delle novità introdotte dalle nuove disposizioni e di quali iniziative concrete sono state avviate per farne fronte si è discusso lo scorso 27 febbraio al Digital Investment Management, primo workshop organizzato da The Innovation Group all'interno del Banking Program 2019 e volto a valutare gli impatti delle nuove disposizioni soprattutto per gli asset manager e per le reti distributive.

A un anno dall'entrata in vigore della MIFID 2 si può, dunque, affermare che essa ha:

- richiesto a tutte le aziende del settore (sia manufacturing che distributrici) di dedicarsi molto di più agli aspetti burocratici a scapito del cliente. È bene, dunque, che il mercato torni a focalizzarsi sulle esigenze dei clienti, non sottovalutando l'importanza dei rapporti e dell'interazione con gli stessi;
- reso più complessi i processi di product governance con conseguente deterioramento del modello dell'open architecture nell'offerta dei prodotti di risparmio gestito;
- creato elevate pressioni sui costi, soprattutto per le asset class meno redditizie.

In questo contesto per gli asset manager si viene a creare la necessità di:

- intensificare l'utilizzo dell'Artificial Intelligence (in particolar modo degli strumenti di analisi e raccolta dati);
- ridisegnare la value proposition e diversificare il portfolio d'offerta (investimenti alternativi come private equity, fondi immobiliari, affiancati anche a fondi di nicchia come le commodity), correlandolo a specifici target di clientela;
- dimostrare capacità di transformation, ovvero di affrontare e realizzare il cambiamento.

Le reti distributive, invece, dovranno:

- estendere la value proposition a tutto il patrimonio complessivo dei clienti, non occupandosi, quindi, di gestire solo la ricchezza finanziaria;
- evolvere le logiche di asset allocation, a fronte di un'offerta di prodotti (siano essi attivi, passivi, alternativi) più complessa;

- affrontare la digitalizzazione a fronte dell'evoluzione dei comportamenti dei clienti e del fenomeno del passaggio intergenerazionale (i clienti del futuro saranno, infatti, i Millenials);
- ridurre la complessità della product governance e promuovere maggiore interazione e dialogo tra produttori e distributori per sviluppare modelli di apertura e condivisione con gli altri operatori.

Se, tuttavia, da un lato l'introduzione della MIFID II ha reso più complesse le dinamiche di erogazione e gestione dei prodotti e dei servizi, dall'altro lo sviluppo e l'applicazione del digitale mette a disposizione dei consulenti diverse opportunità per efficientare i processi e migliorare le relazioni con i clienti, anche se il mercato italiano a tal proposito è da considerarsi ad uno stadio ancora iniziale.

Finora, infatti, il settore dell'Asset & Wealth Management italiano è stato caratterizzato da elevate barriere all'ingresso e da una forte resistenza al cambiamento, ma per il futuro la principale raccomandazione sarà quella di accettare i nuovi trend, adeguandovisi. Si tratta di evoluzioni di una rilevanza tale da rimescolare tutte le carte dei modelli di business: sebbene gli interrogativi siano ancora molti e manchi un business model di validità universale, nei prossimi anni il successo e la ricchezza di ogni Paese saranno determinati dall'aver saputo dare risposte efficaci ai cambiamenti in atto sul mercato.

A fronte di queste trasformazioni, per l'industria finanziaria italiana potrà essere utile anche iniziare a sperimentare modalità di collaborazione con altri player (bancari e non), adottando modelli operativi volti all'open banking: le dinamiche e le strutture su cui si fonda l'attuale industria finanziaria italiana non saranno in grado, da sole, di recepire i nuovi stimoli del mercato. In questo contesto potrebbe rivelarsi strategica la cooperazione con attori che pur esulando dal contesto bancario e finanziario svolgono attività di banking: si pensi, ad esempio, al mondo retail e ai due giganti dell'e-commerce Amazon ed Alibaba e ai loro servizi di pagamento Amazon Pay e Alipay o agli altri "big" come Apple, Google, Facebook e Microsoft. Questi temi verranno trattati il prossimo 15 maggio nell'ambito dell'evento "Open Banking- Sarà questo il futuro del banking e delle banche?", organizzato da The Innovation Group nell'ambito del Banking Program 2019 e volto ad analizzare gli effetti della PSD2, un'altra normativa che ha impattato in maniera significativa i diversi operatori dell'ecosistema finanziario, promuovendo una nuova stagione di partnership e collaborazioni tecnologiche.

CONNECTED MOBILITY

Lavori in corso sulle Smart Road del futuro

Elena Vaciago
Associate Research Manager, The Innovation Group

Uno dei mercati in cui nei prossimi anni assisteremo a un'esplosione di nuovi servizi, nuovi modelli di business e un'innovazione sempre più spinta dell'esperienza d'uso degli utenti è quello della Mobilità Connessa e Autonoma.

Le più recenti stime parlano di vendite di auto connesse che raggiungeranno i 35 miliardi di dollari entro il 2025, con Stati Uniti, Europa e Cina che si contenderanno la posizione di predominio del mercato.

Maggiore confort, più sicurezza sulle strade, funzioni avanzatissime di cui già oggi si vedono i primi prototipi; ma anche tempo liberato dalla guida e potenzialmente fruibile per attività di intrattenimento e nuovi servizi erogati in mobilità; e infine, cambiamento delle abitudini dei consumatori, sempre più interessati a fruire di servizi di Mobility-as-a-service, erogati da app su mobile, in grado di presentare molteplici scelte alternative all'auto di proprietà (quindi car sharing, flotte, car-pooling, servizi collaborativi e peer-to-peer). Saranno questi i driver della mobilità del futuro.

CHI GUIDERA' IL MERCATO DELLA CONNECTED E AUTONOMOUS CAR?

Gli Stati Uniti hanno finora guidato le sperimentazioni di auto connesse e autonome, con un esempio su tutti, l'auto autonoma Waymo di Google, che ha percorso fino ad oggi almeno 10 milioni di chilometri su strada e ha simulato virtualmente oltre 4,3 miliardi di chilometri nel solo 2017, e punta ora alla profittabilità tramite il lancio di servizi commerciali.

Waymo One, lanciato a dicembre 2018 per l'area di Phoenix in Arizona, è il nuovo servizio circa al costo di Uber, ma per ora impiega anche Safety Driver umani dietro il volante ed è stato aperto a un pubblico ristretto (400 persone) che avevano già testato in precedenza il servizio Google.

L'Arizona è tra gli Stati americani che hanno favorito maggiormente le sperimentazioni dell'auto autonoma, tanto che Waymo ha annunciato di recente che raddoppierà i suoi investimenti e stabilimenti nell'area (con il nuovo Technical Service Center di Mesa), creando quindi nuovi posti di lavoro.

Inoltre Waymo ha anche cominciato a commercializzare le proprie tecnologie (il sistema di sensori per la realizzazione delle mappe virtuali) ad altri player del settore dei veicoli autonomi.

L'Europa però non è rimasta a guardare e sta facendo passi avanti, e l'obbligo dell'eCall (la chiamata di emergenza presente su tutti i nuovi veicoli omologati) porterà anche da noi ad avere nel giro di qualche anno un ampio parco circolante di veicoli connessi.

Nel contempo, le infrastrutture stradali diventeranno sempre più "intelligenti", in grado di dialogare con i veicoli e di fornire tutta una serie di nuovi servizi a valore aggiunto: un

esempio di cosa sarà possibile è quanto sta sperimentando nel Regno Unito la Jaguar Land Rover con UK Autodrive (consorzio che per 3 anni ha guidato la sperimentazione di tecnologie per le auto connesse e autonome, nell'ambito di una competizione del Governo UK "Introducing Driverless Cars").

I NUOVI USE CASES DELLA MOBILITA' SMART E CONNESSA IN V2X E V2V

Gli obiettivi dei test di Jaguar Land Rover sono stati:

1. Aumentare la sicurezza, tramite avviso in caso di collisione frontale e posteriore, di incidenti o traffico intenso sul percorso (questo con la comunicazione tra i veicoli, il protocollo V2V, Vehicle-to-vehicle, denominato Intersection Collision Warning), frenata automatica d'emergenza, mantenimento in carreggiata e riconoscimento automatico dei segnali inviati dalla Smart Road con comunicazione V2X (veicolo verso l'infrastruttura);
2. Minimizzare le soste al semaforo: la tecnologia Green Optimal Speed Advisor consente di dialogare con i semafori e informare il guidatore sulla velocità da tenere in prossimità degli incroci, per trovare il semaforo verde;
3. Ridurre i consumi, riducendo ad esempio l'incidenza di frenate e accelerazioni tramite Cruise Control Adattativo (una delle funzioni dei nuovi sistemi ADAS, Advanced Driver Assistance Systems);
4. Ridurre lo stress del guidatore, ad esempio con il Collaborative Parking (assiste il guidatore nella ricerca di un parcheggio indicandogli gli spazi liberi) o con l'Emergency Vehicle Warning (segnala al conducente l'approssimarsi di un veicolo d'emergenza come ambulanza e altro).

LA STRATEGIA ITALIANA PER LE SMART ROAD

Da segnalare anche i percorsi già avviati in questo senso nel nostro Paese, dove l'approvazione nel febbraio 2018 del Decreto Smart Road ha portato adindividuare le modalità con cui sviluppare strade e autostrade che possano dialogare con i veicoli, ottimizzando la gestione del traffico e aumentando la sicurezza di guida, e ha autorizzato la sperimentazione su strada di veicoli a guida autonoma. Iniziative già avviate per le smart road del futuro sono in Italia:

- Il progetto "5G-Carmen", coordinato dalla Fondazione Bruno Kessler di Trentocon la partecipazione di altri 25 partner, finanziato dalla UE evolto a creare un corridoio digitale lungo i 600 chilometri di autostrada tra Monaco e Bologna. Basato sulla sperimentazione della tecnologia 5G servirà a testare come ottenere una migliore risposta in termini di velocità di scambio di dati e tempi di reazione dell'infrastruttura di rete per l'implementazione di veicoli connessi, cooperativi e automatizzati di nuova generazione.
- Il progetto MASA, Modena Automotive Smart Area, nato con l'obiettivo di sviluppare un'area urbana da utilizzare per la sperimentazione dei veicoli di nuova generazione (con la partecipazione di 3 attori principali, il Comune di Modena, l'Università di Modena e la Maserati, a cui si sono uniti altri partner, fortemente interessati a questi sviluppi), e a cui si è anche aggiunto l'autodromo di Modena per studiare i veicoli autonomi in un ambiente privato. L'area MASA si è quindi attrezzata per offrire competenze e infrastrutture abilitanti i test e quindi una "certificazione sul campo". In questo modo car maker, componentisti e altri ricercatori potranno provare i sistemi da portare nei prossimi anni su un mercato che, come emerge anche dagli sviluppi internazionali, sta evolvendo molto rapidamente.
- A Torino è stato firmato il Protocollo di Intesa tra il Comune, FCA e altri 13 partner per la sperimentazione dell'auto a guida autonoma di livello 3. Il capoluogo piemontese sarebbe già pronto a sperimentare il minibus elettrico e a guida autonoma "Navya be fluid", ma serve una norma ad hoc del MIT. Il van gode di un'autonomia di 13 ore, comunica con 17 satelliti, ha sensori per rilevare pedoni e ciclisti, ed è già in uso nei centri storici, nelle stazioni, nei porti e aeroporti di Australia, Spagna e Francia.
- Le sperimentazioni della mobilità connessa con 5G (quello che ad oggi è visto come standard di riferimento per i servizi futuri di questo tipo, in grado di abilitare segnalazioni in real time tra oggetti in reciproco movimento e connettività sicura per situazioni in cui è in gioco la stessa safety delle persone) stanno anche avvenendo in varie città italiane, Bari, L'Aquila e Milano. A Bari il 5G sarà usato per testare servizi relativi alla sicurezza e al controllo di merci e accessi. A L'Aquila è in corso un progetto dedicato ai veicoli connessi e autonomi che utilizza veicoli Ducato di FCA. A Milano con Vodafone sono in corso test relativi a un sistema di pubblica sicurezza (attraverso videocamere veicolari mobili connesse) e consegne dell'ultimo miglio tramite Yape, il veicolo elettrico ultraleggero a guida autonoma di e-Novia.

DIRITTO ICT
IN PILLOLE

Cosa accade se un contratto di licenza d'uso di software personalizzato non mantiene le promesse

Giulia Rizza
Consultant, Colin & Partners

Il Tribunale di Milano, con la sentenza n. 5752/2017, ha chiarito che un contratto di licenza d'uso software che preveda anche l'implementazione di personalizzazioni ad hoc costituisce un'obbligazione di risultato.

Cosa significa in pratica? Indica che, qualora non sia possibile raggiungere e realizzare la concreta utilità pattuita dal contratto stipulato, il committente potrà – in modo legittimo - procedere alla risoluzione dello stesso. Non solo, avrà anche la possibilità di richiedere la restituzione degli importi già versati e il risarcimento dei danni subiti.

> Qualora non sia possibile raggiungere e realizzare la concreta utilità pattuita dal contratto stipulato, il committente potrà, in modo legittimo, procedere alla risoluzione dello stesso

Il caso in breve

La decisione del Tribunale di Milano prende le mosse da due contratti collegati, stipulati fra una società editrice e una software house. Più precisamente, un primo contratto stipulato tra le parti prevedeva la fornitura di un software, con personalizzazioni ad hoc implementate sulla base delle specifiche esigenze della committente. Con il secondo contratto, invece, la software house si impegnava a realizzare un'interfaccia finalizzata alla comunicazione tra il programma stesso e il nuovo sito web, che la società editrice si apprestava a realizzare.

La società editrice si era tuttavia rifiutata di corrispondere il prezzo concordato per la fornitura dei servizi, tenuto conto dell'impossibilità di utilizzare il software sviluppato per soddisfare le esigenze sottese ai contratti.

Ciò a seguito di significative carenze da parte del fornitore e del verificarsi di importanti malfunzionamenti e criticità, come ad esempio la presenza di errori di progettazione, il mancato funzionamento di essenziali implementazioni, la mancanza di un preventivo studio di fattibilità del progetto e l'assenza di manualistica.

In prima battuta era stata la stessa software house a ricorrere alle vie legali, per ottenere in via coattiva il pagamento non corrisposto dalla committente. Quest'ultima, per contro, non solo si era opposta a tale pretesa, ma aveva successivamente intrapreso un ulteriore giudizio lamentando l'inadempimento dei contratti da parte della software house e chiedendone quindi la risoluzione.

Il Tribunale di Milano, all'esito del giudizio, ha rigettato le pretese della software house rispetto ai crediti richiesti e ha dichiarato la risoluzione dei contratti, con conseguente condanna alla restituzione dell'acconto già corrisposto e al risarcimento dei danni subiti a seguito del verificarsi dei malfunzionamenti.

Cosa significa questa sentenza?

Se è pur vero che la committenza avrebbe a disposizione strumenti contrattuali di tutela (si pensi alla previsione di clausole penali, peraltro dovute anche in assenza di prova del danno), la decisione del Tribunale definisce una questione che prescinde dalla forza e dalla capacità negoziale delle parti: indipendentemente dalla qualificazione formale del contratto, l'obbligazione di fornitura di un software personalizzato in licenza d'uso rientra nell'ambito delle obbligazioni di risultato.

Si tratta di un punto importante nella dinamica domanda-offerta: in simili ipotesi, infatti, la semplice esecuzione della prestazione utilizzando la diligenza richiesta dall'incarico non può ritenersi sufficiente affinché il fornitore sia considerato adempiente, ma occorre che questi abbia raggiunto il risultato pattuito. In caso contrario, al verificarsi di determinate condizioni, potrà essere contestato l'inadempimento contrattuale.

Il Tribunale di Milano ha accolto le richieste della committente in quanto i malfunzionamenti lamentati, e successivamente accertati tramite perizia tecnica nel corso del giudizio, consentivano l'attivazione di solo alcune delle funzionalità concordate. Il giudizio sull'inadempimento della software house si fonda dunque sul mancato raggiungimento delle concrete utilità che la stessa si era impegnata a far conseguire alla committente, rappresentate, nel primo contratto, dall'autonoma fruizione del software da parte di quest'ultima e, nel secondo, dal funzionamento dell'interfaccia finalizzata all'interazione tra il software stesso e il nuovo sito.

Per quanto riguarda il risarcimento del danno, i giudici milanesi hanno ritenuto provato il pregiudizio economico rappresentato dal mancato guadagno per la ritardata pubblicazione del nuovo sito. A seguito di quest'ultima, infatti, il fatturato della società editrice è nettamente aumentato. Il Tribunale ha quindi condannato la software house a corrispondere alla committente l'importo che, ragionevolmente, sarebbe stato incassato da quest'ultima se il fornitore avesse rispettato le tempistiche pattuite.

Una sentenza che richiama l'attenzione sulle ricadute che la contrattualistica riveste nell'andamento finanziario e operativo delle imprese. La reciproca consapevolezza di ruoli ed obblighi e un'attenta revisione degli accordi, sono fondamenta necessarie per sviluppare progetti sostenibili.

CYBERSEC E DINTORNI

Facing Forward: il cyber nel 2019

Chiara Zaccariotto
Office Manager ANRA e Direttore Responsabile www.anra.it

Cyberspionaggio industriale, attacchi alle infrastrutture critiche, uso politico dei social network, operazioni dirette dall'alto: sembrerebbero queste le tendenze 2019 nel mondo del cyber risk, secondo il report Facing Forward – Cyber Security in 2019 and Beyond pubblicato da FireEye. Il documento, frutto delle analisi di una serie di esperti della società di sicurezza informatica e corredato dal commento dell'AD della società Kevin Mandia, che ha in curriculum anche diversi anni nel reparto sicurezza del Pentagono, può essere un utile spunto di riflessione per tutti gli operatori del settore.

Un'etica condivisa tra nazioni

Mandia racconta come gli capiti spesso, durante i suoi viaggi e gli incontri con funzionari governativi di tutto il mondo, di sentirsi rivolgere la medesima domanda, indipendentemente dal paese in cui si trova: "Che sia in Medio Oriente, Europa, Asia o Nord America, mi chiedono come poter sviluppare una capacità offensiva per la propria nazione". Dunque non solo strategie difensive, in campo di cybersecurity gli Stati sembrano sempre più protesi a definire anche strategie di attacco. "Alcuni sostengono che le nazioni non dovrebbero farlo, che è poco etico, ma nelle sale dei governi in tutto il mondo probabilmente i funzionari stanno pensando che il proprio Paese debba essere pronto a scatenare azioni offensive per non doverle subire, e per potersi difendere", spiega Mandia. Il problema è che ad oggi, non esistendo un quadro normativo di riferimento unico, i rischi e le conseguenze per chi è responsabile di crimini informatici sono ancora piuttosto incerte, le zone grigie così estese da permettere ad una potenza come la Russia di condurre attività di spionaggio senza di fatto pagare altro se non uno scotto in termini

LA SICUREZZA E I DIRITTI INFORMATICI SONO UN PROBLEMA GLOBALE, CHE NON PUÒ ESSERE AFFRONTATO SE NON CONCERTANDO INTENTI E SOLUZIONI

reputazionali (a cui comunque sembra non dare troppo peso). E' una questione diplomatica: la sicurezza e i diritti informatici sono un problema globale, che non può essere affrontato se non concertando intenti e soluzioni. Se arrivare a una dottrina universalmente condivisa è un'utopia, può non esserlo lavorare insieme per arrivare a una serie di regole comuni che mitighino il rischio cyber a carico di Stati, imprese, individui.

Manipolazione politica sui social media

Il secondo macro trend individuato per il 2019 non è un'assoluta novità: l'utilizzo dei social network per operazioni di social engineering o di phishing. Quest'anno, secondo l'esperta IT Sandra Joyce, si rafforzerà l'impiego delle piattaforme di condivisione come strumento di propaganda politica: "L'obiettivo potrà essere quello di promuovere un particolare partito politico, che potrebbe essere più amichevole verso specifiche politiche estere, o di guidare una narrazione politica, causando conflitti all'interno del Paese", spiega, ricordando casi eclatanti come il già citato Russiagate delle elezioni americane del 2016. Altri Paesi stanno prendendo ad esempio la potenza sovietica: durante le elezioni presidenziali iraniane del 2017, ad esempio, sono stati rilevati diversi falsi account iraniani utilizzati per propagandare sui social media nazionali un'agenda politica e sociale ben precisa, che ha contribuito alla riconferma del Presidente Rouhani.

L'Europa nel mirino

Reti elettriche, gas, Internet, trasporti, comunicazioni delle forze dell'ordine, ospedali: tutto ciò che può definirsi come infrastruttura critica resta un potenziale bersaglio di attacchi informatici. Nel 2019 il rischio per questo genere di target aumenterà ancora (è il terzo macro trend individuato) perché molte organizzazioni non dispongono di una strategia di sicurezza unificata per la struttura informatica e le tecnologie operative. A motivare gli hacker saranno a volte interessi geopolitici o economici, ma anche ideologie e mere dimostrazioni di forza. A causa della sua diversità interna e del numero di impianti dispiegati sul continente, l'Europa sarà probabilmente uno dei prossimi obiettivi principali di questi attacchi. E l'Italia non è un'isola felice: Marco Riboli, vice presidente per l'Europa meridionale di FireEye, fa una breve e puntuale analisi sul nostro paese: "Benchè l'Italia sia tra le eccellenze mondiali nella ricerca sulle misure di protezione cyber" spiega "sarà uno degli obiettivi principali nel corso di quest'anno, soprattutto in virtù del suo tessuto produttivo composto per la maggior parte di piccole e medie imprese che, rispetto alle grandi, scontano nel complesso una maggiore mancanza di competenze interne e misure protettive nei confronti del cyber risk".

VOCI
DAL MERCATO

Il sistema 5G: sicurezza e privacy

Maurizio Decina
Presidente, Infratel

Il sistema 5G offre prestazioni di capacità trasmissiva e latenza molto maggiori dei sistemi precedenti e fornisce una piattaforma di supporto per una grande varietà di servizi eterogenei. I contesti applicativi del 5G sono altamente diversificati e certamente sfidanti per quanto riguarda gli aspetti di sicurezza e privatezza dei servizi offerti e dei dati generati. Si pensi ad applicazioni, quali: il controllo in tempo reale dei robot industriali, i veicoli autonomi, i droni, le operazioni chirurgiche a distanza, la realtà virtuale, le diagnosi a distanza, ecc. Lo sviluppo e la personalizzazione dei servizi sono basati sulla virtualizzazione delle infrastrutture di rete, integrando le funzioni di rete software (computing, storage e switching) nel nucleo della rete (Cloud) e collocandole nei bordi della rete (Edge) per fare fronte alle

applicazioni che richiedono bassa latenza (i servizi cosiddetti time critical). Per fare fronte a questo nuovo scenario di integrazione dei servizi dei mercati verticali è necessario un approccio alla sicurezza completamente diverso da quello adottato per i sistemi cellulari delle precedenti generazioni.

Non si può più adottare l'approccio del tipo "one size fits all" usato nei sistemi 2G/3G/4G, ma bisogna affrontare la diversità dei servizi applicativi con un approccio di "flexible security", e cioè bisogna sviluppare soluzioni di sicurezza diversificate per fare fronte al particolare scenario applicativo considerato. Nel sistema 5G viene quindi introdotto il protocollo detto 5G-EAP-AKA, Extended Authentication Protocol-Authentication and Key Agreement, che funziona da contenitore per procedure di sicurezza diversificate. Per esempio: i dispositivi terminali sono dotati di SIM (Subscriber Identification Module) o sono SIM-less? Vanno messe in conto limitazioni di consumo di energia o di capacità computazionale? Inoltre, i servizi che richiedono bassa latenza necessitano di soluzioni di sicurezza capaci di garantire il rispetto di tali limiti.

Per i sistemi 5G continua poi a valere l'approccio già stabilito per il 4G della "built-in-security", e cioè la sicurezza è direttamente integrata nelle specifiche di sistema "prima" dello sviluppo dei sistemi in campo. Ciò non è avvenuto per i sistemi 2G/3G, mentre si è cercato di applicare la built-in security per i sistemi 4G, anche se ci sono molte aree specifiche in cui la sicurezza dei sistemi 4G può essere significativamente migliorata. Le aree in questione hanno a che fare con la protezione della privacy (ad esempio: localizzazione, dati sensibili, ecc.), con la security assurance, e principalmente riguardano la robustezza degli impianti di rete contro gli attacchi cibernetici, anche in vista dell'evoluzione del malware nei dispositivi mobili. Nel sistema 5G, quando sono in gioco i servizi legati alla Internet of Things, gli attacchi cibernetici possono sfruttare il malware diffuso nei cluster di sensori: gli attaccanti possono prendere il controllo di milioni di dispositivi dando luogo a scenari di attacco di scala e impatto senza precedenti.

Il terzo approccio alla sicurezza del Sistema 5G si chiama "automation". Le prestazioni di sicurezza dipendono anche dalla capacità di gestione della sicurezza da parte degli operatori, e cioè dai tool introdotti per semplificare il security management della rete e per permettere un rapido aggiornamento non solo delle operazioni di gestione, ma anche delle nuove soluzioni di sicurezza introdotte per nuovi servizi.

Gli aspetti di sicurezza del sistema 5G coinvolgono tutte le sezioni della rete e i terminali: si va dall'accesso radio, agli elementi di trasporto della rete (traffico dati e messaggi di segnalazione e controllo), alla protezione dei terminali (smartphone e sensori) e identificazione degli utenti, alla sicurezza delle piattaforme di servizio e delle applicazioni, per arrivare a un sistema di gestione della sicurezza che permetta di verificare le feature di sicurezza funzionanti e la loro configurazione. Un ruolo molto importante assume la sicurezza della virtualizzazione delle reti nel Cloud e nell'Edge Computing, in particolare per affrontare i moderni attacchi cibernetici (ad esempio, i transient execution attacks alle virtual machines).

Infine, il grande numero di stakeholders coinvolti nei servizi verticali richiede grande attenzione per la privacy degli utenti e la rivelazione di dati sensibili. Sono necessarie politiche e regole per governare le attività di profiling degli utenti e lo sfruttamento delle informazioni sul loro comportamento al fine di personalizzare i servizi.

VOCI DAL MERCATO

Edge to Cloud: la visione di HPE

Intervista di **Roberto Masiero** a **Claudio Bassoli**
Vice Presidente HPE

Lo scorso 27 marzo, nell'ambito del Digital Infrastructure Summit abbiamo incontrato Claudio Bassoli, Vice President HPE, che ci ha parlato dei progetti sviluppati da HPE per aiutare le aziende ad estrarre valore dai dati: dalla terza generazione di soluzioni di Intelligent Edge all'utilizzo dell'Artificial Intelligence per permettere di trarre valore dai dati.

Qual è la vostra visione relativamente alle nuove architetture tecnologiche e in particolare la vostra visione di "Edge to Cloud"?

La nostra visione "Edge to Cloud" nasce dalla constatazione per cui ormai da anni viviamo in una società dove i dati, in modo ubiquo, vengono generati ovunque, il che ne rende necessaria la raccolta e l'analisi per poi poterli trasformare in valore per le persone o per le aziende. Per queste ragioni abbiamo introdotto un nuovo livello di tecnologia che abbiamo definito "Intelligent Edge" che permette, da un lato, di fornire le infrastrutture tecnologiche prevalentemente di rete che gestiscono questa mole enorme di dati, dall'altro di poter elaborare questi dati, valorizzandoli laddove vengono generati per poter fornire un servizio.

Va considerato, inoltre, che ad oggi diverse statistiche riportano che il 94% dei dati generati rimane inutilizzato, un vero e proprio spreco di quello che oggi viene considerato il nostro "petrolio", problema che potrebbe essere risolto, appunto, con l'Intelligent Edge.

In che modo quest' innovazione tecnologica su cui state lavorando consente alle imprese di utilizzare i Big Data e di sviluppare nuove applicazioni basate sull'Artificial Intelligence?

Negli ultimi anni noi abbiamo lavorato lanciando nuove architetture sia nell'ambito dell'Intelligent Edge (dove per nuove architetture si intendono nuove modalità di rete, come ad esempio il WiFi 6-802 111 ax-disponibile già da diversi anni e che ha la caratteristica di poter gestire in modo sicuro ingenti moli di dati, o il multicasting) sia nel contesto degli Edge Line, architetture di computer che permettono con oggetti di piccole dimensioni di poter elaborare, archiviare e trasmettere centralmente.

Nell'ambito dei Big Data e dell'Artificial Intelligence le nostre attività sono state prevalentemente due:

- Abbiamo introdotto sul mercato nuove architetture che sono state ingegnerizzate per poter acquisire, immagazzinare ed elaborare grandi moli di dati, usando sia applicativi tradizionali che nuovi algoritmi matematici. Questo è estremamente

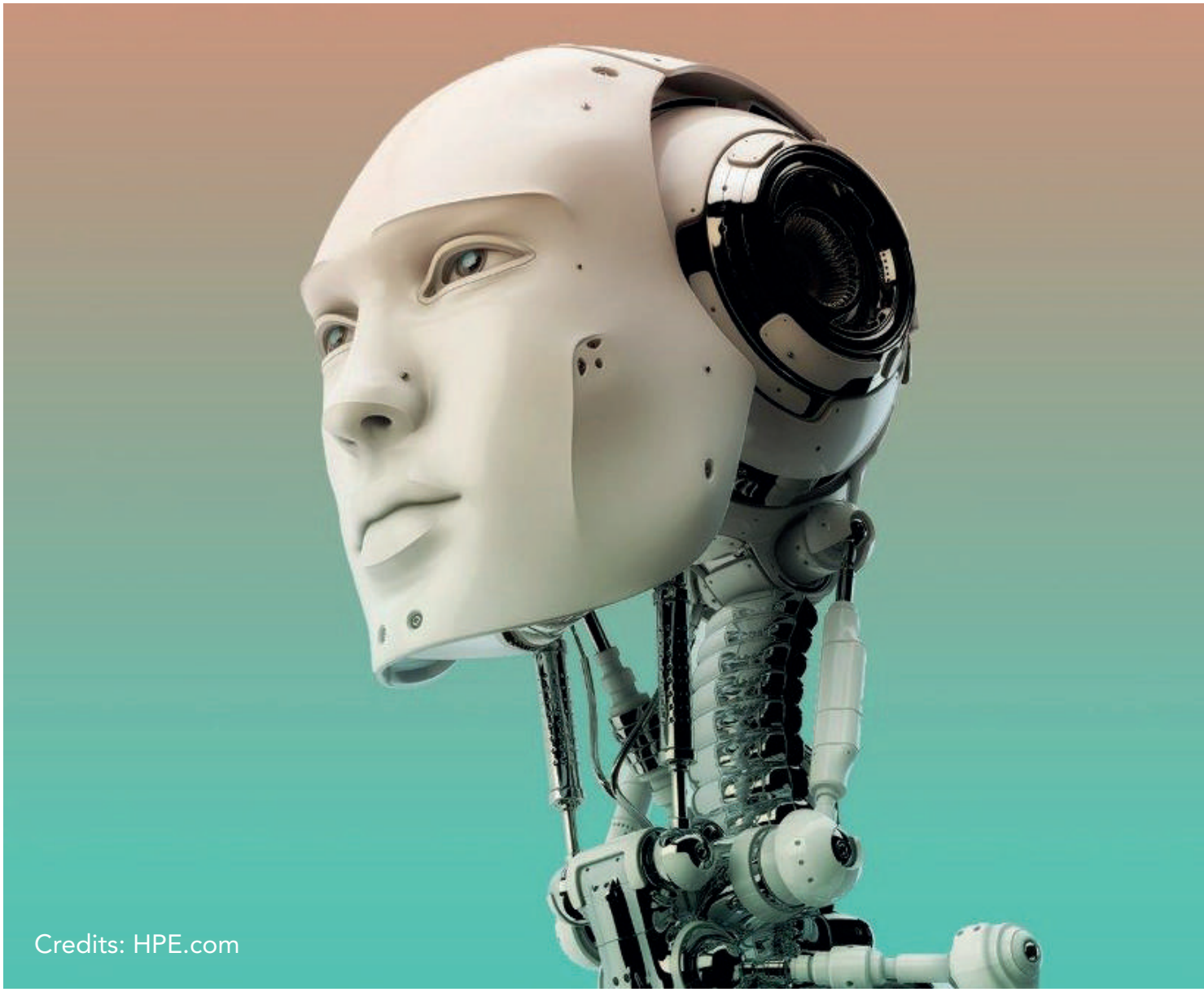
rilevante perché per estrarre il valore dai dati bisogna riuscire, non solo ad estrarre il dato con l'edge ma anche ad avere dei sistemi centrali in grado di analizzare i dati creando valore di business: in questo campo siamo stati i primi ad aver lanciato commercialmente delle architetture che arrivano fino a 48 terabyte di memoria centrale fino nei laboratori dove abbiamo architetture che permettono di avere 120 terabyte di memorie e poter lavorare su questa stessa memoria con processori diversi.

- Abbiamo aiutato i nostri clienti nello sviluppo di nuovi algoritmi. Innovando le infrastrutture abbiamo fatto sì che queste fossero in grado di poter utilizzare algoritmi matematici che in precedenza era impossibile risolvere.

In termini di use case?

Un paio di esempi. Il primo relativo alla guida autonoma: un'ora di guida autonoma produce 9 terabyte di dati, ciò vuol dire che nel ciclo di vita di un anno della macchina vengono generati 180 petabyte di dati. Considerata questa mole non si possono usare le architetture del passato, perché diventerebbe una soluzione eccessivamente costosa; d'altra parte, però, c'è comunque la necessità di elaborare dati sulla macchina e portarli al centro in modo efficiente ed efficace, disponendo di una quantità di memoria e di processori che consentono di fare questo tipo di elaborazioni.

Un altro caso è nell'ambito di quello che noi chiamiamo Intelligent Venue, e qui vorrei riportare come esempio il Levi's Stadium, in California, dove queste tecnologie applicate hanno portato, nella prima stagione in cui sono state utilizzate, a più di 1 milione di dollari di revenues per quanto riguarda il food, beverage, merchandise e parcheggi e a 750 mila dollari in più di introiti pubblicitari nell'app che è stata realizzata. L'app ha, inoltre, avuto un utilizzo del 30% da parte di chi frequentava lo stadio (rispetto a una media del mercato del 5%); il suo successo è stato determinato dal fatto che essa forniva una serie di servizi che senza queste tecnologie non potevano essere erogati. È questo, dunque, il modo in cui i dati si trasformano in petrolio, in ricavi e in profitti.



Credits: HPE.com

NOTE

IL CAFFÈ DIGITALE

ISCRIVITI ALLA NEWSLETTER MENSILE!

RICEVI GLI ARTICOLI
DEGLI ANALISTI DI THE
INNOVATION GROUP
E RESTA AGGIORNATO
SUI TEMI DEL MERCATO
DIGITALE IN ITALIA!

QUESTO MESE ABBIAMO
FATTO COLAZIONE CON...

INTESA SANPAOLO

COMPILA IL FORM DI REGISTRAZIONE SU

www.theinnovationgroup.it