IL CAFFÈ DIGITALE
THE INNOVATION GROUP NEWSLETTER

L'EDITORIALE DI

Roberto Masiero
President, The Innovation Group

CONSIDERAZIONI SUL CASO GOOGLE E LA MULTA RECORD UE

Economie di piattaforma: to be (neutral) or not to be?

E' il caso del giorno: la Commissione UE ha inflitto a Google una multa di 2,42 Miliardi € per abuso di posizione dominante, con l'accusa di aver favorito arbitrariamente il suo "shopping service" rispetto ai concorrenti.

È opportuno citare letteralmente la Commissaria alla Concorrenza Margareth Westagher:

"Google has given its own comparison shopping service an illegal advantage by abusing its dominance in general Internet search. It has promoted its own service, and demoted rival services. It has harmed competition and consumers. That's illegal under EU antitrust rules."…

"This decision requires Google to change the way it operates, and to face the consequences of its actions,"…

"Google's strategy for its comparison shopping service wasn't just about attracting customers by making its product better than those of its rivals. Instead, Google abused its market dominance as a search engine by promoting its own comparison shopping service in its search results, and demoting those of competitors."…

"Google's practices have deprived millions of European consumers of the full benefits of competition, genuine choice and innovation."[1]

Le reazioni ufficiali di Google sono state improntate finora alla massima cautela. Il SVP Ken Walker ha espresso il "rispettoso disaccordo" dell'Azienda e annunciato di considerare un possibile appello. Più decise le reazioni delle Associazioni e dei Think Tank Usa ad esse legati.

Rob Atkinson, Presidente ITIF (IT & Innovation Foundation), ha affermato che l'UE ha di fatto deciso che alcune aziende sono diventate troppo grandi per poter innovare; questa decisione ha creato un clima di incertezza, che renderà le grandi corporation estremamente caute nell'introdurre cambiamenti alla user experience e ai servizi che avrebbero potuto portare nuovi benefici ai consumatori; tale decisione dimostra quindi di voler privilegiare gli interessi dei competitor rispetto a quelli dei consumatori.[2]

Il Direttore della Computer & Communication Industry Association per l'Europa Jakob Kucharczyk ha osservato a sua volta che il settore dell'e-commerce in Europa sta prosperando e che il successo di aziende come Zalando, Asos o Trivago mostra che i consumatori hanno sempre più opportunità di scelta. Anche gli investimenti in aziende e-commerce sono in forte aumento e tutto ciò non depone a favore della tesi di un mercato monopolizzato da un player dominante.[3]

In realtà, la vicenda sembra aprire il confronto su alcuni temi fondamentali:

1. ***Se – e, in caso, come – regolare la competizione tra motori di ricerca orizzontali e verticali***

segue alla pagina successiva >>

LUGLIO 2017

QUESTO MESE ABBIAMO FATTO COLAZIONE CON...

Marco SALVADORI
Responsabile Digital & Innovation, Fastweb

FASTWEB un passo avanti

SOMMARIO

2. ***Il tema della neutralità o meno delle piattaforme***
3. ***L'Europa si trova di fronte a un serio conflitto fra la tutela dei suoi valori fondanti e lo sviluppo dell'innovazione digitale?***

Esaminiamo brevemente questi temi, su cui ci parrebbe opportuno aprire un dibattito più ampio.

1) Se – e, in caso, come – regolare la competizione tra motori di ricerca orizzontali e verticali

"In principio era l'IBM", che negli anni '60 sviluppò un tale dominio del mercato dei computer da indurre il Dipartimento di Giustizia Americano ad aprire una causa per violazione dello Sherman Antitrust Act.

La causa durò 13 anni, ma già nel 1969 IBM risolse gordianamente il dilemma attraverso il cosiddetto unbundling, cioè la decisione di commercializzare separatamente hardware, software e servizi, che prima erano forniti "gratuitamente" all'interno dell'hardware. A questa storica decisione si può fare risalire la nascita di una vera e propria industria del software applicativo, anche se molti anni dovettero passare prima che, con la nascita del PC, il cui sistema operativo fu sviluppato da Microsoft, si aprisse un nuovo enorme mercato software non più controllato da IBM.

Poi venne Microsoft, che a sua volta fece leva sulla sua posizione dominante nel mondo dei sistemi operativi per includervi browser e altri applicativi, al punto da incorrere nei rigori del Commissario Monti. In particolare, Microsoft fu accusata di distribuire insieme al sistema operativo il programma Windows Media Player, un riproduttore per file multimediali, a scapito degli altri produttori di programmi simili, che rimanevano in ombra. Fu assunta quindi una decisione preliminare, ordinando a Microsoft di avviare la produzione di una versione di Windows senza Windows Media Player; alla società fu anche richiesto di fornire più informazioni sui propri software per la gestione dei server, permettendo agli altri produttori di realizzare programmi compatibili e in grado di dialogare con quelli di Microsoft.

Monti comminò per questo a Microsoft una storica multa di 497 milioni di euro, che spiegò in questo modo: "La ragione principale per cui non accettammo un compromesso, pur correndo il rischio che Microsoft ricorresse in giustizia, è che ritenevamo importante stabilire una certezza giuridica su cosa vuole dire abuso di posizione dominante nelle tecnologie dell'informazione e della comunicazione. […] in questi settori la velocità dei fenomeni è tale che c' è una tendenza a vedere imprese in grado, grazie alle loro tecnologie, di trasferire il loro dominio su mercati adiacenti. Per questo è stato importante dare agli operatori un quadro giuridico più chiaro: per casi analoghi, da ora in poi non serviranno tutti gli anni che sono serviti a noi per giungere a una decisione."[4]

Come spesso accade, la storia si ripete: oggi Google è accusata di abuso di posizione dominante perché l'UE ritiene che essa stia approfittando della sua posizione di forza nel settore dei motori di ricerca per trasferire il suo dominio al mercato adiacente dello shopping service.

Ora Google gode certamente di una posizione dominante nel settore dei motori di ricerca orizzontali. Ma è legittimo che essa approfitti di questa posizione per competere da una posizione di vantaggio con i motori verticali (cioè quelli che forniscono informazioni e risorse su uno specifico settore industriale, con un focus molto specifico: i cosiddetti "vortals")?

Se risultasse vero che dal 2010 Google avrebbe modificato l'algoritmo di ricerca e a molti siti di ricerca verticali fosse stato dato un ranking bassissimo perché i contenuti venivano considerati "non originali", i link posizionati in basso nei risultati o addirittura esclusi perché considerati spam, la decisione della Commissaria Westagher non risulterebbe infondata.

2) Il tema della neutralità o meno delle piattaforme

Si tratta di un tema correlato al precedente, ma di natura così vasta che possiamo qui soltanto enunciarlo.

In breve: nella nuova "economia delle piattaforme" – tra l'altro, vere proprie catene di montaggio dei nuovi ecosistemi – va tutelata come un valore la neutralità di queste, considerate strutture neutrali abilitanti, oppure è nella loro natura che piattaforme e contenuti specifici si compenetrino sempre di più? In altre parole, le piattaforme dovrebbero essere definite e tutelate come luoghi aperti in cui si incontrano entità differenti che generano valore attraverso le loro transazioni (come Facebook, come Twitter?), oppure questa caratteristica di "neutralità" è legata semplicemente ad una fase iniziale dello sviluppo delle piattaforme digitali? Ciò considerando anche che esse sono destinate a trasformarsi rapidamente in strumenti per cui il "trasferimento di dominio sui mercati adiacenti" diventa l'obiettivo principale di strategie di penetrazione, di cui quindi le piattaforme digitali rappresentano l'elemento chiave.

E' dalla nascita dell'Informatica che la pressione del mercato tende ad aprire sistemi chiusi, solo per vedere di nuovo i sistemi aperti disseminarsi di trappole "proprietary". L'impressione è che siamo di fronte all'ennesimo capitolo di una saga che tende regolarmente a riprodursi.

3) L'Europa si trova di fronte a un serio conflitto fra la tutela dei suoi valori fondanti e lo sviluppo dell'innovazione digitale?

Questa tesi è stata formulata da Luca De Biase nel suo articolo "Il difficile confine del mercato digitale".[5] Secondo De Biase, "La concorrenza… è un carattere fondativo della costruzione europea… e va in rotta di collisione con piattaforme che quando hanno successo tendono organicamente a trasformarsi in monopoli. … Ci sarebbe da chiedersi se questo attivismo normativo europeo nei confronti delle piattaforme digitali americane non rischi di essere un freno per la crescita delle piattaforme digitali europee."

De Biase solleva due questioni importanti. Sulla prima si potrebbe osservare che non si contesta la "posizione dominante" di per sé, ma il suo abuso nel senso definito da Mario Monti: se è vero che Google ha una posizione dominante sul mercato dei motori di ricerca orizzontali, così come Amazon nel mondo dell'e-commerce, ciò non legittima di per sé il trasferimento del dominio ai mercati adiacenti

Quanto "all'attivismo normativo europeo nei confronti delle piattaforme digitali americane" come potenziale ostacolo allo sviluppo delle piattaforme europee, mi pare che in realtà stia accadendo esattamente il contrario: è l'invasività di Google nel settore dei motori verticali a rappresentare un ostacolo allo sviluppo dei vortals, mentre l'intervento della Commissaria Westagher va nel senso della difesa della contendibilità del mercato: quindi, nessun conflitto. E in questo senso va letto il Comunicato del BEUC – l'organizzazione Europea dei consumatori – che dice che "I consumatori si aspettano che Google mostri risultati neutrali e di qualità invece che ricerche che favoriscono il proprio business."[6] E alle argomentazioni secondo cui la presa di posizione della UE contro Google rappresenterebbe un blocco all'innovazione, l'organizzazione europea dei consumatori replica che è invece la politica di Google a frenare l'innovazione, impedendo ai consumatori di avere un quadro completo dei possibili competitor, con l'effetto di consentire minori scelte e di dover sostenere prezzi più alti.

Note:

1. "Google fined $2.7BN for EU antitrust violations over shopping searches", http://tcrn.ch/2tRdhim
2. Record EU Fine Against Google Risks Creating New "Too Big To Innovate" Standard, Says ITIF – http://bit.ly/2s29v4o
3. Google fined record $2.7 billion in European antitrust case, http://bayareane.ws/2tp0hUw
4. La volta che Monti multò Microsoft – Il Post, http://www.ilpost.it/2011/11/10/la-volta-che-monti-multo-microsoft/
5. Luca De Biase, articolo " Il difficile confine del mercato digitale", Il Sole 24 Ore, 27/6/2017
6. BEUC, "Google record fine paves way for better search results for consumers", http://bit.ly/2tY4zPG

QUESTO MESE ABBIAMO FATTO COLAZIONE CON..

OBIETTIVI E LE PRIORITÀ DELLA DIGITAL & INNOVATION STRATEGY DI FASTWEB

Intervista a **Marco Salvadori**, RESPONSABILE DIGITAL & INNOVATION, FASTWEB

Quali sono gli obiettivi e le priorità della Digital & Innovation Strategy di Fastweb?

Quando sono arrivato in Fastweb a settembre 2014, l'obiettivo era quello di unire e dare forma a due grandi aree, quella Digital e quella Innovation. Per quel che riguarda l'area Digital, questa può essere intesa in diversi modi: in particolare, mi sono occupato dell'iniziativa Digital IQ, ossia di uno strumento di assessment e valutazione delle competenze e delle attitudini digitali, da usare internamente ed esternamente all'azienda. Con l'Università di Maastricht e di Milano-Bicocca, è stato costruito uno schema di valutazione basato sugli individui, sulla loro conoscenza e soprattutto sulle loro attitudini verso il digitale: non solo quanto una persona sa usare uno strumento digitale, ma soprattutto quanto dimostra di avere le attitudini necessarie in un contesto digitale. Questo metodo, una volta messo a punto, è stato applicato internamente e, successivamente, proposto ad altre aziende: questo strumento infatti ben si accompagna con i processi di riqualificazione delle risorse umane in corso in alcune aziende, che riconoscono come la trasformazione digitale non sia fatta solo di tecnologia, ma soprattutto di persone. Per quanto riguarda l'area Innovation, questa non riguarda solo la componente d'innovazione dell'offerta, del go-to-market, che d'altra parte è sempre stata fatta, ma soprattutto l'innovazione di prodotto. Abbiamo infatti cominciato a ragionare sulla possibilità di utilizzare la nostra infrastruttura per veicolare soluzioni software-based, che possono anche essere oggetto di offerte particolari su segmenti specifici attraverso il cloud applicativo.

Quali sono le iniziative che state sviluppando in quest'ambito?

Abbiamo sempre lavorato sulla connettività cercando di offrire la migliore connessione possibile, in termini non solo di velocità, ma anche di stabilità. Ma non solo. Il mercato oggi è saturo e per far fronte a questa situazione abbiamo sviluppato servizi ICT a valore aggiunto puntando su Cloud e servizi di Sicurezza gestita per il mondo Enterprise, che è il nostro mercato di riferimento e di cui siamo fornitori riconosciuti. Disponiamo infatti di un'infrastruttura Cloud, basata su Datacenter di ultima generazione tra cui quello Tier IV di Milano, certificato dall'UpTime Institute di New York che si sta arricchendo sempre di più di componenti software. In particolare, abbiamo appena concluso il trial di un marketplace SaaS che verrà rilasciato commercialmente, con un primo catalogo di applicazioni, in autunno.

In che cosa è innovativo questo marketplace?

Ciò che è innovativo è il posizionamento, dal momento che, contrariamente a quanto fatto da altri competitor che inizialmente si sono rivolti alla fascia delle grandi aziende, Fastweb da subito ha scelto di rivolgersi alle imprese medio- piccole. Le applicazioni sono sviluppate da terze parti, soprattutto da software houses che sviluppano software professionali per le aziende italiane, ossia che sono aderenti alle normative italiane della contabilità, della gestione delle risorse umane, della logistica, ect. Il nostro marketplace offrirà la fruizione del software prevalentemente sulla nostra infrastruttura cloud, mentre le modalità di commerciali e di supporto dipenderanno dallo specifico ISV.

Il business model è quindi quello di un marketplace software?

Sì. In particolare avremo due tipi di offerta: le applicazioni degli ISV, con un catalogo iniziale di qualche decina di titoli, che sono appoggiati su nostro cloud ed evolveranno nel tempo; una selezione di software open source e stiamo stimolando i nostri business partner a creare template di personalizzazione e quindi gestire un business proprio che rafforza il nostro e loro posizionamento sui clienti finali.

Qual è il piano evolutivo di questo progetto nel medio- lungo periodo?

Nel breve periodo l'obiettivo è avviare il marketplace B2B, dopo la sperimentazione pre-commerciale nei mesi scorsi. Poi puntiamo all'arricchimento del catalogo, anche con prodotti verticali per alcuni settori.

Secondo lei, quali sono le tecnologie che nei prossimi anni avranno un impatto significativo nella trasformazione del business di Fastweb?

A mio avviso, particolarmente significative sono tutte tecnologie software- based; in particolare, trovo disruptive soprattutto le strutture di archivi non SQL, non relazionali, tutto quello che è legato ai big data, così come alle logiche del cognitive learning e del machine learning. Come queste tecnologie si possano applicare al business di Fastweb? Ad oggi non abbiamo degli use case già definiti, stiamo lavorando ad alcuni progetti, ad esempio nell'ambito dell'inbound customer service, ossia in processi altamente ripetitivi ormai abbastanza ottimizzati in termini di rapporto costo/ relazione. A questo proposito, abbiamo appena concluso una Request For Information su undici use case legati ai big data, incluso quello relativo allo smart inbound, o legati alla churn prevention, alla predictive maintanance, al lock- in prediction, etc. Sul tema big data stiamo lavorando anche con Swisscom, il nostro azionista: si è infatti appena conclusa una Call for Innovation che è stata organizzata anche in collaborazione con Proximus. Eravamo alla ricerca di proposte che avessero alla base un progetto praticabile di sviluppo di servizi per gli end user, aziende o individui, basati sui dati che noi Telco generiamo. A giugno si tiene il momento finale di premiazione: i vincitori vedranno la loro idea inserita nelle nostre soluzioni o offriremo loro degli accordi di reselling. In futuro abbiamo intenzione, come Fastweb, di ricorrere ancora a questo strumento – la call for innovation – per raccogliere idee e progetti per il nostro nuovo modem: questo modem consentirà infatti di eseguire applicazioni, al proprio interno, in una logica di App Store: non sarà solo un'innovazione di stile, ma anche di contenuti.

BANCHE ITALIANE: DOPO LA "RESA DEI CONTI" SI DEVE GUARDARE AL FUTURO

Di **Ezio Viola**, Managing Director, The Innovation Group

Possiamo dire che le banche si siano lasciate alle spalle la crisi finanziaria a dieci anni dal suo inizio? **Il 2017 sarà l'anno della "resa dei conti" per le banche italiane?** Queste sono alcune delle domande che oggi vengono poste in un contesto in cui le crisi bancarie ancora aperte richiedono di essere risolte il prima possibile e, in alcuni casi, sembrano in via di risoluzione (sia "svendendole" a 1 euro sia con aiuti di Stato!). D'altra parte, per molte banche resta ancora l'urgenza di smaltire la zavorra dei crediti deteriorati, mentre altre, benché sembrino essere tornate in forma rispetto a dieci anni fa, non riescono ad avere ricavi equamente distribuiti.

In particolare, le quotazioni delle banche italiane hanno risentito degli effetti della crisi e dell'aumento del rischio percepito da parte del mercato: per le banche più fragili la flessione è stata più pronunciata e le loro debolezze si sono riflesse sulle quotazioni del comparto. A questo riguardo, un dato interessante riguarda il ROE (Return On Equity) delle banche italiane: a fine 2016 in Italia il ROE medio era di poco più del 2,5%, contro il 5,8% dell'Europa; i best performer delle banche quotate hanno avuto un ROE del 6,7%, mentre le peggiori del -27%, con una media delle banche restanti pari al -16%. Per le banche italiane l'abbattimento del ROE è stato principalmente causato dal costo del nuovo capitale richiesto per gestire i rischi legati ai Non Performing Loan (NPL); inoltre, tra i grandi cambiamenti portati dalla crisi c'è sicuramente una più severa regolamentazione che ha accresciuto i costi, già significativi, di compliance che le banche devono supportare, oltre ad un cambiamento nel livello dei requisiti di capitale per gestire i rischi e la liquidità come imposto anche da Basilea 3.

Proprio sul tema dei NPL dall'ultima relazione del Governatore della Banca d'Italia emerge come, a fine 2016, i crediti deteriorati netti delle banche italiane siano stati pari a 173 miliardi di Euro, di cui le vere sofferenze ammontavano a 81 miliardi. I rischi effettivi che incombono sul settore bancario paiono quindi più limitati, dal momento che il flusso dei nuovi crediti deteriorati è in fase di rallentamento grazie al miglioramento della congiuntura economica. È questa una condizione necessaria e sufficiente per stare tranquilli? Forse ci dobbiamo chiedere se questo può far **tornare i conti** ad azionisti, clienti e dipendenti anche **nel medio-lungo periodo**. Di conseguenza, le domande da porsi sono le seguenti: è sufficiente il numero attuale di banche finanziariamente ed economicamente sane? E queste sono ancora un investimento attraente per i mercati finanziari internazionali? Sapranno inoltre le banche italiane attrarre e fidelizzare i clienti facendo leva sulle potenzialità della rivoluzione digitale e questa sarà compatibile con la iper-regolamentazione e l'unione bancaria prossima ventura?

Se è vero che nell'industria bancaria nulla sarà più come prima occorre non solo riparare i guasti urgenti per far tornare i conti nel breve termine, ma occorre anche che le **banche guardino e lavorino per il futuro**.

L'evoluzione della struttura dei mercati, ma ancora di più la **rivoluzione tecnologica**, impone infatti nuove sfide. La razionalizzazione della rete di sportelli, la revisione dei processi di governance e di gestione dei rischi, la fidelizzazione con modelli innovativi di omnicanalità, il disegno di nuovi servizi per generare nuove fonti di ricavi, sono solo alcune delle opportunità di trasformazione che le banche stanno perseguendo. Come ha ribadito il Governatore, l'industria bancaria e la finanza devono ammodernarsi profondamente per vincere la sfida della concorrenza tecnologica: **pur essendoci stati progressi, questi sono infatti da considerarsi ancora timidi e parziali**.

Le banche italiane sono quindi alla ricerca delle virtù e dei valori della "banca perduta" o anche di un nuovo modo di fare banca? Alla fine in Italia resteranno meno banche, ma più digitalizzate? Ma con quali modelli operativi e di business? Come possono le banche gestire un processo di concentrazione e di trasformazione a passo forzato, che lascia spazi aperti a nuovi competitor, provenienti da altri settori non bancari, e alle nuove realtà del Fintech?

L'espansione di forme e modelli di intermediazione che si basano fortemente sulla tecnologia, le **Fintech**, accresce infatti il panorama competitivo e consente di guardare e ampliare i servizi e le modalità di gestire la relazione con il cliente; Fintech non significa solo disintermediazione e concorrenza con le banche, ma anche modi

nuovi di fare innovazione in banca. In questo senso, sono già presenti e disponibili forti acceleratori dei processi di trasformazione, come le tecnologie per l'analisi avanzata dei dati e dei big data o l'intelligenza artificiale, che innescano processi di trasformazione profondi, cambiando la geografia dei mercati e dei modelli di business delle aziende e dei clienti.

A partire dall'introduzione della Mifid e, nei prossimi mesi, della PSD2 i confini tra banche e altri player tenderanno ulteriormente a sfumare. D'altra parte, **con l'avvento delle Fintech l'apparato concettuale e normativo, oggi utilizzato per la regolamentazione dei mercati, rischia di diventare presto obsoleto, come ha sottolineato recentemente il Presidente della Consob, Giuseppe Vegas**. Nuovi protagonisti stanno infatti entrando nell'industria dei servizi bancari, tra cui alcuni grandi operatori del web, come Facebook, Amazon, Google e Apple, che muovono da posizioni dominanti in altri settori ma che "conoscono" in profondità il cliente. Altre realtà del mondo Fintech si dimostrano invece in grado di intercettare e gestire in modo innovativo la domanda di servizi finanziari ricorrendo a piattaforme e soluzioni tecnologiche di nicchia: la tecnologia ha già cambiato le modalità di erogazione e interazione dei servizi finanziari non solo con la diffusione di nuovi canali digitali, ma anche con nuove forme più sofisticate di servizio come, ad esempio, i **robo- advisor**, in una logica di consulenza personalizzata, ossia piattaforme digitali basate su algoritmi che rendono facilmente scalabile l'assistenza agli investimenti ad un numero esteso di clienti; oppure il **peer-to-peer lending** tra chi richiede e chi presta denaro online senza intermediari, aprendo nuovi accessi al capitale di credito e di rischio anche per le PMI, fino alle potenzialità dirompenti della tecnologia **blockchain** sulla struttura dei mercati finanziari. In questa fase, le promesse delle nuove tecnologie digitali (in particolare dell'Intelligenza Artificiale) e delle Fintech (blockchain, digital currency, open banking, ecc.) sono quindi realistiche? Per esse e anche per le banche si è solo all'inizio perché è appena cominciata una storia diversa da come è stata finora.

In questo senso, **l'approccio passato tipico delle banche del "mee too" non è più sufficiente in una logica di trasformazione digitale**. Questo porta a porsi ancora altre domande:

- Le opportunità e minacce che arrivano dal digitale e dalle Fintech sono interamente compresi dalle banche italiane e dai regolatori?
- In che modo le banche stanno recuperando efficienza e produttività? E con che ritorni per tutti gli stakeholder?
- Come le banche possono ri-orientare gli investimenti tecnologici sulle aree più trasformative e a valore per il business?
- Come possono i nuovi acceleratori tecnologici della trasformazione digitale cambiare processi operativi e decisionali e valorizzare il fattore umano?

Anche l'IT, che costituisce il motore operativo di questo processo, deve evolvere per trasformare digitalmente le banche e questa è una condizione necessaria: Cloud, Big Data, Agile e Devops, Dual IT, API e Microservizi, Open Innovation e Open Organization, sono le parole d'ordine per ridisegnare i modelli di funzionamento e ripensare l'organizzazione dell'IT in banca:

- come concretamente le banche italiane li stanno introducendo e utilizzando?
- Quali sono le nuove capacità e competenze necessarie per accelerare il processo di trasformazione delle attuali legacy tecnologiche e organizzative?

Questi sono solo alcuni dei temi del confronto che si aprirà il 21-22 Settembre in occasione del Banking Summit 2017, organizzato da The Innovation Group a Saint Vincent, che vedrà la presenza di autorevoli leader di banche italiane e internazionali, di istituzioni europee, di società del settore ICT e del mercato digitale.

SERVIZI BLOCKCHAIN PER LE IMPRESE: SUPERARE IL MODELLO BITCOIN

Di **Marcella Atzori**, University College of London, Blockchain Advisor Ifin Sistemi

Fino a oggi, il dibattito sulle potenzialità gestionali della tecnologia blockchain a livello internazionale ha assunto spesso una connotazione ideologica, tesa a privilegiare la decentralizzazione attraverso i network aperti. E' ancora opinione diffusa che soltanto le blockchain interamente distribuite – come Bitcoin – esprimano al meglio il senso originario di questa tecnologia, mentre i network chiusi (o "permissioned") avrebbero un minore impatto innovativo.

Si tratta di un'interpretazione che sebbene straordinariamente comune, è però semplicistica e decisamente poco funzionale rispetto alla logica e alle esigenze delle imprese: In realtà, un network blockchain dovrebbe essere valutato non per il tipo di governance in sé, ma per come questa sia adatta al raggiungimento di determinati obiettivi.

La distribuzione assoluta del potere computazionale tipica dei network aperti risponde molto bene a esigenze di natura libertaria e a funzioni relativamente semplici, quali ad esempio le transazioni finanziarie peer-to-peer. Tuttavia, per le imprese non costituisce affatto un valore assoluto.

Al contrario, il mondo dei servizi digitali è estremamente complesso e un'adeguata diffusione delle architetture decentralizzate deve rispecchiare questa complessità secondi principi di innovazione sostenibile, offrendo agli imprenditori sicurezza e fiducia sistemica, confidenzialità delle transazioni, protezione dei dati a norma di legge e un'equa considerazione degli interessi di tutti i player di mercato. In molto casi, i network aperti non riescono a offrire tutto ciò.

Originariamente concepiti per decentralizzare transazioni di natura finanziaria, non sono ottimizzati per altre funzionalità specifiche e possono risultare quindi poco performanti ad esempio nell'esecuzione di compiti complessi di natura amministrativa o conservativa dei dati. Generalmente questa tipologia di network rende difficile sia l'adeguamento normativo che la protezione della confidenzialità delle transazioni, fattori essenziali per un adeguato sviluppo di molte categorie di servizi. Si tratta inoltre di piattaforme a elevato rischio di volatilità, prive di adeguate garanzie relativamente alla continuità operativa e alla conservazione dei dati nel tempo.

Queste criticità finora hanno ostacolato notevolmente l'adozione di applicazioni blockchain nel mondo dei servizi digitali, a dimostrazione di come la rivoluzione blockchain e la decentralizzazione dei servizi non possa fondarsi soltanto sulla logica del peer-to-peer, ovvero su quella dimensione prevalentemente amatoriale tipica delle comunità online autogestite.

Gli obiettivi delle imprese sono complessi e hanno necessità di una governance blockchain altrettanto complessa per operare efficacemente. Servono quindi reti non multifunzionali, ma dedicate e ottimizzate rispetto a obiettivi di settore, che garantiscano performance tecniche elevate, conformità normativa, continuità del business e conservazione dei dati nel lungo periodo.

In questo ambito, i Trust Service Providers europei possono senz'altro distinguersi, offrendo agli imprenditori e al mondo dei servizi l'unicità del proprio valore aggiunto. Si tratta infatti di aziende regolamentate a livello nazionale ed europeo, la cui mission è l'adeguata gestione e conservazione dei dati per pubblica amministrazione e settore privato. **Agendo come nodi computazionali di un network blockchain in via esclusiva, possono costituire quella dorsale digitale stabile, efficiente e a norma di legge, su cui appoggiare una nuova classe di servizi informatici ad altissima affidabilità per pubblica amministrazione, imprese e settori sensibili – quali ad esempio il banking, la sanità e l'industria**.

La portata della disintermediazione sarà minore, rispetto ai network interamente distribuiti, perché verranno opportunamente reintrodotte forme di trust e di controllo, ma risulterà abbondantemente compensata da una maggiore facilità di implementazione dei nuovi servizi da parte delle imprese, da una gestione sicura di quei dati sensibili che non tollerano volatilità e speculazione, e soprattutto dalla possibilità di sperimentare nuove forme di business più affidabili, sofisticate e remunerative rispetto al passato.

La blockchain è una tecnologia eclettica che permette di creare architetture decentralizzate diverse, a seconda degli obiettivi specifici dei partecipanti coinvolti e degli interessi giuridicamente meritevoli di tutela a livello collettivo. Siamo appena all'inizio del percorso di implementazione di questa tecnologia a livello globale, ma è importante comprendere che fare innovazione non significa ostinarsi su principi di governance aperta o di peer-to-peer ad ogni costo: significa invece essere creativi e liberi da limitazioni ideologiche eccessive, valutando con attenzione in fase progettuale vantaggi, rischi e trade-off che caratterizzano le diverse architetture.

Per approfondimenti:
"Blockchain Governance and The Role of Trust Service Providers"

AWS SUMMIT MILANO 2017: NOVITÀ E TAKE AWAY SUL MERCATO DELL'AI

Di **Camilla Bellini**, Senior Analyst, The Innovation Group

Quest'anno l'intelligenza artificiale è senza dubbio al centro delle analisi e degli approfondimenti di analisti ed esperti del mercato digitale: anche The Innovation Group ha dedicato ampio spazio a questo argomento nei passati numeri de Il Caffè Digitale. D'altra parte, gli stessi player del mercato stanno rafforzando la propria offerta in questo ambito, come ben è emerso dall'AWS Summit 2017 che si è tenuto lo scorso 8 giugno a Milano. In particolare, nel corso dell'evento Marco Argenti, VP Technology di AWS, ha introdotto quella che è la strategia e l'offerta di Amazon nell'ambito dell'Intelligenza Artificiale, che va di pari passo con l'offerta cloud del player americano. In particolare, l'offerta di Amazon in questo ambito si struttura su quattro livelli, partendo dai servizi infrastrutturali ottimizzati per gli algoritmi AI e dallo sviluppo di un vero e proprio framework di deep learning, partecipando all'Apache Communtiy, fino ad arrivare all'offerta di piattaforme per lo sviluppo di algoritmi di machine learning e di servizi più specifici legati alla riconoscimento del linguaggio naturale e alle chatbot.

In questo senso, nella chart che segue, vengono riassunti i quattro livelli appena citati, che nel complesso definiscono l'offerta Amazon AI:

D'altra parte, i servizi in ambito AI su cui AWS pare puntare riguardano tre ambiti:

- il riconoscimento dei testi scritti e la loro traduzione vocale
- il riconoscimento di immagini
- il riconoscimento del linguaggio naturale

A partire da questi tre aspetti si dirama l'insieme dei servizi di Amazon AI. Per quanto riguarda infatti il primo punto, ossia la funzionalità text-to-speech, AWS si posiziona con Amazon Polly, che traduce appunto i testi scritti in vere e proprie conversazioni. Questo servizio può essere utilizzato, ad esempio, per creare applicazioni in grado di "conversare" con gli utenti. Nell'ambito di Amazon Polly, AWS ha inoltre annunciato due novità: la prima è Speech Marks, che consente di sincronizzare testi e voci con le immagini (si pensi ad esempio nel doppiaggio video), mentre l'altra è Whispering, una funzione che consente di caratterizzare la voce come se stesse sussurrando (in inglese "whispering", appunto).

Per quanto riguarda l'ambito del riconoscimento delle immagini, AWS con Amazon Rekognition dà la possibilità di inserire all'interno di un'applicazione funzionalità legate al riconoscimento di volti, oggetti e ambienti presenti in un'immagine, con lo scopo ad esempio di segnalare contenuti inappropriati o di classificare più rapidamente le immagini.

Infine, per quanto riguarda la capacità di comprendere il linguaggio naturale e di analizzare i testi sia in una logica di riconoscimento vocale sia di dettatura, AWS si posiziona con il servizio Amazon Lex, che consente di creare dei veri e propri bot: Amazon Lex offre ovvero il potenziale e la tecnologia di Amazon Alexa a tutti gli sviluppatori, che ne possono quindi sfruttare il potenziale creando ad esempio delle chatbot all'interno di siti ed applicazioni.

Nel complesso dunque si è visto come anche AWS si sta posizionando all'interno del panorama del'offerta in ambito AI, mettendo a disposizione dei developer una serie di strumenti che consentono di inserire logiche di intelligenza artificiale all'interno di qualsiasi applicazioni, in modo pervasivo: se dunque la promessa dell'AI è quella di rendere il business più intelligente, AWS si propone di offrire una serie di strumenti che consentano alle aziende di evolvere da una logica di Big Data analitico ad un modo nuovo di usare i dati in azienda.

INTRODUCING AMAZON AI

INCUBATORI APERTI PER UNA CRESCITA DIGITALE DEL PAESE

Di **Francesco Manca**, Junior Analyst, The Innovation Group

All'interno dell'iniziativa "**Piemonte Digitale**" di The Innovation Group, edizione piemontese del programma nazionale Digital Italy finalizzato allo sviluppo di idee per una crescita ed innovazione digitale del nostro paese, si è parlato anche di formazione, ricerca e startup.

Nel dibattito è emerso come le startup siano essenziali per la crescita e il progresso sia tecnologico che economico, in quanto sono parte integrante del tessuto imprenditoriale giovane ed innovativo del paese.

Incubatori ed acceleratori dovrebbero quindi essere fondamentali fonti di progresso per un paese che, come il nostro, è al 50° posto nel ranking della ease of doing business della World Bank, dopo Mauritius, Serbia e Moldova, paese in cui le vecchie generazioni detengono la maggior parte della ricchezza e che non ripone piena credibilità nei giovani.

Al contrario, questi intermediari e programmi di sviluppo imprenditoriale non son ben diffusi o valorizzati su tutto il territorio nazionale.

Ma perché bisognerebbe riporre fiducia in incubatori ed acceleratori e che cosa sono?

Gli acceleratori "accelerano" lo sviluppo di una società, mentre gli incubatori "incubano" idee dirompenti con l'intento di costruire un business model e un'azienda: sono entrambe elementi essenziali per il sostegno all'innovazione (e quindi alla crescita) di un paese.

Per formare un ambiente favorevole alla nascita e crescita di nuove realtà imprenditoriali è inoltre opportuno modellare un **ecosistema** innovativo sul territorio, in cui si devono sviluppare le future imprese: forgiare imprese su strutture che non rispecchiano le dinamiche del territorio non le abilita ad avere gli strumenti adatti al successo nel mercato reale. Imitare esempi di successo (es. Silicon Valley) ma appartenenti ad altre realtà non è quindi una strategia vincente e di successo.

Marco Cantamessa, presidente del principale incubatore universitario italiano **i3P**, a questo proposito propone un modello di incubatore che si fa forza dei network locali e rispetta le esigenze del luogo.

Fondato nel 1999, i3P ha sede presso il campus principale del Politecnico di Torino ed è uno dei primi incubatori italiani di startup innovative.

La mission di i3P è quella di contribuire alla crescita tecnologica del paese creando un ecosistema florido per le startup, fornendo ai loro fondatori spazi attrezzati, servizi di consulenza e un ricco network internazionale di partner, mentor, clienti, manager e investitori, nonché la possibilità di entrare facilmente in contatto con le competenze del Politecnico di Torino. La novità di un progetto del genere è quella di offrire un network all'interno di un contesto universitario anche ad imprenditori esterni, riconoscendoli attori concreti e non da escludere dell'ecosistema innovativo locale, uscendo così da un ottica autoreferenziale, di chiusura innovativa frequente in altri contesti di ricerca universitaria e di innovazione nazionale.

i3P si rivolge infatti non solo a chi ha solo idee innovative ed imprenditoriali, ma anche a startup in fase embrionale, ad investitori individuali e istituzionali che cerchino target di investimento qualificati ed innovativi, ed ad imprese, di qualsiasi dimensione, interessate all'innovazione che intendano interagire con le start up a livello commerciale o di investimento, o che intendano costituire propri spinoff.

i3P propone quindi un modello di incubatore ad ecosistema, in cui lo spillover di competenze arricchisce il network ed il territorio in cui si trova tramite scambi informativi, formali e non, all'interno di un ambiente fisico (il campus del Politecnico di Torino), già tarato su questo obiettivo.

I numeri dell'incubatore piemontese confermano il successo di questa struttura aperta (49 imprese costituite e 145 progetti lanciati nel 2016), ma Cantamessa ha però sottolineato come a fianco di una struttura efficace come la sua si necessiti anche di una mentalità aperta da parte del territorio e delle imprese tradizionali.

In Italia, e nello specifico in Piemonte, sembra infatti che si debbano fare ancora passi in avanti in questa direzione, in quanto le imprese sono solo apparentemente interessate alle startup ma sono ancora molto reticenti a investire su di esse, non vedendole interlocutori diretti e qualificati su cui instaurare relazioni di business.

La trasformazione della società e dell'economia contemporanea, finché non cambia questa mentalità, non inglobando realtà innovative, sarà sempre aleatoria.

Al contrario lo stesso tessuto imprenditoriale, come anche le strutture degli incubatori, dovrebbe superare i modelli tradizionali chiusi di innovazione e crescita, sviluppando invece nuove logiche aperte di contaminazione dei saperi come quelle ad ecosistema proposte da i3P

VETRI TRASPARENTI FOTOVOLTAICI: INNOVARE I MATERIALI DA COSTRUZIONE

Di **Vincenzo D'Appollonio**, Partner, The Innovation Group

Durante le nostre attività consulenziali, ci siamo imbattuti in una società spagnola, la Onyx Solar, che produce Soluzioni di Architettura Solare, mediante Vetri trasparenti Fotovoltaici integrabili nelle Costruzioni: stiamo ora conducendo un progetto di sviluppo del Mercato Italiano per conto di una società di Pavia che ne è diventata distributore esclusivo per l'Italia.

Come afferma Norman Foster, "L'architettura solare non è una questione di mode, ma di sopravvivenza."

La sempre maggiore sensibilizzazione nei confronti dell'ambiente fa sì che l'ecosostenibilità nel campo dell'edilizia sia un concetto a più alto impatto ambientale: in questo senso la bioedilizia è l'unica via da percorrere.

Come scrive l'architetto Paolo Rava, "in natura la bioedilizia è presente da sempre: la foglia è un pannello fotovoltaico che attraverso la fotosintesi clorofilliana produce energia, la noce ha una pelle che la avvolge a 360° senza ponti termici ed è chiara e lucida per sfruttare al meglio la luce, la pesca ha un "cappotto" di fibra e acqua che protegge il seme interno, e via dicendo. In ogni caso l'obiettivo finale è: usare meno energia possibile".

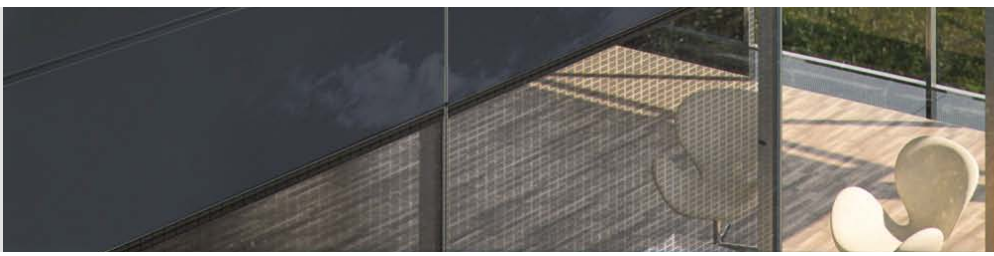
Le Soluzioni della Onyx Solar si calano perfettamente in questo contesto: le proprietà attive dei vetri fotovoltaici di Onyx Solar permettono agli edifici di produrre energia gratuita e pulita, ma anche di consumare meno energia grazie al miglioramento dell'isolamento termico degli edifici in cui i vetri solari sono integrati. Aumentano anche l'efficienza degli edifici, facendo risparmiare energia e denaro! Le facciate solari ventilate sono un esempio di funzionalità e bellezza estetica. Non solo possono essere integrate in qualsiasi tipo di edificio, ma generano anche elettricità e migliorano l'efficienza energetica generale dell'edificio permettendo risparmi in termini di consumi. Inoltre, il vetro Onyx Solar ha dimostrato la sua robustezza e resistenza anche a violenti impatti. Le caratteristiche di estrema sicurezza e qualità dei materiali impiegati stanno rivoluzionando il mercato del fotovoltaico integrato nelle costruzioni, e l'installazione è più veloce e semplice di quanto si pensi, con risultati eccezionali!

La Onyx Solar è già presente in molti paesi del mondo, ed alcune sue realizzazioni sono già una valida testimonianza dell'efficacia delle sue Soluzioni; una delle più recenti è la Union National Bank, situata nel cuore finanziario del Cairo, che ha previsto l'integrazione di 439 mq di vetro fotovoltaico prodotto da Onyx Solar per la facciata ed il tetto della propria sede. A completamento del progetto, l'edificio disporrà di una stupenda facciata di vetro blu amorfo ed un tetto di silicone monocristallino che potranno generare energia 'green' a volontà.

Vi sono almeno tre ragioni che consentono ai Vetri fotovoltaici della Onyx Solar di cambiare le regole del gioco: "Permettono agli edifici di essere autosufficienti nel consumo di Energia, infatti mentre generano elettricità dal Sole, permettono l'ingresso di luce naturale, impediscono il rilascio di CO_2, ed ottimizzano le proprietà di isolamento e filtraggio;

"Risparmiano denaro ed energia ai propri Clienti, infatti è l'unico materiale da costruzione che si ripaga totalmente; "Si integrano perfettamente in una molteplicità e varietà di edifici, adattandosi completamente alla esigenze realizzative ed ai requisiti di ciascun Progetto.

In conclusione, riteniamo che i Vetri Fotovoltaici della Onyx Solar possano rappresentare la perfetta sintesi tra 'ecosostenibilità' ed 'estetica': la gamma illimitata di configurazioni, a cui si aggiunge la possibilità di includere diversi colori, finiture, forme, dimensioni e spessore, li rendono materiali totalmente integrabili, in modo innovativo, nella costruzione di tutti i tipi di edifici e strutture, senza compromettere minimamente Stile e Design.



QUAL È L'IMPATTO DELL'ADEGUAMENTO GDPR SULLE MISURE PER LA SICUREZZA NELLE AZIENDE ITALIANE?

Di **Avv. Valentina Frediani,** Founder e CEO, Colin & Partners

A pochi mesi dalla piena applicabilità del nuovo Regolamento europeo sulla Data Protection il tema suscita ancora dibattito e suggerisce una serie di interrogativi alle imprese; primo fra tutti: come evolverà il concetto di privacy nell'ecosistema aziendale? Di conseguenza, come dovranno agire le risorse coinvolte, in particolare le Direzioni aziendali, per ridefinire i processi interni nell'ambito dell'iter di adeguamento al quadro normativo?

Per costruire un perimetro di tutela efficace, infatti, non è sufficiente un Regolamento. Occorre adottare una logica multidisciplinare, la cosiddetta Cyber Resilience, frutto della sinergia di diversi componenti: compliance, cyber security, gestione del rischio informatico, strategia di prevenzione, risposta rapida ed efficace alle minacce. Ponendo al centro del disegno la tutela delle informazioni aziendali, vera sorgente di valore nella moderna economia digitale, la GDPR rappresenta dunque il punto di partenza e il fine del sistema di governance dei dati.

Traguardo che trova in un approccio strutturato che si muove per obiettivi, lo strumento migliore per raggiungerlo. Partendo dalla gap analysis dei sistemi informativi si compie il primo passo per prendere coscienza del livello di conformità raggiunto dalla propria azienda. I risultati ottenuti consentiranno di pianificare il percorso da intraprendere per raggiungere un livello di aderenza alla norma ottimale rispetto al proprio business.

Un processo di analisi che non deve trascurare l'aspetto contrattuale, sia in riferimento agli accordi pluriennali che a quelli stipulati prima del maggio 2018.

La privacy deve rappresentare uno dei perni attorno ai quali costruire piani di sviluppo e – al tempo stesso – operare una riprogettazione dei processi in essere. La GDPR impone, di fatto, un approccio estremamente lucido e concreto, obbligando ad una valutazione strutturata dell'investimento aziendale da compiere, sia in termini economici, che di tempo e risorse.

Visione d'insieme e pragmatismo divengono dunque i migliori strumenti per calare la normativa all'interno del sistema aziendale e per tradurre gli adempimenti del Regolamento nei vari contesti di business.

Accountability, privacy by design e privacy by default, imponendo ai titolari del trattamento di mettere in atto misure tecniche organizzative adeguate per garantire – ed essere in grado di dimostrare – sin dall'origine che ogni trattamento sia adeguato alla normativa, costituiscono i principi guida su cui basare progetti ed investimenti.

Presupposti, quelli menzionati, fortemente incentivati e rafforzati dal rinnovato **meccanismo sanzionatorio** che può colpire le finanze aziendali fino a 20 milioni di Euro o fino al 4% del fatturato globale mondiale annuo di gruppo.

Per attuare le disposizioni previste dal Regolamento le aziende hanno a disposizione un complesso di soluzioni dall'elevato potenziale che – considerate dal punto di vista dell'Autorità Garante – possono essere lette anche come un efficace apparato strumentale per le attività di verifica.

Privacy impact assessment, registri di trattamento e policy di notifica del "**data breach**" rappresentano le espressioni più concrete dell'evoluzione normativa verso la trasparenza e un sistema di gestione più snello e pratico da attuare.

All'introduzione di tali misure va aggiunta quella che, forse più di tutte, sta muovendo le dinamiche d'impresa, ovvero l'introduzione della figura del DPO.

Pur non rappresentando, nel panorama europeo, una completa novità, il Data Protection Officer – conosciuto anche come Responsabile della Protezione dei Dati – sarà il trait d'union tra impresa, soggetti interessati dal trattamento e Authority per la protezione dei dati personali, assumendo un ruolo chiave nel Privacy compliance Program dell'azienda.

AFFRONTARE IL RISCHIO CYBER NELLE SMART CITIES DEL FUTURO

Di **Elena Vaciago**, Associate Research Manager, The Innovation Group

Non c'è alcun dubbio che ogni città, in futuro, avrà abbracciato in parte o in toto un approccio smart, tramite infrastrutture digitali che renderanno più efficienti, sicuri ed ecologici i servizi pubblici dei grandi conglomerati urbani. Una città interconnessa promette grandi vantaggi, come la possibilità di evitare congestioni del traffico, o il disegno di servizi pubblici basati su effettivi bisogni della comunità. Il problema è che nel **puzzle della digitalizzazione delle città**, un tassello, quello della cybersecurity, ha ricevuto finora un'attenzione troppo bassa.

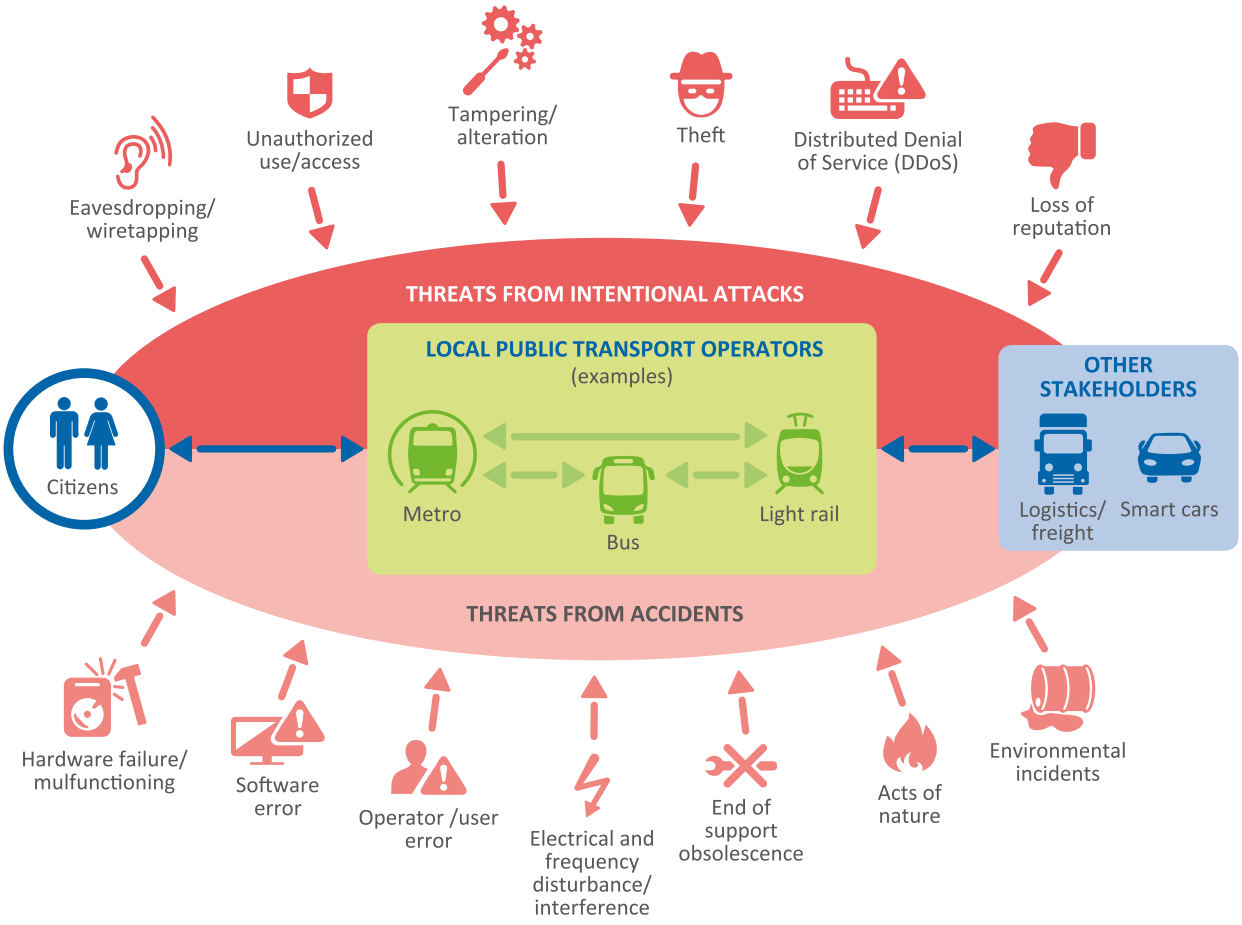
Permane la possibilità che attaccanti malevoli siano in grado di sfruttare le vulnerabilità di sistemi vitali che costituiscono la spina dorsale del funzionamento delle città. Potranno quindi metterla in crisi, arrestando ad esempio la distribuzione dell'energia elettrica, bloccando gli impianti di potabilizzazione dell'acqua o i sistemi di raccolta e trattamento di rifiuti, prendendo il controllo dei sistemi di gestione del traffico.

Quali sono i rischi per una smart city?

La grande eterogeneità dei sistemi intelligenti che possono essere collegati tra loro in uno scenario di smart city (già oggi di 2,3 miliardi di oggetti connessi), i vari livelli di maturità delle tecnologie, la presenza o meno di un controllo centralizzato. Più elementi concorrono a determinare uno scenario complesso di rischio e soprattutto una più ampia "superficie d'attacco", sempre più difficile da mettere in sicurezza. Come mostra la Figura successiva, tratta dal report ENISA di dicembre 2015 "Cyber security for Smart Cities. An architecture model for public transport", sono moltissime le possibili minacce da considerare, e non solo quelle propriamente malevole che rientrano in uno schema classico di attacco (dal furto di identità, al denial of service, all'accesso non autorizzato). Vanno anche analizzate le minacce potenzialmente legate a incidenti non intenzionali, come errori di operatori umani, interferenze elettriche, eventi ambientali, malfunzionamento di sistemi.

Figura 1 Panorama delle minacce da attacchi intenzionali e da incidenti occasionale per i trasporti pubblici

Fonte: ENISA 2015



Qual è la probabilità che avvenga un attacco cyber alle infrastrutture digitali delle città?

Pensiamo ad infrastrutture come reti pubbliche WiFi, telecamere di videosorveglianza, reti elettriche e infrastrutture legate a trasporti e smart mobility, sistemi di public lighting, App mobile per l'accesso a servizi pubblici. Quali problematiche di sicurezza presentano? Le reti pubbliche WiFi, proprio perché aperte a svariati utilizzi da parte dei cittadini, possono rappresentare gravi rischi alla sicurezza. Le reti energetiche sono state già oggetto di attacco, basti pensare a quanto avvenuto per 2 volte di fila in Ucraina, prima del dicembre 2015 (un attacco cyber ha lasciato al buio 230.000 persone), poi a fine 2016 nella sola città di Kiev. Poiché l'energia elettrica è un servizio essenziale, un black out genera tipicamente effetti a cascata. Nell'area dei trasporti, un sistema interconnesso prevede soluzioni che vanno dall'automazione della segnaletica stradale, all'illuminazione intelligente delle strade, alla connect e autonomous car, al car sharing e all'infomobility. I ricercatori di sicurezza si sono già sbizzarriti, dimostrando sia la possibilità di hackerare un veicolo (prendendone il controllo da remoto e agendo sia sul sistema radio interno, sia agendo sui freni), sia la capacità di alterare i segnali del traffico.

Considerate quindi le capacità già raggiunte oggi, unite a vulnerabilità già molto diffuse legate agli sviluppi delle smart cities che stanno avvenendo a velocità sostenute, quanto tempo passerà ancora prima che sia congeniato un attacco più mirato e complesso, in grado di colpire contemporaneamente più sistemi con effetti a cascata, e di diffondere il panico tra la popolazione?

Già si è visto di recente come l'allarme per presunti attacchi terroristici può portare a comportamenti molto pericolosi nel caso di grandi numeri di persone. Una situazione simile è stata quella vissuta nella città di Dallas, in Texas, quando lo scorso 7 aprile, durante la notte (esattamente alle 11.40 di sera) alcuni hacker hanno preso il controllo di **156 sirene di emergenza**, normalmente utilizzate per segnalare condizioni meteorologiche di estrema gravità. Le autorità hanno tentato di avvertire la cittadinanza che in realtà non c'era alcuna emergenza in corso, e hanno anche provato ad arrestare il suono delle sirene, ma finché è durato l'attacco, ossia per 1 ora e 40 minuti, le sirene hanno suonato senza interruzione. I cittadini, temendo un problema serio e presi dal panico, hanno invece continuato a tempestare di chiamate i call center del 911. In definitiva, il sindaco di Dallas, Mike Rawlings, ha dichiarato dalla sua pagina ufficiale su Facebook che si sarebbe cercato di individuare e perseguire gli attaccanti, ma l'impressione generale è stata che l'attacco, che non ha comportato del resto danni reali, sia stato principalmente una "dimostrazione di forza" da parte di alcuni "white hat hacker".

Quali dovrebbero essere quindi le "buone pratiche" per una corretta cybersecurity per le smart cities?

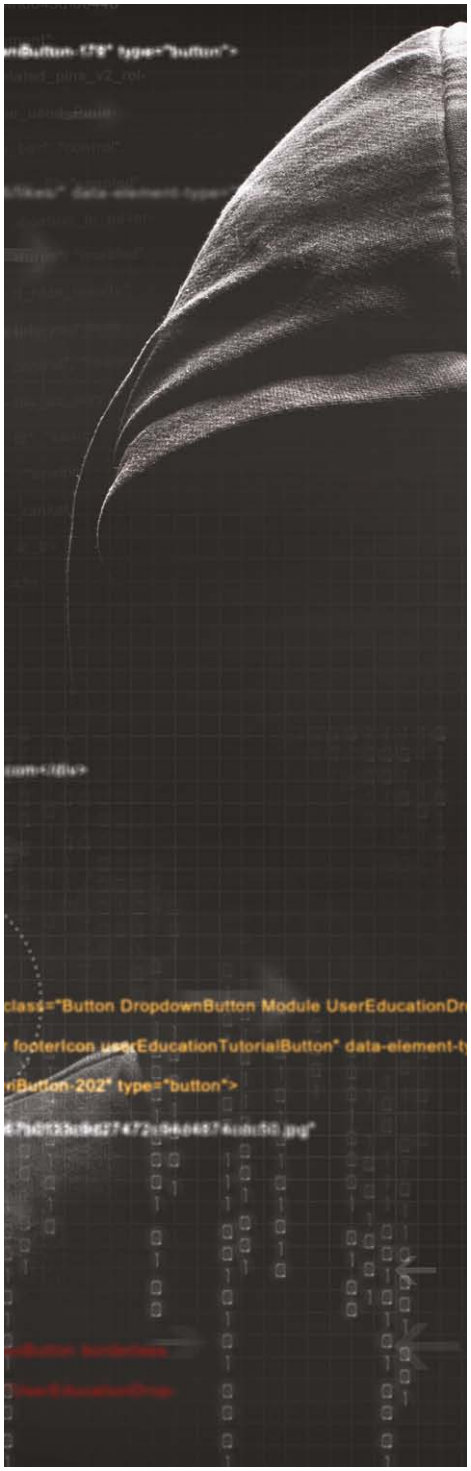
Una maggiore resilienza a interruzioni del funzionamento di servizi critici per la comunità, e la protezione di dati personali relativi a milioni di cittadini, deve essere oggi una priorità nell'agenda dei manager del settore pubblico. A Singapore, città che guida gli sviluppi in ambito urbano, dalla mobilità con auto autonome e connesse, ai pagamenti cashless, smart healthcare ed efficienza energetica, il sito ufficiale della smart city riporta "Cyber security is a key enabler of our Smart Nation. The government, industry and public must all play their part and take measures to safeguard data, and ensure that critical control systems are protected even as we make them smart".

Risolvere gli aspetti di cybersecurity in uno scenario di Internet of Things come quello di una smart city può risultare quasi impossibile, se non molto costoso, se l'approccio scelto è quello di risolvere i problemi via via che questi si presentano, quindi con misure ex post. E' fondamentale che tutte le iniziative di digitalizzazione tengano conto degli aspetti di cybersecurity fin dalla prima fase di **disegno della soluzione**. Al giorno d'oggi questo è possibile perché la disciplina è matura e prevede attività minime, dall'autenticazione degli utenti, alla cifratura dove necessario, alla configurazione sicura dei sistemi. Misure avanzate che aiuteranno a incrementare la sicurezza sono: un monitoraggio dei sistemi per verificare che non siano modificati o sfruttati in modo malevolo; sistemi automatici di rilevamento ed alerting; sistemi di risposta in caso di incidente.

E' anche molto importante designare una **corretta struttura di controllo** su questi temi, perché la mancanza di una chiara leadership sulla cybersecurity non possa diventare la scusa per non occuparsene. Sarebbe importante stabilire un **CERT o CSIRT municipale**, con piena responsabilità sulla supervisione delle attività, in particolare sulla gestione di vulnerability assessment e audit per identificare i problemi, gestire il life cycle dei prodotti e assegnare corrette priorità alla protezione degli asset più critici. Infine, questa struttura andrebbe deputata a gestire piani di risposta in caso di incidenti.

Un ulteriore tema che sta acquistando sempre maggiore rilievo è quello della **protezione dei dati personali**: in una città smart, il tema della privacy dei cittadini andrà affrontato con un giusto rilievo. Per la protezione delle identità digitali sarà fondamentale avere un ID management, con regole e standard di controllo degli accessi a livello distribuito.

Per maggiori informazioni sul tema segnaliamo un paio di ricerche che forniscono un elenco dettagliato delle misure per la protezioni di infrastrutture digitali in contesti di smart cities: il report "Cyber Security Guidelines for Smart City Technology Adoption" pubblicato da CSA (Cloud Security Alliance) nel novembre 2015, e lo studio "The future of smart cities: cyber-physical infrastructure risk", di agosto 2015, in cui il DHS/OCIA USA (Department of Homeland Security's Office of Cyber and Infrastructure Analysis) ha definito come impostare un Infrastructure Risk Assessments per la valutazione dei rischi emergenti di grandi infrastrutture critiche.



DATA CENTER DIGITAL TRANSFORMATION: LA SFIDA DI IBM

Di **Camilla Bellini**, Senior Analyst, The Innovation Group

Lo scorso 14 giugno a Londra abbiamo partecipato all'IBM Cloud Analyst Day 2017, durante il quale abbiamo avuto la possibilità di confrontarci con IBM in merito agli aggiornamenti della sua strategia in ambito cloud, ma non solo.

Nel corso dell'incontro è stato affrontato il tema della digital transformation in tutti i suoi aspetti, benché IBM lo declini soprattutto a partire da quello che storicamente è stato il suo core business, il data center: più che di digital trasformation si usa l'espressione "data center digital transformation".

È proprio a partire dalla trasformazione dei data center, dal loro ripensamento secondo le logiche del Cloud, che IBM ha scelto infatti di riposizionarsi negli ultimi anni, avendo però ben chiaro i diversi approcci da adottare a seconda dell'interlocutore: da un lato, IBM si propone di fornire ai propri clienti storici tutti gli strumenti necessari per trasformare la propria infrastruttura secondo le nuove logiche del cloud; dall'altro, IBM continua la propria attività di posizionamento rispetto al mondo dei developer, la cui rilevanza cresce dentro e fuori l'azienda, puntando in particolar modo sulla piattaforma Bluemix.

In questo senso, anche le innovazioni introdotte nell'ambito del middleware si basano sulla logica di mantenimento dei clienti che da sempre investono in questo ambito con IBM, non dando quindi loro ragione di migrare verso altri sistemi.

Si tenga comunque presente che, più in generale, IBM non ritiene che esista un modello di cloud computing omnicomprensivo, in grado di risolvere ogni esigenza, ma al contrario propone una strategia multi-cloud, in grado di affrontare i diversi workload e le necessità specifiche dei diversi interlocutori con cui si interfaccia.

In questo senso, pur ritenendo che il mercato sia sostanzialmente public cloud-driven e proponendosi di guidare i propri clienti in questa direzione, li supporta nello sviluppo di un approccio "orientato al controllo", ossia in una logica di hybrid cloud, che mantiene il controllo delle scelte e delle strategie IT all'interno delle aziende.

Affrontando quindi la sfida della digital trasformation mantenendo il proprio focus su questi due ambiti, IBM continua a fare passi avanti nel processo di consolidamento delle acquisizioni e della sua offerta cloud.

Come infatti già era stato annunciato nel 2016, IBM ha confermato quest'anno l'unificazione di tutte le sue componenti cloud in un'unica piattaforma d'offerta, che dovrebbe avvenire per fine anno.

In particolare, la "classica" offerta di Softlayer e Bluemix convergerà verso una nuova generazione di servizi, che prendono il nome di Athena (per la componete PaaS) e Genesis (per la componente Iaas): questi due servizi non devono essere però considerati come qualcosa di nuovo, di diverso rispetto a Softlayer e Bluemix, ma al contrario come la loro evoluzione, con l'integrazione di alcuni elementi di "bridge" in diversi ambiti (Portal/IAM/BSS, Container, Network, Data Center).

Inoltre, IBM si propone di coinvolgere e integrare le logiche dell'intelligenza artificiale – per cui ritengono di avere la tecnologia AI più sviluppata sul mercato – attraverso tutta la propria offerta cloud, elemento che diventa differenziante del posizionamento di IBM rispetto agli altri cloud vendor; a questo si aggiunge poi l'esperienza che IBM può mettere a disposizione dei clienti, esperienza che consente di supportare una migrazione consistente dei workload da ambienti on premises al cloud (o tra ambienti private/public cloud).

PANOPTESEC, PER UNA GESTIONE DINAMICA DEL RISCHIO CYBER

Intervista di **Elena Vaciago** a **Andrea Guarino**, Acea

Il progetto di ricerca europeo Panoptesec propone un sistema decisionale (DSS) che analizza vulnerabilità e incidenti informatici in tempo reale, consentendo una gestione dinamica del rischio residuale. Ne abbiamo parlato con Andrea Guarino, Responsabile Security, Privacy & Compliance – Funzione ICT di Acea, società che ha partecipato al progetto in qualità di user agency.

Andrea GUARINO

Dopo la recente diffusione del malware "WannaCry", che in pochi giorni ha colpito oltre 200mila computer in oltre 100 paesi, e dopo la continua scoperta di gravi vulnerabilità, come quella sul sistema AMT di Intel che permetterebbe di prendere il controllo da remoto dei PC dotati di questa caratteristica, molti si stanno chiedendo se è possibile avere una fotografia aggiornata in tempo reale dello stato di rischio cyber della propria azienda.

Il progetto europeo di ricerca "**Panoptesec**" si pone appunto questo obiettivo: disporre di una soluzione per dotarsi di una visibilità il più possibile ampia sulla situazione (il termine in greco antico significa "tutt'occhi"), oltre che essere in grado di mitigare il rischio ed eventualmente di risolvere una situazione di crisi.

Cofinanziato dalla Commissione europea (nell'ambito del FP7) e con un budget complessivo di 7,5 milioni di euro, Panoptesec, oggi in via di conclusione e diffusione dei risultati, ha portato allo sviluppo di un sistema decisionale (DSS) che analizza vulnerabilità e incidenti informatici in tempo reale, consentendo una gestione dinamica del rischio residuale.

La soluzione è in grado di operare in **modo proattivo ma anche reattivo** in caso di incidente: valuta le debolezze del sistema, individua i potenziali percorsi di attacco, propone un elenco di azioni di risposta in ordine di priorità (sulla base delle criticità del singolo business), dà la possibilità di valutazioni preventive, si basa su motori di analisi automatizzata che mostrano i risultati nel dettaglio in dashboard dedicate.

Il progetto è stato indirizzato soprattutto alla protezione di infrastrutture critiche (reti SCADA che controllano servizi primari per la popolazione, strutture vaste come gli aeroporti e installazioni di tipo militare) e alla gestione più efficiente di situazioni di emergenza e incidenti.

Al consorzio hanno aderito vari attori italiani ed europei: l'Università La Sapienza di Roma, l'Università di Lubeck, Epistematica, Alcatel Lucent, Supélec, l'Institut Mines-Télécom di Parigi.

La leadership tecnica è stata di Rhea System SA, mentre **Acea** è stata coinvolta in qualità di user agency, per testare il prototipo e fornire dati legati a situazioni reali sul campo.

"*Il progetto nasce dalla considerazione che oggi non è più sufficiente effettuare un vulnerability assessment un paio di volte all'anno* – spiega **Andrea Guarino**, Responsabile Security, Privacy & Compliance – Funzione ICT di Acea – *gli asset da proteggere cambiano, e anche dove questi dovessero rimanere gli stessi, sono le nuove vulnerabilità scoperte ogni giorno, le nuove minacce, a modificare il profilo del rischio da affrontare. Da qui la necessità di gestire i rischi in modo dinamico*".

Più codice si ha sulle proprie infrastrutture informatiche, più si va incontro a potenziali nuove vulnerabilità che saranno scoperte via via nel tempo, dando origine a **Zero-day** che inizialmente sono sfruttati per scopi precisi (ad es. minacce di tipo persistente come Stuxnet), poi, una volta noti, sono rivenduti nei mercati neri del web o semplicemente riutilizzati per altri fini (ad es. cybercrime).

"*In teoria* – aggiunge Andrea Guarino – *una volta che una vulnerabilità è nota, qualcuno (il produttore del sistema vulnerabile, il distributore, chi ne gestisce la sicurezza, ecc.) dovrebbe intervenire. In alcuni casi però risolvere il problema potrebbe costare molto o essere tecnicamente così complesso, da far valutare alle aziende la possibilità di sostituire integralmente i device attaccabili con una versione aggiornata degli stessi e priva di quella vulnerabilità. Le aziende dovrebbero quindi chiedere e scegliere fin dall'inizio soluzioni che non siano facilmente attaccabili prevedendone comunque meccanismi di aggiornamento, ma anche ipotizzare la scoperta nel tempo di nuove vulnerabilità, e quindi gestire il rischio nel momento in cui esso si dovesse concretizzare. Il progetto Panoptesec risponde appunto a questa esigenza, misurando qual è l'esposizione in un determinato contesto, fornendo suggerimenti su come ridurre il rischio residuo a livelli accettabili, indicando le priorità di intervento, suggerendo infine se e dove è necessario applicare patch e in quale ordine, anche dove questo è controintuitivo*".

Panoptesec monitora costantemente lo stato della cyber security e la capacità di risposta in tempo reale. Valuta in modo proattivo e reattivo le debolezze del sistema, per individuare potenziali attacchi e fornire un elenco di azioni di risposta in ordine di priorità, al fine di gestire automaticamente questo tipo di incidenti.

"*In caso di crisi segnala anche eventuali "sacrifici" da attuare, come separare dalle reti particolari segmenti per evitare effetti domino su scala più ampia: un procedimento che, se fosse stato correttamente applicato in Ucraina, avrebbe probabilmente evitato un black out così ampio e prolungato*" conclude Andrea Guarino.

PANOPTESEC

NOTE

IL CAFFÈ DIGITALE

QUESTO MESE ABBIAMO FATTO COLAZIONE CON...

FASTWEB
un passo avanti

iscriviti alla nostra **Newsletter** mensile per restare in contatto con noi!

Riceverai articoli dei ricercatori di **The Innovation Group**, aggiornamenti sul piano **Eventi**, informazioni sulle **Ricerche** e i **White Paper**, Inviti e promozioni riservate.

COMPILA IL FORM DI REGISTRAZIONE SU

www.theinnovationgroup.it