La sicurezza delle Smart City: non solo una priorità, ma anche una visione

Author : Giovanni Villarosa

Date : 14 Marzo 2019

Nell'ultimo decennio tra i governi dei maggiori Paesi occidentali è maturata la consapevolezza che alcune delle più importanti infrastrutture (sistema produttivo, economico, sociale, etc.) che forniscono **indispensabili servizi** necessari al funzionamento della società, e che assicurano la nostra qualità di vita, siano **vulnerabili**; e lo sono, sia nei confronti delle minacce antropiche (attentati terroristici, cybercrime, malfunzionamenti, etc.) sia a seguito di eventi naturali (black out elettrici, eventi climatici, terremoti, etc.).

Tali minacce rappresentano solo alcune delle motivazioni del perché certe infrastrutture vengono considerate critiche (IC) e, se vogliamo garantirne il corretto funzionamento, dobbiamo proteggerle in maniera adeguata; una protezione che dovrà sempre considerare, e contrastare, una variabile intrinseca negativa conosciuta come ***effetto domino***, ovvero: la reazione secondaria alla propagazione incontrollata degli effetti causati dalla c.d. *loss of service* (la perdita delle funzioni e dei servizi) in caso di anomalo funzionamento di una specifica IC, anche se non appartenente allo stesso settore e/o al complessivo sistema di governo.

Oggi, l'evoluzione socio-tecnologica di un moderno centro urbano ha **modificato profondamente la struttura funzionale di una città**, sia dal punto di vista innovativo, quanto dal lato gestionale; una *città* moderna è il prodotto conseguente dei molteplici cambiamenti che sono avvenuti nel corso della storia, sia dal punto di vista culturale che da quello sociale (urbanesimo), post-rivoluzione industriale del XIX secolo.

Il risultato di tutte queste trasformazioni, *storico-culturali e socio-tecnologiche,* ha delineato sempre di più una **città come un *complesso infrastrutturale articolato***, ormai considerata alla stregua di una vera e propria *infrastruttura critica*, dalla *complessa* gestione.

Ricordo che durante un convegno sul tema presso la Camera dei deputati, nel marzo 2014, il dott. Joseph Bruno (Commissioner Office of Emergency Management di New York city) illustrando il suo progetto della *grande mela smart city,* la poneva a livello di una IC; commentando il suo progetto, applicato peraltro in uno scenario urbano articolato e dal contesto

multiforme come NY City, sottolineava più volte come il **giusto approccio** da seguire fosse proprio quello di considerare il *sistema-città come un complesso infrastrutturale fortemente eterogeneo*, per l'appunto critico, evidenziando, tra le altre cose, un altro particolare aspetto: la necessità di mettere in campo una **partnership tra pubblico e privato**, tramite azioni sinergiche sostanziali al raggiungimento delle finalità progettuali.

Il dott. Bruno evidenziava poi un ulteriore presupposto: la funzione centrale nei **processi ambientali, sociali e di sviluppo** economico nel contesto nazionale; presupposti che daranno forma (politicamente e operativamente) alle *smart city* (SC), *contenitori* sociali, politici, tecnologici che avranno il compito di affrontare le sfide future in ordine a tematiche come *mobility, environment, living, people, economy* e *governance*.

Una metropoli *smart* si definisce tale quando*: gli investimenti in capitale umano e sociale, le infrastrutture di comunicazione tradizionali (trasporti) e le moderne telecomunicazioni (ICT) alimentano una crescita economica sostenibile e una alta qualità della vita, con una gestione oculata delle risorse naturali, attraverso una governance partecipativa;* insomma, quando **l'azione di governo coinvolge in modo proattivo i propri cittadini**, rendendoli parte attiva e integrante del processo gestionale (ambiente, mobilità, trasporti, pianificazione territoriale, infrastrutture, etc), assicurandogli nel contempo la giusta sicurezza e protezione.

E, proprio partendo dal concetto di protezione, osserviamo come il tema della sicurezza - nelle sue accezioni anglosassoni di security-safety-emergency - diventi un argomento imprescindibile; perché nessuna città può diventare smart, come nessuna comunità può essere intelligente, se non garantisce ai suoi cittadini il diritto alla sicurezza.

E per far ciò è significativo mettere in campo **azioni politiche mirate**, attività che si basano su concetti che rappresentano il fondamento del paradigma principe della SC: una città sicura è il risultato di un'osservazione olistica dell'ambito cittadino, perché il livello di sicurezza si misura rapportandolo al segmento più debole, mediante un approccio sistemico.

Ad esempio, in una città il segmento più debole della sicurezza stradale è facilmente identificabile nella **viabilità** stessa, un luogo di mobilità dove *persone & macchine* incrociano le proprie direzioni, e laddove si inserisce una particolare quanto negativa variabile: la fretta.

Benché appaia, apparentemente, un sistema rigidamente normato, la pubblica via sottende il regno del caos, una conseguenza frutto della mole di stimoli e di segnali prodotti da una iper-regolamentazione che ha reso il sistema scarsamente decifrabile, cosa ancor più vera quando il principale protagonista è un elemento fallace come l'essere umano.

Da tutto ciò si comprende come nelle SC la questione sicurezza diventi una *vision,* incardinata all'interno e all'intero processo, da cui non si può prescindere quando le funzioni vengono integrate e delegate alla tecnologia; e quando il sistema centrale di governo di una città passa dall'uomo alle *macchine digitali*, rappresentate dagli elementi dell'*Internet of Things* (IoT), ecco che **la sicurezza diventa non soltanto una priorità, ma appunto una *visione***, *quel qualcosa da non sottovalutare*, perché il funzionamento e la competitività delle moderne città non dipendono solamente dalle infrastrutture materiali (capitale fisico) ma, anche e sempre di più,

dalla disponibilità e dalla qualità delle infrastrutture dedicate alla comunicazione (ICT) e alla partecipazione sociale (capitale intellettuale e sociale).

Ma quale è il significato dell'**acronimo SMART**, molto spesso adoperato in letteratura per richiamare le caratteristiche di un obiettivo ben definito, tipicamente aziendale, di dipartimento o di unità organizzativa?

Lo possiamo così riassumere:

- ***S****pecific* -Specifico- fare riferimento a un'area di miglioramento ben definita;
- ***M****easurable* -Misurabile- quantificabile o almeno riferito a un indicatore di avanzamento;
- ***A****chievable* -Raggiungibile- esiste anche la variante -Assignable- assegnabile a qualcuno;
- ***R****ealistic* -Realistico- l'obiettivo può essere raggiunto con le risorse a disposizione;
- ***T****ime-constrained* -data limite-.

Sappiamo anche come questo acronimo individui **l'insieme organico dei fattori di sviluppo di una città**, peraltro risaltandone l'importanza del *capitale sociale* di cui ogni ambito urbano è dotato; perciò fermandoci al concetto di *città intelligente*, intesa come *città digitale*, isolando dal contesto *l'elemento umano*, rischiamo di commettere un grossolano errore, se non gestissimo in *modalità intelligente* - appunto *smart* - tutte le attività economiche, la mobilità pubblica, il sistema trasporti, le risorse ambientali, le interrelazioni tra persone, le politiche urbanistiche e il modello di amministrazione pubblica.

Qui di seguito proviamo ad analizzare allora alcuni **punti** tra i più strategici di una smart city e più nel dettaglio:

- infrastrutturale: è di fondamentale importanza che le risorse siano utilizzate nella rete per migliorare l'efficienza economica, politica, in modo tale da consentire compiutamente uno sviluppo culturale sociale, culturale e urbanistico, ricorrendo ampiamente all'uso delle tecnologie ICT (telefonia fissa, mobile, reti informatiche, etc.) evidenziando l'importanza della *connettività* quale importante componente di sviluppo;
- economico: approfittare dei vantaggi derivanti dalle opportunità offerte dalle tecnologie ICT per aumentare la crescita e la competitività; ragioniamo quindi sulla creazione di città capaci di attrarre nuove realtà imprenditoriali, elemento questo che, a sua volta, va associato a un'efficiente quanto efficace pianificazione territoriale ed economica;
- sociale: un ruolo fondamentale è svolto dal capitale umano e relazionale nello sviluppo di una *smart city*, città in cui la comunità ha imparato ad apprendere, adattarsi e innovare, con particolare attenzione all'inclusione sociale e alla compartecipazione dei cittadini alla pianificazione urbanistica e territoriale; come fondamentali sono le iniziative di carattere consultivo, come ad esempio la progettazione partecipata on-line, che dà occasione ai cittadini di percepire una reale democrazia in relazione alle decisioni che li coinvolgono;
- ambientale: ambito, questo, molto importante in un mondo dove le risorse scarseggiano e dove le città basano sempre più il loro sviluppo anche sulla disponibilità delle risorse turistiche e naturali, garantendo un uso sicuro e rinnovabile del patrimonio naturale,

specialmente con iniziative tese a ridurre le emissioni di sostanze;

- tecnologico: qui le possibilità sono innumerevoli in merito alle moderne tecnologie di cui può dotarsi una Smart City; consideriamo, ad esempio, tutte le reti di sensori e di strumenti di rilievo in grado di misurare diversi parametri per una gestione efficiente della città, con dati trasmessi in modalità *wireless e realtime* ai cittadini, oppure alle autorità pubbliche, mettendo in grado le amministrazioni, ad esempio, di ottimizzare le risorse energetiche, centralizzare l'illuminazione pubblica, monitorare la concentrazione di inquinamento cittadino, fino al rilevamento di falle nella rete idrica, come alla mappatura del rumore;
- mobilità: nella gestione del traffico e della mobilità urbana troviamo molti aspetti interessanti, quali ad esempio la possibilità di coordinare logicamente i cicli semaforici per il governo della circolazione veicolare, gestita in modalità dinamica, fornendo nel contempo agli utenti utili informazioni in tempo reale, ad esempio, per trovare rapidamente un parcheggio, facendo risparmiare tempo prezioso e carburante e, al contempo, contribuendo alla riduzione delle emissioni inquinanti;
- trasporto pubblico: vanno impiegati specifici sistemi di monitoraggio e di avviso, in *real time*, sulla infomobilità dei mezzi pubblici alle fermate; parallelamente andrà gestita in maniera funzionale la c.d. mobilità *lenta*, con una particolare attenzione alla fondamentale sicurezza (safety) dei pedoni, per esempio mediante l'implementazione di un *adeguate misure* per la mobilità ciclabile urbana.

Altra peculiarità di una SC è il ruolo giocato dalla sicurezza *safety-emergency*, perché assumono funzioni di assoluta importanza: predisporre efficaci **piani di emergenza** comunali, applicabili da un'efficiente organizzazione di protezione civile, rappresenta l'architettura del corretto piano di *resilienza* che ogni città dovrebbe possedere.

Un esempio concreto di utilizzo delle moderne tecnologie a supporto della sicurezza è quello dell'uso dei **sistemi APR** (droni) e della galassia dei **sensori IoT** utili all'analisi di eventi catastrofici come le alluvioni, le frane, gli incendi. Grazie a tale sensoristica, che condivide informazioni analizzate e interpretate da una sala operativa di comando, è possibile determinare *allerte preventive* che possano essere riscontrate e validate, poi, dai droni in interventi preventivi, analizzando lo scenario evolutivo di un evento emergenziale in corso in modo da consentire il dislocamento delle risorse dove più necessarie.

Ma all'aumentare dell'interazione con/tra gli *oggetti* IoT nel vivere quotidiano, **cresce anche il numero degli attacchi informatici verso queste nuove tecnologie**, cresciuti nel 2018 di ben quattro volte rispetto al 2017; a causa di questi malware i *sensori e i device* intelligenti IoT, all'apparenza utili e innocui, possono trasformarsi in un pericolo reale per il *cittadino connesso*, e non solo per la sua *privacy* e la sicurezza dei suoi dati (security), ma soprattutto per la sua sicurezza *fisica* (safety).

Perché accade questo? Perché gli *oggetti IoT*, banalmente, hanno **standard di sicurezza decisamente minimi**! Router, stampanti, termostati, l'intera galassia dei sensori smart - e oggi persino le lavatrici e i frigoriferi - sono interconnessi alla rete, motivo per il quale vengono sfruttati dai cyber criminali per portare a segno i loro attacchi.

L’**esempio finlandese** del novembre 2016 fa scuola, perché abbastanza emblematico: gli inquilini di alcuni edifici della città di Lappeenranta, sulle rive del lago Saimaa (a pochi km dal confine russo) rischiarono di morire assiderati all’interno delle loro stesse abitazioni per mano di un gruppo di hacker che, lanciando un attacco DDoS all’indirizzo del sistema centralizzato di riscaldamento, ne bloccarono il funzionamento, mettendo fuori uso le caldaie connesse in rete.

Questo ci fa capire come le SC, se non correttamente progettate e attentamente amministrate, possano diventare le *infrastrutture* insicure per eccellenza, esponendo al rischio di attacchi di cyber terrorismo la governance pubblica, perché **in una metropoli smart non sono connesse soltanto le apparecchiature private** dei singoli cittadini. Al contrario troviamo interconnesse diverse infrastrutture pubbliche, i c.d. *sistemi di governo intelligenti*: i trasporti, le centrali elettriche, le reti semaforiche, la PA, gli ospedali - tanto per citarne alcune - rappresentano infrastrutture che se violate creano seri danni o, peggio ancora, il caos.

La protezione delle SC, al pari della pubblica sicurezza, gioca un ruolo fondamentale nell’era dei servizi collettivi totalmente digitalizzati, integrati e utilizzabili su un'unica *piattaforma*.

Studi dell’ONU prevedono che la quasi totalità della popolazione mondiale in crescita nel prossimo decennio (entro il 2030) si concentrerà in **aree urbane**. Un dato, questo, che ci indirizza a una precisa considerazione: se da un lato le città stanno evolvendosi per diventare sempre più *intelligenti e interconnesse*, dall’altro l’aumento degli utenti che utilizzeranno i servizi pubblici può creare reali situazioni di rischio per la sicurezza; le aree urbane diventando **sempre più smart, dunque sempre più vulnerabili**, esposte agli attacchi cyber e/o ai malfunzionamenti indotti.

Nonostante tutto ciò, ad oggi non si è ancora concretizzato il pieno processo di trasformazione verso un modello di città completamente smart; e non solo per i sistemi non ancora interamente integrati e pienamente operativi, ma soprattutto perché la *sicurezza* e la *resilienza* delle infrastrutture dovrebbe andare al passo con l’interoperabilità e la sicurezza informatica.

Infatti, con il preponderante dominio dei *device* IoT, è **più che mai necessario associare all’aggettivo *smart* anche quello di *safe*** (safe inteso sia nell’accezione safety, per la sicurezza delle persone, in quella della security, per la sicurezza cyber), per una efficace **visione d’insieme** della governance utile ai processi di gestione dell’emergenza, che vede coinvolti i vari attori che vanno dalle forze di pubblica sicurezza fino ai gestori delle infrastrutture coinvolte nei processi ottenendo, così, azioni coordinate e supportate da tecnologie che permettano interoperabilità e interscambio di informazioni congiunte tra le varie forze.

Abbiamo visto sin qui come il tema delle *smart city* sia complesso ed articolato, per certi versi affascinante, certamente uno dei principali ambiti di ricerca futuri. Finanziamenti pubblici e bandi europei sono sempre più frequenti e consistenti, non dimentichiamo che il primo bando pubblico fu erogato nel 2012; per ottenere questi finanziamenti, però, occorre presentare progetti seri, concreti e fattibili.

Ma, soprattutto, utili a risolvere realmente i problemi delle città.

Riferimenti

- http://www.protezionecivile.gov.it
- http://www.ingegneri.info
- https://inta-aivn.org
- https://www.hexagonsafetyinfrastructure.com/it-it

Articolo a cura di **Giovanni Villarosa**