TAVOLA ROTONDA SIAP ANFP

L'INNOVAZIONE TECNOLOGICA AL SERVIZIO DELLA SICUREZZA NAZIONALE

ROMA, 16 APRILE 2019 - HOTEL QUIRINALE

Smart city è una formula entrata a pieno diritto nella narrazione contemporanea. La sua traduzione è ancora più suggestiva: Città intelligenti, prefigurando un futuro nel quale la connessione di tecnologia e capitale umano renda più sicuro e sostenibile l'ambiente in cui viviamo migliorando la vita dei cittadini, rendendo più accessibili i servizi, accrescendo il loro benessere e il consolidamento di una comunità coesa e serena.

Città intelligenti e sicure, deve voler dire che l'innovazione, la tecnica e il progresso scientifico devono costituire un corredo necessario, un valore aggiunto irrinunciabile all'attività di controllo del territorio che siamo chiamati a svolgere, a quella di ascolto dei bisogni dei cittadini, rappresentata dalla porta delle questure e dei commissariati sempre aperta, dalla responsabile disponibilità a mettersi al servizio senza mai dire: non ho la competenza per agire o per decidere, noi pensiamo che il poliziotto e l'istituzione Polizia di Stato devono sempre offrire una riposta alla domanda di aiuto dei cittadini, in nome di quel patto di fiducia che deve legare la gente alle forze dell'ordine.

Oggi la prevenzione delle nuove forme di crimine richiede un controllo sempre più capillare del territorio inteso non solo in senso fisico, cui si aggiungono le frequenti catastrofi naturali che affliggono il nostro paese, fenomeni di instabilità politica globale da cui scaturiscono nuove sfide e nuovi rischi, immigrazione incontrollata, terrorismo, imponendo sempre più l'esigenza di avere una maggiore capacità non solo di prevedere e prevenire ma soprattutto reagire tempestivamente alle potenziali situazioni di crisi. Nelle città, ma in tutta la nostra geografia nazionale la sicurezza è un bene primario alla base della coesione sociale, per questo devono essere considerate luoghi sicuri e tutelati, un obiettivo che deve coinvolgere attivamente i cittadini, ma soprattutto agevolare gli interventi delle Forze dell'Ordine, favorendo un approccio lungimirante da parte della pubblica amministrazione che superi la cultura dell'emergenza per quella della prevenzione, e che miri a un effettivo incremento della qualità della sicurezza, piuttosto che migliorarne semplicemente la percezione comune o il proliferare di norme e sanzioni, il panpenalismo e una patologia non la soluzione.

Da questo punto di vista è emblematico il caso del proliferare dei sistemi di videosorveglianza: per strade e case sicure non bastano le telecamere intelligenti se non sono interconnesse tra loro per convergere in una piattaforma operativa centralizzata e con sistemi di comunicazione protetti, se i dati registrati non sono analizzati e trasformati in informazioni da trattare in tempo reale. Da qui la necessità di ricondurre la sicurezza non tanto all'esplosione numerica delle telecamere installate, quanto alla loro integrazione, alla gestione e l'analisi delle immagini a favore di un impiego più efficace, come strumenti di prevenzione e di indagine sui reati commessi e introducendo una nuova capacità di identificazione e tracciabilità delle informazioni atte a favorire uno sviluppo sempre più virtuoso delle azioni di vigilanza.

La videosorveglianza oltre ad essere uno strumento vero e proprio per garantire la sicurezza della collettività, deve aiutare le persone a sentirsi più sicure a casa loro: secondo l'Osservatorio Internet of Things del Politecnico di Milano, in Italia, l'attenzione dei consumatori a questo tema aumenta se quasi il 50% dei proprietari di casa dichiara di essere intenzionato ad acquistare prodotti innovativi. Ma anche per proteggere le strutture e le infrastrutture più critiche, offrendo strumenti sempre aggiornati a supporto della pianificazione degli interventi immediati: a questo possono servire le telecamere di rete più moderne, promosse a veri e propri sensori hi-tech capaci non solo di catturare immagini ad una qualità superiore, ma anche di integrare al proprio interno degli algoritmi di analisi che oggi rappresentano un tassello fondamentale della moderna tecnologia che ha fatto di internet un sistema complesso e immenso, in grado di acquisire sempre più informazioni interpretabili con un orizzonte di comprensione contestuale più ampio che spazia dal miglioramento del flusso del traffico al sostegno dei servizi on-demand.

Grazie ai moderni smartphone e tablet tutti e sempre di più saranno in grado di interagire con le istituzioni fornendo informazioni preziose in tempo reale relative allo stato di sicurezza e alla gestione della città, dando modo alle amministrazioni locali e alle forze dell'ordine di estendere la loro rete di sensori in modo dinamico e distribuito a costo zero, decentralizzando i "cervelli" e riducendo il carico di lavoro dei sistemi centrali (compreso il traffico) con il vantaggio di essere informati in anticipo in merito a tutte le possibili allerte.

Si tratta soprattutto in materia di ordine pubblico di coniugare i concetti di safety intesa come l'insieme delle misure di sicurezza preventiva attinenti a dispositivi e misure strutturali a salvaguardia dell'incolumità delle persone, e la security che interessa i servizi di ordine e sicurezza pubblica " sul campo" in modo da dare la migliore attuazione possibile a un modello organizzativo e di governance che metta in luce e contrasti le vulnerabilità della piazza e degli operatori della sicurezza, come si è dimostrato in casi recenti, Torino è un esempio.

Altrettanto si può dire del centralino unico gestito da operatori che valutano chi deve essere allertato e che provvedono a contattare l'ambulanza, i vigili del fuoco oppure gli agenti in grado di arrivare prima, individuati attraverso la radiolocalizzazione, grazie a un sistema in grado di dimezzare i tempi d'attesa. O dei programmi di cablaggio che prevedono l'installazione di tablet, gps e altri elementi tecnologici sulle auto della polizia.

Fondamentale poi è l'applicazione diffusa dell'informatica alle azioni investigative: a questo tende il monitoraggio statistico dei reati**,** basato sulle schede informative che i funzionari redigono sul territorio e che devono spaziare dalla microcriminalità al sospetto di infiltrazioni mafiose, ai cambiamenti di ragione sociale sospetti, dalle analisi scientifiche nei furti, con la rilevazioni di impronte a quelle sulle schede telefoniche in grado di stabilire un nesso tra l'uso di una sim.

Informatica significa, anche nel settore della sicurezza, efficienza e riduzione delle procedure burocratiche, permette di sbrogliare più velocemente le pratiche liberando da incombenze il personale che può essere dirottato sule strade e nelle piazze.

È diventato un nostro slogan la convinzione che la sicurezza non è un costo, ma un investimento. Per questo è indispensabile che anche per l'applicazione e adozione dell'innovazione tecnologica al servizio della sicurezza vengano mobilitate risorse pubbliche da parte delle amministrazioni, per sostenere concretamente l'operato delle forze dell'ordine impegnate quotidianamente con un'azione insostituibile basata sull'ascolto, la responsabilità e l'affidabilità, cui la tecnologia può e deve aggiungere elementi di efficienza ed efficacia.

Si tratta di una mobilitazione necessaria anche a evitare che il valore aggiunto della tecnica contribuisca alla paventata privatizzazione della sicurezza, al primato dei sistemi e dei vigilantes in sostituzione dello Stato e dei suoi apparati: se come è normale le aziende di settore che investono maggiormente in ricerca e sviluppo tanto da rivendicare la propositività nel suggerire soluzioni sempre più sostenibili ed efficaci, se è vero che la sicurezza deve aspirare a applicare criteri e procedure di collaborazione interistituzionale e tra i vari soggetti in campo, altrettanto indispensabile è attribuirne allo Stato la intera gestione senza mediatori e interferenze. In modo che siano tutelate garanzie e diritti, da quelli della privacy a quelli della salvaguardia di cittadini e tutori della legge.

A questo fine però è necessario superare tutte le problematiche legate alla mancanza di connessione che spesso rappresentano uno dei principali limiti a un reale sviluppo di questo nuovo fronte della sicurezza e della lotta alla criminalità e al potenziamento dei sistemi di sicurezza già esistenti. Gli investimenti della pubblica amministrazione dovrebbero essere mirati ad un effettivo miglioramento della sicurezza anziché migliorarne semplicemente la percezione comune. Di contro i professionisti della sicurezza hanno un ruolo altrettanto importante che non può semplicemente limitarsi a quello di comparsa, poiché sono chiamati in prima linea col ruolo di autentici artefici del cambiamento. Sono proprio le aziende di settore che investono maggiormente in ricerca e sviluppo ad essere le maggiori candidate nel proporre e suggerire soluzioni ancor più sostenibili ed efficaci.

In questo millennio la sicurezza e la tecnologia, due concetti indissolubili il primo non può essere offerto al cittadino se le forze dell'ordine, oltre ad una presenza sul territorio non la utilizzano a piene mani in quanto la criminalità organizzata, che dispone di ingenti capitali, la usa in modo massivo.

Un tempo ad incastrare un killer c'erano solo le impronte digitali, oggi c'è il riconoscimento facciale. Esso è un software estremamente complesso che consente all'investigatore di confrontare anche un solo fotogramma con le foto segnaletiche presenti nel sistema per riconoscere il sospettato. Ma la nuova frontiera delle indagini è rappresentata dal teatro virtuale. Esso consente di osservare la scena del crimine da tutti i punti di vista offrendo agli investigatori una ricostruzione completa. Nella scena virtuale vengono inseriti gli elementi emersi nel sopralluogo della Polizia Scientifica, quindi utilizzando una serie di telecamere con un complesso software si ricostruiscono i movimenti delle vittime, dei criminali e dei testimoni essenziali per l'investigatore al fine di individuare i colpevoli dell'azione criminale.

Inoltre, occorre prendere coscienza che per la sicurezza del Paese è necessario armonizzare tra loro sia i sistemi sia di **sicurezza fisica** che **logica**.

Sicurezza fisica

È anche conosciuta come sicurezza passiva ed è un concetto abbastanza generale e si può intendere l'insieme di soluzioni il cui scopo è proteggere un luogo impedendone l'accesso alle persone non autorizzate.

Alcuni esempi di soluzioni per garantire la sicurezza fisica sono:

- Porte di accesso blindate;
- Sistemi di riconoscimento del personale;
- Sistemi di sorveglianza o controllo degli accessi;

Anche in questo settore tutto quello che veniva effettuato a "mano", riconoscimento del personale ora la tecnologia permette il riconoscimento in modo automatico con i dati biometrici (impronta digitale, iride, viso, dna, etc) in modo veloce e certo.

La semplice video sorveglianza in cui una poliziotto poteva controllare da una postazione remota tanti ingressi aumentando l'efficienza e l'incolumità personale oggi può essere fatta in modo automatico con sistemi sempre più evoluti che effettuano analisi della scena, riconoscimenti facciali, analisi comportamentali.

Sicurezza logica

La sicurezza logica serve a impedire l'accesso ai "luoghi digitali" (come server, database e computer) da parte di persone non autorizzate e questa è la nuova frontiera della sicurezza una sicurezza nata con l'avvento del mondo digitale quindi una sicurezza nuova degli ultimi anni in cui ancora non abbiamo una cultura

Un sistema che garantisce la sicurezza logica lavora in tre grandi fasi:

- Fase uno: autenticazione e autorizzazione dell'utente che vuole accedere al sistema (di solito, tramite login).
- Fase due: tracciamento, tramite file di log, di tutte le operazioni che quell'utente sta compiendo nel sistema (questa fase è anche conosciuta come audit o accountability).
- Fase tre protezione dei dati

Su questo ultimo tema la comunità Europea ha varato una normativa GPDR General Data Protecion Regulation che ha avuto un forte impatto sulla vita delle aziende e delle amministrazioni

In Italia nel 2018 sono spesi 1,19 miliardi di euro in sicurezza, prevalentemente (75%) dalle grandi imprese, che hanno varato progetti di adeguamento al Gdpr. Complessivamente il 23% delle imprese si è già adeguata, il 59% ha progetti in corso,

l'88% ha un budget dedicato. Il Data Protection Officer è presente in tre imprese su quattro e una su due ha inserito un Chief Information Security Officer.

Sono i dati salienti della ricerca dell'Osservatorio Information Security & Privacy della School of Management del Politecnico di Milano. E nascono attori innovativi che propongono soluzioni di information security & privacy: sono 417 le startup a livello internazionale, per un totale di 4,75 miliardi di dollari di investimenti raccolti solo su questo comparto.

Quale sarà lo scenario dei prossimi anni della sicurezza e a cosa verteranno gli attacchi cyber nel mondo industriale nei prossimi tre anni le aziende temono soprattutto spionaggio (55%), truffe (51%), influenza e manipolazione dell'opinione pubblica (49%), acquisizione del controllo di sistemi come impianti di produzione (40%). I principali obiettivi degli attacchi sono oggi account email (91%) e social (68%), seguiti dai portali e Commerce (57%) e dai siti web (52%). Nel prossimo triennio, le imprese prevedono che gli hacker si concentreranno su device mobili (57%), infrastrutture critiche come reti elettriche, idriche e di telecomunicazioni (49%), smart home & building (49%) e veicoli connessi (48%).

La principale vulnerabilità è costituita dal comportamento umano: per l'82% delle imprese la prima criticità è la distrazione e scarsa consapevolezza dei dipendenti, seguita da sistemi IT obsoleti o eterogenei (41%) e da aggiornamenti e patch non effettuati regolarmente (39%).

Questo è il punto di vista della vulnerabilità da parte dei sistemi fissi posti in edifici palazzi etc ma è necessari come accade in diversi paesi proliferano ormai iniziative volte sia per proteggere all'interno dei propri confini la infrastruttura critica di comunicazione e la comunicazione stessa, sia per proteggersi da ingerenze esterne considerando la perdita di controllo del proprio traffico dati, dai livelli più bassi a quelli più alti, un gravissimo problema per la sicurezza nazionale.

Va letto in questo contesto il recente conflitto Usa-Cina intorno all'uso di tecnologie 5G cinesi per infrastrutture occidentali (già del 2012 un rapporto del Congresso USA su possibili rischi di spionaggio cyber). Molti operatori stanno sperimentando il 5G avvalendosi di tecnologie cinesi.

Si dice che sia protezionistica la posizione americana per limitare la presenza di tecnologie cinesi. Ma già da tempo soprattutto i Paesi orientali stanno adottando **una politica estremamente protezionistica** che comporta un aumento esponenziale della funzione di controllo sul trasferimento e contenuto dei dati stessi la quale sembra travalicare, o addirittura non considerare, il limite della privacy in nome della sicurezza nazionale.

Considerando che lo spazio cibernetico (l'informatica, le reti a supporto, i dati, i dispositivi) consente a chi produce dispositivi e software di tenere nelle proprie mani le

redini del controllo degli stessi, le soluzioni "protezionistiche" intraprese da alcuni paesi sono state adottate proprio **per salvaguardare le proprie infrastrutture di comunicazione dagli** *hacker* **che potrebbero attentare all'integrità statuale sfruttando proprio le vulnerabilità della nuova rete**.

Più precisamente, volendo intervenire per una miglior gestione del livello di sicurezza necessario agli operatori per operare nel "territorio" del 5G, si è posto espressamente l'accento sulla **necessità di un controllo di queste nuove reti in ragione della sicurezza nazionale esprimendo preoccupazione sia per la intercettabilità abusiva di dati** durante il loro trasferimento sia per la relativa facilità di azioni di *hacking* che comporterebbero conseguenze a vari livelli sulla stabilità del sistema critico della comunicazione.

In conclusione, proprio incentrando la riflessione sul concetto della sicurezza, occorre rilevare che **l'avvento del 5G, in Italia e nel mondo, ha comportato un aumento del rischio** *cyber* **rispetto ai preesistenti sistemi di comunicazione** 4G **che già a loro volta non erano esenti da problematiche di sicurezza**[4]**.** Inoltre, sulla base delle considerazioni riportate, sembrerebbe che l'introduzione di una nuova tecnologia, seppur incredibilmente efficiente e performante, possa provocare criticità o effetti negativi di vario genere per i quali i risultati della sperimentazione in atto sul territorio nostrano sono forse ancora troppo embrionali per poter

Da quanto sopra il tema umano è il punto di partenza sotto molti punti di vista:

- Il piano occupazionale
- Il piano di formazione sia nel mondo civile che in quello delle forze dell'ordine
- Il piano della sicurezza del personale di polizia che utilizza anche telefoni personali

Occorre quindi una cultura della Cyber cultura che deve partire dalla formazione del personale a tutti livelli e guardando in termini politici pensare già ora a portare nelle scuole questa cultura

Essere leader in questo settore porta un incremento della occupazione elemento basilare per avere un paese sicuro in cui la stabilità sociale è assicurata con profili di crescita accettabili

Un tempo ad incastrare un killer c'erano solo le impronte digitali, oggi c'è il riconoscimento facciale. Esso è un software estremamente complesso che consente all'investigatore di confrontare anche un solo fotogramma con le foto segnaletiche presenti nel sistema per riconoscere il sospettato. Ma la nuova frontiera delle indagini è rappresentata dal teatro virtuale. Esso consente di osservare la scena del crimine da tutti i punti di vista offrendo agli investigatori una ricostruzione completa. Nella scena virtuale vengono inseriti gli elementi emersi nel sopralluogo della Polizia Scientifica, quindi utilizzando una serie di telecamere con un complesso software si ricostruiscono i

movimenti delle vittime, dei criminali e dei testimoni essenziali per l'investigatore al fine di individuare i colpevoli dell'azione criminale.