Come cambiano ruoli e strategie di sicurezza nell'era pandemica

Date : 10 Settembre 2020

È più facile spezzare un atomo che un pregiudizio
Albert Einstein

Già dal 2007 il World Economic Forum, all'interno del ***Global Risk Report***, iniziò a considerare, tra i **rischi emergenti**, il possibile pericolo generato da fattori pandemici; nella pubblicazione annuale del forum economico la diffusione massiva di malattie epidemiche veniva considerata, nel breve/medio termine, tra i primi dieci rischi per tipologia d'impatto, mentre come rischio sociale era classificato nei primi sei.

Peraltro, le previsioni degli analisti sullo scenario post Covid-19, sembrano indirizzate verso un forte aumento dei fenomeni criminogeni, come ad esempio gli attacchi terroristici NBCRe, i *cyber attacks* condotti sfruttando le deficienze di sicurezza delle reti, o i crescenti rischi *travel-related*, legati alle operazioni del personale fuori area.

L'emergenza sanitaria SARS-Cov-2 ha generato una crisi sistemica di straordinario impatto nazionale senza precedenti, per vastità del contagio e rapporto di letalità, estendendo rapidamente i suoi effetti malevoli in tutti gli ambiti strategici che compongono il nostro **Sistema Paese**.

Pur tuttavia, questa crisi sanitaria ha messo in risalto altri importanti aspetti: uno è quello rappresentato dai piani di *business continuity,* decisivi nel fronteggiare la fase inter-pandemica quanto fondamentali per tornare il più rapidamente alla normalità operativa, mentre l'aspetto ancora più rilevante sarà quello di superare il vecchio modello di Protezione Civile, che in questi quarant'anni molto ha dato e tanto ha fatto, trasformandolo definitivamente in un dipartimento di ***Homeland Security*** (HS).

Oltre a ciò, mentre il perimetro della sicurezza pubblico-privata, pre-Covid, era diviso principalmente tra gli ambiti ***safety* e *security***, in questa nuova emergenza nazionale ci siamo trovati, obiettivamente, davanti a una nuova minaccia che ha palesato tutta la nostra vulnerabilità: quella della **sicurezza sanitaria** ad impatto nazionale!

Una tipologia di rischio, quella della ***medical security*** , fino ad oggi considerata come un

settore secondario del complesso sistema sicurezza, ma superata l'emergenza Covid questa **dottrina** dovrà essere uno strumento di prevenzione – in interazione con la *medical intelligence* -, il nuovo paradigma che ridisegnerà gli schemi *safety/security,* con effetti di ampia portata in tutte le organizzazioni che dovranno garantire la sicurezza personale dei propri dipendenti (**TU 81/08**).

La sicurezza, ricordiamolo, è una funzione caratterizzata da una significativa trasversalità, in fatto di competenze e conoscenze, che solo una figura professionale come il *Security Manager* può avere; tra l'altro, rappresenta l'unica interfaccia nei rapporti tra le strutture pubbliche e quelle private, una chiave fondamentale nella gestione delle crisi, unica per *skill* e *know how*, indispensabile per impartire i corretti indirizzi nella gestione iniziale e post-incidente.

Dialogare con le prefetture, con gli uffici territoriali delle forze dell'ordine, con le strutture sanitarie e di Protezione Civile, scambiandosi informazioni di vitale importanza, è uno dei punti di forza tra le *soft skills* proprie del professionista della *security*, perché nelle **crisi sistemiche** servono reazioni rapide e lucidità decisionali; solo così si potranno impartire le giuste istruzioni alle altre funzioni verticali presenti in ogni organizzazione, come ad esempio amministratore delegato, CdA, responsabile della protezione e sicurezza (RSPP), medico competente, responsabile della protezione dati (DPO), manager di sistema ICT, CISO, etc.

Detto ciò, appare scontato come la *governance* di un'emergenza di simile portata vada assegnata a *manager* di elevata caratura, piuttosto che a singoli improvvisati o, peggio ancora, tentando di estrarli dal cilindro della politica, come accaduto ad esempio, nella creativa regione Veneto, dov'è nato un futuristico **Covid Manager** (!?).

Del resto, simili scelte politiche sono figlie del **mancato coinvolgimento degli esperti** della *security* pubblica e privata, della mancata sinergia che poteva mettere a punto efficaci strategie per interventi più efficienti, come non è stata certamente utilizzata al meglio tutta la tecnologia disponibile, se non in maniera randomica e con scarsi risultati.

Inoltre, l'estromissione degli esperti di settore - tenuti fuori dai tavoli tecnici per mero pregiudizio politico e sostituiti da figure politicizzate scarsamente competenti in *safety e security* -, ha creato un vero cortocircuito interno alla catena di gestione e comando delle infrastrutture che garantiscono l'essenziale continuità operativa dell'intera nazione.

Appare evidente come il professionista della *security* sia una figura centrale nella filiera della sicurezza; ed **è proprio nelle situazioni di crisi che questa professionalità fa la differenza**, organizzando pianificazioni interagenti a quelle delle FF.OO., interoperabili con quelle di Protezione Civile, fino ad arrivare ai piani di tutela degli *asset* strategici delle infrastrutture critiche.

Per farla breve: è stato evidente, ripercorrendo analiticamente l'emergenza della città di Codogno, lo scollamento tra il settore pubblico/privato, che identifica l'altro aspetto della crisi, quello della mancanza di una reale *partnership*!

La testimonianza di ciò è contenuta nel duro lavoro affrontato dalla prefettura nelle primissime

ore dall'istituzione della cd. zona rossa, investita da centinaia di richieste di autorizzazioni per la gestione della mobilità nell'area contaminata; questione che la dice lunga sulla mancata cooperazione informativa/operativa tra istituzioni e aziende... e non stiamo parlando di piccole organizzazioni, ma piuttosto di quelle che erogano servizi pubblici di primaria necessità!

Infatti, nella crisi emergenziale da Covid-19 si è scoperto che poi, tutto sommato, non ci sono tutti questi piani codificati di *business continuity* e *disaster recovey* condivisi istituzionalmente – almeno nella conoscenza della prefettura - ma solo strategie pianificate all'interno delle singole **unità di crisi**, con informazioni scarsamente condivise, quando non tenute volutamente riservate.

Perché? Qual è il motivo, se mai ve ne fosse uno, per il quale non si attivano ancora i protocolli di *cooperation* nei settori strategici, a tutto vantaggio della sicurezza nazionale?

Ebbene, in una situazione drammatica come la pandemia da Coronavirus, caratterizzata dall'assenza di precedenti riferimenti sui quali misurarsi e confrontarsi, se non si crea una robusta, proattiva e interdipendente *partnership*, si corre il pericolo di aumentarne esponenzialmente le criticità, piuttosto che contrastarle!

Peraltro, eravamo tutti fiduciosi che gli insegnamenti ricevuti, purtroppo, dalla drammatica crisi americana *nine-eleven* concentrassero di più l'attenzione sulla corretta gestione delle emergenze, ponendo maggiormente l'accento sulle **capacità resilienti** di ogni organizzazione, ma soprattutto, che si studiasse finalmente la creazione di un dipartimento di *Homeland Security* nazionale.

Come visto, l'epidemia ha generato una serie di nuovi rischi su cui i *Security Manager* dovranno lavorare, trovandosi di punto in bianco - per via del *remote/smart working* - con i perimetri aziendali allargati e le relative superfici di attacco ampliate e fortemente esposte: problematiche che andranno gestite ben oltre il periodo *post-lockdown*.

Difficoltà queste, che hanno dato una maggiore enfasi proprio sulla sicurezza fisica, spingendo i professionisti della *security* a dedicare un'attenzione più centrale alla tematica, sviluppando precise *policy* aziendali di sicurezza armonizzate alle disposizioni dei DPCM, indicazioni che spingeranno il futuro della sicurezza a una definitiva **convergenza** tra il perimetro fisico e quello logico - in termini di sicurezza degli spazi, degli accessi, delle informazioni e dei dati personali - nei luoghi di lavoro.

E a questo punto dobbiamo porci una domanda: quale sarà il ruolo futuro del *Security Manager* all'interno delle infrastrutture strategiche del Paese?
Su questo interrogativo ho più volte espresso il mio pensiero - dettato anche dell'esperienza consolidata in questi anni come commissario d'esame per le certificazioni UNI 10459 e UNI 11697 - e, senza dubbio, il post Coronavirus aprirà **scenari** nuovi che imporranno di riscrivere tutte le misure di sicurezza.

Viviamo un cambiamento epocale nell'esposizione al *cyber risk,* in uno scenario radicalmente diverso, fatto di un uso promiscuo di dispositivi aziendali e personali connessi alla rete, che

imporranno un ripensamento di tutte le politiche legate alla sicurezza.

Durante il *lockdown,* ad esempio, il *cyber crime* ha interessato il settore sanitario con pericolose incursioni e operazioni di spionaggio dati, pesanti attacchi informatici contro le organizzazioni sanitarie.

Perciò, a valle della pandemia, tanto i settori pubblici quanto quelli privati mostreranno le stesse problematiche nei propri dipartimenti di *security*, che potranno essere affrontate solo da professionalità **verticali e trasversali**, certamente diverse da quelle del periodo pre-Covid-19; tanto è vero che sarà proprio la figura del *security manager* a necessitare di competenze ancor più ampie ed eterogenee, perché mai come in questa emergenza la *governance* della sicurezza - nelle sue componenti di *security, safety, emergency* - si è dimostrata cruciale per la tenuta dell'intero Sistema Paese.

Sarà importante disporre di persone con esperienze professionali e competenze accademiche fortemente trasversali, integrate da specifici percorsi post laurea che spazino dalla *cyber security* alla *travel security*, dalla *medical security* alla *medical intelligence,* per citarne alcuni; ma questi saranno solo taluni degli aspetti che i *manager* post-crisi dovranno saper affrontare.

In ultimo, poi, credo sarà necessario anche un aggiornamento in chiave *light* della norma UNI 10459:2017 che andrà caratterizzata, nel percorso della certificazione personale, con talune peculiarità, come ad esempio un *role play* in sede orale che esalti le reali capacità manageriali del professionista.

Articolo a cura di **Giovanni Villarosa**