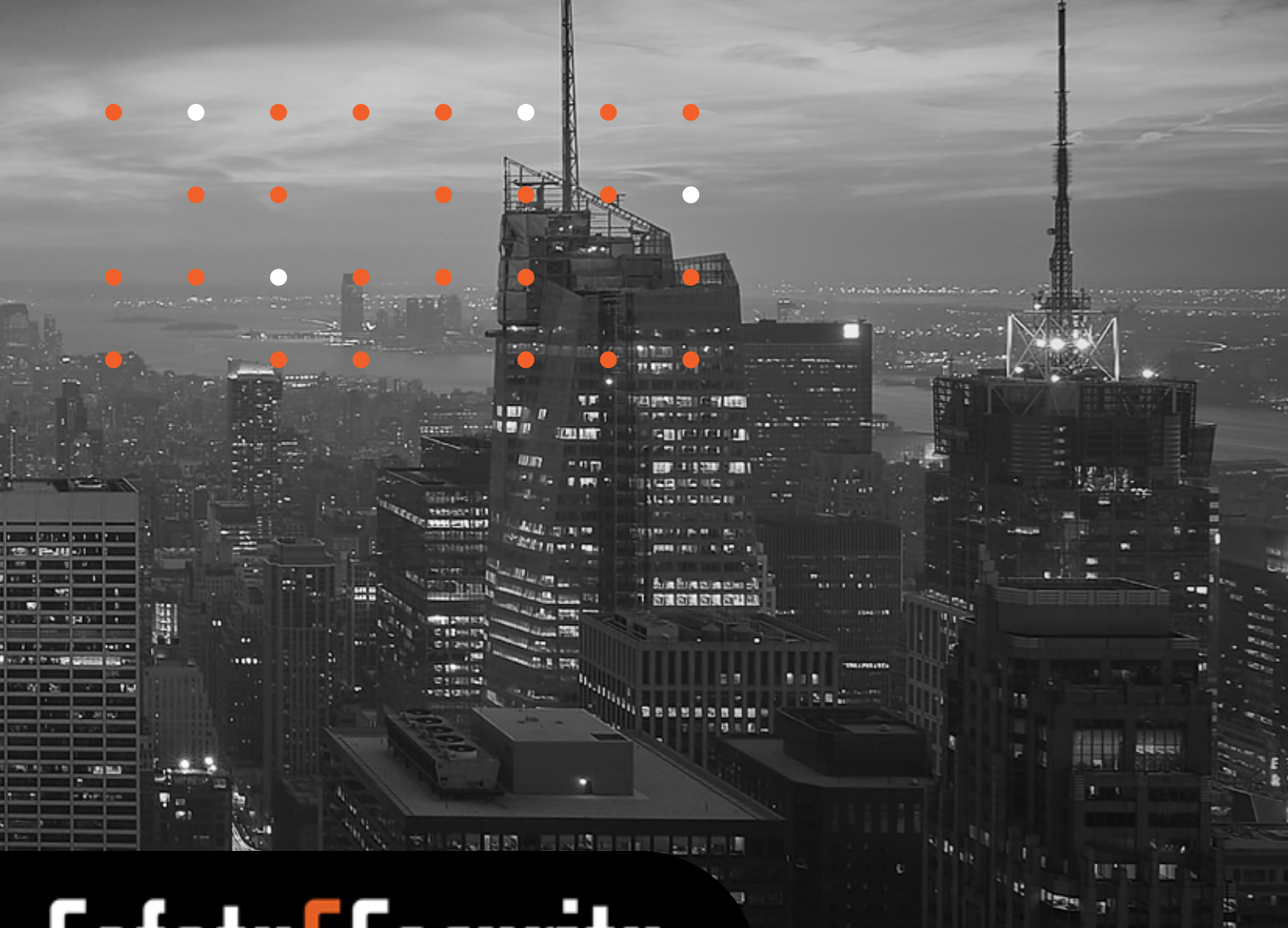




Safety & Security

WHITEPAPER 06/2022

Safety & Security Manager

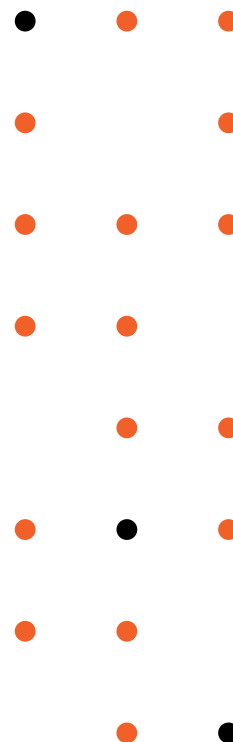
Consigli e aggiornamenti per il
Security Management aziendale

Giovanni Villarosa, *Senior Security Manager*

Safety & Security

www.safetysecuritymagazine.com

Capitoli



04

Convergenza tra Safety & Sicurezza Fisica, Logica e Organizzativa

12

Security Manager e DPO, due figure nate dalla necessità di una maggiore sicurezza aziendale

19

La normativa per la sicurezza e la tutela del patrimonio aziendale

30

Sicurezza dei sistemi aziendali

34

Come cambiano ruoli e strategie di sicurezza nell'era pandemica

39

Travel Security Management – Sicurezza delle trasferte all'estero

44

Medical Security: nuove sfide di sicurezza a fronte di nuove minacce globali

49

L'utilizzo dei Social Network nelle comunicazioni di emergenza

Safety & Security Magazine

L'obiettivo di **Safety & Security** - da **oltre 15 anni** - é quello di fornire uno scenario aggiornato del contesto competitivo del settore della **Sicurezza Fisica** e della **Sicurezza Logica** in Italia, diventando la voce delle istituzioni e dei principali attori operanti nel settore e fornendo una vetrina del mercato nel suo complesso.

Quotidiano online aggiornato con le ultime novità del settore e con approfondimenti mirati a fornire al lettore nuovi spunti e linee guida per migliorare ed ampliare il proprio punto di vista rimanendo al passo con la continua innovazione.

About the Author

Giovanni Villarosa, *Senior Security Manager*

Laureato in scienze dell'intelligence, difesa e sicurezza.

Master in STE-SDI, master in DPO e Privacy expert. Esperto di sicurezza e protezione fisica, gestione della security, intelligence CBRNe, per infrastrutture critiche. Senior security manager UNI 10459 e DPO UNI 11697. Commissario e deliberante per gli schemi di certificazione UNI 10459 e UNI 11697. Docente volontario presso i centri formazioni salesiani "Don Bosco" di Roma. Socio e membro del comitato tecnico scientifico del CESPIS.



Convergenza tra Safety & Sicurezza Fisica, Logica e Organizzativa

Quando mi è stato proposto di scrivere questa riflessione, del tutto personale, sulla convergenza tra la Security e la Safety, mi sono tornati in mente i diversi insegnamenti acquisiti in questi anni professionali passati nel comparto della sicurezza. L'esperienza vissuta sul campo, gli errori, gli studi, i progetti, la partecipazione ai convegni, seminari, workshop, lo scambio di informazioni e di idee sull'argomento, mi hanno portato, nel tempo, alla considerazione finale (oggi come allora giusta o sbagliata che sia), sempre più marcata: **la Security e la Safety devono obbligatoriamente viaggiare per mano!**

In un convegno di qualche anno fa, presso il dipartimento di ingegneria di Roma Tre, sulla **"convergenza tra safety e sicurezza fisica, logica e organizzativa"**, promosso dalla associazione AIIC e capitanata dalla presidente Ing. Luisa Franchina, il relatore della giornata, il Dr Claudio Pantaleo, amico e preparato professionista della security, analizzava magistralmente tutti i punti fondanti dell'argomento, chiarendo, laddove ancora ve ne fosse il bisogno, come i perimetri safety e security non debbano stare più disuniti, ma punti cardini dell'intero processo sistemistico della sicurezza, per il semplicissimo fatto che questi due ambiti rappresentano le due identiche facce della stessa medaglia!

A livello accademico, poi, le cose non cambiano granché; accade molto di rado che il mondo universitario, decisamente più teorico, sia in perfetta sintonia con il mondo professionale, ambito molto pragmatico e operativo sul campo; decisamente meno teorizzato, ma più pratico nelle applicazioni, con punti di osservazioni sì diversi, ma convergenti. Durante l'anno passato al DIE di Roma 2, frequentando il master di II livello STE-SDI (sistemi e tecnologie elettroniche per la sicurezza, difesa e intelligence) abbiamo appreso, nel corso delle lezioni, come diversi insegnamenti facevano riferimento proprio alla convergenza e alla **compenetrazione delle dinamiche di security e di safety, in materia di sicurezza infrastrutturale**.

Il nostro docente, Prof. Roberto Mugavero (mio mentore, uno dei massimi esperti italiani sulla CBRNe intelligence), durante le lezioni sugli scenari applicativi per le tecnologie di difesa militare, difesa e protezione civile, i metodi e le tecnologie di prevenzione e identificazione per la difesa militare, gli attacchi, gli incidenti e le protezioni da eventi CBRNe, metteva sempre in risalto come questa convergenza, tra gli ambiti, fosse il prodotto risultante di una sola fenomenologia. Lo stesso accadeva durante le lezioni di *operation management* per scenari di rischio, del Prof. Caramia: security e safety venivano analizzate in stretta coppia.

Possiamo tranquillamente affermare che la sicurezza rappresenta un sentimento, oltre che un dato di fatto: uno **"stato d'animo"** ormai percepito come prioritario dalla quasi totalità delle imprese e delle organizzazioni pubbliche dei Paesi industrializzati, e alla sua soluzione vengono dedicate attenzione e corpose risorse, sempre più crescenti, anche se con un certo ritardo.

E poiché, più in generale, il senso di sicurezza resta, peraltro, un sentimento oggettivo e molto soggettivo, è bene sempre analizzare le reali ed effettive esigenze di protezione; è proprio partendo da questo assunto "basico" che vanno sviluppati quei concetti di protezione infrastrutturale di tipo globale, che tengano conto di tutti gli elementi rilevanti ai fini della sicurezza generale: una visione d'insieme completa, una analisi ottimale, la massima sicurezza decisionale!

Ma qual è il significato effettivo, reale del sostantivo "sicurezza"?

Nella lingua italiana generalmente viene definita come:

"la condizione di ciò che è sicuro, di ciò che consente di prevenire o attenuare quei rischi tipici che si presentano quando una minaccia sfrutta una vulnerabilità, per un fine ultimo di cagionare un danno".

Ora, questa condizione “ideale” si manifesta solo nei casi di assenza del pericolo, cosa certa in senso assoluto, ma difficilmente realizzabile in condizioni “reali”. Invero, l'applicazione delle cd norme di sicurezza rende, generalmente, più difficile il verificarsi di eventi dannosi e di incidenti, quindi la talcosa avvicina molto l'indice reale a quello ideale, ma certamente non lo pareggerà mai in nessun caso!

Eppure, analizzandolo più profondamente, questo concetto appare ancora piuttosto ambiguo; infatti, nella etimologia della lingua inglese esistono tre diversi termini che la declinano, tipicamente anglosassoni, che meglio la ridefiniscono in ulteriori, se vogliamo, “sostantivi”:

- **Safety**, quale sicurezza di protezione delle risorse umane (incolumità della persona) e delle risorse materiali, da pericoli derivanti da fenomeni naturali, accidentali o da errori umani;
- **Security**, quale sicurezza di protezione delle risorse umane, delle risorse materiali e immateriali, da eventi di natura prevalentemente dolosa o colposa; tutto ciò altro non è che cultura, studio e gestione della sicurezza per la concretizzazione di misure idonee (materiali, infrastrutturali, formative e informative) per la prevenzione.
- **Emergency**, quale attività di soccorso e di sicurezza personale e sociale che devono essere messe in atto nei casi in cui i compiti svolti dalla security e safety non siano sufficienti; l'emergency riguarda quindi il perimetro della protezione e del contenimento del pericolo.

Strutture istituzionali che operano nel mondo della sicurezza in maniera “**convergente**” e “**sinergica**”, a dimostrazione delle tre declinazioni citate, le ritroviamo, ad esempio, tra le forze dell'ordine (security), i vigili del fuoco (safety), il soccorso sanitario (emergency), la protezione civile e la difesa civile (security, safety, emergency), oltre agli istituti di vigilanza privata (safety e security), organismi adibiti a titolo “ausiliario e sussidiario” (sicurezza interna e sicurezza sussidiaria) funzionali nell'ambito di strutture organizzate e areali.

Negli ambiti generali della sicurezza fisica/logica e safety, sia essa aziendale che istituzionale, il concetto della “**convergenza**” di questi perimetri, è sempre più stringente e convergente tra loro; in alcuni casi, tra le altre cose, questa convergenza

risulta pressoché impercettibile, ad esempio: un sistema di videosorveglianza non serve solo a tutelare il patrimonio, ma può salvare la vita di una persona in difficoltà, e non rappresenta uno strumento di controllo del dipendente, ma piuttosto può garantirlo in caso di gravi emergenze aziendali!

Due binomi, quello fisico & logico e di security & safety, che generalmente viaggiano paralleli, proporzionali, senza mai apparentemente “incontrarsi”. Nei postulati matematici, due rette parallele hanno una sola possibilità di intersecarsi, all’infinito; mentre matematicamente questa astrazione euclidea è abbastanza articolata da dimostrare, nel mondo della sicurezza la realtà è molto meno astrattiva e più tangibile, reale.

Un esempio, ne è la minaccia cyber, la così detta minaccia “logica”: **Stuxnet** nel novembre 2008 è la dimostrazione tecnologica tangibile; un attacco materializzato contro un sito nucleare sotto forma di worm informatico, sfruttando una vulnerabilità di windows, in grado di spiare e riprogrammare pc e plc industriali, componenti cardini dei sistemi SCADA. Da ciò, ben si comprende quale reale pericolo rivesta una simile minaccia esterna (ambiti security e safety), nella filiera di una sequenza produttiva industriale: cosa accadrebbe, ad esempio, se durante una produzione farmaceutica, nella sequenza di un processamento chimico si inserisse un simile *bug* che modifichi quantità e sostanze di un medicinale, o molto più pericolosamente, sostituisse i farmaci prodotti da una confezione ad un’altra farmacologicamente diversa?

Altro esempio e altra minaccia da non sottovalutare, per i devastanti effetti di presa psicologica sulla nostra società, è rappresentata dagli attacchi terroristici, la così detta minaccia “**fisica**”, diretta e materiale, contro le infrastrutture che governano e regolano il vivere quotidiano, la nostra stessa vita: l’attacco terroristico alle torri gemelle del **World Trade Center** ne sono la vivente testimonianza e hanno fatto scuola, purtroppo! E qui la sicurezza fisica gioca un ruolo decisamente fondamentale: rappresenta l’insieme di misure che prevengono e dissuadono gli attaccanti dall’accedere a una infrastruttura, a una risorsa o alle informazioni; rappresenta le linee guida su come progettare strutture in grado di resistere ad attacchi, ad atti ostili, perché il fine della protezione fisica è quello di proteggere gli asset, tangibili e intangibili, da eventi di tipo criminogeno. E qui va fatto un piccolo inciso, squisitamente analitico, utile alla progettazione: ricordiamoci sempre, che non si chiude l’anello del processo di security fisica, se non c’è l’esatta “sommatoria” tra una

protezione tipicamente attiva (tecnologie elettroniche) integrata a quella tipicamente passiva (tecnologie meccaniche).

Come visto, dunque, i due casi realmente accaduti e citati ad esempio, pongono in maniera netta problemi delicatamente legati alla security e alla safety, tanto delle infrastrutture quanto dell'incolumità della vita umana. Da ciò si comprende bene come la sicurezza, nel suo insieme **multidisciplinare**, deve essere implementata da processi strutturati che permettano di proteggere il patrimonio aziendale, prevedendo, progettando, e realizzando poi, tutte quelle necessarie misure convergenti di sicurezza logica e fisica dedicate, che raggiungano come obiettivo finale un solido modello di **governance**: controllo accessi, sistemi di protezione antintrusione integrati con videosorveglianza performante, rappresentano insieme a efficaci firewall e ad una robusta crittografia, l'equazione vincente in tema di cooperazione tra security fisica e logica, a tutto vantaggio di questa auspicata convergenza!

Nelle cd infrastrutture critiche, la protezione generale (informazioni, funzionalità, patrimonio, etc) non prescinde mai dalla protezione fisica, ne tantomeno da quella logica; oggi, infatti, la complessità infrastrutturale quanto funzionale dei sistemi di sicurezza fisica costituisce, a sua volta, un potenziale oggetto di attacco esterno tipicamente cyber, alla stregua di qualsiasi altro sistema o servizio di *information technology*; dall'altro lato, la sicurezza fisica diventa un fattore fondante, quanto importante, per realizzare un sistema di protezione infrastrutturale IT completo: la necessità di proteggere strutture che trattano informazioni (o patrimoni) definite critiche e non solo con un insieme di misure di sicurezza logica, ma anche e soprattutto, garantendo che accessi fisici non autorizzati possano compromettere la sicurezza della stessa infrastruttura

Ebbene, come abbiamo detto, poter stabilire il confine di un attacco logico da quello fisico, per certi versi non è sempre facile. Analizziamo allora questo danno derivante dalla compromissione contemporanea di più sistemi di sicurezza intesa come protezione di security e focalizziamo mentalmente tre tipici scenari che potrebbero materializzarsi.

Facciamo degli esempi: un attacco, interno o esterno che sia, compromette il funzionamento dell'intero sistema di protezione antintrusione, bloccando, ad esempio: la sensoristica di rilevazione degli allarmi, gli apparati di segnalazione remota che allertino le ff.oo e/o gli uomini della security interna, tutte le contromisure

elettroniche e meccaniche tipiche e governate dall'antintrusione, come il blocco fisico degli accessi (ingressi, uscite, compartimentazioni antincendio) di determinate aree protette, aree classificate, tutto ciò pone un serio e delicato problema prettamente attinente al perimetro safety, prima ancora che fisico o logico.

Altro esempio molto semplice: poniamo il caso che ad essere sotto attacco sia il solo sistema di videosorveglianza; una cosa molto frequente, più di quanto si pensi, visto che il settore si sta indirizzando sempre più verso sistemi implementati su piattaforme IP video, molto performanti e più facilmente scalabili, di gran moda, ma fortemente esposte a possibili forme di hackeraggio sistematico; attacchi mirati che potrebbero rendere "cieche" un gran numero di telecamere dell'impianto per indurre danni ad asset critici, crearsi dei varchi senza essere visti, o peggio ancora, attacchi dedicati per sabotare le memorie degli archivi video, cancellando quelle prove video fonte di evidenza di crimini commessi.

E ancora, una tipica problematica di un controllo degli accessi: si potrebbero bloccare le disponibilità di uso dello stesso modificando i profili autorizzativi per gli ingressi, le uscite, bloccando aree riservate, negando l'accesso a chi è autorizzato, oppure, autorizzando l'ingresso a chi non ne ha diritto, consentendo l'accesso ai locali CED, contenenti dati sensibili, il patrimonio informativo aziendale, tutti dati e informazioni che potrebbero essere sottratti o distrutti.

Immaginiamo il danno creato, non solo quello reputazionale, dalla sottrazione di determinate "informazioni": a quali pericoli fisici e di incolumità personale verrà esposto tutto il personale interessato dai dati? Qui si pone un delicato problema di **safety**, perché si mette a rischio la vita personale di determinate figure aziendali; ben sappiamo che mettere in pericolo il patrimonio aziendale "**umano**" significa esporre al rischio l'intera integrità strutturale (azienda o istituzione che sia) e la sua stessa sopravvivenza!

Ma si pone anche un altro grosso problema, legato al perimetro della **privacy**; si potrebbero fare i conti in sede civile e penale per aver violato le minime misure di sicurezza previste dall'allegato B del D.Lgs 196/2003, non avendo previsto, o peggio ancora mal progettato, un adeguato sistema di protezione dei dati; questo vuol dire anche non aver previsto intorno allo stesso tavolo gli attori principali della governante della sicurezza: Security Manager, Security Officer, RSPP, e il Responsabile della protezione dei dati (manager cd Data Protection Officer, obbligatorio a livello UE, per

certe infrastrutture, da maggio 2018).

In conclusione, riassumendo. Fino ad oggi, il “parlare” si è concentrato sul miglioramento della tecnologia di sicurezza informatica e dei processi di risposta all’attacco hacking, alle violazioni della sicurezza IT: la cd risposta alla **cyber security**. Di contro, tuttavia, c’è stata scarsa attenzione ad un quadro decisamente più ampio; le aziende dovrebbero adottare, definitivamente, un approccio unificato e paritario sia per la sicurezza fisica che logica. Il risultato sarà certamente più strutturato, omogeneo, proprio nella direzione imposta dalle regole safety.

Le aziende sistematicamente dedicano molte risorse, direi in modo sbilanciato, per unificare le operazioni logiche a quelle fisiche; nella moltitudine dei casi con scarsi risultati, o meglio, con risultati decisamente al di sotto delle aspettative poste, tra gli investimenti messi in gioco e le risultanze ottenute. Altro esempio tipico e sovrapponibile tanto al privato quanto al pubblico: il personale di una infrastruttura aziendale o istituzionale che sovrintende le operazioni fisiche tipiche, come aree di sicurezza, le credenziali per il personale, la manutenzione degli impianti, elettrici e tecnologici, molto spesso è “**separato e scollegato**” dai responsabili delle operazioni IT, dal personale safety. Security Manager, Security Information Officer e RSPP, e in futuro il Data Protection Officer, che non “operano” dallo stesso tavolo, che parlano “linguaggi” diversi, o peggio ancora, dipendono gerarchicamente da strutture aziendali differenti, per assetto e formazione.

Mentre il personale responsabile di simili e delicati processi, dovrebbe avere un unico punto di contatto e di convergenza, perché tutti ben sappiamo che gli attacchi fisici hanno sempre un impatto devastante sulle operazioni IT, come le minacce logiche impattano sempre sulle operazioni fisiche; risulta chiaro che trattare separatamente i due perimetri di minaccia, allontanando la convergenza, produrrà in termini di risposta una inutile confusione, dei ritardi e delle inefficienze inaccettabili quanto pericolose quando una crisi colpisce gli asset strategici.

E questo, soprattutto in considerazione del fatto che le fasi di contrasto per affrontare i problemi di sicurezza (security, safety, emergency) ormai seguono processi molto simili e assimilabili: il rilevamento della minaccia, la valutazione, il contenimento, il rimedio, la rimozione e la risoluzione finale.

Per creare un approccio unificato, necessario ad ospitare questo trend di convergenza, va pensato e creato un punto centrale di gestione e coordinamento

adeguato nel rispondere alle interruzioni delle operatività, causate dalle problematiche fin qui analizzate. Un elemento chiave che consentirebbe risposte rapide e unitarie, potrebbe essere la realizzazione di una rete di comunicazione delle “**crisi**” di nuova generazione: una piattaforma creata per avvisare il personale e facilitare in maniera adeguata lo scambio di informazioni su scala massiva, o su base mirata; se un rilevatore di fumo in una sala server genera un allarme incendio, questa informazione genera certamente un alert dalla triplice valenza: security, safety ed emergency. Avere a disposizione delle immagini di un impianto strettamente legato alla security e correlarle con i dati di allarme incendio generati da un sistema strettamente legato al modo safety rappresenta la concreta convergenza di questi due mondi aziendali, la cui distanza, non fa altro che porre il sistema azienda nella totale **insicurezza** operativa.

Essere in grado di rispondere in maniera adeguata e sicura, rappresenta la necessaria resilienza che ogni infrastruttura, pubblica, privata o critica, deve possedere come patrimonio genetico in risposta ad ogni tipo di minaccia, interna o esterna che sia!

I link proposti danno un contributo riflessivo ed a più ampio spettro sulla sicurezza in generale (security e safety), mettendo in risalto quella delle infrastrutture critiche, tanto pubbliche quanto private, oggetti di attacchi anche di tipologia cd **non convenzionale**.

- [http://gnosis.aisi.gov.it/Gnosis/Rivista48.nsf/ServNavig/48-25.pdf/\\$File/48-25.pdf?openElement](http://gnosis.aisi.gov.it/Gnosis/Rivista48.nsf/ServNavig/48-25.pdf/$File/48-25.pdf?openElement)
- [http://gnosis.aisi.gov.it/Gnosis/Rivista48.nsf/ServNavig/48-23.pdf/\\$File/48-23.pdf?openElement](http://gnosis.aisi.gov.it/Gnosis/Rivista48.nsf/ServNavig/48-23.pdf/$File/48-23.pdf?openElement)
- <http://www.masterstesdi.uniroma2.it/home.html>



Security Manager e DPO, due figure nate dalla necessità di una maggiore sicurezza aziendale

Nella moderna società è maturato un profondo processo di cambiamento della realtà sociale, economica, culturale e politica; il mutato contesto è diventato sempre più incerto e difficile da comprendere, rispetto a logiche passate, infatti osserviamo, su scala universale, come il fenomeno della globalizzazione abbia portato ad una decisa separazione del legame causa/effetto, testimoniato dal fatto che, molto spesso, non riusciamo a comprenderne le fonti.

Peraltro rispetto al passato, dove questi fattori potevano essere ragionevolmente analizzati, nell'attuale scenario sociale un avvenimento dipende da molteplici cause, ricadendo in ambiti disuguali tra loro, ma in qualche modo interconnessi; tutto ciò rende molto più complicato sia comprendere che valutare, da parte dei professionisti della sicurezza, gli effetti delle possibili ripercussioni nei settori della **security**, **safety** e **data protection**, declinazioni specifiche dell'area sicurezza nel suo insieme, ovvero, di quella incertezza che innalzerà in maniera esponenziale la percezione dell'essere esposti ai pericoli, aumentandone contemporaneamente la realtà del rischio stesso.

Già trenta anni fa, Ulrich Beck (1986), nel suo libro "La Società del Rischio" (Carrocci editore, 2000), poneva una questione tangibile:

“viviamo in una società mondiale del rischio”.

Beck fissava una netta distinzione fra una prima e una seconda modernità, descrivendone le conseguenze, e i rischi correlati, analizzando nel contempo le possibili minacce alla nostra realtà sociale, economica, politica; tutto ciò è ancor più vero osservando le difficoltà fronteggiate per analizzare e individuare con logicità, il rapporto che lega il binomio causa/effetto contenuto nel fattore rischio.

L'incertezza rappresenta da sempre una costante che caratterizza il genere umano, e si esprime con il non sapere, con il non riuscire a prevedere, e quindi a prevenire, accadimenti che possono ingenerare forme di pericolo; potrebbe apparire come una banalità, ma **l'incertezza produce insicurezza**.

Ora, tale necessità di creare un quadro di sicurezza in un ambiente perennemente sottoposto all'incertezza ha spinto le aziende alla istituzione di funzioni organizzate in area security (fisica, logica, protezione dati), che traslassero una tipica mentalità concettualmente reattiva, in azioni tipicamente proattive, necessità questa, imperniata al raggiungimento della giusta **capacità resiliente**.

Questo accade perché nell'ultimo decennio abbiamo assistito a una rapida evoluzione del concetto di sicurezza aziendale, al mutare della percezione del rischio all'interno delle organizzazioni globalizzate.

Sappiamo bene come senza una concreta politica della sicurezza, e in assenza di un quadro tattico, non esiste nessuna garanzia di protezione, intesa come disegno strategico globale! **La sicurezza del patrimonio aziendale è un fattore sempre più critico per imprese ed enti pubblici**, costantemente impegnate ad agire su più fronti del problema: tecnologico, organizzativo e formativo; parallelamente, la tutela del patrimonio informativo, al pari di quello aziendale, si occuperà delle misure per fronteggiare le minacce, tese a costruire uno schema di governance funzionale alla compliance diretta ai processi ICT e nel trattamento dei dati e delle informazioni.

Ciò significa che nella identificazione delle aree critiche, la gestione dei rischi nei sistemi, nella rete, delle vulnerabilità, degli incidenti, il controllo degli accessi, la protezione fisica, la gestione del trattamento dei dati, la misurazione dei danni, etc, rappresentano tematiche comuni a due ambiti aziendali ben distinti, ma contigui.

Tematiche queste, che meglio rappresentano le due facce della stessa medaglia, diventate di estrema attualità, al punto tale che diverse grandi organizzazioni (private e pubbliche) hanno deciso di inserire all'interno del proprio organigramma specifiche risorse umane, funzionali alla delicata gestione del **security management** (frodi, furti, perdita dati, etc), e che nella sua complessità richiede due figure professionali dall'elevato profilo e un background consolidato: un **manager della sicurezza aziendale** e un **manager della protezione dei dati**, specialità apparentemente disomogenee, ma con obiettivi comuni, fortemente convergenti.

L'attuale assetto normativo prevede all'interno di strutture organizzate complesse diverse figure professionali (alcune su base volontaria, talune rese obbligatorie) per consentire lo svolgimento di diversificate attività legate all'area sicurezza. Il Security Manager (SM previsto su base volontaria, in tre profili normati dalla UNI 10459:2017, ma imposti dalla UNI 10891:2000 e dal DM 269/2010 per gli IVP, istituti di vigilanza privata), il Responsabile del Servizio di Protezione e Prevenzione (RSPP D.Lgs 81/2008 obbligatorio), il Responsabile della Protezione dei Dati (RPD o DPO, GDPR UE 2016/679 obbligatorio, e normato dalla UNI 11697/2017).

Come visto, dunque, nei moderni contesti organizzati la Corporate Security assume una rilevanza strategica: i recenti fenomeni di terrorismo (primavera arabe), la criminalità organizzata e transnazionale, il bisogno di inviare i propri dipendenti in missione, o temporaneamente distaccati fuori confine (travel security e data protection fuori area), necessità questa, dettata sempre di più dalla crescente interconnessione dovuta alla globalizzazione economica, e data la trasversalità della minaccia, tutto ciò si riflette positivamente anche nell'ambito delle infrastrutture pubbliche.

La *travel security* è una policy aziendale, a garanzia del personale, tra le più delicate perché pone al centro di tutto il capitale umano e non gli asset fisici; rappresenta un obbligo, un dovere di protezione tipicamente safety (D.Lgs 81/08), che il datore di lavoro ha nei confronti dei propri dipendenti (inestimabile capitale), sempre e comunque sia all'interno che all'esterno dei confini nazionali. E non dimentichiamo l'altro aspetto più importante di questo processo: quello relativo alla Business Continuity, la chiave correlata alla capacità resiliente dell'organizzazione, che ne garantisce l'esistenza.

Il possibile pericolo di arrecare danni ai dipendenti (safety), agli asset tangibili (security) e intangibili (data protection), deriva principalmente da due fattori

fondamentali: il valore della minaccia e la vulnerabilità dell'organizzazione. Ogni impresa organizzata in processi e attività contiene delle vulnerabilità intrinseche sfruttabili, illecitamente, da qualunque soggetto antagonista, sia esso interno che esterno, finalizzate ad arrecare danni al patrimonio aziendale (brevetti, policy, dati personali, asset fisici, etc).

Un professionista della security aziendale deve possedere determinate competenze indispensabili, certamente estese, ma per natura differenziate tra loro: competenze tecniche, conoscenze giuridiche e di criminologia, dei crimini informatici e alla tutela delle informazioni sia convenzionali che classificate, la tutela dei dati personali, nozioni sul rischio e sulla protezione aziendale, sulla tutela di marchi e brevetti.

Ciò posto, e sulla base di quanto detto sin ora, la figura del security manager rappresenta concretamente l'interfaccia della sicurezza interna, valutando e gestendo ogni possibile criticità, con gli organismi istituzionali quali l'Autorità Giudiziaria (Polizia Giudiziaria) e quelli della Pubblica Sicurezza (Questore, Prefetto), per garantire costantemente alti standard di sicurezza dell'organizzazione.

Ma se da un lato abbiamo la presenza di un esperto che garantisca a pieno la protezione aziendale dalle minacce esterne e interne che possono colpire l'organizzazione, dall'altro non possiamo trascurare l'altra figura di tutela e garanzia, che la normativa europea, questa volta, istituisce obbligatoriamente come parte attiva nella compliance della data protection; un controllo e una tutela che risponderanno sì a delle esigenze diverse, sebbene con metodi e finalità molto simili a quelli del security manager, ma pur sempre svolgendo un'azione di security, particolarmente quando si trattano determinate categorie di informazioni classificate e dati personali particolari!

La preparazione del DPO dovrà spaziare fra competenze legali, cyber security, tecnico-informatiche, organizzative e gestionali, dovendo in particolare: sorvegliare l'osservanza del Regolamento, valutare i rischi di ogni trattamento alla luce della natura, ambito di applicazione, contesto e finalità; dovrà collaborare con il titolare/responsabile nel condurre una valutazione di impatto sulla protezione dei dati (DPIA art. 35 GDPR), informando, sensibilizzandoli, il titolare e/o il responsabile del trattamento, nonché il personale dipendente, riguardo agli obblighi derivanti dal Regolamento (es. la tenuta del registro delle attività di trattamento) e da altre disposizioni in materia di protezione dei dati, e non ultimo, cooperare con il Garante,

fungendo da punto di contatto con lo stesso e con gli interessati del trattamento.

Peraltro, nell'ambito della security aziendale tra le diverse normative da rispettare indiscutibilmente compare la tutela della privacy, o meglio come recita la nuova normativa, la **protezione del trattamento dei dati personali**, acquisiti e gestiti dall'organizzazione nella sua attività d'impresa. I dati contenuti all'interno di un'azienda, sia essa privata o istituzionale che sia, rappresentano un patrimonio inestimabile, perché sono informazioni personali che riguardano le persone fisiche, e/o i dati che rappresento il core bussiness. E di tutto ciò ne deve essere investito anche il SM!

Il D.lgs. 196/2003, meglio conosciuto come Codice della Privacy (CdP) imponeva esplicitamente l'effettuazione e la documentazione di un'analisi dei rischi, sancendo l'obbligatorietà della redazione di un documento programmatico sulla sicurezza (DPS, abolito nella legge finanziaria del governo Monti 2012), ma non prevedeva, ne volontariamente ne obbligatoriamente, nessuna figura esperta e preposta alla protezione dei dati, mentre il nuovo Regolamento introduce la figura del **Data Protection Officer** (DPO, art. 37 GDPR), quale responsabile della protezione dei dati.

Il rivoluzionario GDPR pretende oggi dai professionisti di settore un cambiamento radicale, culturale nell'approccio al modello di gestione, non più della semplice sfera privacy (realtà più concreta e tangibile), ma più circoscritto al solo dato personale (patrimonio intangibile), che deve essere adeguatamente affrontato applicando una riconsiderazione generale delle misure di sicurezza da adottarsi (art. 32 GDPR), per mezzo di una corretta *Risk Analysis* (art. 35 GDPR), adeguata al singolo contesto organizzativo, e non più una semplice e generica misura minima applicabile a tutti i contesti, ma elaborata caso per caso attraverso una reale mappatura dei rischi applicabile al trattamento dei dati gestiti, e progettata fin dalla nascita del trattamento, secondo i principi della *privacy by default* e *by design* (art. 25 GDPR).

Questo, diversamente dal passato, è il nuovo modello proposto dal legislatore europeo non più basato su una semplice misura minima di sicurezza contenuta in un allegato tecnico (artt. 31-36 e All. B regola 25 D.Lgs 196/2003), essendo posta a carico del titolare del trattamento la responsabilità secondo cui il principio di *Accountability* (art. 5 GDPR) definisce l'attenta analisi dei rischi e le adeguate misure di sicurezza, idonee a garantire la protezione dei dati personali trattati dal titolare stesso o dal responsabile del trattamento.

Nell'art. 37 del GDPR sono indicati gli ambiti per i quali è previsto l'obbligatorietà della nomina del DPO; tra questi ricadono diverse tipologie aziendali, tanto private quanto pubbliche, vincolate alla data del 25 maggio 2018, di procedere alla nomina, comunicando il nominato all'Autorità Garante della protezione dei dati personali.

Dall'analisi sin qui fatta sui rischi e sulle figure a protezione delle organizzazioni, è emerso un quadro d'insieme chiaro: sino ad oggi, la gestione del rischio era orientata secondo le visioni manageriali ad una logica più economica che di tutela degli asset (tangibili e intangibili). Le moderne organizzazioni utilizzano sempre di più apparati complessi e vettori sempre più veloci, sistemi in grado di gestire una quantità enorme di dati e informazioni, trasferiti nella dimensione temporale dello spazio-tempo: miliardi di byte trasferiti in un millisecondo, da e per qualsiasi parte del mondo!

Motivi questi che hanno spinto le aziende a prendere sempre più coscienza del bisogno di proteggersi da un eventuale rischio, esterno o interno che fosse, a una ripartizione dei compiti, delegandoli e dividendoli con determinate figure quali, appunto, il SM per l'aspetto security, e con il nuovo Regolamento europeo sulla data protection con il DPO.

La mancanza di studi universitari, la carenza nella ricerca sulla security aziendale, hanno prodotto come risultato ultimo una mancanza della regola dell'arte su come proteggere le organizzazioni dalle minacce, dai rischi; disciplina, invece, sviluppata interamente e volontariamente dalle stesse aziende.

Mentre a livello statale ci si interessava a normare, esclusivamente, i settori della safety e della privacy (il GDPR arriva poi come normativa di istituzione europea), per la security aziendale (tecniche, modelli organizzativi, prassi, processi, metodologie, etc) non si è mai concretamente intervenuti, considerandola come detto, una prerogativa soggettiva e autonoma delle imprese, esercitata individualmente.

Tutto ciò, nonostante le relazioni in merito da parte di qualificate aree istituzionali (<https://www.senato.it/service/PDF/PDFServer/BGT/698282.pdf>), che sollecitavano il legislatore nel porre un rimedio ad una questione considerata come una prerogativa strategica, tanto per le organizzazioni private che pubbliche, e laddove l'istituzione governativa ancora latita, non fornendo adeguate risposte (http://dati.camera.it/ocd/aic.rdf/aic4_03389_17).

Ma è la convergenza finale sostanzialmente a non cambiare, perchè sia l'una che l'altra figura occupano gli stessi ambiti operativi, affrontano le stesse problematiche, che trattano con le stesse policy aziendali, identiche procedure di sicurezza, stesse metodologie analitiche nell'affrontare i rischi, medesime tecnologie di protezione, uguali misure di sicurezza.

In ultima analisi, e per chiudere il senso del ragionamento fatto sin qui, il dilemma su cui ragionare è: posto che queste due figure, il Security Manager e il Data Protection Officer, sono strategiche per la sicurezza delle organizzazioni private, e delle infrastrutture pubbliche, possono riassumersi in un professionista solo? Sarebbe conveniente dal lato operativo, ancor prima che da quello meramente economico?

Leggendo i contenuti delle due normative di riferimento, beh ci sono molteplici punti di contatto, una trasversalità unica nel suo genere, similitudini che ci indirizzerebbero verso una figura unica. Ma forse è solo una mia sensazione!



La normativa per la sicurezza e la tutela del patrimonio aziendale

*"Clearly worthless security is like a ship without a rudder.
But value without security is like a rudder without a ship."
HENRY KISSINGER*

In ogni azienda **la sicurezza e la tutela del patrimonio aziendale** rappresenta un aspetto fondamentale per la sua continuità operativa, la sua stessa "esistenza fisica"; un capitale che si esprime nelle sue forme più comuni, quali infrastrutture, beni, dati, valori, brevetti, proprietà intellettuale, etc.

Una condizione che richiede un forte e costante impegno, che esige specifiche competenze manageriali sulle tecnologie, i materiali, gli impianti, i sistemi, e non ultimo sulle normative di settore, sempre in continua evoluzione, ma non sempre un "dominio" conoscitivo dei professionisti di settore.

Ecco che, per un Security Manager, rendere compliance il proprio ambito della sicurezza fisica significa tener conto di tutte le esigenze di protezione (safety e security), valutando attentamente, in fase di *Risk Analysis*, tutte le possibili

vulnerabilità e le carenze latenti dell'organizzazione, trasformando tali analisi in concreti sistemi tecnologici di protezione (antintrusione, controllo accessi, videosorveglianza, *building automation*, etc).

Procedure, istruzioni di lavorazioni, capitolati per servizi esternalizzati, ordini di lavoro per specifici impianti, e così via, devono essere attentamente valutati, come abbiamo appena detto, anche sotto l'aspetto della compliance, con una particolare attenzione verso l'aspetto della **conformità normativa tecnico-giuridica di ogni sistema progettato e successivamente installato**.

Il professionista della sicurezza aziendale (UNI 10459) opera quotidianamente insieme ad altri professionisti di settore (installatori, progettisti), un ambito, quello della sicurezza (*security, safety, building automation*), dominato da una serie infinita di norme e disposizioni normative, spesso disomogenee tra loro, quando non curiosamente in antitesi, in fatto di **responsabilità civili/penali**.

Affine per specializzazione al comparto industriale degli impianti elettrici, è del tutto evidente come anche gli adempimenti normativi del settore sicurezza siano fortemente comuni ad entrambi, e seppur con talune sfumature, sempre ricadenti nel perimetro vincolato delle norme [CEI](#), [UNI](#), del [DM 37/08](#) e della [Legge n° 186/68](#), tanto per citarne alcune.

Peraltro, il manager della sicurezza deve sempre assegnare i progetti aziendali, per legge, a professionisti del settore di comprovata e certificata affidabilità, all'altezza del compito loro affidato.

Questo perché, quando i professionisti vengono meno ai vincoli contrattuali, convenuti con la committenza, ne risponderanno in sede civile e penale del **"danno contrattuale"** cagionato, come anche del **"danno extracontrattuale"**, effetto contemplato quando il professionista non è rispettoso della buona **"regola dell'arte"**, e si concretizza, inoltre, quando non presta la dovuta **"diligenza tecnica"** propria delle sue capacità e cognizioni **"tecnico-normative"**.

Ciononostante, abbiamo due casi nei quali il professionista non risponde del danno, ovvero: quando nel contratto di commessa sarà espressamente prevista una certa **"discrezionalità tecnica"** gestita dallo stesso, che dovrà però sempre muoversi nell'alveo dell'obbligatorietà tecnica, mentre in secondo luogo, quando la committenza imponga le sue esigenze, laddove poi il professionista renderà edotta

la stessa sulla reale possibilità di una *“risultanza tecnica imperfetta”* dei lavori commissionati.

Sebbene la nozione regola dell'arte abbia registrato una vasta divulgazione e il suo concetto inserito nei contratti, come nelle sentenze, pur essendo espressamente citata nell'[art. 2224 del Codice Civile](#) (C.C.) dove è scritto che:

“il prestatore d'opera è tenuto a procedere all'esecuzione dell'opera secondo le condizioni stabilite dal contratto e a regola d'arte”

Ebbene, nonostante ciò mai è stata fornita una esplicazione tangibile della *“regola”*.

Invero, è proprio nel settore impiantistico elettrico che rinveniamo una prima definizione della regola dell'arte, infatti, all'interno dei due unici articoli che compongono la **Legge n° 186/1968** sulle *“Disposizioni concernenti la produzione di materiali, apparecchiature, macchinari, installazioni e impianti elettrici ed elettronici”*, così è scritto:

Art. 1, *tutti i materiali, le apparecchiature, i macchinari, le installazioni e gli impianti elettrici ed elettronici devono essere realizzati e costruiti a regola d'arte;*

Art. 2, *i materiali, le apparecchiature, i macchinari, le installazioni e gli impianti elettrici ed elettronici realizzati secondo le norme del Comitato Elettrotecnico Italiano (CEI) si considerano costruiti a regola d'arte.*

Del resto, è lo stesso significato contenuto nella [Legge n° 46/1990](#) sulle *“Norme per la sicurezza degli impianti”*, sostituita poi nel prosieguo del tempo dal Decreto Ministeriale **DM n° 37/2008** *“Regolamento sul riordino delle disposizioni in materia di attività di installazione degli impianti all'interno degli edifici”*, attività regolatoria che interesserà ancor di più i professionisti del settore, decreto che nell'art. 6 dice:

“Le imprese realizzano gli impianti secondo la regola dell'arte, in conformità alla normativa vigente e sono responsabili della corretta esecuzione degli stessi.

Gli impianti realizzati in conformità alla vigente normativa e alle norme dell'UNI, del CEI o di altri Enti di normalizzazione appartenenti agli Stati membri dell'Unione europea o che sono parti contraenti dell'accordo sullo spazio economico europeo, si considerano eseguiti secondo la regola dell'arte”.

Una disciplina di applicazione, questa, basilare in quanto, a caratterizzazione speciale per gli impianti elettrici (residenziali/industriali) ed elettronici (security/safety), completa negli aspetti progettuali, procedurale e documentali, oltremodo precisa nel dettato installativo degli impianti tecnologici.

Concetti questi, ulteriormente rimarcati quando si realizzano installazioni, elettriche o elettroniche che fossero, negli ambienti di lavoro la dove **impera** il [D.LgsI n° 81/2008](#), meglio conosciuto come il “**Testo Unico**” sulla “*Tutela della salute e della sicurezza nei luoghi di lavoro*”, dove nell’art. 81 riafferma parimenti il concetto:

comma 1. *tutti i materiali, i macchinari e le apparecchiature, nonché le installazioni e gli impianti elettrici ed elettronici devono essere progettati, realizzati e costruiti a regola d’arte;*

comma 2. *ferme restando le disposizioni legislative e regolamentari di recepimento delle direttive comunitarie di prodotto, i materiali, i macchinari, le apparecchiature, le installazioni e gli impianti di cui al comma precedente, si considerano costruiti a regola d’arte se sono realizzati secondo le pertinenti norme tecniche;*

Ma tuttavia, quando le norme tecniche (CEI/UNI, etc) non trovano applicazione, ebbene, una risposta alla definizione della regola dell’arte la dobbiamo pur trovare!

Sul punto troviamo una possibile soluzione nella locuzione legislativa “[Bonus pater familias](#)”, ovvero, l’attenzione del buon padre di famiglia, che si concretizza giuridicamente con l’agire con perizia, prudenza e diligenza, secondo quanto contenuto nell’[art. 1176 C.C.](#); indubbiamente, ciò posto rappresenta la diligenza media che si deve presupporre nell’uomo medio, ovverosia, la valutazione di quella diligenza che il codice sollecita affinché non sussista una colpa.

Pertanto, in questa fattispecie, sarà più laborioso e particolarmente macchinoso poter dimostrare come si applichi concretamente la regola d’arte, non avendo più nessun riferimento positivo e vincolante, proposto, ad esempio, dalla normativa tecnico-giuridica.

Orbene, alla luce di quanto accennato sin qui appare chiaro il fatto di non poter certificare, questa “astratta” regola dell’arte, né come realizzarla in una maniera certa, tale da non prestarsi a svariate ed equivoche interpretazioni.

E' tuttavia indubbio, alla stregua di quanto detto, come nel settore elettrotecnico si imponga, per progettare prima e realizzare poi impianti tecnologici "a regola", il rispetto delle regolamentazioni (leggi e norme) che sono articolate in due tipologie di riferimento: la [norma tecnica](#) e la [norma giuridica](#).

Peraltro, la conoscenza delle normative, nella esatta distinzione dottrinale tra norma giuridica e norma tecnica, rappresenta il presupposto fondamentale, imprescindibile per un approccio professionale alle problematiche tipiche del settore impiantistico elettrico ed elettronico; sistemi che andranno realizzati al solo scopo di conseguire quel "**livello di sicurezza accettabile**" che la norma impone, ma che non è mai assoluto, perché al progredire tecnologico seguirà sempre una consequenziale rideterminazione regolatoria fatta sia dall'ente normativo (CEI/UNI, etc), che dal legislatore (Leggi, DPR, DM, D.Lgs, etc).

E allora diamolo uno sguardo, seppur sommario, alla differenza che intercorre tra la norma tecnica e quella squisitamente giuridica.

Per definizione le **norme giuridiche** appartengono alla "famiglia" delle norme di diritto, che impongono, in uno specifico settore, "**regole**" di condotta da seguire e quelle da evitare, mentre le [leggi](#) (scomponibili anche in più norme specifiche) hanno una caratterizzazione di applicabilità di larga portata.

D'altra parte, sebbene queste terminologie siano spesso prese come sinonimi, la norma non va mai erroneamente confusa con la legge, perché anche avendo sì le stesse caratteristiche (imperatività, positività, etc), si sostanziano, e dunque si differenziano, per la portata: la norma possiede un **valore limitato** in uno specifico settore, al contrario della legge che assume un **valore di rilevanza generale**, su regole di vita, di condotta e di comportamento.

Diversamente, l'osservanza delle norme tecniche non è obbligatoria per volontà espressa dal legislatore, che non le connota come "leggi", ma le considera piuttosto come "documenti" che definiscono talune prassi, caratteristiche, processi, secondo uno "**stato dell'arte**" tecnologico del momento, dichiarandone pertanto la volontarietà di queste fonti.

Quindi, a ben vedere, non rappresentano l'esercizio in capo al potere legislativo, in quanto rappresentano il prodotto dell'elaborazione e dell'aggiornamento continuo che

gli enti di normazione, in base allo sviluppo tecnico-scientifico, pongono in essere in delegazione di tutte le parti socioeconomiche interessate.

Questo è sempre vero laddove le norme volontarie sono considerate “isolatamente”; diversamente, non è mai vero quando le norme tecniche e giuridiche si condizionano a vicenda, esercitando un impatto “giuridico” le une sulle altre, nella fattispecie applicativa propria dei loro ambiti di appartenenza, meglio conosciuta come “**sfera di influenza**”.

Un effetto di tal genere diventa cogente nel momento in cui la norma tecnica è richiamata all'interno di una legge, e dunque, questo richiamo fa valere il principio giuridico per cui qualsiasi norma richiamata assume la forza di legge.

E' ben vero allora, e ora lo sappiamo con certezza, che solo quando il professionista applicherà con diligenza tali “indirizzi” dimostrerà un metodo deontologicamente corretto nel soddisfare il dettato applicativo della **legge 186**, garantendo peraltro, quel “**livello minimo di sicurezza**” rispondente proprio alla regola dell'arte, e dunque, applicando la normativa tecnica di riferimento non è più tenuto a dimostrare di avere lavorato secondo legge.

Detto ciò, appare evidente come la regola dell'arte vada considerata quale elemento in continua evoluzione dottrinale, ma riferita sempre allo “stato dell'arte” tecnologico in cui si opera, alla conoscenza tecnica del periodo, della normazione e delle vigenti leggi.

Quanto appena sostenuto sottolinea con forza l'obbligo per il professionista nel mantenersi sempre aggiornato sulla evoluzione tecnico-normativa (CEI, EN, UNI, etc), e su quella legislativa (Leggi, DPR, DM, DLgs, etc.), perché il mancato rispetto delle “**Norme**”, a prescindere dall'osservazione o meno dei singoli vincoli contrattuali, determinerà sempre una **giudiziale responsabilità per danni**, confermata peraltro dalle molteplici pronunce giurisprudenziali (civili/penali), tanto di merito (Tribunali, Corti d'Appello) quanto di legittimità (Suprema Corte di Cassazione).

Né può, del resto, essere mai sottovalutata la responsabilità contrattuale ed extracontrattuale del professionista che opera nel settore della sicurezza, dato che la tal cosa nasce per effetto dell'entrata in vigore di indirizzi specifici contenuti nell'[allegato K](#), appendice nella norma [CEI 79/3:2012](#), oltre all'azione delle sentenze

di condanna nel risarcire danni per negligenza, colpa, errata progettazione/realizzazione, mancato o cattivo funzionamento dei sistemi di sicurezza in occasione di eventi criminosi.

A tale riguardo, ogni professionista è tenuto a mantenere sempre un comportamento diligente necessario alla realizzazione dell'opera, adottando puntualmente tutte quelle misure e cautele necessarie, idonee per la corretta esecuzione della prestazione commessagli, secondo un modello di accuratezza e di abilità tecnica.

Ora, la diligenza si evidenzia nei profili della cura, della cautela, della perizia, della legalità sotto l'aspetto dell'integrità materiale, come nella mancanza di vizi.

Mentre, la perizia si sostanzia invece nell'uso delle abilità supportate da appropriate nozioni tecniche caratterizzanti la professione svolta, anche mediante l'utilizzo della strumentazione adeguata e necessaria all'attività professionale.

Solo per citare qualche esempio, richiamiamo l'attenzione del professionista su alcune sentenze della Cassazione, come la sentenza n° [12879/2012](#), dove è scritto che se un sistema di sicurezza antirapina non funziona correttamente per difetti imputabili alla manutenzione, allorquando il sito protetto è soggetto ad evento rapina, l'azienda incaricata dell'appalto manutentivo ne rispondere in solido dei danni sofferti, visto che:

“... se non si ritenesse che un impianto di allarme specifico possa in qualche misura essere utile per evitare il furto o per attenuarne le conseguenze non vi sarebbe allora alcuna ragione per installarlo (sicché la sua potenziale utilità allo scopo può dirsi costituire nozione di fatto rientrante nella comune esperienza per gli effetti di cui all'art. 115, secondo comma, c.p.c.)...”

In un'altra sentenza, la n° [12995/2006](#), si ribadisce ad esempio come il professionista, anche laddove si attenga rigidamente alle indicazioni del progettista, può essere chiamato alla corresponsabilità per i **“vizi dell'opera”** in quanto, conservando in ogni caso una sua autonomia, non esegue gli impianti secondo la regola dell'arte, o in assenza di specifica formazione; quindi, quando il danno è provocato da elementi non contemplati nei precetti dottrinali, andrà sicuramente esercitato il comportamento del Buon padre di famiglia (perizia, prudenza e diligenza) che l'installatore deve sempre osservare, quando la norma è carente.

Tuttavia, anche quando l'installatore, nei limiti e in base alle cognizioni tecniche da lui conosciute, non segnala al committente le carenze progettuali o gli errori macroscopici dell'opera da realizzare, sarà comunque ritenuto corresponsabile in caso di danno, anche quando abbia eseguito fedelmente il progetto e le indicazioni in esso contenute, nonostante la presa di coscienza degli errori rilevati.

Diversamente, se il professionista rende edotta la committenza, documentando compiutamente i rilievi sulle eventuali carenze e/o errori progettuali, ma quest'ultima gli ordina comunque di eseguire le indicazioni palesemente errate del progettista, lo stesso sarà esente da ogni responsabilità, perché privato oggettivamente dalla libertà decisionale quale "*nudus minister*", perché indotto comunque ad eseguirle su insistenza del committente, e a totale rischio di quest'ultimo (Cassazione sentenza n° **538/2012**).

Partendo da questi capisaldi la Suprema Corte si è spinta oltre, stabilendo un assunto, secondo il quale, anche **in assenza specifica normazione tecnica che obblighi precisi adempimenti**, è configurabile la responsabilità per danni extracontrattuali conseguenti alla mancata osservanza delle generiche **norme di salvaguardia**.

D'altra parte, nel caso dell'installatore, tale figura opera spesso in un contesto eterogeneo, dove regolarmente vengono coinvolti più professionisti, e dunque, costretto a confrontarsi con progettisti, direttore dei lavori, responsabili della sicurezza, un fattore questo che implica possibili e significativi "effetti" in termini di responsabilità legali di "terzi" verso la committenza, però ascrivibili indirettamente anche allo specialista estraneo ai fatti.

Un classico esempio, che racchiude il tutto, è ben rappresentato da installazioni realizzate in zone classificate, e dunque altamente pericolose; ebbene, il mercato offre soluzioni di protezione per ambienti classificati di tipo "**Ex d**" ed "**Ex tb**" che consentono l'impiego, altrimenti impossibile, di strumentazioni e/o tecnologie non progettate per aree pericolose o a rischio di esplosioni.

In questo caso di "**scuola**" osserviamo diverse figure professionali coinvolte, ma con responsabilità interdipendenti tra loro: produttore; progettista; installatore.

Il **produttore** garantisce l'adeguato livello di sicurezza delle apparecchiature e

ne certifica l' idoneità all'installazione nel corretto ambito operativo, vincolato a fornire specifiche tecniche chiare ed esaustive, su impiego, utilizzo, installazione e manutenzione.

Viceversa, il **progettista** è il responsabile del dimensionamento e della corretta selezione dei componenti certificati, sempre vincolata alle esigenze impiantistiche, operative e di utilizzo, nel pieno rispetto della conformità alle norme e ai limiti delle attestazioni funzionali dei componenti.

Invece, la responsabilità dell'**installatore** assume una posizione decisamente più ambigua, nel momento che riceve la documentazione progettuale, giacché a seguire, ricadranno più incombenze su di lui, che sono quelle di attenersi alle indicazioni dettate dal progetto, verificandone però la fattibilità, come il rispetto dei limiti di utilizzo e installazione delle apparecchiature imposti dal produttore, e mai sindacabili, senza apportare modifiche di nessuna natura, anche quando effettuate "**a regola d'arte**", considerando che ogni modifica arbitraria annullerà la sicurezza funzionale, pregiudicandone, peraltro, la conformità alle norme di riferimento e, quindi, la validità stessa del certificato, pregiudicando nel suo complesso l'intera realizzazione.

Proprio su tali motivazioni, la magistratura a preso delle contromisure processuali, affidando sempre più tutte le "indagini tecniche", che riguardassero violazioni nel settore degli impianti tecnologici, con specifici incarichi investigativi volti a verificare la **sussistenza giuridica** di quell'accorgimento (*bonus pater familias*) che, quando non diversamente normato, avrebbe potuto evitare il concretizzarsi del danno e/o di un possibile reato, che si realizza in concreto con quanto già raccontato nella parte iniziale del nostro ragionamento, ossia: **Perizia, Prudenza e Diligenza!**

Ma la responsabilità dei professionisti del settore non si esaurisce esclusivamente nel solo ambito civile, perché per talune fattispecie viene estesa anche in quello penale, che ricordiamo, nell'ordinamento italiano è tipicamente "personale".

Al riguardo è bene tenere a mente il disposto dei due commi dell'**art. 40 del Codice Penale** (C.P.) che dice:

- **c1**, nessuno può essere punito per un fatto preveduto dalla legge come reato, se l'evento dannoso o pericoloso, da cui dipende l'esistenza del reato, non è conseguenza della sua azione od omissione;

- **c2**, non [impedire](#) un evento, che si ha l'obbligo giuridico di impedire, equivale a cagionarlo”.

Altri punti chiave del Codice sono l'[art. 5](#) *ignoranza della legge penale* (leggasi conoscere le leggi della propria professione), l'[art. 483](#), *attestazione di falso in atto pubblico* (leggasi falsa dichiarazione di conformità), l'[art. 449](#), *incendio colposo* (leggasi l'errato dimensionamento di un impianto, la sua cattiva realizzazione, l'utilizzo non conforme di materiale e tecnologie), l'[art. 451](#) *omissione colposa di cautele/difese* (leggasi per colpa, omissione, ovvero rimuovere o rendere inservibili apparecchi destinati alla sicurezza).

Quindi, da questa summa lettura emerge chiaro come in tutti i campi professionali è l'omissione colposa ad essere punita, e dunque, è certamente sulla base di questo elemento principe, ad esempio, che si possono ascrivere ai professionisti fattispecie penali per reati consumati nell'esercizio della propria attività, quando questa ne comporta l'assunzione di una “**posizione di garanzia**” (Cassazione sentenza [n° 38624/2019](#)), quale ad esempio quelle del progettista o dell'installatore degli impianti tecnologici, quando quest'ultimi sono sottoposti a **certificazione di legge**.

In aggiunta a quanto scritto qualche riga più sopra, per concretizzare la condizione di una qualsiasi responsabilità penale del professionista, non occorre necessariamente l'accadimento reale dell'evento, perché in ambito penale sussistono anche i reati di “**mero pericolo**”, una fattispecie penale dove viene punito già il semplice insorgere del possibile pericolo per l'incolumità pubblica.

Riassumendo, possiamo affermare che:

- la regola dell'arte va intesa come quel complesso di regole tecniche da rispettare per garantire la realizzazione di opere con un livello minimo di accettabilità, in termini di gestione, efficienza, sostenibilità, durata e sicurezza del sistema reso;
- un professionista, in buona sostanza, per poter operare conformemente secondo la regola d'arte deve anzitutto conoscere e applicare le relative norme tecniche di settore supportate dalla normativa giuridica di salvaguardia; sul punto, solamente gli impianti realizzati in conformità alle normative **CEI/EN**, sono, per la nostra legislazione, considerati realizzati a regola d'arte;

- ricevendo un progetto, dovrà essere sempre all'altezza di interpretarlo correttamente, come, peraltro, capace di stabilirne le carenze e le non rispondenze, compatibilmente alle conoscenze e capacità tecniche limitate al suo profilo professionale;
- al termine dei lavori dovrà sempre effettuare tutte le prove funzionali e le verifiche di sicurezza, certificando il tutto in [accountability](#) agli obblighi normativi.

In conclusione: uscire erroneamente, o peggio ancora dolosamente, dal *"fil rouge"* che unisce le normative tecniche a quelle giuridiche, danneggerà sempre la credibilità del professionista, giacché le non conformità rappresentano una chiara responsabilità amministrativa, civile e penale, della quale tanto i professionisti, quanto la committenza, ne risponderanno inequivocabilmente di fronte all'Autorità.



Sicurezza dei sistemi aziendali

"In business we plan for success, but in security we have to plan for failure"

Una massima, usata anche in campo ICT, che tutte le organizzazioni – pubbliche o private – esposte a rischi di security e safety connessi alle vulnerabilità legate ai propri assets, dovrebbero osservare come un punto fermo e imprescindibile.

In una moderna (globalizzata) organizzazione, **la sicurezza e la difesa del patrimonio aziendale** sono di vitale importanza, e vanno preservare in ogni aspetto:

- **infrastrutture;**
- **beni tangibili e intangibili;**
- **informazioni e dati;**
- **capitale umano e know how;**
- **proprietà intellettuale e brevetti.**

La Sicurezza Aziendale è una attività che richiede un costante impegno, soprattutto economico, e specifiche competenze professionali relative a tematiche e normative in

continua evoluzione.

Un'efficace protezione del patrimonio deve essere affrontata sempre attraverso una stretta interdisciplinarietà, data la natura della materia e l'oggetto della tutela.

Un'azienda, quale articolazione dei beni organizzati, rappresenta un insieme di ricchezze, materiali, immateriali e capitale umano, la cui protezione richiede una *vision* ad ampio spettro, metodologicamente efficace: mai partire dalla probabile fonte della minaccia, ma piuttosto dal bene che si intende garantire.

Banalmente: se dovrò proteggere una tela preziosa, il mio obiettivo non sarà solo quello di concentrarmi, esclusivamente, su un impianto integrato di security (allarme, videosorveglianza, etc), ma dovrò pormi anche il problema di altre possibili **minacce esogene**, tanto antropiche (dolose e colpose), quanto naturali (inondazioni, incendi, terremoti, etc), perché servirà a poco proteggere la tela da un furto, se questa poi sarà irrimediabilmente danneggiata, e dunque, privata del suo **reale valore economico**.

D'altronde, per converso, sarà del tutto inutile qualsiasi sottoscrizione di leale fedeltà da parte del management aziendale se, poi, i **dati e le informazioni strategiche** non sono adeguatamente protetti, ma alla portata di tutti!

Quindi, rifacendoci a questo ultimo esempio, il **management dell'area security** attiverà tutta una serie diversificata di procedure (furto dati, spionaggio industriale, attacchi al patrimonio informativo, etc), tanto per l'identificazione quanto per il trattamento, sia dei dati che delle informazioni aziendali; lo farà considerando un adeguato sistema tecnologico di [sicurezza cyber](#), di information security, il cd [perimetro logico](#), implementato da un robusto **sistema di gestione delle informazioni**, che racchiuda in sé gli aspetti di sicurezza logica, fisica e organizzativa (es. ISO 27001).

Diversamente, voglio tutelare l'immagine e la reputazione aziendale? E allora focalizzerò l'attenzione, ad esempio, sull'uso interno dei **social network**, seguendo una strategia diametralmente opposta, attuando preliminarmente uno *screening* sistematico e continuo delle attività che i dipendenti compiono sui social, anticipando parallelamente le difese e le contromisure più idonee; tuttavia, tali controlli dovranno essere sempre condotti nel pieno rispetto dei diritti costituzionalmente garantiti (segretezza delle comunicazioni, libertà di pensiero, etc.) e [sorvegliati dall'Autorità](#)

[Garante della privacy](#), in maniera tale da non violare la libertà e la dignità personale degli interessati.

Perciò, nel contesto di una globalizzazione dove i mercati diventano sempre più complessi, la conoscenza, lo studio, l'innovazione, la tecnologia rappresentano gli **strumenti strategici** per esercitare una leadership competitiva; mentre la *vision*, l'*excution* e, in particolar modo, la compliance, caratterizzano i punti di forza dell'organizzazione aziendale che si misura sui mercati.

Security Compliance, certamente; un obbligo per l'organizzazione, tenuta a considerare tutte le esigenze di protezione, valutandole attentamente nella fase di *Risk Analysis*, rispettando tutte le prescrizioni definite nelle **policy aziendali di security**, e approvate come documentazione di **security compliant**.

E qui entriamo nella sfera del **Risk Management** (*Risk Assessment, Risk Reporting, Risk Treatment, Risk Monitoring*, etc), strumento indispensabile al raggiungimento delle *performance* aziendali; un'area dove l'analisi dei rischi sarà ampia e approfondita, considerando tutti i possibili scenari di rischio che potrebbero danneggiare il perimetro aziendale, minandone le capacità operative, la posizione di mercato, la reputazione aziendale, la solidità economica.

Nelle attività di **gestione del rischio** bisogna sempre ricercare il giusto equilibrio al compromesso tra l'eliminazione (prevenzione, protezione) e la riduzione del rischio (compensazione), considerando sempre il trasferimento del rischio (assicurazione, terzi, etc), un elemento residuale del processo.

Pertanto, negli ultimi anni, la gestione del rischio è stata integrata all'interno del nuovo sistema di qualità ISO 9001 (presente anche all'interno dei modelli organizzativi delineati dai D.Lgs 231/2001 e 81/2008).

Nei modelli di gestione del rischio, un altro aspetto fondamentale è dettato dalla **business continuity**; i piani di continuità operativa (*business continuity plan*) rappresentano la chiave primaria nel processo di **resilienza dell'organizzazione**.

Una delle professionalità cardini riservate alla gestione della sicurezza e alla tutela del patrimonio, è quella del [Security Manager \(UNI 10459:2017\)](#); uno specialista in grado di leggere l'evoluzione dei contesti strategici, nazionali e internazionali, e

analizzandone gli scenari, individuerà, misurandoli, i rischi applicabili alla propria organizzazione, proponendo azioni mirate (security e safety), volte alla loro mitigazione e/o riduzione.

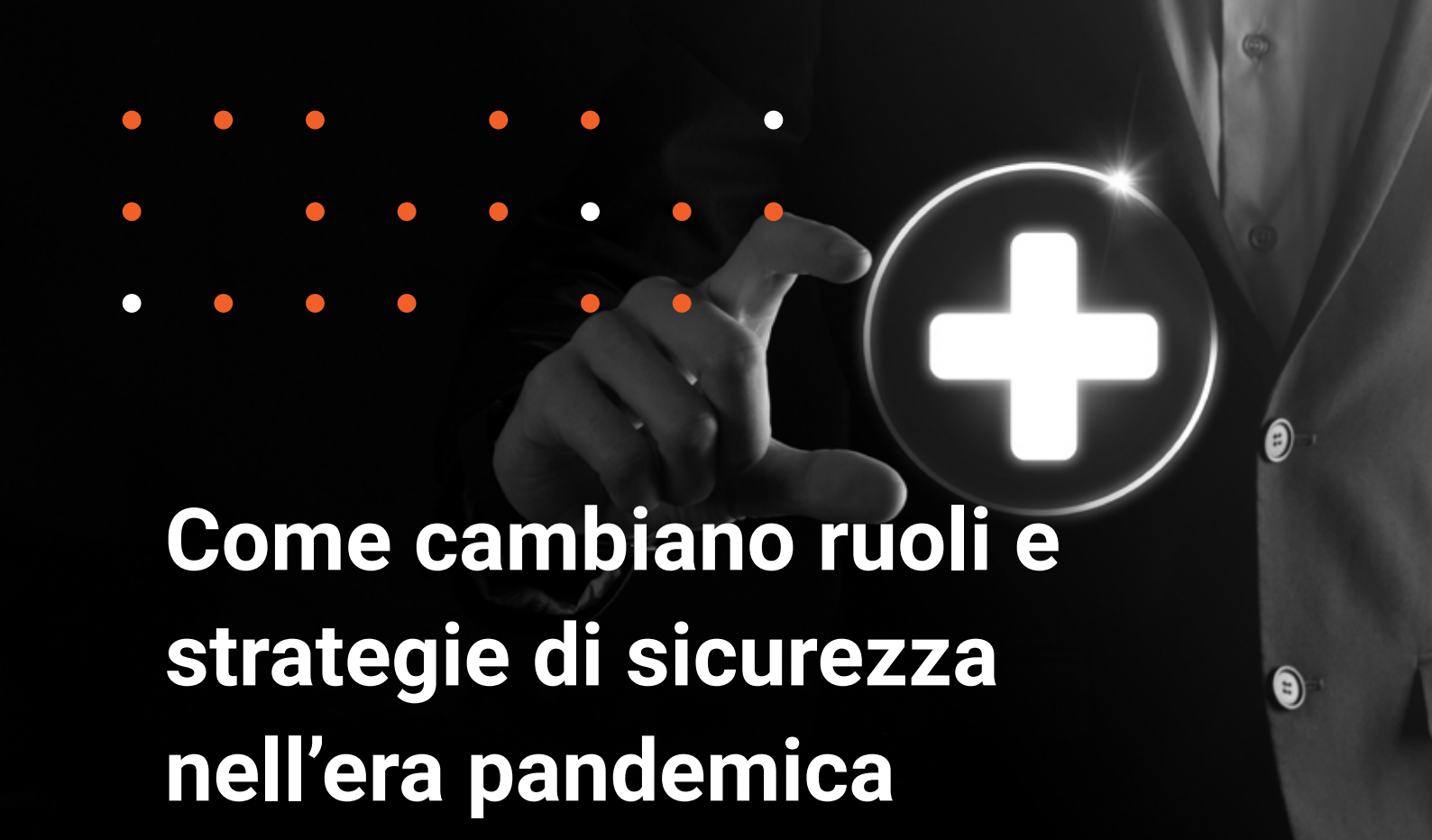
Assistiamo frequentemente a un'espansione dimensionale e insidiosa del rischio, soprattutto nel perimetro cibernetico, laddove proprio **la criminalità organizzata e le organizzazioni terroristiche viaggiano con maggior velocità rispetto alla resilienza dei sistemi.**

Oggi un professionista della Security deve possedere una preparazione trasversale unica: *crisis management, emergency planning, risk analysis, data protection, loss prevention, asset protection, physical security, personnel security, travel security, intelligence, investigations, legal aspects.*

Questo perché diversi sono i campi operativi e le competenze che questo manager deve possedere: le fonti della minaccia si sono diversificate e moltiplicate, per effetto della crescita esponenziale delle tecnologie e del mutato quadro internazionale.

Ma nuove sfide aspettano il mondo della security aziendale. In questi ultimi mesi abbiamo assistito all'emergere di una **nuova vulnerabilità** con la quale le organizzazioni, d'ora in poi, si dovranno confrontare: la medical security, un pericolo conseguente all'epidemia del Coronavirus nCoV2019.

Travel, personnel e medical security saranno parte integrante dei processi e analisi di rischio che le aziende affronteranno quando invieranno i propri dipendenti oltre confine. Un vero processo di **medical intelligence** che dovrà essere attivato ogni qualvolta verrà messa in discussione l'incolumità del **patrimonio umano aziendale**, in trasferte classificate come ad **alto rischio sanitario**.



Come cambiano ruoli e strategie di sicurezza nell'era pandemica

"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 recovery** 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.



Travel Security Management

Sicurezza delle trasferte all'estero

"Imparare è un'esperienza, tutto il resto è solo informazione"

ALBERT EINSTEIN

L'incertezza **pandemica** creata dall'emergenza **Covid-19** ha spesso implicato decisioni del blocco delle trasferte di lavoro, a livello mondiale, con provvedimenti aziendali adottati, talvolta, in maniera sbrigativa, stante la criticità del momento.

In ambito di **Risk e Security Management**, tutte le organizzazioni devono saper riconoscere le minacce a cui sono quotidianamente esposte, e dovrebbero farlo utilizzando i diversi strumenti di prevenzione e contrasto che il settore professionale mette loro a disposizione.

Tali analisi vanno fatte su attività come l'organizzazione e la gestione dei trasferimenti fuori sede, con un particolare riguardo a quelle specifiche, come ad esempio una possibile evacuazione, una immediata esfiltrazione con successivo rimpatrio di tutto il **capitale umano** che l'azienda ha distaccato nei teatri operativi fuori dalla propria nazione.

Orbene, man mano che le varie multinazionali aumentano il loro sviluppo intercontinentale, cresce di pari passo la loro capacità operativa, dunque anche le Piccole Medie Imprese (cd PMI) ad esse collegate diventano sempre più globali, quindi proporzionalmente aumenteranno gli spostamenti per affari dei loro dipendenti.

Una condizione questa che moltiplicherà la pressione sui datori di lavoro, in fatto di responsabilità verso il [TU 81/08](#), in modo tale da poter dimostrare la corretta analisi dei potenziali rischi/pericoli prima di intraprendere qualsiasi **viaggio di lavoro**.

Per natura, i rischi di una trasferta internazionale cambiano continuamente al variare degli scenari; in ogni realtà fuori dai confini, molte situazioni possono mutare in base al periodo dell'anno, al momentaneo clima politico, all'evolversi del quadro geopolitico, oppure da specifici fattori climatici e/o ambientali, motivazioni che andranno analizzate, per ordine logico, in maniera attenta e puntuale, in modo tale da non lasciare nulla al caso, senza perdere del tempo prezioso alla ricerca di rischi inesistenti.

Il più delle volte i viaggi di lavoro scorrono via senza grosse criticità, ma c'è sempre in agguato una piccola possibilità che qualcosa possa andare storto, ecco quindi, che quando i dipendenti viaggeranno per motivazioni professionali di qualsiasi tipologia, **è un onere del datore di lavoro garantirne la sicurezza** individuale e collettiva, sia a livello di security che di safety, dando loro, il più possibile, corrette informazioni su cosa fare e a chi rivolgersi in caso di emergenza.

Dalla lettura di diverse statistiche, emergono alcuni dati davvero singolari, talora preoccupanti: un sondaggio [GBT A](#) ha rilevato che il 46% dei dipendenti viaggiatori lo fanno in contesti aziendali che non hanno politiche di travel concretamente attive, mentre il 22% degli stessi non ha la benché minima idea di chi contattare all'estero in caso di avvenuta emergenza, questo a significare la scarsa preparazione sul tema della **travel e medical security**, come la totale assenza della benché minima pianificazione riferita al semplice buon senso!

Appare evidente poi, dopo aver valutato e misurato il rischio, la necessità di trasmettere al dipendente tutte le vitali informazioni sui principali rischi e minacce che potrebbero incontrare; difatti, una corretta formazione del lavoratore dovrebbe concentrarsi principalmente sulla prevenzione, poiché spesso, è più facile evitarla una

situazione di pericolo piuttosto che risolverla.

Del resto, l'**accountability** legale e morale dell'alta dirigenza aziendale di prendersi cura dei propri dipendenti, anche quando viaggiano fuori dal perimetro aziendale per motivi di ufficio, è nota come **duty of care** (dovere di diligenza).

Sappiamo, infatti, come tutte le organizzazioni, pubbliche o private che fossero, siano tenute a dimostrare di aver adempiuto compiutamente alle normative sul **dovere di diligenza**, ma soprattutto sugli obblighi di tutela dettati dal Testo Unico, nel caso in cui si verificasse una crisi, un incidente, o qualsiasi altra possibile situazione che metta in pericolo l'incolumità del dipendente.

E proprio sulla scia dell'emergenza da Covid-19 che le politiche del duty of care assumono sempre di più una compliance imprescindibile nella gestione e pianificazione dei trasferimenti oltre i confini nazionali, come già contemplato nei sistemi di gestione per la salute e sicurezza sul lavoro, policy tipicamente contenute all'interno della nuova norma [UNI/ISO 45001:2018](#).

Pertanto, avere una politica aziendale di travel security ben definita non solo aiuta a prevenire problemi, evitandoli, ma migliora di certo il modo in cui i dipendenti si rapportano nei confronti della propria struttura che li tutela nelle trasferte.

Difatti, quando un viaggio di lavoro è pianificato a monte come il più agevole e indolore possibile, questo significherà anche che sarà il più produttivo, sotto l'aspetto dei risultati attesi da quella trasferta; infatti, avere dipendenti operativamente più sereni, ridurrà, nondimeno, la possibilità di implicazioni legali di tipo risarcitorio, semmai accadrebbe qualsivoglia tipo di incidente nello svolgimento delle mansioni affidategli.

E' del tutto evidente che policy e procedures sulla sicurezza delle trasferte professionali, nei suoi vari ambiti e sfaccettature, devono essere progettate e attuate da professionisti che all'interno delle organizzazioni, private o pubbliche che siano, ricoprano ruoli ben definiti e specializzati, come ad esempio la figura del [travel manager](#), del **security manager**, o talvolta dello stesso **RSPP**, laddove mancanti le figure specializzate in security.

Ebbene, da tali considerazioni ne consegue che il problema reale della sicurezza

dei dipendenti che affrontano un viaggio di lavoro, assume due aspetti centrali: il cd **dovere di diligenza del datore di lavoro**, e la corretta applicazione delle procedure di **gestione di travel risk**, due argomenti questi, spesso usati in modo intercambiabile e in maniera del tutto errata.

Pertanto, alla base dei due singoli aspetti troviamo, da una parte un obbligo giurisprudenziale e morale in capo al rappresentante legale, che lo obbliga viepiù ad assumersi la responsabilità giuridica della salute, la sicurezza e la protezione del proprio dipendente, indipendentemente dal fatto che si trovi in ufficio piuttosto che in trasferta; dall'altra, rileviamo la gestione del rischio del viaggio, nel suo insieme, quale strategia procedurale che soddisfi tale obbligo.

A tale riguardo, una soluzione il più possibile conforme e che risponda a tali problematiche è rappresentata dal piano d'azione aziendale; ad esempio, la fondazione [International SOS](#), che si occupa della sicurezza, la salute e il benessere del personale operante all'estero, pubblicò in merito al rischio viaggio del dipendente "una road map", identificando dieci buone best practices sulla corretta **diligenza dei doveri**:

1. aumentare la consapevolezza a tutti i livelli dell'organizzazione;
2. coinvolgere tutti gli attori chiave nella pianificazione del duty of care;
3. sviluppare politiche e procedure per la gestione del rischio viaggio;
4. controllare i propri fornitori in termini di duty of care;
5. comunicare, educare e formare i lavoratori e le parti interessate;
6. valutare i rischi prima di trasferire un dipendente per ragioni lavorative;
7. essere in grado di localizzare i lavoratori che viaggiano in qualsiasi momento;
8. implementare un sistema di gestione delle emergenze per i lavoratori;
9. stabilire controlli da parte del management;
10. garantire l'integrazione e il coordinamento dei fornitori di servizi.

Nel loro complesso queste buone pratiche dovranno tenere conto di diversi fattori di rischio, come l'instabilità politica di una nazione, che può influire pesantemente sui programmi di viaggio, mettendo in pericolo i dipendenti che andranno ad operare all'interno di aree geografiche politicamente instabili; ecco che tutto ciò richiederà una preventiva e attenta pianificazione, basata sostanzialmente su **informazioni aggiornate e qualificate**, nonché sul grado di minaccia delle attività terroristiche.

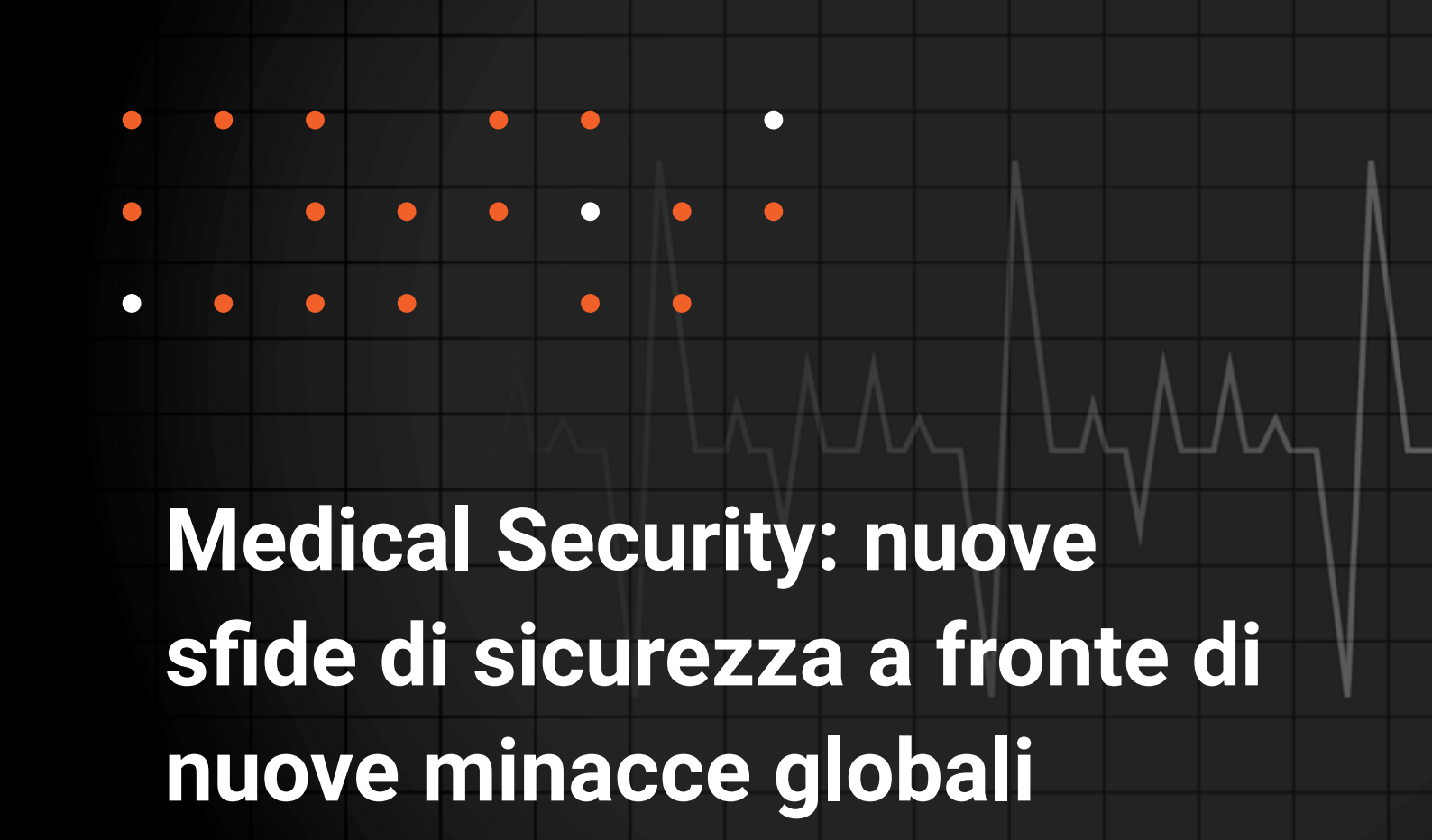
Tale analisi sull'instabilità politica andrà comparata con altre minacce, stavolta di carattere igienico-sanitario, e qui entra in gioco il medico competente; sebbene non sia sempre possibile prevedere talune problematiche di salute, è comunque possibile pianificarne in anticipo la loro gestione sulla base delle anamnesi individuali, ad esempio, considerando la disponibilità di assistenza sanitaria in sito, sia dal punto di vista del personale e delle attrezzature mediche, che di approvvigionamento farmacologico, sempre riferite al quadro clinico del personale.

Sul punto, però, va aggiunta una nota ulteriore, quella della profilassi preventiva; anche qui il medico competente dovrà accertarsi che tutti i dipendenti comandati in trasferta siano protetti rispetto al quadro epidemiologico del Paese di destinazione, prima ancora di intraprendere il viaggio.

Invero, c'è un'altra criticità che ha diretto riflesso sull'aspetto sanitario individuale e collettivo, quello della sicurezza alimentare; vale la pena ricordare, che in alcuni continenti non sempre i primari standard igienici vengono rispettati, tutt'altro, quindi si evitino sempre e comunque cibi crudi, lo *street food*, le acque sfuse e/o non sigillate, tanto per citarne alcuni.

Oltremodo, vanno considerati poi gli altri aspetti legati alla sicurezza dei trasporti, alla tracciatura degli spostamenti e monitoraggio degli itinerari, degli alloggi e del supporto prestato dai cd fornitori locali di terze parti con i quali i dipendenti entreranno in contatto per motivi professionali.

Va peraltro sempre considerato, e mai sottovalutato, un'altro delicato aspetto: la sicurezza delle dipendenti, perché le donne inviate in trasferta corrono rischi più seri rispetto ai colleghi maschi, specialmente in particolari aree geografiche fortemente dipendenti dal fondamentalismo religioso, o con usi e costumi contrari al pensiero occidentale.



Medical Security: nuove sfide di sicurezza a fronte di nuove minacce globali

"Colui che conosce solo il proprio lato della questione, ne conosce ben poco".

JOHN STUART MILL

Il nuovo virus nCoV2019, il cd. Coronavirus, scoperto nella circoscrizione cinese di Wuhan, oltre a suscitare l'ancestrale timore di una **pandemia planetaria** trasmette una sensazione ancora più subdola: il mistero della sua non chiara natura.

Diversi esperti di **intelligence e security** impegnati nel settore della **biosicurezza** hanno analizzato una grande mole di dati da fonti Osint su ogni aspetto di **medical security** e di **crisis management** riguardante il nuovo fenomeno diffusivo del virus, ma siamo ancora lontani da risultati certi e condivisi.

Tanto gli esperti, quanto *mass media* e *social*, hanno dato ampia risonanza alla scoperta del virus, prefigurando diversi scenari, fino ad arrivare persino al più controverso: la possibilità che Covid-19 sia una [bioarma orfana](#), rilasciata (?) da un laboratorio classificato [BSL-4 level](#) (massimo livello di biocontenimento), installazione presente a Whuan, area dell'epicentro epidemico.

Congetture a parte, per il momento l'unica cosa certa è che siamo nel pieno di una **crisi biosanitaria**, emergenza globale nata intorno al nuovo virus, che preoccupa ogni giorno di più i governi centrali, per gli impatti negativi che si potranno avere sul lungo periodo su scala economica e sociale, sui sistemi produttivi, l'incolumità e la salute delle persone.

Del resto, nelle organizzazioni aziendali, sia pubbliche che private, proprio in momenti critici come quelli che sta vivendo il nostro Sistema Paese, purtroppo, si materializza la vera occasione per testare, analizzandole, le **capacità resilienti** della propria struttura organizzativa, le policy e le procedure di **security, emergency e safety**, elaborate a protezione della vita dei propri dipendenti e dell'intero patrimonio aziendale.

Ora, per fronteggiare questa **emergenza globale** ogni datore di lavoro – pubblico o privato che sia – è vincolato per legge ad adottare, tramite il medico del lavoro, tutte le **misure protettive e preventive** necessarie per garantire i lavoratori, creando condizioni idonee per svolgere le attività in modo sicuro.

Infatti, quando le aziende, e le stesse istituzioni, operano in **zone classificate a rischio** – nella fattispecie, sanitario – devono adottare severe **policy di risk management** (misure di contenimento del rischio, sospensione dei viaggi/missione, rimpatrio del personale, etc) da e per le cd. zone **hotspot**, per ridurre i pericoli da esposizione alle minacce sanitarie, o fisiche che siano, intrattenendo un **filo diretto e costante con il Ministero della Sanità**, per le procedure di safety da adottare nell'immediatezza dei casi, e con la [Farnesina \(AISE\)](#) per le operazioni di security nel momento del rimpatrio.

Altra caratteristica fondamentale per la prevenzione e la tutela della salute e dell'incolumità del dipendente in missione, è quella di fornirgli **adeguate informazioni** circa i modelli comportamentali da seguire sui luoghi operativi fuori area, definendo un **piano informativo strutturato**, dati contenuti anche nelle schede Paese consultabili sul sito degli Affari Esteri.

Con **mercati sempre più interconnessi e interdipendenti**, che vede moltissime aziende proiettate fuori dai confini nazionali, ogni settore economico strategico, inevitabilmente, è costretto ad affrontare con maggior frequenza questi nuovi rischi sanitari correlati alla trasferta dei propri lavoratori.

Prestazioni di lavoro, quelle fuori dai confini, classificate nell'ambito delle linee guida della [Società Italiana di Medicina del Lavoro](#) come attività:

“atipica che presenta flessibilità di impiego ed è caratterizzata, oltre che dai rischi della mansione, da fattori correlati alle condizioni di soggiorno del paese ospitante”.

Orbene, in un'ottica di adempimento ai disposti legislativi sulle misure di sicurezza a garanzia dell'incolumità del dipendente ([TU 81/08](#)), ci si pone davanti sempre lo stesso interrogativo: è compito del datore di lavoro proteggere il dipendente, durante lo svolgimento delle sue mansioni, da tutte quelle attività, esogene e/o endogene, dolose e/o colpose, a cui lo stesso viene esposto?

La risposta, decisamente scontata, è scritta appunto nel D.Lgs 81 e rafforzata dall'[art.18 del D.Lgs n° 151/2015](#): responsabilità oggettiva, civile e penale, del datore di lavoro, sia esso pubblico che privato, ma soprattutto analisi dei rischi, degli atti ostili e criminali, l'elaborazione di piani di emergenza ed evacuazione, l'analisi della normativa antinfortunistica locale e delle interrelazioni con quella italiana, pianificazione, organizzazione, coordinamento e gestione della trasferta secondo le prassi contenute nello standard [ISO 31030](#).

Una norma ISO che delinea le compliance del **Duty of Care**, conformità specifica per la gestione dei cd. **rischi da trasferta**, linee guida che dettano gli strumenti per dimostrare, anche in sede giudiziaria, di aver fatto materialmente tutto il possibile ([D.Lgs 231/2001](#)), contro ogni ragionevole dubbio.

Ma per mettere in atto tutte queste misure di protezione e garanzia, quali contromisure vanno poste in atto, e quali figure organizzative andranno coinvolte?

Le [risposte](#) sono diverse; inizialmente va interessato e coinvolto l'ufficio del Security Manager, che affronterà tutte le attività di safety e security (*safety e security management, travel risk, medical security, etc.*) che coinvolgano, in maniera diretta o indiretta, il personale dipendente impegnato.

Tuttavia, oltre ai rischi di sicurezza legati alla specifica mansione esercitata, si dovranno valutare anche i nuovi rischi emergenti di medical security (igiene, supporti sanitari di emergenza, ricoveri locali, esfiltrazione sanitaria, etc.) legati all'area del Paese ospitante; dunque, [Security Manager, RSPP e medico competente](#) in sinergia

tra loro, e su preventive informazioni rese dal datore di lavoro, gestiranno tutti gli aspetti legati alla salute e alla sicurezza in operazioni fuori area.

Ma il mutato **scenario internazionale**, come si è visto in questi giorni virulenti, impone sempre più specifiche precauzioni e conoscenza del quadro sovranazionale, non solo a livello geopolitico: difatti, alla luce di quanto accaduto, d'ora in avanti tutta la problematica degli spostamenti esteri andrà programmata secondo **nuovi processi di medical security, che supportino fattivamente i piani di travel security**.

Processi che dovranno trovare riferimenti stabili nelle capability contenute nella **medical intelligence (Medint)** che, come tutte le attività di *intelligence*, si articola nelle tipiche fasi di raccolta delle informazioni sanitarie della nazione interessata e di analisi dei dati raccolti, per delineare verosimilmente più scenari possibili, rilasciando un prodotto informativo che gli uffici di sicurezza aziendale inseriranno nelle relative schede Paese.

Ma per una corretta compilazione delle prescrizioni di sicurezza in uso al personale che sarà impiegato fuori dal territorio nazionale, a differenza di altre informazioni, la medical security richiede una consolidata competenza medica nelle fasi di gestione e trattazione del ciclo informativo ricevuto (ospedali, malattie, igiene pubblica, epidemie, farmaci, etc.).

Ecco allora come l'azione sinergica tra Security Manager, RSPP e medico competente diventa fondamentale per la costruzione di un sistema di protezione individuale dei dipendenti, e un indiretto ritorno positivo a tutto vantaggio delle iniziative economiche strategiche per gli uffici che gestiscono le azioni di **business intelligence**.

In ultimo, l'attuale crisi pandemica ha mostrato anche l'altra faccia della medaglia: quella del pericolo da **epidemia tecnologica**, che dovrà indurci ad attente riflessioni, perché dopo la grande crisi economico-finanziaria mondiale dovuta al drammatico attentato 9/11 alle Torri Gemelle, che cambiò la percezione del pericolo nella società globale, anche questa nuova e subdola vulnerabilità (sociale, psicologica, tecnologica) classificata come **epidemia cyber** avrà negative ripercussioni sul sistema socio-finanziario mondiale.

Infatti, mentre il virus continua la sua inarrestabile cavalcata contagiosa sulla società, di pari passo sul web cresce esponenzialmente l'**infezione da malicious**

attacks (*intrusion, malware, phishing*), **sfruttando vantaggiosamente le deficienze di sicurezza delle reti** (cyber security).

Le prime avvisaglie la [Polizia di Stato](#) (**CNAIPIC**) le ha già intercettate, lanciando un preciso allarme ai tentativi di truffe informatiche testate in rete in questi ultimi giorni, con pesanti **attività di phishing legate al Covid-19**.

D'altronde le **infrastrutture Telco**, wireless o cablate che siano, utilizzate dalla **sanità moderna** rimangono il mezzo informativo centrale nella lotta all'epidemia; non voglio immaginare neanche per un istante quale catastrofe potrebbe accadere se un ospedale, un sito farmaceutico o altri centri fondamentali per la sanità pubblica dovessero cadere sotto i colpi di un pesante attacco cyber!



L'utilizzo dei Social Network nelle comunicazioni di emergenza

Secondo la definizione dell'organizzazione mondiale della sanità, la comunicazione dei rischi nelle emergenze sanitarie deve sempre includere tutte le funzioni necessarie a sollecitare un processo decisionale informato, come, ad esempio, l'adozione di comportamenti positivi nella gestione degli eventi impattanti la salute pubblica, disseminando nel contempo, tutte quelle informazioni relative ai rischi per la salute, tramite un insieme di metodi basati principalmente sulla **bidirezionalità delle comunicazioni sociali**.

Durante le fasi di una criticità pandemica, la comunicazione del rischio riveste un ruolo centrale; difatti, tanto la disponibilità delle informazioni quanto il corretto comportamento della cittadinanza, rappresentano i fattori essenziali di una **corretta governance dell'emergenza**.

Un comportamento collaborativo della popolazione durante la gestione di una crisi sanitaria, seguendo attentamente le istruzioni mediche, ma ancor più durante la gestione di talune malattie trasmissibili, prefigura il punto focale del corretto governo di qualsiasi emergenza sanitaria; tanto è vero, che la corretta percezione della minaccia da parte della popolazione, inquadra nel giusto conteso il controllo dei

contagi.

Quanto detto è fondamentale nell'approccio comunicativo generale, perché talune e specifiche caratteristiche delle epidemie, come ad esempio i tassi di infezione, la disponibilità di determinate misure protettive, le mirate profilassi terapeutiche, possono falsare la reale percezione del rischio.

Risulta dunque evidente, come tutte quelle iniziative informative, seppur dettate dallo stato emergenziale, che non tengano in considerazione i fattori appena esposti, al di là della loro possibile inefficacia, assumeranno, nel contempo, un potenziale decisamente controproducente.

Ecco perché è fondamentale che qualsiasi comunicazione verso la cittadinanza, in uno stato di crisi pandemico, sia sempre strutturata sul dialogo bidirezionale, e mai cadere nell'errore di comunicazioni verticalizzate e unidirezionali!

Peraltro, nell'ambito della comunicazione istituzionale collettiva, un altro aspetto centrale riguarda la pianificazione di questa attività, perché ricordiamo sempre, che nessun progetto, nessuna linea tattica inerente la comunicazione sociale del rischio risulterà mai efficace se non sia stata preventivamente sviluppata e testata poi, ancor prima il verificarsi degli eventi critici; tanto è vero che, laddove manca un piano di comunicazione sui cui far riferimento negli stati di necessità, l'intero processo di **emergency recovery** si complica enormemente, dilatando i tempi necessari per poter uscire dallo stallo emergenziale.

In una emergenza epidemica come quella attuale, da Covid-19, la circolazione tempestiva di informazioni affidabili svolge un ruolo fondamentale per la mitigazione del rischio, il contenimento della diffusione del virus, con il conseguente contenimento del danno socioeconomico; cosicché, ad esempio, tali informazioni potrebbero essere vettorate proprio attraverso **l'uso intelligente delle piattaforme social**.

Analizzando i dati contenuti nel [report Digital In 2022](#), relativi all'utilizzo di internet, dei supporti social e di tutti i device mobili, osserviamo come 4,95 mld di individui – sui 7,91 mld componenti la popolazione mondiale - risultano connessi ad internet e circa 4,62 mld sono quelli che utilizzano regolarmente i social network, mentre sfiorano quota 5,31 mld quelli che utilizzano giornalmente i diversi dispositivi mobili.

Dati questi, che fotografano un fatto oggettivo, vale a dire, come una singola **innovazione tecnologica** abbia di fatto agevolato la strada ad una più ampia **rivoluzione culturale**, e dunque, persino psicologica e comunicativa.

Ora, nell'era della conoscenza globalizzata tutto ciò rappresenta, senza alcun dubbio, una trasformazione epocale, generata in una società dove i flussi di notizie nascono e si espandono, principalmente attraverso i canali *online* e *social*, perché l'accessibilità alle informazioni costituisce una prerogativa indispensabile per una comunicazione incisiva, soprattutto in settori come la protezione civile che opera spesso in (per) situazioni di emergenza.

D'altra parte, quanto detto è stato riscontrato, ahinoi, durante l'emergenza delle Torri gemelle, che nel settembre 2001 colpì gli USA; ebbene, furono proprio i canali [internet](#) i primi ed unici vettori informativi – collassando poi per sovraccarico – ad essere utilizzati dalla popolazione, per fornire e reperire notizie riguardanti l'evoluzione di quella particolare emergenza collettiva.

E non poteva essere altrimenti, perché in questi casi, ogni evento critico crea l'interruzione fisica istantanea delle linee telefoniche, e dove ancora funzionanti il collasso funzionale delle stesse generato dal congestionamento infrastrutturale.

E' del tutto evidente, come i diversi canali social **Facebook, Twitter, Instagram, Whatsapp** e altri, in tali situazioni emergenziali possano fornire una concreta alternativa, fondamentale nell'ottenere informazioni necessarie ai soccorsi; di fatto, i vettori social hanno creato nel tempo una nuova architettura sociale proprio nella comunicazione dei rischi, stravolgendo di fatto, tutti i modelli comunicativi tradizionali, dal momento che gli utenti non saranno più soltanto dei semplici ricettori dell'informazione, quanto piuttosto i nuovi generatori *real time* delle stesse, **trasformando la classica verticalizzazione informativa (istituzione-cittadino), in una struttura decisamente più orizzontale, partecipativa (amplificazione esponenziale della condivisione) e bidirezionale (istituzione-cittadino-istituzione)**, una situazione che farà certamente la differenza nel ciclo della gestione del rischio.

Rimane in capo all'istituzione, invece, l'analisi delle informazioni raccolte, disseminandole successivamente verso l'utenza interessata dagli eventi, o come semplici *alert*, o come vere e proprie istruzioni comportamentali in risposta al rischio.

Pur tuttavia, solamente un uso integrato delle varie piattaforme *social* concretizzerà un'efficace comunicazione dell'emergenza/pericolo, tanto è vero che è proprio la popolazione durante gli stati di crisi, a farne un uso condiviso, giacché lo stesso web consente l'utilizzo integrato e istantaneo di diverse piattaforme multimediali, garantendo così la gestione puntuale delle informazioni, a seconda del *target* di riferimento e del contenuto informativo.

Ad esempio, **Twitter**, con la sua connotazione di istantaneità, e funzionalità, finisce per facilitare l'ordinata catalogazione di grossi flussi informativi attraverso i suoi **#hashtag**, particolarità che ne fa uno degli strumenti social maggiormente utilizzati nelle emergenze. Una piattaforma che con una potenzialità di appena 140 caratteri, favorisce perfettamente la diffusione di informazioni istantanee, utili nelle comunicazioni ambientali critiche, ma di estrema importanza nel coordinamento delle operazioni di primo intervento; tra l'altro, questo social contiene delle altre peculiarità, come i post realtime, la messaggistica pubblica, un contenitore di *followers*, la possibilità del *retweet* e dei *tag*, ebbene, l'integrazione di tutto ciò crea un dispositivo di più ampia portata nella disseminazione delle informazioni.

Sulle potenzialità intrinseche e sull'uso di questo social nel campo delle emergenze è intervenuto persino un organismo dell'ONU, l'**OCHA** (*Office Coordination Humanitarian Affairs*), mediante una sua standardizzazione pubblicata in una guida, dove si indicano i tre principali hashtag, utilizzabili nei post (geolocalizzati) utilizzati nelle fasi emergenziali: # nome della calamità, # *public reporting* e # richiesta di soccorso.

Ma la rilevanza dei social network nelle calamità collettive fu rimarcata già nel 2015, con il **Sendai Framework for Action**, la Conferenza Mondiale dell'ONU sulla riduzione del rischio catastrofi, un documento approvato dalla **World Conference on Disaster Risk Reduction**, all'interno del quale si includevano per la prima volta i *social media* come strumenti ufficiali per la gestione delle emergenze, naturali o sanitarie che fossero.

Appare evidente come l'inclusione delle **piattaforme digitali** sia ormai una componente irrinunciabile nelle attività di **communication e governance del rischio** nelle fasi di qualsiasi emergenza; pur tuttavia, rimane assolutamente necessaria la supervisione dei *social network* da parte delle istituzioni preposte, in modo tale da organizzare, ottimizzandolo, il grosso delle informazioni provenienti dal campo, affinché tutti i dati e le notizie raccolte vengano preventivamente analizzate, avendo

così la garanzia di restituire ai cittadini, informazioni tempestive, verificate e il più possibile dettagliate, ma soprattutto utili per raggiungere una concreta mitigazione del rischio, sviluppando nel contempo, una reale cultura di protezione civile supportata positivamente dall'azione informativa della cittadinanza.



per ricevere aggiornamenti sulle
prossime iniziative. Seguici sui canali
social: [Linkedin](#), [Facebook](#), [Twitter](#)

