Il ruolo del security manager

Umberto Saccone
Direttore della Security dell'ENI.

1. La security aziendale e la figura del security manager

La legge sulla privacy, il modello 231, il codice etico, il T.U. n. 81 del 2008, i riferimenti ai codici (civile e penale) ed alla giurisprudenza (sentenze della corte costituzionale, della magistratura ordinaria e del lavoro), le normative relative al codice I.S.P.S.(1) ed all'A.D.R.(2), il problema delle Infrastrutture Critiche, le previsioni relative al segreto di stato, l'aderenza agli standard, i principi di sostenibilità, rappresentano un quadro di riferimento unitario che, attraverso un corretto processo di Security Risk Management (SRM), permette una sintesi tra norme, attività, esigenze aziendali ed esigenze statuali.
Il concetto di SRM sta a indicare quella qualità, in tutti gli aspetti della gestione, che garantisce correttezza, trasparenza, legalità, controllo e verificabilità, finalizzate non solo alla difesa degli interessi degli azionisti di riferimento, ma anche di tutti gli stakeholder. Nell'ambito delle componenti del SRM, l'analisi dei rischi assume un ruolo di rilievo che, unitamente alle vulnerabilità registrate, contribuisce a fornire gli elementi necessari alla mitigazione dei rischi stessi ed al soddisfacimento degli obblighi imposti alla funzione della Security Aziendale.
Qualsiasi decisione strategica importante, quale l'apertura di nuovi mercati o l'istituzione di nuovi insediamenti, le innovazioni che possono influenzare la qualità della vita dei dipendenti o i progetti d'ingegneria complessi, devono essere accompagnati da un processo di analisi e da una valutazione dei possibili danni che colpirebbero non solo gli azionisti di riferimento, ma anche le altre categorie interessate.
È quasi superfluo accennare al fatto che quando un'azienda si espande e conquista nuovi territori - in senso letterale e in senso metaforico - è necessario che la funzione di Security segua l'espansione e si evolva anch'essa. Anche se il compito principale della predetta funzione, di fatto, non subisce variazioni - ovvero rimane quello di analizzare i rischi e di gestirli in modo proattivo e, laddove necessario, reattivo - tuttavia occorre che essa si munisca degli strumenti propri della Corporate Social Responsability (CSR) per potersi confrontare con un ambiente la cui complessità cresce costantemente.
Se si considerano i territori il cui livello di rischio è classificabile come sensibile(3), e nei quali la Security diventa il canale di comunicazione principale fra la società e gli esponenti delle comunità locali - che diventano quindi dei portatori di interesse di primaria importanza - allora quanto sopra detto assume un rilievo inedito.
I comportamenti e le azioni messi in atto dal Security Manager diventeranno, infatti, il metro di paragone mediante il quale le comunità autoctone giudicheranno l'azienda nel suo complesso e stabiliranno se costei è un interlocutore con cui collaborare o, invece, un nemico da contrastare.
Questo è vero a maggior ragione laddove la Security ha anche il compito di mantenere i contatti con le forze dell'ordine e le agenzie di sicurezza. Anche sotto questo profilo è necessario che la funzione del Security Manager sia portatrice dei valori e dei comportamenti etici dell'azienda.
Obiettivo centrale di ogni programma di CSR proprio delle aziende è lo sviluppo socio-economico delle aree nelle quali esse operano. A livello sociale, si tratta di creare possibilità di impiego per gli autoctoni, obiettivo che sarà centrale nella valutazione dell'azienda da parte delle comunità. Sotto questo risvolto, la Security sarà incaricata di fare le idonee verifiche sul personale locale che si vuole reclutare, ma anche di fornire le più importanti informazioni al personale espatriato o in missione. Dovrà, però, anche diramare la cultura aziendale presso le nuove leve autoctone. Pertanto, i Security Manager dovranno conoscere molto bene i posti nei quali l'azienda è radicata, per capire i meccanismi interni dell'area - spesso sottili e mal percepibili da chi non appositamente formato - e, al contempo, farsi portavoce dei valori, della filosofia e dell'etica aziendale.
Nel suo specifico dominio, la Security richiede pertanto una forte componente di Governance dove l'analisi dei rischi è l'elemento centrale per assicurare che i sistemi di protezione progettati e attuati siano coerenti con le minacce pertinenti e le relative probabilità di accadimento, nonché con i vincoli legali esistenti.
È in tale ambito che in aderenza alle previsioni di legge si deve collocare un sistema di gestione della sicurezza strutturato ed omogeneo. Tale sistema di gestione è, di fatto, l'elemento abilitante del SRM. Esso mette a disposizione un sistema organico che costituisce la trama operativa in grado di correlare obiettivi, attività e strumenti, facilitando le attività di gestione, coordinamento e controllo della Security.
Il SRM viene quindi abilitato dal fatto che le decisioni possono essere prese sulla base di informazioni che risultano consistenti ed affidabili proprio in quanto originate da processi noti, stabili e misurabili. Le linee guida di Corporate Governance si indirizzano precipuamente all'identificazione di più ampie aree di rischio, cercando di includere tutti gli eventi relativi a violazioni della sicurezza che potrebbero avere conseguenze sull'azienda.
Solo un processo sistematico di analisi dei rischi consente di considerare gli elementi descritti e di definire in modo proattivo le misure da adottare. Infine, un processo costantemente attivo di analisi consente di avere sempre disponibile l'evidenza della consistenza del sistema di protezione attuato e la possibilità di monitorarlo a soddisfacimento delle esigenze di protezione aziendale.
Elemento pregnante è comunque quello di assicurare il rispetto delle norme di legge vigenti. In tale contesto l'analisi dei rischi deve considerare i vincoli imposti da leggi e norme che, in taluni casi, prevedono responsabilità anche di carattere penale per i contravventori. Pertanto nel SRM gioca un ruolo attivo la capacità, propria solo di un professionista della Security, di coniugare le norme vigenti in un contesto unitario, a tutela dell'azienda e nel rispetto dell'interesse pubblico.

2. Normativa di riferimento

a. La tutela della privacy (D. Lgs. 196/2003)

La normativa impone esplicitamente l'effettuazione e la documentazione di un'analisi dei rischi e al punto 19 dell'Allegato B ("Disciplinare Tecnico in Materia di Misure Minime di Sicurezza") sancisce l'obbligatorietà della redazione di "un documento programmatico sulla sicurezza contenente idonee informazioni riguardo", tra l'altro, "l'analisi dei rischi che incombono sui dati" (punto 19.3).
Si osservi che i dati cui si riferisce la norma sono i dati personali di cui l'azienda è titolare e che tali dati nella maggioranza dei casi non coincideranno completamente con le informazioni aziendali da proteggere, poiché critiche per l'azienda stessa. Inoltre i rischi da considerare nell'ambito della legge differiscono da quelli considerati a fini aziendali. Infatti, l'obiettivo del Codice, come definito all'art.1, è quello di garantire il "rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali". Pertanto, i rischi considerati dalla legge sono quelli che potrebbero ledere tali diritti e, specificatamente, come definito all'art. 31:
- di distruzione o perdita, anche accidentale, dei dati stessi;
- di accesso non autorizzato;
- di trattamento non consentito o non conforme alle finalità della raccolta.

Rischi, analisi dei rischi e piani di sicurezza richiedono necessariamente un approccio sistematico attraverso un processo di SRM, proprio di una struttura di Security Aziendale.

b. La responsabilità amministrativa (D.Lgs. 231/2001)

Il Decreto Legislativo 8 giugno 2001 n. 231 ha introdotto una disciplina inedita in Italia. Sostanzialmente, il D.lgs. 231 ha superato l'affermazione che "societas delinquere non potest" e ha introdotto una forma di responsabilità amministrativa dell'impresa(4), come conseguenza dei comportamenti illeciti di soggetti ad essa legati, messi in atto allo scopo di favorire l'ente. Inoltre, essa ha messo decisamente in risalto le funzioni aziendali della Security e dell'internal audit, che in altri paesi, soprattutto quelli anglosassoni, da tempo godono di ben maggiore prestigio e lustro.
Una corretta articolazione delle suddette funzioni, infatti, è necessaria affinché l'impresa si doti di un modello di organizzazione e di gestione idoneo a prevenire la commissione dei reati riportati nel D.lgs. 231 e che, quindi, esprima una forza esimente nei confronti del giudizio di responsabilità dell'ente.
È importante rilevare che il D.lgs. 231 non ha abolito la responsabilità (penale) individuale in capo a chi materialmente ha compiuto il fatto reato: tuttavia, ha ricondotto una specifica responsabilità nei confronti dell'azienda quando gli illeciti sono commessi - come già anticipato - a favore o a vantaggio dell'ente (art. 5) da soggetti in posizione apicale (ovvero i vertici aziendali) e/o da persone che invece ricoprono un ruolo sottoposto, da lavoratori autonomi o da consulenti.
La responsabilità per la società non si configura, invece, laddove i soggetti di cui sopra abbiano agito per finalità proprie o di terzi. Il D.Lgs. 231 estende la sua tutela anche in materia di contrasto alla criminalità organizzata. Quest'ultima è, infatti, sicuramente una delle minacce da cui le aziende devono difendersi.
Negli ultimi anni le tradizionali configurazioni criminali organizzate - mafia, 'ndrangheta e camorra - sono state inoltre affiancate da altre associazioni a delinquere. Sia le tre storicamente più antiche, sia le nuove associazioni sono caratterizzate dalla transnazionalità.
In questo contesto, la lotta a tali forme criminali necessita di strumenti incisivi e di strategie integrate. L'allargamento della 231 fino a ricomprendere fra i reati da essa sanzionati anche quelli legati alle ipotesi associative - in particolare quella di stampo mafioso - trova riferimento nella Decisione quadro 2008/841/GAI del 24 ottobre 2008 relativa alla lotta contro la criminalità organizzata.
La predetta decisione quadro, ha come scopo preminente il miglioramento delle azioni comuni dell'Unione Europea e dei suoi Stati membri al fine di contrastare la criminalità organizzata transnazionale mediante l'adozione di una strategia comune. Con gli articoli 5 e 6 della Decisione quadro 2008/841/GAI viene introdotta la responsabilità delle persone giuridiche per i reati relativi riconducibili alla criminalità organizzata.
In particolare, l'articolo 5 individua che gli enti dotati di personalità giuridica possano essere ritenuti responsabili per i reati di cui sopra quando essi sono stati commessi a loro beneficio da un soggetto in posizione apicale ovvero da un subordinato qualora il fatto avvenga per una mancanza organizzativa o di controllo. Questa non è l'unica analogia con il D.lgs. 231 del 2001, dal momento che al comma 3 dell'articolo 5 della Decisione quadro si rileva che la responsabilità dell'ente non esclude la responsabilità penale degli autori materiali dei reati.
Ulteriori somiglianze si rilevano per quanto concerne le pene applicabili alle persone giuridiche (art. 6). In primo luogo viene precisato che le pene devono essere effettive, proporzionate e dissuasive, comprendenti sanzioni pecuniarie e di altra natura.
Sulla base della Decisione Quadro, l'articolo 2, comma 29 della legge del 15 luglio 2009, n. 94, ha inserito nel D.lgs. 231 l'articolo 24-ter, ampliando la responsabilità degli enti anche ai delitti di criminalità organizzata.
In particolare, soprattutto per la realtà italiana, sono di estrema importanza le associazioni di tipo mafioso, descritte dall'articolo 416-bis, comma 3, del Codice Penale: "l'associazione è di tipo mafioso quando coloro che ne fanno parte si avvalgono della forza di intimidazione del vincolo associativo e della condizione di assoggettamento e di omertà che ne deriva per commettere delitti, per acquisire in modo diretto o indiretto la gestione o comunque il controllo di attività economiche, di concessioni di autorizzazioni, appalti e servizi pubblici per realizzare profitti o vantaggi ingiusti per sé o per altri ovvero al fine di impedire od ostacolare il libero esercizio del voto o di procurare voti a sé o ad altri in occasione di consultazioni elettorali".
È importante considerare anche il profilo giuridico del reato di concorso esterno in associazione mafiosa. Esso mira a colpire le articolazioni della mafia, della camorra, della 'ndrangheta nei campi dell'economia e della politica e gli influssi su essi esercitati.
Il rischio più concreto relativo ai rapporti fra mafia e aziende è, infatti, rappresentato dalle infiltrazioni delle cosche nelle piccole imprese, e nel sistema degli appalti e delle forniture, prevalentemente ma non solo nel sud del Paese. In particolare si segnalano:
- le infiltrazioni nella fase di predisposizione dei bandi di gara;
- le offerte anomale;
- gli accordi di cartello;
- i subappalti non autorizzati.

La funzione di Security deve essere pertanto costantemente impegnata nell'attività di studio, sviluppo e attuazione delle strategie, delle politiche e dei piani operativi volti a prevenire e superare ogni comportamento colposo o doloso che potrebbe provocare danni diretti o indiretti alle persone e/o alle risorse materiali e immateriali dell'azienda.
La Security è la funzione che, in costante raccordo con le autorità, cerca di soddisfare i diritti costituzionalmente rilevanti creando una bilanciata e fattiva sinergia tra pubblico e privato.

c. Sicurezza sui luoghi di lavoro (D.Lgs. 81/2008).

L'omessa adozione da parte del datore di lavoro delle misure idonee a proteggere il lavoratore dai rischi connessi allo svolgimento dell'attività lavorativa comporta a carico dell'Amministratore Delegato della società o del Responsabile della sicurezza dell'unità produttiva precise responsabilità civili e penali.
La giurisprudenza civile e penale è sempre più orientata nel considerare connessi all'attività lavorativa non solo i rischi tipici della materia antinfortunistica, ma anche i rischi atipici, ovvero quelli che possano scaturire da attività criminose di terzi di varia natura, comprese quelle terroristiche. A livello applicativo, tale principio comporta l'impossibilità per il datore di lavoro di escludere la sua responsabilità civile e penale anche nel caso in cui il danno subito dal lavoratore sia la conseguenza di azioni commesse da terzi e, pertanto, teoricamente al di fuori della sua sfera di controllo (es. attentato/aggressioni).
Dal punto di vista penalistico, i profili di responsabilità sono molto gravi essendo configurabile un'imputazione per omicidio colposo per omissione aggravato, con pena da uno a cinque anni di reclusione (art. 589 c.p; art. 40.2 c.p). La responsabilità penale per l'omessa adozione delle misure idonee a proteggere il lavoratore dai rischi connessi allo svolgimento dell'attività lavorativa deriva dalla posizione di garanzia che assume il datore di lavoro nei confronti del lavoratore e che si sostanzia nell'obbligo giuridico di proteggere i lavoratori da tutti i rischi connessi allo svolgimento dell'attività lavorativa (art. 15 d.lgs. 81/'08). Tale obbligo è stato interpretato dalla giurisprudenza in modo molto ampio, volto a comprendervi tutte le attività finalizzate alla prevenzione e contenimento dei rischi, tenuto conto del contesto ambientale in cui si svolge l'attività lavorativa. Al fine di escludere la sua responsabilità, il datore di lavoro non potrà dunque limitarsi a dimostrare di aver adottato generiche misure di sicurezza, ma gli sarà richiesto di fornire la prova di aver svolto tutte le indagini utili a rilevare i rischi cui erano esposti i propri lavoratori in un determinato contesto e di aver adottato le conseguenti idonee misure.
Al comma 1 della predetta norma viene inequivocabilmente riportato che il datore di lavoro deve eseguire una valutazione di tutti i rischi, concetto ripreso e ampliato nell'articolo 28.
La valutazione dei rischi deve culminare con la redazione di un documento di valutazione dei rischi (DVR) che, oltre a una relazione sulla valutazione stessa, e insieme alla esplicitazione dei criteri adottati per eseguirla, deve riportare anche le misure di prevenzione e di protezione attuate e quelle da implementare nel tempo. "Tutti i rischi", però, è una formula vaga che viene ulteriormente precisata. Nel Testo Unico 81, infatti, si legge che devono essere presi in considerazione tutti i "rischi connessi" all'attività lavorativa. Tale ampliamento conferma viepiù quanto sostenuto fino ad ora: se oggetto della valutazione del rischio devono essere tutti i "rischi connessi" con l'attività lavorativa e non più solo quelli "a causa" dell'attività lavorativa (locuzione invece utilizzata nella 626/94), allora è chiaro il riferimento non solo ai rischi tipici, ma anche a quelli atipici, compresi quelli legati a possibili atti di terrorismo.
Anche per quanto concerne la compilazione del DVR occorre un approfondimento: sebbene la responsabilità sia in capo unicamente al datore di lavoro, ciò non significa che sia costui a dover fisicamente scrivere il documento. Il datore di lavoro soventemente non dispone delle competenze tecniche e specialistiche necessarie alla corretta e completa valutazione dei rischi, e perciò il DVR può e deve essere compilato con l'ausilio di esperti. Il datore di lavoro, tuttavia, firmando il DVR, si assume la paternità del documento.
Secondo alcuni orientamenti di giurisprudenza, infatti, il datore di lavoro deve scegliere dei collaboratori con delle capacità specifiche in materia di tutela e di protezione dei lavoratori.

d. Il codice ISPS

La materia è disciplinata dalla normativa internazionale emessa dall'Agenzia delle Nazioni Unite IMO (International Maritime Organization) nel dicembre 2002, che ha emendato la Convenzione SOLAS sulla salvaguardia della vita umana in mare e ha introdotto un nuovo Codice di Security denominato ISPS Code (International Ship & Port Facility Security Code) destinato a regolamentare l'applicazione dei principi di Security sia sulle navi che nei porti. Tale norma, recepita e fatta propria da tutti gli Stati membri - compresa l'Italia, è entrata in vigore dal 1° luglio 2004.
A ciò si è aggiunto il Parlamento Europeo il quale, nel marzo 2004, ha emesso un proprio Regolamento, n. 725/2004, con cui viene disciplinato in maniera più incisiva il mondo della navigazione nell'ambito dei paesi dell'Unione Europea. Per migliorare la procedura e fronteggiare il fenomeno terroristico, il parlamento europeo ha emanato la Direttiva 2005/65/CE ripresa dal governo italiano con il Decreto Legislativo 6 novembre 2007 n. 203.
Il concetto di security introdotto in questo settore si basa sulla necessità che, per garantire livelli di sicurezza idonei a contrastare analoghi livelli di minaccia, le navi ed i porti siano adeguatamente organizzati, protetti e collegati tra loro da un processo di comunicazione che consenta la circolazione delle informazioni relative allo stato di sicurezza fornite dalle Autorità di Governo preposte.
In sostanza, le Compagnie di navigazione e le imprese che gestiscono gli impianti portuali, per essere dichiarati conformi alla legge, hanno dovuto:
- istituire e formare la figura del Responsabile societario di security (Company Security Officer);
- istituire e formare la figura del Responsabile di sicurezza per ciascuna nave (Ship Security Officer) e per ciascun impianto portuale (Port Facility Security

Officer);
- realizzare e mettere in atto un piano di security per ciascuna nave e per ciascun impianto;
- assicurare la realizzazione di tutte quelle misure protettive e procedurali indicate in ciascun piano per definire il controllo del perimetro, la videosorveglianza, la disciplina del controllo accesso nelle aree comuni e nelle aree riservate, il controllo delle merci e dei bagagli e tutte le procedure di pronto intervento per gestire al meglio le eventuali emergenze.

e. La normativa ADR

La normativa ADR (European Agreement Concerning the International Carriage of Dangerous Goods by Road)(5) è una delle normative internazionali che regolano, in Italia e in Europa, il trasporto di merci pericolose.
Con tale locuzione s'intendono tutte quelle materie il cui trasporto è vietato o autorizzato soltanto secondo delle condizioni espressamente previste. L'accordo vero e proprio, composto di 17 articoli, è stato sottoscritto dai vari paesi a partire dal 1957 ed è stato recepito in Italia con la legge n. 1839/62. Quelle che normalmente sono state chiamate "Norme ADR" sono contenute negli Allegati tecnici, che sono oggetto di aggiornamento periodico con cadenza biennale.
A seguito degli eventi dell'11 settembre 2001 i legislatori internazionali hanno ritenuto necessario introdurre e attuare misure di sicurezza contro il possibile rischio di terrorismo, e questo anche per quanto riguarda il trasporto di merci pericolose. È per questo motivo che, nell'edizione del 2005 dell'ADR, sono stati presi in considerazione, per la prima volta, gli aspetti di Security delle merci pericolose per evitare usi impropri delle stesse. Infatti, in tale edizione viene introdotto il Capitolo 10.1 "Disposizioni concernenti la security", in uno degli allegati tecnici (Allegato A), successivamente riproposto poi nelle edizioni del 2007 e del 2009 della normativa ADR.
Per security, ai fini del capitolo in questione, si intendono le misure o le precauzioni da prendere per minimizzare il furto o l'utilizzazione impropria di merci pericolose che possano mettere in pericolo le persone, gli asset fisici o l'ambiente.
Tali disposizioni sono obbligatorie per tutte le parti coinvolte nella catena di trasporto, in aggiunta alle consuete misure di sicurezza tecnica e antinfortunistica. Il procedimento di attuazione delle suddette misure dipende da circostanze proprie dell'impresa, dalla valutazione dei rischi e dai possibili esiti.
Nella sezione 1.10.3 vengono introdotte norme specifiche e più onerose per quelle merci particolarmente pericolose perché comportano un maggiore rischio potenziale, facendo riferimento non solo a un loro uso improprio in generale e ai pericoli connessi, ma più specificatamente a un uso a scopi terroristici e alle gravi conseguenze che da esso potrebbero derivare.
Il capitolo relativo alla security è suddiviso in cinque sezioni: in questa sede verranno evidenziate le prime tre, i cui argomenti vanno dalle disposizioni generali, alla formazione sulla security a disposizioni concernenti le merci pericolose ad alto rischio.
La prima delle predette sezioni detta una serie di regole riguardo alle persone coinvolte nel trasporto di merci pericolose e alle aree di stoccaggio temporaneo delle merci stesse. In particolare, si segnala la necessità che ogni persona coinvolta sia a conoscenza dei rischi derivanti da un uso improprio delle merci pericolose. Inoltre, le imprese devono assicurare la responsabilità e l'affidabilità del personale impiegato. Per tale motivo, è necessario che esse dispongano di una documentata evidenza dell'esperienza di ciascun addetto.
La seconda sezione ha come oggetto la formazione sulla security. Le imprese, in definitiva, sono tenute a formare il proprio personale - e a organizzare moduli di aggiornamento - per quanto concerne la natura dei rischi di security, il riconoscimento di questi ultimi, come minimizzarli e come agire di fronte a falle o a carenze nel sistema di sicurezza. Inoltre, devono essere predisposti appositi approfondimenti sui comportamenti appropriati in caso di attacco o di dirottamento.
La terza sezione, invece, tratta specificatamente delle merci pericolose considerate ad alto rischio, ovvero quelle utilizzabili a fini terroristici e il cui uso improprio potrebbe avere effetti devastanti in termini di perdita di vite umane o distruzioni di massa. In questa fase, obbligo primo in capo a trasportatori e spedizionieri è quello di redigere e mettere in atto un piano di security basato sulla situazione generale dell'impresa e non sui singoli trasporti. Più in dettaglio, il piano di sicurezza deve essere formulato sulla base dell'identificazione delle tipologie di minacce. Successivamente devono essere identificate le sostanze che devono essere protette e, in particolare, deve essere valutata la vulnerabilità a un attacco terroristico. L'ultima fase consiste nel prendere in considerazione le azioni necessarie per ridurre il rischio a un livello accettabile.
La redazione dei piani non è però sufficiente: essi devono anche essere realizzati e scrupolosamente seguiti, essere periodicamente rivisti e aggiornati, laddove necessario, e testati a intervalli regolari.
Riguardo al contenuto dei piani, la normativa ADR individua gli elementi che devono essere obbligatoriamente contenuti:
- precisa attribuzione di responsabilità a persone competenti, qualificate e dotate della necessaria autorità;
- registrazione delle merci pericolose o delle loro tipologie;
- valutazione delle modalità operative contingenti e dei rischi per la security connessi al processo di trasporto;
- chiara definizione delle misure da adottare per ridurre i rischi relativi alla security;
- procedure efficaci ed aggiornate per fronteggiare le minacce;
- procedure di verifica e di valutazione dei piani di security
- misure per assicurare la tutela fisica delle informazioni relative al trasporto;
- procedure che assicurino che le informazioni vengono fornite agli addetti ai lavori sulla base del principio della "necessità di conoscere".

f. Le infrastrutture critiche Europee

È nuovamente la lotta al terrorismo che ha portato il Consiglio dell'Unione Europea a emanare una Direttiva, la n. 2008/114/CE, in tema di Infrastrutture Critiche. Con tale termine s'identificano i sistemi, le risorse e i processi la cui distruzione, interruzione o anche parziale o momentanea indisponibilità ha l'effetto di indebolire in maniera significativa l'efficienza e il funzionamento normale di un Paese, ma anche la sicurezza e il sistema economico-finanziario e sociale, compresi gli apparati della Pubblica Amministrazione centrale e locale. In altre parole, le infrastrutture critiche sono quelle che consentono l'erogazione dei servizi che caratterizzano la vita dei paesi occidentali. La loro esistenza e corretta funzionalità è sinonimo di necessità di salvaguardare la qualità della vita. L'interdipendenza fra le strutture non fa solo sì che le IC siano fra loro strettamente interrelate: obbliga, di fatto, che lo siano anche le misure poste per la loro protezione. La cooperazione, la comunicazione e la coordinazione non sono solo degli obiettivi da raggiungere a livello nazionale: essi diventano fondamentali quando si considera il contesto comunitario.
Al fine di incrementare il livello di protezione delle infrastrutture critiche, sia nazionali sia europee, diversi sono gli obblighi cui devono sottostare i Paesi della UE e gli operatori/ i proprietari delle ECI che ivi sono collocate. Per ogni infrastruttura, infatti:
- deve essere formulato un "Piano di Sicurezza per gli Operatori" (Operator Security Plan - da qui PSO). La Direttiva fornisce un'indicazione dei contenuti minimi che dovranno essere trattati nel piano; in particolare, il PSO deve identificare i beni dell'infrastruttura critica e le soluzioni in atto o in corso di implementazione per la loro protezione. Lo scopo di questo piano consiste nell'identificare quegli asset che soddisfano i requisiti per essere denominati "Infrastrutture Critiche Europee". In seguito, occorrerà proporre e implementare soluzioni che ne permettano una capillare ed efficace protezione. In particolare il piano dovrebbe prevedere:
• un momento di identificazione degli asset importanti;
• una fase di risk assessment, durante la quale si devono prendere in considerazione gli scenari riguardanti le minacce più probabili;
• la progettazione e la messa in atto delle procedure e delle misure di prevenzione e protezione;
- deve essere nominato un Funzionario di Collegamento in materia di Security (Security Liaison Officer, o SLO). Lo scopo di tali funzionari, sarà quello di facilitare la cooperazione e la comunicazione con le autorità nazionali competenti in materia di protezione delle IC. La loro presenza è, però, essenziale, dal momento che, come ribadisce la Linea Guida all'implementazione della Direttiva, la loro presenza è il prerequisito per poter formulare il PSO. Non è specificato qual è la tempistica massima entro la quale nominare il Funzionario; egli deve però essere in carica in tempo per preparare il PSO entro la scadenza dei termini prevista per quest'ultimo.

g. Le previsioni relative al segreto di stato

Il 16 aprile 2008 sono entrate in vigore, a seguito della pubblicazione in Gazzetta Ufficiale, le nuove norme in materia individuazione di informazioni, documenti, atti, attività e luoghi suscettibili di essere oggetto di segreto di Stato.
È quanto contenuto nel Decreto del Presidente del Consiglio dei Ministri 8 aprile 2008 il quale, "in attuazione dell'art. 39 della legge 3 agosto 2007, n. 124, disciplina i criteri per l'individuazione delle notizie, delle informazioni, dei documenti, degli atti, delle attività, delle cose e dei luoghi suscettibili di essere oggetto di segreto di Stato, nonché individua gli uffici competenti a svolgere, nei luoghi coperti da segreto di Stato, le funzioni di controllo ordinariamente svolte dalle aziende sanitarie locali e dal Corpo nazionale dei vigili del fuoco".
In particolare, il provvedimento stabilisce che potranno essere oggetto del segreto di Stato le notizie, le informazioni, i documenti, gli atti, le attività, i luoghi

e ogni altra cosa la cui diffusione sia idonea ad arrecare un danno grave a interessi supremi da difendere con il segreto di Stato.
Rilevante novità del provvedimento è costituita dalla possibilità, ferma restando la necessità di valutare in concreto ogni singolo caso, di richiedere l'apposizione del segreto di Stato a notizie, documenti etc., attinenti agli impianti civili per la produzione di energia (ad es. siti per il deposito delle scorie nucleari, centrali nucleari, rigassificatori e inceneritori) ed altre infrastrutture critiche. Il segreto si estende anche agli iter autorizzativi, di monitoraggio, di costruzione e della logistica. Si ricorda, inoltre, che l'articolo 261 del Codice penale prevede, per chi rivela un segreto di Stato, una pena non inferiore ai cinque anni di reclusione.
Di là da ogni possibile valutazione che coinvolga il merito, il provvedimento rappresenta un utile spunto di riflessione dal punto di vista di una possibile sottoposizione a segreto di Stato d'infrastrutture energetiche qualificate come critiche. Tal eventualità appare più che mai concreta se si riflette sull'importanza che sta assumendo a livello nazionale ed europeo la protezione delle infrastrutture critiche, anche energetiche.
D'altra parte, la protezione di alcune di queste infrastrutture, si pensi ai rigassificatori, ben potrebbe coniugarsi con l'esigenza di tutelare supremi interessi dello Stato.
Occorre a questo punto evidenziare come la sottoposizione a segreto di Stato di un'infrastruttura critica di proprietà o detenuta dall'azienda, avrebbe evidenti riflessi in tema di security (controllo accessi, rilascio dei NOS, etc.) e a questo riguardo appare opportuno compiere un successivo sforzo, finalizzato a una valutazione preventiva sull'implementazione, specie nei siti più critici, di adeguate misure di sicurezza. Se tale valutazione, infatti, si presenta oggi necessaria, la stessa diventa imprescindibile per quelle infrastrutture che, domani, potrebbero essere oggetto di segreto di Stato.
Il primo punto decisivo che connette la legge 124/2007 con le tematiche di security è contenuto nell'allegato del Decreto del Presidente del Consiglio dei Ministri emanato nell'aprile del 2008 che riporta i criteri per l'individuazione delle notizie, delle informazioni, dei documenti, degli atti, delle attività, delle cose e dei luoghi suscettibili di essere oggetto di segreto di Stato, che, al 17esimo punto, riporta come a "gli stabilimenti civili di produzione bellica e gli impianti per la produzione di energia e altre infrastrutture critiche" possa essere apposto il segreto. Nel medesimo allegato, al comma 17, viene riportato che qualunque cosa, luogo, evento, informazione ecc. coperto dal segreto deve essere dotato di specifiche misure di sicurezza.
Fondamentale anche il Decreto del Presidente del Consiglio dei Ministri del 3 febbraio 2006 "Norme unificate per la protezione e la tutela delle informazioni classificate", dove vengono individuati i compiti del Funzionario alla Sicurezza, mediante il combinato disposto degli articoli 27 e 29.
Con specifico riguardo al Capo VI del predetto DPCM, "Tutela delle informazioni classificate nel settore industriale" l'articolo 27 "Responsabilità della protezione e della tutela delle informazioni classificate nell'ambito delle imprese" attribuisce la relativa responsabilità al Rappresentate Legale dell'impresa, prevedendo, in realtà societarie complesse e articolate, la possibilità di delegare tale responsabilità, con l'esercizio dei compiti e delle funzioni in materia di protezione e tutela delle informazioni classificate ad un Funzionario, di elevato livello gerarchico ed adeguatamente abilitato ai fini della sicurezza, che assume la denominazione di Funzionario alla Sicurezza.
Il successivo articolo 29 "Compiti del Funzionario alla Sicurezza della sede principale od unica dell'impresa" disciplina le attribuzioni e le relative competenze di tale figura, elencando dettagliatamente compiti e responsabilità.
Il combinato disposto di questi due articoli, con esame connesso tra responsabilità dell'impresa nella tutela delle informazioni classificate e compiti attribuiti in materia al Funzionario alla Sicurezza, induce ad affermare che, in realtà societarie complesse, articolate e rilevanti per dimensioni, fatturato ecc la necessità di visione di insieme delle attività di tutela poste in essere dalla Funzione aziendale della Security e l'esigenza di rapporti verso le istituzioni del comparto in maniera unitaria fa ritenere funzionale ed opportuno che l'incarico di Funzionario alla Sicurezza possa essere espletato dal Security Manager della Società.
h. Gli standard internazionali

L'attività di normazione consiste nell'elaborare documenti tecnici che, pur essendo di applicazione volontaria, forniscano riferimenti certi agli operatori e possano pertanto avere una chiara rilevanza contrattuale. A volte l'argomento trattato dalle norme ha un impatto così determinante sulla sicurezza del lavoratore, del cittadino o dell'ambiente che le Pubbliche Amministrazioni fanno riferimento ad esse richiamandole nei documenti legislativi e trasformandole, quindi, in documenti cogenti. In ogni caso, a mano a mano che si diffonde l'uso delle norme come strumenti contrattuali e che, di conseguenza, diventa sempre più vasto il riconoscimento della loro indispensabilità, la loro osservanza diventa quasi "imposta" dal mercato. In tale contesto è evidente che l'attività normativa nazionale si sta via via limitando a temi più specificatamente locali o non ancora prioritari per studi sovranazionali e sta sempre più organizzando le proprie risorse per contribuire alle attività europee ed internazionali. Oggi l'attività di normazione ha per oggetto anche la definizione dei processi, dei servizi e dei livelli di prestazione. Non solo: oggi la normazione si occupa anche di definire gli aspetti di sicurezza, di organizzazione aziendale (UNI EN ISO 9000) e di protezione ambientale (UNI EN ISO 14000), così da tutelare le persone, le imprese e l'ambiente. O come la già citata norma UNI 10459 che norma la Security e la figura professionale del Security Manager(6). Tale norma assume più vigore laddove ne è ripresentata la centralità nel sistema di sicurezza aziendale, quando si rimanda a essa nella norma UNI 10891 che regola gli Istituti di Vigilanza Privata. Valenza internazionale assume poi la figura del Security Manager quando ne è tracciato il ruolo negli standard internazionali, fra cui l'australiano ASZ(7), che norma il Security Risk Management.

3. La security in ottica di sostenibilità

La Security, nell'ambito delle competenze attribuitele allo scopo di tutelare da minacce esterne il personale, gli asset societari, le informazioni e il Know-how dell'azienda, deve analizzare e implementare le soluzioni più idonee, di tipo sia organizzativo sia tecnologico, nel pieno rispetto dei principi di Sostenibilità in ambito nazionale ed estero. L'aggiornamento costante delle condizioni di Security in tutte le realtà operative aziendali, l'adozione di adeguate misure protettive e la gestione delle opportune iniziative di comunicazione, in coordinazione con quelle logistiche a supporto del personale e dei familiari, rappresenta, dunque, obiettivo primario del complesso delle attività di Security.
Gli indicatori di criticità continuano a disegnare scenari che potrebbero avere diretta incidenza sugli ambiti aziendali, e il personale operante nei paesi cosiddetti a rischio può essere tra gli obiettivi di questa minaccia. L'impatto di eventuali azioni contro tali interessi figura nelle agende internazionali, dove si cerca, in un'ottica collaborativa, una maggiore sinergia tra pubblico e privato con l'obiettivo di mitigare i rischi inerenti a quelle che possono essere considerate infrastrutture critiche nazionali. È in tale quadro che viene con sistematicità rafforzata la collaborazione con le entità statuali preposte alla sicurezza, in Italia ed all'estero, per rafforzare e migliorare il dispositivo di reazione rispetto alle tipologie di eventi che possono compromettere la stabilità del business, l'integrità delle persone la sicurezza delle infrastrutture.
La partnership pubblico-privato (PPP) è uno dei temi fondamentali su cui si sono impegnate le principali agenzie internazionali che operano nell'ambito della sicurezza. La sua importanza nella lotta al terrorismo è stata chiaramente rilevata nel documento che fissa la strategia globale delle Nazioni Unite contro il terrorismo (The United Nations Global Counter - Terrorism Strategy, 2006). Sulla base di ciò, l'UNICRI (l'istituto di ricerca per il crimine internazionale e la giustizia delle Nazioni Unite) e l'OSCE (Organizzazione per la Sicurezza e la Cooperazione in Europa) hanno dato vita a un progetto congiunto volto a promuovere la collaborazione fra le aziende private e il settore pubblico; il predetto progetto ha come settore di riferimento le infrastrutture critiche che producono energia non nucleare.
La partnership fra il pubblico e il privato promossa dall'OSCE e dall'UNICRI è volta primariamente allo scambio di quelle informazioni che sono vitali per la prevenzione di attentati terroristici diretti contro le predette infrastrutture critiche e che possono migliorare le risposte e gli interventi in caso di attacco.
In questo contesto, nell'ottica promossa dall'OSCE e dall'UNICRI, la figura del Security Manager viene individuata come quella più indicata per interloquire con gli organismi pubblici - nazionali e internazionali - al fine di instaurare la partnership di cui sopra. Essendo parte integrante della struttura aziendale, costui è in grado di comunicare all'esterno le problematiche più rilevanti cui deve fare fronte l'impresa privata, e quindi di indirizzare il legislatore e gli apparati dello Stato nei processi decisionali e nell'adozione delle più efficaci strategie per la tutela del patrimonio aziendale del Paese. Tuttavia, il Security Manager ha anche le conoscenze tecniche necessarie per comprendere appieno le informazioni provenienti dalle agenzie pubbliche, per poterle valutare efficacemente e per attuare le azioni opportune e adeguate in base al contesto di riferimento. Sono infatti definiti una serie di processi e di scambi informativi di dati sensibili che possono essere gestiti solo da un professionista della sicurezza riconosciuto come tale, che sia in grado di parlare "lo stesso linguaggio" dell'Autorità pubblica.
L'obiettivo di mitigazione del rischio, in linea con i principi di sostenibilità, ha reso pregnanti anche per la Security alcuni principi che sono divenuti fondanti, quali il rispetto dei diritti umani e delle best practice internazionali. L'adesione ai Voluntary Principle for Security and Human Rights rappresenta una delle azioni dove assume particolare valenza una corretta gestione della Security.
Questi articolati obiettivi, e questi continui richiami delle norme delimitano un perimetro che, in aderenza agli standard internazionali, richiama forte la necessità di coniugare in un unico ambito specializzato gli aspetti concernenti la Security.
È ormai diffusa la percezione che, negli ultimi anni, ci siano stati drammatici e profondi cambiamenti nella natura del contesto imprenditoriale e nella società in generale. In particolare è stato detto, quasi fino alla nausea, che il mondo è cambiato a partire dall'11 settembre.
Tuttavia, molti di questi 'nuovi cambiamenti' hanno semplicemente evidenziato i problemi che le aziende e le comunità hanno affrontato per molti decenni. È quindi emersa l'imperativa esigenza di considerare questioni che in precedenza non facevano parte della coscienza collettiva. Come società, siamo stati informati della necessità, e dell'esistenza di misure di sicurezza. Quando la sicurezza ha a che fare con la vita lavorativa ordinaria, pero, spesso viene vista come un ostacolo alla routine quotidiana.
Gli atteggiamenti sono però cambiati notevolmente negli ultimi tempi, concentrandosi su una maggiore attenzione alla sicurezza. Eppure, questo cambiamento negli atteggiamenti è spesso guidato da un'errata percezione, alimentata dai media che a volte diffondono una visione eccessivamente

drammatica del contesto di riferimento. Il risultato è che gli investimenti sulla sicurezza potrebbero essere erroneamente indirizzati dove c'è 'caos informativo' e non dove è veramente necessario che siano impiegati.
Una migliore comprensione della natura del rischio favorisce un processo decisionale più informato, aumenta le capacità di sfruttare le opportunità e riduce i danni.
Tradizionalmente, l'industria della sicurezza e l'attenzione delle professioni a rischio, si sono concentrate sulla minimizzazione del rischio, con attività finalizzate alla prevenzione degli infortuni, senza necessariamente considerare a fondo la natura e il livello del rischio.
Oggi bisogna fornire alle aziende i mezzi per prendere decisioni ragionate sulla necessità di migliorare la sicurezza e di utilizzare appropriatamente il budget e le altre risorse per investire in essa.
Nella sua forma più sostanziale, la Security si concreta nella capacità di fornire la struttura e i mezzi per determinare la natura delle minacce, tracciare il 'corso delle vulnerabilità', comprendere le potenziali conseguenze di eventi futuri, e sviluppare un approccio più strategico per queste attività.
Questo approccio è nato per considerare le cause profonde, le pressioni dinamiche e le condizioni pericolose. Il Security Manager deve saper cogliere nella sua analisi dinamica ed olistica le cause profonde, quali ideologie basate su diversi sistemi politici, economici e sociali, negazione dei fondamentali diritti umani e della libertà, aumento della conflittualità sociale e della discordia.
Le pressioni dinamiche come mancanza di istituzioni governative, sociali e locali; ostacoli alle capacità di sviluppo, alle opportunità d'impiego e ai livelli d'investimento.
Le condizioni pericolose, come un ambiente fisico fragile, segmentato da zone pericolose, con edifici non protetti e infrastrutture deboli, condizioni economiche locali variabili, incapacità di gestire le emergenze. È in tali ambiti che bisogna implementare la comunicazione e la consultazione con gli stakeholder interni ed esterni, saper determinare il contesto, strutturare le attività, sviluppare criteri di valutazione.
Avere le conoscenze per poter identificare i rischi, determinare le minacce, individuare gli elementi critici, organizzativi e collettivi, determinare la vulnerabilità di tali elementi alle minacce individuate, identificare specifici eventi e scenari e le loro possibili conseguenze. Saper effettuare una analisi del rischio in grado di valutare i controlli esistenti, determinare le conseguenze derivanti dal concretizzarsi del rischio, determinare le probabilità che da un tale rischio scaturiscano specifiche conseguenze, definire il livello di rischio su una combinazione di conseguenze e probabilità. Ed inoltre poter effettuare una valutazione del rischio per determinarne la tolleranza e l'eventuale necessità di ulteriori trattamenti. Stabilire le raccomandazioni e le strategie per il trattamento dei rischi prioritari, assegnare le responsabilità e verificare l'adeguatezza dei fondi necessari per le attività di trattamento dei rischi per poi iniziare il ciclo di controllo e revisione finalizzato al rilevamento di eventuali cambiamenti.
Revisionare i rischi e le rispettive strategie di trattamento, monitorare e revisionare i progressi compiuti e i risultati di ciascuna delle fasi del processo.
Stiamo parlando di quella cultura aziendale in grado di valutare le strutture e i processi che sono diretti verso la massimizzazione dei benefici e la minimizzazione degli svantaggi in materia di security, compatibilmente con il raggiungimento degli obiettivi di business. Laddove security si definisce come la preparazione, la tutela e la protezione delle persone, dei beni e delle informazioni sia materiali che immateriali.
L'efficace gestione del rischio security è un requisito fondamentale con cui le aziende, gli individui e chi è incaricato della tutela delle nostre comunità deve ora operare.
Ci sono naturalmente una vasta gamma di rischi interni ed esterni all'azienda, agli individui o alla comunità, che vanno al di là delle preoccupazioni relative alla sicurezza. Tuttavia, il rischio security rappresenta una fonte di preoccupazione per i governi, i datori di lavoro, i dipendenti e i cittadini.
L'identificazione del rischio, elemento centrale del processo di risk management riguarda la selezione chiara e ragionevole delle fonti dei rischi e degli eventi che possono potenzialmente avere un impatto sugli obiettivi delle persone, dell'azienda o della comunità. L'identificazione del rischio può essere affiancata dalla considerazione che le conseguenze di approcci più tradizionali come la minaccia, la criticità, la vulnerabilità, possono comunque essere contributi preziosi per il processo di identificazione.
Il processo infatti, sarà più completo una volta sintetizzate queste informazioni, anche se l'identificazione del rischio è molto più di una semplice valutazione separata della minaccia, della criticità, e della vulnerabilità. I termini "minaccia" e "rischio" sono di solito utilizzati alternativamente. Tuttavia, "rischio" non è sinonimo di "minaccia", e anche se i due termini alla fine sono correlati, in realtà sono molto diversi. In molte circostanze una "minaccia" sarà fonte di uno o più rischi. L'interazione della minaccia con qualcuno o con qualcosa, in un preciso momento, o dopo il trascorrere di un certo periodo di tempo, determinerà un rischio. Le minacce possono esistere, ma non necessariamente rappresentano un rischio.
L'esame del contesto di Security, e le considerazioni sulle valutazioni della minaccia, criticità e vulnerabilità, permetteranno di identificare i potenziali rischi. I rischi dovrebbero essere descritti e analizzati nel modo più completo e dettagliato possibile, così da permettere al management di comprendere appieno la situazione.
Il rischio appare come "La possibilità che accada qualche cosa che possa avere un impatto sugli obiettivi."
Questa è una definizione molto importante perché esprime la crescente maturità nel considerare i rischi che si sono concretizzati negli ultimi tempi. L'applicazione di questa definizione allo svolgimento di una professione inerente alla sicurezza, dovrebbe sollecitare a non identificare il rischio solamente con la minaccia, ma a inquadrarlo in una nozione molto più ampia.
Le cause profonde, alle quali facevamo riferimento in premessa possono essere relative a tematiche storiche come il fondamentalismo islamico (vedi il Wahabbismo), le percezioni anti-islamiche, le convinzioni dell'esistenza di cambiamenti nelle democrazie occidentali, le percezioni di un dissesto economico. Da queste cause profonde possono poi sorgere ed innestarsi altri fattori causali come l'antagonismo nei confronti del pensiero occidentale, l'ingiustizia dei regimi governativi occidentali, l'impotenza culturale nei confronti di culture sempre più dominanti.
Questi fattori hanno portato alla creazione di ideologie fondamentaliste, di comportamenti e strutture che diventano minacce o fonti di rischio. Per esempio, la nascita di gruppi islamici come Al-Qaeda, o Jemaah Islamiyah, la costituzione dell'Intifada nei territori palestinesi, il fallimento di società funzionanti o dell'ordine pubblico, in zone come la Somalia, il Sudan, la Sierra Leone, l'Iraq, l'Afghanistan, Papua Nuova Guinea, le Isole Salomone, il Congo, la Colombia, il Nepal. Da queste fonti nasce il rischio, come un attacco mirato a immobilizzare una struttura critica, attacchi saltuari contro la popolazione locale finalizzati a creare il panico e la perdita di fiducia nelle istituzioni, o attacchi (omicidio o rapimento) finalizzati a rimuovere gli elementi chiave del management o i tecnici dell'azienda.
Ciascun rischio dà vita ad una serie di potenziali conseguenze. Se uno dei suddetti rischi dovesse verificarsi - l'evento - allora una o più conseguenze potrebbero verificarsi.
L'identificazione del rischio consiste quindi nel comprendere la natura della minaccia (la fonte di rischio), interagendo con importanti elementi come ad esempio la comunità, gli assetti aziendali, (la cui importanza è espressa attraverso la criticità), e in che modo la natura di questi elementi può facilitare o inibire questa interazione (espressa attraverso la vulnerabilità).
Le informazioni sul contesto, sviluppate nella fase iniziale del processo, forniscono un ideale punto di partenza per individuare la minaccia e il rischio. Tuttavia, questi elementi potrebbero comunque non fornire i dettagli sufficienti per ottenere un'individuazione e un'analisi completa. Un'attività di ricerca più dettagliata potrebbe pertanto essere richiesta per sviluppare un'affidabile individuazione del rischio.
È importante che i dati e le fonti di informazioni siano affidabili e accurati, al fine di fornire l'analisi e la successiva decisione avendo appropriati punti di riferimento e ponderazione. La valutazione della criticità (anche conosciuta come risk assessment), coinvolge l'individuazione degli asset critici (le persone, le proprietà, le informazione e i processi che li supportano) i quali potrebbero essere esposti alla, o danneggiati dalla, minaccia. La valutazione della criticità è un passo vitale per l'identificazione del rischio poiché fornisce il punto di partenza per considerare le minacce pertinenti e la vulnerabilità dell'azienda, della comunità o degli individui, a tali minacce. In molte circostanze, sarebbe difficile e costoso condurre una dettagliata valutazione del rischio per ogni bene, luogo e persona. La valutazione della criticità consente di concentrare l'analisi su quegli asset ritenuti di maggior importanza per l'azienda, per la comunità o per l'individuo.
Si tratta in pratica di una funzione trasversale ad elevata specializzazione che percorre orizzontalmente l'azienda raccogliendo e sistematizzando le norme che presiedono alla funzione e ridistribuendole all'interno dell'azienda in un ciclo continuo di verifica e controllo a soddisfacimento degli stakeholder e degli interessi aziendali coniugando l'eticità dell'impresa in aderenza al principio costituzionale di utilità. Tra l'altro le norme surrichiamate oltre al minimo comune denominatore di poter essere considerate per la loro atipicità rispetto al mondo del lavoro e dei doveri a capo del datore del lavoro, tutte parlano di valutazione del rischio e di piani di sicurezza. Appare pertanto evidente che tutte devono inquadrarsi nella loro unitarietà ed unicità in un contesto di Security Risk Management magnificamente illustrata e dettagliata dalla sopra richiamata norma AS HB 167:2006.

4. Conclusioni

Il legislatore ha colto tutti questi aspetti frammentandoli in varie iniziative legislative con un minimo comune denominatore che percorre tutte le norme esaminate. Infatti, in tutte si parla di analisi del rischio, di prevenzione delle minacce diversificate, di piani di security, di nomina del funzionario alla sicurezza e della necessità di conferire tali attribuzioni di responsabilità a persone competenti qualificate e dotate della necessaria autorità.
Alla luce di quanto tratteggiato, appare evidente che l'intenzione del legislatore sia stata comunque quella di ampliare la portata della normativa italiana in materia di salute e sicurezza sul lavoro per far ricadere sotto il cappello delle leggi sull'argomento anche quegli eventi che si caratterizzano per il loro profilo di atipicità e quindi devono essere inquadrati nell'ambito della security. Tali principi, affermati da una giurisprudenza ormai conclamata, trovano ampio riferimento in norme e standard internazionali (UNI10891, UNI 10459 AS HB 167:2006).
Le leggi, in combinato disposto con le su richiamate norme pongono l'accento su come il legislatore ha di fatto previsto che anche le minacce cosiddette atipiche debbano essere considerate e come su queste debbano essere monitorate da una funzione professionale con le necessarie competenze. La

norma, suffragata da copiosa giurisprudenza di merito e di legittimità, provvede poi a sanzionare quel datore di lavoro che nell'attività di delega individui risorse con competenze non provate.
In questo modo, le norme e la giurisprudenza italiane si allineano alle leggi presenti negli altri paesi occidentali che da diversi anni hanno preso atto dei cambiamenti in tema di sicurezza a livello globale. La sfida che si trova davanti il legislatore nazionale è, nel prossimo futuro, quella di saper cogliere gli spunti che arrivano dalle organizzazioni sovranazionali e dall'Unione Europea. Un'occasione di fondamentale importanza è rappresentata dalla ormai prossima legislazione in tema d'infrastrutture critiche europee. L'OSCE e l'organizzazione Anti terrorismo dell'ONU (UNICRI), nei loro piani di sviluppo connessi alla protezione delle infrastrutture critiche, hanno, infatti, correttamente individuato nella funzione di Security e nel Security Manager in particolare, l'interlocutore obbligato, per conoscenze, competenze, capacità di azione e reazione alle emergenze(8). La tematica della protezione delle infrastrutture critiche, infatti, impone un approccio globale che coinvolga il settore privato non solo nella situazione di crisi, ma anche e soprattutto nella definizione dei piani e delle contromisure idonee a prevenire gli attacchi terroristici. Attività, funzioni e processi che possono essere assolti solo da una ben organizzata struttura di Security aziendale.

Approfondimenti
(1) - International Ship & Port Facility Security Code.
(2) - European Agreement Concerning the International Carriage of Dangerous Goods by Road
(3) - Si pensi, ad. es. all'Iraq, alla Nigeria, al Congo etc.
(4) - Si ricordi che, a norma dell'art. 27 della Costituzione, "la responsabilità penale è personale".
(5) - European Agreement Concerning the International Carriage of Dangerous Goods by Roas - ADR.
(6) - La security è definita come "lo studio, sviluppo ed attuazione delle strategie, delle politiche e dei piani operativi volti a prevenire, fronteggiare e superare eventi in prevalenza di natura dolosa e/o colposa che possono danneggiare le risorse materiali, immateriali, organizzative ed umane di cui l'azienda dispone o di cui necessita per garantirsi un'adeguata capacità concorrenziale nel breve, nel medio e lungo termine.
(7) - HB 167: 2006 - In questa norma si spiega chiaramente come la security sia un indispensabile supporto al business che deve operare in modo sinergico e coordinato con tutte le alte funzioni ma, anche e soprattutto, come sia richiesto che la persona che si occupa di security risk management sia un professionista con una completa padronanza della materia.
(8) - Vds. par. n. 3.