PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 28 - numero 6197 di Mercoledì 18 novembre 2026

Fatto naturale e atto ostile: la doppia anima del piano di emergenza aziendale

Gestione delle emergenze e continuità operativa: come integrare Safety e Security nei piani di emergenza aziendali. Analisi e indicazioni normative. A cura di Antonello Rubino, RSPP

Le recenti ondate di falsi ***allarmi bomba*** *nelle scuole hanno sollevato interrogativi urgenti sulla gestione delle emergenze, portando anche a nuove indicazioni ministeriali. Sul delicato tema ospitiamo un contributo del nostro lettore* ***Antonello Rubino*** *che svolge attualmente l'incarico di RSPP in una Pubblica Amministrazione, ma che ha rivestito incarichi nei Servizi di Prevenzione e Protezione in vari ambiti pubblici e privati. L'autore si sofferma sul tema della gestione di queste tipologie di emergenze e sulla distinzione e integrazione tra Safety e Security, anche con riferimento ad una recente* ***direttiva del Ministero dell'Interno*** *e al* ***Decreto legislativo 2 novembre 2026, n. 208****.*

Pubblicità

Premessa

Che l'inglese disponga di due parole per dire "sicurezza" ? **Safety** e **Security** ? è ormai un leitmotiv di convegni e seminari. Succede, a parti invertite, come con il verbo to play, che l'italiano rende con parole diverse: giocare, suonare, interpretare. Con **Safety** si indica la protezione delle persone e dei beni da eventi non intenzionali: un incendio accidentale, un guasto, un sisma, un infortunio. Con **Security**, la protezione da atti intenzionali e ostili: un furto, un'aggressione, un sabotaggio, una minaccia. In breve, la prima ci difende da ciò che accade, la seconda da chi agisce contro di noi. Ma la distinzione non è soltanto lessicale: la duplicità che quei due termini designano ci accompagna da sempre, anche quando la nostra lingua la raccoglie sotto un'unica parola.

Il problema, semmai, è un altro. La differenza la riconosciamo in teoria, ma in pratica **affrontiamo la Security con i metodi della Safety**: procedure automatiche, segnale d'allarme generale, esodo lungo le vie ordinarie verso il punto di raccolta. I fatti dell'11 novembre ? un'ondata di email minatorie che ha svuotato aule, mobilitato le forze dell'ordine e messo alla prova l'organizzazione dell'emergenza in migliaia di istituti ? lo hanno mostrato con evidenza: la tentazione di rispondere a una minaccia intenzionale come si risponderebbe a un incendio resta fortissima.

Nel frattempo, è la Security stessa a cambiare volto. La possibilità di recapitare, in sostanziale anonimato e a costo pressoché nullo, lo stesso messaggio a migliaia di destinatari nello stesso istante, direttamente nelle caselle riservate alle comunicazioni istituzionali, trasforma la natura della minaccia: non più l'atto isolato contro un singolo bersaglio, ma un'azione **seriale e distribuita**, capace di mettere sotto pressione un intero sistema nello stesso momento. E se lo scopo è paralizzare, all'autore

basta che ciascuno reagisca in automatico. Per questo alle pratiche di Security è richiesto un salto di qualità e di livello: non basta più distinguerle dalla Safety, occorre dotarle di metodi propri.

Il contesto degli studi e il contributo di queste pagine

Il tema, naturalmente, non nasce oggi. Nella letteratura internazionale la distinzione tra safety e security è consolidata e si fonda proprio sul carattere intenzionale e malevolo dell'evento (Pièrre-Cambacédès e Chaudet 2010; Jore 2019); da tempo si discute anche di come ricondurre i due ambiti a un quadro unitario di analisi del rischio (Aven 2007; Pièrre-Cambacédès e Bouissou 2013). Sul versante operativo, la valutazione della minaccia (*threat assessment*) è una disciplina strutturata, sviluppata a partire dagli studi del Secret Service statunitense, che distingue tra chi formula una minaccia e chi rappresenta davvero un pericolo (Fein, Vossekuil e Holden 1995; Borum et al. 1999; Meloy e Hoffmann 2014). Le linee guida britanniche e statunitensi sulle minacce di ordigno raccomandano da anni di non evacuare in automatico, di valutare la credibilità della minaccia ? chiedendosi, tra l'altro, se essa faccia parte di una serie ? e di scegliere tra più opzioni: nessuna evacuazione, ricerca, riparo interno (invacuazione), evacuazione parziale o totale (NaCTSO 2020; DHS-DOJ, Bomb Threat Guidance).

Il contributo di queste pagine si colloca dunque altrove, su tre piani: una **chiave di lettura giuridica**, che interpreta la distinzione attraverso le categorie del fatto e dell'atto e collega la validazione dell'evento al giudizio ex ante sulla colpa; l'uso del **momento della validazione** ? prima, durante e dopo l'evento ? come criterio ordinatore del Piano di Emergenza; un'**analisi a caldo** delle scelte compiute dalle istituzioni italiane nel novembre 2026. A ciò si aggiunge il contesto nazionale: la manualistica italiana sul Piano di Emergenza resta in larga parte costruita sul modello antincendio, e l'integrazione della security nella pianificazione dell'emergenza appare ancora poco sviluppata.

Nella progettazione di un **Piano di Emergenza Aziendale** (**PEA**) efficace, uno degli errori metodologici più frequenti consiste nel trattare tutte le emergenze con la medesima logica operativa: suona l'allarme, si abbandona l'edificio, ci si ritrova al punto di raccolta.

Sebbene questo schema funzioni perfettamente per un incendio o un terremoto, applicarlo meccanicamente a una lettera minatoria o a una telefonata di allarme ordigno può rivelarsi non solo inefficace, ma persino fatale. Per comprendere il perché, occorre esplorare il confine tra Safety e Security, attingendo a una sorprendente simmetria con la teoria generale del diritto.

1. Safety vs. Security: Il parallelo con fatti e atti giuridici

2. L'Attenuazione della differenza: dal pericolo al rischio valutato

3. La svolta operativa: il meccanismo di validazione

4. Tabella di sintesi: due logiche a confronto

5. Il Banco di Prova: Le Circolari di Palazzo Chigi e del Viminale

6. L'adeguatezza delle garanzie e il rischio tecnologico

1. Safety vs. Security: Il parallelo con fatti e atti giuridici

In ambito giuridico si distingue tradizionalmente tra **fatti giuridici in senso stretto** ? accadimenti naturali o materiali a cui l'ordinamento ricollega effetti prescindendo dalla volontà umana (un fulmine, un crollo, un sisma) ? e **atti giuridici**, ovvero comportamenti umani volontari e consapevoli, guidati da uno scopo (animus). Questa stessa dicotomia strutturale governa la gestione delle emergenze in azienda:

- La **Safety come "Fatto"**: Gli scenari di incendio accidentale o terremoto rispondono a leggi fisiche e probabilità statistiche. Nel momento in cui si manifestano, non vi è alcuna volontà ostile da decodificare: il fuoco brucia e la terra trema oggettivamente. La risposta aziendale deve quindi essere meccanica, standardizzata e immediata (allarme generale ed esodo rapido verso l'esterno; nel caso del sisma, a scossa terminata).
- La **Security come "Atto"**: Una lettera minatoria, un pacco sospetto o un allarme bomba sono atti illeciti dolosi. Dietro l'evento c'è una mente umana che agisce con una finalità precisa: intimidire, paralizzare la produzione, estorcere o colpire un bersaglio. Proprio perché l'evento è frutto di una strategia, l'aggressore potrebbe aver posizionato un ordigno proprio lungo le vie di fuga o nel punto di raccolta, sfruttando a proprio vantaggio la reazione automatica dell'azienda.

2. L'Attenuazione della differenza: dal pericolo al rischio valutato

A un'analisi più approfondita, la distinzione netta tra "fatto naturale" e "atto umano" subisce una significativa attenuazione nel momento in cui entrambi gli eventi entrano nel **Documento di Valutazione dei Rischi** (**DVR**) e nel **PEA**. Un terremoto o un incendio nascono come pericoli fisici, ma nel momento in cui vengono inseriti in un sistema di gestione aziendale smettono di essere mere fatalità per trasformarsi in **rischi scientificamente valutati**, governati dalla nota relazione:

Rischio = Probabilità (Frequenza) × Gravità (Danno) × Esposizione

- Nella **Safety**: Il datore di lavoro non governa il sisma in sé, ma misura la vulnerabilità strutturale dell'edificio, il carico d'incendio e il numero di persone esposte.
- Nella **Security**: Analogamente, si valuta l'esposizione reputazionale o strategica dell'azienda (settore merceologico, conflitti sindacali, appalti sensibili) e la vulnerabilità organizzativa (controllo accessi, gestione della corrispondenza).

Sul piano della responsabilità legale (art. 2087 c.c. e D.Lgs. 81/08), i due binari convergono: l'azienda non risponde del verificarsi del sisma o del gesto del folle, ma risponde dell'omissione preventiva qualora non abbia calcolato la propria vulnerabilità e predisposto adeguate misure di protezione.

3. La svolta operativa: il meccanismo di validazione

Se entrambi i fenomeni diventano "rischi valutati" a tavolino, dove risiede allora la vera differenza operativa nel Piano di Emergenza? Risiede nel **meccanismo di validazione** e nel **momento temporale** in cui esso si attiva.

Nella Safety: validazione ex-ante (risk assessment & commissioning)

Nella Safety, la validazione avviene prima che l'emergenza accada. Attraverso il *Risk Assessment* ingegneristico, il collaudo degli impianti (*Commissioning*) e le prove pratiche di evacuazione (*Emergency Drills*), l'azienda valida la tenuta del sistema a

monte. Di conseguenza, durante l'emergenza la **discrezionalità è ridotta al minimo**: se il sensore rileva fumo non si fa alcuna verifica di credibilità, perché validare sul momento costerebbe secondi preziosi e vite umane. Residua soltanto una verifica minima e procedimentalizzata: il preallarme con cui l'addetto conferma la segnalazione del rivelatore prima dell'allarme generale, o il controllo dell'agibilità di scale e percorsi che, nel sisma, precede l'esodo a scossa terminata.

Nella Security: validazione in itinere (threat credibility assessment)

Nella Security, al contrario, la valutazione fatta a tavolino serve solo a preparare gli strumenti per validare l'evento nel momento stesso in cui si manifesta. Poiché non è possibile modellizzare matematicamente la mossa di una mente ostile, quando arriva una chiamata minatoria o un plico sospetto si attiva il *Threat Credibility Assessment* (TCA) ? denominazione qui adottata per una valutazione che in letteratura rientra nel più ampio *threat assessment*:

1. **Niente allarme cieco**: Si evita di far scattare subito le sirene per non innescare il panico o spingere i lavoratori verso aree non bonificate.
2. **Analisi degli indizi**: L'operatore (es. reception) compila una checklist osservazionale (tono della voce, rumori di fondo, conoscenza dei locali da parte del chiamante, anomalie del plico).
3. **Filtro con le Autorità**: Il Crisis Management Team aziendale si interfaccia immediatamente con le Forze dell'Ordine per incrociare i dati e decidere se procedere con un'evacuazione mirata, una ricerca discreta o il blocco degli accessi.

Il TCA, tuttavia, non può restare un'intuizione affidata al buon senso dell'operatore. Perché la validazione in itinere sia affidabile ? e giuridicamente difendibile ? occorre precisare che cosa si valida, con quali criteri, in quanto tempo e da parte di chi.

3.1 Che cosa si valida: tre oggetti distinti

Dietro l'espressione "validare l'evento" si celano in realtà tre domande diverse:

1. **L'evento** ? si è verificato davvero? È giunta una telefonata, esiste un oggetto anomalo?
2. **La minaccia** ? è credibile? È specifica? Chi la formula ha l'intenzione e la capacità di attuarla?
3. **La risposta** ? l'azione che si sta per disporre è sicura? Percorsi e punto di raccolta sono stati verificati?

Nella Safety la prima validazione è pressoché immediata (il fumo c'è o non c'è) e la seconda non esiste: il fuoco non ha intenzioni. Nella Security il baricentro si sposta sulla seconda, e la terza diventa decisiva, perché **la risposta stessa può essere il bersaglio**.

3.2 Validare non significa accertare la verità

La validazione in itinere non approda quasi mai alla certezza: nessun indizio consente di escludere in modo assoluto la presenza di un ordigno. Essa è dunque una **decisione assunta in condizioni di incertezza**, esposta a due errori di segno opposto e di costo profondamente diverso:

- **Falso negativo** (non si evacua e l'ordigno c'è): evento raro, ma catastrofico e irreversibile.
- **Falso positivo** (si evacua per una minaccia infondata): evento frequente, il cui costo unitario è contenuto ma si accumula ? interruzione del servizio, incentivo all'emulazione, assuefazione del personale ai falsi allarmi, possibile esposizione a un'azione ostile all'esterno dell'edificio.

Ne discende un principio da recepire espressamente nel Piano: la **soglia di azione deve abbassarsi quanto più grave è l'indizio**. Una minaccia generica può tollerare alcuni minuti di verifica; il rinvenimento di un oggetto sospetto no.

3.3 I criteri di credibilità

Il TCA diventa operativo solo se esplicita i fattori da ponderare.

Fattori che aumentano la credibilità	Fattori che la riducono (senza mai azzerarla)
• Specificità: luogo, orario, tipo di ordigno • Conoscenza dei locali da parte dell'autore • Movente plausibile e coerente con il contesto (conflitti, procedimenti in corso, appalti sensibili) • Comunicazione rivolta a un solo destinatario • Riscontri materiali: oggetto fuori posto, accesso anomalo	• Genericità del messaggio • Diffusione a molti destinatari (es. email massive) • Campagna seriale in corso, segnalata dalle Forze dell'Ordine • Incoerenze interne al messaggio

Le ondate di minacce via email rivolte agli istituti scolastici ne offrono un esempio: il medesimo messaggio recapitato a decine di destinatari riduce la credibilità per il singolo istituto, ma non autorizza a ignorarlo. Indica piuttosto la risposta proporzionata ? vigilanza rafforzata e ispezione dei locali ? anziché l'evacuazione generalizzata.

3.4 Il fattore tempo: la validazione non è un'attesa

Una validazione priva di limiti temporali degenera in paralisi, e la paralisi è essa stessa una decisione ? la peggiore. Il Piano deve pertanto stabilire:

- un **tempo massimo di decisione**, predeterminato e graduato secondo il livello di allerta;
- un'**azione di default** da attuare se entro quel termine la validazione non si chiude (ad esempio, riparo in aree interne protette ? la cosiddetta invacuazione ? o evacuazione mirata su percorsi verificati);
- **fattori di escalation immediata** (rinvenimento di un oggetto, nuova comunicazione con dettagli, indicazioni delle Forze dell'Ordine) e **di de-escalation** (campagna seriale accertata).

La validazione in itinere è quindi **continua e rivedibile**: non un giudizio unico, ma una valutazione che si aggiorna man mano che affluiscono nuove informazioni.

3.5 Chi valida: la separazione dei ruoli

Il principio può essere espresso così: **chi riceve non decide, chi decide non è solo**.

- Chi riceve la minaccia (centralino, protocollo, portineria) **raccoglie** le informazioni mediante la checklist, senza valutarle.
- Il **decisore**, nominato nel Piano e affiancato da un sostituto, valuta e sceglie.

- Le **Forze dell'Ordine** apportano elementi non disponibili all'organizzazione, come il collegamento con altri episodi; la responsabilità della tutela dei lavoratori resta tuttavia in capo al datore di lavoro, salvo diverso provvedimento dell'Autorità.

3.6 Il giudizio ex ante e la tracciabilità della decisione

Il parallelo con la teoria del diritto trova qui il suo sviluppo più fecondo. Nella valutazione della colpa il giudice ricostruisce la condotta con un **giudizio ex ante in concreto** (la cosiddetta *prognosi postuma*): si chiede che cosa fosse conoscibile, in quel momento, da un agente modello, non che cosa sia emerso dopo. La validazione in itinere va organizzata proprio in vista di quel giudizio.

Ne deriva un'indicazione operativa: un **registro della decisione** che annoti ora, informazioni disponibili, opzioni considerate, scelta adottata e motivazione. Esso tutela le persone, perché impone di ragionare con metodo, e tutela il decisore, perché documenta la ragionevolezza della scelta rispetto a quanto era conoscibile.

3.7 I tre tempi della validazione

Così riformulata, la distinzione tra Safety e Security non oppone semplicemente un "prima" a un "durante", ma articola in modo diverso tre momenti:

Tempo	Safety	Security
Ex ante	Si valida la **risposta**: impianti, percorsi, prove di evacuazione.	Si valida la **capacità di validare**: checklist, ruoli, esercitazioni a tavolino sul TCA.
In itinere	Verifica minima e procedimentalizzata (preallarme, agibilità dei percorsi dopo il sisma).	Valutazione centrale e continua della minaccia e della risposta.
Ex post	Analisi dell'evento e aggiornamento del DVR.	Analisi dell'evento, ricalibrazione dei criteri di credibilità, aggiornamento del DVR e del PEA.

> *Nella Safety si valida in anticipo la risposta; nella Security si valida in anticipo la capacità di decidere.*

Il Piano di Security, in altre parole, non contiene la soluzione, ma il **metodo per trovarla sotto pressione**.

4. Tabella di sintesi: due logiche a confronto

Dimensione	Ambito Safety (Incendio / Terremoto)	Ambito Security (Minacce / Ordigni)
Natura giuridica	Assimilabile al **fatto giuridico** (oggettività fisica).	Assimilabile all'**atto giuridico illecito** (volontarietà e dolo).
Base della valutazione	Statistica, fisica, ingegneria strutturale.	Analisi comportamentale, *intelligence*, esposizione strategica.
Validazione	**Ex-ante** (*Risk Assessment* e collaudo impianti).	**In itinere** (*Threat Credibility Assessment* durante l'evento), preparata ex ante.
Oggetto della validazione	L'evento (verifica minima).	L'evento, la credibilità della minaccia, la sicurezza della risposta.
Tempo della decisione	Immediato.	Predeterminato e graduato, con azione di default.
Chi decide	Procedura automatica; addetti all'emergenza.	Decisore designato (e sostituto), in raccordo con le Forze dell'Ordine.
Gestione dell'allarme	Automatica, immediata e generalizzata.	Riservata, filtrata e coordinata con le Forze dell'Ordine.
Tracciabilità	Verbali di collaudo e delle prove di evacuazione.	Registro della decisione, in vista del giudizio ex ante.

5. Il Banco di Prova: Le Circolari di Palazzo Chigi e del Viminale

L'impostazione fin qui proposta ha trovato un immediato banco di prova nelle scelte compiute dalle istituzioni nei giorni successivi all'11 novembre. Due atti di indirizzo, adottati a distanza di poche ore l'uno dall'altro, hanno ridisegnato la gestione delle minacce diffuse via email.

5.1 Che cosa hanno stabilito

- La **nota della Presidenza del Consiglio dei Ministri** (12 novembre), trasmessa alle scuole dal Ministero dell'Istruzione e del Merito e destinata a tutte le amministrazioni, stabilisce che, «in assenza di elementi concreti ulteriori rispetto alla semplice ricezione di email massive che facciano ritenere sussistente un pericolo», non si proceda all'evacuazione degli edifici.
- La **circolare del Ministro dell'Interno** a prefetti e questori qualifica come inattendibile la minaccia che presenti carattere «manifestamente seriale»: messaggi identici o sostanzialmente analoghi, con la medesima provenienza, indirizzati indiscriminatamente a una pluralità di destinatari. Se invece emergono elementi che rendono plausibile la minaccia ? tra cui il ritrovamento di oggetti sospetti, precedenti minacce, riferimenti precisi a luoghi o persone ? il Questore dispone le verifiche opportune e, solo ove necessario, propone al Prefetto l'evacuazione della struttura. Dichiarato l'obiettivo: mantenere, ove le condizioni di sicurezza lo consentano, la regolarità delle attività e dei servizi.

5.2 Dove le circolari confermano l'impostazione

- **La fine dell'allarme automatico**. Per le minacce via email lo Stato abbandona espressamente la logica della Safety: il «niente allarme cieco» diventa indirizzo ufficiale.
- **La serialità come criterio di credibilità**. È uno dei fattori che, nel paragrafo 3.3, riducono la credibilità della minaccia. La circolare lo eleva però a qualcosa di più: una vera presunzione relativa di inattendibilità (iuris tantum), superabile soltanto da elementi concreti contrari. In termini giuridici, un'inversione dell'onere della prova applicata alla minaccia.
- **La continuità operativa come fine dichiarato**. Il tema annunciato fin dall'intestazione di queste pagine entra esplicitamente nell'atto di indirizzo.
- La separazione dei ruoli. Chi riceve non decide: la scelta dell'evacuazione è collocata presso l'autorità di pubblica sicurezza.

5.3 Dalla validazione locale alla validazione di sistema

Il passaggio più significativo, alla luce di quanto detto sulla validazione, è un altro. Lo Stato ha compiuto una **validazione in itinere su scala nazionale** e l'ha tradotta in una **regola ex ante** per ciascun ente. Ciò che per il sistema è stato un giudizio formulato durante l'evento, per la singola scuola o il singolo ufficio diventa una procedura già decisa. La distinzione tra Safety e Security non viene meno: si sposta di livello.

La cronologia della seconda ondata lo mostra con chiarezza. Il 12 novembre le email hanno raggiunto 3.788 istituti e soltanto 77 sono stati evacuati; secondo Palazzo Chigi, quelle evacuazioni sono state disposte subito dopo l'arrivo dei messaggi, prima che giungessero le indicazioni dei ministri. Dove la validazione di sistema è arrivata in tempo, ha funzionato; dove non era ancora arrivata, ha ripreso il sopravvento l'automatismo della Safety.

5.4 Il rischio di un nuovo automatismo

Il pericolo è sostituire un automatismo con un altro di segno opposto: prima «email, quindi evacuo», ora «email seriale, quindi non evacuo». Ma l'avversario osserva e si adatta. Già nella seconda giornata, secondo le ricostruzioni di stampa, i messaggi sarebbero partiti da più indirizzi anziché da un unico account, mettendo alla prova proprio il criterio della «medesima provenienza». E nulla esclude che una minaccia reale possa nascondersi all'interno di un'ondata seriale, usandola come copertura.

Per questo le circolari **non eliminano la validazione locale: la rendono più importante**. Gli «elementi concreti ulteriori» non arrivano dal centro; qualcuno, nell'ente, deve cercarli: l'oggetto fuori posto, l'accesso anomalo, il riferimento preciso ai locali, la minaccia che si discosta dal testo seriale.

5.5 Il nodo della responsabilità e della classificazione

Resta aperta una questione giuridica. Il datore di lavoro conserva gli obblighi di tutela previsti dal D.Lgs. 81/08 (artt. 18 e 43), mentre la decisione sull'evacuazione viene ricondotta all'autorità di pubblica sicurezza. Il Piano di Emergenza deve perciò disciplinare il **raccordo** tra i due piani: chi ricerca gli elementi ulteriori, entro quanto tempo, attraverso quale canale li porta al Questore, e come si documenta la decisione, in coerenza con il registro richiamato al paragrafo 3.6.

La circolare precisa, inoltre, che le segnalazioni in questione «non costituiscono attacchi informatici». È una scelta di classificazione che merita discussione: il **vettore è digitale**, ma il **bersaglio è fisico e organizzativo**. Le difese digitali ? filtri sulle caselle istituzionali, conservazione dei messaggi e delle intestazioni, segnalazione tempestiva alla Polizia Postale ? restano

parte integrante della risposta, ed è significativo che gli stessi dirigenti scolastici abbiano chiesto sistemi per riconoscere e filtrare le email minatorie.

5.6 Un cantiere aperto

Le indicazioni di questi giorni sono il primo tassello di un protocollo comune per tutte le amministrazioni, affidato al Comitato interministeriale per la sicurezza della Repubblica (CISR). Ogni Piano di Emergenza dovrà recepirlo, ma non potrà limitarsi a richiamarlo: dovrà tradurlo in procedure locali, ruoli, tempi e strumenti di verifica. È, ancora una volta, la differenza tra possedere una regola e possedere un metodo.

Un Piano di Emergenza Aziendale moderno non può limitarsi a gestire la fuga da un pericolo fisico. Deve saper integrare la ***rapidità esecutiva della Safety*** *? progettata per sottrarre le persone a un danno oggettivo ? con la* ***lucidità investigativa della Security****, indispensabile per non trasformare la risposta aziendale nell'obiettivo stesso di un aggressore. E poiché nella Security l'evento si valida mentre accade, il Piano vale quanto vale il metodo con cui quella validazione è stata preparata.*

6. L'adeguatezza delle garanzie e il rischio tecnologico

Un ulteriore elemento di sviluppo della distinzione tra Safety e Security si rinviene nel D.Lgs. 2 novembre 2026, n. 208, attuativo della direttiva (UE) 2024/2831. L'art. 23 interviene sull'art. 15 del D.Lgs. 81/2008, richiamando, fra le misure generali di tutela, i rischi connessi all'impiego di sistemi di monitoraggio e decisionali automatizzati e la «valutazione della adeguatezza delle garanzie» di tali sistemi rispetto ai rischi individuati, in considerazione delle caratteristiche specifiche dell'ambiente di lavoro.

Il decreto nasce nel contesto del lavoro mediante piattaforme digitali e l'art. 11 disciplina specificamente la tutela dei lavoratori interessati. La modifica dell'art. 15, disposizione generale del Testo unico, pone una questione interpretativa di più ampia portata, da affrontare attraverso una lettura coordinata delle norme: non consente, da sola, di estendere automaticamente a ogni datore di lavoro gli obblighi settoriali previsti per le piattaforme.

Per il Piano di Emergenza Aziendale il richiamo è soprattutto metodologico. Non basta che un dispositivo rilevi un'anomalia o attivi un allarme: occorre valutare se le garanzie e la risposta predisposte siano adeguate al rischio e all'ambiente concreto, tenendo conto di configurazione dei locali, vie di esodo, affollamento, accessi e vulnerabilità. Ciò non significa che qualsiasi sensore o impianto antincendio ricada, per ciò solo, nella definizione normativa dei sistemi automatizzati.

Nella Security, rilevazione, interpretazione della minaccia e scelta della risposta restano momenti distinti. Un meccanismo protettivo può produrre un rischio ulteriore quando, ad esempio, un allarme non verificato determina un esodo verso un'area esposta. Il criterio dell'adeguatezza rafforza dunque la tesi centrale: validare non soltanto l'evento, ma anche la sicurezza della risposta. Resta ferma, nella Safety, l'esigenza di non ritardare indebitamente le misure immediate necessarie davanti a un pericolo accertato.

Antonello Rubino, *RSPP*

Scarica la normativa di riferimento:

Ministero dell'Interno ? Gabinetto del Ministro - Direttiva prot. n. 0103407 del 13 novembre 2026 (Protocollo Uscita), Gestione delle segnalazioni di minaccia diffuse mediante comunicazioni telematiche aventi riflessi sull'ordine e la sicurezza pubblica. Indirizzi per il coordinamento informativo e l'adozione di misure di sicurezza.

Decreto legislativo 2 novembre 2026, n. 208 - Attuazione della direttiva (UE) 2024/2831 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, relativa al miglioramento delle condizioni di lavoro nel lavoro mediante piattaforme digitali.

Riferimenti bibliografici

- Aven T. (2007), A unified framework for risk and vulnerability analysis covering both safety and security, «Reliability Engineering & System Safety», 92(6), pp. 745?754.
- Borum R., Fein R., Vossekuil B., Berglund J. (1999), Threat assessment: Defining an approach for evaluating risk of targeted violence, «Behavioral Sciences & the Law», 17(3), pp. 323?337.
- DHS?DOJ, Bomb Threat Guidance, U.S. Department of Homeland Security ? U.S. Department of Justice.
- Fein R.A., Vossekuil B., Holden G.A. (1995), Threat Assessment: An Approach to Prevent Targeted Violence, U.S. Department of Justice, National Institute of Justice, NCJ 155000.
- Jore S.H. (2019), The conceptual and scientific demarcation of security in contrast to safety, «European Journal for Security Research», 4(1), pp. 157?174.
- Meloy J.R., Hoffmann J. (a cura di) (2014), International Handbook of Threat Assessment, Oxford University Press.
- NaCTSO ? National Counter Terrorism Security Office (2020), Bomb Threats, Protect UK,
- Piètre-Cambacédès L., Bouissou M. (2013), Cross-fertilization between safety and security engineering, «Reliability Engineering & System Safety», 110, pp. 110?126.
- Piètre-Cambacédès L., Chaudet C. (2010), The SEMA referential framework: Avoiding ambiguities in the terms "security" and "safety", «International Journal of Critical Infrastructure Protection», 3(2), pp. 55?66.
- U.S. Cybersecurity and Infrastructure Security Agency (CISA) (2025), Bomb Threat Guide, Version 1, agosto 2025.

Riferimenti normativi, giurisprudenziali e istituzionali

- Codice civile, art. 2087.
- D.Lgs. 9 aprile 2008, n. 81, artt. 18 e 43.
- ISO (2018), ISO 31000:2018, Risk management ? Guidelines, 2ª ed., International Organization for Standardization, Ginevra. Riferimento generale per il quadro di gestione e analisi del rischio.
- Torrente A., Schlesinger P. (2021), Manuale di diritto privato, a cura di F. Anelli e C. Granelli, 25ª ed., Giuffrè Francis Lefebvre, Milano, ISBN 978-88-288-2954-6.
- Presidenza del Consiglio dei Ministri, nota del 12 novembre 2026 sulle email massive di segnalazione di allarme, trasmessa agli istituti scolastici dal Ministero dell'Istruzione e del Merito.
- Ministero dell'Interno ? Gabinetto del Ministro, Direttiva prot. n. 0103407 del 13 novembre 2026 (Protocollo Uscita), «Gestione delle segnalazioni di minacce diffuse mediante comunicazione telematica», indirizzata ai Prefetti della

Repubblica, ai Questori e ai vertici delle Forze di polizia.

- Ministero dell'Istruzione e del Merito, Nota prot. n. 9220 del 13 novembre 2026, di trasmissione alle istituzioni scolastiche della direttiva del Ministero dell'Interno.
- Nota metodologica. La ISO 31000 fornisce il quadro generale per la gestione del rischio; non prescrive la specifica espressione moltiplicativa «Probabilità × Gravità × Esposizione» riportata nel testo, che va intesa come schematizzazione adottata dall'autore.
- Decreto legislativo 2 novembre 2026, n. 208, «Attuazione della direttiva (UE) 2024/2831 [...] relativa al miglioramento delle condizioni di lavoro nel lavoro mediante piattaforme digitali», G.U. Serie Generale n. 266 del 14 novembre 2026, artt. 11 e 23 (entrata in vigore: 2 dicembre 2026). L'art. 23 modifica l'art. 15 del D.Lgs. 81/2008.


Licenza Creative Commons
I contenuti presenti sul sito PuntoSicuro non possono essere utilizzati al fine di addestrare sistemi di intelligenza artificiale.
