«Non evacuate più»: la linea del Viminale contro gli allarmi bomba. Il Protocollo di sicurezza su tutti i settori di Rinaldo Frignani e Valentina Santarpia

La circolare ai prefetti e ai questori dopo l'ondata di mail minatorie che hanno portato a controlli in circa diecimila scuole in due giorni. Ma a rischio ci sono anche ospedali, trasporti, centri commerciali, stadi e infrastrutture critiche

(Fonte: https://roma.corriere.it/ 13 novembre 2026)



La circolare del Viminale è stata firmata e già venerdì mattina sarà diramata ai prefetti e a tutti i ministeri: «In assenza di elementi concreti ulteriori rispetto alla semplice ricezione di e-mail massive che facciano ritenere sussistente un pericolo, non si proceda all'evacuazione degli edifici». **È questa l'indicazione che arriva al termine di una serie di riunioni a palazzo Chigi** per mettere a punto il dispositivo di intervento che eviti il caos, così come invece accaduto mercoledì scorso. Adesso saranno stilati «protocolli specifici di comportamento» **per ogni settore.** Vale a dire ospedali, carceri, uffici aperti al pubblico. Ma si dovrà anche mettere a punto un piano per fronteggiare eventuali attacchi hacker in settori strategici come quello della grande distribuzione, le infrastrutture e tutti gli altri ambiti che potrebbero essere attaccati.

Le scuole

All'indomani dell'allarme bomba inviato a oltre 6 mila istituti scolastici, replicato ieri in altri 3.700 circa, a tutti i dirigenti è arrivata l'indicazione da parte del ministero dell'Istruzione e del Merito sul fatto che resta ferma la facoltà del prefetto «di disporre misure di evacuazione qualora disponga di elementi specifici e concreti che configurino una situazione di effettivo rischio.

Pertanto, le scuole, qualora ne ravvisino i presupposti, possono fornire al prefetto territorialmente competente ogni elemento e informazione utile per le necessarie valutazioni».

Ma, di fatto, visto il caos dei giorni scorsi, **i presidi come dovranno comportarsi?** «Dopo essersi consultato con le forze dell'ordine, un preside valuta la minaccia e decide cosa fare, sempre in un'ottica di prudenza», spiega Antonello Giannelli, capo dei presidi. Significa che non esiste «un comportamento giusto o sbagliato», ma che ciascun dirigente ha, in base al ruolo che riveste, anche come pubblico ufficiale, **la responsabilità della incolumità degli studenti e può effettuare la scelta che ritiene giusta in quel momento, considerate le circostanze:** «Non bisogna né caricarlo di responsabilità che non sono nel suo mandato né esautorarlo».

Detto ciò, sarebbero utili due elementi per facilitare il loro compito, suggerisce Giannelli: «Un sistema di filtraggio e di riconoscimento dei modelli ricorrenti applicato agli indirizzi di posta elettronica delle scuole a elle caselle istituzionali per evitare che ogni scuola debba fronteggiare in solitudine i messaggi minatori». **E poi «un canale di allerta centralizzato in grado di avvisare in tempo reale le scuole quando è in corso un attacco massivo».** Anche perché il rischio, come avverte la Uil, è che le «responsabilità siano scaricate tutte sui dirigenti, lasciandoli soli di fronte a decisioni così delicate».

Ospedali e carceri

Ma l'indicazione generale anche in altri settori ritenuti a rischio è sempre quella di prendere decisioni delicate — proprio come le evacuazioni — solo di fronte a fatti concreti. **Uno scenario che comprende ospedali e strutture sanitarie, carceri, centri commerciali, luoghi di aggregazione** come cinema, stadi e teatri. Ogni amministrazione responsabile dovrà rivolgersi al prefetto nel caso le comunicazioni d'allarme evidenzino luoghi precisi, persone, circostanze riferibili a uno specifico obiettivo.

I fondi della Difesa

Quella delle mail minatorie è solo una parte della minaccia ibrida in atto che chiama in causa la cyber sicurezza nazionale soprattutto contro le azioni degli hacker. **Un ambito nel quale anche la Difesa nella programmazione 2019-2040 proprio per il contrasto alla minaccia ibrida** prevede stanziamenti per oltre otto miliardi di euro, più di 1,7 nel periodo 2029-2031 e più di due nel 2032-2040, per sistemi ad alta tecnologia militare, anche classificati, che possono però essere utilizzati per la protezione di obiettivi e servizi civili.

Gli attacchi hacker

L'attenzione di Palazzo Chigi e del Viminale è infatti orientata alla prevenzione di incursioni informatiche che potrebbero prendere di mira infrastrutture critiche nazionali, come quelle che gestiscono l'approvvigionamento energetico — di superficie e sotterraneo, oltre che sottomarino —

le centrali elettriche, gli acquedotti, la rete di trasporto pubblico. Il piano che si sta mettendo a punto prevede iniziative che possano bloccare gli attacchi hacker come quelli a distanza alla grande distribuzione alimentare dei giorni scorsi in Francia e in altri Paesi, con qualche caso anche in Italia, e successivamente al cantiere del maxi tunnel del Brennero. Obiettivi strategici compresi in una lunga lista che deve essere protetta.