Poliziamoderna

Venti di cybersicurezza

Ricorre quest'anno il ventennale dalla nascita della Specialità della Polizia di Stato, da quel decreto istitutivo del Servizio polizia postale e delle comunicazioni del 1° marzo 1998 che ne ha disegnato struttura e competenze. Tutelare i servizi postali e delle telecomunicazioni, reprimere i reati contro l'inviolabilità della corrispondenza, sorvegliare l'interno delle sedi e degli impianti appartenenti al ministero delle Poste e delle Comunicazioni, vigilare gli uffici postali, garantire servizi di scorta per le operazioni di trasporto di valori e tutelare il diritto d'autore e delle radiofrequenze: erano queste le principali attività svolte all'inizio dagli operatori per garantire la tutela e la regolarità delle comunicazioni che, in passato, erano basate sulla carta e sulla corrispondenza. La rivoluzionaria evoluzione che ha interessato il settore delle comunicazioni ha trasformato anche le competenze tradizionali della polizia postale e delle comunicazioni la quale, oramai, ha assunto una nuova *mission*, quella della sicurezza informatica e della tutela delle comunità virtuali. Internet e le tecnologie, infatti, rappresentano una irrinunciabile costante nella vita di ognuno di noi e della quale tutti, più o meno consapevolmente, ricaviamo enormi benefici. La Rete sicuramente costituisce una notevole opportunità di sviluppo e di progresso per cittadini, istituzioni e operatori economici ma rappresenta anche un importante fattore di attrazione per gli interessi della criminalità comune e organizzata, nazionale e internazionale. Ciò ha reso stringente l'esigenza di creare una rete strutturata volta alla prevenzione e contrasto del cybercrime, per questo la polizia postale e delle comunicazioni ha raccolto questa nuova necessità facendone la sua nuova mission istituzionale: la tutela della corrispondenza e della logistica rappresentano oggi solo una parte degli ambiti tradizionali di intervento della Specialità la quale costituisce un punto di riferimento in materia di sicurezza informatica e tutela delle comunità virtuali.

Questo nuovo modo di intendere la sicurezza, innovativo nelle forme e nelle proiezioni esterne, ha richiesto anche un mutamento delle strategie di intervento le quali, pur non abbondonando il tradizionale modo di "fare polizia", si sono arricchite di ulteriori contenuti. Per questo la polizia postale e delle comunicazioni ha potenziato i rapporti con i portatori di interessi nell'ambito della sicurezza informatica, sviluppando forme coordinate e integrate di collaborazione e avvalendosi del partenariato sia di soggetti privati che pubblici.

La tutela delle infrastrutture critiche informatizzate è diventata, senza dubbio, un obiettivo primario che, peraltro, è stato ulteriormente valorizzato dalla recente direttiva Nis (*Network and information security*) volta a migliore il livello di cyber security all'interno dell'Unione europea. D'altronde è noto il clamore che hanno suscitato le campagne internazionali di cyber attacchi commessi tramite la diffusione dei malware come *Wannacry* e *Not-Petya*, che hanno visto numerosi Paesi subire reali, ingenti danni in termini di interruzione di servizi essenziali e di interi settori economico-industriali.

In tale ambito, la Specialità riveste un ruolo fondamentale nella rinnovata architettura nazionale (dpcm 17 febbraio 2017) dedicata alla cyber sicurezza grazie al lavoro svolto dal Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (Cnaipic), organo del ministero dell'Interno deputato, in via esclusiva, alla prevenzione e repressione dei crimini informatici di matrice comune, organizzata o terroristica, aventi per obiettivo le realtà strategiche, erogatrici di servizi essenziali per il Paese (acqua, energia, trasporti, pubblica amministrazione, telecomunicazioni, finanza). In ragione di tali esclusive competenze, la recente implementazione nazionale delle direttiva europea Nis (decreto legislativo nr. 65 del 18 maggio 2018) ha individuato la polizia postale quale Autorità di contrasto nazionale, chiamata a collaborare con gli altri soggetti istituzionali individuati dalla normativa europea. La trasversalità della minaccia cyber ha, inoltre, richiesto una cooperazione rafforzata e un approccio multilivello con enti, sia pubblici che privati. Recentemente il dpcm 17 febbraio 2017, ha cesellato definitivamente l'architettura nazionale di "cyber defence", convogliando all'interno di una strutturata azione di coordinamento, le capacità di risposta delle diverse Amministrazioni centrali componenti il Comitato nazionale per la sicurezza della repubblica (Cisr). I rappresentanti della polizia postale e delle comunicazioni, in qualità di specialisti per il ministero dell'Interno in materia cyber, partecipano ai lavori del rinnovato Nucleo sicurezza cibernetica (Nsc), istituito presso il Dipartimento informazioni e sicurezza e presieduto dal vice direttore del Dis, organismo competente per la valutazione e la gestione di eventuali situazioni di crisi cibernetica.

Non tutto ciò che emerge dalla Rete è immediatamente visibile e fruibile: esiste, infatti, un mondo

virtuale sommerso nel quale proliferano le attività illecite grazie a raffinate tecniche di anonimizzazione che dissimulano le tracce informatiche e rendono più complesse le attività di accertamento delle identità on line. Il cosiddetto *dark web*, è un vero e proprio luogo di installazione di imponenti mercati mondiali virtuali che mettono a disposizione ogni tipo di servizio o prodotto, soprattutto di natura illecita come droga, armi, credenziali bancarie, dati personali nonché materiale pedopornografico. Proprio quest'ultimo settore rappresenta un importante ambito di intervento della polizia postale e delle comunicazioni la quale, attraverso il Centro nazionale per il contrasto alla pedopornografia on line (Cncpo), svolge quotidianamente un'attività di monitoraggio della rete a tutela dei minori dagli abusi su Internet. Senza dubbio la *darknet*, rappresentando una dimensione privilegiata per le comunità pedofile che scambiano e divulgano materiale pedopornografico, costituisce un importante ambito di indagine per gli operatori della Specialità ma non risulta neanche l'unico giacché sono costantemente monitorate anche le piattaforme di navigazione più comuni. Alcune di queste, quali i social network, sono ritenute "sensibili" ed è elevata la soglia di attenzione della Specialità perché anche in queste community proliferano sempre nuove modalità di adescamento di minori e emergono diversificati atti di repressione e vessazione riconducibili a forme di devianza minorile on line. *Cyberbullismo*, *grooming*, *sexting*, blog incitanti all'anoressia o al suicidio: questi sono solo alcuni dei pericoli che il Web può riservare ai ragazzi e la consapevolezza che la repressione di questi fenomeni possa non essere sempre sufficiente, ha richiesto il coinvolgimento sistemico di tutti gli operatori che, a qualsiasi titolo, intervengono nella catena di crescita e protezione dei ragazzi, nell'ottica di una prospettiva multidisciplinare e sinergica. In tal senso, iniziative condivise per metter a fattor comune esperienze e azioni hanno assicurato interventi strutturati e performanti come è avvenuto, ad esempio, con la ricerca scientifica "Quanto Condividi?" svolta in collaborazione con la facoltà di psicologia dell'Università degli studi Sapienza di Roma e il Dipartimento per la giustizia minorile e di comunità, che ha rappresentato un ottimo modello di studio e di elaborazione di linee di azione efficaci, utili per operatori scolastici e di polizia per interpretare comportamenti e fattori di rischio. Altresì significativo è il progetto *Safer internet center Italy*, nel quale la polizia postale e delle comunicazioni, seduta nel board dei principali stakeholder di settore, mette a disposizione di enti pubblici e privati l'esperienza concreta di prevenzione e contrasto a tutte le forme di abuso dei minori in rete. Preziose, inoltre, sono le collaborazioni con le principali *helpline* nazionali nonché la cooperazione con enti istituzionali quali il Garante per la privacy, il Dipartimento per la giustizia minorile e di comunità e il ministero dell'Istruzione, dell'Università e della Ricerca, dalle quali sono nate consolidate procedure di gestione condivisa delle richieste di aiuto. Altrettanto significativo è l'impegno della Specialità nelle campagne di educazione e sensibilizzazione volte alla promozione, soprattutto tra i più giovani, della cultura della legalità sul web. La campagna educativa *Una vita da Social*, giunta oramai alla V edizione, ha permesso di incontrare finora circa 1 un milione e 500mila studenti di oltre 12mila istituti scolastici in tutto il territorio nazionale, coinvolgendo anche genitori e insegnanti che sicuramente sono i primi a intercettare eventuali fattori di rischio e disagio dei ragazzi. È, inoltre, di solare evidenza come il Web abbia assunto un ruolo fondamentale nelle strategie di comunicazione del *Daesh* e di ogni forma di propaganda di natura terroristica, soprattutto di matrice islamica. Con particolare riferimento alla prevenzione e contrasto al terrorismo internazionale di matrice jihadista, alla polizia postale e delle comunicazioni è affidato il costante monitoraggio della Rete volto al contrasto del fenomeno della radicalizzazione e della propaganda islamica su Internet, che oramai è divenuto un necessario complemento per le tradizionali attività in materia di antiterrorismo, sia nazionali che estere.

In ultimo, la continua evoluzione degli strumenti di pagamento elettronico (*e-payment*, *mobile-payment* , criptovalute), aumentando la velocità e la semplicità degli scambi, ha contribuito a innalzare vertiginosamente il volume globale dei traffici, con conseguenti ripercussioni sul versante della sicurezza. La polizia postale e delle comunicazioni è, dunque, fortemente impegnata nel contrasto al *financial cybercrime*, nei settori dell'antifrode e dell'antiriciclaggio, con l'obiettivo di prevenire e reprimere fenomeni criminosi volti ad arrecare danni patrimoniali ingenti a singoli cittadini, piccole e medie imprese e grandi aziende. In questo quadro, gli scenari di contrasto indirizzano l'azione delle forze di polizia verso la ricerca di modelli finalizzati a conseguire la più rapida cognizione di elementi investigativi, con la consapevolezza che la tempestività degli interventi sia assolutamente necessaria per contenere i danni economici. In tal senso, già dal 2010 la polizia postale ha ideato e realizzato una piattaforma informatica, denominata *Of2cen – On line fraud cyber centre and expert network*, che costituisce una piattaforma comune e condivisa tra Servizio, Compartimenti territoriali e istituti di credito convenzionati. A seguito della simultanea condivisione dei dati economico-informatici relativi a una frode, gli istituti di credito hanno la possibilità di creare una black list e intraprendere autonomamente le azioni di protezione di natura preventiva a tutela dei propri utenti.

La polizia postale e delle comunicazioni, dunque, rappresenta oggi un laboratorio dove esperienza e innovazione si fondono per creare un sistema di protezione informatica aggiornato e completo, a garanzia dei diritti fondamentali dei cittadini. La Specialità si è guadagnata sul campo un posto strategico nella prevenzione e contrasto al cybercrime ottenendo importanti risultati per la sicurezza dei cittadini ed è pronta ad affrontare le nuove sfide che la attendono. ?

* *direttore del Servizio polizia postale e delle comunicazioni*