Resoconto attività della Polizia Postale e delle Comunicazioni nel 2018

In uno scenario nel quale la continua evoluzione tecnologica influenza ogni azione del nostro vivere quotidiano, l'impegno della Polizia Postale e delle Comunicazioni nell'anno 2018 è stato costantemente indirizzato alla prevenzione e al contrasto della criminalità informatica in generale, con particolare riferimento ai reati di precipua competenza di questa Specialità.

CNCPO

Nell'ambito della **pedopornografia online,** nell'anno in corso, sono stati eseguiti **43** arresti e denunciate **532** persone; tra le operazioni più significative, coordinate dal Centro Nazionale del Servizio Polizia Postale e delle Comunicazioni, si segnala l'operazione "Ontario" che ha consentito l'esecuzione di **22** perquisizioni, **4** persone tratte in arresto e **18** persone denunciate in stato di libertà; nell'ambito dell'operazione "Safe Friend" sono state eseguite **15** perquisizioni che hanno consentito di arrestare **2** persone e denunciarne **13.**

Le indagini svolte anche in modalità sotto copertura nell'Operazione "Good Fellas" hanno consentito di eseguire **14** perquisizioni, portando all'arresto di 4 persone, nonché di denunciare in stato di libertà altri **10** indagati.

L'Operazione denominata "*Showcase*" si è conclusa con l'esecuzione di **15** perquisizioni, la denuncia di **14** persone e l'arresto di un altro indagato.

Dalle complesse attività di prevenzione, è scaturita una assidua attività di monitoraggio della rete che ha riguardato **33086** siti internet, di cui **2182** inseriti in black list.

Le indagini relative al fenomeno dell'adescamento di minori online hanno portato all'arresto di **3** persone e alla denuncia di **136** indagati.

Fondamentale importanza assume la collaborazione con organismi internazionali dalla quale prendono avvio importanti attività investigative tra

le quali alcune iniziate negli ultimi mesi con approfondimenti tuttora in corso.
Il Centro rivolge massima attenzione al contrasto di fenomeni emergenti che scaturiscono da fragilità psico-emotiva dei minori tra i quali emergono episodi di istigazione all'autolesionismo e al suicidio, strutturati anche in modalità di sfida o di gioco. In particolare, dal 2017, il Centro ha avviato un'attività di monitoraggio della rete finalizzata a contrastare il fenomeno noto come "Blue Whale", attività rivolta a individuare le vittime e i "curatori" e che ha fatto registrare circa **700** segnalazioni, delle quali **270** confluite in comunicazioni di notizie di reato alle Procure. Nell'ambito dei reati contro la persona perpetrati sul web, il **ricatto on line** è un fenomeno in continua crescita con 940 casi trattati dall'inizio dell'anno, atteso che il dato emerso è parziale e fortemente ridotto rispetto alla reale entità del fenomeno. Sono 20 le persone denunciate e 2 le persone arrestate in Italia nel 2018. Anche grazie a una complessa attività condotta in ambito internazionale in collaborazione con la Gendarmerie Royale del Marocco, tramite gli organi di coordinamento istituzionali, sono stati arrestati 23 cittadini marocchini destinatari delle transazioni finanziarie provento di estorsioni a sfondo sessuale. Dal mese di gennaio ad oggi, sono state denunciate 955 persone e 8 persone sono state tratte in arresto, per aver commesso estorsioni a sfondo sessuale, stalking, molestie sui social network, minacce e trattamento illecito di dati personali. Tra i reati contro la persona, in costante aumento sono le **diffamazioni on line,** soprattutto ai danni di persone che ricoprono incarichi istituzionali o che sono note. In questo ambito, nel 2018, sono state denunciate 685 persone. Si registra inoltre una continua evoluzione nella tipologia dei reati commessi. L'ultima modalità della violenza sulle donne è il fenomeno dei c.d. stupri virtuali: all'interno di gruppi chiusi i partecipanti di sesso maschile condividono foto, ricercate sui social o copiate da contatti whatsapp, di donne ignare, ritratte nella loro vita quotidiana, dando poi sfogo a fantasie violente e comportamenti offensivi.

L'aumento del numero degli adolescenti presenti sul web ha determinato una crescita esponenziale del numero di minorenni vittime di reati contro la persona: dai 104 casi registrati nel 2016 si è passati a 177 nel 2017 e 202 casi trattati nel 2018, le vittime hanno tutte un'età compresa tra i 14 e i 17 anni.

Di rilievo è l'attività condotta dal Servizio Polizia Postale e delle Comunicazioni nel contrasto ai reati d'incitamento all'odio, svolgendo il prezioso ruolo di punto di contatto nazionale per il **contrasto all'hate speech on line**. Sono oltre **5000** gli spazi virtuali monitorati nel 2018 per condotte discriminatorie di genere, antisemite, xenofobe e di estrema destra.

Le **truffe on line** sono in continua crescita: nel 2018 la Specialità ha denunciato **3355** persone, ne ha arrestato **39**, ha sequestrato **22.687** spazi virtuali, ha ricevuto e trattato circa **160.000** segnalazioni di truffe o tentate truffe. Significativa l'attività svolta sulle cosiddette frodi delle assicurazioni. Questa tipologia di truffa viene commessa attraverso la commercializzazione di polizze assicurative mediante la creazione di portali, in taluni casi con riproduzioni di pagine web di compagnie note, sulle quali sono promosse polizze assicurative temporanee false, esercitando in tal modo l'attività di intermediazione assicurativa in difetto di iscrizione al registro degli intermediari assicurativi.

CNAIPIC

Di evidente incremento è l'attività di contrasto alla minaccia cyber svolta dal Centro Nazionale Anticrimine per la Protezione delle Infrastrutture Critiche (C.N.A.I.P.I.C.), attestata dal rilevante aumento del numero di alert diramati alle infrastrutture critiche nazionali che, rispetto al 2017, è quasi raddoppiato sino a raggiungere **55843 segnalazioni di sicurezza**.

La tempestiva condivisione dei c.d. "indicatori di compromissione" dei sistemi informatici con le più importanti infrastrutture critiche ha consentito di rafforzare gli strumenti volti alla protezione della sicurezza informatica, garantita anche dalla costate attività di monitoraggio informativo in ambienti di interesse investigativo.

Inoltre in particolare la Sala Operativa del Centro ha gestito:

- **442** attacchi informatici nei confronti di servizi internet relativi a siti istituzionali e infrastrutture critiche informatizzate di interesse nazionale;
- **97** richieste di cooperazione nell'ambito del circuito "High Tech Crime Emergency".

Tra le attività investigative condotte, in tale ambito, si segnalano **68** indagini avviate nel **2018** per un complessivo di **15** persone deferite in stato di arresto ovvero in stato di libertà alle competenti AA.GG .

Tra le attività più significative si segnala un'operazione, frutto di una proficua attività di collaborazione internazionale intrapresa con la polizia olandese, che ha ricevuto il supporto di Europol per il tramite dell'European Cyber Crime Centre della Joint Cybercrime Action Taskforce. Il Centro, con l'ausilio della Sezione Polizia Postale di Cosenza ed il supporto logistico della Stazione dei Carabinieri di San Giorgio Albanese (CS) ha eseguito una perquisizione locale e personale nei confronti di un ventottenne italiano residente nella provincia di Cosenza resosi responsabile del reato di "intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche" (Art. 617 quater C.P.).

Nel corso della perquisizione sono stati sequestrati computer e supporti informatici utilizzati per portare a compimento l'attività illecita.

Nell'ottica di un'efficace condivisione operativa, il Centro ha proseguito la stipula di specifici protocolli a tutela delle infrastrutture critiche nazionali: al riguardo, nel 2018 sono state sottoscritte 8 nuove convenzioni con le società WindTre, Sky Italia, Fincantieri, MM S.p.A., Monte dei Paschi di Siena, Consip S.p.A., Nexi S.p.A. e BT Italia, oltre al rinnovo delle convenzioni in essere con Sogei, ATM, ENI, RAI, ENAV e TERNA.

Si rappresenta, altresì, che analoghe forme di collaborazione sono state avviate dagli uffici territoriali della Specialità con strutture sensibili di rilevanza territoriale, sia pubbliche che private, al fine di garantire un sistema di sicurezza informatica capillare e coordinato.

SEZIONE FINANCIAL CYBERCRIME

Con riferimento al **financial cybercrime,** le sempre più evolute tecniche di *hackeraggio,* attraverso l'utilizzo di *malware* inoculati mediante tecniche di phishing, ampliano a dismisura i soggetti attaccati, soprattutto nell'ambito dei rapporti commerciali, anche per l'utilizzo di particolari tecniche di *social engineering* e di *cyber profiling*. Infatti lo scopo delle organizzazioni criminali è quello di intromettersi nei rapporti commerciali tra aziende, attraverso le

informazioni acquisite, dirottando asset finanziari verso conti correnti nella disponibilità dei malviventi. Il BEC (business e-mail compromise) o CEO (Chief Exeutive Officer) fraud sono la moderna applicazione della tecnica di attacco al sistema economico nazionale denominata "man in the middle".

Nonostante la difficoltà operativa di bloccare e recuperare le somme frodate, soprattutto perché inviate verso paesi extraeuropei (Cina, Taiwan, Hong Kong), grazie alla versatilità della piattaforma **OF2CEN** (On line Fraud Cyber Centre and Expert Network) per l'analisi e il contrasto avanzato delle frodi del settore, nell'anno 2018, la Specialità a fronte di una movimentazione in frode denunciata di **38.400.000,00 €** ha potuto già recuperare e restituire **circa 9 milioni** mentre sono in corso attività di cooperazione internazionale finalizzate al recupero delle restanti somme. La piattaforma in questione frutto di specifiche convenzioni intercorse mediante ABI con gran parte del mondo bancario, consente di intervenire in tempo reale sulla segnalazione bloccando la somma prima che venga polverizzata in vari rivoli di prestanome.

Nell'ambito della Cooperazione Internazionale appare opportuno segnalare la recente operazione di respiro internazionale denominata "Emma4", coordinata dal Servizio Polizia Postale con la collaborazione di **30 Paesi** Europei e di Europol, volta a identificare i c.d. "money mules", riciclatori primi destinatari delle somme provenienti da attacchi informatici e campagne di phishing, che offrono la propria identità per l'apertura di conti correnti e/o carte di credito sui quali vengono poi accreditate le somme illecitamente carpite.

L'operazione ha consentito sul territorio nazionale di identificare **101** ***money mules*** di cui ben **50 tratti in arresto e 13 denunciati in stato di libertà.**

Le transazioni fraudolente sono state **320**, per un totale di circa **34 milioni di euro,** di cui **20 milioni di euro** sono stati bloccati e/o recuperati grazie alla piattaforma per la condivisione delle informazioni denominata "OF2CEN", realizzata appositamente al fine di prevenire e contrastare le aggressioni al sistema economico finanziario.

Anche in ambito nazionale il settore per il contrasto al Financial Cyber Crime ha prodotto notevoli risultati operativi ed in particolare nel marzo dell'anno

in riferimento è stata condotta un'articolata operazione di Polizia giudiziaria denominata "Bruno" condotta dalla Specialità in collaborazione con le Autorità rumene, che ha consentito di denunciare complessivamente **133** soggetti, **14** sottoposti a ordinanza di custodia cautelare **3** dei quali in territorio rumeno, per associazione a delinquere transnazionale dedita ad attacchi e frodi informatiche su larga scala e riciclaggio. Da questa operazione per la prima volta sono emersi elementi dell'interessamento da parte della criminalità organizzata di tipo mafioso verso il settore del Financial Cyber Crime.

Nel luglio si è conclusa l'Operazione denominata "Sim Swap" che prende il nome dalla particolare tecnica utilizzata dai malviventi, che rappresenta una modalità innovativa di attacco ai sistemi di home banking, che prevede la sostituzione, attraverso dealers compiacenti, delle sim telefoniche attraverso le quali giungono ai titolari dei conti attaccati le OTP (one time password) per effettuare le disposizioni di trasferimento di denaro. L'operazione si è conclusa con l'esecuzione di **14 ordinanze di custodia cautelare**.

Nel novembre si è conclusa l'Operazione denominata "Travellers" nella quale la Specialità ha eseguito **6 ordinanze** di custodia cautelare, verso un gruppo criminale definito dall'AG. "itinerante" in quanto operante indistintamente su tutto il territorio nazionale. L'associazione disponeva di un proprio "apparato tecnico-finanziario" che si occupava di dotare gli associati di conti correnti (intestati a società inesistenti o appositamente create), apparati POS portatili (anche operativi su circuiti internazionali) abilitati a transazioni con carte di credito e carte prepagate con funzioni *on-line*, attraverso i quali riciclare i proventi delittuosi.

SEZIONE CYBER TERRORISMO

La recente direttiva del Sig. Ministro dell'Interno sui comparti di specialità ha confermato in capo alla Polizia Postale e delle Comunicazioni, sia a livello centrale che territoriale, le competenze in materia di contrasto al fenomeno del terrorismo di matrice jihadista in rete, con particolare riferimento al monitoraggio del *web*, quale principale strumento di strategia mediatica del *Daesh*, già espletato da personale della Polizia Postale e delle Comunicazioni, affiancato da un qualificato, supporto di mediazione linguistica e culturale.

Tale rinnovato, rafforzato, impegno della Polizia Postale e delle Comunicazioni in tale ambito ha reso necessario implementare le attività in argomento, ampliando il coinvolgimento di un maggior numero di Compartimenti nel summenzionato monitoraggio, nonché un potenziamento del numero dei mediatori linguistici e culturali, il cui prezioso apporto, per la peculiarità della materia e dei relativi contenuti multimediali presenti nella rete, risulta assolutamente indispensabile.

Nell'ambito della prevenzione e contrasto al terrorismo internazionale di matrice jihadista e, in particolare, ai fenomeni di radicalizzazione, la Polizia Postale e delle Comunicazioni ha svolto attività sia di iniziativa, che su specifica segnalazione, al fine di individuare i contenuti di eventuale rilevanza penale all'interno degli spazi e servizi di comunicazione on line, siti o spazi web, weblog, forum, portali di social network e i cosiddetti "gruppi chiusi", anche a seguito di informazioni pervenute dai cittadini tramite il Commissariato di P.S. Online.

L'attività, funzionale a contrastare il proselitismo e prevenire fenomeni di radicalizzazione, ha portato a monitorare circa **36.000** spazi web e alla rimozione di diversi contenuti (**250**).

Nel corso di tale attività di monitoraggio, si è inoltre riscontrato un effettivo incremento dell'azione da parte dei maggiori fornitori di servizi Internet (*Facebook, Google, Twitter, etc.*) volta alla rimozione di contenuti illeciti presenti sulle proprie piattaforme, grazie anche alla richiesta di maggiore collaborazione elaborata in numerose sedi istituzionali nell'ambito di progetti internazionali (es. *EU Internet Forum*), ai quali ha preso parte la Specialità.

A seguito di tale strategia, si è rilevato un repentino passaggio dei fenomeni di diffusione e divulgazione dei contenuti riconducibili al radicalismo islamico su piattaforme di comunicazione *social* ritenute più sicure (*Telegram, WhatsApp*), in quanto garantiscono maggiore riservatezza. Inoltre, fornendo ai propri utenti un grado di anonimato più elevato, come da *policies* aziendali, di fatto finiscono per attrarre la quasi totalità delle attività di diffusione di contenuti illeciti, o comunque di propaganda, poste in essere da soggetti contigui ad ambienti filo-jihadisti e agli stessi membri delle organizzazioni terroristiche.

Nell'ultimo anno, in concomitanza con le recenti perdite territoriali da parte del c.d. Stato Islamico, si è riscontrato un significativo decremento

dell'attività mediatica del Daesh, in particolare per quanto concerne la diffusione di nuovi contenuti di proselitismo nel web, sia in termini quantitativi, che qualitativi. Infatti, si è notato che i pochi filmati e le infografiche emanati hanno standard qualitativi palesemente inferiori a quelli precedenti, segno, verosimilmente, che il Califfato è in fase di riorganizzazione/trasformazione e sta ristrutturando il suo network interno e ridelineando la propria strategia. In particolare, si sta passando da forme di comunicazione di massa, ben strutturate, alla diffusione di materiale autoprodotto attraverso l'utilizzo di mezzi più semplici, quali smartphones, ma che comunque trovano diffusione attraverso canali sommersi e forme di comunicazione compartimentate.

L'attività preventiva e informativa della Polizia Postale e delle Comunicazioni ha visto, inoltre, momenti di collaborazione con la Direzione Centrale della Polizia di Prevenzione e le locali Digos, anche per la collaborazione specialistica in caso di necessari approfondimenti tecnici in relazione a posizioni emergenti o monitorate sul territorio nazionale.

Infatti, la Polizia Postale e delle Comunicazioni concorre con altri organi di Polizia e di *intelligence* alla prevenzione e al contrasto dei fenomeni di proselitismo on line e di radicalizzazione, sia a livello nazionale che internazionale, posti in essere attraverso l'utilizzo di strumenti informatici e di comunicazione telematica. La sinergia tra i diversi comparti in tale ambito è divenuta sempre più incisiva, sia nell'ambito del raccordo info-investigativo che di quello tecnico-operativo.

Per quanto concerne, invece, l'attività di contrasto, la Polizia Postale e delle Comunicazioni si avvale di profili sotto copertura creati *ad hoc* e gestiti dagli operatori, con l'affiancamento dei mediatori linguistici e culturali. L'utilizzo di uno di tali account fittizi, nel tempo fatto "maturare" dagli investigatori nel corso delle diverse, quotidiane, attività di monitoraggio informativo e, dunque, accreditato all'interno dei canali e gruppi frequentati dagli internauti sostenitori dello Stato Islamico, ha permesso di condurre diverse, complesse, attività tecnico-investigative.

A titolo esemplificativo, si evidenziano, in particolare, due significativi risultati investigativi.

Il primo risultato investigativo (*Operazione ANSAR*) ha portato all'individuazione di un **minore italiano, di seconda generazione, di origine**

algerina, il quale, attraverso la rete, svolgeva un'intensa campagna di **proselitismo di matrice jihadista su Telegram**, istigando altri utenti a commettere delitti di terrorismo, fatti aggravati in quanto le azioni venivano compiute attraverso strumenti informatici e telematici. All'interno del canale Telegram, frequentato da circa 200 utenti e considerato tra i principali veicoli della narrativa dell'IS, venivano pubblicati messaggi testuali, immagini, video, infografiche e audio di propaganda del Daesh, tradotti in lingua italiana e rivolti in particolare ai c.d. "lupi solitari" presenti sul territorio nazionale.

Considerata l'impossibilità di acquisire elementi investigativi utili all'identificazione dell'amministratore del canale attraverso vie ufficiali dirette, il Servizio Polizia Postale ha attivato una mirata attività tecnico-investigativa che ha permesso di orientare le indagini finalizzate a individuarne l'amministratore, la cui identificazione è risultata complicata, in quanto il minore si è dimostrato particolarmente abile e competente a livello informatico, poiché utilizzava tecniche di anonimizzazione evolute (connessioni attraverso servizi di VPN e nodi TOR).

È stato possibile raggiungere il risultato sperato soltanto a seguito di una difficile e articolata attività tecnica svolta da personale del Servizio Polizia Postale anche attraverso l'utilizzo di software sviluppati ad hoc e rivelatisi di particolare efficacia. Le successive attività d'indagine, svolte attraverso l'attivazione di servizi di intercettazione delle comunicazioni telematiche, telefoniche e ambientali, nonché riscontrate da servizi di diretta osservazione, hanno consentito di acquisire concreti elementi di prova a carico di un cittadino italiano minorenne di "seconda generazione", nato in Italia da genitori di origine algerina, che è stato indagato per aver compiuto attività di proselitismo a favore dell'IS mediante diffusione e traduzione di contenuti di propaganda on line. Nonostante la giovane età, il minore risultava in possesso di elevate capacità tecnico-informatiche, padronanza linguistica non comune e approfondita conoscenza dei principali testi sacri dell'Islam, proponendosi quale punto di riferimento per tutti coloro che intendevano contribuire attivamente alla causa jihadista.

L'attività investigativa ha consentito di riscontrare e raccogliere elementi in ordine al percorso di **autoradicalizzazione** del minore, intrapreso esclusivamente in rete e sfociato in una successiva diffusione on line del proselitismo di matrice jihadista. Infatti, nella vita reale il ragazzo non

frequentava la moschea, né ambienti contigui all'estremismo islamico. Anche il contesto familiare, sebbene musulmano, risultava di impostazione musulmana, ma non integralista.

Oltre ai risultati operativi conseguiti, tale indagine ha presentato anche profili di rilevanza giudiziaria e sociale, in quanto è stata riconosciuta la pericolosità reale delle iniziative adottate dell'indagato, le quali, lungi da esaurire i propri effetti nella "dimensione virtuale", sono risultate concretamente rilevanti. Il puntuale intervento della Procura dei minori e della Polizia di Stato ha consentito di superare la mera fase accertativa della responsabilità penale del minore, avviando un dedicato percorso di recupero e deradicalizzazione, reso possibile dallo "scollegamento" del giovane dalla rete della c.d. *"cyber jihad"*. Come noto, infatti, ormai il web assurge a un ruolo fondamentale quale strumento strategico di propaganda dell'ideologia del Daesh, di reclutamento di nuovi combattenti, di finanziamento, di scambio di comunicazioni riservate nella pianificazione degli attentati e di rivendicazione degli stessi.

Infine, la seconda Operazione, denominata ***"Lupi del deserto"*** si è conclusa nell'**arresto di un cittadino egiziano** di 22 anni, irregolare sul territorio nazionale, per associazione con finalità di terrorismo internazionale e istigazione e apologia per delitti di terrorismo.

Le indagini, avviate nel 2017 con intercettazioni telefoniche, ambientali, telematiche e specifici servizi di osservazione e pedinamento h24. Il giovane arrestato è un appartenente all'ISIS, indottrinatosi con il materiale di propaganda di DAESH reperito on line. Gli elementi raccolti hanno evidenziato che il predetto ascoltava in continuazione, in una sorta di ***"brain washing"***, files audio di Imam radicali e della rivista "Dabiq" inneggianti all'odio per l'occidente, alla jihad e a sostegno degli atti di martirio. Dalle intercettazioni telematiche e accertamenti tecnici svolti dalla Polizia Postale e delle Comunicazioni, è emerso che il giovane è altresì organico anche alla macchina della propaganda del sedicente stato islamico. Infatti, gestiva gruppi e canali chiusi su Telegram, nei quali venivano diffuse le notizie delle attività dello Stato Islamico, tramite le agenzie mediatiche del Califfato. In particolare, era in assiduo contatto **con due connazionali**, anch'essi radicalizzati, con i quali scambiava video e audio Jihadisti e inneggianti l'Islam radicale.

Nei loro confronti il Ministro dell'Interno ha emesso un **decreto di espulsione** dal territorio italiano.

Trattandosi di un fenomeno a carattere transnazionale, sia per la natura internazionale del fenomeno, che per la stessa connaturata struttura della rete, risulta imprescindibile l'attivazione efficiente degli strumenti della cooperazione sovranazionale, sia ordinari che "nuovi", soprattutto per la condivisione di informazioni che, collegate a situazioni peculiari interne, riescono ad apportare indiscusso valore aggiunto alle attività di prevenzione messe in atto dalle diverse forze di polizia nazionali.

In ambito europeo, il Servizio Polizia Postale e delle Comunicazioni è il punto di contatto nazionale dell'Internet Referral Unit (IRU) di Europol, Unità preposta a ricevere dai Paesi Membri le segnalazioni relative ai contenuti di propaganda jihadista diffusi in rete e di orientarne l'attività. Lo scambio delle informazioni tra Paesi Membri viene effettuato attraverso l'utilizzo di specifiche piattaforme tecnologiche, tra cui *Check-the-Web* (CTW) e *SIRIUS*, appositamente create in ambito IRU a supporto del monitoraggio e delle indagini nell'ambito di terrorismo in Internet.

Parallelamente all'incremento dell'uso di strumenti telematici, sono cresciute le aspettative di sicurezza da parte del cittadino.

La Polizia Postale e delle Comunicazioni è impegnata, ormai da diversi anni, in campagne di sensibilizzazione e prevenzione sui rischi e pericoli connessi all'utilizzo della rete internet, rivolte soprattutto alle giovani generazioni.

Nello specifico si evidenzia la campagna itinerante della Polizia Postale e delle Comunicazioni *"Una Vita da Social"*, grazie alla quale sino ad oggi sono stati incontrati oltre **1 milione e 700 mila studenti, 180.000 genitori, 100.000 insegnanti** per un totale di **15.000 Istituti scolastici** e **250** città italiane.
Un progetto dinamico, innovativo e decisamente al passo con i tempi, che si avvicina alle nuove generazioni evidenziando sia le opportunità del web che i rischi di cadere nelle tante trappole dei predatori della rete, confezionando un vero e proprio "manuale d'uso", finalizzato ad evitare il dilagante fenomeno del cyberbullismo e tutte quelle forme di uso distorto della rete in generale e dei social network.
A disposizione degli utenti è presente la pagina **facebook e twitter** di "Una vita da social", gestita direttamente dalla Polizia Postale e delle Comunicazioni, dove vengono pubblicati gli appuntamenti, le attività, i contributi e dove i giovani internauti possono *"postare"* direttamente le loro impressioni ad ogni appuntamento.

Grande consenso ha riscosso la campagna **#cuoriconnessi**, che ha coinvolto 30.000 studenti, attraverso la proiezione di un docufilm e le testimonianze dirette dei minori vittime di prevaricazioni, vessazioni e violenze online.

Inoltre nel corso dell'anno sono stati realizzati incontri educativi su tutto il territorio nazionale raggiungendo oltre **300 mila studenti** e circa **3000 Istituti scolastici** per i quali è stata messa a disposizione anche un'email dedicata: progettoscuola.poliziapostale@interno.it.

Il portale del Commissariato di P.S. online è divenuto il punto di riferimento specializzato per chi cerca informazioni, consigli, suggerimenti di carattere generale, o vuole scaricare modulistica e presentare denunce.

Uno strumento agevole che consente al cittadino, da casa, dal posto di lavoro o da qualsiasi luogo si desideri, di entrare nel portale ed usufruire dei medesimi servizi di segnalazione, informazione e collaborazione che la Polizia Postale e delle Comunicazioni quotidianamente ed ininterrottamente offre agli utenti del web.

Di particolare importanza le denunce e le segnalazioni giunte anche sul sito del Commissariato di P.S. on-line per i reati di cyberbullismo, perpetrati soprattutto in ambito scolastico da parte di studenti nei confronti di compagni e perpetrati attraverso i social media, con atti denigratori e diffamatori nei confronti delle giovani vittime. Alcune attività sono sfociate nell'emissione da parte dei Questori di provvedimenti di ammonimento anche al fine di responsabilizzare minori autori del reato.

Attività del Commissariato di PS online

Richieste di informazioni evase	**19.088**
Segnalazioni ricevute dai cittadini	**18.722**
Denunce presentate dagli utenti	**10.922**

Ministero dell'Interno
Compartimento Polizia Postale e delle Comunicazioni
Lazio

Comunicato stampa

Resoconto dell'attività svolta dal Compartimento Polizia Postale e delle Comunicazioni del Lazio nel 2018

In un contesto socio-economico continuamente stravolto dalla diffusione di nuove tecnologie, è noto come negli ultimi anni ad un costante incremento del benessere dei cittadini abbia fatto da contraltare la continua diffusione sul mondo digitale di una serie di reati che in precedenza erano presenti esclusivamente nel mondo "reale".

In tale scenario "digitale", per molti particolarmente insidioso, si rende sempre più necessaria l'adozione di strategie di prevenzione e contrasto dei reati, al pari del mondo reale.

La Polizia Postale e delle Comunicazioni, dunque, ha il compito di indagare su tutto ciò che accade nel Web, ma anche vigilare e soccorrere gli internauti in difficoltà, svolgendo altresì una costante e puntuale attività di prevenzione grazie alle innumerevoli iniziative volte a fornire le dovute informazione sui rischi del Web.

Di seguito si indicano i risultati dell'attività espletata nell'anno 2018 dal Compartimento Polizia Postale e delle Comunicazioni per il Lazio.

Attività di prevenzione

Nell'ambito dell'attività volta a prevenire la commissione dei reati di propria competenza, il Compartimento ha svolto un'importante campagna di sensibilizzazione ed informazione dei cittadini.

In particolare, oltre alle 4722 denunce, la Polizia Postale ha trattato circa 1298 e-mail e segnalazioni.

Inoltre, nell'ambito di una vasta campagna, a livello nazionale, per la prevenzione dei rischi connessi alla navigazione in internet di adolescenti, gli operatori del Compartimento Polizia Postale e delle Comunicazioni di Roma hanno effettuato numerosi incontri presso gli Istituti Scolastici del Lazio, coinvolgendo circa 29195 studenti, 2376 docenti e 2739 genitori, trattando argomenti come phishing, hackering, adescamento on line, truffe, furti di identità e cyberbullismo.

Controllo del territorio

Al fine di prevenire e contrastare i reati commessi nell'ambito del circuito postale, questo Compartimento ha garantito 997 pattuglie sul territorio che si sono occupati di vigilare gli uffici postali della Regione, soprattutto per evitare rapine in danni di anziani intenti a ritirare la pensione

In tale ambito si segnala come siano stati recuperati 25.835 € derivanti da furto di corrispondenza e 191.373 € in seguito a tentate rapine.

Attività di repressione

Le indagini svolte dal Compartimento seguono le materie delineate dalla *Direttiva Ministeriale del 15 Agosto 2017*, che sono le seguenti:

- Pedopornografia e violenza su minori online;
- Cyber terrorismo;
- Hacking e financial cybercrime;
- Attacchi Cyber e protezione delle Infrastrutture Critiche del Paese;
- Reati postali.

In tale ambito, nell'anno 2018, per quanto attiene al contrasto alla pedopornografia online, sono stati centinaia di casi, che hanno portato all'arresto di 5 persone ed alla denuncia in stato di libertà di 65 soggetti per detenzione e condivisione di materiale pedopornografico.

Nel corso di tale attività sono stati inoltre visionati oltre 24.893 spazi virtuali.

In tale ambito, appare opportuno evidenziare, all'esito di un'articolata attività di indagine, l'esecuzione della misura cautelare degli arresti domiciliari nei confronti di un cittadino italiano, A.M. di anni 40, per il reato di detenzione e divulgazione di materiale pedopornografico.

Il soggetto, già noto a questo Compartimento per aver già commesso in passato i medesimi, recentemente era stato oggetto anche di un servizio giornalistico della trasmissione televisiva "Le Iene". L'indagine muoveva da una segnalazione fatta da un cittadino, abituale frequentatore di siti di incontri sessuali per adulti, il quale si accorgeva di aver ricevuto durante una sessione di chat con il quarantenne foto ritraenti una minore, indicata dall'interlocutore come figlia della sua attuale compagna.

L'immediata attività di indagine consentiva di identificare il soggetto autore dell'illecita divulgazione che, conseguentemente, veniva sottoposto a perquisizione personale, locale ed informatica. All'esito degli accertamenti di tipo tecnico-informatico effettuati sui dispositivi sequestrati venivano rinvenute n. 1256 immagini e n. 449 video dal chiaro contenuto pedopornografico, caratterizzati da particolare efferatezza in quanto coinvolgenti minori in giovanissima età, anche neonati, sottoposti a brutali atti sessuali.

Nell'ambito del cyber terrorismo nel corso del 2018 è stato effettuato un costante monitoraggio della rete, volto ad individuare fenomeni di eversione e terrorismo attuati tramite internet, sia a livello nazionale che internazionale, visionando circa 4040 spazi virtuali (siti web, media, blog, forum, profili di Social Network). In particolare, sono stati trattati 725 casi che hanno condotto alla denuncia di 41 persone, 3 arresti e 5 perquisizioni.

Tra le attività più significative in questo settore, si segnala un'operazione scaturita da un Ordine di Indagine Europeo proveniente dalla Francia e riguardante il rintraccio in territorio italiano di un cittadino francese nato in Algeria di 32 anni, responsabile di aver ucciso a coltellate un connazionale nel corso di una rissa svoltasi a Cenon (Francia).

Gli operatori di questo Compartimento, muovendo dalle tracce informatiche lasciate in seguito agli accessi effettuati dal latitante sul proprio profilo Facebook utilizzando la connessione alla rete Wi-fi pubblica di una nota libreria di Milano, riuscivano ad individuare l'ambito territoriale frequentato dall'uomo. La successiva attività di indagine, attuata anche attraverso complessi servizi tecnici che permettevano di monitorare gli spostamenti dello smartphone in uso al latitante, consentivano la sua precisa localizzazione sul treno Regionale Firenze-Rom; pertanto, personale di questo Compartimento si recavano alla stazione di Orte per evitare che il ricercato, una volta giunto a Roma, potesse dileguarsi. Il latitante, dunque, veniva così individuato, tratto in arresto e condotto presso la Casa Circondariale di Regina Coeli.

In materia di contrasto ai reati informatici contro la persona (molestie, minacce, trattamento illecito dei dati personali, accesso abusivo sui profili social network, stalking, cd. sextortion e diffamazione on line) sono stati trattati circa 1215 casi, monitorando oltre 8069 spazi virtuali, riscontrandone circa 177 con contenuti illeciti.

L'attività investigativa in questo settore ha portato alla denuncia di 110 persone ed all'esecuzione di 8 perquisizioni.

In materia e-commerce, contrasto al phishing o alla clonazione di carte di credito e/o debito, perpetrate con il furto di identità digitali e al furto di ingenti somme da conti correnti di società o risparmiatori (Financial cyber crime), sono state eseguite operazioni di particolare interesse anche a livello nazionale.

L'attività investigativa ha portato all'arresto di 6 persone ed all'esecuzione di 14 perquisizioni.

Le attività investigative del Compartimento in materia di e-commerce e telefonia, con oltre 1886 casi trattati ed un danno stimato superiore ai 2,5 milioni di euro, coprono una vasta casistica dalla falsa vendita on line di biglietti di eventi come concerti e partite di calcio, falsi annunci di locazione di case vacanza pubblicati in rete internet, false vendite on line di materiale telefonico ed informatico, di mezzi agricoli, di materiale elettrico, di autovetture, di TV.

Le indagini hanno riguardato molteplici siti internet di compravendita ed hanno portato alla denuncia di 274 persone per truffa, sostituzione di persona, appropriazione indebita, ricettazione, inosservanza dei provvedimenti dell'autorità e simulazione di reato).

Occorre evidenziare, infine, come nel corso del 2018 siano aumentati considerevolmente i casi di truffa online commessi mediante l'utilizzo di piattaforme di trading online illeciti; in tutte le segnalazioni ricevute, infatti, è possibile individuare il medesimo *modus operandi.*

In particolare, in seguito ai primi investimenti effettuati su portafogli virtuali, si ha da subito la percezione di ottenere grossi guadagni, e si è così invogliati ad effettuare ulteriori versamenti di somme di denaro sempre più consistenti, magari pressati da sedicenti consulenti della società che sollecitano il raggiungimento di risultati ancora migliori. Tuttavia, dopo i primi guadagli si iniziano a manifestare sul portafoglio virtuale le prime perdite che, sempre in seguito ai suggerimenti forniti dai sedicenti consulenti finanziari, si cerca di recuperare con nuovi investimenti, ma in tutti i casi si perde la somma che si è investito.

In tale contesto, questo Compartimento ha eseguito, in seguito all'emissione di apposito decreto da parte della competente Autorità Giudiziaria, il sequestro preventivo mediante oscuramento di oltre 15 siti utilizzati per commettere la specifica condotta criminosa.