Resoconto attività 2023
della Polizia Postale e delle Comunicazioni e dei Centri Operativi Sicurezza Cibernetica[1]

Il 2023 ha visto la Polizia di Stato porre in campo mirate attività volte a fronteggiare i complessi scenari legati ai crimini informatici.

In particolare l'impegno della Polizia Postale e delle Comunicazioni è stato costantemente indirizzato negli ambiti della prevenzione e contrasto alla pedopornografia online, alla protezione delle infrastrutture critiche di rilevanza nazionale, al financial cyber crime e a quelle relative alle minacce eversivo-terroristiche, riconducibili a forme di fondamentalismo religioso e di estremismo politico ideologico, anche in contesti internazionali.

CENTRO NAZIONALE PER IL CONTRASTO ALLA PEDOPORNOGRAFIA ONLINE (C.N.C.P.O.)

In uno scenario nel quale la continua evoluzione tecnologica influenza ogni azione del nostro vivere quotidiano, lo sforzo della Polizia Postale e delle Comunicazioni nell'anno 2023 è stato costantemente indirizzato alla prevenzione e al contrasto della criminalità informatica in generale, con particolare riferimento ai reati in danno di minori.

Il Centro Nazionale per il Contrasto alla Pedopornografia Online (C.N.C.P.O.) ha confermato il suo ruolo di punto di riferimento nazionale nella lotta alla pedofilia e pornografia minorile online.

A fronte di un numero complessivo di casi in diminuzione, non sembra ridursi il rischio per bambini e preadolescenti di essere oggetto di attenzioni sessuali da parte di adulti, mentre sono online, guardando i loro video preferiti e giocando ai videogiochi. Le denunce relative ai casi di adescamento online, infatti, raccontano di un numero di casi in lieve flessione, più alto per le fasce di potenziali vittime che non superano i 13 anni. Giova ancora evidenziare come si tratti di bambini e ragazzi che non dovrebbero avere accesso ai social e che dovrebbero essere puntualmente sorvegliati dai genitori, proprio perché particolarmente fragili per la tenera età.

Nell'anno in corso si è rilevato un incremento dei casi di *sextortion*, considerato negli ultimi anni un evidente fronte di rischio per i minori. In passato era appannaggio del mondo degli adulti, attualmente coinvolge frequentemente gli adolescenti, in particolare, in modo preoccupante, ragazzi tra i 15 e i 17 anni.

[1] Dati statistici rilevati al 21 dicembre 2023

Fondamentale è l'azione che il C.N.C.P.O. svolge nell'ambito della prevenzione, attraverso la continua e costante attività di monitoraggio della rete, per limitare la circolazione di foto e video a sfondo sessuale realizzati con l'utilizzo di minori degli anni 18.

Nell'anno che si sta concludendo sono stati visionati e analizzati **28.265** spazi web, di cui **2.739** inseriti in *black list* e oscurati, in quanto presentavano contenuti pedopornografici.

Altrettanto importante è il lavoro di contrasto effettuato dal Centro e dalle articolazioni territoriali della Specialità. L'impegno e la preparazione delle donne e degli uomini della Polizia Postale hanno permesso, nel 2023, di deferire **1.224** soggetti.

PEDOPORNOGRAFIA E ADESCAMENTO ONLINE	**2022***	**2023****
Persone indagate	1459	1224
Siti in Black List	2662	2739
* -dati rilevati al 21/12/2022 **- dati rilevati il 21/12/2023		

Adescamento online

Nel 2023 è stato rilevato un lieve calo dei casi di adescamento on line, confermando però in larga parte il coinvolgimento di minori di età compresa tra i 10 e i 13 anni. Infatti, la fascia dei preadolescenti è quella che maggiormente ha avuto interazioni sessuali tecno-mediate, **206** rispetto ai **351** casi totali.

Persiste il lento incremento dei casi relativi a bambini adescati di età inferiore ai 9 anni, *trend* che sta diventando più consistente in seguito all'avvicinamento precoce agli strumenti informatici dei bambini più piccoli. I minori sotto i 9 anni di età, adescati in rete nel periodo di rifermento sono stati **31**, pari al **9%** dei casi trattati dalla Polizia Postale.

Social network e videogiochi online sono i luoghi di contatto tra minori e adulti più frequentemente teatro delle interazioni nocive, a riprova ulteriore del fatto che il rischio si concretizza con maggiore probabilità quando i bambini e i ragazzi si esprimono con spensieratezza e fiducia, nei linguaggi e nei comportamenti tipici della loro età.

Cyberbullismo

L'analisi dei dati di cyberbullismo ha confermato la diminuzione dei casi dovuta alla normalizzazione delle abitudini dei ragazzi, non si può escludere che il ritorno ad una vita sociale priva di restrizioni abbia avuto un'influenza positiva sulla qualità delle interazioni sociali, delle relazioni tra coetanei e che la costante opera di sensibilizzazione svolta dalla Polizia Postale così come da altre istituzioni e organizzazioni del terzo settore, presso le strutture scolastiche, abbia mantenuto alta l'attenzione degli adulti e dei ragazzi stessi sulla necessità di agire responsabilmente e correttamente in rete.

Nel 2023 sono stati trattati **284** casi di cyberbullismo. Di contro, è stata registrata una flessione del numero dei minori segnalati all'Autorità Giudiziaria, **104** rispetto ai **127** dello scorso anno.

CYBERBULLISMO	**2022***	**2023****
Casi trattati vittime 0-9 anni	17	8
Casi trattati vittime 10-13 anni	87	71

Casi trattati vittime 14-17 anni	219	205
TOTALE	**323**	**284**
* -dati rilevati al 21/12/2022 **- dati rilevati il 21/12/2023		

	2022*	**2023****
Minori denunciati per Cyberbullismo	127	104
* -dati rilevati al 21/12/2022 **- dati rilevati il 21/12/2023		

Sextortion

Nell'anno di riferimento è stato registrato un incremento dei casi di *sextortion* in danno di minori, passando dai **130** casi del 2022 ai **136** registrati nel 2023. Il fenomeno, che di solito colpisce gli adulti in modo violento e subdolo, spesso fa leva su piccole fragilità ed esigenze personali, minacciando, nel giro di qualche click, la tranquillità delle persone.

Questo reato sta coinvolgendo sempre più spesso vittime minorenni, con effetti lesivi potenziati, quali la vergogna e la frustrazione che si ingenera per la difficoltà nel gestire la diffusione di immagini intime magari legate ad una precoce sessualità.

La maggior parte dei casi riguarda minori di età compresa tra i 14 e i 17 anni, prevalentemente maschi.

C.N.C.P.O. – ATTIVITÀ DI POLIZIA GIUDIZIARIA

Si riportano di seguito, le attività investigative di maggior rilievo del Centro Nazionale per il Contrasto alla Pedopornografia online:

Operazione "Shadow Man") L'unità sotto copertura del Centro Nazionale Contrasto alla Pedopornografia Online ha eseguito una custodia cautelare in carcere, nei confronti di un cinquantenne, produttore di materiale di pornografia minorile, per anni attivo nella comunità virtuale pedofila *The Love Zone (TLZ)*, ove si era distinto per il significativo contributo apportato, in termini di materiale pedopornografico, anche autoprodotto.
L'operazione trae origine da complesse e lunghe indagini svolte sul Darkweb in collaborazione con Europol e la polizia britannica (*Online CSA Covert Intelligence Team - OCCT*). L'uomo, conosciuto con lo pseudonimo di *Shadow*, per oltre un decennio era riuscito ad eludere le indagini e rimanere anonimo, continuando nel mentre le condotte di violenza sessuale aggravata, commessa ai danni di minori di anni 10; associazione per delinquere finalizzata alla diffusione di pratiche di pedofilia, alla condivisione di notizie utili all'adescamento di minori e allo scambio, detenzione e diffusione di materiale pedopornografico. L'utente rappresentava un *high value target* internazionale nell'ambito delle indagini delle polizie di tutto il mondo impegnate in attività sotto copertura online nel contrasto alla pornografia minorile all'interno delle citate comunità pedofile virtuali.

Arresto di un cittadino di origine turca per produzione e detenzione di materiale pedopornografico Personale della Sezione Operativa per la Sicurezza Cibernetica della Polizia Postale e delle Comunicazioni di Bolzano ha eseguito, congiuntamente al personale del C.N.C.P.O., la perquisizione nei confronti di un soggetto di nazionalità turca. Lo stesso inviava ad un suo connazionale immagini a contenuto pedopornografico su *Twitter*. Dall'analisi delle suddette immagini veniva identificato il figlio infante dell'indagato, il quale veniva sottoposto

ad abusi sessuali registrati con dispositivi digitali. L'attività si è conclusa con l'esecuzione della misura cautelare in carcere nei confronti del padre della vittima.

Operazione "Fast and done" Nel mese di agosto u.s., personale del C.N.C.P.O. - Centro Nazionale per il Contrasto della Pedopornografia Online del Servizio Polizia Postale di Roma ha dato esecuzione a un decreto di perquisizione per detenzione e diffusione di materiale di pornografia e violenza sessuale su minore emesso dall'Autorità giudiziaria capitolina nei confronti di un 36enne.
L'indagine trae origine da una segnalazione del collaterale australiano relativa a un utente del *Dark Web*, verosimilmente riconducibile al territorio italiano. Da ulteriori riscontri venivano collegate all'indagine due segnalazioni ricevute dal C.N.C.P.O. nell'ambito della cooperazione internazionale di polizia. Dall'incrocio dei dati oggetto di tutte le citate segnalazioni sono emersi elementi allarmanti circa un attuale pericolo concreto di abusi sessuali perpetrati su un minore di anni 10, nonché in merito all'autoproduzione e alla diffusione di materiale di pornografia minorile. Nel corso della perquisizione, richiesta ed eseguita in urgenza, sono stati rinvenuti oltre 20.000 *files*, che hanno consentito di procedere all'arresto in flagranza di reato per produzione, divulgazione e detenzione di ingente quantitativo di materiale pedopornografico e per violenza sessuale aggravata, ai danni di un minore.

Operazione "Ciaoamigos" Nel mese di settembre u.s., il Centro Nazionale per il Contrasto alla Pedopornografia Online (C.N.C.P.O.) del Servizio Polizia Postale e delle Comunicazioni ha coordinato l'esecuzione di 6 decreti di perquisizione delegati dalla Procura della Repubblica di Salerno nei confronti di altrettanti indagati, ritenuti responsabili di detenzione e diffusione di materiale di pornografia minorile. L'indagine, condotta in modalità sotto copertura sul portale *ciaoamigos.it* dal personale della Sezione Operativa per la Sicurezza Cibernetica della Polizia Postale di Salerno, è scaturita su impulso del C.N.C.P.O., a seguito della segnalazione di un cittadino tramite il *Commissariato di P.S. Online*. L'operazione ha coinvolto, nella fase esecutiva, gli Uffici di Specialità della Campania, Toscana, Calabria, e Lombardia.

Operazione "Lucignolo" Il Centro Operativo per la Sicurezza Cibernetica Polizia Postale per il Piemonte e Valle D'Aosta, coordinato dal C.N.C.P.O. - Centro Nazionale per il Contrasto della Pedopornografia Online del Servizio Polizia Postale, ha svolto per diversi mesi un'attività *sotto copertura* su una nota applicazione di messaggistica, finalizzata all'individuazione di soggetti, dediti alla pubblicazione e divulgazione di materiale realizzato mediante sfruttamento di minori degli anni 18 e conclusasi nel decorso mese di ottobre. Oltre 100 investigatori cibernetici della Polizia di Stato sono stati impegnati in tutta Italia nell'esecuzione di 30 perquisizioni delegate dalla Procura della Repubblica di Torino.
Gli indagati, con l'utilizzo di accorgimenti tecnici volti al mantenimento dell'anonimato, scambiavano in rete materiale illecito di diversa natura, che documentava anche violenze sessuali. I provvedimenti emessi dall'Autorità Giudiziaria di Torino hanno consentito di denunciare 30 utenti, responsabili di aver condiviso in rete materiale, realizzato mediante lo sfruttamento sessuale di minori, di cui 3 tratti in arresto in flagranza di reato per detenzione di ingente quantità di materiale di pornografia minorile.

Operazione "Seven" Gli investigatori del Centro Operativo per la Sicurezza Cibernetica Polizia Postale per la Lombardia, dopo oltre un anno di indagini condotte in modalità "*sotto copertura"* sulla rete Internet, nel decorso mese di novembre hanno concluso un'indagine grazie alla quale sono stati identificati 29 soggetti che, sfruttando le potenzialità di una nota applicazione di messaggistica, partecipavano a "*canali*" e "*gruppi*" finalizzati alla produzione e alla condivisione di foto e video pedopornografici ritraenti violenze sessuali su minori; gli abusi, in particolare, riguardavano prevalentemente bambine e bambini in tenera età e, in alcuni casi, anche neonati. Le perquisizioni personali, locali e sui sistemi informatici, emesse

dalla Procura Distrettuale meneghina e coordinate dal C.N.C.P.O. - Centro Nazionale per il Contrasto della Pedopornografia Online del Servizio Polizia Postale di Roma, hanno impegnato più di 150 uomini della Polizia di Stato in oltre 20 province di 9 regioni italiane, consentendo di trarre in arresto 10 soggetti in flagranza di reato per detenzione di ingente quantità di materiale realizzato mediante l'utilizzo di minori di 18 anni e di denunciarne 16 in stato di libertà, nonché sequestrare numerosi telefonini, tablet, hard disk, pen drive, computer e account di email e profili social. Tra i membri del gruppo è stato possibile distinguere promotori, organizzatori e partecipi, con ruoli e compiti ben definiti, riuscendo a individuare una vera e propria associazione a delinquere finalizzata ad acquisire e diffondere materiale pedopornografico.

Esecuzione 2 OCC per Live Distant Child Abuse Nel corrente mese di dicembre, personale del Centro Nazionale per il Contrasto alla pedopornografia Online (C.N.C.P.O.), unitamente a quello della Sezione Operativa per la Sicurezza Cibernetica della Polizia Postale di Varese, ha eseguito due misure cautelari nei confronti di un uomo e una donna ritenuti responsabili di aver commesso - dietro corrispettivo in denaro - sessioni *live* di abusi sessuali su minori. Si tratta del c.d. Live Streaming Child Abuse. L'attività trae origine da un'indagine condotta dal C.N.C.P.O. e scaturita da una segnalazione di operazioni sospette pervenuta, tramite Guardia di Finanza, dall'Unità di Informazione Finanziaria (UIF) della Banca d'Italia, successivamente confermata da ulteriori informazioni ricevute dalla Polizia Postale dalla Homeland Security Investigation (HSI) nell'ambito della cooperazione internazionale di polizia relativa ad un network di soggetti coinvolti nel Live Streaming Child Abuse. Gli abusanti, di nazionalità filippina, ricevevano versamenti da account PayPal riconducibili a utenti europei per poter assistere a spettacoli video in diretta, aventi a oggetto abusi sessuali su minori, commissionati sul momento dagli utenti interessati. Tra questi vi era anche un cittadino italiano che, tra il 2019 e il 2020, aveva effettuato pagamenti per acquistare filmati preregistrati e spettacoli in *live streaming* con protagonisti minori. Nel decorso mese di novembre, la Polizia Postale di Milano effettuava, una perquisizione domiciliare e informatica sui dispositivi in uso all'indagato, la cui analisi forense consentiva di far emergere evidenze probatorie a carico dell'indagato e della moglie di nazionalità filippina, la quale, nel periodo in cui viveva all'estero, faceva parte del citato network e offriva a pagamento sessioni di *Live Streaming Child Abuse* in danno dei due figli minori e permetteva l'emissione della misura della custodia cautelare in carcere nei confronti dell'uomo, mentre per la moglie, madre di un infante, è stato previsto l'obbligo di presentazione alla polizia giudiziaria e il divieto di espatrio.

Operazione "Viper" Nel mese di dicembre il Servizio Polizia Postale e delle Comunicazioni ha coordinato l'esecuzione, su tutto il territorio nazionale, di 57 decreti di perquisizione delegati dalla Procura della Repubblica di Venezia nei confronti di altrettanti indagati, nell'ambito del contrasto alla pedopornografia online. L'operazione ha coinvolto gli Uffici di Specialità delle Marche, Puglia, Emilia Romagna, Sardegna, Sicilia orientale e occidentale, Toscana, Liguria, Lombardia, Campania, Umbria, Abruzzo, Calabria, Lazio e Piemonte.
L'indagine, condotta dal Centro Operativo per la Sicurezza Cibernetica della Polizia Postale di Venezia e coordinata, anche sul piano internazionale, dal Centro Nazionale per il Contrasto alla Pedopornografia Online (C.N.C.P.O.) del Servizio Polizia Postale, è scaturita dall'analisi dei dispositivi informatici sequestrati a un precedente indagato, tratto in arresto in flagranza, nell'ottobre 2022, per detenzione di ingente quantitativo di materiale pedopornografico. Nel corso della successiva analisi forense, è emerso che il soggetto era molto attivo sulla piattaforma *Viber* ed era iscritto a 42 gruppi e 247 canali dediti allo scambio di materiale realizzato mediante l'utilizzo di minori di 18 anni. I cospicui contenuti multimediali scambiati tra gli utenti, raffiguravano anche torture perpetrate in danno delle piccole vittime.
L'attività, condotta in modalità sotto copertura dal personale del COSC Veneto, ha consentito di identificare, oltre a numerosi utenti italiani, anche molteplici stranieri, riconducibili a 44

diversi Stati esteri, per i quali il C.N.C.P.O. ha proceduto ad attivare i canali di cooperazione internazionale di polizia, tramite Europol, Interpol e Ameripol, con i quali è stata pianificata una *Joint Action*, alla quale hanno aderito diversi collaterali, che, a partire dalla prossima settimana, daranno esecuzione ai provvedimenti delle rispettive AA.GG. nazionali. Le perquisizioni hanno consentito di arrestare 28 soggetti e di denunciarne in stato di libertà 24.

CENTRO NAZIONALE ANTICRIMINE PER LA PROTEZIONE DELLE INFRASTRUTTURE CRITICHE (C.N.A.I.P.I.C.)

Lo scenario aggiornato della minaccia cyber vede ormai stabilmente aggiungersi, ad una matrice puramente criminale, seppur presente, un'origine riconducibile anche ad attori statuali, conseguenza della estrema instabilità dello scenario geopolitico di riferimento.

Il conflitto russo-ucraino ha definitivamente dimostrato come, in epoca attuale, il dominio del cyberspazio abbia assunto una valenza fondamentale. Il dominio cibernetico è così divenuto nuova dimensione, spazio imprescindibile per lo sviluppo delle nuove guerre. Le offensive hacktiviste russe hanno mantenuto una significativa intensità dall'inizio del conflitto, in particolare sono state lanciate decine di offensive contro l'Ucraina e i Paesi NATO. Ad esempio, il gruppo hacker filorusso, *NoName05,* ha iniziato a lanciare una serie di offensive contro realtà italiane in segno di protesta contro la politica del nostro Paese, definita "russofoba". Le offensive hanno impattato tra l'altro realtà governative, strutture del comparto sanitario, operatori del trasporto locale, istituti bancari e provider delle telecomunicazioni.

Allo stesso modo, rilevanti sono le proiezioni nel dominio cibernetico del conflitto Israele-Hamas. Sin dall'inizio del conflitto, infatti, gruppi hacker hanno iniziato a dirigere attacchi per compromettere le infrastrutture critiche israeliane, arrecare disservizi alla popolazione, estendendo le azioni ostili ai danni di infrastrutture di paesi occidentali, tra cui l'Italia, ritenuti vicini alla causa israeliana.

Le attività di indagine in questo particolare ambito risultano molto complesse, sia per l'assoluto livello tecnologico e quindi delle capacità tecniche degli attori, sia per la natura transnazionale dell'azione offensiva, che richiede, regolarmente, l'attivazione di canali di cooperazione internazionale. L'ostacolo primario è costituito dalla disomogeneità dei sistemi legislativi nazionali, soprattutto in tema di regole per l'acquisizione della prova digitale e in materia di data retention.

La Polizia Postale ha affinato le tecniche info/investigative, implementando l'attività informativa e di monitoraggio ad ampio spettro, esteso anche al darkweb.

Per mitigare gli effetti degli attacchi e svolgere un'azione incisiva, il C.N.A.I.P.I.C. del Servizio Polizia Postale e delle Comunicazioni assume, per ciascuno dei maggiori incidenti di sicurezza, la guida degli accertamenti tecnico/investigativi, in supporto ai responsabili tecnici degli Enti attaccati, in sinergia con gli altri attori pubblici dell'architettura nazionale di cyber sicurezza.

Nell'anno in corso il C.N.A.I.P.I.C., sotto la direzione della Procura della Repubblica di Roma, ha partecipato alla vasta operazione internazionale condotta dall'FBI, Europol ed Eurojust, che ha visto lo smantellamento di uno dei market underground più famosi noto come Genesis Market.

Tale attività ha portato all'emissione di 37 decreti di perquisizione personale, locale e informatica, eseguite dal C.N.A.I.P.I.C. e dai Centri Operativi per la Sicurezza Cibernetica di Campania Basilicata e Molise, Lazio, Lombardia, Puglia, Emilia Romagna, Calabria, Veneto, Sicilia Occidentale, Abruzzo, Friuli Venezia Giulia, Liguria, Toscana, Trentino-Alto Adige ed Umbria.

Attività di monitoraggio e prevenzione sono state svolte dal Centro, in regime h24, per grandi eventi di interesse nazionale come il 73° Festival della Canzone Italiana di Sanremo, l'80^ Mostra Internazionale d'Arte Cinematografica di Venezia e il Cultural Heritage in 21st Century organizzato dal Ministero degli Affari Esteri a Napoli.

Attacchi infrastrutture critiche ad istituzioni, aziende e privati	**2022***	**2023****	**Variazione percentuale**
Attacchi rilevati	12.825	11.930	-7%
Persone indagate	332	220	-34%
Alert diramati	112.271	75.956	-32%
Richieste di cooperazione HTC	75	79	+5%
* -dati rilevati al 21/12/2022 **- dati rilevati il 21/12/2023			

CYBER FRAUDS

Nell'ambito delle competenze della Polizia Postale si segnala l'intensificazione dell'attività di prevenzione attraverso il monitoraggio attivo della rete e un'articolata attività di contrasto alle **attività predatorie online** (***oltre 3.500 le persone deferite all'A.G.)***, in particolare nel settore dell' e-commerce.

Truffe OnLine	**2022***	**2023***	**Variazione percentuale**
Casi trattati	15.394	16.325	**+6%**
Persone indagate	3511	3571	**+2%**
Somme sottratte	**€ 114.459.014**	**€ 137.202.592**	**+20%**
* -dati rilevati al 21/12/2022 **- dati rilevati il 21/12/2023			

In relazione alle truffe sul web, anche nel corso del 2023, si è riscontrato un significativo incremento degli illeciti legati al fenomeno del **falso trading online** (**3.360** ***i casi trattati, 188 le persone denunciate per un totale di 109.536.088 Euro di profitti illecit)***, con l'aumento del numero di portali che propongono programmi speculativi, apparentemente redditizi e l'utilizzo di tecniche molto sofisticate per contattare le vittime.

L'attività investigativa, qualora la denuncia sia tempestiva, prevede l'immediata attivazione dei canali di Cooperazione Internazionale di Polizia, con la richiesta del blocco urgente delle somme versate e l'effettuazione di accertamenti sui flussi finanziari, che normalmente sono destinati all'estero.

I REATI CONTRO LA PERSONA ONLINE

Sono stati **31** i casi di ***Codice Rosso*** che hanno visto la Polizia Postale impegnata direttamente nel contrasto dei reati commessi contro la persona attraverso la rete.

Reati contro la persona perpetrati OnLine[1]	**2022***	**2023****	**Variazione percentuale**
Casi trattati	9.200	9.433	+3%
Persone indagate	1.158	1.235	+7%

[1] – *Stalking* / diffamazione online / minacce / *revenge porn* / molestie / sextortion / illecito trattamento dei dati / sostituzione di persona / hate speech / propositi suicidari
* -dati rilevati al 21/12/2022
**- dati rilevati il 21/12/2023

Specifiche iniziative sono state rivolte all'attività di prevenzione e contrasto al fenomeno degli atti intimidatori nei confronti della categoria dei giornalisti e servizi di monitoraggio dei canali di diffusione, costituiti da siti web, piattaforme digitali, profili e pagine presenti sui social network più noti (Facebook, Twitter, Instagram, Telegram, Pinterest e Youtube), finalizzati ad arginare la diffusione del linguaggio d'odio (hate speech).

La Sezione Operativa è stata impegnata anche nell'individuazione di proposte di vendita online di prodotti contraffatti e dell'utilizzo illecito di segni distintivi dei marchi registrati, per la tutela del made in italy sempre più messo in pericolo dal c.d. fenomeno dell'*italian sounding*.

Il monitoraggio di siti e spazi *web* (blog, gruppi social e siti dedicati) dediti a giochi e scommesse clandestine è un altro settore particolarmente seguito dalla Polizia Postale e delle Comunicazioni, sia per contrastare la diffusione irregolare o illegale, che per tutelare gli interessi dei consumatori, specie se minori d'età: numerosi sono i siti con sedi legali presso paesi esteri, che operano in Italia, anche se privi della prevista autorizzazione per poter esercitare legalmente la raccolta di scommesse.

Nel corso del 2023 sono state implementate anche le attività di monitoraggio relative alla vendita online di tabacchi, sigarette elettroniche e liquidi da inalazione in rete, su siti sprovvisti delle relative autorizzazioni da parte dell'Agenzia delle Dogane e Monopoli.

Di primaria importanza, altresì, è stata l'attività rivolta all'individuazione di persone che hanno manifestato intenti anticonservativi, attraverso le piattaforme social, con la tempestiva attivazione di tutte le procedure necessarie per la salvaguardia delle vite umane, anche attraverso l'ausilio degli uffici di polizia competenti territorialmente (**166** le segnalazioni veicolate attraverso il Commissariato di P.S. OnLine agli uffici territoriali e **37** gli interventi eseguiti sul territorio direttamente dai C.O.S.C. della Polizia Postale e delle Comunicazioni).

ATTIVITÀ DI POLIZIA GIUDIZIARIA

Arresto di 8 persone responsabili di truffe romantiche. Identificate 32 vittime. Oltre 400mila euro sottratti Il Centro Operativo per la Sicurezza Cibernetica della Polizia Postale di Roma ha arrestato otto persone, in esecuzione di una ordinanza applicativa di misure cautelari emessa dal G.I.P. di Roma per truffa aggravata, riciclaggio e sostituzione di persona.

Le indagini della Polizia Postale hanno avuto l'obiettivo di contrastare il sempre più diffuso e odioso fenomeno delle cd. "truffe romantiche", reati contro il patrimonio commessi in danno di persone fragili, che i criminali ricercano e individuano sui social network, portando poi a termine il progetto criminale, sfruttando le debolezze e le vulnerabilità delle vittime.
Questa indagine prende le mosse dalla denuncia di una signora, contattata su Facebook da "Larry Brooks", sedicente ufficiale dell'esercito statunitense, di stanza in Siria, con la foto profilo raffigurante un affascinante uomo di mezza età. Per rendere più verosimile la truffa architettata, i criminali si spingevano a creare fittizie identità di studi legali che confermavano, utilizzando comunicazioni via mail, le esigenze ed urgenze economiche di "Larry Brooks".
I primi accertamenti effettuati in rete e sui flussi finanziari confermavano i sospetti che il profilo fake "Larry Brooks" avesse mietuto molte vittime e truffato decine di donne; nel corso delle indagini emergevano ben 32 vittime accertate, con un provento illecito di circa **400.000 euro** nel periodo dal 2018 al 2021.
La lunga e complessa attività investigativa è stata condotta affiancando tecniche classiche di investigazione ad attività di analisi del traffico delle comunicazioni internet e dei flussi finanziari e ha consentito di identificare nel Lazio gli autori.
Sui conti correnti, riferibili al gruppo criminale, sono transitate somme di denaro provento delle truffe, inviate direttamente dalle vittime, per poi essere incassate o trasferite su conti nelle disponibilità dei complici, in molti casi con rimesse di denaro all'estero, per la condivisione dei proventi della truffa.
In relazione al quadro indiziario emerso, la Procura della Repubblica di Roma ha contestato il concorso in truffa, aggravata dall'aver approfittato delle condizioni di minorata difesa delle vittime e dalla transnazionalità del reato, nonché il reato di riciclaggio dei proventi del reato.

Truffa "Sei arruolato, vieni a prendere le misure per la divisa" La Polizia Postale ha denunciato per il reato di sostituzione di persona e detenzione abusiva d'armi un uomo di Frascati, di 54 anni, indiziato per aver raggirato un giovane disoccupato, promettendogli un posto di lavoro e per aver gettato discredito sulla Gendarmeria Vaticana.
L'indiziato, venuto a conoscenza delle aspirazioni del giovane disoccupato, si presentava falsamente come Ufficiale dell'Arma dei Carabinieri e, millantando rapporti privilegiati con la Gendarmeria Vaticana, si proponeva quale intermediario per l'assunzione del giovane nel Corpo della Gendarmeria.
Il giovane e il padre si convincevano a versare una somma di denaro in cambio del fattivo interessamento; seguiva un fitto scambio di mail false con la Gendarmeria Vaticana per trarre in inganno la vittima del reato, con tanto di compilazione di test selettivi di ingresso, indicazione del buon esito delle prove e addirittura riferimenti ad una futura convocazione presso la sede della Gendarmeria Vaticana per le *"prove della divisa"*.
Il giovane, convinto del buon esito delle selezioni, si presentava personalmente presso gli uffici della Gendarmeria Vaticana, scoprendo di essere caduto vittima di un truffatore.
La Gendarmeria Vaticana, resasi conto della truffa e preso atto del discredito in danno della prestigiosa Istituzione e del suo Comandante, segnalava i fatti al Centro Operativo per la Sicurezza Cibernetica – Polizia Postale di Roma, facendo scattare le indagini, coordinate dalla Procura della Repubblica capitolina, che consentivano, attraverso l'esame delle evidenze informatiche, di individuare e denunciare il sospetto autore.
Su delega della Procura si procedeva a perquisizione locale personale nei confronti del soggetto indagato, consentendo il rinvenimento e successivo sequestro di device e di materiale predisposto per simulare l'appartenenza ad un corpo di polizia, in particolare due pistole replica senza il previsto tappo rosso di sicurezza e due portatessere con placche metalliche riconducibili all'agenzia governativa americana FBI.

Associazione a delinquere finalizzata alla truffa e al riciclaggio: il COSC Umbria dà esecuzione a 18 decreti di perquisizione Personale della Specialità, coordinato dalla Procura

della Repubblica presso il Tribunale di Spoleto, ha dato esecuzione a 18 decreti di perquisizione nei confronti di altrettante persone, operative su tutto il territorio nazionale, indagate per i reati di truffa, ricettazione e riciclaggio.
Le complesse indagini, avviate a seguito della presentazione di numerose querele da parte delle vittime di truffe "romantiche" e di altri reati hanno consentito di delineare una rete criminale articolata su due livelli:
il primo livello, fortemente gerarchizzato e prevalentemente radicalizzato nei paesi dell'Africa centro occidentale, si occupava di creare falsi profili al fine di adescare ignare vittime;
il secondo livello, invece, costituito da decine di persone deputate al riciclaggio del denaro fraudolentemente ottenuto, aveva l'incarico di mettere a disposizione i propri conti ovvero di reclutare persone disposte a fornire, talvolta inconsapevolmente, il proprio conto corrente per far confluire le transazioni illecite in cambio di una percentuale già stabilita dal gruppo criminale.
Gli indagati, situati capillarmente sull'intero territorio nazionale, sono stati in grado di raggiungere vittime in svariati paesi europei ed extraeuropei, seguendo un modus operandi relativamente semplice.
In particolare, una volta ottenuto il contatto con la potenziale vittima su uno dei numerosi social network, la stessa veniva coinvolta in un legame affettivo virtuale tale
da convincerla a versare spontaneamente somme di denaro al suo "amato virtuale" per consentirgli di "risolvere" asseriti problemi. In caso di rifiuto, gli indagati erano arrivati persino ad effettuare delle vere e proprie estorsioni, minacciando le vittime di pubblicare foto e video "intimi" o conseguenze legali per dei supposti comportamenti illeciti della vittima.
Successivamente, i proventi così ottenuti venivano smistati su diversi conti correnti ed utilizzati per l'acquisto di beni di varia natura, automobili, materiale edile, condizionatori ecc. che venivano poi spediti verso la Nigeria all'interno di alcuni container.
Le indagini informatiche eseguite su alcuni apparati mobili a disposizione dei correi hanno consentito di constatare l'esistenza di veri e propri gruppi su dei social network,
creati con utenze straniere, per mantenersi in contatto e con lo scopo di gestire le "vittime - clienti", di riciclare il denaro, nonché le percentuali da condividere in considerazione della tipologia "dell'affare".
L'incisivo impulso della magistratura nell'attività di indagine effettuata nei confronti dei compartecipi ubicati in diversi Paesi UE – extra UE e il decisivo intervento del Servizio Polizia Postale e delle Comunicazioni, anche tramite l'attivazione dei canali di cooperazione internazionale (Europol/Interpol), hanno permesso di scoprire un giro d'affari di oltre un milione di euro in due anni.
Altrettanto preziosa è stata la collaborazione di Poste Italiane S.p.A. e di altri istituti di credito, che hanno, in tempi brevi, fornito i riscontri necessari per individuare la catena di trasferimenti di denaro originata dalle attività illecite compiute dalla struttura malavitosa.
Le indagini svolte dal Centro Operativo per la Sicurezza Cibernetica Umbria hanno portato all'individuazione e consequenziale esecuzione di 18 perquisizioni, coordinate dal Servizio Centrale di Polizia Postale e delle Comunicazioni e la collaborazione dei Centri Operativi della Campania, Emilia Romagna, Lazio, Liguria, Marche, Sicilia e Veneto, nelle province di Modena, Padova, Genova, Pesaro, Latina, Caserta, Campobasso, Palermo ed il concorso del Reparto Prevenzione Crimine Veneto coinvolto dalla Direzione Centrale Anticrimine.

Estorsioni in Rete: utenti di siti di incontri minacciati e costretti a pagare da sedicenti sfruttatori. La Procura della Repubblica di Perugia emette sei decreti di perquisizione

Personale del Centro Operativo Sicurezza Cibernetica di Perugia ha eseguito 6 decreti di perquisizione personale, locale ed informatica, emessi dalla procura di Perugia nei confronti di altrettanti cittadini di nazionalità straniera, ma residenti in Italia, indagati per i reati di estorsione e minacce in danno di alcuni utenti di siti di incontro.

L'attività di indagine, condotta dal personale della Specialità unitamente alla Squadra Mobile della Questura di Perugia, è originata dalla denuncia di un uomo che, dopo aver contattato delle ragazze su un sito di incontri, è stato minacciato da ignoti soggetti, che hanno paventato mali ingiusti a lui e ai familiari e che lo hanno costretto a pagare – a più riprese – un importo complessivo superiore a 3000 euro.
Dagli approfondimenti investigativi è emerso che il "*modus operandi"* usato dagli autori delle minacce - operanti sull'intero territorio nazionale, è sempre stato lo stesso: dopo essersi presentati come "gestori" di alcune ragazze presenti sui siti d'incontri, hanno inviato ai fruitori, tramite applicativi di messaggistica istantanea, una serie di minacce con la scusa di aver fatto perdere del tempo – e quindi degli introiti – alle "loro" ragazze, denaro che avrebbe dovuto essere necessariamente ristorato dalle vittime per evitare il concretizzarsi delle minacce.
Gli investigatori della Squadra Mobile e della Polizia Postale perugina, a questo punto, hanno incrociato migliaia di dati, tra tabulati telefonici e file di log, che hanno portato all'individuazione di 6 soggetti, che potrebbero avere un diretto coinvolgimento nella vicenda.
Le attività di perquisizione locale, personale e informatica – eseguite nel capoluogo ligure è stata coordinata dal Servizio Polizia Postale e delle Comunicazioni ed è stata effettuata in sinergia con il Centro Operativo per la Sicurezza Cibernetica – Polizia Postale e delle Comunicazioni Liguria e con la Squadra Mobile di Genova.
All'esito delle perquisizioni, gli operatori hanno sottoposto a sequestro numerosi supporti informatici che saranno oggetto di specifici accertamenti tecnici.

Esecuzione della misura cautelare del divieto di avvicinamento nei confronti del marito La Procura Distrettuale di Catania ha delegato la Polizia di Stato all'esecuzione di una misura cautelare di divieto di avvicinamento e installazione del cosiddetto "braccialetto elettronico", emessa dal GIP del Tribunale nei confronti di un uomo di anni 39, residente a Catania, ritenuto responsabile dei delitti di atti persecutori aggravati. La vicenda trae origine da una segnalazione via *e-mail* al Centro Operativo Sicurezza Cibernetica della Polizia Postale di Catania in cui un utente riferiva che, mentre era in attesa in una sala di un nosocomio catanese, aveva dato in uso il suo telefono ad un uomo che, essendone momentaneamente privo, aveva urgente necessità di chiamare la moglie.
Nel corso di quella telefonata, il segnalante aveva udito delle frasi minacciose rivolte dall'uomo all'interlocutore. Le indagini, da subito avviate, hanno permesso di identificare una donna come titolare dell'utenza telefonica formulata. A questo punto, gli operatori della Polizia postale hanno ascoltato la signora, madre di minori, che ha raccontato le vicende di minacce e molestie subite nel corso del tempo dal marito dopo la separazione. È emerso che l'indagato minacciava la donna con frasi quali *"Se ti vedo con un altro ti ammazzo davanti la scuola", "prima che mi denunci ve la faccia finire male a tutti";* tempestava la vittima di innumerevoli telefonate e messaggi, tanto da ingenerare in lei un costante timore per l'incolumità sua e dei figli e costringendola a modificare le sue abitudini di vita. Le risultanze investigative acquisite dalla Polizia Postale hanno consentito al Pubblico ministero di richiedere ed ottenere una misura cautelare nei confronti dell'indagato.

Ordinanza di custodia cautelare nei confronti di un giovane 19enne in relazione al reato di atti persecutori La Polizia di Stato ha dato esecuzione ad un'ordinanza di custodia cautelare agli arresti domiciliari con braccialetto elettronico, emessa dal Gip presso il Tribunale di Foggia, su proposta della locale Procura della Repubblica, nei confronti di un giovane 19enne, sottoposto alle indagini preliminari in relazione al reato di atti persecutori.
In particolare, l'attività d'indagine condotta dal personale della Sezione Operativa per la Sicurezza Cibernetica di Foggia, coordinata dalla locale Procura della Repubblica, prendeva avvio dalla querela presentata da una giovane donna che lamentava un grave stato di ansia e timore per la propria incolumità, con conseguente destabilizzante turbamento psicologico,

dovuto alle reiterate minacce e molestie, poste in essere dal soggetto, a seguito del rifiuto della proposta di intrattenere con lui una relazione sentimentale.
L'arrestato, dopo le formalità di rito, veniva accompagnato presso la sua abitazione per ivi rimanere sottoposto agli arresti domiciliari.

MANIFESTAZIONI ESTREMISTE IN RETE - CYBERTERRORISMO

L'utilizzo delle piattaforme di comunicazione online, social network e di applicazioni di messaggistica istantanea, rappresentano ormai il principale canale di comunicazione per la diffusione di contenuti propagandistici di varia natura ed origine, il cui continuo e vertiginoso incremento rappresenta un segnale di allarme da non sottovalutare.

Cyberterrorismo[1]	2022*	2023**
Casi trattati	1.193	236
Persone indagate	66	60
Spazi virtuali monitorati	170.908	178.756
Spazi oscurati per attività infoinvestigative	321	2.670

[1]- Estremismo internazionale religioso / estremismo razziale, antagonista ed anarchico
* -dati rilevati al 21/12/2022
**- dati rilevati il 21/12/2023

Nell'ambito della prevenzione e del contrasto alla diffusione di contenuti terroristici online e, in particolare, dei fenomeni di radicalizzazione sul web, il personale della Polizia Postale e delle Comunicazioni effettua costantemente il monitoraggio del web e svolge attività investigative, sia d'iniziativa che su specifica segnalazione (anche grazie a quelle che giungono dai cittadini tramite il portale del Commissariato di P.S. Online), al fine di individuare i contenuti illeciti presenti all'interno degli spazi e dei servizi di comunicazione online di ogni genere.

In particolare, il personale impiegato nel settore della prevenzione e del contrasto dei fenomeni terroristici in rete svolge attività informativa ed investigativa nell'ambito della prevenzione e del contrasto alla diffusione di contenuti terroristici online e, in particolare, dei fenomeni di radicalizzazione sul web.

Il target operativo di tale settore, dunque, si concretizza nella prevenzione e repressione dei reati che utilizzano la dimensione virtuale per finalità terroristiche, minando l'ordine e la sicurezza pubblica per ragioni riconducibili sia a forme di fondamentalismo religioso, sia a forme di estremismo politico ideologico, anche in contesti internazionali.

In ambito di cooperazione internazionale per la prevenzione e contrasto del cyber terrorismo il Servizio Polizia Postale e delle Comunicazioni costituisce il punto di contatto italiano della rete Europol IRU - Internet Referral Unit, coordinata dal Centro ECTC di Europol (European Counter Terrorism Center) – per il monitoraggio dei contenuti terroristi online e partecipa, insieme agli operatori di polizia di altri paesi agli Action Day, azioni ad alto impatto per la rimozione di contenuti illegali, che in tale ambito vengono promossi con notevoli risultati operativi.

Il continuo e vertiginoso incremento dell'utilizzo delle piattaforme di comunicazione online, social network e applicazioni di messaggistica istantanea, ha determinato parallelamente un considerevole incremento, ad una platea pressoché illimitata, di qualsiasi tipo di contenuti propagandistici riconducibili al terrorismo, sia di matrice islamista, sia formazioni di estrema destra (neonazismo, neofascismo, tifoserie strutturate, suprematismo), formazioni di estrema sinistra (movimenti di lotta armata, anarchici, insurrezionalisti, antagonisti), formazioni separatiste.

In tale ambito viene garantita dagli specialisti della Polizia Postale sia l'esecuzione di una costante attività di monitoraggio investigativo della rete e dei canali di messaggistica istantanea, per l'identificazione e il deferimento all'Autorità Giudiziaria dei responsabili della diffusione dei contenuti illeciti, sia un costante scambio informativo con la Direzione Centrale della Polizia di Prevenzione e con le Agenzie di Intelligence, competenti in materia di contrasto al terrorismo.

Nell'ambito del contrasto al fenomeno del c.d. cyberterrorismo e, in generale, dell'estremismo in rete gli investigatori della Sezione Cyberterrorismo hanno concorso alla prevenzione e al contrasto dei fenomeni di eversione e terrorismo, sia a livello nazionale che internazionale, posti in essere attraverso l'utilizzo di strumenti informatici e di comunicazione telematica.

L'attività, funzionale al contrasto del proselitismo e alla prevenzione dei fenomeni di radicalizzazione estremista religiosa e dell'eversione di estrema destra e antagonista, ha permesso di sviluppare una dedicata attività informativa in contesti di interesse, per oltre **178.000 spazi web** oggetto di approfondimento investigativi; tra questi **2.600** risorse digitali sono state oscurate poiché caratterizzati da un contenuto illecito.

L'attività di monitoraggio del web effettuata dalla Specialità ha permesso di riscontrare in primis come la diffusione di contenuti propagandistici jihadisti, nel corso del tempo, abbia subito un sensibile peggioramento qualitativo, determinato sia dalla scomparsa del Califfato, sia dalle perdite di tecnici e social media manager cui era devoluto l'incarico di gestire la propaganda, nonché per l'utilizzo sempre più frequente algoritmi ed impiego di intelligenza artificiale sulle principali piattaforme web, per la scansione (e rimozione) dei contenuti pubblicati dagli utenti.

Si rappresenta, infine, che il 24 luglio 2023 è stato pubblicato in Gazzetta Ufficiale il decreto legislativo n. 107, in vigore dal 26 agosto u.s., per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2021/784, relativo al contrasto della diffusione di contenuti terroristici online.

Il quadro normativo unionale e la normativa attuativa, determinano per il Servizio Polizia Postale e delle Comunicazioni, Organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione, l'attribuzione di importanti competenze e un ruolo cardine nel nuovo scenario nazionale ed internazionale relativo al contrasto della diffusione di contenuti terroristici online.

Per l'adempimento delle incombenze imposte dal Regolamento europeo e dalla normativa nazionale di recepimento, la Polizia Postale curerà l'utilizzo dello strumento informatico denominato PERCI, con il coordinamento svolto dall'EU-IRU di Europol, e dovrà occuparsi delle segnalazioni ai fornitori di servizi di hosting delle risorse web con contenuti illeciti di carattere terroristico, di volta in volta interessati dalla segnalazione.

ATTIVITA' DI POLIZIA GIUDIZIARIA

Identificazione e deferimento di 2 promotori del gruppo no-vax "Vi-Vi" Gli specialisti della Polizia Postale hanno condotto una complessa attività investigativa che ha permesso di identificate e denunciate, tra gli altri, anche due promotori del gruppo no-vax denominato "guerrieri ViVi", e di oscurare alcuni canali di comunicazione in rete.

In particolare, all'esito di un primo filone investigativo che già nel 2022 aveva consentito di denunciare ventiquattro appartenenti al gruppo no vax - no green pass denominato "guerrieri Vivi", il Centro Operativo per la Sicurezza Cibernetica di Genova ha eseguito nello scorso mese di gennaio alcune perquisizioni a Brescia, Verona e Matera, delegate dalla D.D.A. della Procura della Repubblica di Genova, a carico di tre soggetti di cui due indiziate di essere promotori del sodalizio nell'ambito di un procedimento per violazione degli artt. 1 e 2 c. 1 e 2 della l. n. 17/1982 (associazione segreta) e degli artt. 110 - 414 c. 1 n.1 e c.3, in relazione all'art. 340 c.p. (istigazione all'interruzione di un servizio di pubblica necessità).

Il Centro Operativo per la Sicurezza Cibernetica della Liguria ha identificato i capi dell'organizzazione dopo mesi di serrate indagini informatiche che hanno consentito di setacciare centinaia di chat su numerosi social e documenti postati in rete, scardinando l'anonimato che gli autori ritenevano di avere conseguito grazie all'utilizzo di reti VPN e del sistema di messaggistica Telegram.

L'attività di proselitismo e istigazione a delinquere del gruppo no-vax ha quotidianamente preso di mira rappresentanti istituzionali e appartenenti all'ordine dei medici attraverso commenti "violenti", postandoli in maniera coordinata e ripetitiva sui profili social delle vittime, soprattutto di chi esprimeva opinioni a favore dei vaccini, imbrattando con scritte in vernice rossa le sedi di alcune Asl, di hub vaccinali, ospedali, ordini dei medici, scuole, sedi di alcuni sindacati e testate giornalistiche.

Con la conclusione delle restrizioni legate alla pandemia, il gruppo no vax, dichiaratamente ossessionato da ogni presunta forma di controllo, non ha interrotto la propria attività di proselitismo e si è orientato verso gli argomenti dei sistemi di pagamento e di identità digitale, dei cambiamenti climatici, del 5G, "attaccando" in rete, con lo stesso modus operandi, talvolta anche con minacce, chi esprimeva opinioni a favore dello sviluppo di tali tecnologie o tematiche.

Gli attacchi venivano coordinati su gruppi Telegram creati ad hoc e sugli stessi gruppi venivano poi pubblicizzate le incursioni, con immagini o screenshot di quanto vandalizzato.

Sono state create anche alcune challenge con cui i promotori invitavano gli adepti a compiere azioni illecite, come posizionare striscioni o adesivi ritraenti il logo del gruppo su sedi Istituzionali, in una sorta di gara che prevedeva un premio in bitcoin da assegnare all'autore dell'azione più eclatante.

Le perquisizioni eseguite dagli investigatori del Centro Operativo per la Sicurezza Cibernetica di Genova, con l'ausilio degli Uffici di Milano, Venezia, Campania, Basilicata e Molise, e il coordinamento del Servizio Polizia Postale e delle Comunicazioni di Roma, presso le residenze degli indagati, i loro luoghi di lavoro e un maneggio in provincia di Brescia presso cui si incontravano, hanno consentito di acquisire evidenze informatiche di conferma dell'attuale operatività dei "ViVi" e di procedere al sequestro preventivo dei loro mezzi di comunicazione e propaganda in rete, emesso dal GIP del Tribunale di Genova.

Esecuzione di Mandato di Arresto Europeo (MAE) nei confronti di un cittadino turco Il 26 gennaio, a seguito di attivazione da parte del Servizio Centrale Operativo e del Servizio per la Cooperazione Internazionale di Polizia-Gruppo ENFAST-Divisione SIReNE, ha permesso al personale del Servizio di Polizia Postale e delle Comunicazioni di Roma, unitamente alla Squadra Mobile di Rimini, di eseguire un Mandato di Arresto Europeo emesso dalla Germania per omicidio volontario, nei confronti di un trentenne di nazionalità turca, incensurato in Italia, ricercato su tutto il territorio Schengen, che veniva rintracciato presso una struttura ricettiva di questo centro.
In particolare, fin dalla giornata del 25 gennaio erano stati effettuati dalla Squadra Mobile accertamenti di natura tecnica e dinamica, a riscontro dell'attività svolta dal Servizio di Polizia Postale e delle Comunicazioni, che aveva proceduto allo sviluppo della labile traccia informatica relativa ad un dato telematico anonimo ed alle successive attività di OSINT, individuandone la posizione in zona Marina Centro, accertamenti a seguito dei quali, si giungeva all'individuazione certa dello stesso.
Il turco, sottoposto a perquisizione presso l'hotel dove aveva preso alloggio con false generalità, veniva trovato in possesso di una pistola calibro 9x19 marca "Glock", con doppio caricatore e nr. 14 cartucce 9x19 con ogiva blindata, catalogabili come munizionamento "da guerra". All'esito degli immediati accertamenti svolti, l'arma era da ritenersi clandestina in quanto non censita sul catalogo Nazionale delle Armi, risultando altresì oggetto di segnalazione della Polizia Tedesca, per fatti accaduti su qual territorio. Venivano trovati anche documenti d'identità falsi, alcuni smartphone e altro materiale di interesse investigativo.
Il soggetto quindi è stato tratto in arresto, oltre che per il MAE anche per la flagranza di reato riguardo alla detenzione e porto dell'arma clandestina, nonché del munizionamento da guerra e per il possesso dei documenti falsi. Al termine delle incombenze di rito è stato associato presso la casa circondariale di Rimini a disposizione delle Autorità Giudiziarie procedenti.

Esecuzione di Mandato di Arresto Europeo (MAE) nei confronti di un cittadino straniero La Polizia Postale, nell'ambito dello scambio informativo all'interno della rete di uffici dell'European Network Fugitive Active Search Teams (E.N.F.A.S.T.), la Polizia Postale ha avviato, a seguito della segnalazione pervenuta dalla Direzione Centrale della Polizia Criminale - Servizio Cooperazione Internazionale di Polizia -Divisione S.I.Re.N.E. inoltrata dal collaterale ufficio tedesco, una attività investigativa che ha portato all'identificazione di un cittadino straniero destinatario di una Mandato di Arresto Europeo.
Personale della Squadra Mobile e del Centro Operativo per la Sicurezza Cibernetica di Palermo ha tratto in arresto un cittadino straniero di 26 anni, ricercato in Italia e in ambito Schengen poiché destinatario di un mandato d'arresto europeo emesso dalla Germania, per i reati di tentato omicidio in concorso ed istigazione a delinquere. Lo stesso era anche ricercato in Italia poiché destinatario di un ordine di carcerazione emesso dalla Procura della Repubblica presso il Tribunale di Ferrara, dovendo espiare la pena definitiva di anni 9 e giorni 1 di reclusione per reati di spaccio di stupefacenti, detenzione di armi clandestine, furto aggravato, resistenza e minacce a P.U.
In particolare, gli approfondimenti informatici condotti nell'immediato dal Servizio Polizia Postale e delle Comunicazioni, effettuati sulle connessioni internet all'account social del ricercato, hanno permesso di localizzare il ricercato nella zona del centro storico palermitano.
La prosecuzione degli accertamenti investigativi condotti da personale del C.O.S.C. e della sezione omicidi della Squadra Mobile di Palermo, anche attraverso una complessa attività di

O.C.P., ha consentito la sua compiuta identificazione, nonostante utilizzasse documenti falsi e numerazioni telefoniche intestate ad altri connazionali.
Appreso che il ricercato necessitava di trattamenti medici di emodialisi per una grave malattia, sono state condotte in meno di 24 ore accurate ricerche dagli operatori delle strutture investigative, presso le strutture sanitarie del capoluogo siciliano, deputate al trattamento di tale patologia. Pertanto lo stesso è stato individuato, nonostante le false generalità dichiarate, presso il reparto di nefrologia di un ospedale di Palermo e tratto in arresto e condotto, dopo le formalità di rito, presso la Casa Circondariale "A. Lorusso" Pagliarelli di Palermo.

Operazione "Alchimia" (giugno 2023) Le attività investigative condotte dal personale della Specialità hanno permesso l'identificazione di diversi minori che sperimentavano miscele esplosive con sostanze chimiche acquistate su internet, i cui effetti venivano documentati con la pubblicazione di foto e video sui social.
Grazie ad una complessa attività di polizia giudiziaria, condotta tra ottobre 2022 e febbraio 2023, gli investigatori del Centro Operativo per la Sicurezza Cibernetica di Milano hanno individuato alcuni spazi Telegram utilizzati da adolescenti per condividere le loro esperienze su armi ed esplosivi.
Gli internauti, tutti minorenni e residenti in diverse aree geografiche del territorio italiano, erano accumunati dalla passione per le armi. A tal proposito, qualcuno ha affermato "I miei genitori sono contrari alle armi allora me le fabbrico io oppure me le prendo da qualche parte [...] Ci ho sparato con una glock vera... [...] Te lo dico perché le modifico da quando avevo 14 anni [...]".
Nelle chat i minori affermavano di andare in giro con coltelli e a volte persino con pistole (a salve o da softair), incuranti di possibili controlli da parte delle forze dell'ordine, come riscontrato in altre frasi del seguente tenore: "Io avevo una glock però poi ci sono andato a scuola perché lo avevo visto in un film americano [...] io sono andato con un multitool con coltello, rischiato molto di andare al minorile [...] Io portavo quello a scatto nel giubbino".
Spesso pubblicavano anche foto e video che mostravano armi da taglio, da sparo e da softair, esposte in posa o durante l'effettivo utilizzo.
Nelle loro discussioni su Telegram richiedevano informazioni e consigli su come confezionare molotov, esplosivi e detonatori, pubblicando anche foto degli ordigni realizzati, scrivendo "avete mai fatto una molotov? io si [...] martedì provo a fare del napalm [...] Qualcuno ha un video Tutorial per un detonatore? [...] buon pomeriggio, ecco a voi un piccolo dispositivo. [...]".
Al termine dell'indagine, coordinata dal Tribunale per i Minorenni di Milano, nella mattinata del 28 giugno scorso la Polizia Postale, in collaborazione con le DIGOS e con l'ausilio di unità cinofile specializzate della Polizia di Stato, ha eseguito 8 perquisizioni nelle città di Avellino, Lecce, Milano, Pisa, Sassari, Nuoro e Treviso.

Esecuzione di 2 custodie cautelari (ottobre 2023) Una complessa attività d'indagine coordinata dalla Procura della Repubblica di Milano, ha consentito di dare esecuzione a due misure di custodia cautelare in carcere, a carico di altrettanti soggetti di origine egiziana di 44 e 49 anni, ritenuti responsabili di partecipazione ad associazione con finalità di terrorismo ed istigazione a delinquere con finalità di terrorismo.
In particolare, l'attività investigativa condotta dalla D.I.G.O.S. di Milano - Sezione Antiterrorismo e dal Centro Operativo per la Sicurezza Cibernetica di Perugia, in collaborazione con la Direzione Centrale della Polizia di Prevenzione e con il Servizio Centrale Polizia Postale e delle Comunicazioni, ha avuto inizio nell'agosto del 2021 quando, sulla base

di acquisizioni d'intelligence e del compendio investigativo emerso da altro procedimento penale, gli investigatori hanno avviato mirati approfondimenti nei confronti dei due indagati, entrambi evidenziatisi per la comune presenza su gruppi WhatsApp di matrice jihadista e riconducibili allo "Stato Islamico".
L'indagine ha confermato la centralità del cyberspazio e dei circuiti mediatici internazionali, nella diffusione del messaggio jihadista finalizzato al proselitismo ed all'esaltazione delle azioni terroristiche da parte dell'organizzazione a cui hanno aderito gli indagati.
In particolare, è stato riscontrato l'utilizzo della rete per una sorta di addestramento diffuso, cristallizzando a carico dei due soggetti indagati i seguenti elementi indiziari:
1.copioso materiale inneggiante ad azioni terroristiche violente, in diversi casi con bambini protagonisti;
2.condivisione sui propri account Facebook di contenuti jihadisti, con commenti e like di approvazione su profili altrui;
3.presenza su canali Telegram e gruppi Whatsapp direttamente riconducibili allo Stato Islamico o ad esso affiliati, con la partecipazione di centinaia di utenti, registrati con numerazioni siriane, afgane, irachene, nord-africane, ma anche europee e sudamericane;
4.versamenti di denaro disposte a favore di nominativi stanziati in Yemen e Palestina;
5. indottrinamento religioso svolto nei confronti dei familiari, con particolare riferimento ai figli minori.
Nel corso della lunga indagine, il quadro probatorio si è ulteriormente aggravato con un giuramento di fedeltà allo Stato Islamico, postato su un profilo Facebook da uno degli indagati nel maggio 2022.
A riprova dell'assoluta gravità degli elementi ricostruiti, è stata rilevata da parte degli indagati un expertise nell'uso delle armi e la disponibilità a dare consigli a chi volesse essere introdotto al loro impiego.
Inoltre, sono state individuate, sempre sul medesimo profilo Facebook, delle minacce dirette a cariche istituzionali italiane.

FINANCIAL CYBERCRIME

Le evidenze acquisite nella più recente azione di contrasto ai fenomeni criminali di carattere finanziario hanno permesso di registrare una persistente diffusione di condotte predatorie realizzate attraverso campagne di *phishing* (anche nelle varianti del c.d. "*vishing*" e del c.d. "*smishing*")[2], consumate in danno di persone fisiche, PMI e grandi società, perpetrate per il tramite di e-mail che, dietro apparenti comunicazioni di Ministeri, organizzazioni pubbliche, istituti di credito ed altri enti, consentono in realtà di acquisire i dati personali e sensibili, le *password* di accesso a domini riservati, utili per perpetrare reati contro il patrimonio.

[2] L'illecito procacciamento di codici "*one-time*", *token* virtuali e *password* dispositive si realizza mediante il ricorso a chiamate vocali o a messaggi ed sms che sembrano provenire da banche o altri enti apparentemente legittimati a richiedere informazioni sensibili.

Analogamente, si registra la persistente aggressività sociale delle frodi basate sulle tecniche di *social engineering*, con particolare riferimento al c.d. *BEC fraud*,[3] facilitata anche dall'aumento delle comunicazioni commerciali a distanza e dall'uso dilagante della rete nelle transazioni commerciali.

L'azione di contrasto realizzata nelle più recenti investigazioni ha offerto evidenze significative in termini di un'oggettiva crescita del livello qualitativo dei contesti criminali impegnati nel c.d. *financial cybercrime*: la possibilità di realizzare ingenti guadagni attraverso condotte delinquenziali che possono essere realizzate massivamente e su larga scala ha, infatti, inevitabilmente determinato un innalzamento dello spessore delinquenziale dei soggetti attivi, con il conseguente interesse di consorterie criminali un tempo impegnate esclusivamente in altre fenomenologie delittuose.

La particolare natura delle specifiche condotte criminose impone, nell'ottica di un'efficace azione di contenimento, che l'attività investigativa di contrasto debba esplicarsi anche con l'ausilio dei canali ufficiali di cooperazione internazionale, attesa la necessità, in numerosi casi, di ricercare tracce informatiche e finanziarie oltre i confini nazionali. Tale circostanza rende talora complessa la raccolta delle evidenze ricercate, laddove i paesi stranieri impattati nella richiamata ricerca non supportino in maniera collaborativa l'Autorità Giudiziaria italiana.

Nonostante le segnalate difficoltà operative, di ostacolo anche al recupero delle somme provento di frode informatica, (spesso inviate verso paesi extraeuropei quali 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, la Specialità è riuscita a recuperare, nell'anno in corso, consistenti somme illecite, riferibili al particolare fenomeno BEC/CEO FRAUD.

La piattaforma, frutto di specifiche convenzioni intercorse, mediante ABI con le maggiori realtà bancarie italiane, consente di porre in essere tempestivi interventi per bloccare le somme sottratte.

Un ulteriore elemento di interesse e di difficoltà operativa è costituito dal sempre più frequente ricorso alle "criptovalute"[4], le cui transazioni (registrate attraverso sistemi di *blockchain*) si caratterizzano per una maggiore difficoltà di tracciamento.

L'abilità tecnica, richiesta per movimentare capitali ingenti attraverso il ricorso a criptovalute, è stata rapidamente acquisita anche dalle organizzazioni criminali di stampo mafioso, le quali, nella recente storia, si sono caratterizzate per aver assicurato alle giovani generazioni di affiliati accresciuti livelli di professionalità e specializzazioni funzionali al successo dell'impresa criminosa.[5]

Alla luce della complessiva analisi, è di tutta evidenza, quindi, come settore del *financial cybercrime* sia un bacino molto remunerativo e, per questo, sempre più appetibile per organizzazioni criminali strutturate, anche estere, che sovente utilizzano gli illeciti profitti, derivanti da tali condotte delittuose per finanziare ulteriori e diversificate attività illecite.

In Italia, nell'anno in corso, sono state **colpite 65 grandi, medie e piccole imprese**, per un ammontare complessivo di **oltre 19 milioni di euro** di profitti illeciti, dei quali **6 milioni** sono stati recuperati in seguito all'intervento della Polizia Postale e delle Comunicazioni.

---

[3] Frode realizzata attraverso la compromissione di caselle di posta elettronica realizzata allo scopo di acquisire informazioni utili al perfezionamento della condotta illecita.

[4] Utilizzate come strumento per perfezionare l'efficace riciclaggio dei proventi illeciti.

[5] La circostanza che le criptovalute si caratterizzino per una elevata volatilità (in un mercato che, peraltro, è attivo senza soluzione di continuità 365 giorni all'anno H24), potenziale ostacolo al loro utilizzo nell'azione di riciclaggio può essere agevolmente superata attraverso la conversione delle più utilizzate criptovalute in *stablecoin*: *crypto asset* con valore stabile ancorato o ad una valuta fiat (generalmente il dollaro USA, esempio THETER, BUSD o USDC) o al prezzo dell'oro (suscettibile di ben minori fluttuazioni: come ad esempio la criptovaluta DIGIX GOLD).

Le indagini svolte sui reati commessi attraverso l'utilizzo di tecniche quali ***phishing, smishing e vishing***, sono state identificate deferite all'AG **917 persone**.

Frodi Informatiche	**2022***	**2023****	**Variazione percentuale**
Casi trattati	9.229	10.606	+15%
Persone indagate	849	917	+8%
Somme sottratte	**€ 38.506.316**	**€ 40.151.375**	**+4%**
* -dati rilevati al 21/12/2022 **- dati rilevati il 21/12/2023			

FINANCIAL CYBERCRIME – ATTIVITÀ DI POLIZIA GIUDIZIARIA

Operazione nei confronti di un'organizzazione criminale dedita alle frodi finanziarie c.d. del "Trading online" radicata in Albania La Sezione Operativa per la Sicurezza Cibernetica di Pordenone, il Centro Operativo per la Sicurezza Cibernetica di Trieste e la Squadra Mobile di Pordenone, con il coordinamento del Servizio Centrale Operativo e del Servizio Polizia Postale, hanno svolto un'indagine transnazionale nei confronti di un'organizzazione criminale dedita alle frodi finanziarie c.d. del "*Trading online*" radicata in Albania.
Nel corso delle indagini sono emerse decisive evidenze a seguito dell'analisi svolta sul materiale informatico e in particolare sugli oltre sessanta computer rinvenuti nel sequestro di due *call center* siti in Tirana, da cui si è potuto ricostruire il ruolo di ciascun componente all'interno del sodalizio criminoso.
L'attività investigativa ha sin da subito evidenziato la particolare complessità del sistema criminale, soprattutto dal punto di vista tecnico, caratterizzato dall'adozione di sofisticate tecniche di *spoofing* e *social engineering*, che hanno permesso di celare alle potenziali vittime la vera identità degli interlocutori inducendole a credere di essere in contatto con reali *broker* e quindi a concludere l'investimento.
La collaborazione tra le forze di polizia e le rispettive autorità giudiziarie è stata formalizzata con la costituzione di una squadra investigativa comune il cui lavoro in sinergia ha portato all'esecuzione di 13 ordinanze di custodia cautelare ed al deferimento in stato di libertà di 61 cittadini albanesi risultati essere tutti membri, con specifici compiti e ruoli, dell'organizzazione criminale transnazionale dedita alle truffa finanziaria del falso *trading online*.

Operazione "Grandi Firme" Nell'ambito di un'indagine della Polizia postale di Catania finalizzata al contrasto della vendita online di abbigliamento ed accessori di marchi contraffatti sono state eseguite perquisizioni domiciliari ed informatiche nei confronti di 11 indagati per associazione per delinquere finalizzata all'introduzione nello Stato ed al commercio di prodotti con segni falsi e impiego di denaro, beni o utilità di provenienza illecita.
L'attività investigativa, coordinata dalla locale Procura della Repubblica, ha consentito il sequestro di numerosi capi di abbigliamento ed accessori falsi riconducibili a noti brand, nonché dei dispositivi utilizzati per pubblicizzare online la merce, venduta a prezzi considerevolmente inferiori a quelli ufficiali con grave nocumento alle imprese del settore.

Operazione "Cremonese Calcio" Gli specialisti del Servizio Polizia Postale e delle Comunicazioni si sono attivati il 9 ottobre u.s. in seguito alla denuncia presentata dall'U.S. Cremonese Calcio per una patita frode informatica di tipo B.E.C. Fraud (Business Email Compromise).
In particolare, gli ignoti autori del reato, mediante la violazione dei sistemi di posta elettronica aziendali, si inserivano nella corrispondenza intrattenuta tra la U.S. Cremonese Calcio e

l'omologa Belga del Genk, riuscendo a modificare le coordinate bancarie per il pagamento della seconda rata dell'acquisto del calciatore belga Cyriel Dessers.
Indotta in errore, la U.S. Cremonese Calcio disponeva in data 28 settembre 2023, un bonifico di euro 1.719.500,00 su un conto corrente attestato presso la banca belga ING di Avenue Marnix 24 – Bruxelles.
L'immediata attivazione dei canali di cooperazione internazionale di polizia, ha consentito il blocco cautelativo del conto corrente contenente l'intera somma frodata.

Operazione "Ghost Money" I Centri Operativi per la Sicurezza Cibernetica (COSC) di Roma e di Torino, coordinati da Servizio Polizia Postale e delle Comunicazioni hanno eseguito provvedimenti di custodia cautelare, emessi dal G.I.P. di Roma nei confronti di 6 indagati per truffa aggravata, frodi informatiche, riciclaggio e auto riciclaggio.
Le indagini, condotte da personale del COSC di Roma, sono state avviate in relazione ad una serie di frodi realizzate attraverso la tecnica del c.d. SIM SWAP. Le vittime venivano private della funzionalità della propria utenza cellulare attraverso l'indebita sostituzione della SIM telefonica e quindi della numerazione destinataria dei codici dispositivi dell'home banking, poi utilizzati dai criminale per sottrarre denaro dai conti correnti.
Le perquisizioni e la conseguente analisi dei dispositivi sequestrati hanno consentito di acquisire evidenze di rilevanza probatoria in relazioni a numerose condotte delittuose che hanno consentito illeciti guadagni per circa 4 milioni.

Operazione "Piazza Italia" Nel contesto di un'indagine avviata dal C.O.S.C. di Napoli su una truffa di $ 375.929,83, compiuta mediante la tecnica del B.E.C. (Busines Email Compromise), in danno della Società italiana "Piazza Italia S.p.a." con sede legale a Milano, il Servizio Polizia Postale ha attivato i canali diretti esistenti con l'Homeland Security Investigations, operante presso l'ambasciata americana in Italia, al fine di richiedere l'immediato blocco delle somme sottratte. Sulla base delle informazioni fornite dagli investigatori italiani, la predetta agenzia statunitense ha realizzato i necessari, richiesti, approfondimenti che hanno permesso, per un verso di avviare una propria indagine su frodi consumate in danno di società operanti negli USA e, per altro verso, di recuperare $ 220.000,00, restituiti alla predetta azienda italiana.

Operazione "EMMA" Si è conclusa a fine novembre 2023, l'Operazione di polizia ad alto impatto denominata EMMA, giunta alla sua nona edizione, messa in campo anche quest'anno dalla Polizia Postale e delle Comunicazioni e dalle Forze di polizia cyber di altre 27 Nazioni e coordinata da Europol ed Interpol.
I numeri complessivi dell'Operazione nei diversi Paesi europei, frutto del lavoro di tutte le Forze di polizia estere impegnate insieme alla Polizia italiana, sono ragguardevoli: anche grazie al supporto di oltre 2.822 istituti bancari e altre istituzioni finanziarie, sono state individuate 10.736 transazioni bancarie fraudolente, sono state avviate oltre 4.659 autonome indagini, riuscendo a prevenire frodi per una danno stimato in 32 milioni di euro.
Più di 10.759 i money-mule individuati (titolare di un conto bancario, che trasferisce denaro dal proprio conto corrente in cambio di contanti), e 474 organizzatori e coordinatori di muli identificati.
L'iniziativa è stata resa possibile anche grazie alla fattiva collaborazione delle banche e degli istituti di credito italiani, che, attraverso CERTFin e ABI, hanno assicurato un supporto in tempo reale agli investigatori, grazie alla piattaforma per la condivisione delle informazioni denominata "OF2CEN", realizzata appositamente dall'Italia al fine di prevenire e contrastare le aggressioni criminali ai servizi di home banking e monetica.

Operazione nazionale contro lo streaming illegale Nel mese di dicembre il Servizio Polizia Postale ha coordinato una vasta operazione della Polizia di Stato contro la pirateria audiovisiva.

Nell'ambito di un primo filone investigativo, avviato con la Procura Distrettuale di Catania, sono state eseguite 21 perquisizioni nei confronti di altrettanti soggetti indagati (attivi nelle città di Catania, Messina, Siracusa, Cosenza, Alessandria, Napoli, Salerno, Reggio Emilia, Pisa, Lucca, Livorno e Bari) a cui la procura etnea ha contestato a vario titolo reati quali associazione per delinquere a carattere transnazionale finalizzata alla diffusione di palinsesti televisivi ad accesso condizionato, danneggiamento di informazioni, dati e programmi informatici, accesso abusivo a sistema informatico e frode informatica.
Le indagini, avviate dal Centro Operativo Sicurezza Cibernetica di Catania con il diretto coordinamento del Servizio Centrale Polizia Postale, hanno permesso di delineare l'esistenza di un'associazione criminale organizzata in modo gerarchico secondo ruoli ben precisi e con promotori attivi sul territorio nazionale, avente come finalità la costante distribuzione, ad un elevatissimo numero di utenti, in ambito nazionale ed internazionale, di palinsesti live e contenuti on demand protetti da diritti televisivi, di proprietà delle più note piattaforme (quali Sky, Dazn, Mediaset, Amazon Prime, Netflix) attraverso il sistema delle IPTV illegali, con profitti mensili per svariati milioni di euro.
Le perquisizioni sono state eseguite anche nei confronti di altri 10 soggetti (attivi nelle città di Napoli, Bari, Catanzaro, Palermo, Teramo e Bergamo) identificati in un secondo filone di indagine coordinato dalla Procura della Repubblica presso il Tribunale di Catanzaro. Nella circostanza, le investigazioni sono state avviate dalla Polizia di Stato del Centro Operativo per la Sicurezza Cibernetica Calabria e dalla dipendente Sezione Operativa per la Sicurezza Cibernetica di Catanzaro, con il consueto coordinamento del Servizio Polizia Postale.
Partendo dall'analisi di vari canali Telegram, è stato possibile riscostruire le condotte delittuose consumate in diverse province del territorio nazionale, al solito finalizzate alla diffusione illecita, dietro pagamento di corrispettivo, del segnale audiovisivo dei canali delle più note piattaforme che offrono servizi di PayTv (Sky, Dazn, Now, Disney Plus, Discovery Plus). Gli indagati, ritenuti responsabili allo stato delle indagini, di violazione del diritto di autore e di accesso abusivo a sistema informatico e telematico, costituiscono l'articolazione operativa di un organizzazione che vede quale soggetto di spicco un cittadino italiano con precedenti di polizia specifici, emerso anche nelle indagini coordinate dalla Procura della Repubblica di Catania.
L'illecito flusso economico generato è diverse centinaia di migliaia di euro.
La complessiva operazione di polizia giudiziaria ha coinvolto personale dei Centri Operativi Sicurezza Cibernetica di Catania, Reggio Calabria, Roma, Torino, Napoli, Bologna, Palermo, Milano, Pescara, Firenze e Bari e ha consentito di sequestrare n. 21 pannelli di gestione utenti e n. 2 pannelli di gestione flussi, consentendo l'inibizione dell'illecita diffusione dei segnali audiovisivi diretti a circa 50.000 utenti. Nel medesimo contesto sono stati sequestrati anche numerosi dispositivi cellulari ed informatici contenenti evidenze utili a riscontrare le ipotesi investigative.

COMMISSARIATO DI P.S. ONLINE

L'uso crescente delle nuove tecnologie ha reso necessario il potenziamento di nuovi strumenti di comunicazione che consentissero alla Polizia di Stato di mettersi in contatto diretto con gli utenti del *web*.

In tale ottica il portale del Commissariato di PS online ha permesso al cittadino, abituato ormai a utilizzare la rete internet per svolgere le principali attività quotidiane, di rivolgersi alla Polizia Postale in qualsiasi momento e ovunque si trovi. Attraverso il computer l'utente può esprimere il proprio disagio per un torto subito, segnalare comportamenti che giudica illeciti e chiedere aiuto per superare difficoltà e problematiche, anche nei casi in cui potrebbe essere fonte di disagio rappresentarle di persona.

La facilità con cui il cittadino ha interagito con la piattaforma dedicata ha reso possibile raccogliere le segnalazioni di quegli utenti che, mossi da spirito altruistico e di collaborazione,

si sono rivolti alla Polizia Postale in un'ottica di sicurezza partecipata - nella sua declinazione online, fornendo utili evidenze su fenomeni emergenti potenzialmente lesivi, così contribuendo, in termini di efficace prevenzione, ad evitare che altri internauti potessero cadere nelle trappole della Rete.

L'analisi delle oltre **82.000** segnalazioni ricevute dal sito nell'anno 2023 ha evidenziato che in molti casi gli internauti non adottano quelle piccole e necessarie accortezze di *cyber hygiene,* che consentirebbero loro di prevenire e limitare la maggior parte degli attacchi informatici e il perpetrarsi di attività delittuose. Al fine di migliorare l'attività preventiva è stata ampliata la sezione dedicata agli *alert*, dove vengono raccolti e pubblicati gli "avvisi agli utenti" che, proprio perché costantemente aggiornati e facilmente raggiungibili, costituiscono un efficace strumento di autotutela messo a disposizione del cittadino. Per rendere ancora più incisiva la comunicazione è stata attivata una preziosa collaborazione con il giornalista Marco Camisani Calzolari per la realizzazione di clip video di approfondimento sulle insidie della Rete e sugli accorgimenti per riconoscerle. Tra i fenomeni riscontrati con maggior frequenza nell'anno 2023 annoveriamo, a titolo esemplificativo, le truffe basate sulla tecnica dello spoofing che, replicando numerazioni di uffici di polizia o istituti di credito, inducono le vittime a trasferire i loro risparmi su conti fraudolenti; campagne massive di smishing, sms fraudolenti che informano di presunti accessi anomali su conti correnti bancari al fine di carpire i dati di accesso delle vittime; furti di profili social e false comunicazioni di assistenza per il recupero degli account rubati. In continua crescita il numero delle segnalazioni di estorsioni a sfondo sessuale, di truffe sugli acquisti online, che colpiscono parimenti acquirente e venditore, e di false proposte di investimenti online.

L'attività più delicata ha riguardato la gestione delle numerose segnalazioni di cittadini che hanno manifestato situazioni di disagio e minacciato di compiere gesti estremi. Nel 2023 gli interventi dedicati alla prevenzione di **intenti suicidari** sono stati **166**.

Le richieste di aiuto in alcuni casi sono state inviate direttamente al sito, tramite il servizio "Segnala online", in altri sono state ricevute dalla redazione di note trasmissioni televisive che le hanno successivamente trasmesse agli agenti del Commissariato di PS online. In tali circostanze, agli operatori del Centro, è stato richiesto un tempestivo e coordinato intervento che coinvolge anche gli uffici territoriali delle Questure per raggiungere nel più breve tempo possibile la persona in pericolo. Nel mese di luglio, ad esempio, gli operatori del Commissariato online hanno ricevuto la segnalazione di una donna con sfratto esecutivo che minacciava di suicidarsi. Gli accertamenti svolti hanno consentito di individuare il luogo di residenza e chiedere l'intervento immediato di una volante sul posto. La donna si presentava agli agenti in forte stato confusionale e nel giardino dell'abitazione veniva rinvenuto materiale atto a dare seguito al gesto estremo. Lo scorso ottobre, gli operatori hanno gestito una segnalazione di un uomo che aveva manifestato l'intenzione di togliersi la vita gettandosi da un ponte. Nell'immediato, utilizzando tecniche di OsInt e le banche dati a disposizione delle forze di polizia, gli agenti sono riusciti a identificare l'uomo e, con la collaborazione della locale Questura, impedirgli di porre in essere le manifestate intenzioni suicidarie; nel mese di marzo tramite il servizio "Richiedi Informazioni" una donna si è rivolta al Commissariato di PS online perché vittima di violenza fisica e psicologica che per paura non era mai riuscita a denunciare. Grazie alla sensibilità e alle rassicurazioni ricevute dal personale del Centro la donna, in un primo momento reticente è riuscita ad aprirsi, raccontare gli episodi di violenza e chiedere aiuto agli agenti di polizia della locale Questura.

La popolarità del sito è avvalorata dal numero degli accessi che sono stati nel periodo di riferimento oltre **43 milioni.**

ATTIVITA' DI PREVENZIONE

La Polizia Postale se da un lato svolge un'incisiva attività di repressione dei reati informatici, altrettanto importante risulta essere l'azione preventiva a tutela dei minori, soprattutto per il fenomeno del cyberbullismo e di tutte le forme di prevaricazione online, fenomeni che destano grande allarme sociale.

Tra le iniziative educative si riporta il coinvolgente format teatrale itinerante e in streaming **#cuoriconnessi** che ha coinvolto oltre **340mila** studenti sul territorio nazionale.

Di rilievo è anche la campagna educativa itinerante di sensibilizzazione e prevenzione sui rischi e pericoli legati ad un uso non corretto della rete internet da parte dei minori denominata *Una vita da social* .

L'iniziativa, arrivata quest'anno alla sua XI edizione e coinvolto oltre **3 milioni** di studenti**,** attraverso il Truck didattico multimediale della Polizia Postale, ha proseguito la sua attività itinerante in Italia e all'estero.

Il progetto si cala nella filosofia dei giovani interlocutori, interagendo con un linguaggio comunicativo semplice ma esplicito, adatto a tutte le fasce di età, coinvolgendo così dai più piccoli ai docenti ai genitori, con la finalità di combattere la violenza e la prevaricazione dei giovani bulli.

L'impegno profuso dagli specialisti della Polizia Postale nell'azione di sensibilizzazione e informazione ha consentito, nell'anno appena trascorso, di realizzare incontri con docenti e genitori in circa **2.300** istituti scolastici e di coinvolgere oltre **335.000** studenti.

ATTIVITA' DI FORMAZIONE INNOVAZIONE E RICERCA NEL SETTORE DELLE TECNOLOGIE ICT E DI REALIZZAZIONE DEL CERT MINISTERO DELL'INTERNO

Nel corso dell'anno 2023, il Servizio Polizia Postale e delle Comunicazioni ha proseguito nelle attività di collaborazione con le Istituzioni Scientifiche ed Enti di Ricerca, volte ad individuare nuove metodologie di lavoro in ambito info-investigativo e di prevenzione e contrasto al *cyber crime*. In tal senso, sono stati individuati una serie di percorsi formativi specialistici di settore, con riferimento alle tematiche emergenti in ambito *cyber security*.

In particolare, sono continuate le attività di progettazione e realizzazione dei due Centri di eccellenza che opereranno sotto l'egida del nuovo Servizio per la Sicurezza Cibernetica, il quale sarà incardinato all'interno della Direzione Centrale per la Polizia Scientifica e per la Sicurezza Cibernetica, unitamente al Servizio Polizia Scientifica e al Servizio Polizia Postale e Sicurezza Cibernetica.

Il *Computer Emergency Response Team* del Ministero dell'Interno sarà chiamato a svolgere un'efficace attività di presidio e risposta interdipartimentale contro gli incidenti informatici, coordinando le attività di contenimento e ripristino, per la prevenzione e la gestione degli attacchi informatici, delle reti e dei sistemi informativi del Ministero dell'Interno mentre il *Centro di Valutazione* del Ministero dell'Interno avrà l'onere di definire le procedure e le modalità di svolgimento delle attività di verifica e valutazione dei beni ICT che l'Amministrazione vorrà dotarsi prima della collocazione degli stessi nei propri contesti infrastrutturali. I beni ICT da conferire all'interno del Perimetro di Sicurezza Nazionale Cibernetica dovranno dapprima essere valutati e certificati secondo le normative di sicurezza vigenti.

Nel corso del 2023 sono state oggetto di approfondimento le nuove tecnologie in ambito *Threat Intelligence* e *Data Feed,* con particolare riferimento allo studio e sperimentazione di nuove piattaforme *cyber*. Il personale è stato impegnato in una serie di cicli formativi in ambito

Vulnerability Assessment e *Penetration Testing* e nel testing di piattaforme *cyber range* progettate per tali scopi in collaborazione con enti esterni.
Analogamente alla preparazione tecnica degli operatori, si è proceduto alla gestione del processo di consolidamento del Perimetro di Sicurezza Nazionale Cibernetica relativo al conferimento da parte degli Uffici Dipartimentali dei propri asset ICT secondo le direttive stabilite dalla Agenzia Nazionale per la Cybersicurezza (ACN), condividendo le linee guida ricevute nonché le azioni da intraprendere in ossequio ai termini previsti dal conferimento al PSNC con particolare riguardo alle misure di sicurezza di tipo A e quelle di tipo B da realizzare entro il 2023.