POLIZIA POSTALE E PER LA SICUREZZA CIBERNETICA

REPORT ANNUALE 2024

Maggiori Informazioni:
www.commissariatodips.it

Dati aggiornati al 21 dicembre 2024

C3 Combating Cyber Crime

Sommario

Analisi statistica e rielaborazione dati a cura di: Ispettore della Polizia di Stato Gaetano Martucci.

Raccolta dati statistici a cura di: Ispettore della P. di S. Gaetano Martucci, Assistente Capo della P. di S. Luigi Ummaro, Agenti della P. di S. Matteo Menghini e Valeria Pettirossi.

Editing & Grafica a cura di: Ispettore della Polizia di Stato Gaetano Martucci

Copertina a cura di: Ispettore della P. di S. Gaetano Martucci, Assistente della P. di S. Antonio Spuma

Coordinatori delle attività: Primo Dirigente della Polizia di Stato Barbara Strappato, Vice Questore Aggiunto della Polizia di Stato Roberta Mestichella e Vice Questore Aggiunto della Polizia di Stato Alessandro Tundo.

PREMESSA

Ivano Gabrielli, *Dirigente Superiore della Polizia di Stato, Direttore del Servizio Polizia Postale e per la Sicurezza Cibernetica*

La complessiva realtà in cui sviluppiamo le nostre individualità, le nostre economie e la nostra società in generale, ha oggi acquisito una nuova dimensione, un nuovo dominio, che si aggiunge a quelli esplorati dall'esperienza senziente, all'interno del quale parimenti viviamo, realizzando, attraverso l'esercizio delle libertà costituzionalmente garantite, lo sviluppo della nostra personalità.

Sul fronte della proiezione criminale, che come ogni altra attività umana viene ad integrarsi nel dominio cibernetico, sono state molteplici le sfide affrontate nel 2024 dalla Polizia Postale.

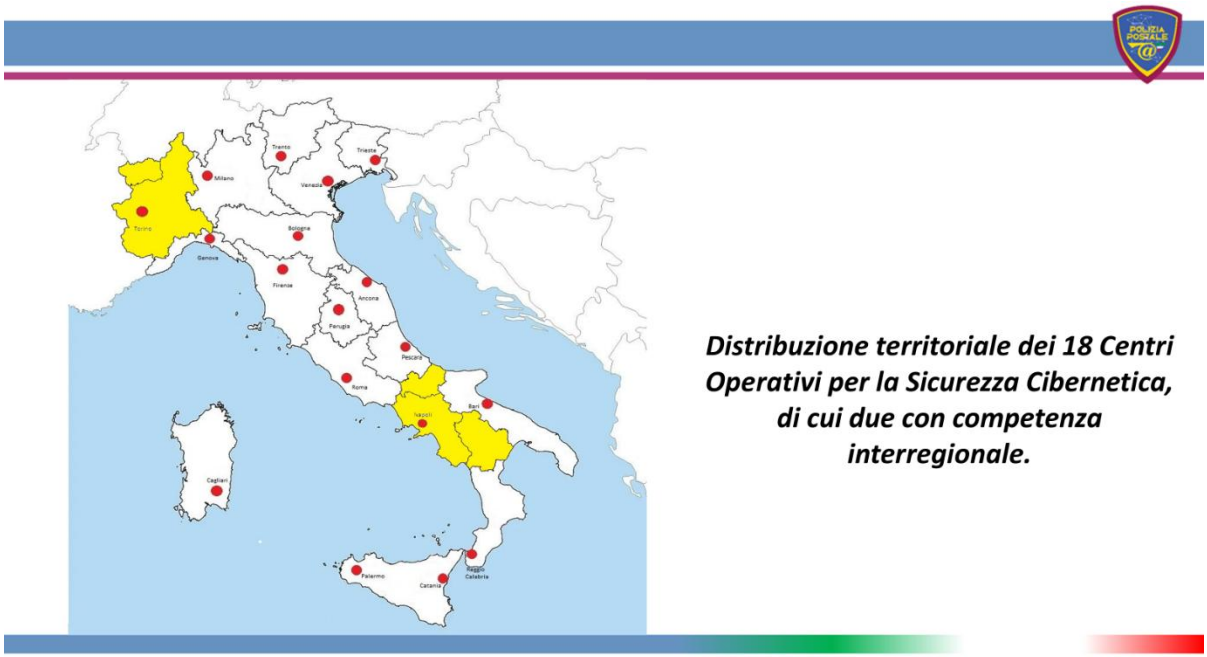
L'aumento delle minacce cibernetiche dovute ai conflitti internazionali e la crescente sofisticazione degli attacchi informatici contro le infrastrutture del Paese hanno reso necessaria una risposta più pronta e innovativa.

L'approvazione del DDL Cybersicurezza (L. 90 del 2024) ha potenziato le nostre capacità di prevenzione e contrasto, dotandoci di strumenti normativi avanzati e di una più completa architettura istituzionale che, arricchita dalla capacità di coordinamento della DNA, oggi permette la più efficace osmosi operativa tra Forze dell'ordine, Magistratura e Presidenza del Consiglio.

A questo si aggiunge l'avvio del Comitato di Analisi per la Sicurezza Cibernetica (CASC), un tavolo interistituzionale voluto dal Ministro dell'Interno, al quale periodicamente tutte le componenti delle Forze dell'Ordine, e con la partecipazione della Difesa, del comparto intelligence e di ACN, portano le proprie competenze e *know how* operativo per la condivisione di scelte coordinate nel contrasto alla minaccia criminale in ambito cyber e a supporto delle funzioni di sicurezza e gestione dell'ordine pubblico.

Tale rinnovata struttura di cooperazione interistituzionale ha a disposizione la rete dei 18 Centri Operativi per la Sicurezza Cibernetica (COSC) della Polizia Postale, attivi nei principali capoluoghi di regione e delle 82 Sezioni Operative per la Sicurezza Cibernetica, presenti nelle province, al cui vertice è posto il rinnovato Servizio Polizia Postale e per la sicurezza

cibernetica, oggi al centro della Direzione centrale per la polizia scientifica e la sicurezza cibernetica del Dipartimento della PS, dedicata all'alta investigazione tecnologica ed alle scienze forensi.



Distribuzione territoriale dei 18 Centri Operativi per la Sicurezza Cibernetica, di cui due con competenza interregionale.

Una struttura strategicamente diffusa, in grado di rispondere prontamente agli attacchi cibernetici, garantendo una copertura territoriale capillare in modalità 24/7 grazie all'impegno del Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC) dal quale dipendono gli omologhi Nuclei Operativi Sicurezza Cibernetica (NOSC), presidio di sicurezza per le pubbliche amministrazioni e le imprese strategiche del Paese, in un unico grande "sistema" di pubblica sicurezza cyber, nella disponibilità dell'Autorità Nazionale e delle Autorità Provinciali, alter ego e allo stesso tempo concorrente nel contribuire alla Sicurezza nazionale.

Sotto il profilo più strettamente criminale, la criminalità economica e finanziaria rappresenta la più significativa area di azione di organizzazioni complesse, internazionalmente distribuite. Con l'aumento delle transazioni online, frodi informatiche e furto di dati sensibili bancari, sono diventati minacce quotidiane. In tale ambito si è investito per lo sviluppo di competenze di analisi finanziaria e di cripto asset, che determinino una più efficace risposta investigativa, da sostenersi in ambito nazionale ed internazionale.

Il Centro Nazionale per il Contrasto alla Pedopornografia Online (CNCPO) permane in prima linea nella lotta contro lo sfruttamento sessuale dei minori sulla rete. Abbiamo intensificato gli sforzi, implementando nuove strategie e collaborazioni internazionali per migliorare l'efficacia delle nostre operazioni, che mirano a smantellare sistemi criminali che generano proventi enormi arrivando a offrire servizi in diretta per abusi sessuali su piccole vittime. Le nostre strutture investigative in tale settore hanno ruoli chiave in delicate indagini internazionali, nei quali siamo chiamati a condividere le tecniche di investigazione undercover perfezionate nel corso degli anni.

Le attività di sensibilizzazione e prevenzione, a partire proprio dai più piccoli, divengono quindi fondamentali, nella costruzione di consapevolezze circa i rischi presenti in rete, per lo sviluppo di competenze in termini di sicurezza che preparino i cittadini digitali del futuro. Attraverso campagne come "Una vita da social", "Cuori Connessi" e il progetto avviato con Geronimo Stilton dedicato proprio ai più piccoli, collaboriamo con scuole e comunità per educare i giovani sui pericoli della rete e promuovere comportamenti sicuri online. Monitoriamo e contrastiamo i reati contro la persona, con particolare attenzione alle donne, spesso vittime di cyber stalking e molestie e quindi di violenze che, se ben comprese e affrontate per tempo, favoriscono la più efficace attività di prevenzione.

Nella lotta alla diffusione di contenuti terroristici online, il costante monitoraggio della rete è essenziale per la precoce individuazione di minacce e per la corretta gestione dell'ordine e la sicurezza pubblica. In tale ambito le strutture della Polizia Postale operano, con importanti risultati, in costante raccordo con gli uffici specialistici della Polizia di Stato, DIGOS e Direzione centrale per la polizia di prevenzione, per prevenire fenomeni di radicalizzazione sul web e garantire quindi una completa analisi della minaccia estremista.

La formazione continua del personale e l'innovazione tecnologica sono pilastri della nostra efficienza operativa, ogni anno vengono quindi garantiti a ciascun settore operativo dedicati momenti di formazione attraverso l'erogazione di corsi bisettimanali, che permettono la crescita continua delle competenze e di mantenere il passo delle forme più evolute di criminalità informatica.

Investiamo nella ricerca e nello sviluppo di nuove tecnologie, tra cui l'intelligenza artificiale, valorizzando il rapporto costante col mondo accademico, per migliorare le nostre capacità tecnico investigative.

Quello che segue è quindi il bilancio che restituisce in numeri, il risultato di un anno di sforzi che hanno visto impegnati le donne e gli uomini della Polizia di Stato, che da oltre vent'anni sono chiamati a garantire nel dominio cibernetico la sicurezza dei cittadini.

LA PRIMA DIVISIONE DEL SERVIZIO POLIZIA POSTALE E PER LA SICUREZZA CIBERNETICA

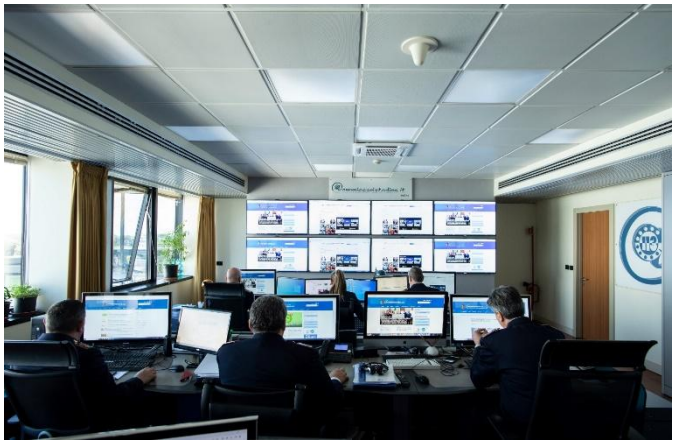
Barbara Strappato, *Primo Dirigente della Polizia di Stato, Direttore*

La **Prima Divisione** del Servizio Polizia Postale e per la sicurezza cibernetica svolge un ruolo fondamentale nella protezione dell'ambiente digitale, affrontando sfide sempre più complesse derivanti dal rapido cambiamento del mondo cibernetico.

Le attività della Divisione sono articolate in diversi settori operativi, ciascuno mirato a rispondere alle esigenze emergenti in ambito di sicurezza digitale, prevenzione del crimine informatico e protezione degli utenti della rete.

Il settore Analisi e Pianificazione Strategica, di recente istituzione, si occupa di raccogliere e analizzare i dati provenienti dall'intero territorio nazionale, al fine di fornire informazioni strategiche utili a orientare le politiche di prevenzione e contrasto al cybercrime e grazie a un costante aggiornamento delle metodologie investigative e di analisi, questo settore è in grado di definire piani operativi efficaci da condividere con gli uffici territoriali. Da tali analisi è scaturita la decisione di concentrare la gran parte delle attività di prevenzione sui minori e in particolare sui minori di anni 14, attraverso alcune attività a loro mirate seguite dal settore Relazioni Esterne. In particolare è stato adottato un approccio olistico per promuovere la sicurezza digitale, dalle campagne di sensibilizzazione sull'uso consapevole della rete al contrasto alla pedopornografia online con la mostra fotografica itinerante "Supereroi", alla pubblicazione del libro "Sulle tracce dell'hacker", realizzato in collaborazione con la Fondazione Geronimo Stilton.

Nel contesto dell'educazione alla sicurezza digitale, anche quest'anno il progetto "Una Vita da Social" ha raggiunto migliaia di studenti nelle piazze italiane e l'iniziativa "Cuori Connessi" ne ha coinvolti altrettanti on line. Queste attività si confermano eccezionali strumenti di sensibilizzazione e di formazione delle nuove generazioni, preparandole a navigare in sicurezza



nel mondo digitale. Ancora una conferma, quella del Commissariato di P.S. Online, il nostro "ponte" continuo con i cittadini, dei quali raccoglie quesiti, dubbi, problemi e ai quali fornisce informazioni, approfondimenti e *alert* relativi alle minacce emergenti nel cyberspazio, contribuendo a creare una rete di supporto e prevenzione contro i crimini informatici. Il sito web ha ricevuto quest'anno circa 3.000.000 di visite, 82.000 segnalazioni e 23.000 richieste di assistenza, riguardanti fenomeni come truffe online, *spoofing*, *smishing* ed estorsioni a sfondo sessuale.

In un ambito caratterizzato da un non spazio e dalla transnazionalità delle attività, nell'anno di Presidenza italiana del G7, rinnovate energie sono state dedicate al settore Relazioni Internazionali che ha lavorato per rafforzare la cooperazione internazionale, organizzando corsi di formazione, workshop e incontri con le forze di polizia di altri paesi, con un focus particolare sulla collaborazione con le principali agenzie di *law enforcement* statunitensi. Proprio in occasione della presidenza italiana del G7, sono stati istituiti e sviluppati gruppi di lavoro dedicati all'uso dell'intelligenza artificiale e ai rischi ad essa collegati, con l'obiettivo di creare soluzioni comuni per affrontare le nuove minacce digitali.

Di particolare rilievo è la partecipazione attiva ai gruppi di lavoro internazionali, che ha portato anche alla recente introduzione della ricezione diretta dei dati SIENA da parte del settore Archivio, migliorando la gestione delle informazioni sensibili in ambito internazionale

Nell'anno che ha visto istituita la nuova Direzione Centrale, con le sue peculiari, nuove esigenze, sono state intraprese tutte le attività necessarie a garantirne il funzionamento: il settore Personale e Servizi ha gestito quelle connesse alla gestione del personale ed è stata effettuata una mirata attività di scouting, organizzata dal Settore rapporti territoriali in tutte le scuole di polizia che hanno ospitato i corsi di formazione di allievi agenti e vice ispettori per individuare

personale altamente qualificato, con competenze tecniche avanzate, in grado di operare efficacemente in scenari operativi di elevata complessità.

A questa attività si aggiunge quella seguita dal Settore Formazione, che ha implementato percorsi formativi specifici per la formazione di nuove figure professionali, tra cui l'Analista di Fonti Aperte (O.S.I.N.T., SOC.M.INT.), l'Operatore Cyber e il *Child Sexual Exploitation Operator*, con l'obiettivo di fornire al personale le competenze necessarie per operare in ambienti digitali altamente specializzati e per contrastare in modo efficace i reati informatici, in particolare quelli a danno dei minori. In aggiunta a questi percorsi formativi specialistici, il Settore Formazione ha promosso il Master in "*Cyber Security*, Legislazione e Gestione della Sicurezza", con l'intento di approfondire le conoscenze in ambito giuridico e operativo legate alla sicurezza informatica.

L'insieme dei programmi formativi, affiancati da attività di ricerca e progettazione di proposte normative riguardanti l'intelligenza artificiale, il rafforzamento degli strumenti di contrasto alle frodi e le operazioni sotto copertura - curata dal Settore Studi e Affari Giuridici - sono essenziali per garantire una preparazione sempre aggiornata e adeguata alle nuove minacce emergenti nel cyberspazio.

In risposta alle crescenti necessità operative, è stato anche implementato il parco veicolare dei Centri Operativi per la Sicurezza Cibernetica, potenziamento curato dal Settore Automezzi. Un miglioramento reso possibile anche grazie alla collaborazione con Poste Italiane e con il supporto del Dipartimento della Pubblica Sicurezza.

LA SECONDA DIVISIONE DEL SERVIZIO POLIZIA POSTALE E PER LA SICUREZZA CIBERNETICA

Maria Rosaria Romano, *Primo Dirigente della Polizia di Stato, Direttore*

IL CENTRO NAZIONALE PER IL CONTRASTO ALLA PEDOPORNOGRAFIA ONLINE (CNCPO)

In qualità di organo del Ministero dell'Interno, il Servizio Polizia Postale ha competenze istituzionali esclusive riconosciute dalla legge istitutiva del **Centro Nazionale per il Contrasto alla Pedopornografia Online (CNCPO)**, a cui sono demandate funzioni di contrasto e prevenzione per i reati di pedopornografia e sfruttamento sessuale dei minori online.

Le competenze del CNCPO in ambito di protezione dei minori sono state significativamente ampliate per contrastare l'aumento dei crimini correlato all'accesso a servizi e applicazioni da parte di giovani utenti che condividono online contenuti video e immagini. Il riconoscimento del ruolo centrale del Centro ha portato all'adozione di normative che mirano a creare una rete di intervento strutturata per supportare tempestivamente le vittime e rafforzare le tutele contro i pericoli del web. L'approccio si concentra sulla prevenzione e il contrasto della pedopornografia, delle violenze sui minori e dei rischi legati a fenomeni giovanili come le *challenge* e i giochi pericolosi, con un'attenzione particolare alla sicurezza in rete, al monitoraggio e all'analisi delle nuove minacce.

La struttura del Centro è suddivisa in aree di competenza che coordinano i 18 Centri Operativi per la Sicurezza Cibernetica e le 82 Sezioni Operative, che contribuiscono alla prevenzione e contrasto dei crimini, oltre che all'identificazione delle vittime di sfruttamento minorile online in base al territorio di competenza.

Nel 2024 l'attenzione principale è stata rivolta al potenziamento del monitoraggio dei siti web che diffondono materiale **CSAM** (*child sexual abuse material*) attraverso l'Area Operativa 'Black List' del CNCPO. Questo sforzo ha portato alla sorveglianza di 42.031 siti web e all'inserimento di 2.775 di questi nella cosiddetta *black list*, grazie alla raccolta di tutte le segnalazioni ricevute. Questa attività ha rappresentato un passo significativo nella lotta contro la diffusione di contenuti illeciti online.

L'attività di contrasto si è focalizzata sull'identificazione delle vittime, seguendo le linee guida internazionali. Questo ha incluso l'implementazione della banca dati e la condivisione di

informazioni con le controparti estere tramite canali di cooperazione. Un'area investigativa specializzata si occupa dell'analisi e dell'inserimento dei file illeciti nella Banca Dati I.C.S.E. (*International Child Sexual Exploitation Database*), accessibile tramite Interpol e utilizzata globalmente dalle forze di polizia. Inoltre, questa area riceve informazioni **dall'Unità d'Informazione Finanziaria** (U.I.F.) della Banca d'Italia riguardanti pagamenti sospetti legati alla commercializzazione di materiale di sfruttamento sessuale dei minori online.

Grazie agli strumenti normativi che permettono indagini sotto copertura online, sono state condotte operazioni nel *Dark Web* e nel *Deep Web* per contrastare lo sfruttamento sessuale dei minori tramite sistemi informatici. Gli Uffici territoriali hanno ricevuto supporto tecnico-investigativo dal CNCPO, che ha cooperato con agenzie estere per lo scambio di informazioni e buone pratiche, inclusa la gestione di operazioni internazionali sotto copertura.

Il CNCPO ha anche studiato fenomeni emergenti come le *challenge*, diffondendo *alert* per aumentare la resilienza delle potenziali vittime e adottando misure di sicurezza per proteggere bambini e ragazzi. L'Unità di Analisi del Crimine Informatico (UACI), composta da psicologi della Polizia di Stato, integra conoscenze psico-sociali con azioni di prevenzione e contrasto ai rischi online per i minori. Il CNCPO ha rinnovato il suo impegno, collaborando con enti del terzo settore come Telefono Azzurro, *Save The Children*, *Terre des Hommes*, Associazione *Meter*, *Operation Underground Railroad*, *Child Rescue Coalition* e il *National Centre for Missing and Exploited Children*, creando protocolli operativi di collaborazione basati su partenariato pubblico e privato.

L'analisi dei dati statistici relativi alle attività coordinate dal Centro Nazionale per il Contrasto della Pedopornografia Online (CNCPO) mette in luce, rispetto al 2023, un rafforzamento complessivo delle azioni di prevenzione e contrasto al fenomeno della pedopornografia online.

In tale ambito l'incremento del numero degli arrestati, passato da 108 nel 2023 a 144 nel 2024, rappresenta un aumento percentuale del 33% ed evidenzia un rafforzamento delle azioni di contrasto diretto e una maggiore capacità di tradurre le attività investigative in misure di repressione efficaci.

Tale dato dimostra un netto incremento delle capacità operative del CNCPO e dei Centri Operativi per la Sicurezza Cibernetica e rappresenta il risultato di un approccio integrato che combina l'utilizzo di strumenti tecnologici avanzati, cooperazione internazionale e una strategia investigativa più incisiva.

L'aumento significativo dei monitoraggi, che sono passati da 28.625 a 42.031 con una crescita del 47%, evidenzia come il Centro abbia potenziato le proprie capacità di "sorveglianza" anche attraverso l'intensificazione della cooperazione internazionale. Tale circostanza risulta particolarmente rilevante perché consente di intercettare con maggiore tempestività contenuti illeciti, permettendo un intervento precoce e riducendo la possibilità di diffusione di materiale pedopornografico online.

Parallelamente, anche il numero delle perquisizioni ha registrato un incremento del 7%, aumentate da 911 a 974, evidenziando l'impegno crescente della Polizia Postale nelle attività di contrasto che si affiancano alla sorveglianza preventiva e ne rappresentano un naturale proseguimento.

A fronte di questo rafforzamento operativo, il numero delle persone indagate rispetto al 2024 risulta sostanzialmente invariato evidenziando un approccio mirato e strategico della Polizia Postale, dimostrando la capacità di indirizzare le attività investigative verso obiettivi di maggiore rilevanza, mirando a smantellare organizzazioni più strutturate e pericolose.

Per quanto riguarda i siti inseriti nella black list, il dato mostra una crescita contenuta dell'1%, con un aumento da 2.739 a 2.775. Questo incremento suggerisce una vigilanza costante della rete svolta dalla Polizia Postale che consente di intercettare i contenuti illeciti online, assicurando l'inibizione alla fruizione di contenuti pedopornografici e limitando l'accesso a materiale illegale.

In sintesi, l'analisi dei dati evidenzia come il CNCPO abbia saputo coordinare e rafforzare le attività di prevenzione e repressione. L'aumento del numero delle persone arrestate, dei

monitoraggi e delle perquisizioni dimostra un impegno crescente e una capacità operativa più efficace, risultato di una combinazione di fattori quali l'adozione di nuove tecnologie, l'ottimizzazione delle risorse e il rafforzamento della cooperazione internazionale.

La Sezione Operativa

Nel corso dell'anno 2024 incisiva è stata l'attività della **Sezione Operativa** riguardo il contrasto ai reati contro la persona commessi attraverso l'utilizzo dei dispositivi informatici e i social network, svolgendo altresì un'attività di monitoraggio attiva degli spazi web, in particolare delle piattaforme social, finalizzata alla prevenzione e contrasto di condotte penalmente rilevanti, riguardante principalmente i reati commessi contro la persona (*revenge porn, cyber stalking, romantic scam, sex extortion, ecc.)*.

Con riferimento a questa tipologia di reati, particolare attenzione è stata dedicata a tutte quelle forme di aggressione espressamente previste dalla recente normativa che va sotto il nome di "*codice rosso*", che, avendo introdotto una maggiore tempestività nella risposta giudiziale, ha reso più efficace l'attività della Polizia Giudiziaria e quindi più efficace la protezione delle vittime.

Anche per le cd. truffe romantiche (*romantic scam*) l'attività di contrasto è stata particolarmente attenta, soprattutto in relazione alla situazione di forte disagio in cui la vittima viene a trovarsi dopo aver scoperto e realizzato di aver subito un raggiro sentimentale, creando un danno psico-fisico, oltre a quello economico.

La proliferazione di tale tipologia di reato è sicuramente collegata all'uso sempre maggiore dei social network e dei siti di *dating* (incontri).

Tale connotazione *transnazionale* dei reati di competenza della Sezione Operativa ha permesso di poter accedere ai canali di collaborazione internazionale, interessando i collaterali attraverso gli uffici di Europol e Interpol, anche per favorire una capillare **azione di coordinamento** a livello nazionale delle attività effettuate ad opera degli uffici della Specialità dislocati su tutto il territorio nazionale.

Si segnalano, inoltre, specifiche iniziative 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, Instagram, Telegram, Pinterest e Youtube, ecc.), finalizzati ad arginare la diffusione del linguaggio d'odio (*hate speech*), in costante collaborazione con l'Osservatorio per la Sicurezza contro gli Atti Discriminatori.

Sono state oggetto di attività di pubblico soccorso le numerose segnalazioni ricevute da social network, dal Servizio di Cooperazione Internazionale e attraverso il portale del Commissariato

di PS Online, per manifesti intenti suicidari, fenomeno che ha visto una consistente crescita dei casi, la cui gestione ha previsto anche l'attivazione di sistemi di tracciamento (cd. *positioning)* legati ai dispositivi elettronici (smartphone) utilizzati.

Le attività coordinate dalla Sezione Operativa hanno evidenziano un impegno incisivo nel contrasto di reati legati a minacce, stalking ed estorsione. Tra le principali operazioni spiccano gli arresti di diverse persone accusate di atti persecutori, sia contro ex colleghi che contro partner, utilizzando strumenti informatici.

Sono stati inoltre arrestati individui accusati di circonvenzione di incapace e di estorsione mediante la minaccia di pubblicazione di foto intime. Infine, a seguito di un'indagine durata due anni, è stata smantellata un'attività illecita di monetizzazione di bonus statali, con la denuncia di cinque persone coinvolte in diverse Regioni.

LA TERZA DIVISIONE DEL SERVIZIO POLIZIA POSTALE E PER LA SICUREZZA CIBERNETICA

Cristiano Leggeri, *Primo Dirigente della Polizia di Stato, Direttore*

IL CENTRO NAZIONALE ANTICRIMINE INFORMATICO PER LA PROTEZIONE DELLE INFRASTRUTTURE CRITICHE (CNAIPIC)

Anche per il 2024 l'azione della Polizia Postale svolta dal **CNAIPIC** nel settore della protezione dagli attacchi informatici verso le infrastrutture critiche informatizzate si è declinata lungo il duplice crinale dell'attività di prevenzione, a beneficio delle realtà - pubbliche o private, di rilevanza nazionale e locale - eroganti servizi pubblici essenziali, e l'attività di contrasto, con rilevanti attività d'indagine concluse nell'anno.

L'attività di prevenzione, che racchiude le capacità di monitoraggio e analisi della minaccia cyber da parte del **CNAIPIC**, è strutturalmente basata sulle virtuose logiche del partenariato pubblico-privato, attraverso la stipula di accordi di collaborazione in grado di stabilire un ecosistema permanente di collegamento tra esperti di polizia e responsabili tecnici delle infrastrutture critiche, nazionali e locali.

Il risultato è apprezzabile nelle migliaia di informazioni di sicurezza preventiva rilasciate tra Polizia Postale e Infrastrutture critiche, con un incremento dello scambio informativo utile a limitare numero e impatto degli attacchi effettivamente registrati.

Le metodologie criminali confermano un'elevata incidenza di attacchi *ransomware*[1] e di DDoS[2] diretti ad ampio spettro a infrastrutture pubbliche, nazionali e territoriali – con particolare riferimento alle pubbliche amministrazioni locali, specie Comuni e Aziende Sanitarie – e verso aziende erogatrici di servizi essenziali in diversi settori (es. Trasporti, Finanze, Sanità, Telecomunicazioni).

In linea generale, lo scenario aggiornato della minaccia cyber vede ormai stabilmente aggiungersi, ad una matrice puramente criminale, un'origine riconducibile all'operare di attori *state-sponsored*, anche in conseguenza della estrema instabilità dello scenario geopolitico di riferimento.

I conflitti russo-ucraino e mediorientale rendono il dominio cibernetico uno spazio imprescindibile per lo sviluppo delle ostilità, generando altresì campagne di matrice ideologica da parte di gruppi *hacktivisti* verso i paesi occidentali, inclusa l'Italia.

Le attività preventive del CNAIPIC hanno trovato una rilevante dimensione applicativa sul fronte della gestione dei grandi eventi, dove la tutela del perimetro informatico ha garantito – e garantisce – lo svolgimento delle più importanti iniziative registrate sul territorio nazionale.

Il riferimento va innanzitutto al Vertice del G7 svoltosi in Puglia dal 13 al 15 giugno, alla presenza dei Capi di Stato e di Governo degli Stati Membri, oltre al Presidente del Consiglio Europeo e alla Presidente della Commissione Europea. Non meno importante, per durata e visibilità mondiale dell'evento, è il Giubileo della Speranza 2025 che preso avvio a partire da Natale e che vede la Postale, con il Centro Anticrimine Informatico e le articolazioni territoriali costituite dai NOSC, attivamente impegnata nella predisposizione di un dispositivo di sicurezza delle infrastrutture informatiche maggiormente esposte incentrato su una costante attività di monitoraggio della rete volta all'individuazione di potenziali minacce, sia fisiche che cyber.

Sul fronte, infine, dell'attività investigativa, il 2024 ha visto la conclusione da parte del CNAIPIC di una tra le più rilevanti operazioni di polizia mai realizzate nel settore, con

---

[1] **112** attacchi a I.C., O.S.E. e P.A.L. Gli attacchi comprese le aziende e realtà economiche più piccole nel 2024 sono al 21 dicembre, **283**.

[2] **21** attacchi a I.C., O.S.E. e P.A.L. Gli attacchi comprese le aziende e realtà economiche più piccole nel 2024 sono al 21 dicembre, **46**.

l’individuazione degli autori della manovra ostile ai danni del sistema informatico del Ministero della Giustizia, qualificabile come il più vasto attacco informatico sinora registrato ai danni di un’infrastruttura servente una funzione essenziale dello Stato.

La Sezione Cyberterrorismo

La proiezione operativa della **Sezione Cyberterrorismo** si rivolge al monitoraggio della propaganda estremista ed è funzionale alla prevenzione e repressione dei reati che utilizzano la dimensione virtuale per fini terroristici.

Nel corso del 2024 sono stati censiti molteplici spazi di natura estremista; tale monitoraggio ha consentito di svolgere un *"RAD - Referral Action Day"* sotto l'egida di Europol, che ha condotto all'oscuramento di 2000 contenuti dal tenore negazionista e suprematista.

La sezione gestisce attivamente, inoltre, i numerosi casi SIENA in entrata, generandone di ulteriori in uscita sulla base di spunti investigativi originati dal territorio italiano.

L'ideologia radicale jihadista - come evidenziato dalle molteplici attività di perquisizione svolte sul territorio - risulta spesso commista a situazioni di disagio e scarsa integrazione sociale, fattori che aggravano l'isolamento dei potenziali "*lone wolves*"; in tali circostanze gli strumenti digitali possono diventare un fattore di accelerazione delle individualità estremiste, inducendole all'attivazione di progettualità concrete anche attraverso il reperimento o la costruzione "*home made*" di armi rudimentali.

Sono state svolte, inoltre, numerose attività investigative sul fenomeno del cyber-terrorismo di matrice accelerazionista/neonazista, che hanno consentito di delinearne l'estrema attualità, individuando il pericoloso decorso di processi di radicalizzazione individuale, in particolare nelle fasce di utenti minorenni o comunque di giovane età.

È noto come le piattaforme virtuali di comunicazione rappresentino uno degli ambienti più agevoli per la diffusione di notizie false, che possono incidere sui processi di formazione del consenso elettorale nonché, più in generale, sulla percezione dei fenomeni sociali. La tematica della disinformazione, pertanto, è stata oggetto di puntuale approfondimento tramite tecniche

O.S.Int, volte ad individuare i soggetti che si rendono responsabili della propagazione di notizie idonee a turbare l'ordine e sicurezza pubblica.

Sul piano operativo nel corso del 2024 la Sezione Cyberterrorismo ha coordinato numerose attività di perquisizione sul territorio nazionale. Ultima in ordine cronologico è l'attività del Centro Operativo per la Sicurezza Cibernetica della Lombardia, che insieme a DIGOS e agli uffici territoriali della Polizia Postale, ha eseguito perquisizioni in tutta Italia contro soggetti accusati di propaganda e istigazione a delinquere per motivi di discriminazione razziale, etnica e religiosa.

Si aggiunge, infine, che nell'ambito del contrasto al c.d. "hate speech" e ai crimini d'odio sono state avviate una serie di attività d'indagine, originate sia da segnalazioni OSCAD, sia da monitoraggio svolto d'iniziativa dalla Sezione.

LA QUARTA DIVISIONE DEL SERVIZIO POLIZIA POSTALE E PER LA SICUREZZA CIBERNETICA

Luigi Bovio, *Vice Questore della Polizia di Stato, Direttore reggente*

Nel delineare gli elementi afferenti all'ambito economico finanziario c.d. ***Financial cybercrime*** corre l'obbligo di segnalare che difficilmente tale contesto risulta immune agli effetti del crimine.

Le evidenze acquisite nella più recente azione di contrasto ai citati fenomeni criminali hanno permesso di registrare una persistente diffusione di condotte truffaldine, tali da necessitare l'istituzione di una apposita Divisione con il precipuo intento di contrastare i reati finanziari.

Si è potuto accertare che le principali modalità di realizzazione delle truffe avviene attraverso campagne di *phishing* (anche nelle varianti del c.d. "*vishing*" e del c.d. "*smishing*")[3], consumate ai danni di persone fisiche, PMI e grandi società e perpetrate per il tramite di email 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 la successiva commissione di reati contro il patrimonio.

Analogamente, si registra la persistente aggressività sociale delle frodi basate sulle tecniche di *social engineering*, con particolare riferimento alla c.d. *BEC fraud*,[4] 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 crescita del livello qualitativo dei contesti criminali impegnati nel c.d. *financial cybercrime*: la possibilità di conseguire ingenti guadagni attraverso condotte delinquenziali che possono essere realizzate massivamente e su larga scala, infatti, ha inevitabilmente determinato

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

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

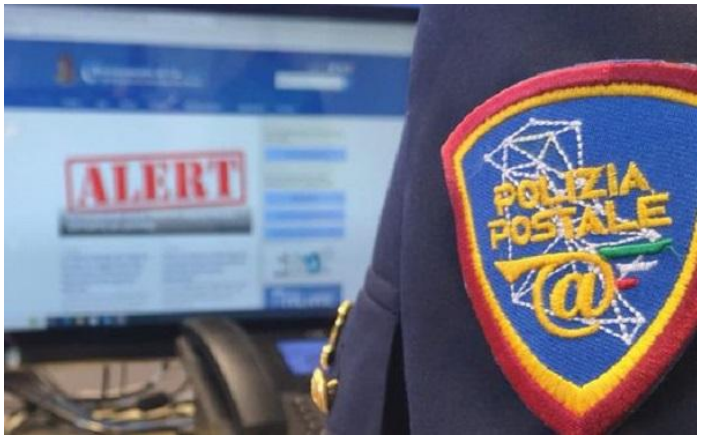
un innalzamento dello spessore delinquenziale dei soggetti attivi, spesso associati in consorterie criminali.

La particolare natura delle specifiche condotte delittuose 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; circostanza che talora rende complessa la raccolta delle evidenze ricercate, laddove i paesi stranieri impattati nella richiamata ricerca non supportino in maniera collaborativa l'Autorità Giudiziaria italiana.

Ulteriore elemento di interesse e di difficoltà operativa, è costituito dal sempre più frequente ricorso alle "criptovalute"[5], le cui transazioni (registrate attraverso sistemi di *blockchain*) si caratterizzano per una maggiore difficoltà di tracciamento e per la conseguente necessità di impegnare professionalità con elevati livelli di competenze. Al fine di contrastare tale fenomeno sono stati specializzati 42 operatori, 6 del Servizio Polizia Postale e per la Sicurezza Cibernetica e 2 per ciascuno dei 18 Centri Operativi per la Sicurezza Cibernetica diffusi su tutto il territorio nazionale.

Nell'ambito del panorama delittuoso di interesse si segnala la forte espansione delle truffe attuate tramite proposte di investimenti di capitali online (il c.d. *trading online*). Le evidenze più recenti riportano, infatti, una decisa crescita delle denunce e, conseguentemente dei capitali investiti sottratti alle vittime, con un coinvolgimento di soggetti passivi del reato non più circoscritto a persone vulnerabili come gli anziani, ma esteso a diverse tipologie di "investitori", segno della sempre maggiore capacità organizzativa della sottesa struttura criminale, ramificata per lo più all'estero.

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



L’uso dilagante dell’informatica, più in particolare della rete internet, in ogni settore della vita sociale, ha agevolato anche la consumazione di reati contro la proprietà intellettuale, con il conseguente diretto coinvolgimento della Polizia Postale e per la Sicurezza Cibernetica anche nella prevenzione e repressione dei reati in violazione del diritto d’autore, qualora consumati con l’utilizzo della rete internet. Tra i principali settori interessati al fenomeno della contraffazione, sulla base di quanto emerge dalle denunce e dalle susseguenti attività investigative, emergono le piattaforme Pay-tv – IPTV, Moda-tessile, luxury goods, polizze assicurative, falsi biglietti per l’accesso a eventi culturali, siti clone – utilizzo di marchi depositati, contraffazione del marchio CE e diffusione illecita di film.

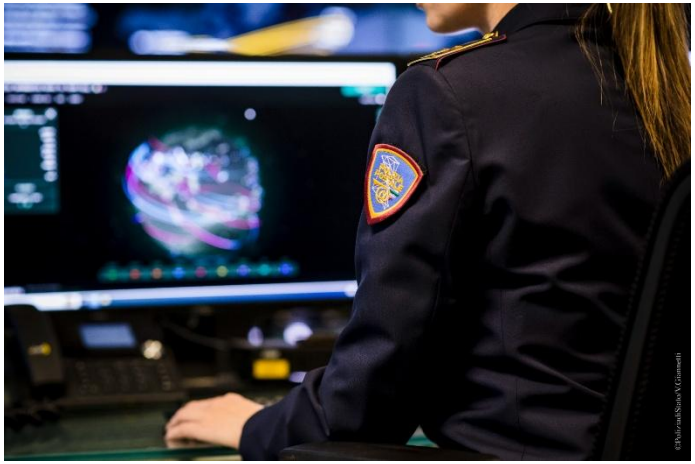
LA QUINTA DIVISIONE DEL SERVIZIO POLIZIA POSTALE E PER LA SICUREZZA CIBERNETICA

Santo Mirabelli, *Primo Dirigente Tecnico della Polizia di Stato, Direttore*

Nell'ambito delle attività svolte dalla **Quinta Divisione** del Servizio Polizia Postale nel corso del 2024, è stato dato particolare impulso all'avvio di un importante programma di potenziamento delle dotazioni tecnologiche a supporto delle investigazioni nel settore del Cybercrime.

Un ulteriore settore che ha visto un significativo coinvolgimento della Divisione è stato il potenziamento delle tecnologie di sicurezza informatica, sia per la protezione delle infrastrutture IT degli uffici territoriali e centrali del Servizio Polizia Postale e per la Sicurezza Cibernetica, sia per supportare le attività di analisi degli incidenti informatici e le conseguenti investigazioni correlate. In particolare, sono state avviate e finalizzate numerose procedure amministrative, che hanno portato al rinnovo e all'acquisizione di nuove tecnologie a supporto delle investigazioni nonché all'ampliamento delle postazioni di lavoro fisse e mobili degli uffici territoriali e centrali, con oltre 900 nuove postazioni.

Rilevante è stato l'impegno profuso in contesti internazionali, che ha visto la Quinta Divisione impegnata su vari tavoli. Di particolare rilievo è stato il ruolo svolto nell'ambito del G7 - Italia, nel sottogruppo denominato High Tech Crime, e in Europol, dove sono stati ricoperti vari ruoli nel Consiglio di amministrazione dell'European Cyber Board, un organismo volto a individuare le tecnologie più innovative a supporto delle investigazioni. Inoltre, la Divisione ha partecipato a vari tavoli di lavoro per l'analisi del Regolamento Europeo sull'Intelligenza Artificiale, recentemente pubblicato nella Gazzetta Ufficiale Europea, la cui effettiva entrata in vigore avverrà nel nuovo anno.



In riferimento alla tematica dell'Intelligenza Artificiale e al suo impiego nel settore della Cyber Security, significativi sono stati gli sforzi della Divisione sia in ambito formativo, con la realizzazione di numerosi moduli formativi sull'*awareness* e la conoscenza di tale tecnologia, sia nell'analisi dei benefici derivanti da un corretto uso e dei rischi associati a un uso inappropriato. Questi moduli formativi sono stati resi disponibili sia al personale della Polizia di Stato (in vari ruoli direttivi e non direttivi), sia a determinate categorie di utenza, inclusi i partecipanti al corso di Cyber Academy realizzato con gli Istituti ITS.

Inoltre, è stato dato forte impulso agli aspetti di Innovazione e Ricerca, con la Quinta Divisione impegnata in approfondite attività di ricerca di mercato per comprendere le tecnologie disponibili e in via di sviluppo. Sono state consolidate collaborazioni con il mondo accademico attraverso la condivisione di progetti innovativi che vedono l'impiego dell'Intelligenza Artificiale per la Cyber Security sia nel settore delle investigazioni, sia nella protezione delle infrastrutture critiche.

REPORT STATISTICO

A cura del Settore Analisi e Pianificazione Strategica (Ispettore della Polizia di Stato Gaetano Martucci, Assistente Capo della Polizia di Stato Luigi Ummaro, Agente della Polizia di Stato Matteo Menghini e Agente della Polizia di Stato Valeria Pettirossi)

Con grande impegno e dedizione il Servizio Polizia Postale e per la sicurezza cibernetica ha svolto un'intensa attività durante tutto il 2024, affrontando e superando numerose sfide legate alla criminalità informatica. Questa sezione del report è dedicata all'analisi dei dati statistici che rappresentano analiticamente le attività svolte nel corso dell'anno.

Per finalità di resoconto di fine anno, la rilevazione dei dati a livello nazionale è stata effettuata il 21 dicembre 2024. Si prevede che la pubblicazione dei dati consolidati, aggiornati al 31 dicembre 2024, avverrà nella terza decade del mese di gennaio 2025.

La rappresentazione analitica delle attività di prevenzione e contrasto attuate dalla Specialità Cibernetica della Polizia di Stato ripercorrerà le divisioni che formano il Servizio Polizia Postale. Questa metodologia permetterà di offrire una visione chiara e dettagliata dell'impegno profuso e dei risultati ottenuti in ogni ambito di competenza.

POLIZIA POSTALE E PER LA SICUREZZA CIBERNETICA - OVERVIEW

Nel corso dell'anno 2024 la Polizia Postale e per la sicurezza cibernetica ha svolto un'intensa attività investigativa, aprendo 54.554 fascicoli di indagine, denunciando 7.884 persone. Tale impegno ha permesso di mantenere un livello operativo in linea con i risultati conseguiti nell'anno precedente.

Polizia postale e per la sicurezza cibernetica
Sicurezza informatica

	Dal 01/01/2023 al 21/12/2023		Dal 01/01/2024 al 21/12/2024	
	Casi totali	**Persone indagate**	**Casi totali**	**Persone indagate**
Attacchi IC – OSE – PAL, privati ed aziende	11.930	220	11.887	178
Pedopornografia e adescamento on-line	2.662	1.224	2.809	1.172
Prevenzione antiterrorismo	236	60	138	59
Reati contro la persona	9.433	1.235	9.191	1.382
Frodi informatiche e monetica	10.606	917	8.468	919
Truffe on-line	16.325	3.571	18.714	3.581
Reati in ambito postale	517	36	466	42
Altri reati	2.936	517	2.881	551
TOTALE	**54.645**	**7.780**	**54.554**	**7.884**

© Polizia Postale - Report annuale 2024 - Aggiornamento 21/12/2024

IL COMMISSARIATO DI P.S. ONLINE

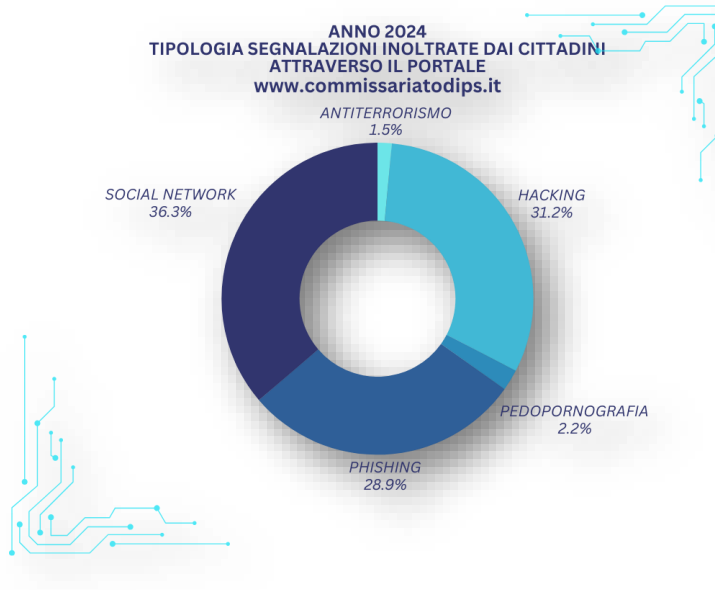
Nel contesto della crescente digitalizzazione della nostra società, la sicurezza cibernetica assume un ruolo fondamentale nella protezione delle infrastrutture critiche e nella salvaguardia dei cittadini. Il Commissariato di P.S. Online rappresenta un punto di contatto essenziale tra la Polizia Postale e i cittadini, offrendo un servizio continuo e accessibile per la segnalazione di reati informatici e per la diffusione di informazioni e consigli sulla sicurezza online.

Il Commissariato di P.S. Online non solo risponde alle segnalazioni e ai bisogni dei cittadini, ma svolge anche un ruolo proattivo nella prevenzione delle attività criminali sul web. Attraverso il sito www.commissariatodips.it, il Commissariato promuove campagne di sensibilizzazione e prevenzione, informando gli utenti sui rischi della rete e promuovendo comportamenti sicuri online.

RICHIESTA INFORMAZIONI	VISITE AL SITO www.commissariatodips.it	ACCESSI AL SITO www.commissariatodips.it
23.135	2.895.314	53.426.009

Un aspetto particolarmente notevole di questo servizio è la sua abilità nel rispondere prontamente alle nuove sfide del cyberspazio. Monitorando costantemente la rete, gli esperti del Commissariato identificano minacce emergenti e lavorano proattivamente per neutralizzarle prima che possano causare danni. Questo impegno costante alla protezione e all'educazione rende il Commissariato di P.S. Online un baluardo di sicurezza in un mondo sempre più interconnesso.

ALERT DIRAMATI	SEGNALAZIONI SOCCORSO PUBBLICO
31	195



SEGNALAZIONI	
Antiterrorismo	1.216
Hacking	25.778
Pedopornografia	1.815
Phishing	23.896
Social Network	29.970
Totale	**82.675**

© Polizia Postale - Report annuale 2024 - Aggiornamento 21/12/2024

Il diagramma presenta le segnalazioni ricevute dal portale www.commissariatodips.it nel corso del 2024, fino al 21 dicembre. I dati sono suddivisi in cinque categorie principali:

- **SOCIAL NETWORK (36.3%)**: La maggior parte delle segnalazioni riguarda problemi legati ai social media. Questo dato riflette l'ubiquità e l'uso quotidiano delle piattaforme sociali, che possono essere sfruttate per varie forme di abuso e crimine digitale, come il cyberbullismo e le molestie online.
- **HACKING (31.2%)**: Le segnalazioni relative all'hacking rappresentano una parte consistente del totale. Questo indica la crescente preoccupazione per la sicurezza dei sistemi informatici e la necessità di proteggere le informazioni sensibili da accessi non autorizzati.
- **PHISHING (28.9%)**: Il phishing continua a essere una delle principali minacce, con un numero significativo di segnalazioni. Questi attacchi mirano a ingannare gli utenti

per ottenere informazioni personali e finanziarie, sottolineando l'importanza dell'educazione e della sensibilizzazione su come riconoscere e prevenire tali truffe.

- **PEDOPORNOGRAFIA (2.2%)**: Sebbene rappresentino una percentuale minore rispetto ad altre categorie, le segnalazioni riguardanti la pedopornografia sono di estrema gravità e richiedono un intervento tempestivo per proteggere i minori e perseguire i colpevoli.
- **ANTITERRORISMO (1.5%)**: Anche se in percentuale minore, le segnalazioni relative all'antiterrorismo sono fondamentali per garantire la sicurezza nazionale e prevenire atti di violenza.

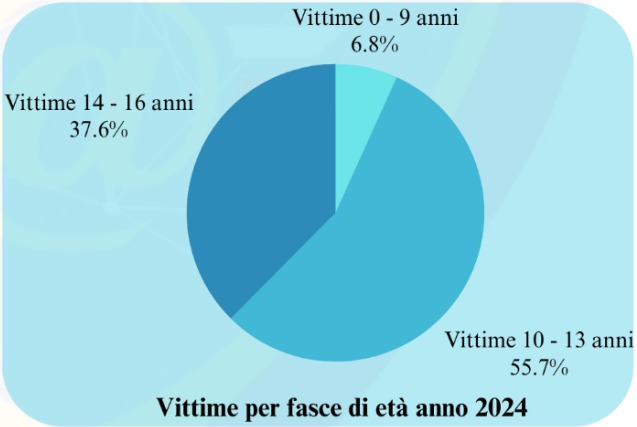
PEDOPORNOGRAFIA E ADESCAMENTO ONLINE

	Casi trattati	Persone arrestate	Persone denunciate	Perquisizioni	Siti presenti in black list	Siti visionati
Anno 2024	2.809	144	1.028	974	2.775	42.031
Anno 2023	2.662	108	1.116	911	2.739	28.625
Var. %	+6%	+33%	-8%	+7%	+1%	+47%

I dati del 2024 mostrano un aumento complessivo nei casi trattati e nelle operazioni di contrasto, con un numero maggiore di persone arrestate e perquisizioni effettuate.

Adescamento minori online	TOTALE casi trattati	%	Casi trattati vittime 0-9 anni	%	Casi trattati vittime 10-13 anni	%	Casi trattati vittime 14-16 anni	%
Anno 2024	370	+5%	25	-19%	206	+0%	139	+22%
Anno 2023	351		31		206		114	

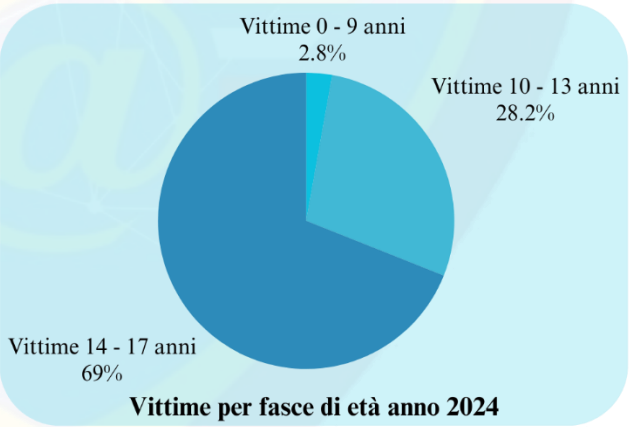
I dati evidenziano un incremento generale del 5% nei casi totali di adescamento di minori online dal 2023 al 2024. La fascia d'età 0-9 anni ha visto una diminuzione del 19% nei casi, mentre la fascia 10-13 anni è rimasta stabile. Tuttavia, la fascia 14-16 anni ha registrato un incremento significativo del 22%, segnalando una crescente vulnerabilità in questo gruppo di età.



Vittime per fasce di età anno 2024

Cyberbullismo	TOTALE casi trattati	%	Casi trattati vittime 0-9 anni	%	Casi trattati vittime 10-13 anni	%	Casi trattati vittime 14-17 anni	%
Anno 2024	319	+12%	9	+13%	90	+27%	220	+7%
Anno 2023	284		8		71		205	

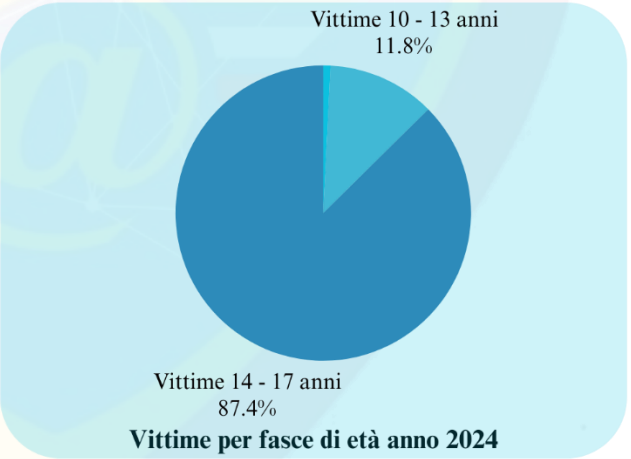
L'analisi dei dati indica un aumento complessivo del 12% nei casi di cyberbullismo trattati nel 2024 rispetto al 2023. Le fasce d'età 0-9 anni e 10-13 anni hanno registrato gli incrementi più significativi, rispettivamente del 13% e del 27%. La fascia d'età 14-17 anni ha visto un aumento più moderato del 7%, ma continua a essere la fascia più colpita con il 69% dei casi totali.



Vittime per fasce di età anno 2024

Sextortion	TOTALE casi trattati	%	Casi trattati vittime 0-9 anni	%	Casi trattati vittime 10-13 anni	%	Casi trattati vittime 14-17 anni	%
Anno 2024	127	-7%	1	-50%	15	-25%	111	-3%
Anno 2023	136		2		20		114	

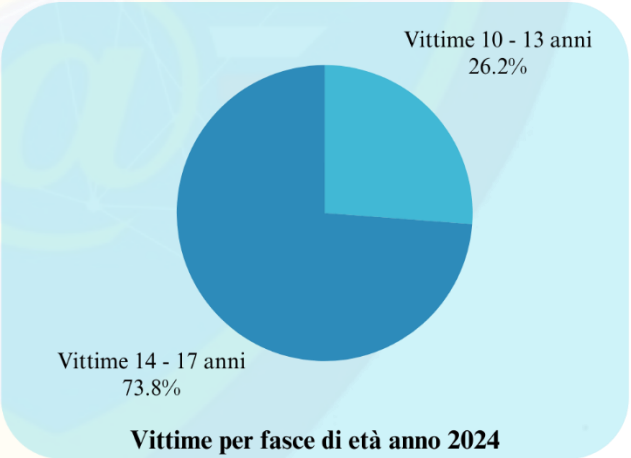
L'analisi dei dati evidenzia una riduzione complessiva del 7% nei casi di sextortion dal 2023 al 2024. Tutte le fasce d'età hanno registrato una diminuzione nei casi trattati. Tuttavia, la fascia d'età 14-17 anni rimane la più colpita, rappresentando la maggioranza dei casi in entrambi gli anni.



Vittime per fasce di età anno 2024

Revenge Porn	TOTALE casi trattati	%	Casi trattati vittime 0-9 anni	%	Casi trattati vittime 10-13 anni	%	Casi trattati vittime 14-17 anni	%
Anno 2024	42	+45%	0	+0%	11	+83%	31	+35%
Anno 2023	29		0		6		23	

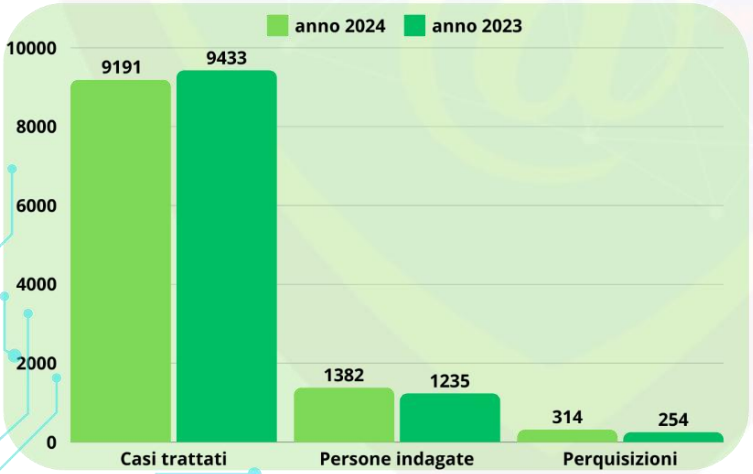
L'analisi dei dati evidenzia un aumento complessivo del 45% nei casi di revenge porn dal 2023 al 2024. La fascia d'età 10-13 anni ha registrato l'incremento più significativo (+83%), mentre la fascia 14-17 anni rimane la più colpita con 31 casi nel 2024.



Vittime per fasce di età anno 2024

REATI CONTRO LA PERSONA

	Casi totali	Persone indagate	Perquisizioni
Anno 2024	9.191	1.382	314
Anno 2023	9.433	1.235	254
Var. %	-3%	+12%	+7%



I reati online contro la persona
Questi reati includono diffamazione, minacce, estorsioni sessuali e altre forme di abuso che possono avvenire attraverso internet. Nel 2024, le denunce totali per reati online contro le persone hanno registrato una flessione del 3% rispetto al 2023. Nonostante ciò, il numero delle persone indagate è aumentato del 12%.

DETTAGLIO CYBERSTALKING

	Casi trattati	Vittime uomini	Vittime donne	Persone indagate
Anno 2024	185	59	126	123
Anno 2023	184	67	117	80
Var. %	+1%	-12%	+8%	+54%

Anno 2024

Cyberstalking: Il cyberstalking è una forma di persecuzione online in cui l'autore utilizza la tecnologia per intimidire, molestare o minacciare le vittime (art. 612 bis c.p.).
Al 21 dicembre 2024, i casi registrati di cyberstalking sono stati 185, di cui 59 hanno riguardato uomini e 126 donne (il 68% del totale), mostrando un aumento significativo delle vittime femminili rispetto allo scorso anno.

DETTAGLIO REVENGE PORN

Anno 2024

Revenge Porn: Il "revenge porn" riguarda la diffusione non consensuale di immagini o video intimi di un individuo (art. 612 ter c.p.). Nel 2024, si è osservato un decremento del 6% nelle denunce presentate presso la Polizia Postale rispetto all'anno precedente. Tuttavia, le donne continuano a rappresentare la maggioranza delle vittime di questo fenomeno, costituendo il 73% del totale.

	Casi trattati	Vittime uomini	Vittime donne	Persone indagate
Anno 2024	264	72	192	93
Anno 2023	281	79	202	114
Var. %	-6%	-9%	-5%	-18%

DETTAGLIO MOLESTIE

	Casi trattati	Vittime uomini	Vittime donne	Persone indagate
Anno 2024	541	208	333	80
Anno 2023	620	183	437	73
Var. %	-13%	+14%	-24%	+10%

Anno 2024

Molestie online: Le molestie online, sono comportamenti intimidatori o molesti attuati attraverso strumenti digitali quali social media, e-mail o messaggi (art. 660 c.p.). Nel 2024, le denunce per molestie online hanno registrato una diminuzione del 13% rispetto all'anno precedente. Tuttavia, è stato osservato un aumento del 14% delle vittime maschili e una diminuzione del 24% delle vittime femminili che rappresentano il 62% del totale. Le persone indagate per tali reati sono aumentate del 10%.

DETTAGLIO SEXTORTION

Anno 2024

Sextortion: La sextortion è una forma di estorsione sessuale in cui le vittime vengono ricattate con la minaccia di diffondere immagini o video intimi. Nel 2024, i casi denunciati presso la Polizia Postale sono aumentati del 3% rispetto all'anno precedente, passando da 1.460 a 1.507. Le vittime uomini sono aumentate del 4%, mentre le vittime donne sono diminuite del 3%. Gli uomini rappresentano l'86% delle vittime di questo reato.

	Casi trattati	Vittime uomini	Vittime donne	Persone indagate
Anno 2024	1.507	1.295	212	130
Anno 2023	1.460	1.241	219	165
Var. %	+3%	+4%	-3%	-21%

DETTAGLIO MINACCE ONLINE

	Casi trattati	Vittime uomini	Vittime donne	Persone indagate
Anno 2024	613	321	292	119
Anno 2023	820	396	424	123
Var. %	-25%	-19%	-31%	-3%

Anno 2024

Minacce online: Le minacce online costituiscono un reato in cui individui o gruppi utilizzano internet per intimidire, molestare o minacciare altre persone (art. 612 c.p.). Nel 2024, sono stati trattati 613 casi, con 321 vittime uomini e 292 vittime donne. La variazione percentuale tra il 2023 e il 2024 mostra una diminuzione del 25% nei casi trattati, del 19% nelle vittime uomini e del 31% nelle vittime donne. Questi dati evidenziano una riduzione complessiva delle denunce, con una diminuzione più marcata tra le vittime donne.

DETTAGLIO DIFFAMAZIONE ONLINE

Anno 2024

Diffanazione online: La diffamazione online è un fenomeno in cui vengono diffusi, attraverso internet, contenuti falsi o offensivi che danneggiano la reputazione di individui o gruppi (art. 595 c.p.). I dati del 2024 mostrano una diminuzione del 4% nei casi trattati. Gli uomini rappresentano il 62% delle vittime di questo reato. Il numero delle persone indagate è aumentato del 19%.

	Casi trattati	Vittime uomini	Vittime donne	Persone indagate
Anno 2024	1.954	1.205	749	620
Anno 2023	2.038	1.254	784	522
Var. %	-4%	-4%	-4%	+19%


TOTALE ATTACCHI RILEVATI NEL 2024
Target: Infrastrutture critiche, Operatori Servizi Essenziali,
Pubbliche Amministrazioni locali, Aziende e Privati
Totale attacchi 11.887
Persone indagate 178
Alert diramati 59.373
Richiesta di cooperazione
internazionale High Tech Crime G8
63


Distribuzione attacchi durante il 2024
1400
1200
1000
800
600
400
200
0
1008
1027
1006
959
1037
866
1360
1099
974
1026
879
646
Gennaio
Febbraio
Marzo
Aprile
Maggio
Giugno
Luglio
Agosto
Settembre
Ottobre
Novembre
Dicembre (al giorno 21)

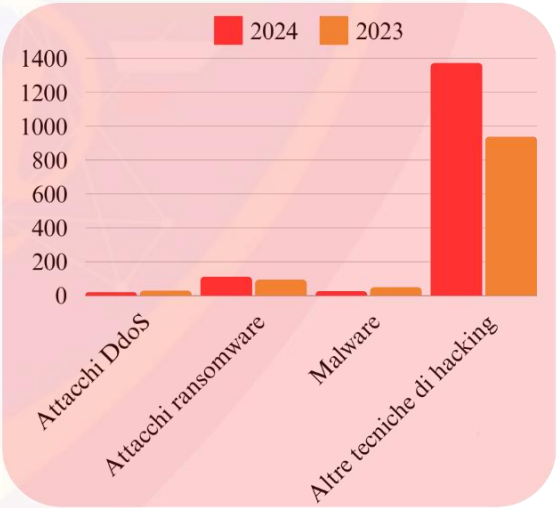
DETTAGLIO ATTACCHI A INFRASTRUTTURE CRITICHE, OPERATORI SERVIZI ESSENZIALI E PUBBLICHE AMMINISTRAZIONI LOCALI

	Attacchi I.C., O.S.E. e P.A.L.	Persone denunciate	Attacchi DdoS	Attacchi ransomware	Malware	Altre tecniche di hacking
Anno 2024	1.533	60	21	112	27	1.373
Anno 2023	1.113	112	30	95	50	938
Var. %	+38%	-46%	-30%	+18%	-46%	+46%

Nel corso del 2024, la Polizia Postale ha rilevato un totale di 1.533 attacchi alle infrastrutture critiche (I.C.), agli operatori di servizi essenziali (O.S.E.) e alle Pubbliche Amministrazioni Locali (P.A.L.), registrando un aumento del 38% rispetto ai 1.113 attacchi documentati nel 2023.

La diminuzione del 46% nel numero delle persone denunciate, che sono passate da 112 a 60, evidenzia le sfide legate al perseguimento dei responsabili di tali crimini. Questo fenomeno è aggravato dalla difficile situazione geopolitica legata ai conflitti bellici russo-ucraino e in Medio Oriente. Gli autori di tali crimini, infatti, operano frequentemente da paesi in cui la cooperazione internazionale giudiziaria e di polizia risulta difficoltosa o impraticabile.

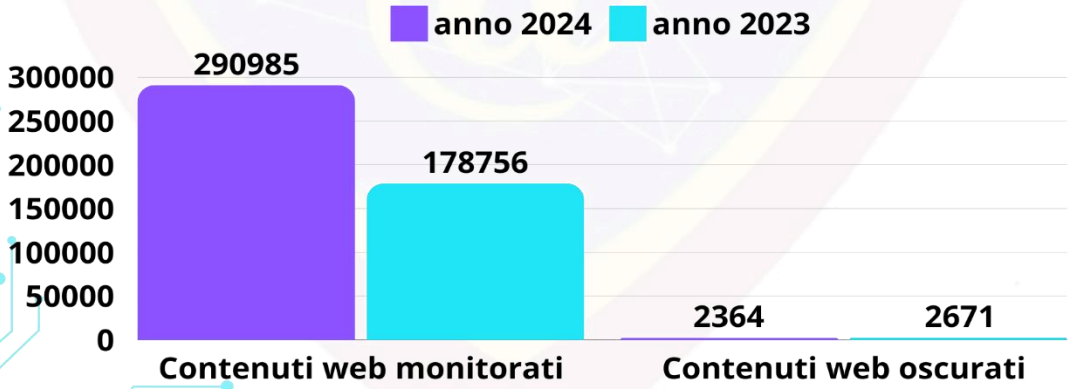
Per quanto riguarda le modalità di attacco, si registra una riduzione del 30% negli attacchi DDoS, mentre gli attacchi ransomware sono aumentati del 18%. Parallelamente, il numero di malware è diminuito del 46%, mentre le altre tecniche di hacking hanno registrato un incremento del 46%.



ATTIVITÀ DI PREVENZIONE ANTITERRORISMO (EVERSIONE INTERNAZIONALE ESTREMISMO RELIGIOSO E POLITICO - EVERSIONE NAZIONALE ESTREMA DESTRA, AREA ANTAGONISTA, ATTIVITÀ IN CIRCOSTANZE DI EMERGENZA)

	Persone indagate	Contenuti web monitorati	Contenuti web oscurati
Anno 2024	59	290.985	2.364
Anno 2023	60	178.756	2.671
Var. %	+0%	+63%	-11%

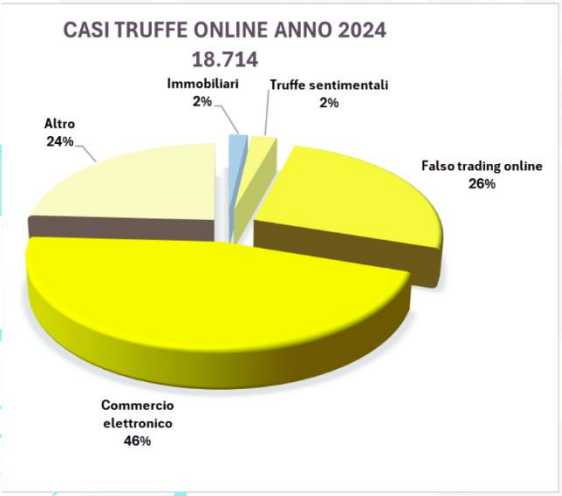
Attività di contrasto al Cyberterrorismo e attività sovversive online. Il grafico illustra l'evoluzione delle attività di contrasto svolte dalla Polizia Postale nel biennio 2023 -2024. Si evidenzia un significativo incremento del +63% nel numero di contenuti web monitorati nel 2024, a fronte di una leggera diminuzione del -11% dei contenuti web oscurati. Il numero di persone indagate è rimasto sostanzialmente stabile

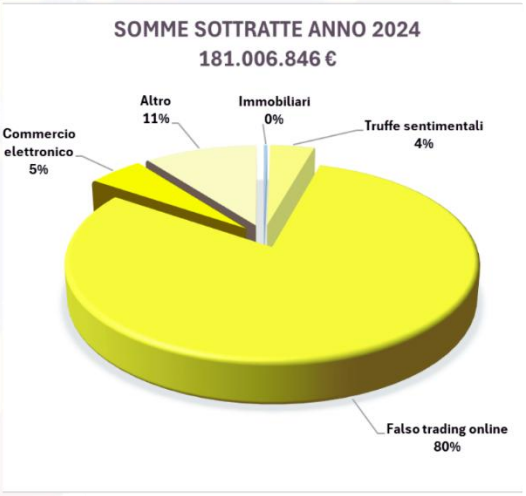


TRUFFE ONLINE

	Casi trattati	Persone indagate	Somme sottratte
Anno 2024	18.714	3.581	€ 181.006.846
Anno 2023	16.325	3.571	€ 137.202.592
Var. %	+15%	+0%	+32%

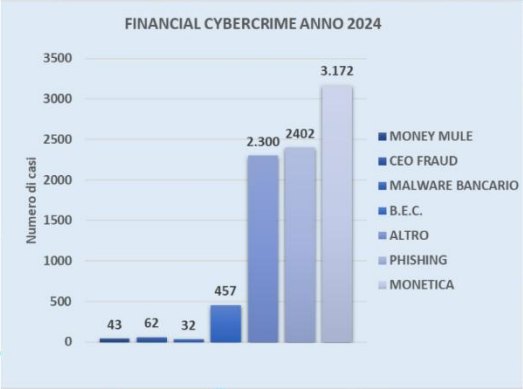
Nel 2024, sono stati trattati 18.714 casi, con un incremento del 15% rispetto ai 16.325 casi del 2023. Il numero di persone indagate è rimasto pressoché invariato, con 3.581 individui nel 2024 rispetto ai 3.571 del 2023. Tuttavia, le somme sottratte hanno subito un notevole aumento del 32%, passando da €137.202.592 nel 2023 a €181.006.846 nel 2024.





	Casi trattati	Persone indagate	Somme sottratte
Anno 2024	8.468	919	€ 48.117.336
Anno 2023	10.606	917	€ 40.151.375
Var. %	-20%	+0%	+20%

La tabella illustra i dati relativi ai casi di frodi informatiche e monetica investigati dalla Polizia Postale negli anni 2023 e 2024. Nel 2024, sono stati trattati 8.468 casi con 919 persone indagate e somme sottratte pari a €48.117.336. Rispetto al 2023, i casi trattati sono diminuiti del 20%, rimanendo stabili nel numero di persone indagate. Le somme sottratte sono aumentate del 20%, evidenziando la crescente sofisticazione delle attività fraudolente online




LEX
SVB LEGE LIBERTAS