

**COMUNICATO STAMPA**

***C3 – Combating Cyber Crime:* prevenzione e contrasto dei crimini informatici. L’impegno della Polizia di Stato nel report 2024 della Polizia Postale e per la Sicurezza Cibernetica[[1]](#footnote-1).**

Tutela della persona e in particolare dei minori dai possibili reati commessi online; tutela del patrimonio di privati, imprese e istituzioni dalla criminalità finanziaria in rete; contrasto al cyberterrorismo; protezione delle infrastrutture critiche informatizzate strategiche per il Sistema Paese.

Sono state molteplici nel 2024 le sfide affrontate dalla Polizia Postale e compendiate nel **report** diffuso nella giornata odierna, che può contare su una rete di 100 uffici territoriali coordinati dal Servizio Polizia Postale e per la Sicurezza Cibernetica, oggi inserito nella nuova Direzione Centrale per la Polizia Scientifica e la Sicurezza Cibernetica del Dipartimento della Pubblica Sicurezza, dedicata all’alta investigazione tecnologica e alle scienze forensi.

Una struttura, quella della Polizia Postale, strategicamente diffusa e in grado di rispondere prontamente alle istanze di sicurezza dei cittadini, sempre più proiettate nel dominio cibernetico, anche attraverso l’azione dei suoi Centri: il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC), presidio di sicurezza per le pubbliche amministrazioni e le imprese strategiche del Paese, in un unico grande “sistema” di pubblica sicurezza cyber; il Centro Nazionale per il Contrasto alla Pedopornografia Online (CNCPO), in prima linea nella lotta contro lo sfruttamento sessuale dei minori sulla rete; il Commissariato di PS online, sito ufficiale della Polizia Postale e strumento di diretto contatto con i cittadini, ai quali vengono fornite informazioni, approfondimenti e aiuto, nelle situazioni più delicate.

**\*\*\***

**CENTRO NAZIONALE PER IL CONTRASTO ALLA PEDOPORNOGRAFIA ONLINE**

I dati del 2024 relativi alle attività del Centro Nazionale per il Contrasto alla Pedopornografia Online (CNCPO) mostrano un aumento complessivo di casi trattati e di operazioni di contrasto, con un maggior numero di persone arrestate e di perquisizioni effettuate. Il Centro ha coordinato oltre 2.800 indagini, con circa 1.000 perquisizioni, 144 arresti e 1.028 denunce. Molte di queste indagini hanno riguardato la detenzione, lo scambio e la produzione di materiale pedopornografico, oltre all'adescamento online di minori.

L'attività di monitoraggio della rete ha portato all'analisi di oltre 42.000 siti web, di cui 2.775 inseriti nella *black list* per contenuti pedopornografici.

Con riferimento al cyberbullismo, rispetto al 2023 si è registrato un lieve aumento dei casi, oltre 300. L’analisi dei dati ha consentito di osservare come la fascia d’età più colpita sia quella 14-17 anni, sebbene gli incrementi più significativi siano legati alle fasce d’età 0-9 e 10-13 anni.

Estorsioni sessuali in rete e diffusione non autorizzata di immagini o video intimi hanno colpito vittime anche minorenni; l’analisi dei dati evidenzia che dal 2023 al 2024, i primi sono in diminuzione e i secondi in aumento.

**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, e particolare attenzione è stata dedicata a tutte quelle forme di aggressione previste dal “*codice rosso*”. In generale, i reati contro la persona perpetrati attraverso la rete sono in aumento. Tra questi, 1500 casi di sextortion – le cui vittime maggiorenni sono state principalmente uomini – e 264 casi di diffusione non consensuale di immagini o video intimi, prevalentemente nei confronti di donne *–* che hanno portato alla denuncia di oltre 200 persone.

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

Nel 2024 l’azione della Polizia Postale svolta dal **Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (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 nella gestione dei grandi eventi – tra tutti, per il 2024, il Vertice del G7 svoltosi in Puglia dal 13 al 15 giugno – e l’attività di contrasto, con rilevanti attività d’indagine concluse nell’anno.

Il Centro nel 2024 ha gestito circa 12.000 attacchi informatici significativi, diramando oltre 59.000 *alert* per prevenire e contrastare attacchi ai sistemi informatizzati di interesse nazionale. Quale punto di contatto nazionale e internazionale per il monitoraggio e la gestione degli eventi di sicurezza cibernetica, il CNAIPIC ha gestito 63 richieste di cooperazione internazionale, consentendo l’identificazione e il deferimento di circa 180 persone.

Le metodologie criminali confermano un’elevata incidenza di attacchi *ransomware* e di DDoS 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, a una matrice puramente criminale, un’origine riconducibile all’operare di attori *state-sponsored*, anche in conseguenza del contesto geopolitico internazionale.

**CYBERTERRORISMO**

Con riferimento al contrasto al **cyberterrorismo**, il costante monitoraggio della rete risulta essenziale per la precoce individuazione di minacce e per la corretta gestione dell’ordine e la sicurezza pubblica. In tale ambito, la Polizia Postale opera in costante raccordo con gli uffici specialistici della Polizia di Stato per prevenire fenomeni di radicalizzazione sul web e garantire quindi una completa analisi della minaccia estremista. Nel 2024 sono stati monitorati oltre 290.000 siti web, dei quali 2.364 oscurati.

**FINANCIAL CYBERCRIME**

Le esperienze di contrasto ai fenomeni del **crimine finanziario *online*** hanno fatto registrare una persistente diffusione di condotte truffaldine che hanno portato, nel quadro del generale rinnovamento della struttura organizzativa del Servizio Polizia Postale, all’istituzione di una Divisione operativa dedicata.

I principali fenomeni criminosi osservati riguardano campagne di *phishing* (anche nelle varianti del c.d. “*vishing*” e del c.d. “*smishing*”)[[2]](#footnote-2) in danno di persone fisiche, PMI e grandi società e le frodi basate sulle tecniche di *social engineering*, con particolare riferimento alla c.d. *BEC* *fraud*,[[3]](#footnote-3) facilitata anche dall’aumento delle comunicazioni commerciali a distanza e dall’uso della rete nelle transazioni commerciali. In forte espansione il fenomeno delle truffe attuate tramite proposte di investimenti di capitali online (falso *trading online*).

Nel contesto investigativo, elemento di interesse è costituito dal sempre più frequente ricorso alle “criptovalute”[[4]](#footnote-4), 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.

**COMMISSARIATO DI P.S. ONLINE E CAMPAGNE DI PREVENZIONE**

Nel contesto della crescente digitalizzazione della 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, infatti, 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 favorendo comportamenti sicuri online. Il sito web ha ricevuto quest’anno circa 3.000.000 di visite, oltre 82.000 segnalazioni e 23.000 richieste di assistenza, riguardanti fenomeni come truffe online, *spoofing*, *smishing* ed estorsioni a sfondo sessuale.

Accanto alle attività di contrasto nei settori di specifica competenza, la Polizia Postale è impegnata in attività di **sensibilizzazione e prevenzione**, considerate 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 la Fondazione Geronimo Stilton dedicato proprio ai più piccoli, viene portata avanti la collaborazione con scuole e comunità per educare i giovani sui pericoli della rete e promuovere comportamenti sicuri online. Allo stesso modo, ulteriori iniziative sono state intraprese su tutto il territorio per la prevenzione delle più comuni tipologie di reati online, attraverso la diffusione di brevi clip con la collaborazione di numerosi stakeholder, tra cui aziende di trasporto pubblico locale, aeroporti, autostrade, stazioni ferroviarie.

**L’ATTIVITÀ DELLA POLIZIA POSTALE IN LOMBARDIA**

Il bilancio dell’attività svolta nel 2024 dal Centro Operativo per la Sicurezza Cibernetica di Milano e dalle 8 Sezioni Operative provinciali (presenti a Bergamo, Brescia, Como, Cremona, Mantova, Pavia, Sondrio e Varese) restituisce un crescente impegno della Polizia di Stato nella prevenzione e nel contrasto del crimine informatico, evidenziando evoluzioni significative rispetto al 2023.

**Reati in ambito postale**. Nel 2024, i reati che colpiscono l’attività del *servizio postale universale* garantito da Poste Italiane hanno registrato una significativa flessione, passando da 46 casi nel 2023 a 30. In particolare, i furti di corrispondenza presso i centri di smistamento di lettere e pacchi si sono ridotti (16 rispetto ai 21 del 2023), mentre le frodi commesse agli sportelli hanno mostrato un calo ancora più netto, passando da 18 a soli 5 casi. In controtendenza il dato relativo ai furti registrati presso gli uffici postali, che sono passati da 4 a 6. In questo ambito investigativo si è assistito a un incremento delle persone denunciate, passate da 2 a 16, a conferma dell’efficacia e dell’incisività dell’azione investigativa della Polizia di Stato. Particolare attenzione è stata riservata, nel corso dell’anno, al controllo del territorio - mediante pattuglie automontate - nei pressi degli uffici postali lombardi, in particolare nei giorni dedicati al pagamento delle pensioni, al fine di scongiurare la consumazione di reati predatori in danno degli stessi uffici e degli utenti.

**Reati contro i minori**. L’impegno nella tutela dei minori rimane una priorità assoluta della Polizia Postale. Nel 2024 i reati legati alla pedopornografia - come la detenzione e la diffusione di materiale pornografico realizzato attraverso lo sfruttamento di minorenni - sono aumentati rispettivamente del 5% e del 17%. Sono inoltre cresciuti i casi di istigazione a pratiche di pedofilia, passati da 1 a 4. Parallelamente, i reati di adescamento online hanno registrato un calo significativo (-16%), con una particolare riduzione negli ambienti online dei social network e delle piattaforme di gaming. Merita tuttavia una particolare attenzione il dato relativo alla produzione di materiale pedopornografico, che nel 2024 ha raggiunto i 12 casi partendo dallo zero l’anno precedente. Particolarmente incoraggiante è invece il sensibile calo (-26%) dei casi di cyberbullismo, scesi a 27 contro i 41 del 2023. Per quanto riguarda l’attività di indagine e di contrasto, il bilancio del 2024 appare decisamente positivo: sostanzialmente stabile il numero dei soggetti arrestati (31 nel 2023 e 30 nel 2024), mentre il numero delle persone denunciate a piede libero sale da 160 a 179. Tra le principali operazioni di polizia giudiziaria svolte in tale settore nel corso del 2024 si segnalano l’Operazione “Bittersweet” (14 perquisizioni nel milanese e 3 soggetti arrestati nella flagranza del reato di detenzione di materiale pornografico realizzato attraverso lo sfruttamento di minorenni al termine di un’indagine partita dall’analisi di segnalazioni giunte da organi di polizia esteri), l’Operazione “Ontario 3” (21 perquisizioni nelle province lombarde di Como, Lodi, Monza Brianza, Milano, Pavia e Varese, con l’arresto in flagranza di reato di 4 persone per detenzione di materiale pedopornografico e di un soggetto che, per anni, ha commesso abusi sessuali ai danni di due bambine in età preadolescenziale - a lui legate da vincolo di parentela - e di una loro amichetta). Si segnala inoltre un’attività svolta dal C.O.S.C. di Milano in collaborazione con la Sezione Operativa per la Sicurezza Cibernetica di Bergamo, che ha portato all’arresto di un sessantenne bergamasco colto nella flagranza del reato di detenzione di materiale pornografico realizzato attraverso lo sfruttamento di minorenni. Partita dall’analisi di una serie di segnalazioni internazionali relative al caricamento di file pedopornografici su due popolari piattaforme cloud, l’indagine ha richiesto una complessa e laboriosa analisi delle connessioni internet utilizzate a tale scopo, al termine della quale è stato possibile risalire al sessantenne bergamasco. A seguito dei successivi approfondimenti investigativi sono stati individuati oltre 1000 file di natura pedopornografica, che vedevano coinvolti bambine e bambini, anche in tenerissima età.

**Reati contro la persona (maggiorenni)**. Il 2024 ha visto una riduzione complessiva (-15%) di questa casistica criminale, con un totale di 261 casi rispetto ai 306 del 2023. Oltre alle querele per stalking (passate da 27 a 22), sono diminuite anche quelle per minacce e molestie attraverso social network e app di messaggistica. In controtendenza il dato relativo alle diffamazioni online, passate da 172 a 184 casi. Perfettamente stabile il fenomeno del cosiddetto “revenge porn” (35 casi in entrambi gli anni), mentre i casi di estorsione sessuale (c.d. “sextortion”) sono calati del 27% (159 rispetto ai 217 del 2023). Anche le sostituzioni di persona sono leggermente diminuite, passando da 255 a 242. I casi di “hate speech” fanno invece registrare un lieve incremento, in particolare per episodi di antisemitismo e discriminazione. Per quanto riguarda l’attività investigativa, a fronte di un calo degli arrestati (nessuno nel 2024 contro i 2 del 2023), si è registrato un netto incremento delle persone scoperte e identificate, che passano da 63 a 96 (+52%).

**Prevenzione e contrasto del terrorismo e dell’eversione**. Nell’ambito della prevenzione e del contrasto della diffusione dei contenuti terroristici online, la Polizia Postale lombarda ha effettuato, nel corso del 2024, un costante monitoraggio della Rete, nonché attività investigative finalizzate all’individuazione di contenuti illeciti. In particolare, sono state monitorate numerose piattaforme di comunicazione online, social network e app di messaggistica istantanea, individuando contenuti propagandistici riconducibili al terrorismo di matrice islamista e a formazioni di estrema destra e di estrema sinistra. Complessivamente, i siti monitorati sono passati dagli 8026 del 2023 ai 41259 del 2024. Nel corso dell’anno appena trascorso il C.O.S.C. di Milano e la Sezione Operativa di Brescia hanno intensificato la propria attività con 22 casi trattati (a fronte dei 12 del 2023). Di questi, 6 riguardano il fondamentalismo religioso di matrice islamica. Particolarmente feconda è risultata l’attività di contrasto dell’eversione politica di estrema destra, sfociata nell’operazione “Genus Album” nel mese di dicembre, con 12 perquisizioni eseguite in tutta Italia nei confronti di altrettanti soggetti - di cui uno ancora minorenne - responsabili di condotte di propaganda e istituzione a delinquere per motivi di discriminazione razziale, etnica e religiosa.

**Computer Crime**. Per quanto riguarda gli attacchi hacker a infrastrutture critiche, aziende e privati, osservando il dato numerico relativo ai casi trattati si assiste a un calo complessivo del 22% (1232 rispetto ai 1572 del 2023). Gli attacchi di tipo “ransomware” contro le infrastrutture critiche, ad esempio, sono diminuiti del 40%, confermando l’efficacia delle contromisure adottate grazie al costante dialogo tra istituzioni, aziende ed autorità preposte alla prevenzione e al contrasto di tali insidiosi fenomeni criminali (dialogo favorito anche da specifici Protocolli di Intesa, come ad esempio quello stipulato lo scorso luglio con l’A.N.C.I. Lombardia). A fronte di una diminuzione del numero di casi, tuttavia, si registra un continuo affinamento delle tecniche di attacco utilizzate dagli hacker, ragion per cui l’impegno della Polizia di Stato nel combattere il computer crime è sempre ai massimi livelli. Tale impegno è culminato in tre rilevanti operazioni di polizia: Operazione “TrustApp” (9 indagati in Italia e 5 in portogallo per frodi informatiche in operazioni di compravendita di criptovalute e connesse condotte di riciclaggio, con perquisizioni eseguite in Lombardia, Lazio, Piemonte e Sardegna); Operazione “Energy Switch” (32 indagati in Italia e 3 in Albania - appartenenti a vario titolo a due società energetiche e a 12 call center - per associazione a delinquere finalizzata al compimento di frodi nella fornitura di gas ed energia elettrica); Operazione “Elicious” (3 soggetti indagati e 1 arrestato in Francia, appartenenti a un’organizzazione criminale dedita ad attacchi informatici di tipo “ransomware”, con infezione dei dispositivi delle vittime, cifratura dei dati in essi contenuti e richiesta di riscatto in criptovaluta).

**Financial cybercrime**. Nel 2024 le frodi informatiche hanno subito una contrazione del 21%, con 564 casi rispetto ai 713 del 2023. Tuttavia, gli importi persi sono aumentati del 30%, passando da 7,4 milioni di euro a 9,6 milioni, a dimostrazione della continua evoluzione delle tecniche criminali. Tra le tipologie in crescita spiccano (+62%) le cosiddette “CEO fraud”, ovvero frodi in cui il truffatore, spacciandosi per l’Amministratore Delegato o comunque un alto dirigente di un’azienda, si mette in contatto con un dipendente della medesima e lo convince, attraverso argomentazioni credibili, a disporre bonifici di importi elevatissimi verso conti correnti esteri riferibili all’organizzazione criminale. Per quanto riguarda invece le altre tipologie di truffa, se rispetto al 2023 l’aumento dei casi risulta essere lieve (+3,3%), le somme di denaro sottratte alle vittime hanno fatto registrare un aumento vertiginoso nel 2024, passando da 2,6 a 32,7 milioni di euro (+1158%). A pesare in maniera particolarmente significativa su questo bilancio sono le truffe relative al finto trading online e ad altre simili forme di investimento. Si tratta di fenomeni che rappresentano il 48% - quindi quasi la metà - del totale delle truffe online registrate in Lombardia nel corso del 2024 e rispetto ai quali è essenziale promuovere la prevenzione attraverso una costante attività di informazione e sensibilizzazione rivolta ai cittadini, specie quelli più vulnerabili e indifesi. Sul piano dell’attività investigativa condotta dal C.O.S.C. Lombardia in tale settore, nel 2024 sono state portate a termine numerose operazioni di polizia giudiziaria. Tra quelle più significative, si segnalano l’Operazione “Polo Est” (12 perquisizioni nei confronti di un cittadino italiano, un senegalese e 10 nigeriani, responsabili di estorsione nei confronti di un cittadino italiano residente in Cina il quale, ritenendo autentica un’e-mail recante il logo della Polizia Postale e la firma di un funzionario di polizia realmente esistente, è stato indotto a versare ai criminali la somma di 117500 euro dietro la minaccia di un finto procedimento penale per reati di pornografia minorile), l’Operazione “Nessie” (5 perquisizioni nei confronti di altrettanti dipendenti di Poste italiane che avevano fornito a una banda criminale informazioni sensibili su ignari correntisti postali, indispensabili per l’attivazione di 105 carte di credito sottratte da un centro di smistamento di corrispondenza prima che venissero recapitate ai legittimi intestatari) e l’Operazione “Portorico” (18 perquisizioni e sequestri di materiale informatico nelle province di Caserta, Napoli, Salerno e Livorno nei confronti dei membri di un’organizzazione criminale dedita ad attività di phishing e smishing su scala nazionale).

**Attività di prevenzione e sensibilizzazione**. Accanto all’attività investigativa e di repressione dei reati informatici, nel corso del 2024 la Polizia Postale lombarda ha svolto un’importante azione preventiva a tutela delle fasce più vulnerabili della popolazione - e in particolare dei minori - contro il cyberbullismo e tutte le forme di prevaricazione online, fenomeni che destano un particolare allarme sociale. Oltre ad eventi, conferenze e incontri nelle scuole e nei centri di aggregazione giovanile, sono stati organizzati anche momenti di incontro e riflessione con gli adulti, al fine di accrescere la consapevolezza dei cittadini rispetto ai rischi della rete e di suggerire idonee misure di autodifesa dalle più insidiose forme di truffe online. Infine, un’attenzione particolare è stata rivolta alle donne, sempre più spesso vittime di reati online quasi interamente “al femminile”, come il cyberstalking, il “revenge porn” e le “truffe sentimentali”. In tutti questi casi il silenzio è il peggiore dei nemici e l’invito della Polizia di Stato è quello di denunciare sempre, superando imbarazzo e vergogna. Complessivamente, gli eventi di sensibilizzazione organizzati nel 2024 - sia in presenza che in videoconferenza - hanno coinvolto ben 138512 persone, a fronte delle 7003 del 2023.

Roma, 3 gennaio 2025

1. Dati rilevati al 21 dicembre 2024. [↑](#footnote-ref-1)
2. 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. [↑](#footnote-ref-2)
3. Frode realizzata attraverso la compromissione di caselle di posta elettronica, realizzata allo scopo di acquisire informazioni utili al perfezionamento della condotta illecita. [↑](#footnote-ref-3)
4. Utilizzate come strumento per perfezionare l’efficace riciclaggio dei proventi illeciti. [↑](#footnote-ref-4)