Resoconto attività Polizia Postale e delle Comunicazioni Anno 2021

Nel 2021, la Polizia Postale e delle Comunicazioni è stata impegnata nel far fronte a continue sfide investigative con riferimento alle macro-aree di competenza, in particolare negli ambiti della prevenzione e contrasto alla pedopornografia online, della protezione delle infrastrutture critiche di rilevanza nazionale, del financial cybercrime e di quelle relative alle minacce eversivo-terroristiche in rete, riconducibili sia a forme di fondamentalismo religioso che a forme di estremismo politico ideologico, anche in contesti internazionali.

Il Centro Nazionale per il Contrasto della Pedopornografia Online, C.N.C.P.O., ha coordinato 5.515 complesse attività di indagine (+ 70% rispetto all'anno precedente) all'esito delle quali sono state eseguite oltre 1.400perquisizioni (+ 87% rispetto all'anno precedente).
Nel corso del 2021 si è verificato, infatti, un significativo incremento dei casi di sfruttamento sessuale dei minori e di adescamento online: eseguiti 137 arresti(+98% circa rispetto al 2020) e denunciate 1400 persone(+17% rispetto al 2020).
L' incremento sale al +127% per le persone arrestate e del +295% rispetto ai casi trattati, se confrontiamo i dati prepandemici del 2019
Pe quanto attiene l'attività di prevenzione sono stati analizzati oltre 29.000 siti internet, 2.539 dei quali, riscontratone il carattere pedopornografico, sono stati oscurati mediante inserimento nella black list istituita ai sensi della L.38/2006.

Tra le indagini più significative condotte direttamente dal **C.N.C.P.O.,** si segnala una delicata attività svolta

nell’ambito delle **darknet**, che ha consentito di trarre in arresto un libero professionista 50enne, produttore di materiale di pornografia minorile. L’operazione è stata condotta con la cooperazione internazionale di polizia con altre Agenzie investigative estere attivata da Europol. L’uomo abusava in via continuativa di due minori di 6 e 8 anni. Avvalendosi delle sue capacità manipolatorie, era riuscito a carpire l’affetto e la totale fiducia dei bambini e, in soli due anni, ha filmato le violenze ai loro danni per un totale di circa **9.000 video**. In virtù della fiducia in lui riposta da parenti e amici, riusciva a ottenere la disponibilità dei minori anche per diversi giorni.

Il Compartimento Polizia Postale per il Lazio, in tale ambito, nell’anno 2021, ha trattato oltre 588 casi e sono state avviate numerose indagini, che hanno portato all’esecuzione di 110 perquisizioni, all’arresto di 7 persone ed alla denuncia in stato di libertà di 116 soggetti indagati a vario titolo per i reati di adescamento di minori e di detenzione e diffusione di materiale pedopornografico; procedendo contestualmente al sequestro di oltre 19.095 gigabyte di contenuti multimediali di tale illecita natura.

Nel corso di tale attività sono stati inoltre visionati 16.341 spazi virtuali.

Tra le indagini più significative avviate dal Compartimento Polizia Postale per il Lazio si segnala:

- A seguito dell’attività investigativa scaturita da una segnalazione veniva individuato un soggetto resosi responsabile del caricamento di alcuni file pedopornografici sulla piattaforma TUMBLR. L’identificazione del responsabile è stata ostacolata dal tentativo dell’utente di coprire le tracce delle connessioni sfruttando le reti wi-fi di utenze fisse non direttamente riconducibili a lui. A seguito di emissione da parte della Procura della Repubblica presso il

Tribunale di Roma di decreto di perquisizione, durante l'esecuzione dell'attività di perquisizione informatica sul materiale rinvenuto, il soggetto veniva trovato in possesso di un ingente quantitativo di materiale pedopornografico, pertanto veniva tratto in arresto e sottoposto al regime degli arresti domiciliari.

- A seguito di analisi forense su una micro SD rinvenuta casualmente da un privato cittadino, contenente numerosi file pedopornografici e altri file riconducibili al titolare di una ludoteca romana, veniva emesso, da parte della Procura della Repubblica presso il Tribunale di Roma, un decreto di perquisizione a carico dello stesso. Si rappresenta che molte delle fotografie rinvenute all'interno della micro SD ritraevano i minori all'interno dei locali della ludoteca e che nelle immagini venivano spesso ritratti i piedi dei minori. L'attività di perquisizione dava riscontro positivo in quanto il soggetto veniva trovato in possesso di circa 500 file immagine e 4.000 file video a carattere pedopornografico, pertanto veniva tratto in arresto per detenzione di ingente quantitativo di materiale pedopornografico e, come disposto dal P.M. di turno, sottoposto agli arresti domiciliari. La successiva più approfondita analisi dei dispositivi sequestrati consentiva di accertare che il soggetto, anche durante il periodo del lock-down, forniva un servizio di ludoteca da remoto, intrattenendo i minori attraverso la piattaforma Meet e Zoom, attraverso videochiamate dallo stesso registrate, durante le quali organizzava giochi per i minori che prevedevano l'uso dei piedi.

Il soggetto veniva tratto in arresto e sottoposto al regime degli arresti domiciliari.

- A seguito di alcune segnalazioni provenienti sia dalla FIU (Financial Intelligence Unit) che dalla Banca di Italia, relative ad alcune transazioni finanziarie

sospette, con le quali presumibilmente era stato acquistato materiale pedopornografico in live streaming, veniva individuato tra gli acquirenti un dipendente del Comune di Latina, affetto da tetraparesi spastica. L'attività di perquisizione informatica dava riscontro positivo in quanto il soggetto veniva trovato in possesso di numerosissimi file video a carattere pedopornografico, alcuni particolarmente raccapriccianti, per un totale di 109 ore di visione, pertanto veniva tratto in arresto per detenzione di ingente quantitativo di materiale pedopornografico e, come disposto dal P.M. di turno, in considerazione anche della sua disabilità, sottoposto agli arresti domiciliari. La successiva più approfondita analisi dei dispositivi sequestrati consentiva di accertare che il soggetto non si limitava a scaricare materiale reperibile in rete, ma attraverso l'applicativo Skype lo stesso effettuava videochiamate con soggetti che avevano la disponibilità di minori e dopo aver pattuito il prezzo e inviato il pagamento attraverso un servizio di money transfert, dava indicazioni all'interlocutore su quali atti sessuali compiere sui minori, assumendo lui stesso il ruolo di regista dei video a lui dedicati in via esclusiva, acquistati per pochi euro. Il soggetto veniva tratto in arresto e sottoposto al regime degli arresti domiciliari.

- A seguito dell'attività investigativa scaturita da segnalazione, veniva individuato un soggetto resosi responsabile del caricamento di un'unica immagine pedopornografica "uploadata" sulla piattaforma Skype. Durante l'esecuzione dell'attività di perquisizione informatica, oltre all'ingente quantitativo di materiale pedopornografico che consentiva l'arresto del soggetto, veniva rinvenuta una chat Telegram denominata "Famiglie da Abusi" costituita da una ristretta cerchia di utenti, nella quale i partecipanti, oltre a scambiarsi materiale pedopornografico, condividevano episodi di atti sessuali

compiuti o da compiere con i propri figli minori. Dall'accurata analisi sui dispostivi in uso al predetto, anche con l'ausilio del Compartimento di Bologna coinvolto nelle attività investigative, venivano identificati tutti i partecipanti al gruppo, nonché altri due soggetti, con i quali lo stesso intratteneva conversazioni relative agli abusi compiuti o da compiere con le rispettive figlie attraverso gli applicativi Whatsapp e Facebook. Nel corso dell'attività di perquisizione, eseguita da personale di quest'Ufficio, sul territorio di competenza della Sezione di Messina, ove risiedeva uno dei due soggetti citati, venivano repertati utili elementi di prova, ovvero indumenti in uso alla figlia e ricognizione fotografica degli ambienti domestici, che consentivano attraverso la comparazione con il materiale pedopornografico condiviso, di accertare l'autoproduzione dello stesso e gli abusi subiti dalla figlia di anni 7, per i quali, come disposto dalla locale Procura, il predetto veniva sottoposto alla misura cautelare della custodia in carcere, mentre la di lui compagna veniva colpita dalla misura dell'obbligo di allontanamento dalla casa familiare e del divieto di avvicinamento alla persona offesa.

- A seguito dell'attività investigativa scaturita da segnalazione veniva individuato un soggetto resosi responsabile del caricamento di alcuni file pedopornografici sulla piattaforma KIK. Durante l'esecuzione dell'attività di perquisizione informatica, il soggetto veniva trovato in possesso di un ingente quantitativo di materiale pedopornografico, che lo stesso condivideva con numerosi utenti attraverso l'applicazione Telegram, pertanto veniva tratto in arresto e, come disposto dal P.M. di turno, sottoposto agli arresti domiciliari.
- A seguito di denuncia sporta presso i nostri uffici dalla madre di una minore adescata via social, veniva

emesso decreto di perquisizione a carico di un dipendente di una ditta di onoranze funebri. Dopo l'accurata analisi sui dispostivi sequestrati nel corso dell'attività di perquisizione, veniva rinvenuta oltre la chat di interesse, anche quella con un ulteriore soggetto minore. Accertato il modus operandi del soggetto che fingendosi un adolescente convinceva le minori a produrre video pedopornografici, veniva emessa ed eseguita a suo carico un'ordinanza di custodia cautelare in regime degli arresti domiciliari.

- A seguito della ricezione del decreto di perquisizione emesso dalla A.G. capitolina il personale della Sezione di Latina ha eseguito le attività delegate compiendo contestualmente anche la perquisizione informatica all'esito della quale è stata accertata la detenzione 463 filmati di natura pedopornografica per una durata totale di circa 43 ore di visione. La peculiarità delle evidenze individuate consiste proprio nella tenera età dei soggetti coinvolti che si è ragionevolmente individuata in circa 3 anni, costretti a subire rapporti sessuali con soggetti palesemente adulti. Il soggetto veniva tratto in arresto e sottoposto agli arresti domiciliari.

Nell'ambito dei reati contro la persona commessi attraverso la rete, i dati nazionali mostrano un significativo aumento dei fenomeni di ***sextortion (+54% rispetto al 2020)*** e ***revenge porn*** (***+78% rispetto al 2020)*** con oltre **500** casi trattati e **190 autori di reato deferiti all'A.G.**

Nel complesso per reati contro la persona commessi sul web, sono stati denunciati oltre **1.400** soggetti.

Il Compartimento Polizia Postale e delle Comunicazioni per il Lazio, nell'ambito dei reati contro la persona, nell'anno 2021, ha trattato più di 800 casi, monitorando oltre 9000 spazi virtuali. L'attività investigativa in questo settore ha portato alla denuncia di 216 persone per aver commesso reati

annoverati nella legge 19 luglio 2019 n. 69, cosiddetto “Codice Rosso”, estorsioni a sfondo sessuale, molestie, minacce, diffamazioni sui social network ed all’esecuzione e sono state 107 perquisizioni locali.

Una particolare rilevanza ha assunto l’attività di contrasto ai reati sanciti dall’art. 612 c.p.; nell’anno in cui ha preso il via il vaccino anti Covid-19 e la propaganda negazionista no-vax, si è visto un maggior incremento del reato inerente le minacce perpetrate via web ai danni di politici, personaggi di spicco mediatico e di rilievo istituzionale.

Dal mese di Gennaio ad oggi sono stati trattati oltre 40 casi e più di 15 sono state le persone indagate per reati connessi alla “campagna no-vax”.

Un impegno costante profuso anche con un’ampia attività di prevenzione e contrasto dei reati d’incitamento all’odio, con analisi ed il monitoraggio di migliaia di spazi virtuali nel corso 2021. Di particolare rilievo è l’Ammonimento del Questore previsto dal D.L. 93/2013, nel caso in cui non sia stata sporta querela e non siano stati perpetrati reati procedibili d’Ufficio, per il fenomeno dello stalking e del cyberbullismo, Nel 2021 sono state rivolte alle rispettive Questure, quali autorità locali di P.S. di Pubblica Sicurezza, 16 istanze di ammonimento nei confronti degli autori delle condotte moleste.

Tra le attività di polizia giudiziaria condotte in questo settore, si segnalano alcune di particolare rilievo:

- A seguito della ricezione della delega di indagine emessa dalla autorità giudiziaria il personale della Sezione di Latina ha svolto una intensa attività di indagine che ha permesso di individuare ben 9 soggetti che attraverso l’uso dei social, hanno posto in essere gravi affermazioni diffamatorie nei confronti di un noto

giornalista di “La Repubblica”.

- Importante attività di polizia giudiziaria è scaturita da una segnalazione della Direzione Centrale della Polizia Criminale – Servizio per la Cooperazione Internazionale di Polizia -, nella quale il Collaterale Ufficio di Polizia tedesco informava che la locale Autorità Giudiziaria aveva avuto notizia della presenza, nel *Dark Web,* di conversazioni inerenti un omicidio su commissione da effettuarsi a Roma. Individuata la parte offesa ed il responsabile ed è stata eseguita la misura della custodia cautelare in carcere unitamente alla Squadra Mobile di Roma;

Per quanto riguarda il settore della **cybersicurezza** ed in particolare la protezione delle Infrastrutture Critiche, nell’ambito delle attività di prevenzione e contrasto ad attacchi e minacce aventi per obiettivo le infrastrutture sensibili di interesse nazionale (pubbliche e private), il **C.N.A.I.P.I.C.** – nell’ambito del complessivo **Sistema Informativo Nazionale per il Contrasto al Cyber Crime**[1], ha gestito:

- **434** attacchi informatici significativi nei confronti di servizi informatici relativi a sistemi istituzionali, infrastrutture critiche informatizzate di interesse nazionale, infrastrutture sensibili di interesse regionale, grandi imprese;
- ha diramato**524***alert* di sicurezza riferibili a minacce per sistemi informatici/telematici oggetto di tutela del Centro;
- ha ricevuto **60** richieste di cooperazione, gestite dall’Ufficio del punto di contatto *HTC Emergency* presente all’interno del CNAIPIC nell’ambito della Rete 24-7 “High Tech Crime” del G7.

Le attività investigative avviate dal Centro e dai Compartimenti, hanno portato al deferimentodi complessive **187**

persone per accesso abusivo e danneggiamento di sistemi informatici afferenti sistemi critici ovvero servizi essenziali,diffusione di *mallware,* trattamento illecito di dati su larga scala.

L'azione della Polizia Postale si è diretta alla prevenzione e contrasto alle violazioni dei sistemi informatici critici e in maniera massiva alla lotta alle falsificazioni e commercializzazioni di certificati Green Pass illegali, sia sul clear che sul dark web.

L'azione della Polizia Postale si è diretta, ad ampio spettro:

1. al contrasto ai fenomeni di sottrazione illecita, dai sistemi critici, di interi archivi contenenti centinaia di green pass appartenenti a cittadini italiani, certificati che venivano rivenduti o addirittura posti a disposizione del pubblico su piattaforme di file-sharing per lo scaricamento gratuito, al fine di un successivo utilizzo illecito da parte degli acquirenti;
2. al contrasto ai fenomeni di truffa, basati sulla pubblicazione, su darkweb e canali social, di annunci fraudolenti in cui sedicenti falsari, al solo scopo di adescare le proprie vittime convincendole a rivelare i propri dati personali e a disporre pagamenti anticipati, si dichiarano in grado di fabbricare falsi green pass.
3. Al contrasto ai fenomeni di intrusione informatica nei sistemi sanitari regionali, allo scopo di poter inserire dati relativi a vaccinazioni e tamponi mai eseguiti, finalizzati ad ottenere il rilascio di certificati green pass.

Risale infatti a pochi giorni fa la messa a segno da parte della polizia postale di una vasta operazione – la più avanzata sinora realizzata nel settore – relativa alla messa in commercio di certificazioni **green pass**radicalmente false, ma in grado di resistere anche ai controlli possibili mediante l'apposita app di verifica, generate mediante furto delle

credenziali dei farmacisti e successivo accesso illegale ai sistemi sanitari regionali di **Campania, Lazio, Puglia, Lombardia, Calabria e Veneto**.

Le credenziali di accesso erano carpite alle farmacie mediante sofisticate tecniche di **phishing,** attraverso email che simulavano la provenienza dal sistema sanitario, e che inducevano le vittime a collegarsi ad un sito web, anch'esso falso, perfettamente identico a quello della sanità regionale, in grado di sottrarre le preziose credenziali.

In altri casi, i falsi green pass risultavano prodotti ricorrendo a servizi di chiamata VoIP internazionali, capaci di camuffare il vero numero di telefono del chiamante e simulare quello del sistema sanitario regionale, attraverso cui gli hacker si spacciavano per agenti del supporto tecnico della Regione interessata ed inducevano il farmacista ad installare nel proprio sistema un insidioso software che consentiva di assumere il controllo da remoto del computer e rubare così le credenziali di accesso ai sistemi informativi regionali.

Le indagini – consistite nell'analisi dei dati di connessione, di tabulati telefonici, delle caselle email e delle altre tracce lasciate dai traffici illeciti – hanno consentito di verificare che le tecniche criminose appena indicate sono state messe in campo anche per produrre i cd. Super green pass, a fronte di vaccini mai effettuati.

120 falsi green pass sono stati sinora localizzati nelle province di Napoli, Avellino,

Benevento, Caserta, Salerno, Bolzano, Como, Grosseto, Messina, Milano, Monza-Brianza, Reggio Calabria, Roma e Trento, ma sono in corso accertamenti finalizzati a definire il numero reale, che si stima essere assai più ampio, di coloro che si sono rivolti nel tempo all'organizzazione criminale oggetto delle indagini per sfruttarne gli illeciti servizi.

Le perquisizioni, operate dai vari Reparti della Polizia Postale e delle Comunicazioni interessati sul territorio nazionale hanno riguardato le 15 persone già sottoposte ad indagini quali ipotetici appartenenti all'associazione criminosa che risulta aver assicurato la regia degli accessi abusivi ai sistemi informatici e delle conseguenti falsificazioni, nonché 67 dei loro clienti. Con la collaborazione del Ministero della Salute, i falsi green pass individuati sono stati disabilitati, in modo da impedirne ogni ulteriore utilizzo

In tema di Attacchi Cyber, protezione delle Infrastrutture Critiche del Paese e analisi di dispositivi informatici il **Compartimento Polizia Postale per il Lazio** ha trattato oltre 582 casi, eseguito 29 perquisizioni anche in collaborazione con altri uffici investigativi e deferito n.6 persone in stato di libertà all'Autorità giudiziaria per il reato di accesso abusivo a sistema informatico, sono state inviate ai referenti già individuati nell'ambito dei protocolli di intesa per il monitoraggio delle infrastrutture critiche di competenza, n. 106 segnalazioni inerenti a più di 1000 eventi di sicurezza informatica relativi a vulnerabilità, violazioni di dati, *malware* o altre attività di minaccia informatica corredati dai relativi IOC (indici di compromissione).

Le indagini, a livello nazionale, riguardanti il fenomeno delle **truffe online in materia di ecommerce** ovvero nell'ambito di piattaforme per l'offerta di beni e servizi, hanno consentito l'individuazione di oltre 3.200 presunti autori deferiti all'A.G..

Nel settore del ***financial cybercrime***, si registrano sull'intero territorio nazionale, per il 2021, ben **126 attacchi informatici ai sistemi finanziari di grandi e medie imprese**, per un ammontare complessivo di oltre **36 milioni di euro sottratti illecitamente** mediante complesse frodi

telematiche, **17 milioni** dei quali recuperati a seguito dell'attivazione tempestiva della Polizia Postale e delle Comunicazioni.

Gli attacchi al mondo dell'impresa, mediante frodi basate su tecniche di social engineering risultano particolarmente condizionati dalla pandemia in corso, soprattutto per l'utilizzo diffuso di sistemi di comunicazione per la gestione economica da remoto, conseguenti all'adozione su larga scala di processi di smart-working.

In merito ai fenomeni di ***phishing, smishing e vishing***, tecniche utilizzate per carpire illecitamente dati personali e bancari, si rileva il sensibile aumento dei casi trattati dalla Specialità **(+27%)** per un totale oltre **18.000 casi trattati** di furto di credenziali per accesso ai sistemi di *home banking*, di numeri di carte di credito, di chiavi private di wallet di cryptovalute a fronte dei quali sono state deferite all'A.G. **781 persone**.

Il Compartimento Polizia Postale e delle Comunicazioni per il Lazio, nell'ambito delle truffe on line e del financial Cybercrime ha trattato 7424 casi, eseguito 48 perquisizioni e monitorati circa 3181 spazi virtuali, principalmente siti di e-commerce e portali che offrono opere dell'ingegno o servizi di investimento.

L'attività investigativa ha portato all'arresto di 2 persone ed all'esecuzione di numerose perquisizioni con il sequestro ed il recupero di ingenti somme di denaro originariamente sottratte ai rispettivi titolari.

Le attività investigative del Compartimento in materia di e-commerce e telefonia, sono riferibili ad una vasta casistica che va dalla falsa vendita *on line* di biglietti per eventi vari (come concerti e partite di calcio), ai falsi annunci di locazione di case vacanza pubblicati in rete internet ed alle false vendite on line di materiale vario, hanno permesso di

indagare 565 soggetti.

Nell'ambito del contrasto al fenomeno del c.d. **cyberterrorismo**, ed in generale **dell'estremismo in rete**, gli investigatori della Polizia Postale e delle Comunicazioni hanno concorso alla prevenzione ed 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 **117.000** spazi web oggetto di approfondimento investigativo.

Tra questi **1.095** sono risultati caratterizzati da contenuti illeciti, che hanno determinato in **471** casi l'oscuramento della risorsa digitale.

Con riferimento alle attività investigative di settore, denunciati **39** soggetti ritenuti responsabili di attività di propaganda *jihadista*, ovvero legati all'estremismo di destra o a movimenti anarchici, mentre nell'ambito dei movimenti afferenti la complessa galassia dei movimenti NO-VAX e NO GREENPASS sono state denunciate**101** persone.

In ambito di collaborazione internazionale, proprio al fine di contrastare la diffusione dal web di contenuti terroristici online legati all'estremismo di destra, lo scorso 27 maggio l'Unità EUIRU di Europol ha promosso un *Referral Action Day* con l'obiettivo di rimuovere dai *Social Network, siti web, blog, forum* etc., materiale *online* riportante loghi di gruppi, manifesti, manuali, tutorial, media file prodotti e disseminati da organizzazioni di estrema destra, ovvero relativo a precedenti attacchi terroristici connotati dalla medesima ideologia.

Nel dettaglio, all'esito dei lavori, ai quali hanno partecipato operatori della Specialità ed operatori di polizia di altri 27 Stati, sono state segnalate **1038 URL** ai Provider al fine di ottenerne l'oscuramento; in particolare, l'Italia ha segnalato **77 URL** tra cui profili social di Facebook, Twitter e VKontacte, nonché una serie di account e canali Telegram.

La grave emergenza socio-sanitaria, tuttora in corso, accompagnata dalle restrizioni introdotte dai decreti governativi per contrastare la diffusione del virus Covid-19, ha infine orientato una specifica attività di monitoraggio informativo dei canali e gruppi all'interno delle varie piattaforme di comunicazione *online,* per l'individuazione precoce di eventi ovvero manifestazioni di piazza non autorizzate.

Diverse le attività concluse che hanno portato al complessivo deferimento di **86 persone per reati quali il falso, la frode informatica**, in un caso con **15 soggetti** protagonisti di una vera e propria associazione a delinquere finalizzata alla produzione di certificazioni false mediante violazione dei sistemi informatici sanitari.

Si segnala che, a seguito dei fatti avvenuti nella Capitale il 9 ottobre u.s., con l'attacco alla sede della **CGIL in Roma** nel corso di una manifestazione NO-VAX/NO GREEN PASS, grazie al monitoraggio effettuato dal **Servizio polizia Postale e dalla DIGOS di Roma**, è stato accertato che attraverso il sito ufficiale di Forza Nuova, venivano diffusi, da parte dei componenti dello Staff e della Redazione del movimento, numerosi comunicati e dichiarazioni volte ad incitare alla violenza contro le Istituzioni e, pertanto, si è proceduto ad informare la competente A.G., che ha ritenuto di emettere un decreto di sequestro preventivo del sito www.forzanuova.eu.

Tale provvedimento è stato eseguito in data 11 ottobre u.s. dal personale della Specialità, tramite la sostituzione della

homepage con un'apposita "stop page".

[1] Si tratta del più ampio progetto SINC3, che prevede collegati in rete il CNAIPIC, a tutela delle infrastrutture critiche nazionali, ed i Nuclei operativi sicurezza cibernetica – NOSC dei Compartimenti, di prossima istituzione con la riorganizzazione dei presidi territoriali della Specialità, quest'ultimi a tutela dei rispettivi asset cibernetici regionali. Il progetto prevede tra l'altro la formazione degli operatori NOSC e la creazione di una piattaforma informatica per la gestione degli eventi e per la condivisione delle informazioni di sicurezza finanziata con fondi ISF, che, oramai avviata la fase sperimentale, potrà essere inaugurata il prossimo anno.

In tale contesto, il **Compartimento Polizia Postale per il Lazio** ha esaminati oltre 3470 spazi virtuali tra siti, profili, canali e gruppi all'interno delle varie piattaforme di comunicazione online nelle quali sono stati pubblicati numerosissimi commenti in cui emergeva la volontà di reagire alle decisioni governative attraverso vere e proprie azioni di piazza, anche violente.

In tema di contrasto all'eversione sono stati trattati oltre 136 casi, effettuate 12 perquisizioni e denunciati 2 soggetti.

Di rilievo anchel'attività sviluppata dagli Uffici di Specialità per la tutela e la sicurezza dei **servizi postali**, nell'ambito della convenzione con il partner Poste Italiane: oltre **6400le pattuglie** impiegate nel corso dell'anno a tutela dei servizi erogati da Poste Italiane per oltre **46.000 controlli**. Attività che hanno portato al deferimento di **229persone (+394% rispetto all'anno precedente)** per c.d. "reati postali[1]".

Il **Compartimento Polizia Postale e delle Comunicazioni per il Lazio,** ha garantito 924 pattuglie sul territorio che hanno

assicurato la vigilanza degli uffici postali della Regione Lazio, con particolare riferimento ai giorni in cui è previsto il pagamento delle pensioni, effettuando oltre 5100 controlli.

Nell'anno in esame, il portale del Commissariato di P.S. *online* si è confermato quale punto di riferimento specializzato per la ricerca di informazioni, consigli, suggerimenti di carattere generale per la sicurezza in rete, rafforzandosi ulteriormente in termini di popolarità con **52.000.000** di accessi.

La struttura operativa che gestisce il portale ha trattato oltre **28.000** richieste di informazioni, ricevuto **114.000** segnalazioni dai cittadini **(+103% rispetto all'anno precedente)**.

Nell'ottica della cennata azione di prevenzione il **Compartimento Polizia Postale per ilLazio** ha trattato oltre 2200 segnalazioni/richieste pervenute via e-mail o centralino, nel cui contesto sono state fornite ai cittadini richiedenti informazioni utili, soprattutto, per prevenire possibili frodi. Di queste, oltre 50 segnalazioni anonime hanno riguardato situazioni di grave minaccia o di pericolo per le persone, oppure richieste di aiuto da parte di persone in evidente stato di disagio emotivo e psicologico che preannunciavano propositi suicidari tramite web, sulle varie piattaforme social e/o via email e sono state risolte con l'identificazione ed il rintraccio del soggetto segnalante, poi avviato alle strutture mediche competenti sul territorio.

Nell'ambito delle campagne di sensibilizzazione e prevenzione sui rischi e pericoli connessi all'utilizzo della rete internet, rivolte soprattutto ai giovani, la Specialità ha promosso la **XIedizione** del progetto "***Una Vita da Social***", campagna itinerante grazie alla quale sino ad oggi sono stati raggiunti oltre **2milioni e 600mila studenti sia nelle piazze che nelle scuole**, **225.000 genitori,132.000 insegnanti** per un

totale di **19.500 Istituti scolastici** e **400** città raggiunti sul territorio nazionale.

Nel corso del ***lockdown***l'attività sul territorio nazionale di sensibilizzazione e prevenzione nelle scuole è proseguita attraverso piattaforme di video conferenze coinvolgendo oltre **371.000 studenti**, più di **5.000 insegnanti**, per un totale di **3.069 Istituti scolastici coinvolti**.

Gli operatori del **Compartimento Polizia Postale e delle Comunicazioni del Lazio** hanno effettuato incontri in 171 Istituti Scolastici della Regione, coinvolgendo 31920 studenti, oltre 1487 docenti e 1384 genitori, trattando argomenti come phishing, hacking, adescamento on line, truffe, furti di identità e cyberbullismo.

Si evidenzia infine per importanza l'attività di progettazione ed alta formazione specialistica finalizzata all'avvio del CERT (*Computer Emergency Response Team*) – del Ministero Interno. Avvalendosi della collaborazione istituzionale con il CI.Fi.Ge (Centro interforze Formazione Intelligence – Stato maggiore della Difesa) è stato sperimentato un prezioso e produttivo scambio formativo per il quale è stata formata la prima aliquota di personale assegnato al Centro per la sicurezza informatica del Dicastero.

L'obiettivo futuro di definizione di un lessico comune e qualificazione di un adeguato profilo di specializzazione di operatore cyber per le esigenze del CERT e del correlato Centro di Valutazione delle infrastrutture informatiche.

Infine, a completamento e per la migliore valorizzazione del percorso evolutivo della Specialità, si sono di recente avviate le progettualità finanziate con fondi PNRR per la realizzazione di 27 laboratori *cyber* sul territorio, la realizzazione di mezzi mobili tattici a supporto delle attività investigative, forensi e per la gestione della

sicurezza informatica in occasione di grandi eventi.

Con gli stessi fondi è allo studio l'ipotesi di finanziare l'infrastruttura informatica del CERT e del dipendente Centro di Valutazione che sarà chiamato a svolgere il delicato compito di valutare i profili di sicurezza degli *asset* delle strutture informatiche che supportano le funzioni essenziali del Ministero dell'Interno (sistemi elettorali, rete Prefetture, AFIS etc.)