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 **1.400 perquisizioni (+ 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.

C.N.C.P.O.	**2020**	**2021**	**Incremento**
Casi trattati	3.243	5.515	+70,06%
Persone indagate	1.192	1.400	+17,15%
Arrestati	69	137	+98,55%
Perquisizioni	757	1416	+87,05%
Gb di materiale sequestrato	215.091	280.106	+30,23%

*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.*

Nell'ambito di altra attività di indagine ***sottocopertura,*** *denominata* ***"WILD TELEGRAM – FASE FINALE****" condotta dal Compartimento Polizia Postale di Genova, sono stati individuati sul territorio nazionale* ***12 utenti*** *della Rete, che attraverso la piattaforma Telegram, si sono resi responsabili dei reati di cui agli artt. 600 ter e 600 quater c.p., nei cui confronti l'A.G. ligure ha emesso altrettanti decreti di perquisizione.*
L'attività si è conclusa con 10 denunciati e 2 arrestati.

Nell'ambito dell'operazione ***"LOLITA"*** *condotta dalla Sezione Polizia Postale di Brescia, unitamente alla locale Squadra Mobile, inerente la veicolazione di video e immagini pedopornografiche autoprodotte da una minore e divulgate attraverso la piattaforma Whatsapp ad altri utenti, l'A.G. procedente ha emesso nr.* ***16 decreti*** *di perquisizione espletati sul territorio nazionale nei confronti di altrettanti soggetti ritenuti responsabili dei reati di cui agli artt. 600 ter e 600 quater c.p.*
L'attività si è conclusa con 16 denunciati

All'esito di un'indagine denominata ***"BORGHETTO",*** *condotta dal Compartimento Polizia Postale di Catania, sono stati individuati* ***11 soggetti maggiorenni e 16 soggetti minorenni****, tutti sedenti nel territorio di Catania e provincia, responsabili di aver divulgato attraverso la piattaforma di messaggistica WhatsApp contenuti pedopornografici, nei cui confronti la locale Procura ordinaria e quella per i Minorenni hanno emesso altrettanti decreti di perquisizione.*
L'attività si è conclusa con 27 denunciati.

Nell'ambito dell'operazione ***"THE PUNISHER"*** *svolta dal Compartimento di Firenze, sono stati individuati 7 soggetti che attraverso la piattaforma WhatsApp, si sono resi responsabili di condotte illecite ai sensi degli artt. 600 ter e quater c.p. e nei cui confronti la locale A.G. ha emesso altrettanti decreti di perquisizione.*
L'attività si è conclusa con 6 denunciati.

Nell'ambito dell'operazione ***"CANADA 2.0"*** *svolta dal Compartimento di Reggio Calabria, su impulso del Servizio Polizia Postale e delle Comunicazioni, l'A.G. di Catanzaro ha emesso nr.* ***119 decreti*** *di perquisizione nei confronti di altrettanti soggetti ritenuti responsabili di condotte illecite ai sensi dell'art. 600 ter e 600 quater c.p. che sono statti eseguiti disgiuntamente sul territorio nazionale.*
L'attività si è conclusa con 116 denunciati e 3 arrestati.

Nell'ambito dell'operazione ***"COMETA"*** *condotta dalla Sezione Polizia Postale di Brescia inerente la diffusione sui Social Network di immagini intime ritraenti una minore affetta da ritardo cognitivo, sono stati individuati 5 utenti nei cui confronti l'A.G. bresciana ha emesso 5 decreti di perquisizione.*
L'attività si è conclusa con 5 denunciati.

*All'esito dell'operazione "****MAPLE MAZE"*** *svolta dal Compartimento Polizia Postale di Milano, su segnalazione del collaterale organo di polizia canadese, sono stati individuati 31 utenti della Rete, responsabili attraverso la piattaforma KIK Messenger dei reati di*

cui agli artt. 600 ter e 600 quater nei cui confronti la locale Procura ha emesso altrettanti decreti di perquisizione personale ed informatica che sono stati espletati sul territorio nazionale.

L'attività si è conclusa con 27 denunciati e 4 arrestati.

Nell'ambito dell'operazione ***"BIG SURPRISE"*** *condotta dal Compartimento Polizia Postale di Firenze, su segnalazione del collaterale organo di polizia canadese, sono stati individuati* ***24 utenti*** *della Rete, responsabili attraverso la piattaforma KIK Messenger dei reati di cui agli artt. 600 ter e 600 quater nei cui confronti la locale Procura ha emesso altrettanti decreti di perquisizione personale ed informatica che sono stati eseguiti sul territorio nazionale.*

L'attività si è conclusa con 22 denunciati e 2 arrestati

All'esito di un'indagine ***"ONTARIO 2"*** *svolta dal Compartimento Polizia Postale di Milano, su segnalazione del collaterale organo di polizia canadese, sono stati individuati* ***17 utenti*** *della Rete, responsabili attraverso la piattaforma KIK Messanger dei reati di cui agli artt. 600 ter e 600 quater nei cui confronti la locale Procura ha emesso altrettanti decreti di perquisizione personale ed informatica che sono stati espletati sul territorio lombardo.*

L'attività si è conclusa con 16 denunciati e 1 arrestato.

Nell'ambito dell'operazione ***"DICTUM"*** *condotta dal Compartimento Polizia Postale di Milano sono stati individuati* ***29 utenti della Rete****, responsabili attraverso la piattaforma Mega.NZ dei reati di cui agli artt. 600 ter e 600 quater nei cui confronti la locale Procura ha emesso altrettanti decreti di perquisizione personale ed informatica che sono stati espletati sul territorio lombardo.*

L'attività si è conclusa con 19 denunciati 7 arrestati e 3 irreperibili.

Al termine di un'indagine avviata a seguito di una segnalazione dell'Organizzazione statunitense NCMEC dal Compartimento Polizia Postale di Catania, sono stati individuati 7 utenti della Rete, responsabili dei reati di cui agli artt. 600 ter e 600 quater nei cui confronti la locale Procura ha emesso altrettanti decreti di perquisizione personale ed informatica.

L'attività si è conclusa con 7 denunciati.

All'esito di un'indagine sotto copertura denominata ***"MEET UP"****, svolta dal Compartimento Polizia Postale Piemonte e Valle d'Aosta sulla piattaforma Telegram, la Procura della Repubblica di Torino ha emesso 26 decreti di perquisizione.*

L'operazione si è conclusa con 23 denunciati e 3 arrestati.

Nell'ambito dell'operazione ***"GREEN OCEAN"*** *condotta anche in modalità sotto copertura dal Compartimento di Palermo su canali di file sharing, su piattaforme di chat e nel dark web, la Procura della Repubblica di Palermo ha emesso 34 decreti di perquisizione*

L'operazione si è conclusa con 21 denunciati e 13 arrestati.

Nell'ambito dei reati contro la persona commessi attraverso la rete, significativo è l'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.

	2020	2021	Incremento
Stalking	**143**	**176**	**+23%**
Revenge Porn	**126**	**225**	**+78%**
Sextortion	**636**	**984**	**+54%**

Le indagini riguardanti il fenomeno delle truffe *online* in materia di *e-commerce* 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.**.**

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:

- **5.434** 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 **110.524** *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 deferimento di complessive **187 persone** per accesso abusivo e danneggiamento di sistemi informatici afferenti sistemi critici ovvero servizi essenziali, diffusione di *malware*, 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:
***a)** 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;*

[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.

b) *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.*
*Lo scorso mese di agosto, nell'ambito di una complessa indagine denominata "**Fake pass**" – condotta dal Servizio centrale di Roma e dalle polizie postali di Milano e Bari, ha così individuato e perquisito 4 persone, tra cui 2 minorenni, che gestivano canali social specializzati nell'offerta illegale di certificati green pass Covid-19 falsi, sequestrando i 32 canali Telegram sui quali veniva veicolata la frode.*
Grazie al monitoraggio dei pagamenti im cryptovalute effettuati dai clienti per ottenere gli inesistenti green pass, la Polizia postale ha ricostruito la rete di vendita, giungendo a disarticolare quelle che, in alcuni casi, si trasformavano in vere e proprie estorsioni: non di rado, infatti, dopo aver millantanto di poter fabbricare i falsi green pass, ed essere così entrato in possesso dei dati personali e dei documenti di riconoscimento delle vittime, il truffatore passava a ricattare queste ultime, minacciando denunce alla polizia o ulteriori attacchi informatici nei loro confronti, se non avessero proceduto al pagamento di ulteriori somme di denaro.

c) *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.

Nel settore del ***financial cybercrime***, si registrano 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**.

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[2].

[2] Proprio con riferimento alla grave emergenza socio-sanitaria, accompagnata dalle restrizioni introdotte dai decreti governativi per contrastare la diffusione del virus Covid-19, è stata dedicata 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 con modalità non consentite
In tale contesto, tra le varie attività di contrasto poste in essere dalla Specialità si segnala, ad esempio, l'attività investigativa avviata condotte dal Compartimento Polizia Postale e delle Comunicazioni di Milano e dalla locale D.I.G.O.S. e coordinata dalla Sezione Distrettuale Antiterrorismo della Procura di Milano, che ha portato, lo scorso 9 settembre 2021, all'esecuzione di 8 decreti di perquisizione delegata nei confronti di altrettanti soggetti indagati per istigazione a delinquere aggravata che figuravano tra i membri

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 EU-IRU 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: **oltre 300 i canali su piattaforme di messaggistica e gli spazi web oggetto di monitoraggio.**

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.

*Con riferimento alle attività investigative svolte nel corrente anno da questa Specialità nell'ambito del contrato alla diffusione di contenuti terroristici online, si segnala che sono stati denunciati **3** soggetti ritenuti responsabili di attività di propaganda jihadista, **29** soggetti legati all'estremismo di destra, **7** soggetti legati a movimenti anarchici, mentre nell'ambito dei movimenti NO-VAX e dell'emergenza COVID-19 sono state denunciate **101** persone.*

---

attivi di un gruppo Telegram denominato "I guerrieri" nel quale venivano progettate azioni violente da realizzare – anche con l'uso di armi ed esplosivi fai da te – in occasione delle manifestazioni "no green pass" organizzate su tutto il territorio nazionale.

Ed ancora, a titolo esemplificativo, si segnala l'ulteriore attività avviata dal Compartimento Polizia Postale e delle Comunicazioni di Torino, unitamente alla locale DIGOS, nei confronti degli attivisti NO Vax/NO GreenPass che ha portato all'esecuzione nella mattinata del 15 novembre 2021 di 17 decreti di perquisizione a carico dei soggetti più radicali affiliati al noto canale Telegram "Basta Dittatura", uno degli spazi web di maggiore riferimento nella galassia dei negazionisti del COVID 19.

Tra le molteplici attività investigative in tale contesto, appare opportuno segnalare anche quella avviata dal Compartimento Polizia Postale di Genova, che ha portato all'esecuzione di ventiquattro perquisizioni nell'ambito di una vasta operazione, coordinata dalla DDA della Procura della Repubblica di Genova, tesa ad individuare i vertici e le figure intermedie di un'associazione segreta NO VAX/NO GREEN PASS i cui appartenenti operavano prendevano il nome di Guerrieri ViVi, all'interno di canali *Telegram* segreti, compiendo attività illecite pianificate da un numero ristretto di individui.

Ed ancora, 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".

Proprio con riferimento alla grave emergenza socio-sanitaria, accompagnata dalle restrizioni introdotte dai decreti governativi per contrastare la diffusione del virus Covid-19, è stata dedicata 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 con modalità non consentite

In tale contesto, tra le varie attività di contrasto poste in essere dalla Specialità si segnala, ad esempio, l'attività investigativa avviata condotte dal Compartimento Polizia ***Postale e delle Comunicazioni di Milano*** *e dalla locale D.I.G.O.S. e coordinata dalla Sezione Distrettuale Antiterrorismo della Procura di Milano, che ha portato, lo scorso 9 settembre 2021, all'esecuzione di 8 decreti di perquisizione delegata nei confronti di altrettanti soggetti indagati per istigazione a delinquere aggravata che figuravano tra i membri attivi di un gruppo Telegram denominato "I guerrieri" nel quale venivano progettate azioni violente da realizzare – anche con l'uso di armi ed esplosivi fai da te – in occasione delle manifestazioni "no green pass" organizzate su tutto il territorio nazionale.*

Ed ancora, a titolo esemplificativo, si segnala l'ulteriore attività avviata dal Compartimento ***Polizia Postale e delle Comunicazioni di Torino****, unitamente alla locale DIGOS, nei confronti degli attivisti NO Vax/NO GreenPass che ha portato all'esecuzione nella mattinata del 15 novembre 2021 di 17 decreti di perquisizione a carico dei soggetti più radicali affiliati al noto canale Telegram* ***"Basta Dittatura****", uno degli spazi web di maggiore riferimento nella galassia dei negazionisti del COVID 19.*

Tra le molteplici attività investigative in tale contesto, appare opportuno segnalare anche quella avviata dal Compartimento Polizia Postale di Genova, che ha portato all'esecuzione di ventiquattro perquisizioni nell'ambito di una vasta operazione, coordinata dalla ***DDA della Procura della Repubblica di Genova****, tesa ad individuare i vertici e le figure intermedie di un'associazione segreta* ***NO VAX/NO GREEN PASS*** *i cui appartenenti operavano prendevano il nome di Guerrieri ViVi, all'interno di canali* ***Telegram segreti****, compiendo attività illecite pianificate da un numero ristretto di individui.*

Ed ancora, 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".

Prevenzione Antiterrorismo *Eversione Internazionale Estremismo religioso e politico*	**2020**	**2021**
Persone indagate	1	12
Contenuti web monitorati	34.676	74306
Contenuti web oscurati	0	383

Prevenzione *Eversione nazionale estrema destra, area antagonista, attività in circostanze di emergenza*	**2020**	**2021**
Persone indagate	15	60
Contenuti web monitorati	3312	42787
Contenuti web oscurati	0	88

Di rilievo infine l'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 **6400 le 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 **229 persone (+394% rispetto all'anno precedente)** per c.d. "reati postali[3]".

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)**.

Grazie alle segnalazioni pervenute al Commissariato di P.S. *online*, **sono stati 70** gli interventi per **casi di suicidio annunciati in rete** da parte di utenti individuati in emergenza dal personale specializzato, a seguito dello sviluppo di attività di indagine informatica.

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 **XI edizione** 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 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**.

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

[3] Furto di corrispondenza, incasso fraudolento di assegni etc.

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.).

Con riferimento alla realtà abruzzese il Compartimento Polizia Postale e delle Comunicazioni di Pescara e le sezioni di L'Aquila Teramo e Chieti continuano nell'attività di prevenzione e repressione dei fenomeni criminali su elencati.

Nel 2021 di particolare rilievo sono state tre distinte attività investigative che hanno portato all'arresto di tre uomini responsabili di detenzione di ingente materiale pedopornografico.

Venivano inoltre denunciate in stato di libertà 156 persone, sequestrati 98 apparati informatici ed effettuati 7100 monitoraggi internet.

Nell'ottica di una fattiva collaborazione volta a prevenire e contrastare gli attacchi/danneggiamenti informatici, questo Compartimento ha sottoscritto un protocollo d'intesa a tutela di una infrastuttura critica locale.

Nell'ambito poi delle campagne informative finalizzate alla cultura della legalità e alla navigazione sicura su internet, personale del Compartimento Polizia Postale e delle Comunicazioni "Abruzzo" ha tenuto numerosi incontri presso le scuole della Regione, sia in presenza che "a distanza" mediante video collegamenti con dirette streaming cui hanno partecipato oltre 3400 studenti e numerosi docenti.