Resoconto attività 2020 Polizia Postale e delle Comunicazioni

VITERBO- L'anno 2020 è stato caratterizzato da mutamenti profondi delle nostre abitudini di vita. In modo repentino, quasi tutte le nostre attività (lavoro – scuola – tempo libero – formazione – cultura – relazioni) hanno conosciuto una rimodulazione basata in larga parte sull'utilizzo della rete, con un allargamento della platea degli utenti anche a soggetti normalmente poco adusi alle nuove tecnologie, fattore il quale, se da un lato ha accelerato un processo di modernizzazione certamente già in atto, ha, del pari, determinato una accresciuta esposizione alle aggressioni della cyber-criminalità.

In questo scenario, l'impegno della Polizia Postale e delle Comunicazioni si è indirizzato verso la prevenzione ed il contrasto di un insieme assai vasto ed eterogeneo di attacchi informatici, diretti a colpire il patrimonio personale dei cittadini come l'integrità del tessuto economico-produttivo del Paese, la regolarità dei servizi pubblici essenziali come il mondo delle professioni, la sicurezza e la libertà personale di adulti e ragazzi con particolare riferimento alla protezione dei bambini e delle persone più vulnerabili.

C.N.C.P.O.	2019	2020	Incremento %
Casi trattati	1396	3.243	+ 132,30 %
Persone indagate	617	1192	+ 93.19 %
Arrestati	37	69	+ 86.48 %
Perquisizioni	510	757	+ 48.43 %
Gb di materiale sequestrato	127.269	215.091	+ 69.00 %

1. **N.C.P.O.**

Nel corso del 2020, il *Centro Nazionale per il Contrasto alla Pedopornografia Online* (C.N.C.P.O.) ha confermato il ruolo centrale della Polizia Postale e delle Comunicazioni nella

lotta alla pedofilia e pornografia minorile online.

Dall'inizio della diffusione pandemica da COVID-19, la Polizia Postale ha intensificato il monitoraggio della rete con lo scopo di scongiurare l'aumento di reati relativi allo sfruttamento sessuale dei minori online, determinato dalle misure restrittive assunte. E' stato svolto un lavoro di valutazione settimanale dei dati relativi alla vittimizzazione dei bambini e dei ragazzi in rete, al fine di monitorare la minaccia cibernetica in un momento di fragilità emotiva nazionale.

	2019	2020
Diffamazione online	2.234	2.234
Stalking	168	143
Revenge porn	131	126
Sextortion	516	636

Con la sospensione delle attività scolastiche e la conseguente attivazione della didattica a distanza per tutti gli Istituti, molteplici sono state le segnalazioni relative a episodi di intrusione nelle piattaforme dedicate alla formazione degli studenti; la Polizia Postale ha svolto un assiduo monitoraggio anche sulle *app* di messaggistica istantanea, al fine di individuare i responsabili degli accessi non autorizzati, accertando la presenza di gruppi dedicati.

Le condotte delittuose che hanno registrato un incremento di circa il **110%** rispetto allo stesso periodo dell'anno precedente, riguardano i reati relativi allo **sfruttamento sessuale dei minori online** e dell'**adescamento di minori online**, per i quali sono stati eseguiti **69** arresti e denunciate **1192** persone.

Per quanto concerne l'attività di prevenzione svolta dal C.N.C.P.O. attraverso una continua e costante attività di monitoraggio della rete, sono stati visionati 33.681, di cui 2.446 inseriti in black list e oscurati in quanto presentavano contenuti pedopornografici.

	2019	2020
Attacchi rilevati	239	507
Alert diramati	77.596	79.209
Indagini avviate	88	99
Persone arrestate	3	21
Persone denunciate	53	79
Richiesta di cooperazione internazionale in ambito Rete 24/7 High Tech Crime G8 (Convenzione Budapest)	74	65

Il Compartimento Polizia Postale per il Lazio, in tale ambito, nell'anno 2020, ha trattati oltre 380 casi e sono state avviate numerosi indagini, che hanno portato all'esecuzione di 110 perquisizioni, all'arresto di 7 persone ed alla denuncia in stato di libertà di 157 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 18.900 gigabyte di contenuti multimediali di tale illecita natura.

Nel corso di tale attività sono stati inoltre visionati 16.150 spazi virtuali.

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

- A seguito dell'attività investigativa scaturita da segnalazione del C.N.C.P.O. , condotta da personale del Compartimento Polizia Postale di Roma, veniva individuato un soggetto nei confronti del quale la Procura della Repubblica presso il Tribunale di Roma, emetteva decreto di perquisizione. Durante l'esecuzione dell'attività di perquisizione informatica, il soggetto veniva trovato in possesso di un ingente quantitativo di materiale pedopornografico, pertanto

PERIODO	NR. VISITE	ACCESSI
TOTALE 2019	1.014.446	28.580.287
TOTALE 2020	3.191.633	65.094.386
INCREMENTO %	+214,6 %	+127,7 %

veniva tratto in arresto e sottoposto agli arresti domiciliari.
- L'attività investigativa condotta a seguito di numerose segnalazioni relative al caricamento di file di natura pedopornografica su un servizio di cloud storage, consentiva di individuare il responsabile in un romano di 42 anni. Nei confronti dello stesso veniva emesso decreto di perquisizione e la successiva perizia sul materiale posto sotto sequestro ha consentito di accertare la presenza di un ingente quantitativo di materiale illecito sui *device* Veniva pertanto emessa ed

eseguita ordinanza di custodia cautelare.

- L’attività investigativa scaturita da segnalazione consentiva di individuare un soggetto nei cui confronti veniva svolta attività di perquisizione. L’esecuzione del decreto di perquisizione consentiva di rinvenire sui supporti sequestrati un ingente quantitativo di materiale illecito detenuto, che consentiva l’arresto in fragranza di reato del soggetto, il quale veniva accompagnato presso la casa circondariale di Viterbo.
- A seguito di perquisizione informatica disposta dalla Procura della Repubblica presso il

PERIODO	SEGNALAZIONI FAKE NEWS	ALERT DIRAMATI
TOTALE 2019	21	29
TOTALE 2020	134	136
INCREMENTO PERCENTUALE RISPETTO ALLO STESSO PERIODO DELL'ANNO PRECEDENTE	+ 436,0%	+ 353,3 %

Tribunale di Catanzaro, personale del Compartimento di Roma rinveniva durante l’attività di *preview* numerosi file immagine e video di natura pedopornografica. Nei confronti dell’indagato, che teneva esposte in casa anche fotografie di minori nudi, veniva pertanto arrestato e condotto presso la casa circondariale di “Rebibbia”.

- A seguito di denuncia sporta da una società, per la quale il soggetto lavorava in regime di smart working, che aveva notato un traffico dati anomalo sulla linea internet utilizzata dallo stesso, si effettuavano alcune verifiche sulla provenienza dei files scambiati. La successiva perquisizione informatica consentiva di rinvenire una quantità impressionante di materiale catalogato in maniera meticolosa. Il soggetto pertanto veniva tratto in arresto e accompagnato presso il carcere di “Regina Coeli”.
- Nell’ambito delle indagini sotto copertura condotte dal Compartimento di Milano, veniva organizzata un’imponente operazione di polizia volta al contrasto della

pedopornografia online, denominata “Luna Park”. L’esecuzione dei numerosi decreti di perquisizione su tutto il territorio nazionale vedeva coinvolto anche personale del Compartimento di Roma. L’ingente quantitativo di materiale illecito rinvenuto, in sede di perquisizione informatica, sui supporti sequestrati, ha consentito di trarre in arresto un soggetto, già condannato per il medesimo reato nel 2009, veniva accompagnato presso il carcere di “Rebibbia”.

1. **TRUFFE ON LINE – FINANCIAL CYBERCRIME E REATI CONTRO LA PERSONA**

Il fenomeno delle **truffe online,** ha riguardato anche la **contraffazione del marchio CE**. Sono state scoperte numerose partite di materiale, venduto all’ingrosso, proveniente soprattutto dall’estero, riportanti marchi CE contraffatti: la merce era destinata, in alcuni casi, alla vendita al dettaglio anche attraverso il circuito delle farmacie ignare della contraffazione.

Nei primi mesi dell’anno, sono stati riscontrati numerosi casi di truffe online nella vendita di **dispositivi di protezione individuale,** considerata la ricerca pressante di mascherine, guanti, liquidi igienizzanti, attraverso la proliferazione di numerosi siti di e-commerce truffaldini dedicati al commercio di tali prodotti.

Sono state anche raccolte numerose segnalazioni e avviate altrettante attività d’indagine, inerenti le **false raccolte fondi,** poste in essere attraverso siti web apparentemente riconducibili ad enti ospedalieri o accreditate da falsi patrocini di Istituzioni o Enti Pubblici (Regioni – Comitati vari). Il *modus operandi* dei cybercriminali, facendo leva sul generale e diffuso sentimento di vicinanza della cittadinanza al personale medico ed infermieristico, incessantemente impegnato nella lotta al **Covid 19,** dava la possibilità di effettuare dei versamenti di denaro e/o bonifici su IBAN

legati a conti correnti o carte ricaricabili attivati ad hoc.

Inoltre, è stato osservato, contemporaneamente alla chiusura dei luoghi di lavoro a seguito dell'introduzione delle misure di contenimento del virus, un incremento del fenomeno dei **falsi annunci di lavoro**.

Nell'ambito delle **truffe online**, nel corso del 2020 sono stati trattati complessivamente **98.000** casi.

Nel corso del periodo in esame, è stata implementata l'attività di contrasto al diffuso fenomeno del **falso trading online** (**358 casi trattati** con oltre **20 milioni** di euro di danno) che ha visto aumentare a dismisura la perdita di ingenti capitali verso Paesi esteri, con la prospettiva di facili guadagni derivanti da investimenti **"sicuri**".

Il diffondersi dell'epidemia da Covid-19 ha senz'altro inciso, anche sulla qualità e quantità dei fenomeni legati al **cybercrime,** con particolare riferimento al crimine di tipo economico-finanziario.

In via generale, le ricerche più autorevoli hanno rilevato nei primi sei mesi un aumento del 600% nel numero di e-mail di phishing in tutto il mondo, che utilizzava temi correlati al Coronavirus per colpire persone e aziende. Di queste, il 45% puntava su siti-clone, inducendo gli utenti di Internet a digitare le proprie password su domini malevoli. La restante parte dei casi ha riguardato, per lo più, l'utilizzo di temi correlati al Covid-19 all'interno di messaggi email che inducevano a cliccare su allegati contenenti malware di varia natura.

Le frodi basate sul social engineering vedono stabili nei numeri i fenomeni di Bec fraud (frodi realizzate attraverso la compromissione di caselle di posta elettronica), che risultano tuttavia influenzati dall'epidemia del Covid-19 sia a causa dell'abbassamento delle difese aziendali, determinato dallo stato di difficoltà psicologica o "logistica" di lavoratori ed

amministratori, sia dall'aumento delle comunicazioni commerciali a distanza, conseguente all'adozione su larga scala di processi di smart-working.

Alcuni Bec fraud risultano specificamente collegati al tema-Covid, perché relativi direttamente a frodi commerciali nell'acquisto di mascherine e dispositivi sanitari.

Con riguardo all'esperienza italiana, in pochi mesi, oltre ad un costante numero di casi "minori" (nell'ordine delle decine di migliaia di euro), sono state frodate 48 grandi e medie imprese, per un ammontare complessivo di oltre 25 milioni di euro di profitti illeciti, dei quali quasi 15 milioni sono stati già recuperati in seguito all'intervento della Polizia Postale e delle Comunicazioni che, al 10 dicembre 2020, ha complessivamente identificato ed indagato 674 persone di cui 24 tratte in arresto (nell'analogo periodo del 2019 furono complessivamente indagate 531 persone di cui 8 in stato di arresto).

L'obiettivo criminale del trafugamento dei dati personali e delle credenziali di accesso a servizi finanziari, utili alla disposizione di pagamenti in frode, è raggiunto attraverso massive campagne di phishing, consumate mediante le due modalità in assoluto più ricorrenti, rappresentate dall'invio di email contenenti allegati malevoli e dall'impiego di siti-clone.

Parallelamente, il procacciamento di codici "one-time", token virtuali e password dispositive avviene mediante il ricorso all'insidiosa variante "vocale" del phishing, il cosiddetto "vishing", ed alle tecniche di sim-swap.

L'attività investigativa realizzata dalla Polizia Postale e delle Comunicazioni, funzionale al contrasto di tali fenomeni delittuosi, ha permesso di identificare ed indagare 3741 persone a fronte dei 3473 denunciati nello stesso periodo dell'anno precedente.

Particolare attenzione è stata indirizzata all'attività di prevenzione e contrasto al **revenge porn** con **126** casi trattati e **59 denunciati;** alla **diffamazione on line** con **2.234** casi e **906** persone denunciate; **143** sono stati i casi relativi allo "**stalking" con 7 arrestati e 73 denunciati** e alla cosiddetta "**sextortion" con 636 casi trattati, una persona arrestata e 36 denunciate.**

I reati afferenti al cosiddetto **"Codice Rosso"**, le cui indagini sono profuse non soltanto per giungere all'identificazione del responsabile del reato, ma anche per la rimuovere i contenuti dal web o, quantomeno, per limitarne la divulgazione massiva, hanno visto nella Polizia Postale un punto di riferimento per le tante vittime di reato.

Anche nella repressione dei reati di **minacce e molestie**, perpetrate attraverso i social network ovvero con "mezzi tradizionali", massimo è stato l'impegno della Polizia Postale con **1001 casi trattati, 2 arrestati e 270 persone denunciate.**

Il Compartimento Polizia Postale e delle Comunicazioni per il Lazio, nell'ambito delle truffe on line e Financial Cybercrime ha trattato 1831 casi, eseguito 33 perquisizioni e monitorati circa 7.000 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 3 persone ed all'esecuzione di numerose perquisizioni con il sequestro ed il recupero di ingenti somme di denaro originariamente sottratte ai rispettivi titolari.

Da ultimo, le attività investigative del Compartimento in materia di e-commerce e telefonia, 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 670 soggetti.

Si segnalano i seguenti casi di particolare rilevanza:

- Dopo una lunga attività di indagine e vari accertamenti è stata denunciata in stato di libertà una donna per il reato di circonvenzione di incapaci, con sequestro di conti e depositi intestati alla medesima, in quanto la stessa approfittandosi della P.O., persona sola e anziana, gli sottraeva reiteratamente denaro della pensione accompagnandolo falsamente in ausilio alla riscossione presso l'ufficio postale.
- Nel corso dell'anno è stata condotta una elaborata indagine che ha consentito l'identificazione di un soggetto che, sostituendosi ad un correntista, ha prima attivato un conto corrente per poi tentare di versare su di esso un assegno di 200.000,00 euro contraffatto;
- "Operazione "Romance Scam"; a partire dal primo semestre di quest'anno, è stata individuata un'associazione a delinquere localizzata sul territorio romano finalizzata alla perpetrazione del noto sistema di truffa denominato "Romance Scam" o truffa romantica. La vittima, una donna romana, credendo di intessere una relazione virtuale con un noto tennista, è stata raggirata e indotta a versare, in più tranche, la somma complessiva di € 140.000, importo che sarebbe servito per consentire il ricongiungimento in Italia della stessa con il fantomatico spasimante. Le indagini, concentrate sullo studio dei flussi finanziari, hanno consentito di deferire all'A.G. n. 9 cittadini africani, facenti parte di una articolata consorteria criminale con ramificazioni in altre zone del paese, in Francia, in Grecia, e in Gran Bretagna.
- "Riscossione in frode Rimborsi fiscali IRPEF". Nell'ambito di un'attività di indagine, finalizzata al contrasto del fenomeno della riscossione in frode dei rimborsi fiscali IRPEF, sono state contestualmente

eseguite – nel Lazio e presso Terni – 6 perquisizioni sulla base di provvedimenti emessi dalla locale Procura della Repubblica a carico di altrettanti soggetti facenti di un associazione dedita ai reati di falso, truffa, sostituzione di persona, riciclaggio.

- Una importante attività di indagine ha consentito di individuare ed eseguire poi, su delega della locale Procura della Repubblica, l'oscuramento di un sito denominato covidtoken.org, avente server negli Stati Uniti, che consentiva di guadagnare su una criptovaluta il cui valore, e la relativa macabra possibilità di guadagno, dipendeva dall'aumento dei decessi causato da COVD-19. La stesso sito prometteva falsamente, che una parte dei guadagni, sarebbe stato reinvestito per finanziare la Croce rossa per iniziative di contenimento del contagio;
- Presso gli Uffici del Compartimento Polizia Postale di Roma si presentava la vittima di una truffa al fine di integrare una denuncia precedentemente resa in altro ufficio, nella circostanza, durante la stesura dell'atto, venivano presi contatti con la banca del denunciante, intervenendo sul blocco della somma di euro 15.796,92 indebitamente sottratti alla parte offesa, prima che venissero monetizzati dal truffatore;
- A seguito di acquisizione di numerose denunce di vittime di truffa, poi incardinate nello stesso procedimento penale e quindi in un'unica attività di indagine, venivano denunciati in stato di libertà, due soggetti italiani, che operando per conto di una società, in qualità di mediatrice di una società svizzera", proponevano al pubblico una formula di acquisto di autovetture nuove, consistente nell' acquisto al normale prezzo di mercato, gravato di un ulteriore costo pari a 5.500 Euro per una attività pubblicitaria (applicazione sulla carrozzeria di adesivi pubblicitari ed impegno di scattare delle foto dello stesso automezzo con le pubblicità di volta in volta fatte applicare dalla

società proponente, condividendole, sui profili personali nei principali social network) che avrebbe garantito di pagarsi a costo zero, le rate del finanziamento autonomamente richiesto dalla vittima al proprio istituto di credito. Quindi, una volta sottoscritto il contratto, acquistata a proprie spese l'autovettura, la vittima di turno, non riceveva i previsti rimborsi mensili coincidenti con la somma della rata del finanziamento da saldare, vedendo di fatto sottrarsi, le rispettive quote pari a 5500,00 euro, anticipate per le pubblicità e bonificate a favore della citata società italiana S.r.l., direttamente riconducibile ai due soggetti deferiti all'A.G.

- A fronte di denuncia sporta da una azienda di telefonia mobile, venivano identificati e deferiti in stato di libertà tre soggetti di nazionalità italiana, titolari di altrettante attività commerciali collegate tra loro, di tipo dealer, tramite le quali, gli indagati hanno percepito fraudolenti bonifici di rimborso corrispondente al costo dei numerosi telefoni e relativo margine di profitto, spettante per le vendite in abbinamento alle contestuale attivazione di utenze mobili, risultate fittizie e falsamente documentate al gestore telefonico che, una volta accertata la frode, ha revocato le autorizzazione ad operare in qualità di dealer.

Il Compartimento Polizia Postale e delle Comunicazioni per il Lazio, nell'ambito dei reati contro la persona, nell'anno 2020, ha trattato 187 casi, monitorando oltre 5650 spazi virtuali, riscontrandone 295 con contenuti illeciti.

L'attività investigativa in questo settore ha portato alla denuncia di 185 persone ed all'esecuzione di 7 perquisizioni.

Particolare rilevanza ha assunto l'attività di contrasto ai reati di competenza annoverati nella legge 19 luglio 2019 n. 69, cosidetto "Codice Rosso"; dal mese di gennaio ad oggi sono

stati trattati oltre 35 casi e sono state indagate più di 15 persone.

Di particolare rilievo, nell'anno appena trascorso, è il *trend* in crescita delle richieste di ammonimento del Questore, istituto previsto dal D.L. 93/2013, nel caso in cui non sia stata sporta querela e non siano stati perpetrati reati procedibili d'ufficio. La normativa ha concesso agli operatori di Polizia del Compartimento Polizia Postale di Roma uno strumento efficace per incidere sul fenomeno dello stalking e del cyberbullismo, e su tutti quei comportamenti che pur non integrando reati procedibili d'ufficio, sconvolgono la vita della vittima portandola all'esasperazione. Nel corso del 2020 il Compartimento Polizia Postale e delle Comunicazioni di Roma ha rivolto al Questore, quale Autorità di Pubblica Sicurezza, nr. 10 istanze di ammonimento nei confronti degli autori di condotte moleste.

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

OPERAZIONE "STALKING", L'attività di indagine, è scaturita dalla denuncia e successive integrazioni sporta da una vittima di stalkingad opera di un soggetto ignoto, che la perseguitava con pedinamenti, invio di email da account artatamente create, comunicazioni con app (applicazione mobile) di messaggistica con "apparati e utenze anonime" e intrusioni informatiche. La vittima, che nel frattempo pensava di trovare sostegno e protezione nel suo ex compagno, era inconsapevole del fatto che poi sarebbe risultato proprio quest'ultimo responsabile dei fatti illeciti. La vicinanza dello stalker, ne ha determinato un'evidente pericolosità essendo nelle condizioni di poter trasformare il suo morboso interesse in odio e violenza. Le indagini sono state ancora più complesse per il fatto che, al fine di rafforzare la sua posizione e depistare le indagini, l'ex fidanzato si proclamava vittima dei medesimi fatti denunciati dalla donna, denunciando a sua volta la ricezione delle stesse email e minacce, facendo

cadere esplicitamente i sospetti su un altro soggetto, che aveva fatto parte, in un lontano passato, della vita intima della reale vittima. Identificato l'autore nel suo ex compagno e collega di lavoro, è stata richiesta, ottenuta ed eseguita ordinanza di custodia cautelare agli arresti domiciliari, con contestuale perquisizione ed accertamenti tecnici positivi.

OPERAZIONE "MINACCE ANONIME" A seguito di telefonata anonima, giunta al centralino del Compartimento Polizia Postale di Roma, in cui l'ignoto interlocutore rivolgeva gravi minacce nei confronti di una alta carica istituzionale, veniva richiesto e acquisito il traffico in entrata dell'utenza riconducibile al centralino stesso, tramite apposito decreto di tabulati telefonici, la cui analisi consentiva di individuare, come selettivo utilizzato per effettuare la chiamata oggetto di indagine, quello riconducibile ad un soggetto maschile, italiano, nato e residente in Calabria, riscontro che risultava sovrapponibile alle informazioni acquisite in merito alla telefonata minatoria, ovvero all'accento meridionale con cui si esprimeva l'interlocutore. Elementi che portavano alla denuncia in stato di libertà della persona identificata.

Un impegno costante, anche con un'ampia attività di prevenzione, è stato rivolto al contrasto dei reati d'incitamento all'odio, indicatori di violenza di genere e condotte discriminatorie di genere, antisemite e xenofobe, con oltre 8000 spazi virtuali monitorati.

In tale contesto, si segnala l'OPERAZIONE "MANLIO GERMANO"; a seguito della pubblicazione di un post sulla pagina Facebook "Manlio Germano", dai contenuti offensivi e di discriminazione e odio razziale rivolti nei confronti di Willy Montiero Duarte, vittima di tristi e noti fatti di cronaca, sono stati denunciati, dalla Sezione Polizia Postale di Latina, due soggetti per il reato di istigazione a delinquere aggravato dalla finalità dell'odio razziale; è stato inoltre denunciato, dalla Sezione Polizia Postale e delle Comunicazioni di

Frosinone, un terzo soggetto per il reato di propaganda e istigazione a condotte discriminatorie raziali, dopo aver realizzato e divulgato su internet un video anch'esso inerente i noti fatti di cronaca ai danni di Willy Monteiro Duarte.

OPERAZIONE "NO BULLISMO" Sono stati deferiti, alle compenti autorità giudiziarie quattro giovani (tre minorenni e uno maggiorenne), accusati di un grave episodio di bullismo per aver aggredito, malmenato e ridicolizzato sui social attraverso la pubblicazione di un video, un ignaro quindicenne, agli stessi sono stati contestati i reati di percosse, violenza privata e diffamazione aggravata.

1. **CNAIPIC**

L'analisi del dato emergente dalle attività del **C**entro **N**azionale **A**nticrimine Informatico per la Protezione delle Infrastrutture Critiche (**CNAIPIC**), relativo al periodo intercorso tra **gennaio e dicembre 2020**, permette di rilevare, in primo luogo, come, sia gli attacchi diretti alle grandi infrastrutture erogatrici di servizi essenziali (approvvigionamento idrico ed energetico, pubblica amministrazione, sanità, comunicazione, trasporti, finanza sistemica), che gli attacchi apparentemente isolati (diretti a singoli enti, imprese o cittadini), siano connotati da una dimensione criminale organizzata, essendo ascrivibili all'operato di sodalizi ben strutturati, spesso operanti a livello transnazionale.

Le tipologie di eventi cyber che hanno maggiormente impegnato gli operatori del Centro sono rappresentate dagli attacchi a mezzo malware, soprattutto di tipo ransomware, attacchi DDoS con finalità estorsiva, accessi abusivi con l'intento di carpire dati sensibili, campagne di phishing e, in ultimo, campagne APT (*Advanced Persistent Threats*), particolarmente insidiose poiché ricollegabili ad attori malevoli dotati di notevole expertise tecnico e rilevanti risorse.

L’emergenza Covid-19, in particolare, ha costituito un’ulteriore occasione per strutturare e dirigere attacchi ad ampio spettro, volti a sfruttare per scopi illeciti la situazione di particolare esposizione e maggior vulnerabilità in cui il Paese è risultato, e tuttora risulta, esposto.

Nello specifico, alcune delle più rilevanti infrastrutture sanitarie impegnate nel trattamento dei pazienti “Covid” sono state oggetto di campagne di cyber-estorsione volte alla veicolazione all’interno dei sistemi ospedalieri di sofisticati ransomware – concepiti allo scopo di rendere inservibili, mediante cifratura, i dati sanitari contenuti al loro interno – a fronte di richieste di pagamento del prezzo estorsivo, per lo più in cryptovalute (es. Bitcoin), onde ottenere il ripristino dell’operatività.

Il sistema sanitario e della ricerca è stato inoltre bersaglio di diversi attacchi APT, con lo scopo della esfiltrazione di informazioni riservate riguardanti lo stato di avanzamento della pandemia e l’elaborazione di misure di contrasto, specie con riguardo all’approntamento di vaccini e terapie anti-Covid.

Si sono moltiplicati i casi di phishing ai danni di enti ed imprese, veicolati attraverso messaggi di posta elettronica i quali, dietro apparenti comunicazioni di Ministeri, organizzazioni sanitarie ed altri enti, relative all’andamento del contagio o alla pubblicazione di misure di contrasto, nascondevano in realtà sofisticati virus informatici in grado di assumere il controllo dei sistemi attaccati (c.d. virus RAT) e procedere così all’esfiltrazione di dati personali e sensibili, alla captazione di password di accesso a domini riservati, finanche all’attivazione di intercettazioni audio-video illegali.

L’aggiornato quadro informativo riferibile alle specifiche fenomenologie delittuose può essere agevolmente evidenziato attraverso la tabella statistica, di seguito indicata, che

offre il confronto tra il periodo **gennaio/dicembre 2019** e quello riferibile **all'anno 2020**, periodo, quest'ultimo, caratterizzato dall'emergenza epidemiologica in atto che ha favorito, come detto, l'andamento crescente del numero di attacchi complessivamente verificatisi ai danni delle Infrastrutture critiche del nostro Paese:

Dalla tabella si evince che, ad oggi, gli attacchi rilevati sono più che raddoppiati, con un conseguente quasi equivalente incremento delle persone identificate ed indagate.

Tra le attività di polizia giudiziaria più significative si segnala:

OPERAZIONE "DATA ROOM"

Il CNAIPIC nell'ambito di una lunga ed articolata attività di indagine ha effettuato quella che può essere ritenuta la prima operazione su larga scala volta alla tutela di dati personali trafugati, culminata con l'esecuzione, effettuata con l'ausilio di personale dei Compartimento Polizia Postale e delle Comunicazioni di Roma, Napoli, Perugia ed Ancona, a 13 ordinanze di custodia cautelare e 7 ordinanze che dispongono l'obbligo di dimora nel comune di residenza ed il divieto di esercitare imprese o ricoprire incarichi direttivi in imprese e persone giuridiche.

Al vertice del sistema due dipendenti infedeli di TIM S.p.A., oltre ai responsabili di alcune società che offrono servizi di call center, avevano messo i piedi una complessa ed articolata attività criminale finalizzata al commercio illecito dei dati personali di centinaia di migliaia di utenti di società operanti nella fornitura di servizi essenziali, nel settore telecomunicazioni ed energia.

I 26 indagati complessivi, tutti destinatari di provvedimenti di perquisizione locale e personale, sono stati ritenuti responsabili, a vario titolo ed in concorso tra loro, della violazione aggravata dei reati previsti all'art. 615 ter c.p.

(accesso abusivo a sistema informatico), all'art.615 quater c.p. (detenzione abusiva e diffusione di codici di accesso), riguardando le condotte sistemi di pubblico interesse, e della violazione della legge sulla privacy art. 167-bis D. Lgs. 193/2003 (comunicazioni e diffusione illecita di dati personali oggetto di trattamento su larga scala).

Le estrazioni dei dati dai database dei fornitori dei servizi, per come verificato nel corso delle indagini, venivano sistematicamente portate avanti con un volume medio di centinaia di migliaia di record al mese, che gli indagati modulavano a seconda della illecita "domanda" di mercato.

Nel corso delle attività, svolte grazie alla collaborazione di TIM S.p.A. ed all'importante apporto della struttura di sicurezza aziendale dell'azienda, è venuto alla luce un complesso "sistema" che vedeva, da un lato una serie di tecnici infedeli procacciare i dati, dall'altro una vera e propria rete commerciale che ruotava attorno alla figura di un imprenditore Campano, acquirente della preziosa "merce", che poi veniva poi piazzata sul mercato dei call center, 13 sono quelli già individuati nella prima fase delle indagini, tutti in area campana, ed oggetto di altrettante attività di perquisizione.

Nell'ottica di un'efficace condivisione operativa, il Centro ha proseguito la stipula di specifici Protocolli a tutela delle infrastrutture critiche nazionali: al riguardo, nel 2020 sono **state sottoscritte 7 nuove convenzioni** con le società **Borsa Italiana, EFSA (European Food Safety Authority), IREN S.p.A., SACBO Aeroporto di Bergamo, SAIPEM S.p.A., SIA S.p.A. e SIOT TAL Oleodotto Transalpino**.

Si rappresenta, altresì, che analoghe forme di collaborazione sono state avviate dal **Compartimento Polizia Postale per il Lazio**, con strutture sensibili di rilevanza locale, sia pubbliche che private, al fine di garantire un sistema di sicurezza informatica capillare e coordinato.

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 circa 137 deleghe emesse dall'autorità giudiziaria, deferito n.6 persone in stato di libertà all'A.G. per il reato di accesso abusivo a sistema informatico,effettuato 41 segnalazioni ai referenti regionali individuati nell'ambito dell'attività volta alla prevenzione e repressione di attacchi informatici ramsomware per colpire ospedali e strutture sanitarie impegnate nella gestione dell'emergenza Covid-19.

Sono state inoltrate ai referenti individuati nell'ambito delle attività di monitoraggio delle infrastrutture critiche, circa 106 segnalazioni inerenti più di 1000 eventi di sicurezza informatica relativi a vulnerabilità, violazioni di dati, malware o altre attività di minaccia informatica.

E' stato denunciato in stato di libertà un soggetto resosi responsabile del reato previsto dall'art. 615 ter c.p. perché effettuava accesso abusivo al portale di gestione dell'applicazione LAZIOdrCOVID sviluppata e gestita dalla società LazioCrea S.p.a. – per conto della Regione Lazio, applicazione creata al fine di facilitare il collegamento telematico tra medico di base e i propri pazienti.

1. **CYBER-TERRORISMO**

Come noto, il 2020 è stato caratterizzato da eventi, sia a livello globale, sia nazionale, che hanno avuto notevoli riflessi sulle attività di prevenzione, monitoraggio ed investigative quotidianamente svolte dal personale della Polizia Postale e delle Comunicazioni e finalizzate al contrasto delle azioni eversive, del terrorismo internazionale, dei fenomeni di radicalizzazione sul web.

Consistenti sono stati gli sforzi dedicati al contrasto dei fenomeni di radicalizzazione jihadista, nonché volti ad arginare la propaganda del *Daesh*, che attualmente è veicolata

da vari *Media Center* insistenti nelle province del Califfato che si appoggiano ai c.d. Supporter Generated Content per la diffusione dei contenuti illeciti all'interno delle varie piattaforme di comunicazione.

In questo ambito, gli investigatori della Polizia Postale e delle Comunicazioni hanno concorso con altri organi di Polizia e di intelligence alla prevenzione e al contrasto dei fenomeni di eversione e terrorismo, sia a livello nazionale che internazionale, posti in essere attraverso l'utilizzo di strumenti informatici e di comunicazione telematica. L'attività, funzionale al contrasto del proselitismo e alla prevenzione dei fenomeni di radicalizzazione, ha permesso di sviluppare un dedicato monitoraggio di circa **36.000** spazi web e alla rimozione di diversi contenuti inneggianti alla jihad.

In particolare, nel corso del 2020 sono proseguite le attività svolte dal personale del Servizio Polizia Postale e delle Comunicazioni all'interno dei tavoli di lavoro internazionali deputati al contrasto del Cyberterrorismo, con il coordinamento di Europol e con il coinvolgimento di tutte le Forze dell'Ordine degli Stati Membri, nonché dei rappresentanti dei maggiori *Internet Service Provider*, tra i quali soprattutto *Telegram* (che è stato il fornitore di servizi online che ha ricevuto la maggior parte delle richieste di rimozione e che ha allontanato dalla propria piattaforma una parte significativa degli attori chiave all'interno della rete di diffusione della propaganda IS).

Ed ancora, in tale contesto operativo, tra le principali attività svolte nel corso del 2020 dal personale del Servizio Polizia Postale e delle Comunicazioni si evidenzia la partecipazione all'azione denominata *"RAD – Referral Action Day on instructional material online"* svoltasi il 2 luglio 2020 e promossa da Europol al fine di procedere – tramite la segnalazione ai rispettivi *Provider* interessati – alla rimozione di ogni tipo di contenuto didattico in formato digitale utilizzato per la pianificazione e realizzazione di

attacchi terroristici.

Durante l’azione, gli esperti della Sezione Cyberterrorismo hanno rilevato, valutato e segnalato i contenuti online, inclusi manuali e *tutorials* su come preparare ed attuare attacchi terroristici, come selezionare gli obiettivi, come utilizzare le armi e costruire bombe. Alcuni dei documenti individuati contenevano anche le istruzioni su come rimanere anonimi online e su come evitare di essere individuati durante la pianificazione di un attacco terroristico.

All’esito delle attività è stato segnalato per la successiva rimozione un numero complessivo di **1724** url riconducibili a **113** piattaforme web utilizzate per la propaganda jihadista e n. **182** url su **67** piattaforme web nell’ambito dei contenuti riferibili all’area dell’ultradestra ed antagonista/anarchica.

. Per quanto concerne, invece, l’attività di contrasto, la Polizia Postale e delle Comunicazioni si avvale della possibilità prevista per legge di avviare attività sotto copertura, con l’impiego di profili o meglio di vere e proprie identità virtuali, costruiti ad hoc e fatti “maturare” nel tempo, gestiti da personale specializzato, con l’affiancamento dei mediatori linguistici e culturali.

Oltre alle suindicate attività sia preventive, sia di Polizia Giudiziaria connesse al terrorismo di matrice jihadista, la Polizia Postale e delle Comunicazioni ha registrato nel corso degli ultimi anni un notevole incremento nell’ambito del settore della propaganda online legata all’estremismo razzista e xenofobo, riscontrando un trend di forum e discussioni dedicate all’argomento in costante aumento.

Anche in tale contesto, dunque, sono stati indirizzati gli sforzi operativi del personale della Polizia Postale e delle

Comunicazioni, che lo scorso 3 novembre ha preso parte all'azione operativa denominata "JAD – Joint Action Day to combat hate postings", sotto il coordinamento di Europol e la partecipazione dell'unità specializzata del Centro europeo antiterrorismo (ECTC) e rappresentanti delle polizia di diversi Paesi europei, con l'obiettivo di contrastare la pubblicazione online di messaggi d'odio connotati da aspetti xenofobi, razzisti ovvero discriminatori.

L'attività è stata condotta a livello territoriale dalle DIGOS e dai Compartimenti Polizia Postale, con il coordinamento della Direzione Centrale della Polizia di Prevenzione e del Servizio Polizia Postale e delle Comunicazioni.

Nell'ambito delle attività di monitoraggio svolta dal **Compartimento Polizia Postale per il Lazio** ha svolto una rilevante attività di monitoraggio dei 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.

Nel contesto di tali monitoraggi il Compartimento di Roma segnalava un soggetto che organizzava una manifestazione in Roma con partenza da Massa Carrara, in violazione del DPCM in vigore. A seguito di tale segnalazione, veniva controllato e deferito all'Autorità Giudiziaria per violazione dell'art.650 cp;

La squadra Cyberterrorismo del Compartimento riscontrava altresì la presenza di un account che pubblicava all'interno dello stesso profilo fotografie di armi ed esplosivi. Dagli elementi contenuti all'interno del profilo è stato possibile identificare il detentore dell'account quindi procedere a perquisizione locale e personale ai sensi dell'art. 41 TULPS, accertando l'omessa custodia delle armi regolarmente dichiarate, che venivano ritirate.

Venivano infine individuati i profili di 93 soggetti, titolari di un account sulla piattaforma social network Facebook, presenti nella Banca Dati AFIS in quanto sottoposti a rilievi fotodattiloscopici come personaggi gravitanti nell'ambito dell' estremismo Islamico:

2. **COMMISSARIATO DI PS ONLINE**

Il portale del Commissariato di P.S. online è divenuto il punto di riferimento specializzato per chi cerca informazioni, consigli, suggerimenti di carattere generale, o vuole scaricare modulistica e fare segnalazioni.

Uno strumento agevole che consente al cittadino, da casa, dal posto di lavoro o da qualsiasi luogo si desideri, di entrare nel portale ed usufruire dei medesimi servizi di segnalazione, informazione e collaborazione che la Polizia Postale e delle Comunicazioni quotidianamente ed ininterrottamente offre agli utenti del web.

Di particolare importanza le segnalazioni giunte anche sul sito del Commissariato di P.S. on-line per i reati di cyberbullismo, perpetrati da studenti nei confronti di compagni di scuola e non, attraverso i social media, con atti denigratori e diffamatori. Alcune attività sono sfociate nell'emissione da parte dei Questori di provvedimenti di ammonimento anche al fine di responsabilizzare minori autori del reato.

FAKE NEWS

Nell'ambito del diversificato contesto operativo della Polizia Postale e delle Comunicazioni, particolare attenzione viene costantemente rivolta anche al fenomeno della "disinformazione", con un impegno ancor maggiore nel contesto emergenziale vissuto a causa della diffusione del virus Sars-Cov2: la crescente proliferazione delle cd. fake news, sovente caratterizzata da un potenziale impatto negativo sulla salute pubblica e sulla corretta ed efficace comunicazione

istituzionale ha imposto di innalzare i livelli di attenzione nell'ottica di un efficace contenimento del particolare fenomeno.

L'azione di contrasto attuata, rispetto alle varie fenomenologie delittuose che hanno caratterizzato la fase dell'emergenza Covid-19 (talora agevolate dalla diffusione di fale notizie e/o informazioni), è stata, quindi, realizzata non soltanto sotto il profilo della repressione dei reati tentati o consumati, ma anche nell'ottica di interventi di tipo preventivo, tesi a veicolare alla cittadinanza le informazioni utili per contenere ed impedire le condotte delittuose sopra richiamate.

In tale direzione, il potenziamento dell'operatività del Commissariato di PS online ha permesso di innalzare i livelli di interazione con i cittadini, i quali, in una situazione di emergenza sanitaria, hanno mostrato un accresciuto bisogno di strumenti idonei a garantire rapidi ed efficaci riferimenti istituzionali a cui poter indirizzare le proprie segnalazioni e le proprie preoccupazioni e da cui poter apprendere informazioni corrette, utili anche a prevenire il consumarsi di condotte delittuose.

Al riguardo, dall'inizio dell'emergenza COVID-19, sono stati individuati 136 eventi, riconducibili al fenomeno della disinformazione, rispetto ai quali è stato predisposto uno specifico alert funzionale alla veicolazione delle corrette informazioni.

ATTIVITA' DI PREVENZIONE

Parallelamente all'incremento dell'uso di strumenti telematici, sono cresciute le aspettative di sicurezza da parte del cittadino. La Polizia Postale e delle Comunicazioni è impegnata, ormai da diversi anni, in campagne di sensibilizzazione e prevenzione sui rischi e pericoli connessi all'utilizzo della rete internet, rivolte soprattutto alle

giovani generazioni.

Nello specifico si evidenzia la campagna educativa itinerante della Polizia Postale e delle Comunicazioni "***Una Vita da Social***", grazie alla quale sino ad oggi sono stati incontrati oltre **2milioni e mezzo di studenti sia nelle piazze che nelle scuole**, **220.000 genitori, 125.000 insegnanti** per un totale di **18.500 Istituti scolastici** e **350** città raggiunte sul territorio nazionale.

Nell'ottica della cennata azione di prevenzione il **Compartimento Polizia Postale per il Lazio** ha trattato oltre 2000 segnalazioni pervenute via e-mail nel cui contesto sono state fornite ai cittadini richiedenti informazioni utili, soprattutto, per prevenire possibili frodi. Di queste, oltre 50 segnalazioni anonime hanno riguardato 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 del Territorio.

Inoltre, nell'ambito della consueta azione di sensibilizzazione per la prevenzione dei rischi connessi alla navigazione in internet di adolescenti, gli operatori del Compartimento Polizia Postale e delle Comunicazioni del Lazio hanno effettuato incontri in 57 Istituti Scolastici della Regione, coinvolgendo quasi 8600 studenti, oltre 516 docenti e quasi 500 genitori, trattando argomenti come phishing, hacking, adescamento on line, truffe, furti di identità e cyberbullismo.

Controllo del territorio

Al fine di prevenire e contrastare i reati commessi nell'ambito del circuito postale, il Compartimento Polizia

Postale e delle Comunicazioni per il Lazio ha garantito 488 pattuglie sul territorio che hanno assicurato la vigilanza degli uffici postali della Regione, con particolare riferimento ai giorni in cui è previsto il pagamento delle pensioni.

Nell'ambito di tali attività di controllo del territorio è stato possibile **trarre in arresto nr. 2 soggetti colti in flagranza del reato di rapina in danno della banca Popolare della Puglia e Basilicata,** filiale di Frosinone. Un successivo supplemento di indagine ha inoltre consentito di attribuire ad uno dei due rei anche una rapina consumata presso l'ufficio Postale di Tecchiena di Alatri (FR).