Resoconto attività 2022
della Polizia Postale e delle Comunicazioni e del Centro Operativo Sicurezza Cibernetica – Campania, Basilicata e Molise

Nel 2022 la Polizia Postale è stata chiamata a far fronte a continue e sempre più evolute sfide investigative sulle 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, riconducibili sia a forme di fondamentalismo religioso che a forme di estremismo politico ideologico, anche in contesti internazionali.

CONTRASTO ALLA PEDOPORNOGRAFIA ONLINE E ABUSI SU MINORI IN RETE

In uno scenario nel quale la continua evoluzione tecnologica influenza ogni azione del nostro vivere quotidiano, lo sforzo della Polizia Postale e delle Comunicazioni nell'anno 2022 è stato costantemente indirizzato alla prevenzione e al contrasto della criminalità informatica in generale, con particolare riferimento ai reati in danno di minori.

Il **Centro Nazionale per il Contrasto alla Pedopornografia Online (C.N.C.P.O.)** nel 2022 ha confermato il suo ruolo di punto di riferimento e di coordinamento nazionale dei **Centri Operativi Sicurezza Cibernetica – COSC** della Polizia Postale nella lotta alla pedofilia e pornografia minorile online.

L'analisi dei dati relativi all'anno di riferimento ha confermato la lieve diminuzione dei casi trattati già evidenziata nella rilevazione di medio termine. La flessione negativa dei dati è stata riscontrata anche in riferimento al numero delle segnalazioni provenienti da organismi internazionali attivi nella protezione dei minori in rete. L'impegno profuso dalla Specialità si è concentrato nel reprimere episodi di particolare gravità, con l'effetto rilevabile di evidenziare un maggior numero di individui sottoposti a pene detentive.

Nell'ambito poi delle segnalazioni relative alla pubblicazione di contenuti pedopornografici su social network, si è evidenziato un fenomeno per il quale veniva intaccata la reputazione dei vari titolari di profili social attraverso la pubblicazione di materiale scabroso di natura pedopornografica con accessi abusivi massivi a profili privati di ignari cittadini e di persone dotate di rilevanza mediatica, politica o di altra natura.

La fine dell'emergenza sanitaria, con la progressiva ripresa delle attività nella direzione di un recupero della normalità, potrebbe aver contribuito a ridurre l'isolamento sociale, facendo rilevare nel 2022 una riduzione della circolazione globale di materiale pedopornografico su circuiti internazionali, che non ha però inciso sull'attività di contrasto.

Infatti, **è stato registrato un aumento dei soggetti individuati e deferiti per violazioni connesse ad abusi in danno di minori**.

In particolare, nell'ambito dell'attività di contrasto coordinata dal Centro sono stati trattati complessivamente **4.542 casi**, che hanno consentito di indagare **1.463 soggetti**, di cui **149 tratti in arresto** per reati connessi alla materia degli abusi tecnomediati in danno di minori, con un aumento di persone tratte in arresto di circa il **+8%** rispetto allo stesso periodo dell'anno precedente.

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 **25.696** siti, di cui **2.622** inseriti in black list e oscurati, in quanto presentavano contenuti pedopornografici.

PEDOPORNOGRAFIA E ADESCAMENTO ONLINE	**2021**	**2022***	**Variazione percentuale**
Persone indagate	1.419	1.463	**+3%**
Siti in Black List	2.543	2.622	**+3%**
* - dati rilevati il 27/12/2022			

Campania

Per quanto concerne la **Campania** i casi trattati in materia di **abusi su minori in rete** nel 2022 sono 101 e le indagini condotte hanno portato all'arresto di 20 persone (13 nel 2021), alla denuncia di 116 soggetti e a 139 perquisizioni.

Basilicata

Per quanto concerne la **Basilicata** i casi trattati in materia di **abusi su minori in rete** nel 2022 sono 4 e le indagini condotte hanno portato alla denuncia di 4 soggetti e a 4 perquisizioni.

Molise

Per quanto concerne ila **Molise** i casi trattati in materia di **abusi su minori in rete** nel 2022 sono 5 e le indagini condotte hanno portato alla denuncia di 1 soggetto e a 1 perquisizione.

ADESCAMENTO ONLINE

Nel periodo di riferimento sono stati trattati **424** casi per adescamento online: anche quest'anno la fascia dei preadolescenti (età 10-13 anni) è quella più coinvolta in interazioni sessuali tecnomediate, **229** rispetto al totale.

Continua a preoccupare il lento incremento dei casi relativi a bambini adescati di età inferiore ai 9 anni, trend che è diventato più consistente a partire dalla pandemia. Social network e videogiochi online sono i luoghi di contatto tra minori e adulti più frequentemente teatro delle interazioni nocive, a riprova ulteriore del fatto che il rischio si concretizza con maggiore probabilità quando i bambini e i ragazzi si esprimono con spensieratezza e fiducia, nei linguaggi e nei comportamenti tipici della loro età.

Campania

Per quanto concerne la **Campania**, i casi trattati in materia di **adescamento** nel 2022 sono 51 e le indagini condotte hanno portato all'arresto di 3 persone, alla denuncia di 51 soggetti e a 35 perquisizioni.

Molise

Per quanto concerne il **Molise**, i casi trattati in materia di **adescamento** nel 2022 sono 2.

CYBERBULLISMO

Si registra una leggera flessione anche dei casi di cyberbullismo che può essere interpretata come effetto della normalizzazione delle abitudini dei ragazzi: non si può escludere che il ritorno ad una vita sociale priva di restrizioni abbia avuto un'influenza positiva sulla qualità delle interazioni sociali, delle relazioni tra coetanei e che la costanza dell'opera di sensibilizzazione svolta dalla Polizia Postale, presso le strutture scolastiche, abbia mantenuto alta l'attenzione degli adulti e dei ragazzi stessi sulla necessità di agire responsabilmente e correttamente in rete.

Nel periodo di riferimento sono stati trattati **323** casi di cyberbullismo.

CYBERBULLISMO	**2021**	**2022***
Casi trattati vittime 0-9 anni	27	17
Casi trattati vittime 10-13 anni	112	87
Casi trattati vittime 14-17 anni	319	219
TOTALE	**458**	**323**
* - dati rilevati il 27/12/2022		

	2021	**2022***
Minori denunciati per Cyberbullismo	117	128
* - dati rilevati il 27/12/2022		

Campania

Per quanto concerne la **Campania**, i casi trattati in materia di **cyberbullismo** nel 2022 sono 24 (43 nel 2021) e le indagini condotte hanno portato alla denuncia di 6 minori (13 nel 2021).

Basilicata

Per quanto concerne la **Basilicata**, i casi trattati in materia di **cyberbullismo** nel 2022 sono 2 (3 nel 2021).

Molise

Per quanto concerne il **Molise**, i casi trattati in materia di **cyberbullismo** nel 2022 sono 5 (5 nel 2021).

REATI CONTRO LA PERSONA

A livello nazionale sono stati trattati i seguenti casi di reati contro la persona perpetrati online:

Reati contro la persona perpetrati OnLine[1]	2021	2022*
Casi trattati	10.297	9.278
Persone indagate	1.693	1.167
[1] – *Stalking* / diffamazione online / minacce / *revenge porn* / molestie / sextortion / illecito trattamento dei dati / sostituzione di persona / hate speech / propositi suicidari * - dati rilevati il 27/12/2022		

Per quanto concerne il territorio di competenza del C.O.S.C. Campania, Basilicata e Molise, si riportano i seguenti dati afferenti ai reati contro la persona:

CAMPANIA		
	2021	**2022**
Casi trattati	1942	2759
Persone indagate	63	56
Persone arrestate	9	4
Perquisizioni	21	34

BASILICATA		
	2021	**2022**
Casi trattati	190	278
Persone indagate	9	3
Perquisizioni	3	3

MOLISE		
	2021	**2022**
Casi trattati	135	146
Persone indagate	14	9
Perquisizioni	4	1

FOCUS SULLA SEXTORTION

È un fenomeno che di solito colpisce gli adulti in modo violento e subdolo, fa leva su piccole fragilità ed esigenze personali, minacciando, nel giro di qualche click, la tranquillità delle persone.

Recentemente le **sextortion** stanno interessando sempre più spesso vittime minorenni, con effetti lesivi potenziati: la vergogna che i ragazzi provano impedisce loro di chiedere aiuto ai genitori o ai coetanei di fronte ai quali si sentono colpevoli di aver ceduto e di essersi fidati di perfetti e "avvenenti" sconosciuti.

La sensazione di sentirsi in trappola che sperimentano le vittime è amplificata spesso dalla difficoltà che hanno nel pagare le somme di denaro richieste. Nel corso dell'anno sono stati trattati **130 casi,** la maggior parte dei quali nella fascia **14-17 anni,** più spesso in danno di vittime maschili.

Nel 2022 in **Campania** sono stati trattati 97 casi di **sextortion**, in **Basilicata** 56 e in **Molise** 3.

PROTEZIONE DELLE INFRASTRUTTURE CRITICHE INFORMATIZZATE

Nell'esercizio della propria missione istituzionale, il Servizio Polizia Postale e delle Comunicazioni - Organo del Ministero dell'interno per la sicurezza delle telecomunicazioni garantisce, fra l'altro, ai sensi dell'art. 7 bis DL 144 del 2005 e del DM 15 agosto 2017 - Direttiva sul riordino dei comparti di Specialità delle Forze di Polizia – la protezione delle infrastrutture critiche informatizzate del Paese.

Nell'attuale e particolare contesto internazionale, l'*escalation* delle tensioni geopolitiche connesse al conflitto in Ucraina continua ad avere significativi riverberi anche in materia di sicurezza cibernetica. Risultano, infatti, in corso campagne massive a livello internazionale dirette verso infrastrutture critiche, sistemi finanziari e aziende operanti in settori strategici quali comunicazione e difesa, tra le quali figurano campagne di *phishing*, diffusione di *malware* distruttivi (specialmente *Ransomware*), attacchi Ddos, campagne di disinformazione e *leak* di database. Inoltre, alcuni tra i più pericolosi gruppi di hacker criminali hanno deciso di schierarsi a favore della Russia, altri con l'Ucraina, prendendo di fatto parte al conflitto nel c.d. "dominio cibernetico".

In tal senso, come noto, il conflitto russo-ucraino ha comportato una recrudescenza nell'attività di attori ostili, connotati per l'esecuzione di attacchi ransomware – volti a paralizzare servizi e sistemi critici mediante la cifratura dei dati contenuti – campagne DDoS, volti a sabotare la funzionalità di risorse online e, soprattutto, attacchi di tipo ATP (Advanced Persistent Threat), condotti da attori ostili di elevato expertise tecnico, in grado di penetrare i sistemi più strategici mediante tecniche di social engineering o sfruttamento di vulnerabilità, al fine di garantirsi una persistenza silente all'interno dei sistemi a scopo di spionaggio o successivo danneggiamento.

La proliferazione di gruppi ostili, si è attuata poi mediante il ricorso a crew hacker di c.d. *crime as a service*, ordinariamente attive nel fornire supporto tecnologico ad attori criminali ed oggi sempre più contigue a gruppi di ascendenza statuale.

In particolare, il Servizio polizia postale ha implementato l'attività informativa e di monitoraggio ad ampio spettro, esteso anche al *dark web*, attivando canali di diretta interlocuzione dedicati allo scenario in atto con Europol, oltre che con Interpol e FBI, con l'obiettivo di elevare il livello di attenzione con particolare riguardo al settore economico/finanziario, tradizionalmente oggetto di interesse da parte di compagini criminali con connotazione *state sponsored*.

Il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC), attraverso dedicati *alert* ha diffuso indicatori di compromissione e avvisi di informazione di sicurezza alle infrastrutture informatiche dicasteriali, alle infrastrutture critiche nazionali e ai potenziali *target* di azioni ostili, individuati attraverso la permanente attività informativa assicurata dal Centro.

I Centri Operativi per la Sicurezza Cibernetica della Polizia Postale hanno svolto adeguati servizi di monitoraggio e analisi, condividendo ogni evidenza utile in relazione al quadro internazionale in parola.

L'attività del CNAIPIC del Servizio Polizia Postale e delle Comunicazioni, oltre agli approfondimenti investigativi, si è tradotta nell'analisi tecnica della minaccia, volta all'elaborazione di informazioni di sicurezza preventiva, nonché nel supporto operativo alle

infrastrutture attaccate, che hanno contribuito al ritorno alla piena operatività dei sistemi informatici colpiti.

Attacchi infrastrutture critiche ad istituzioni, aziende e privati	2021	2022*	Variazione percentuale
Attacchi rilevati	**5.434**	**12.947**	**+138%**
Persone indagate	**187**	**332**	**+78%**
Alert diramati	**110.524**	**113.226**	**+2%**
Richieste di cooperazione HTC	**60**	**77**	**+28%**
* - dati rilevati il 27/12/2022			

SEZIONE CYBERTERRORISMO

Nel corso degli ultimi anni, il continuo e vertiginoso incremento dell'utilizzo delle piattaforme di comunicazione online, social network e di applicazioni di messaggistica istantanea, ha determinato un'allarmante diffusione di contenuti propagandistici riconducibili al terrorismo, ad una platea pressoché illimitata, sia di matrice islamista (*jihadista, ISIS, Al Qaeda, Al Shabaab* ed altre articolazioni locali), sia di formazioni suprematiste di estrema destra (neonazismo, neofascismo, tifoserie strutturate), nonché di estrema sinistra (movimenti di lotta armata, anarco/insurrezionalisti, antagonisti).

Cyberterrorismo[1]	2021	2022*
Casi trattati	1.321	1.193
Persone indagate	80	66
Spazi virtuali monitorati	126.998	173.306
[1]- Estremismo internazionale religioso / estremismo razziale, antagonista ed anarchico * - dati rilevati il 27/12/2022		

In tale ambito, la Polizia Postale garantisce sia l'esecuzione di una costante attività di monitoraggio investigativo della rete e dei canali di messaggistica istantanea, per l'identificazione e il deferimento all'Autorità Giudiziaria dei responsabili della diffusione dei contenuti illeciti, sia un costante scambio informativo con la Direzione Centrale della Polizia di Prevenzione competente in materia di contrasto al terrorismo.

Trattandosi, in particolare, di un fenomeno di carattere transnazionale, sia per la natura internazionale del fenomeno che per la stessa connaturata struttura della rete, risulta imprescindibile l'attivazione efficiente degli strumenti della cooperazione sovranazionale, soprattutto per la condivisione di informazioni che, collegate a situazioni peculiari interne, riescono ad apportare un indiscusso valore aggiunto alle attività di prevenzione messe in atto dalle diverse forze di polizia nazionali.

In ambito europeo, proprio al fine di garantire la cooperazione internazionale, il Servizio Polizia Postale e delle Comunicazioni rappresenta il punto di contatto nazionale dell'Internet Referral Unit (IRU) di Europol, Unità preposta a ricevere dai Paesi Membri le segnalazioni relative ai contenuti terroristici diffusi in rete e di orientarne l'attività.

In tale ambito, l'attività di monitoraggio del web effettuata dalla Specialità ha permesso di riscontrare, in primis, come la diffusione di contenuti propagandistici jihadisti, nel corso del tempo, abbia subito un sensibile peggioramento "qualitativo", determinato sia dal ridimensionamento del Califfato sul territorio, sia dalle perdite di tecnici e social media manager cui era devoluto l'incarico di gestire la propaganda, nonché per l'utilizzo sempre più frequente dell'Intelligenza Artificiale sulle principali piattaforme web, per la scansione (e rimozione) dei contenuti pubblicati dagli utenti.

Sul punto, tra le attività effettuate dalla Specialità si segnala quella effettuata dal Centro Operativo per la Sicurezza Cibernetica e dalla DIGOS di Perugia, all'esito della quale un cittadino marocchino di 54 anni è stato espulso dal territorio nazionale, in quanto autore di una prolifica attività propagandistica sul social network Facebook realizzata attraverso numerosi post e commenti a sostegno dei "fratelli musulmani" e del Jihad, specificamente della Palestina contro Israele, nel corso della quale si è definito un "mujahidin" pronto ad aiutare la causa.

In analogia a quanto sin qui evidenziato con riferimento alla propaganda jihadista, anche nell'ambito dei fenomeni di radicalizzazione online legati all'ideologia neofascista e xenofo/razziale, il web si conferma lo strumento strategico per la diffusione della propaganda delle ideologie estremiste e violente, nonché per il reclutamento di nuovi combattenti, il finanziamento, lo scambio di comunicazioni riservate nella pianificazione degli attentati e di rivendicazione degli stessi.

Appare opportuno evidenziare come il movimento "suprematista" si basi su una importante attività di propaganda di dottrine ideologiche come il neonazismo, il razzismo, l'identitarismo e l'etnocentrismo, che avviene soprattutto all'interno di piattaforme di comunicazione online "riservate", diverse dai principali social network.

La costante attività di monitoraggio informativo ed investigativo ha permesso di accertare come nel corso degli ultimi mesi si sia stato registrato un notevole incremento dei trend e delle discussioni all'interno di chat in diverse piattaforme; si passa dai tradizionali gruppi Facebook (molti dei quali risultano essere già stati bloccati) a social meno noti, come Reddit, fino a piattaforme come 8chan, vk.com (Vkontakte), nonché Telegram, privilegiando tutte quelle piattaforme che per la propria policy garantiscono l'anonimato e rendono più complicata l'identificazione degli autori dei messaggi.

Alla luce di quanto premesso, appare opportuno evidenziare come gli operatori della Specialità abbiano intensificato le attività di monitoraggio proprio in tali contesti e, in raccordo con la Direzione Centrale della Polizia di Prevenzione, abbiano avviato numerose attività investigative, con il deferimento alle competenti Autorità Giudiziarie dei soggetti identificati – anche attraverso attività sotto copertura e perquisizioni – quali autori dei messaggi connotati dalla discriminazione razziale, etnica e religiosa.

Tra le numerose attività investigative espletate dalla Specialità nel corso del 2022, si segnala quelle che ha condotto al deferimento alla competente A.G. da parte del Centro Operativo di Milano di un uomo di 60 anni, residente nella provincia di Como, quale utilizzatore di un account Twitter, autore di due messaggi contenenti gravi minacce nei confronti del Capo dello Stato.

Ed ancora, appare opportuno evidenziare quella che ha permesso di identificare l'amministratore di un canale Telegram – caratterizzato dalla presenza di numerosi messaggi connotati da ideologie antisemite, da teorie complottiste contrarie ai vaccini, dall'incitamento alla violenza nel corso di manifestazioni pubbliche, nonché per la presenza di gravi minacce nei confronti di varie cariche istituzionali, tra le quali il Presidente del Consiglio Mario Draghi, il Presidente U.S.A. Joe Biden - in un cinquantenne originario della provincia di Napoli, ma da tempo domiciliato in Germania per motivi professionali.

Sulla base degli accertamenti compiuti, l'amministratore del canale Telegram monitorato, è stato fermato al momento del suo ingresso nel territorio nazionale, proveniente dalla Germania, proprio per partecipare ad una manifestazione no-vax in programma nella città di Roma, per la quale aveva esortato i componenti della chat, oltre 21.418 iscritti, ad armarsi e a sopraggiungere in gran numero, fornendo precise indicazioni volte a eludere le attività di prevenzione e controllo delle Forze dell'Ordine.

L'uomo è stato deferito alla competente Autorità Giudiziaria dal personale del Centro Operativo per la Sicurezza Cibernetica di Napoli che, unitamente alla locale DIGOS, ha dato esecuzione al decreto di perquisizione informatica, emesso nei suoi confronti dalla Procura della Repubblica presso il Tribunale del capoluogo partenopeo, riscontrando utili tracce informatiche in merito alla pubblicazione dei messaggi di propaganda e istigazione a delinquere per motivi di discriminazione razziale ed etnica.

Infine, considerando il carattere transnazionale che spesso connota le attività investigative in argomento, risulta imprescindibile l'attivazione efficiente degli strumenti della cooperazione sovranazionale, soprattutto per la condivisione di informazioni che, collegate a situazioni peculiari interne, riescono ad apportare indiscusso valore aggiunto alle attività di prevenzione messe in atto dalle diverse forze di polizia nazionali. In ambito europeo, il Servizio Polizia Postale e delle Comunicazioni è il punto di contatto nazionale dell'Internet Referral Unit (IRU) di Europol, Unità preposta a ricevere dai Paesi Membri le segnalazioni relative ai contenuti di propaganda terroristica diffusi in rete e di orientarne l'attività.

Lo scambio delle informazioni tra Paesi Membri viene effettuato attraverso l'utilizzo di specifiche piattaforme tecnologiche appositamente create in ambito IRU a supporto del monitoraggio e delle indagini in materia di terrorismo in Internet.

Proprio nell'ambito della lotta ai crimini ispirati dall'odio, nello scorso mese di aprile, la Polizia Postale ha partecipato alla giornata di azione congiunta a livello dell'U.E., sostenuta da *Europol,* che, oltre l'Italia, ha coinvolto 10 Paesi (Austria, Bulgaria, Francia, Germania, Lituania, Lussemburgo, Norvegia, Portogallo, Romania e Spagna).

Le attività investigative hanno permesso di identificare in tutta Europa 176 persone in relazione alla diffusione online di messaggi di incitamento all'odio xenofobo-razziale, nonché istigazione alla violenza.

Nella circostanza, le Forze dell'ordine degli Stati membri hanno anche lavorato insieme per far aumentare la consapevolezza di individui e gruppi che Internet non rappresenta un "vuoto giuridico", dando così un chiaro segnale alle persone che diffondono odio violento online che le azioni investigative congiunte saranno sempre più frequenti e consistenti.

Da ultimo, lo scorso 15 dicembre, la Polizia Postale e la D.C.P.P. hanno partecipato ad una seconda giornata congiunta, coordinata dall'European Union Internet Referral Unit (EU IRU) di Europol, nell'ambito del *Referral Action Day* (RAD) contro i contenuti violenti dell'estremismo di destra e del terrorismo online. L'attività ha coinvolto anche le Unità

specializzate di 14 Paesi, tra cui 13 Stati membri dell'Unione Europea e un Paese non appartenente all' UE.

Le autorità partecipanti sono state coinvolte nell'individuazione e nella segnalazione di contenuti terroristici ai fornitori di servizi online e nel valutare le loro risposte. Le attività hanno portato alla segnalazione di **831 elementi a 34 piattaforme** interessate. Il materiale in questione include contenuti vietati prodotti da organizzazioni estremiste di destra o in favore di queste, nonché contenuti diffusi relativi ad attacchi terroristici motivati dall'estremismo violento.

Tali materiali includono *livestream*, manifesti, rivendicazioni e celebrazioni di attentati. L'estremismo violento è ancora una preoccupazione crescente dopo i fatti di Bratislava (Slovacchia) e Buffalo (USA).

Gli autori di questi attentati facevano parte di comunità *online* transnazionali e si sono ispirati ad altri estremisti di destra violenti e terroristi. Nei loro manifesti, i terroristi hanno evidenziato il ruolo centrale della propaganda *online* nei processi di radicalizzazione. Questo dimostra come l'abuso di internet continui ad essere centrale per l'avvio di percorsi di radicalizzazione e reclutamento della destra violenta.

Dal primo *Referral Action Day* dedicato a questo tipo di contenuti online nel 2021, la minaccia rappresentata dall'estremismo violento e dal terrorismo è ancora in aumento.

I RAD consolidano gli sforzi delle forze dell'ordine per contrastare la creazione e la diffusione di propaganda estremista e terroristica online. Durante le attività coordinate, i partecipanti segnalano i contenuti legati al materiale di propaganda ai fornitori di servizi online invitandoli a valutare e rimuovere i contenuti che violano i loro termini di servizio. Le piattaforme sono invitate a rafforzare i loro protocolli di moderazione per evitare questo tipo di abuso in futuro.

REATI CONTRO IL PATRIMONIO ONLINE

Nell'ambito delle competenze della Polizia Postale si segnala il rafforzamento dell'attività di prevenzione attraverso il monitoraggio attivo della rete e un'articolata attività di contrasto alle **truffe online** con **3541 persone deferite all'Autorità Giudiziaria**, in particolare nel settore dell'e-commerce e *market place.*

Truffe OnLine	**2021**	**2022***	**Variazione percentuale**
Casi trattati	15.083	15.508	**+3%**
Persone indagate	3.403	3.541	**+4%**
Somme sottratte	€ 73.245.740	€ 115.457.921	**+58%**
* - dati rilevati il 27/12/2022			

Nell'ambito delle truffe sul web anche nel corso del 2022, importante l'incremento degli illeciti legati al fenomeno del **trading online** (**3.020** ***i casi trattati, 130 le persone)***, con l'aumento del numero di portali che propongono programmi speculativi, apparentemente redditizi, e l'utilizzo di tecniche molto sofisticate per contattare le vittime. L'attività investigativa, qualora la denuncia sia tempestiva, prevede l'immediata attivazione dei canali di Cooperazione Internazionale di Polizia, con la richiesta del blocco urgente delle somme versate e l'espletamento di accertamenti sui flussi finanziari normalmente destinati all'estero.

Proprio per dare maggior impulso alle indagini che vedono coinvolti cittadini stranieri,

Il Servizio Polizia Postale, nel corso dell'anno 2022, ha attivato **260 richieste di cooperazione internazionale** attraverso il canale Europol che, in più di un'occasione, si sono rivelate determinanti per l'individuazione degli autori dei reati investigati.

La Polizia Postale è stata impegnata anche nell'individuazione di proposte di vendita online di prodotti contraffatti o all'utilizzo illecito di segni distintivi dei marchi registrati, per la tutela del c.d. *italian sounding.*

Il monitoraggio di siti e spazi *web* (blog, gruppi social e siti dedicati) dediti a giochi e scommesse clandestine è un'altra attività operativa particolarmente seguita dalla Polizia Postale e delle Comunicazioni, sia per contrastare la diffusione irregolare o illegale, che per tutelare gli interessi dei consumatori, specie se minori d'età: numerosi sono i siti con sedi legali presso paesi esteri, che operano in Italia anche se privi della prevista autorizzazione per poter esercitare legalmente la raccolta di scommesse.

Nel corso del 2022 sono state implementate anche le attività di monitoraggio relative alla vendita online di tabacchi, sigarette elettroniche e liquidi da inalazione in rete, su siti sprovvisti delle relative autorizzazioni da parte dell'Agenzia delle Dogane e Monopoli.

L'anno 2022 ha vissuto, subendoli, gli strascichi dell'emergenza sanitaria da Covid19, che ha comportato il cambiamento radicale di alcune abitudini di vita consolidate. La sostituzione della socializzazione diretta con quella telematica e lo svolgimento dell'attività lavorativa non in presenza, imposti dall'avvio della pandemia fin dal 2020, si sono, in parte, stabilizzati, aprendo la strada a nuove consuetudini: molte aziende hanno proseguito con forme di telelavoro e *smartworking*, contribuendo a incrementare la frequenza di navigazione in rete da parte dei soggetti adulti anche attraverso *devices* quali *tablet*, *smartphone*, pc molto spesso utilizzati anche per scopi personali a scapito della sicurezza.

Nel solco di questi cambiamenti si è registrato un aumento dei reati informatici che ha raggiunto livelli altissimi, mettendo in luce come il crimine post pandemia nel nostro Paese stia cambiando radicalmente.

Il settore del *financial cybercrime* rappresenta un bacino molto remunerativo ed appetibile sfruttato da molte organizzazioni criminali, anche estere, come veicolo per finanziare le proprie attività illecite, il più delle volte attraverso l'utilizzo di sofisticate tecniche di *social engineering* per manipolare le vittime e indurle a fornire informazioni riservate.

Le conseguenze di un attacco riuscito possono essere drammatiche e avere effetti devastanti non solo su singoli utenti o investitori, ma anche con riverberi negativi per ciò che concerne piccole e medie imprese, con ingenti perdite economiche e danni d'immagine difficilmente quantificabili.

Nel settore del contrasto al *financial cybercrime*, il fenomeno dei "*money mules*" rappresenta senz'altro una delle modalità più frequenti e consolidate per realizzare frodi online: con la funzione di "teste di legno" cibernetiche, personalità di dubbia moralità si prestano ad essere l'ultimo anello della catena attraverso il quale i criminali monetizzano i proventi del reato. La diffusione di questa modalità e il numero dei soggetti che si prestano a svolgere tale funzione criminale sono in costante crescita e rappresentano ormai una realtà criminale quasi endemica in tutto il mondo.

Anche il 2022, inoltre, è stato caratterizzato dalla crescita dell'interesse per le ***Cryptovalute***: i cittadini italiani, anche con bassa scolarizzazione informatica, sono sempre più frequentemente attratti dagli investimenti in ***Cryptovalute***, con la speranza di realizzare i facili e veloci guadagni pubblicizzati.

Quello delle *Cryptovalute* costituisce un mondo eterogeneo e virtuale, peraltro, non dissimile da quello reale. In tale contesto sono realizzate attività investigative finalizzate a

fermare i tentativi di *phishing* verso i ***Wallet*** che le contengono: i truffatori informatici agganciano le vittime attraverso richieste di natura tecnica, su chat ufficiali o semi ufficiali, con la promessa di risolvere i loro problemi gestionali previa cessione delle chiavi private, che permettono la movimentazione delle Crypto (cd. SEED), in realtà queste consentono ai malfattori di prendere il pieno possesso del *Wallet* e di impadronirsi del contenuto.

Forte anche l'impegno per contrastare il fenomeno del riciclaggio perpetrato attraverso la conversione delle somme frodate in *Cryptovalute*, sono state infatti coordinate dal Servizio Polizia Postale diverse attività investigative che hanno visto truffe informatiche ad alto contenuto tecnico conosciute come le BEC, le CEO fraud, *Vishing*, *phishing* tentare di realizzare i proventi criminali inviando le somme sottratte tramite bonifico bancario ad *exchange* di *cryptovalute* non collaborativi con la Polizia, convertendo la valuta ufficiale in *Bitcoin* o *Ethereum*. Tale procedimento consente facilmente lo spostamento e spacchettamento delle somme, in attesa di fare *cashout*.

Per tale ragione è stata intensificata la collaborazione con le grandi società di Exchange di Crypto per i report operativi e per il congelamento delle somme sottratte, così come è stata intensificata anche l'analisi delle transazioni *Crypto* con la collaborazione degli specialisti di Europol.

La mancanza di confini geografici in Internet consente sempre più frequentemente la formazione di gruppi criminali con nazionalità eterogenee ed è questo che caratterizza ormai quasi l'intero panorama dei reati commessi attraverso le nuove tecnologie.

In Italia sono state **frodate 156 grandi, medie e piccole imprese**, per un ammontare complessivo di **oltre 20 milioni di euro** di profitti illeciti, dei quali oltre **4 milioni** sono stati recuperati in seguito all'intervento della Polizia Postale e delle Comunicazioni.

In merito ai fenomeni di *phishing, smishing e vishing,* tecniche utilizzate per carpire illecitamente dati personali e bancari, per operare sui sistemi di *home banking*, sono state **identificate ed indagate 853 persone (+9% rispetto all'anno precedente).**

Frodi Informatiche	**2021**	**2022***	**Variazione percentuale**
Persone indagate	779	853	**+9%**
Somme sottratte	€ 33.258.422	€ 38.678.134	**+16%**
* - dati rilevati il 22/12/2022			

Per quanto concerne il territorio di competenza del C.O.S.C. Campania, Basilicata e Molise, si riportano i seguenti dati afferenti ai reati contro il patrimonio online:

CAMPANIA		
	2021	**2022**
Casi trattati	3634	2603
Persone indagate	361	283
Persone arrestate	15	9
Perquisizioni	137	193
Somme recuperate in Euro	794.547	213.594

BASILICATA		
	2021	**2022**
Casi trattati	674	575
Persone indagate	14	9
Perquisizioni	7	1
Somme recuperate in Euro	4.003	2.000

MOLISE		
	2021	**2022**
Casi trattati	572	426
Persone indagate	55	135
Perquisizioni	8	2
Somme recuperate in Euro	108.444	16.836

COMMISSARIATO DI P.S. ONLINE

L'uso crescente delle nuove tecnologie ha reso necessario lo sviluppo e il potenziamento di nuovi strumenti di comunicazione che consentissero alla Polizia di Stato di mettersi in contatto diretto con gli utenti del *web*.

In tale ottica, il portale del Commissariato di PS online ha permesso al cittadino, abituato ormai a utilizzare la rete internet per svolgere le principali attività quotidiane, di rivolgersi agli agenti della Polizia Postale in qualsiasi momento e ovunque si trovi. Attraverso il computer, l'utente può segnalare comportamenti che giudica illeciti e chiedere aiuto per superare difficoltà e problematiche, anche nei casi in cui potrebbe essere fonte di disagio rappresentarle di persona.

La facilità con cui il cittadino ha interagito con la piattaforma dedicata, ha reso possibile raccogliere le segnalazioni di quegli utenti che, mossi da spirito altruistico e di collaborazione, si sono rivolti alla Polizia Postale in un'ottica di sicurezza partecipata - nella sua declinazione online - fornendo utili evidenze su fenomeni emergenti potenzialmente lesivi, così contribuendo, in termini di efficace prevenzione, ad evitare che altri internauti potessero cadere nelle trappole della Rete.

L'esigenza di innalzare al massimo i livelli dell'azione preventiva ha imposto di introdurre una nuova sezione, dedicata agli *alert*, dove vengono raccolti e pubblicati gli "avvisi agli utenti" che, proprio perché costantemente aggiornati e facilmente raggiungibili, costituiscono un efficace strumento di autotutela messo a disposizione del cittadino.

Tra i fenomeni riscontrati con maggior frequenza nell'anno 2022 annoveriamo, a titolo esemplificativo, i furti di *account social*, le estorsioni a sfondo sessuale, il *phishing* ai danni di correntisti di istituti bancari, le proposte di falsi investimenti online, nonché falsi siti di vendita di quei prodotti che, in un determinato contesto temporale, risultano essere maggiormente richiesti sul mercato.

Le segnalazioni che richiedono l'intervento tempestivo del Commissariato di PS online sono molteplici. Emblematico è quanto avvenuto lo scorso 18 marzo, quando è giunta la richiesta di aiuto di una figlia preoccupata per la madre, vittima di una truffa sentimentale.

In particolare, la donna è stata contattata attraverso un noto social network da un uomo dalle maniere gentili che ha iniziato a corteggiarla con insistenza fino a farla innamorare. Dopo aver conquistato la fiducia della donna, il truffatore, confidandole di avere una figlia gravemente malata, che necessitava di cure molto costose alle quali non riusciva a far fronte, le ha richiesto un sostanzioso aiuto economico. La vittima, particolarmente colpita dalla triste vicenda, ha iniziato a inviare a più riprese ingenti somme di denaro sino a dilapidare il suo intero patrimonio.

Tutti i tentativi esperiti dai familiari della donna per farle capire di essere caduta vittima di un raggiro, sono risultati vani.

A quel punto, a seguito della segnalazione, il poliziotto del Commissariato di PS online, contattando la donna, è riuscito a farle comprendere che la persona che credeva essere il suo amato era in realtà un abile truffatore.

Grazie a questo intervento, la donna, oramai consapevole di quanto le era accaduto, ha interrotto la relazione e trovato il coraggio di sporgere denuncia.

Sul sito, inoltre, giungono segnalazioni da parte di utenti che si trovano in situazioni di pericolo o che minacciano gesti estremi; in tali circostanze, ai poliziotti della sala operativa del Commissariato di PS online è richiesto un tempestivo e coordinato intervento che coinvolge gli uffici territoriali delle Questure interessate dall'evento.

Lo scorso 19 gennaio, ad esempio, il personale del Commissariato ha gestito una segnalazione proveniente da un ragazzo che aveva manifestato l'intenzione di togliersi la vita dopo essere stato vittima di un'estorsione sessuale.

Il poliziotto che ha preso in carico la segnalazione ha immediatamente contattato telefonicamente il giovane che si è mostrato inizialmente reticente, timoroso e particolarmente spaventato, rifiutando di fornire indicazioni utili alla sua localizzazione.

Intuendo il suo grave disagio, e nonostante la ritrosia dimostrata dal ragazzo, l'operatore è riuscito ad instaurare un rapporto di empatia e fiducia col suo giovane interlocutore convincendolo a non commettere gesti estremi.

Il poliziotto ha intrattenuto il ragazzo al telefono per consentire agli operatori della Sala di esperire tutti gli accertamenti necessari per identificarlo e, una volta geolocalizzato, con l'ausilio di una pattuglia è stato possibile prestargli l'assistenza necessaria.

Gli interventi finalizzati alla prevenzione di **intenti suicidari** da parte di utenti dei vari social network, segnalati attraverso il Commissariato di P.S. online **sono stati 64.**

L'analisi delle oltre **100.000** segnalazioni ricevute dal sito del Commissariato di PS online nell'anno 2022, ha evidenziato che in molti casi gli internauti sconoscono e/o non adottano quelle piccole e necessarie accortezze di *cyber hygiene* che consentirebbero loro di prevenire e limitare la maggior parte degli attacchi informatici e il perpetrarsi di attività delittuose.

Per questo motivo, è stata introdotta sul sito una specifica sezione con cui vengono veicolate al cittadino pillole di sicurezza informatica, funzionali a ridurre al minimo i rischi legati all'uso di dispositivi informatici.

La popolarità del sito è avvalorata dal numero degli accessi che sono stati, nel periodo di riferimento, oltre **42.200.000**.

Nella costante ricerca di nuove e incisive strategie di comunicazione per fornire ad un'utenza sempre più ampia, si è passati da una comunicazione verso il cittadino a una interazione con il cittadino.

ATTIVITÀ DI PREVENZIONE

La Polizia Postale se da un lato svolge un'incisiva attività di repressione dei reati informatici, dall'altro lato svolge un'importante azione preventiva a tutela dei minori, soprattutto per quanto concerne il fenomeno del cyberbullismo e di tutte le forme di prevaricazione online, fenomeni che destano grande allarme sociale.

Tra le iniziative educative si riporta il coinvolgente format teatrale itinerante e in streaming **#cuoriconnessi** che ha coinvolto oltre 270mila studenti sul territorio nazionale.

Di rilievo è anche la campagna educativa itinerante di sensibilizzazione e prevenzione sui rischi e pericoli legati ad un uso non corretto della rete internet da parte dei minori denominata *Una vita da social*.

L'iniziativa, arrivata quest'anno alla sua X edizione, ha coinvolto oltre **2milioni e 800mila studenti,** attraverso il truck didattico multimediale della Polizia Postale, e ha proseguito la sua attività itinerante in Italia e all'estero.

Il progetto si cala nella filosofia dei giovani interlocutori, interagendo con un linguaggio comunicativo semplice ma esplicito, adatto a tutte le fasce di età, coinvolgendo così dai più piccoli ai docenti ai genitori, con la finalità di combattere la violenza e la prevaricazione dei giovani bulli.

L'impegno profuso dagli specialisti della Polizia Postale nell'azione di sensibilizzazione e informazione ha consentito, nell'anno appena trascorso, di realizzare incontri con docenti e genitori in oltre 2.800 istituti scolastici e di coinvolgere oltre **820mila** studenti.

Per quanto concerne la **Campania**, nel 2022 le attività di prevenzione in ambito scolastico hanno interessato 35.791 studenti, 2.881 docenti, 1.640 genitori e 214 istituti scolastici di vario ordine e grado.

Per quanto concerne il **Molise**, nel 2022 le attività di prevenzione in ambito scolastico hanno interessato 2.495 studenti, 210 docenti, 30 genitori e 30 istituti scolastici di vario ordine e grado.

Per quanto concerne la **Basilicata**, nel 2022 le attività di prevenzione in ambito scolastico hanno interessato 296 studenti, 25 docenti, 100 genitori e 10 istituti scolastici di vario ordine e grado.

ATTIVITA' DI FORMAZIONE INNOVAZIONE E RICERCA NEL SETTORE DELLE TECNOLOGIE ICT E DI REALIZZAZIONE DEL CERT MINISTERO DELL'INTERNO

Nel corso dell'anno 2022, la Polizia Postale e delle Comunicazioni ha proseguito nell'attività di collaborazione con diverse Istituzioni Scientifiche ed Enti di Ricerca volta ad individuare e valorizzare nuove tecniche e metodologie di lavoro nel contesto info-investigativo. In tal senso, di significativa rilevanza è la pianificazione di percorsi formativi di settore, con particolare riferimento alle tecnologie emergenti (5G, blockchain, IoT, AI) ed al complesso mondo dei sistemi criptati ed al loro dilagante utilizzo criminale.

Di assoluta importanza è stata l'attività di progettazione ed alta formazione specialistica finalizzata all'avvio del CERT (Computer Emergency Response Team) – Ministero Interno. Tale costituendo organismo, che opererà sotto l'egida della nuova Direzione Centrale per la Polizia Scientifica e la Sicurezza Cibernetica, sarà chiamato a svolgere un'efficace attività di presidio e risposta interdipartimentale contro incidenti informatici, coordinando le attività di contenimento e ripristino, per la prevenzione e la gestione degli attacchi cibernetici, delle reti e dei sistemi informativi del Ministero dell'Interno.

Si è dato avvio ad una formazione specialista di altissimo profilo a beneficio degli operatori già impegnati nello specifico contesto.

PRINCIPALI ATTIVITÀ DI POLIZIA GIUDIZIARIA SVOLTE DAL CENTRO OPERATIVO PER LA SICUREZZA CIBERNETICA – CAMPANIA, BASILICATA E MOLISE

OPERAZIONE BLACK ROOM - L'attività di indagine è stata condotta dagli investigatori partenopei in modalità *undercover* e ha consentito di smantellare una rete di utenti che sulla nota piattaforma Telegram gestiva la compravendita di materiale prodotto mediante lo sfruttamento sessuale di minori anche di tenera età.

Gli operatori, dopo essersi introdotti in alcuni canali di condivisione del materiale illecito, sono riusciti ad instaurare un rapporto di fiducia con alcuni interlocutori che si mostravano interessati allo scambio o alla cessione in cambio di somme di denaro che variavano in base all'età delle minori vittime degli abusi.

L'attenzione degli investigatori si è focalizzata in modo particolare sulla presenza di alcuni gruppi chiusi, in cui veniva divulgato una grande quantità di materiale pedopornografico, ai quali potevano accedere soltanto gli utenti ritenuti affidabili dagli amministratori previo pagamento di una somma di denaro che abilitava all'iscrizione al gruppo.

L'analisi delle tracce informatiche lasciate in rete dagli internauti e la ricostruzione meticolosa dei flussi finanziari hanno consentito di identificare 26 soggetti, residenti in 9 diverse regioni italiane, destinatari dei decreti di perquisizione emessi dalla Procura di Napoli.

Sono state, quindi, eseguite contestualmente le perquisizioni su tutto il territorio nazionale, ad esito delle quali sono stati tratti in arresto 6 soggetti e denunciati in stato di libertà 20 persone per commercio, diffusione e detenzione di materiale pedopornografico.

STALKING E SEXTORTION - Un'articolata attività di indagine condotta dalla Polizia Postale e delle Comunicazioni di Napoli ha consentito di eseguire un'ordinanza cautelare con la quale è stata disposta la misura coercitiva della custodia cautelare in carcere nei confronti di una donna, cinquantunenne, residente nella provincia di Caserta, ritenuta responsabile di stalking e sextortion (estorsione a sfondo sessuale) ai danni di diversi uomini.

La donna attraverso dei falsi profili creati sul social network Facebook, utilizzando foto di donne avvenenti, entrava in contatto con le vittime, per lo più uomini residenti nella provincia di Pescara, con le quali instaurava vere e proprie relazioni virtuali nel corso delle quali chiedeva ed otteneva l'invio di immagini intime dei suoi interlocutori.

Una volta entrata in possesso di tali immagini iniziava a minacciare le vittime di diffonderle a parenti e amici qualora non le avessero pagate delle somme di denaro.

Una delle vittime, spinta dal timore delle possibili conseguenze della diffusione delle proprie immagini intime ed esasperata delle condotte persecutorie di cui era oggetto, è stata costretta a consegnare la somma di 3.000 Euro.

Nei confronti degli uomini che decidevano di interrompere la relazione virtuale intrattenuta con la donna iniziava una vera e propria attività persecutoria realizzata mediante la diffusione on line delle immagini dal contenuto sessualmente esplicito e con delle continue diffamazioni e minacce inoltrate sia attraverso dei profili social creati ad hoc sia mediante telefonate sulle utenze delle vittime e dei familiari delle stesse.

Sulla base dei dati investigativi acquisiti veniva poi eseguita una perquisizione presso l'abitazione dell'indagata durante la quale venivano raccolti ulteriori e decisivi elementi di prova che consentivano all'Autorità Giudiziari di adottare il provvedimento cautelare.

RISSA SALERNO - Su disposizione della Procura della Repubblica presso il Tribunale per i Minorenni, la Squadra Mobile di Salerno, la Sezione di Polizia Giudiziaria di questo Ufficio e la Polizia Postale di Salerno hanno dato esecuzione a 15 ordinanze di custodia cautelare a carico di minori, delle quali 10 provvedimenti di custodia presso Istituto Penitenziario Minorile ed altre 5 di collocamento in comunità disposte dal Giudice per le Indagini Preliminari presso il Tribunale per i Minorenni di Salerno, per i gravi fatti relativi ad una violenta rissa che si sviluppava, in data 15 maggio u.s., a lungo ed in più luoghi, per tutto il centro nel centro della città di Salerno, durante un classico sabato della "movida" giovanile. I fatti per la loro ampiezza e gravità mettevano a repentaglio la stessa incolumità delle moltissime persone che quel giorno, pacificamente, affollavano le strade cittadine. La grave

vicenda oggetto d'indagine, in particolare, riguardava lo scontro tra due opposti gruppi di giovani che si erano affrontati colpendosi anche con bastoni, mazze, tirapugni e coltelli tanto che due dei corrissanti venivano attinti da fendenti in prossimità di organi vitali. A seguito di laboriose indagini coordinate da questo Ufficio e svolte dai suddetti organi di p.g. con grande abnegazione e professionalità, e, in particolare, attraverso la capillare visione delle immagini videoregistrate da telecamere installate presso alcuni esercizi commerciali presenti nelle aree in cui si erano verificati i fatti, si risaliva all'identità di alcuni dei ragazzi, oggi tratti in arresto, coinvolti nella violenta rissa. A seguito di tali accertamenti, venivano disposte, nei confronti di tali minori, perquisizioni domiciliari, nel corso delle quali venivano reperiti e sequestrati, a riscontro delle prime risultanze, alcuni indumenti del tutto coincidenti con quelli visibili dai filmati che avevano ripreso alcune fasi della rissa, nonché alcuni strumenti atti ad offendere.

Inoltre si procedeva al sequestro di alcuni telefoni cellulari in uso ai suddetti minori. E grazie alla attività investigativa effettuata proprio sul contenuto di tali apparecchi, si è giunti alla compiuta identificazione dei 15 giovani oggi tratti in arresto, alla ricostruzione dei fatti e delle cause che hanno fatto scatenare la furia dei due opposti gruppi.

In particolare, emergeva che la violenta rissa del 15 maggio 2022 trovava spiegazione in un'acerrima rivalità tra due opposti gruppi di giovani che da tempo si fronteggiano nella città di Salerno al fine di affermare secondo logiche tipiche da "gang" il proprio predominio sul territorio.

Così, su richiesta di questa Procura, il Giudice, ritenuta la sussistenza di gravi indizi di colpevolezza in relazione alle imputazioni di rissa aggravata per tutti i 15 indagati, e tentativo di omicidio per 10 di loro, ha adottato le misure cautelari oggi eseguite, con la precipua finalità di salvaguardare l'esigenza di tutela della collettività, impedendo, con le restrizioni alla libertà personale dei giovani indagati, la reiterazione di fatti analoghi, trattandosi, come si è detto, non solo di un fenomeno oramai sempre più radicato nella realtà del Distretto, ma reso ancora più allarmante dalla volontà di vendetta da parte dei corrissanti emersa dalle indagini, con il conseguente rischio di incontrollabili e violente reazioni a catena.

CANALI TELEGRAM - Nel corso delle attività investigative espletate dalla Polizia Postale di Salerno è stato evidenziato all'A.G. che il comportamento dell'imputato minorenne, che attraverso annunci su gruppi pubblici Telegram invitava allo scambio di materiale pedopornografico in sessioni private di chat, era una forma di commercio.

Il G.I.P. del Tribunale dei Minorenni di Salerno e la Corte di Cassazione (sentenza della III Sezione Penale, n. 577 del 13.03.2022, pubblicata il 13.07.2022) hanno accolto tale interpretazione, riconoscendo la contestabilità della fattispecie di cui al comma 2 dell'art. 600 ter c.p., con conseguente ampliamento degli strumenti investigativi volti al contrasto della pedopornografia online.

SMISHING - Gli agenti del Commissariato di Torre del Greco e della Polizia Postale di Napoli hanno effettuato un controllo presso un appartamento a Torre del Greco, dove hanno sorpreso quattro uomini intenti ad utilizzare dei computer e che, alla vista degli operatori, hanno tentato di darsi alla fuga. Gli agenti li hanno bloccati e controllati, trovando tre di loro in possesso di due carte di debito, un cellulare e di 5.305 Euro, mentre nell'abitazione hanno trovato 134 cellulari con relative schede sim, 113 carte di credito e di debito, 3 computer, 2 router Wi-Fi ed una chiavetta USB con dati relativi a bonifici e conti correnti. Infine, gli operatori hanno accertato che dalle utenze di alcuni cellulari trovati nell'appartamento erano state perpetrate delle frodi informatiche il mese scorso e nella prima

metà di ottobre. Quattro persone di 20, 21, 24 e 47 anni, tra cui le ultime due con precedenti di polizia, sono state denunciate per frode informatica.

OPERAZIONE ATENEO – La Polizia Postale di Napoli, sotto la direzione della Procura della Repubblica presso il Tribunale del capoluogo campano, ha sottoposto alla misura cautelare degli arresti domiciliari due soggetti, responsabili dei reati di accesso abusivo a sistema informatico e istigazione alla corruzione attiva, per aver proposto in anticipo ai candidati, dietro compenso in denaro, le risposte ai test di ingresso al corso di laurea magistrale in Scienze Motorie presso l'Università degli studi di Napoli – Parthenope per l'anno accademico 2019/2020.

Le indagini sono state avviate in seguito alla denuncia del Rettore dell'ateneo campano, formulata nell'ottobre del 2019, sulla base della segnalazione effettuata da uno studente, il quale, a sua volta, aveva ricevuto un messaggio WhatsApp, il cui testo recitava che un "collaboratore stretto di un professore", previo pagamento della somma di 200 Euro, avrebbe potuto fornire anticipatamente le risposte ai test di ingresso.

Le attività investigative svolte dalla Polizia Postale di Napoli hanno consentito di indentificare i responsabili delle condotte illecite. Il primo è un trentenne di Napoli, ex studente di Scienze Motorie presso l'Università Parthenope; dopo aver conseguito la laurea e aver frequentato un master nello stesso ateneo, l'interessato era divenuto assistente presso il Dipartimento di Scienze Motorie e del Benessere fino al febbraio del 2019; da ultimo, egli svolgeva la professione di docente presso un istituto superiore della provincia di Roma.

Il complice, un cinquantenne originario di Napoli, dal 2017 al 2020 aveva svolto funzioni tecnico-amministrative presso la segreteria del Dipartimento di Scienze Motorie e del Benessere dell'Università Parthenope; dal gennaio 2020 si era trasferito in provincia di Milano, per svolgere le medesime mansioni presso l'Università Bicocca.

Dalle indagini è emerso che i due si erano conosciuti presso l'ateneo partenopeo e avevano continuato a tenersi in contatto anche dopo il trasferimento di uno dei correi nel capoluogo lombardo.

Le attività investigative, basate anche sugli accertamenti tecnici svolti sui dispositivi informatici in uso agli interessati, hanno permesso di ricostruire le modalità con cui gli indagati avevano elaborato il disegno criminoso.

Dopo che la Commissione di esame dell'Università Parthenope aveva predisposto il test di ingresso al corso di laurea magistrale in Scienze Motorie, la relativa documentazione è stata riposta in buste sigillate e custodite in uffici chiusi a chiave. Uno degli indagati, addetto ai servizi tecnico-amministrativi dell'ateneo campano, aggiornava il complice sui movimenti del personale universitario, al fine di concertare il momento giusto in cui acquisire illecitamente i test.

All'approssimarsi della data della selezione, in un tardo pomeriggio dell'ottobre 2019, dopo il termine della giornata lavorativa, approfittando dell'assenza del restante personale, gli interessati si sono introdotti illecitamente negli uffici dell'Università ove erano custoditi i test e hanno acquisito la documentazione, effettuando delle fotocopie.

I due indagati hanno successivamente contattato a mezzo WhatsApp numerosi studenti, per proporgli in anticipo le risposte dietro compenso di 200 Euro. I contatti telefonici dei candidati sono stati carpiti mediante accesso abusivo alla banca dati dell'Università, contenente i dati personali degli aspiranti frequentatori.

L'analisi dei dispositivi informatici degli indagati è stata fondamentale per la ricostruzione dei reati, poiché sugli stessi sono stati rinvenuti numerosi file contenenti i test d'ingresso illecitamente sottratti. Le prove delle condotte penalmente rilevanti sono emerse anche dalle chat WhatsApp: in numerose conversazioni gli interessati si sono confrontati sulle modalità di acquisizione dei test e sull'elaborazione del messaggio da inviare ai candidati,

contenente la proposta corruttiva. I due indagati, inoltre, hanno scattato e successivamente condiviso alcune foto ritraenti il momento in cui essi si sono introdotti illecitamente negli uffici ove era custodita la documentazione dell'esame.

La collaborazione della Direzione e del corpo docente dell'Università di Napoli – Parthenope è stata fondamentale per l'accertamento delle condotte illecite. Inoltre, immediatamente dopo la segnalazione di possibili irregolarità e prima della selezione, l'ateneo campano ha avviato le procedure a tutela dell'integrità dell'esame di ammissione, provvedendo a rielaborare i test di ingresso al corso di laurea magistrale in Scienze Motorie per l'anno accademico 2019/2020.