Polizia di Stato

INTERNET, IL PAESE DELLE MERAVIGLIE…?

5 maggio 2024

Giornata Nazionale contro la Pedofilia e Pedopornografia

INDICE

Introduzione

In occasione della Giornata Mondiale contro la Pedofilia e Pedopornografia, ci confrontiamo con un panorama digitale in continua evoluzione, dove le sfide della sicurezza cibernetica si rinnovano e si intensificano ogni giorno. Negli ultimi anni, abbiamo assistito all'incremento di nuovi *trend*, tra cui l'uso dell'intelligenza artificiale generativa e di strumenti volti a garantire l'anonimato nel *web*. Queste tecnologie avanzate aprono nuove frontiere per la creatività e l'innovazione, ma allo stesso tempo introducono minacce inedite. La stessa copertina di questa *brochure* è stata realizzata con un *software* di intelligenza artificiale generativa, volendo mostrare le potenzialità dell'IA nel creare immagini e contenuti che possono avere un impatto emotivo sorprendente, anche se non reali.

Il messaggio che si vuole veicolare è che il *web* può essere un Paese delle Meraviglie, in considerazione delle possibilità che offre, in termini di contenuti fruibili, agli utenti di tutte le età, ma al suo interno si nascondono anche coloro che sfruttano l'innocente curiosità dei più piccoli per scopi illeciti. Conoscere questi pericoli ci consente di prevenire e contrastare le nuove forme di sfruttamento sessuale dei minori *online,* impedendo la commissione di nuovi reati.

La Polizia Postale e delle Comunicazioni continua a lavorare con dedizione per monitorare e fronteggiare tutti i rischi del *web*. Attraverso l'adozione di metodologie investigative all'avanguardia e la promozione di una cooperazione sempre più stretta tra il settore pubblico e privato, si impegna a mantenere internet uno spazio sicuro, in particolar modo per i più piccoli e le persone vulnerabili, accompagnandoli in una navigazione consapevole nella rete.

Quotidianamente, i nostri operatori, unitamente ai collaterali organi di Polizia esteri, si adoperano per identificare i responsabili e le loro vittime e per assicurare che nell'ambiente digitale possano essere garantiti luoghi di crescita sana e positiva per tutti i cittadini e riaffermando il diritto per i minori di scoprire il *web* senza temere insidie nascoste. Il contrasto internazionale alla pedofilia e pedopornografia *online* è un valore aggiunto nella lotta a questi crimini odiosi, che consente alle polizie di tutto il mondo di operare in sinergia.

La Giornata Mondiale contro la Pedofilia e Pedopornografia è un momento per riaffermare questo impegno e per rinnovare la nostra determinazione nella lotta a un crimine senza confini, che si evolve al passo con la tecnologia.

Il Direttore del Servizio Polizia Postale e delle Comunicazioni
Ivano Gabrielli

La pedopornografia e l'abuso tecnomediato

Nel campo dello sfruttamento sessuale dei minori, le vittime subiscono una tipologia di abuso, sia *online* che *offline*, che continua a protrarsi nel tempo. Infatti, il materiale pedopornografico creato e condiviso *online* tra adulti di tutto il mondo, determina una perdurante vittimizzazione dei bambini ritratti. Questo danno ulteriore si verifica ogni volta che i *files* vengono visualizzati da nuovi utenti e per ogni giorno in cui il materiale rimane in circolazione. La Polizia Postale si impegna per arrestare il ciclo della vittimizzazione tecnomediata, che perpetua il danno concreto dell'abuso subito ingiustamente da bambini e ragazzi, sfruttando le potenzialità di diffusione che internet purtroppo offre a pedopornografi e pedofili.

I numeri del contrasto

2.739

siti illegali in *black list*

Nel 2023 sono stati analizzati complessivamente 28.355 siti, di cui 2.739 resi irrangiungibili e inseriti nella *black list* dei siti che contengono rappresentazioni di sfruttamento sessuale di minori, per inibirne la visualizzazione e impedire alle immagini di abuso di continuare a circolare, evitando la vittimizzazione secondaria .

1.131

persone individuate e denunciate per reati di pedopornografia

Questo il numero delle persone individuate e denunciate per aver scaricato, condiviso e scambiato foto e video di abuso sessuale ai danni di minori nel 2023. I soggetti sono prevalentemente uomini, incensurati, anche se desta preoccupazione l'aumento dei reati di pedopornografia commessi da soggetti molto giovani.
Lo scorso anno sono stati numerosi gli arresti di soggetti con alto livello di pericolosità, colti in flagranza di reato, ovvero detentori di ingente quantità di materiale pedopornografico o abusanti.

137

casi di *sextortion* nel 2023

Nell'anno di riferimento è stato registrato un incremento dei casi di *sextortion*, passando dai 118 casi del 2022 ai 132 registrati nel 2023.

353

casi di adescamento *online* nel 2023

Nel 2023 è stato rilevato un lieve calo dei casi adescamento *online*, confermando però il coinvolgimento di minori di età compresa tra i 10 e i 13 anni. Infatti, la fascia dei preadolescenti è quella che maggiormente ha avuto interazioni sessuali tecnomediate, 200 rispetto ai 341 casi totali.

Le *Partnership* con il settore privato

La collaborazione tra settore pubblico e privato è fondamentale nella lotta allo sfruttamento sessuale dei minori *online*. Questa *partnership* combina risorse, competenze e tecnologie, essenziali per sviluppare strategie di prevenzione e protezione più efficaci per i minori nell'era digitale.
Sono in essere i seguenti Protocolli di intesa tra il Ministero dell'Interno – Dipartimento della Pubblica Sicurezza e:

Save the Children Italia ONLUS

Per favorire l'accesso dei minori ad un **ambiente online più sicuro**, per prevenire i rischi connessi a un utilizzo non consapevole della rete, per contrastare gli abusi sessuali *online*, promuovendo attività di prevenzione, segnalazione ed emersione di potenziali abusi.

Telefono Azzurro – Dalla parte dei Bambini

Per il potenziamento dell'attività di **prevenzione e di contrasto alle violenze** in danno dei minori in rete attraverso la trasmissione al CNCPO, per la successiva trattazione, delle segnalazioni ricevute dalla *Hotline* 114 Emergenza Infanzia.

Comunità di Sant'Egidio

La Convenzione è volta alla realizzazione di **campagne di sensibilizzazione** per bambini e ragazzi, volte a un uso consapevole e sicuro delle tecnologie digitali e di iniziative congiunte per l'individuazione delle vittime di eventuali abusi *online*.

Meter onlus – Dalla parte dei Bambini

L'accordo disciplina la realizzazione di iniziative congiunte per la **promozione dei diritti dell'infanzia e dell'adolescenza** nell'ambito della tutela dei minori da ogni forma di aggressione *online*, promuovendo l'educazione di minori e famiglie a un uso consapevole della rete.

National Center for Missing & Exploited Children – www.missingkids.com

Il ***National Center for Missing and Exploited Children*** (*N.C.M.E.C.*) trasmette quotidianamente al CNCPO, per la successiva trattazione, centinaia di segnalazioni relative a materiale di natura pedopornografica presente nel *web* che coinvolgono utenti italiani.

OPERATION UNDERGROUND RAILROAD

La collaborazione con la ONG ***Operation Underground Railroad*** ha rafforzato la lotta contro lo sfruttamento sessuale dei minori *online*, migliorando la **formazione e l'innovazione tecnologica**. Questa *partnership* ha potenziato le capacità di intervento e prevenzione.

Terre des hommes – Aiuto all'infanzia.

Recentemente, con la sigla del protocollo di intesa tra Polizia Postale e la ONG ***Terre des Hommes,*** è stato ulteriormente estesa la *partnership* con il settore privato in ambito di segnalazioni per casi di minori in pericolo, implementando le misure di protezione e risposta tempestiva.

Le principali minacce *online* ai danni di bambini e ragazzi: *trend* attuali

Lo sfruttamento sessuale dei minori *online* è un fenomeno complesso e multidimensionale, che si aggrava constantemente a livello globale. Dal 2019 il *National Center for Missing and Exploited Children (NCMEC)* ha registrato un aumento del 87% dei casi. Gli autori di questi reati sono spesso persone insospettabili, che conducono una vita ordinaria e hanno un'età che, nel 70% dei casi, non arriva ai 45 anni. Sempre più spesso sfruttano i servizi di messaggistica e *socialnetworking* legali volti a garantire l'anonimato, per mascherare le loro intenzioni e la loro identità, tentando di eludere le investigazioni delle forze di polizia.
La complessità dei fenomeni di abuso sessuale *online* richiede un approccio sempre più integrato tra il *framework* normativo del nostro Paese, le attività investigative sempre più sofisticate, anche a livello tecnico e la massima attenzione nei confronti delle specifiche peculiarità psicologiche degli autori di reato e delle vittime. La presenza di un *pool* di psicologi dell'Unità di Analisi dei Crimini Informatici (UACI) presso il Servizio Polizia Postale ha progressivamente aperto la strada a un confronto costante con gli aspetti più definitamente umani, che correlano con queste gravi crimini.

L'adescamento di minori *online*

Rimane emergente la minaccia legata ai **casi di adescamento *online* che riguardano minori di età inferiore ai 13 anni**. La diffusione sempre più capilalre tra bambini e ragazzi di *smartphones* e *tablets* di ultima generazione non sfugge all'attenzione di pedofili e adescatori *online*. Sempre più spesso, infatti, i primi contatti tra questi soggetti e le piccole vittime avvengono proprio nei luoghi deputatai agli "esercizi evolutivi" di bambini e adolescenti. I videogiochi, divenuti popolari attraverso *app* di gioco scaricabili su cellulari e *consolles* agili, diventano un luogo dove i bambini si misurano con mondi fantastici e ruoli da protagonisti, esercitandosi a crescere. I *social network* sono ormai la vetrina cibernetica attraverso la quale gli adolescenti della Generazione Z effettuano un necessario lavoro di sperimentazione sociale e sessuale. Entrambi questi luoghi virtuali diventano un terreno su cui chi ha cattive intenzioni può sfruttare la necessità di esplorare in modo manipolatorio. Gli adescatori agganciano i bambini e i ragazzi sui loro spazi preferiti, mirano poi a spostarsi su *App* di messaggistica con crittografia *end-to-end*, progressivamente si avvicinano a temi sessuali e inducono la vittima a produrre e condividere immagini intime, autoprodotte, si assicurano che i cellulari non siano controllati dai genitori, incitano alla segretezza dei contatti, promettono esattamente quello che i bambini e i ragazzi vogliono, l'ultima *skin* del videogioco preferito o il provino per una serie televisiva. Dall'analisi dei casi gestiti dagli Uffici territoriali emerge come questa minaccia sia trasversale al genere e riguardi bambini e ragazzi con caratteristiche anche molto diverse: dai più timidi ai più spigliati, l'aggancio è facilitato dalla familiarità che i ragazzi hanno nell'interagire con soggetti sconosciuti. Quali cittadini di un mondo globalizzato, le nuove generazioni approcciano l'altro con apertura e fiducia. E' tuttavia innegabile che la gravità e la diffusione progressiva del fenomeno rendono indispensabile che bambini e ragazzi, insieme a genitori e insegnanti, conoscano questo tipo di minaccia e segnalino qualsiasi situazione sospetta.

La *sextortion*

Si tratta di un fenomeno in crescita, che in passato coinvolgeva soltanto gli adulti, ma che negli ultimi anni impatta anche sui minori, la cui naturale curiosità viene sfruttata per trasportarli in un incubo fatto di ricatti, richieste di denaro e minacce di distruggere la reputazione, diffondendo sui *social* immagini sessualmente esplicite, autoprodotte. Si tratta di estorsione sessuale perpetrata anche da gruppi criminali organizzati, nei confronti di bambini e adolescenti. Gli estorsori, fingendosi ragazze avvenenti, contattano ragazzi per lo più di 15 - 17 anni tramite i *social media*, inducendoli a realizzare video/immagini sessualmente espliciti, con la minaccia di diffonderli tra amici e familiari del minore, in caso di mancato pagamento di una somma in denaro.

Materiale sessualmente esplicito autoprodotto e *Revenge Porn*

Un altro pericolo in cui i minori rischiano di imbattersi consiste nello scambio consensuale, tra pari, di materiale volontariamente autoprodotto (c.d. *Sexting*), ad esempio nell'ambito di relazioni sentimentali, che viene successivamente diffuso dalla "controparte" senza il consenso dell'altro. Si tratta del *Revenge Porn,* che letteralmente significa "*vendetta porno*" o "*vendetta pornografica*", ovvero quella pratica consistente nel vendicarsi di qualcuno (spesso l'*ex partner*) diffondendo materiale sessualmente connotato che lo ritrae. Il codice penale punisce chi, dopo averli realizzati o sottratti, invia, consegna, cede, pubblica o diffonde immagini o video a contenuto sessualmente esplicito, destinati a rimanere privati, senza il consenso delle persone rappresentate. È inoltre punibile anche chi, avendo ricevuto o comunque acquisito le immagini e i video di cui al primo comma, li invia, consegna, cede, pubblica o diffonde senza il consenso delle persone rappresentate al fine di recare il loro nocumento. Fino al 2020 questa fattispecie di reato non veniva presa in considerazione laddove le immagini sessualmente esplicite raffiguravano minori degli anni 18, in quanto, in questi casi, venivano contestati i reati di produzione, diffusione e detenzione di immagini pedopornografiche. Tuttavia, a partire dal 2021, sulla scorta di alcune riflessioni scaturite dalla sentenza della C. Cass., sez. III, n. 11675 del 21.03.2016, che confermava l'assoluzione di alcuni minorenni dai reati di pornografia minorile in un caso in cui gli imputati avevano detenuto e divulgato immagini sessualmente esplicite di un loro coetaneo, che precedentemente le aveva spontaneamente a loro cedute dopo averle autonomamente e volontariamente autoprodotte, si applica la norma in questione se le persone coinvolte sono tutte minorenni.

L'intelligenza artificiale generativa nell'ambito della pedopornografia

L'intelligenza artificiale generativa sta cambiando il modo in cui interagiamo con il mondo digitale, in considerazione della possibilità di creare contenuti nuovi come immagini, video, testi e audio. Purtroppo, si sta verificando un aumento nei casi di abuso di questi strumenti per creare materiale di sfruttamento sessuale dei più piccoli. Tale fenomeno può riguardare sia minori reali, la cui immagine può essere artificialmente modificata in contenuto pedopornografico, ovvero può essere utilizzata per creare contenuti illeciti raffiguranti bambini inesistenti nel mondo reale.

Recentemente, si è dimostrato che l'intelligenza artificiale può essere utilizzata per agevolare condotte di adescamento *online*, *revenge porn* e *sextortion*. Infatti, le capacità di generare messaggi su misura per il tipo di interlocutore può essere sfruttata dai malintenzionati per aumentare le possibilità di interazione con le loro vittime. In tal senso L'IA può sopperire al *gap* generazionale, originando messaggi realistici come se fossero scritti da minorenni, in modo da instaurare interlocuzioni digitali con i minori.

L'aspetto realistico delle immagini prodotte con l'intelligenza artificiale generativa determina una nuova sfida per le forze di polizia e la necessità di reinterpretare l'evoluzione normativa in questo settore. In primo luogo gli investigatori dovranno cimentarsi con l'analisi dell'immagini per verificarne l'autenticità e quindi stabilire se vi siano vittime minori da identificare. In secondo luogo, la facilità e velocità di produrre contenuti multimediali illeciti comporta la previsione di norme più severe per coloro che si rendano autori di queste condotte, contaminando il *web* e l'ambiente di crescita di minori con rappresentazioni multimediali distorte.

In questo contesto, lo scorso 23 aprile il Governo ha proposto un disegno di legge sull'Intelligenza Artificiale (IA), con l'obiettivo di regolamentare il futuro dell'AI in Italia, in termini di bilanciamento tra le opportunità offerte dalle nuove tecnologie e i rischi associati a un uso improprio e dannoso, a integrazione di quanto già previsto dal Regolamento europeo sull'Intelligenza Artificiale ("AI Act") approvato lo scorso marzo.

Il disegno di legge prevede una serie di misure volte a punire i reati commessi tramite l'uso di sistemi di intelligenza artificiale in maniera più severa. Anzitutto, è prevista una specifica aggravante per i reati commessi con l'ausilio dell'AI. Inoltre, il testo stabilisce che la diffusione illecita di contenuti generati o manipolati dall'IA per indurre in inganno sulla loro genuinità (come nel caso dei cosiddetti *deepfake*) sia punita con la reclusione. Sono poi introdotte circostanze aggravanti speciali per punire reati in cui l'uso dell'IA abbia una elevata capacità di propagare l'offesa.

Questi sforzi normativi, sia a livello nazionale che europeo, riflettono l'importanza di affrontare le sfide poste dall'AI in modo olistico e responsabile, considerando le implicazioni etiche, sociali ed economiche di questa tecnologia. È interessante vedere come l'Italia stia cercando di posizionarsi al centro del dibattito globale sulla regolamentazione dell'AI.

Live Streaming Child Abuse

Consiste nello sfruttamento sessuale di minori a distanza, *on demand*. Si tratta di abusi commissionati in *live chat*, in tempo reale, su internet che, solitamente, sono facilitati da un altro adulto presente fisicamente vicino al minore, che lo costringe a compiere atti sessuali con adulti o con altri coetanei, attraverso piattaforme dedicate.
In questo modo, dietro il corrispettivo in denaro di somme piuttosto ridotte (anche 20-30 euro), si può comprare la possibilità di dirigere via webcam, in diretta, le violenze commesse su bambini che si trovano in Paesi dove la normativa non tutela adeguatamente i minori (di solito le Filippine, etc.).
Si tratta di un fenomeno che vede coinvolti bambini anche di età inferiore ai 12 anni.
Le investigazioni in tale ambito sono complesse, in quanto il tracciamento delle transazioni finanziarie effettuate non è sufficiente a individuare con certezza il contenuto di questi scambi e dalle causali delle transazioni non è agevole capire se le operazioni siano da imputare al materiale di abusi su minori. Un'ulteriore criticità è rappresentata dalle caratteristiche tecnico-informatiche dei circuiti nei quali avvengono i collegamenti in *streaming*: *Skype* e le altre piattaforme per le videochiamate spesso non sono in grado di fornire tracce utili all'accertamento dei contenuti scambiati tra gli utenti, in quanto si tratta di sessioni live e, come tali, non vengono registrate, rendendo quindi ardua l'identificazione sia delle vittime che degli acquirenti.

Il *cyberbullismo*

Le prepotenze online fra minori rappresentano una realtà che affligge bambini e ragazzi in fasce d'età sempre più precoci. Il legame tra questo fenomeno e la pedopornografia è purtroppo in via di incremento: attraverso la diffusione incontrollata di immagini intime, sessualmente esplicite, su *chat* di classe, si realizzano vere e proprie campagne denigratorie in danno di coetanei, i quali, esposti loro malgrado al giudizio sommario di gruppi di altri minori, diventano bersaglio di attacchi tecnomediati duraturi. I meccanismi di viralizzazione risultano poi particolarmente rapidi e violenti quando riguardano "materiale scottante" e per le vittime si apre la strada dell'isolamento sociale, della vergogna e della difficoltà di trovare interlocutori in grado di aiutarli a risolvere un problema di cui si sentono spesso corresponsabili.

Le *social challenges* e i "gruppi dell'orrore"

Le "prove di coraggio" che in molte culture rappresentavano la celebrazione del passaggio dall'infanzia all'età adulta, nell'era digitale hanno assunto la forma più evanescente delle *challenges online*, in cui l'esercizio di misurarsi con i propri limiti attraverso un *test* di coraggio assume forme talvolta singolari e decisamente problematiche.

Gia da qualche anno è emersa la tendenza di adolescenti a ricercare *online* non solo sfide che prevedano azioni irrazionali o pericolose in cui cimentarsi, filmandosi con gli *smartphones* per poi diffonderli in rete e guadagnare popolarità.

Più recentemente, accade che i ragazzi accettino di partecipare a gruppi chiusi di messaggistica, popolati da migliaia di utenti sconosciuti, nei quali circola e si partecipa a far circolare materiale impressionante: da esecuzioni capitali a incidenti mortali, dalle violenze sessuali fino alla pedopornografia e alle torture. Ogni immagine visionata sconvolge e colpisce lo stomaco, favorendo una desensibilizzazione dei giovani e giovanissimi, con evidenti effetti negativi sul loro sviluppo psicoemotivo e con ripercussioni importanti anche da un punto di vista legale.

Indagini ad alto impatto

Shadow Man

L'operazione trae origine da complesse indagini svolte in modalità sotto copertura nel *DarkWeb* da personale specializzato del *Centro Nazionale per il Contrasto alla Pedopornografia Online (CNCPO)* del Servizio Polizia Postale e delle Comunicazioni nell'ambito di comunità virtuali pedofile, in collaborazione con Europol e la polizia britannica. Tra i molteplici membri di tali *communities*, originari da tutto il mondo, si era distinto un utente, per il significativo contributo apportato, in termini di materiale pedopornografico, anche autoprodotto, messo a disposizione degli altri partecipanti. L'uomo, che per oltre un decennio era riuscito a eludere le indagini della Polizia Postale nel *Darkweb*, sfuggendo anche alla cattura degli altri membri, è stato identificato e arrestato per violenza sessuale aggravata, commessa ai danni del figlio minore di anni 10; associazione per delinquere finalizzata alla diffusione di pratiche di pedofilia, alla condivisione di notizie utili all'adescamento di minori e allo scambio, detenzione e diffusione di materiale pedopornografico, nonché di consigli utili per porre in essere tali attività illecite e diffusione di materiale raffigurante abusi sessuali su minori, anche inedito e autoprodotto utilizzando il figlio minore. Lo spessore criminale dell'indagato ha fatto sì che abbia rappresentato un *high-value-target* internazionale nell'ambito delle polizie di tutto il mondo impegnate in attività sotto copertura *online* nel contrasto alla pornografia minorile all'interno delle citate comunità pedofile virtuali. Anche grazie alla condivisione di importanti informazioni ottenute dai collaterali esteri, è stato possibile giungere alla identificazione dell'uomo.

Fast and done

Un 36enne romano è stato arrestato per violenza sessuale aggravata ai danni di un bambino di 10 anni per produzione, cessione e detenzione di ingente quantitativo di materiale pedopornografico. L'uomo è stato fermato dagli operatori del *C.N.C.P.O.* al termine di un'indagine-lampo scaturita da una segnalazione del collaterale australiano al termine di una perquisizione domiciliare e informatica. Si tratta di una vicenda di eccezionale gravità perché gli abusi, ripresi con uno *smartphone*, venivano commessi nei confronti del minore figlio di un'amica dell'indagato. Le foto e i video venivano poi inviati ai frequentatori di una comunità pedofila *online* di livello internazionale, attiva nel *DarkWeb*. Quando hanno avviato le indagini, gli investigatori della Polizia Postale non avevano alcuna pista da seguire, a parte i *files* illeciti pubblicati e un *nickname* di fantasia. L'utilizzo del *DarkWeb*, infatti, garantisce ai propri utilizzatori l'anonimato, complicando notevolmente le indagini. Tuttavia, incrociando i risultati delle ricerche con tecniche di OSINT (*Open Source INTelligence*), congiuntamente all'analisi degli ambienti e dei luoghi è stato possibile risalire all'identità dell'abusante e della giovanissima vittima. La svolta nelle indagini si è avuta dopo ore di incessante attività condotta con ritmi serratissimi sul duplice fronte della *Clear Net* e del *DarkWeb*, in una vera e propria corsa contro il tempo per scongiurare il pericolo di ulteriori violenze. I dati raccolti durante la perquisizione informatica hanno confermato tutte le ipotesi investigative, il materiale è stato posto sotto sequestro, mentre l'indagato è stato condotto in carcere.

Viper

Nel mese di dicembre il C.N.C.P.O. ha coordinato l'esecuzione, su tutto il territorio nazionale, di 57 decreti di perquisizione delegati dalla Procura della Repubblica di Venezia nei confronti di altrettanti indagati, nell'ambito del contrasto alla pedopornografia *online*. L'operazione ha coinvolto gli Uffici della Polizia Postale di Marche, Puglia, Emilia Romagna, Sardegna, Sicilia orientale e occidentale, Toscana, Liguria, Lombardia, Campania, Umbria, Abruzzo, Calabria, Lazio e Piemonte. L'indagine, condotta dal Centro Operativo per la Sicurezza Cibernetica della Polizia Postale di Venezia e coordinata, anche sul piano internazionale, dal C.N.C.P.O., è scaturita dall'analisi dei dispositivi informatici sequestrati a un precedente indagato, tratto in arresto in flagranza nell'ottobre 2022, per detenzione di ingente quantitativo di materiale pedopornografico. Nel corso della successiva analisi forense, è emerso che il soggetto era molto attivo sulla piattaforma *Viber* e iscritto a 42 gruppi e 247 canali dediti allo scambio di materiale realizzato mediante l'utilizzo di minori di 18 anni. I cospicui contenuti multimediali scambiati tra gli utenti raffiguravano anche torture perpetrate in danno di bambini. L'attività, condotta in modalità sotto copertura dal personale del COSC Veneto, ha consentito di identificare, oltre a numerosi utenti italiani, anche molteplici stranieri, riconducibili a 44 diversi Stati, per i quali il C.N.C.P.O. ha proceduto ad attivare i canali di cooperazione internazionale di polizia, tramite Europol, Interpol e Ameripol, con i quali è stata pianificata una *Joint Action*, alla quale hanno aderito diversi collaterali. Le perquisizioni hanno consentito di arrestare 28 soggetti e di denunciarne 24 in stato di libertà.

Operazione di contrasto al Live Streaming Child Abuse

Nel mese di dicembre 2023, personale del CNCPO, unitamente a quello della Sezione Operativa per la Sicurezza Cibernetica della Polizia Postale di Varese, ha eseguito due misure cautelari nei confronti di un uomo e una donna ritenuti responsabili di aver commesso - dietro corrispettivo in denaro - sessioni *live* di abusi sessuali su minori (*Live Streaming Child Abuse*). L'attività trae origine da un'indagine condotta dal CNCPO e scaturita da una segnalazione di operazioni sospette per presunto acquisto di materiale pedopornografico, successivamente riscontrata da ulteriori informazioni ricevute dalla *Homeland Security Investigation (HSI)* nell'ambito della cooperazione internazionale di polizia. Gli abusanti, di nazionalità filippina, ricevevano versamenti da *account* PayPal riconducibili a utenti europei per poter assistere ad abusi su minori, commissionati sul momento dagli utenti interessati e trasmessi in diretta *streaming*. Tra questi vi era anche un cittadino italiano che, tra il 2019 e il 2020, aveva effettuato numerosi pagamenti. A seguito di analisi forense sui dispositivi sequestrati a suo carico, è emerso che la moglie filippina, nel periodo in cui viveva all'estero, offriva a pagamento sessioni di *Live Streaming Child Abuse* ai danni dei due figli minori.

La prevenzione

Il Commissariato di P.S. *online*

Il Commissariato di P.S. online si propone come strumento, al passo con i *social network*, che permette ai cittadini di ottenere informazioni e risposte immediate, in tempo reale. Il sito *web* ***www.commissariatodips.it***, del Servizio Polizia Postale e delle Comunicazioni, è gestito da operatori esperti che garantiscono un servizio attivo in materie giuridiche e sociali. I cittadini, anche minorenni, possono inoltrare segnalazioni in modo anonimo.

Le campagne di informazione

Nel 2023 è proseguita la più importante campagna educativa itinerante realizzata dalla Polizia di Stato e dal MIUR, per la sensibilizzazione e la prevenzione dei rischi e dei pericoli del *web* per i minori. Gli operatori della Polizia Postale e delle Comunicazioni e degli Uffici Scolastici Regionali del Ministero dell'Istruzione hanno coinvolto oltre **3 milioni di studenti** sia nelle piazze che nelle scuole, **230.000 genitori, 146.000 insegnanti** per un totale di **20.000 Istituti scolastici, 450 città** raggiunte sul territorio e due pagine *Twitter* e *Facebook* con **134.000 *like* e oltre 12 milioni di utenti** mensili sui temi della sicurezza *online*.

L'8 febbraio 2023 è ripartita la Campagna di sensibilizzazione ideata e realizzata dalla Polizia di Stato in collaborazione con Unieuro, in occasione del *Safer Internet Day*, istituito nel 2014 dalla Commissione europea, per promuovere un utilizzo consapevole e responsabile delle nuove tecnologie, soprattutto tra i più giovani.

La Polizia Postale partecipa al progetto *Safer Internet Centre* – Generazioni Connesse, co-finanziato dalla Commissione Europea nell'ambito del programma *Digital Europe* e coordinato dal MIUR, con il partenariato di alcune delle principali realtà italiane che si occupano di sicurezza in Rete: *l'Autorità Garante per l'Infanzia e l'Adolescenza, gli Atenei di Firenze e 'La Sapienza' di Roma, Save the Children Italia, Telefono Azzurro, la cooperativa EDI Onlus, Skuola.net e l'Ente Autonomo Giffoni Experience.*

La Polizia Postale ha inoltre preso parte al gruppo di lavoro coordinato dal Dipartimento per la trasformazione digitale con l'obiettivo di contribuire alla costruzione di una cultura dei videogiochi, per il fine di co-progettare iniziative utili a promuovere la consapevolezza sulle sfide e sulle opportunità di questo importante medium. La pubblicazione *"Sfide e opportunità del Gaming per la diffusione delle competenze digitali"* ha visto la definizione di consigli e suggerimenti utili ai piccoli *gamer* e ai loro genitori per sfruttare solo le opportunità e ridurre al minimo i rischi connessi all'uso dei videogiochi.

#neipannidicaino

Il progetto *"Nei panni di Caino per capire e difendere le ragioni di Abele"*, finanziato con fondi PON, avviato nel 2019 e concluso nel corso del 2023, ha determinato la costruzione di un nuovo protocollo formativo che fa sperimentare le prospettive della vittima e dell'autore di un reato *online*, attraverso la proiezione, su visori 3D, di scenari costruiti per indurre gli stati emozionali propri dei diversi fenomeni di rischi online. Sono state coinvolte scolaresche di Campania, Basilicata, Puglia, Calabria e Sicilia. I ragazzi hanno indossato dei visori Oculus e hanno potuto osservare, dalla prospettiva della vittima o di un partecipante, le situazioni di rischio *online*, vivendole "direttamente" sulla loro pelle: 12 gli scenari stimolo proposti, scegliendo tra quelli più vicini alle difficoltà specifiche dei singoli istituti. *Hate speech, grooming online*, falsificazione dell'identità personale, *sexting, social challenge, sextortion*, istigazione al suicidio, disturbi alimentari, gioco d'azzardo online, inclinazione all'appartenenza ad organizzazioni criminali, sono i rischi che sono stati discussi con i ragazzi, condivisi con gli insegnanti, con la partecipazione degli operatori della Polizia Postale, con l'ambizioso obiettivo di promuovere maggiori livelli di consapevolezza.

Consigli per i genitori

- ✓ State al passo con l'evoluzione dei mezzi di comunicazione, dei meccanismi delle *App* e dei *social* e dei nuovi *trend online*;
- ✓ Limitate la pubblicazione in internet delle foto dei vostri figli;
- ✓ Attivate il controllo parentale sui dispositivi dei vostri figli;
- ✓ Ricordate che la legge prevede che un utente possa avere accesso ai *social media* solo dopo aver compiuto 13 anni;
- ✓ Monitorate la navigazione e l'uso delle *App social*, anche stabilendo un tempo massimo da trascorrere connessi. Mostratevi curiosi verso ciò che tiene i ragazzi incollati agli *smartphones*: potrete capire meglio cosa li attrae e come guidarli nell'uso in modo da essere sempre al sicuro;
- ✓ Se ai vostri figli capita di essere vittima di reato *online*, non giudicateli, ma tenete presente che la vergogna e il senso di panico che possono provare li mettono a rischio di compiere atti impulsivi. Ascoltateli, acquisite con calma tutte le informazioni utili a un'eventuale denuncia e rassicurateli che non sono i soli a essere incappati in questo tipo di situazioni;
- ✓ Dialogo, ascolto e comunicazione sono fondamentali per aiutare i vostri figli a navigare consapevolmente. Se avete bisogno di ulteriori informazioni, potete consultare il sito della Polizia Postale: ***www.comissariatodips.it;***
- ✓ Installate *antivirus* e *firewall* sui dispositivi in uso ai vostri figli e mantenete sempre aggiornati i programmi per garantire la protezione dei *devices*;
- ✓ Segnalate alla Polizia Postale tutti i casi sospetti su ***www.comissariatodips.it.***

Consigli per i ragazzi

- ✓ Non condividete informazioni personali come nome, cognome, indirizzo, numero di telefono. Ricordate che il display del cellulare e lo schermo del computer possono occultare le vere identità e intenzioni di chi vi contatta;
- ✓ Siate riservati con le vostre immagini e con quelle degli altri. Una volta immessi in rete, i contenuti multimediali non sono più controllabili. Evitate di condividere immagini e video intimi, soprattutto se siete riconoscibili;
- ✓ Comportatevi *online* come fareste nel mondo reale: trattate gli altri con rispetto e segnalate contenuti offensivi o inadeguati alla Polizia Postale tramite il sito ***www.comissariatodips.it*;**
- ✓ Nel caso in cui siano state pubblicati *online* foto e video inappropriati, che vi riguardino, chiedete alla piattaforma interessata la rimozione dei contenuti compromettenti;
- ✓ Gli scherzi *online*, le prese in giro, possono avere effetti dolorosi sugli altri: evitate di ritrovarvi a essere bulli senza l'intenzione di fare del male;
- ✓ I malintenzionati utilizzano la rete e i *social*, le piattaforme di gioco per adescare minorenni allo scopo di ottenere immagini sessualmente esplicite, spesso fingendosi coetanei;
- ✓ Se qualcuno vi parla di sesso senza che lo vogliate, vi minaccia o vi fa sentire a disagio, parlatene con i vostri genitori, insegnanti o adulti di riferimento. Potete anche rivolgervi alla Polizia Postale tramite il sito ***www.comissariatodips.it***;
- ✓ Non accettate di incontrare persone conosciute su Internet senza avvertire i genitori o un adulto di riferimento;
- ✓ Se venite a conoscenza che un minore sia vittima di reato, non restate indifferenti e segnalatelo a un adulto di riferimento;
- ✓ Se siete vittime di reato *online*, mettete al sicuro le possibili prove: non cancellate i messaggi, né le immagini e i video e non chiudete i profili *social* sui quali siete stati contattati prima di aver fornito queste informazioni alla polizia (fare gli *screen shot* delle conversazioni e della *url* identificativa del profilo);
- ✓ Se siete vittime di *sextortion*: non pagate! Interrompete i contatti con il ricattatore e non reagite ai messaggi;
- ✓ Se utilizzate circuiti di *file sharing* per condividere musica, film o altro, controllate sempre il materiale che ricevete. Alcuni *files* potrebbero essere illegali. Se vi imbattete in materiale sospetto, avvertite subito i vostri genitori e valutate insieme se segnalarlo alla Polizia;
- ✓ Fare subito denuncia alla polizia: la tempestività in questi casi è fondamentale per le indagini;
- ✓ Chi ha più di 14 anni può sporgere una denuncia, anche in modo autonomo, in qualsiasi ufficio di Polizia;

Chiunque contribuisca a diffondere immagini sessuali e di violenza che riguardino minorenni commette un reato: segnalatelo alla Polizia Postale tramite il sito ***www.comissariatodips.it*;**

Elaborazione a cura del C.N.C.P.O. – Vice Questore Eva Claudia Cosentino e Commissario Capo Federico Becchetti e del UACI – Dir. Tec. Sup. Cristina Bonucchi
Realizzazione immagini grafiche originali a cura del Commissario Capo Federico Becchetti