GLOBAL RESEARCH GloRES PUBLISHING HOUSE

A cura di:
Vincenzo Maria Mastronardi

Istituto Internazionale Scienze Criminologiche e Psicopatologico-Forensi

CRIMINOLOGIA

INVESTIGAZIONE PSICOPATOLOGIA E SCIENZE FORENSI INTERNAZIONALI -RIVISTA UFFICIALE IISCPF

CRIMINOLOGY

INVESTIGATION, PSYCHOPATHOLOGY AND INTERNATIONAL FORENSIC SCIENCE

seeking knowledge&finding solutions

Volume 56 Issue 4
September-December
2024

ISSN: 1826-7130

Dalla ***Collana di Criminologia, Psicopatologia forense e Psicologia investigativa*** *dell'International Institute for Criminological and Forensic Sciences- IISCPF (Italia -USA) a cura di Vincenzo Maria Mastronardi*

Criminologia Investigazione Psicopatologia e Scienze Forensi Internazionali –

Rivista Ufficiale IISCPF

(Criminology, Investigation, Psychopathology and International Forensic Science – Official Journal of the IISCPF)

VOLUME 56
Issue 4
September-December 2024
Registration Civil Court of Rome
No. 560/2004 (22-12-2004)

Rivista di Criminologia, Investigazione, Psicopatologia e Scienze Forensi Internazionali.
Criminology, Investigation, Psychopathology, and International Forensic Science
Periodico a carattere scientifico.
Rivista ufficiale di IISCPF – ***(Online scientific quarterly - Official Journal of the IISCPF)***

Istituto internazionale di Scienze criminologiche e psicopatologico-forensi (Italia – USA).

Soci onorari **R. Hazelwood+, M.R.Napier Supervisors FBI Quantico (Usa), R.Kocsis (Australia), H.Wan Marley (Olanda), J.Endrass (Switzerland) , G. Palermo +(Las Vegas)**

(International Institute for Criminological and Psychopathological Forensic Sciences (Italy – USA) ***Honorary Fellow:*** **R.Hazelwood+, M.R. Napier Supervisors FBI Quantico (Usa), R.Kocsis (Australia),H.Wan Marley (Olanda), J.Endrass (Switzerland)**

Editorial Staff:

Prof. Virgil Serban

Editor-in-Chief e Direttore Organizzativo *(Organizing Director):*

Vincenzo Maria Mastronardi

Honorary Editor:

George B. Palermo +

Managing Editor:

Monica Calderaro

Gli elaborati vanno inviati al Prof. Vincenzo Mastronardi e al Prof. Virgil Serban.

(Entries should be submitted to Prof. Vincenzo Mastronardi and Prof. Virgil Serban)

Mail: iiscppf@gmail.com and

criminologia.internazionale@globalresearchpublishing.com

Registrazione al Tribunale Civile di Roma n° 560/2004 (22.12.2004) (Registration at the Civil Court of Rome No. 560/2004 - 22.12.2004)

N.D.R.: La presente rivista online nasce da una esigenza manifestata da più contesti universitari internazionali e si presenta in continuum con la Rivista di Psicopatologia Forense, Medicina Legale, Criminologia (di proprietà dell'Università di Roma "La Sapienza") con i suoi contenuti mirati specificamente al settore della Criminologia, Investigazione, Psicopatologia e Scienze forensi in generale e viene pubblicata in più lingue con abstract in italiano, inglese, spagnolo.

Note: This online journal was born from the need expressed by many Editors' international university contexts, and it is provided in continuum with the Review of Forensic Psychopathology, Legal Medicine, Criminology (owned by the University of Rome "La Sapienza"). Its contents are specifically targeted at Criminology, Investigation, Psychopathology and Forensic Sciences as a whole, and it is published in a number of languages, with abstracts in Italian, English and Spani

CONTENTS

Criminologia Investigazione Psicopatologia e Scienze Forensi Internazionali

Volume 56 * Issue 4* 2024

Note redazionali. Breve storia della Rivista	
Editorial notes. A brief history of the Journal	**6**
Vincenzo Maria Mastronardi	
Note Editoriali mirate al presente numero della rivista	**8**
INTERPOL: Contrasto alla pedopornografia online	**9**
Bianca Francesca Berardi	
INTERPOL: Contrasto alla pedopornografia online (PARTEII)	**26**
Bianca Francesca Berardi	
Operazioni congiunte di cooperazione internazionale nel contrasto alla pedopornografia online: Prospettiva italiana	**42**
Bianca Francesca Berardi	
Analisi delle attività di prevenzione alla pedopornografia online: Il Caso italiano	**53**
Bianca Francesca Berardi	

Note redazionali

Breve storia della Rivista.

La presente Rivista trae ispirazione dal prezioso incontro academico con alcuni dei docenti noti al panorama scientifico internazionale quale **George Palermo di Las Vegas, nonché Roy Hazelwood , Michael Napier e Gregory Vecchi già formatori FBI a Quantico in Virginia,** nonché da tutti gli incontri accademici nell'arco di vari decenni e dal 1988 dalla fondazione da parte del Prof. Vincenzo M. Mastronardi già Direttore della Cattedra di Psicopatologia forense dell'allora Dipartimento di Scienze Psichiatriche dell'Università di Roma Sapienza, di più Master in Criminologia e Scienze Forensi, [4 in Italia (2 presso la Università Sapienza di Roma, 1 pressola Unitelma- Sapienza e 1 presso Università degli Studi internazionali di Roma), nonché 2 in Sud America (uno a Buenos Aires con la Università de Ciencias Empresariales Y Sociales UCES diretto dal Rettore L.M. De Simoni dell'Università de la Policia federal Argentina e l'altro a Montevideo con la Universidad de la Empreza in convenzione della Policia Uruguayense)]. Le sue fondamenta poi hanno assistito a tutta una serie di eredità scientifico-culturali dello stesso Prof. Mastronardi e le sue dirette collaborazioni con il Prof. Francesco Carrieri Neuropsichiatra e Medico Legale dell'Università di Bari, il Prof. Franco Ferracuti Psichiatra forense dell'Università di Roma Sapienza e il Prof. Franco Granone dell'Università di Torino, ricordato come il primo neuropsichiatra che diede un corpus accademico e scientifico all'ipnosi clinica con il suo Trattato di ipnosi, edito dalla UTET.
Alla rivista hanno poi fornito il proprio contributo alcuni Autori della **"Rivista di Psicopatologia forense, Medicina Legale, Criminologia"** dell'Università di Roma "Sapienza" che ha dismesso le sue pubblicazioni nel 2021

Vincenzo M. Mastronardi

Editorial notes

A brief history of the Journal.

This Journal draws inspiration from the valuable academic encounter with some well-known lecturers, acclaimed from the international scientific scene, like **George Palermo of Las Vegas, as well as Roy Hazelwood, Michael Napier and Gregory Vecchi – former FBI Trainers inQuantico, Virginia** – as well as from all the academic encounters over decades and, since 1988, from the establishment of several Master's Degrees in Criminology and Forensic Science - founded by Prof. Vincenzo M. Mastronardi, former Holder of the Chair of Forensic Psychopathology of the then Department of Psychiatric Sciences (of Sapienza University, Rome): 4 Master's Degrees were activated in Italy (2 at the Sapienza University in Rome, 1 at Unitelma – Sapienza and 1 at the University of International Studies of Rome – UNINT), as well as 2 in South America (1 in Buenos Aires with the Universidad de Ciencias Empresariales y Sociales – UCES, directed by the Rector L.M. De Simoni of the Universidad de la Policía Federal Argentina and 1 in Montevideo with the Universidad de la Empresa, partnering with the Uruguayan Police).

Its foundations have then witnessed the vast scientific and cultural heritage of Prof. Mastronardi himself and his direct collaborations with Prof. Francesco Carrieri - Neuropsychiatrist and Medical Examiner - of the University of Bari, with Prof. Franco Ferracuti - Forensic Psychiatrist - of the Sapienza University in Rome, and with Prof. Franco Granone of the University of Turin, remembered as the first Neuropsychiatrist who gave an academic and scientific body to clinical hypnosis with his "Hypnosis Treaty" published by UTET.
Some Authors of the "**Journal of Forensic Psychopathology, Forensic Medicine, Criminology** (Rivista di Psicopatologia forense, Medicina Legale, Criminologia)" – owned by the Sapienza University in Rome, which divested its publications in 2021 - have also provided their contributionsto this Journal.

Vincenzo M. Mastronardi

Notas editoriales.

Breve historia de la revista.

Esta revista se inspira en el precioso encuentro académico con algunos de los profesores más conocidos en el panorama científico internacional, como **George Palermo de Las Vegas, Roy Hazelwood, Michael Napier y Gregory Vecchi ex entrenadores del FBI en Quantico en Virginia,** así como de todas las reuniones académicas en el lapso de varias décadas y desde 1988 desde la fundación por el Prof. Vincenzo M. Mastronardi ex Director de la Cátedra de Psicopatología Forense del entonces Departamento de Ciencias Psiquiátricas de la Universidad de Roma Sapienza, con Maestría en Criminología y Ciencias Forenses, (4 en Italia; 2 en la UniversidadSapienza de Roma, 1 en la Unitelma-Sapienza y 1 en la Universidad de Estudios Internacionales de Roma), así como 2 en Sudamérica (uno en Buenos Aires con la Universidad de Ciencias Empresariales Y Sociales UCES dirigida por el Rector L.M. De Simoni de la Universidad de la Policía federal Argentina y la otra en Montevideo con la Universidad de la Empreza en convenioión de la Policía Uruguayense)]. Sus cimientos han sido testigos de toda una serie de legados científico-culturales del propio Prof. Mastronardi y sus colaboraciones directas con el **Prof. Francesco Carrieri Neuropsiquiatra y Médico Forense de la Universidad de Bari, el Prof. Franco Ferracuti Psiquiatra Forense de la Universidad Sapienza de Roma y el Prof. Franco Granone de la Universidad de Turín**, recordado como el primer neuropsiquiatra que dio uncorpus académico y científico a la hipnosis clínica con su Tratado de hipnosis, publicado por la UTET.
Algunos autores de la **"Revista de Psicopatología Forense, Medicina Legal, Criminología"** de la Universidad de Roma "Sapienza" dieron su contribución a la revista, que cesó sus publicaciones en 2021.

Vincenzo M. Mastronardi

NOTE EDITORIALI MIRATE AL PRESENTE NUMERO DELLA RIVISTA

L'argomento della pedopornografia online riveste ormai grande interesse soprattutto relativamente all'intelligenza artificiale la quale si presenta in grado di simulare tutta una serie di immagini azioni e interazioni con la sovrapposizione per esempio di voci e volti noti oltre che nell'ambito di soggetti minori.

Questo argomento ha voluto interessare non soltanto gli organi di investigazione nazionale ma anche sovranazionale con diversi contatti ormai estremamente fertili e con diverse parti del mondo.

Il capitolo pertanto ha tratto ispirazione nella sua approvazione da tutta una serie di studi già iniziati allorquando personalmente ebbi l'incarico dal ministro delle comunicazioni italiane di interessarmi del capitolo internet e minori e relativo all'autoregolamentazione in qualità di coordinatore del gruppo di lavoro famiglia minori e internet.

L'interesse personale per l'argomento ha avuto peraltro origine da alcuni casi per l'Italia affidatemi dalla magistratura italiana e talvolta per difesa dei minori e delle famiglie vittime di orribili reati.

Tra i casi affidatemi vi compare quello di Potenza in cui un'insegnante di sostegno collegandosi dal suo computer con il computer dell'abitazione degli stessi bambini abusati, inviava in tutto il mondo finanche in Malesia abbondanti immagini pedo pornografiche dei due bambini down che assisteva, firmandoli nel bagno della scuola.

La consulenza tecnica psichiatrica della difesa del pedopornofrafo, invocava un disturbo ossessivo grave della personalità in realtà chi scrive è riuscito a dimostrare che il soggetto in questione non soffriva di alcun disturbo di personalità non solo non inficiante a livello forense, bensì trattavasi unicamente di una parafilia di antica data che nulla aveva a che fare con qualsivoglia diagnosi psicopatologica.

Da quel momento storico risalente agli anni 2000 sono passati oltre vent'anni e le tecniche utilizzate dai pedopornografi sono diventate estremamente sofisticate ma ci conforta l'assunto che altrettanto sofisticate sono diventate le strategie investigative ormai a nostra disposizione che in tempo reale possono essere attivate.

Sussiste la problematica delle competenze territoriali internazionali ma gli ormai distesi e fisiologici rapporti tra organi di controllo dalle diverse nazioni, consentono ormai la possibilità di intervenire in modo estremamente capillare anche in altre parti del mondo distanti tra loro.

L'autrice dei lavori riportati in questo numero dedicato della rivista ha voluto approfondire le azioni degli organi di controllo nazionali ed internazionali quali per esempio l'Europol.

Per questo abbiamo scelto di dedicare l'intero volume a tale peculiare approfondimento.

Vincenzo Mastronardi
direttore
della rivista

INTERPOL: contrasto alla pedopornografia online

Bianca Francesca Berardi[1]

RIASSUNTO:

Con la crescente diffusione di Internet e del Dark Web, la produzione e la condivisione online di materiale di abuso e sfruttamento sessuale di minori hanno subito un incremento significativo, rendendo indispensabile la cooperazione internazionale per il contrasto a questo fenomeno.

In tale contesto, l'Organizzazione Internazionale di Polizia Criminale (INTERPOL) ha sviluppato l'International Child Sexual Exploitation (ICSE) Database, un sistema di categorizzazione di file multimediali contenenti materiali pedopornografici, creato per facilitare l'identificazione delle vittime, degli autori di reato e dei luoghi in cui avvengono gli abusi. Il sistema si avvale di programmi integrati, come software di riconoscimento facciale e di identificatori geografici, e algoritmi di analisi e confronto di immagini che ottimizzano l'identificazione e accelerano le indagini. Dal 2001, l'INTERPOL ha contribuito a identificare 42.300 minori vittime di abuso e sfruttamento sessuale in tutto il mondo, mentre l'ICSE Database è utilizzato da ben 70 paesi per la condivisione di informazioni tra le forze di polizia. Permangono tuttavia limiti strutturali, come discrepanze nelle legislazioni dei paesi aderenti, che inficiano la gestione soggettiva della categorizzazione dei file multimediali.

Questo studio analizza il funzionamento e l'utilizzo dell'ICSE Database, approfondendo le categorie in cui vengono suddivise immagini e video, i programmi integrati, i suoi limiti e le varie implicazioni nel contrasto alla pedopornografia online, mettendo in evidenza l'importanza di una cooperazione internazionale combinata con la condivisione di risorse tecnologiche.

Parole chiave: Contrasto alla pedopornografia online; Interpol; ICSE database; Cooperazione internazionale; Condivisione di tecnologie

ABSTRACT:

With the increasing spread of the Internet and the Dark Web, the production and online sharing of child sexual abuse and exploitation material has significantly risen, making international cooperation essential to combat this phenomenon.

In this context, the International Criminal Police Organization (INTERPOL) developed the International Child Sexual Exploitation (ICSE) Database, a multimedia file categorization system designed to facilitate the identification of victims, offenders, and locations where the abuse occurs. The system utilizes integrated programs, such as facial recognition software, geographic identifiers,

[1] Dottoressa magistrale in Investigazione, Criminalità e Sicurezza Internazionale - Università degli Studi Internazionali di Roma (UNINT)

and image analysis and comparison algorithms, which optimize identification processes and accelerate investigations. Since 2001, INTERPOL has helped identify 42,300 minors who have been victims of abuse and sexual exploitation worldwide, while the ICSE Database is used by 70 countries for sharing information among law enforcement agencies. However, structural limitations persist, such as discrepancies in the legislations of participating countries, which affect the subjective management of multimedia file categorization.

This study examines the functioning and the use of the ICSE Database, exploring the categories into which images and videos are divided, the integrated programs, its limitations, and the various implications for combating online child pornography, highlighting the importance of international cooperation combined with the sharing of technological resources.

Keywords: Countering online child pornography; Interpol; ICSE database; International cooperation; Sharing technologies

RESUMEN:

Con la creciente difusión de Internet y la Dark Web, la producción y el intercambio en línea de material de abuso y explotación sexual infantil ha aumentado significativamente, lo que hace imprescindible la cooperación internacional para contrarrestar este fenómeno.

En este contexto, la Organización Internacional de Policía Criminal (INTERPOL) desarrolló el International Child Sexual Exploitation (ICSE) Database, un sistema de categorización de archivos multimedia que contiene material de pornografía infantil, diseñado para facilitar la identificación de las víctimas, los autores de los delitos y los lugares donde ocurren los abusos. El sistema utiliza programas integrados, como software de reconocimiento facial, identificadores geográficos y algoritmos de análisis y comparación de imágenes, que optimizan el proceso de identificación y aceleran las investigaciones. Desde 2001, INTERPOL ha contribuido a la identificación de 42.300 menores víctimas de abuso y explotación sexual en todo el mundo, mientras que el ICSE Datbase es utilizado por 70 países para compartir información entre las fuerzas policiales. Sin embargo, persisten limitaciones estructurales, como discrepancias en las legislaciones de los países miembros, que afectan la gestión subjetiva de la categorización de los archivos multimedia.

Este estudio analiza el funcionamiento y el uso de el ICSE Database, profundizando en las categorías en las que se dividen las imágenes y videos, los programas integrados, sus limitaciones y las diversas implicaciones en la lucha contra la pornografía infantil en línea, destacando la importancia de la cooperación internacional combinada con el intercambio de recursos tecnológicos.

Palabras clave: Lucho contra la pornografía infantil en línea; Interpol; base de datos CISE; Cooperación internacional; Compartir tecnologías

1. Introduzione

Nella società odierna lo sfruttamento e l'abuso sessuale su minori sono un fenomeno globalmente diffuso che, a causa del sempre più frequente utilizzo di Internet e in particolare del Dark web, si è reso sempre più vasto e complesso: un solo sito contenente immagini sensibili può raggiungere Stati e continenti differenti. Oltre a rendere più facile produrre, condividere e accedere a materiale CSAM (Chils Sexual Abuse Material: materiale di abuso sessuale su minore) riducendo il rischio di essere tracciati, ha ampliato a livelli spropositati il mercato della pedopornografia e ha reso ancora più facile entrare in contatto con bambini che spesso accedono indifesi a siti in cui si sentono protetti. Purtroppo, proprio a causa della portata degli abusi che vengono perpetrati online, diventa difficile trovare prove empiriche indiscutibili di tali sfruttamenti. Proprio per questo, la cooperazione internazionale volta al contrasto di questo crimine è diventata fondamentale.

L'INTERPOL, organizzazione internazionale di polizia criminale, è un'organizzazione dedita alla cooperazione di polizia e al contrasto del crimine su scala internazionale.[2] Nata nel 1914, ad oggi conta 196 paesi membri. Durante il corso degli anni ha sviluppato degli obiettivi di rilevanza globale, chiamati "Global Policing Goals (GPG)", che richiedono l'attenzione e la collaborazione da parte di tutte le forze di polizia su scala globale, descrivendo anche come la comunità debba lavorare e cooperare per un'azione collettiva. Fra questi obiettivi, viene specificato "migliorare la risposta delle forze dell'ordine per proteggere le comunità vulnerabili". A far parte delle comunità vulnerabili vi sono chiaramente i minori. In particolare, vengono specificati come obiettivi la prevenzione, la rilevazione e infine l'interruzione dello sfruttamento sessuale dei minori online. [3]

In questo contesto, l'INTERPOL gioca un ruolo fondamentale a livello nazionale e internazionale e, a partire dal 2001, ospita l'International Child Sexual Exploitation Database, database globale all'avanguardia, costantemente aggiornato e in miglioramento, il cui scopo è quello di facilitare l'identificazione della vittima, dell'offensore e del luogo in cui avviene il crimine, sotto la supervisione della Crimes Against Children Unit, unità dell'INTERPOL specializzata. Ne verrà spiegato il funzionamento attraverso l'analisi dettagliata del sistema di categorizzazione del database e il suo utilizzo, assieme ai programmi integrati al database volti alla vera e propria facilitazione alle indagini di identificazione.

[2] Ministero dell'Interno, (2012), Cos'è l'Interpol, https://www1.interno.gov.it/mininterno/export/sites/default/it/sezioni/sala_stampa/notizie/polizia/2012_11_09_Interpol_storia.html

[3] Interpol, (Ottobre 2023), Global Policing Goals, https://www.interpol.int/content/download/12922/file/Global%20Policing%20Goals%202023_EN.pdf

2. Nascita dell'International Child Sexual Exploitation Database

L'INTERPOL è sempre stata all'avanguardia nel campo della protezione dei minori e, adottando un approccio che parte dalla vittima, ha sviluppato: un database, concentrato sull'identificazione della vittima, l'International Child Sexual Exploitation Database, e una task force apposita.

Si pensò allo sviluppo del database all'inizio degli anni '90, dopo che la polizia svedese sventò un'importante rete pedopornografica, sequestrando un grandissimo numero di video che riportavano prove di abusi sessuali su minori. Le autorità svedesi analizzarono immagini e video fotogramma per fotogramma e identificarono indicatori di geo localizzazione, fornendo ad altri paesi informazioni geografiche (per esempio elementi quali vegetazione, formazioni rocciose e scene all'aperto) che consentirono agli investigatori di giurisdizione di determinati paesi di restringere le ricerche a regioni specifiche nelle quali venivano prodotte le immagini. Grazie a questo lavoro vennero identificate numerose vittime e operati i relativi arresti. Il risultato consentì di ottenere il finanziamento perla creazione di un database di immagini che aveva l'obiettivo di catalogare in due categorie le vittime minorenni: "identificate" e "non identificate". Il database continuò a crescere grazie alle numerose richieste di aiuto provenienti da tutto il mondo per determinare lo stato delle vittime.[4]

Nel 1999, ad una conferenza indetta dall'INTERPOL, la polizia svedese presentò un programma in grado di riconoscere immagini in base a colore e forma. Il segretario generale dell'INTERPOL, Ronald K. Noble, intravide immediatamente l'utilità del programma utilizzato con il database di identificazione di vittime minori di abuso e sfruttamento sessuale già in sviluppo (divenuto operativo nel 2001) e chiese alla polizia svedese una copia del programma di riconoscimento da utilizzare presso la sede centrale a Lione.[5]

Ad oggi, 70 paesi sono collegati con l'ICSE database tramite il sistema di comunicazione sicuro "I-24/7" e, accedendo all'archivio del database contenente più di 4,9 milioni di immagini e video, hanno la possibilità di stabilire se il materiale delle loro indagini sia nuovo, noto o identificato. Questa opportunità consente di avere risposte immediate ed evita l'eventuale duplicazione del lavoro delle forze dell'ordine.[6]

[4] Onemi Global Solution, (2024), Our Story, https://www.onemi-global.com/ourstory

[5] Interpol (15 maggio 2003), Major child pornography operation broken in Sweden, https://www.interpol.int/News-and-Events/News/2003/Major-child-pornography-operation-broken-in-Sweden

[6] Interpol General Assembly in Monaco, (4 novembre 2014), Interpol´s International Child Sexual Exploitation Database, https://www.interpol.int/content/download/5433/file/83%20GA%20-%20Ministerial%20-%20P2.1%20-%20Germany.pdf

3. Funzionamento dell'ICSE Database

Nel corso di un'indagine nella quale vengano rilevati materiali pedopornografici che necessitano la verifica per l'identificazione di luogo, vittima e autori del reato, le forze dell'ordine certificate possono avvalersi dell'ICSE database e inserire al suo interno le immagini e i video rilevati per un'analisi immediata dei contenuti: la risposta istantanea che si riceve è se tali materiali siano già raccolti all'interno del database, come identificati o non identificati, o se invece siano nuove immagini, comunque utili all'interno del database per una futura identificazione.[7]
Nel database è possibile caricare singoli file, o raggruppamenti di immagini e video costruiti su sospetto o conoscenza di relazione a un singolo caso. I raggruppamenti di file si suddividono in due tipi:
1. "Series": raggruppamento di immagini e/o video secondo criteri ritenuti rilevanti per l'indagine da chi carica i file;
2. "Investigations": raggruppamento di "series" che segnala un'indagine in corso su tali serie.

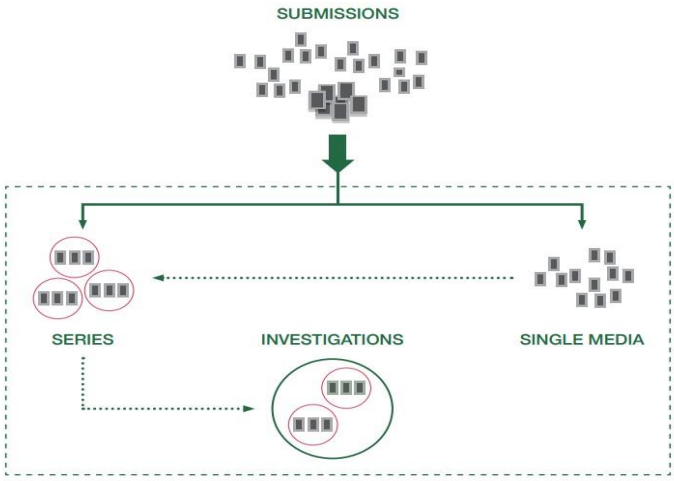

Figura 2: Organizzazione dei materiali nell'ICSE Database

Un paese membro dell'INTERPOL, per entrare a far parte della connessione al International Child Sexual Exploitation database, deve soddisfare determinati criteri: deve essere già presente e operativa un'unità contro l'abuso e lo sfruttamento sessuale dei minori e deve essere in vigore una legislazione che penalizzi la produzione, la distribuzione o il possesso di materiale pedopornografico. A tutti i paesi con i requisiti necessari viene fornita una formazione sull'utilizzo del database riguardo la classificazione e la funzionalità ai fini dell'identificazione.[8]
Ogni file multimediale viene caricato nell'ICSE database su volontà dei singoli che ritrovano il materiale nel corso delle loro indagini (forze di polizia e associazioni certificate), ma non esiste nessun mandato internazionale che obblighi i paesi a mantenere sempre aggiornato il database. Il compito di mantenere aggiornato il database è svolto dagli agenti delle forze dell'ordine, mossi da

[7] Interpol, (2018), Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material - February 2018, Technical report, pp. 5-6

[8]Interpol, (2024), International Child Sexual Exploitation Database, https://www.interpol.int/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database

senso etico e spirito di collaborazione, nazionale e internazionale. Sono proprio loro a promuovere una cooperazione più efficace e funzionante tra le diverse giurisdizioni.[9]

3.1. Sistema di Categorizzazione

L'ICSE database si basa su un sistema di categorizzazione: le prime informazioni di classificazione vengono fornite da chi carica sul database i file, il quale dovrebbe fornire informazioni dettagliate su ciò che viene raffigurato in tali immagini e video, sia inserendole nei campi prestabiliti nell'interfaccia del database, sia nel modulo di presentazione a testo libero dei casi, consegnato insieme a immagini e video. In seguito, l'unità specializzata dell'INTERPOL, Crimes Against Children Unit, avvia un processo di controllo e analisi del materiale. [10]

I tipi di file multimediali che vengono caricati all'interno del database dell'INTERPOL si possono suddividere in due categorie:

1. Qualsiasi immagine o video rappresentante pornografia minorile definita ad Articolo 20 comma 2 della Convenzione del Consiglio d'Europa sulla Protezione dei bambini contro lo sfruttamento e gli abusi sessuali (2007): "qualsiasi materiale che ritrae o rappresenta visivamente un bambino impegnato in atti sessuali espliciti, reali o simulati, o qualsiasi rappresentazione di organi sessuali di bambini a fini essenzialmente sessuali".[11] La definizione di bambino o minore è individuabile ad Articolo 3 della medesima Convenzione: "per "minore" si intende qualsiasi persona di età inferiore a 18 anni".[12]
2. Qualsiasi altra immagine o video che non rientri nella definizione di pornografia minorile, ma che potrebbe essere utile ai fini di indagine per l'identificazione del luogo, della vittima o dell'autore del reato. La scelta di archiviazione nel database di questo tipo di file multimediale ricade sull'ufficiale investigativo, il quale deve valutare il valore di ogni file a fini investigativi.[13]

Le prime categorie di informazioni che vengono assegnate a ciascun file multimediale appena caricato sono numeri arbitrari, i quali identificano in modo univoco ciascun file multimediale, serie

[9] Interpol, (2018), Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material - February 2018, Technical report, pag.6

[10] Ibidem, pag.7

[11] Convenzione del Consiglio d'Europa sulla Protezione dei bambini contro lo sfruttamento e gli abusi sessuali, (25 Ottobre 2007), https://rm.coe.int/16809f545d , pag.9

[12] Ibidem, pag.3

[13] Interpol, (2018), Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material - February 2018, Technical report, pag.7

di file raggruppati o ciascuna indagine avviata su una specifica "investigation". Viene successivamente indicato il formato dei file multimediali, se l'autore del reato contenuto nel file sia identificato o non identificato, il luogo sospettato o identificato in cui è avvenuto l'abuso e la prima data in cui il file è stato caricato all'interno del database.[14]

L'ulteriore categorizzazione viene progettata per l'analisi di informazioni concentrata su tre aspetti del contenuto di ciascun file multimediale: si cerca di categorizzare il maggior numero di informazioni riguardanti vittima, autore di reato e natura e gravità di vittimizzazione. Per questa categorizzazione l'interfaccia del database lascia poco spazio di descrizione, sono già presenti dei campi prestabiliti in cui inserire la codifica delle prove visibili. Per quanto riguarda le informazioni su vittima e autore di reato viene rilevato il numero visibile, l'età, il genere e l'etnia visibile. Per determinare la natura e la gravità della vittimizzazione presente nei file multimediali viene utilizzata la scala COPINE e la presenza o meno di temi parafiliaci. [15]

La scala COPINE (COmbating Pedophile Information Networks in Europe) venne creata per ridurre un problema di comunicazione fra paesi differenti, in quanto molti paesi hanno legislazioni differenti per la pedopornografia infantile e vengono utilizzati termini soggettivi per descrivere il contenuto delle immagini probatorie, e tenta di fornire una tipologia fissa di classifica per le immagini di pedopornografia. È espressa in 10 gradi o livelli di vittimizzazione mostrati nei materiali di abusi, in base al livello viene indicata la gravità della vittimizzazione (da 1 a 4 indica materiale pedopornografico con assenza di abusi o sfruttamento, 5 e 6 indicano materiale abusivo, da 6 a 10 indica materiale di sfruttamento): [16]

- Livello 1 / Indicativo – Immagini non erotiche e non sessualizzate che provengono da contesti di normalità come giornali, album di famiglia, fotografie di bambini che giocano. Il contesto e l'organizzazione delle immagini indicano inappropriatezza.
- Livello 2 / Nudista – Immagini di nudità o seminudità di minori provenienti da fonti legittime in cui contesto ed organizzazione risultano inappropriati.
- Livello 3 / Erotico – Immagini catturate di nascosto in ambienti sicuri che mostrano minori in biancheria intima o vari gradi di nudità.
- Livello 4 / Posa – Immagini di minori deliberatamente in posa, possono essere vestiti, seminudi o nudi. Il contesto e l'organizzazione devono suggerire interesse sessuale.
- Livello 5 / Posa erotica – Immagini di minori, vestiti o nudi, in pose provocatorie o sessuali.

[14] Ibidem, pag.28

[15] Ibidem, pag.31 e pp.77-81

[16] Quayle E., (2008), The COPINE Project, Irish Probation Journal, vol.5, pp.66 -69; Interpol, (2018), Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material - February 2018, Technical report, pag.79

- Livello 6 / Posa erotica esplicita – Immagini che mettono in risalto le zone genitali del minore, il quale può essere vestito o nudo.
- Livello 7 / Attività sessuale esplicita – Immagini che ritraggono minori, senza la partecipazione di adulti, in attività di masturbazione reciproca, autoerotismo, sesso orale e rapporti sessuali tra minori.
- Livello 8 / Assalto – Immagini di minori vittime di violenza sessuale consistente in toccamento da parte di un adulto.
- Livello 9 / Grave aggressione – Immagini di minori vittime di violenza sessuale che comprende penetrazione, masturbazione o sesso orale con adulti.
- Livello 10 / Sadico-Bestiale – Indica immagini che mostrano minori sottoposti ad azioni che implicano dolori (come essere legati, vincolati, picchiati, ecc.) o immagini che raffigurano il coinvolgimento di un animale nell'attività sessuale con un minore.

La presenza o meno di temi parafiliaci viene indicata per avere una griglia più dettagliata sul materiale pedopornografico raccolto e per avere un'idea più chiara della sofferenza della vittima.[17] Parafilia è un termine con cui si indicano comportamenti atipici e inusuali, necessari a chi ne è affetto, per ottenere eccitamento e soddisfazione sessuale. Questi comportamenti sono solitamente caratterizzati da utilizzo di oggetti non umani, attività di sofferenza o umiliazione e attività sessuale con partner non consenzienti. [18] Le parafilie prese in considerazione per quantificare la natura della vittimizzazione presente nei file multimediali sono:

- Feticismo delle parti del corpo: immagini concentrate su determinate e specifiche parti del corpo come capelli, piedi, mani, ecc.
- Feticismo per gli oggetti inanimati: concentrazione su oggetti inanimati quali giocattoli sessuali, calze, fumo etc. durante l'atto sessuale.
- Sadomasochismo: concentrazione su azioni volte a provocare e infliggere dolore e umiliazione, come giochi sessuali crudeli, bondage, tortura e temi BDSM.[19]
- Biastofilia: immagini che ritraggono attività sessuali coercitive, che implicano forza, minaccia o simile e che non prevedono il consenso del bambino.
- Zoofilia: immagini che ritraggono attività sessuali in cui sono coinvolti animali.

[17] Interpol, (2018), Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material - February 2018, Technical report, pp.79 e 81

[18] Quattrini F., Parafilie e devianza - psicologia e psicopatologia del comportamento sessuale atipico, Bologna, Giunti Editore, 2015, pp.13-14

[19] Ibidem, pag.71

- Travestitismo: concentrazione sul travestitismo, che può rivelare schemi di preferenza.
- Voyeurismo: immagini di nudo o atti sessuali riprese di nascosto, senza il consenso di chi è raffigurato.[20]
- Urofilia/Coprofilia: immagini raffigurante particolare concentrazione su minzione e defecazione.
- Necrofilia: immagini raffiguranti atti sessuali con cadaveri, immagini di cadaveri in posa, di autopsie e di scene di omicidi.
- Esibizionismo: immagini di sé stessi nella propria nudità, in particolare l'area genitale, mostrata pubblicamente ad altri, ad insaputa di questi ultimi. [21]

3.2. Baseline System

"Baseline System è un'iniziativa dell'INTERPOL volta a consentire, a terze parti, di rilevare e interrompere l'ulteriore circolazione di alcuni dei materiali più noti riguardanti abusi sessuali su minori eventualmente presenti sui propri sistemi."[22]

Baseline System è una categoria dell'ICSE database creata dall'Interpol con lo scopo di isolare i materiali pedopornografici più esecrabili, che dovrebbero essere illegali nella maggior parte delle giurisdizioni nazionali in cui esiste una legislazione in materia di pedopornografia. Viene impostata come standard internazionale per aiutare i vari paesi aderenti a identificare più velocemente quei materiali che provano abusi e sfruttamenti gravi di minori. Consiste in un elenco di impronte digitali proprie di tali file multimediali, che per essere inclusi nel Baseline System, devono soddisfare determinati criteri[23]:

- I minori raffigurati nei materiali devono essere "reali", non creati tramite Intelligenza Artificiale;
- L'età dei minori raffigurati non deve superare l'età puberale (nessun segno o primissimi segni di pubertà, inferiore ai 13 anni);
- I minori devono essere coinvolti o essere testimoni di attività sessuali;
- I media devono chiaramente concentrarsi sull'area sessuale o anale dei minori;

[20] Ibidem, pag.58

[21] Ibidem, pag.48

[22] Interpol, (2024), Blocking and Categorizing Content, https://www.interpol.int/Crimes/Crimes-against-children/Blocking-and-categorizing-content

[23] Interpol, (2018), Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material - February 2018, Technical report, pag.8

- L’abuso deve essere considerato grave, per calcolare la gravità si fa riferimento alla scala COPINE (verrà inserito tutto il materiale di livello COPINE da 6 a 10, e valutato il materiale di livello COPINE 5).

Affinché una determinata impronta digitale venga aggiunta all’interno della categoria del Baseline System non basta che vengano soddisfatti tutti e tre i criteri sopra elencati, ma vi è la necessità che tali criteri, sullo stesso materiale, siano confermati da almeno due diversi paesi o agenzie. Questi criteri devono poi essere ulteriormente verificati e confermati dall’unità Crimes Against Children dell’INTERPOL.

4. Utilizzo dell’ICSE Database

L’analisi dell’effettivo contenuto dei materiali caricati nell’ICSE database viene successivamente svolta dalla Crimes Against Children Unit e si concentra sulle impronte digitali (“hash”) proprie di ogni immagine o video, sul riconoscimento della vittima e, se presente, dell’autore del reato di abuso, e sull’analisi dell’ambiente e degli elementi esterni. All’ICSE database, per un’analisi più veloce e dettagliata a cui la Crimes Against Children Unit sovrintende, sono integrati diversi programmi che aiutano con il riconoscimento.[24]

Vi è un software di confronto immagini che aiuta gli specialisti all’identificazione della vittima e al raggruppamento di ogni possibile frame che la raffiguri, può identificare e rilevare similarità fra immagini o video. Vi è inoltre un ulteriore programma di confronto e riconoscimento immagini in base a colore e forma, questo aiuta la formazione di un raggruppamento di materiali riguardanti lo stesso caso o lo stesso luogo. Il programma è in grado di riconoscere dettagli materiali e piccoli e grandi particolari importanti a determinare identificatori geografici per capire dove le immagini o i video sono stati creati.[25]

[24] Interpol, (2024), Crimes Against Children, https://www.interpol.int/Crimes/Crimes-against-children

[25] Interpol, (14 aprile 2015), Global efforts to identify child abuse victims via INTERPOL boosted with Microsoft technology, https://www.interpol.int/en/News-and-Events/News/2015/Global-efforts-to-identify-child-abuse-victims-via-INTERPOL-boosted-with-Microsoft-technology

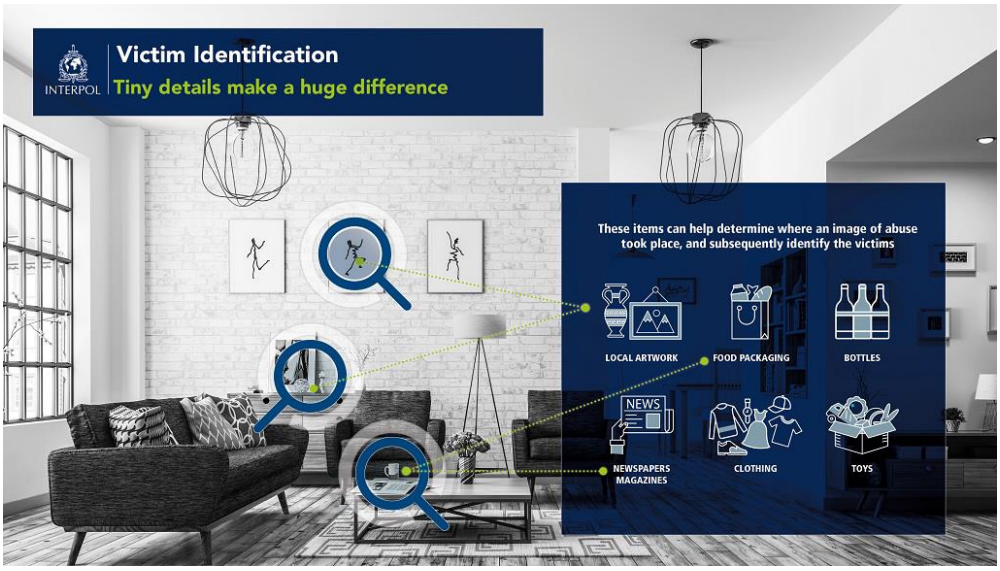

Figura 3: Victim Identification Program[26]

PhotoDNA è un programma creato da Microsoft e integrato dall'INTERPOL nell'ICSE database nel 2015. È in grado di assegnare impronte digitali a immagini e frame dei video, il programma trasforma i frame in formato bianco e nero e lo divide in quadrati, gli assegna poi un valore numerico che rappresenta l'ombreggiatura unica di ogni quadrato, l'insieme dei valori numerici compone l'"hash" (impronta digitale). L'"hash" è univoco e rimanda alla medesima fonte anche se l'immagine dovesse essere riprodotta o modificata di dimensioni e colori.[27]

Per arrivare allo scopo di identificazione di vittima, luogo e autore di reato di abuso, oltre ai programmi integrati all'ICSE database, la Crimes Against Children Unit può utilizzare tutti i mezzi di cui l'INTERPOL dispone. Un esempio è il Facial Recognition System (IFRS), adottato dall'INTERPOL nel 2016. Si tratta di un sistema di riconoscimento facciale che funge da database globale di immagini facciali ricevute dalla maggior parte dei suoi paesi membri. È in grado di confrontare e analizzare forme e proporzioni, tratti e contorni facciali utili per le identificazioni di criminali e persone scomparse.[28] Viene sviluppato tramite un'applicazione software biometrica automatizzata fornita da IDEMIA[29]. L'identificazione biometrica si basa su dati ottenuti da determinate caratteristiche fisiche e comportamentali che vengono confrontati con dati precedentemente acquisiti e conservati nei database del sistema. Questo si basa su due tipi di dati biometrici: morfologici (struttura del corpo e forma del viso, possono

[26] Interpol, Victim Identification Task Force, https://www.interpol.int/var/interpol/storage/images/7/4/6/5/155647-1-eng-GB/adb3991e86a9-038-48-Infographic_Victim-identification-Lab_03.jpg

[27] Microsoft, (2024), PhotoDAN, https://www.microsoft.com/en-us/PhotoDNA

[28] Interpol, (2024), Facial Racognition, https://www.interpol.int/How-we-work/Forensics/Facial-Recognition

[29] "IDEMIA è una società tecnologica francese che fornisce servizi di sicurezza, software per il riconoscimento facciale e sistemi di identificazione biometrica a società private e governi" IDEMIA, (2024), https://www.idemia.com/

essere mappati con l'utilizzo di scanner digitali, i quali tengono conto di invecchiamento, chirurgia, abuso di alcool e droghe) e comportamentali (modelli unici di una persona come modo di camminare e parlare).[30]

Il Facial Recognition System è automaticamente collegato con il sistema di "Notices" dell'INTERPOL, con cui è collegato anche l'ICSE Database e di cui si avvale la Crimes Against Unit Children. Le "Interpol Notices" sono un sistema di richieste di cooperazione internazionali relative alla criminalità e alle persone scomparse. I paesi membri possono inoltrare diversi tipi di "Notices" facendo richiesta al proprio Ufficio Centrale Nazionale INTERPOL. Per quanto riguarda i crimini contro i bambini l'INTERPOL prevede tre tipi di "Notices"[31]:

1. Green Notice: per informare riguardo una specifica attività criminale di un individuo autore di tratta di bambini a scopi sessuali o di detenzione di siti online di pedopornografia, abuso e sfruttamento sessuale di minori, o qualsiasi attività considerata una minaccia per i bambini.
2. Blue Notice: per raccogliere informazioni riguardo un individuo coinvolto in un crimine, che sia la sua attività, posizione o identità.
3. Yellow Notice: emessa, in questo caso, per aiutare a localizzare un minore ritenuto scomparso o rapito, caduto vittima di tratta e registrato in siti di pedopornografia e abuso sessuale.

La Crimes Against Children Unit, che sovraintende il lavoro di analisi del database, integra quindi tutti i programmi e mezzi di ricerca di cui l'INTERPOL dispone, concentrandosi sui numerosi casi esistenti e irrisolti, per ricavare più informazioni possibili e arrivare all'identificazione della vittima e dell'autore di abuso. Inoltre, vi sono operatori con il compito specifico di sovrintendere l'analisi dei singoli file caricati allo scopo di creare "Series" di file multimediali, per arrivare così a formare una "Investigation" e avviare una vera e propria indagine volta all'identificazione della vittima. Se il lavoro di analisi dell'unità porta all'identificazione della vittima o dell'autore del reato, vengono informati gli Uffici Centrali Nazionali INTERPOL competenti attraverso il sistema di comunicazione sicuro "I-24/7": vengono avvisati i paesi che hanno inserito le immagini originali all'interno del International

[30] Kaspersky, (2024), Cos'è la biometrica? Come viene utilizzata nella sicurezza?, https://www.kaspersky.it/resource-center/definitions/biometrics

[31] Interpol, (2024), Victim Identification, https://www.interpol.int/Crimes/Crimes-against-children/Victim-identification

Child Sexual Exploitation database ed eventualmente i paesi ritenuti originari della vittima o dell'autore del reato di abuso identificati.[32]

5. Limiti del Database

Non tutto il materiale ritrovato durante le indagini e i monitoraggi viene o può essere inserito in modo adeguato all'interno dell'International Child Sexual Exploitation Database. I casi più comuni registrati in un rapporto scritto da ECPAT International e dall'INTERPOL circa il database nel 2018 sono: i casi di abusi sessuali su minore in live streaming, le immagini autoprodotte dai minori stessi e un determinato numero di immagini che non vengono inserite all'interno del database in quanto non ritenute "pedopornografia" da determinati paesi membri secondo le loro leggi.[33]

5.1. Abuso sessuale di minori in live streaming

Questa pratica consiste nello sfruttamento sessuale di minori in diretta streaming online, prevede la visione da parte di un pubblico pagante che, tramite apposite chat, può dettare come determinate pratiche sessuali debbano essere eseguite. I minori costretti a tali atti sessuali li possono compiere con altri minori o con adulti. L'abuso di minori in live streaming può quindi comportare molteplici forme di abuso e sfruttamento come la prostituzione minorile e la produzione di materiale pedopornografico, inoltre diventa sempre più preoccupante a causa dello sfruttamento finanziario della vittima da parte degli autori di reato.[34]

Durante questi live streaming non è possibile registrarne il contenuto, in quanto consterebbe in una duplicazione di materiale che andrebbe a ri-vittimizzare ulteriormente i minori raffigurati, pertanto, a meno che uno degli autori di reato partecipante alla sessione live streaming non registri i contenuti e gli abusi, lo streaming tende a non lasciare tracce utili all'identificazione dei minori. Inoltre, l'abuso sessuale di minori in diretta streaming rende confusa la distinzione legale tradizionale di chi abusa tramite contatto con minore e chi abusa il minore riproducendo e diffondendo materiale pedopornografico. In particolare, in quei paesi in cui non vi è

[32] Interpol, (2024), Our response to crimes against children, https://www.interpol.int/Crimes/Crimes-against-children/Our-response-to-crimes-against-children

[33] Interpol, (2018), Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material - February 2018, Summary Report

[34] Polizia di Stato, (5 maggio 2024), INTERNET, IL PAESE DELLE MERAVIGLIE...?, https://www.poliziadistato.it/statics/20/brochure-5-maggio-2024.pdf

legislazione ferrea sull'argomento, come le Filippine: dal 2021 l'età del consenso è stata alzata a 16 anni, prima del 2021 era 12 anni, per di più il mero possesso di pornografia infantile non è punito in quanto legale, è invece illegale la produzione e la distribuzione. A causa di queste falle legislative sono sempre più comuni i "child sex webcam centers" che fanno aumentare il traffico di bambini proprio a scopo di sfruttamento sessuale da remoto.

5.2. Immagini sessuali autoprodotte dai minori

Le immagini sessuali autoprodotte dai giovani in circolazione sono vastissime, possono essere divise in due categorie[35]:

- Materiali realmente autoprodotti dai minori raffigurati;
- Materiali prodotti e condivisi online attraverso coercizione o adescamento.

Indipendentemente dal motivo per cui tali immagini siano state scattate, una volta distribuite, diventano parte integrante di tutto il materiale pedopornografico e, dove provabile, riguardante vero e proprio abuso e sfruttamento sessuale di minori. La sfida è quella di riuscire a distinguere in modo affidabile i comportamenti di "sexting"[36] fra minori considerabili innocui e materiale che presenta evidente abuso e sfruttamento sessuale, dove quindi esiste un crimine perseguibile con autori di reato.[37]

5.3. Inserimento dati soggettivo

Le immagini e i video inseriti nel database vengono presentate e categorizzate da personale delle forze dell'ordine formato e certificato o da analisti non appartenenti alle forze dell'ordine accreditati. Secondo il rapporto scritto da ECPAT International e dall'Interpol circa il database nel 2018, vi sono incoerenze e omissioni nell'inserimento dei dati e informazioni nella categorizzazione e presentazione di immagini e video dei singoli utenti e paesi. Viene evidenziato come l'interfaccia di immissione dei dati sia progettata fornendo un vasto numero di campi vuoti come opzione di classificazione. Anche i moduli di presentazione dei casi sono completamente a testo libero. Riducendo il numero di opzioni di campi vuoti e standardizzando

[35] Interpol, (2018), Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material - February 2018, Technical report, pp.14-15

[36] Con sexting si intende generalmente lo scambio messaggi, audio, immagini o video - specialmente attraverso smartphone o chat di social network - a sfondo sessuale o sessualmente espliciti, comprese immagini di nudi o seminudi. Questo fenomeno si è molto diffuso negli ultimi anni, anche tra i minori." Save the Children, (2024), Il sexting e gli adolescenti: cos'è e perché è diffuso, https://www.savethechildren.it/blog-notizie/il-sexting-e-gli-adolescenti-cos-e-perche-e-diffuso

[37] Interpol, (2018), Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material - February 2018, Technical report, pp.14-15, 49-51

il modulo di presentazione si riuscirebbe ad armonizzare la categorizzazione dei file. Inoltre, viene considerato che aumentando i campi di informazione sulle tipologie di aggressioni, tipologie di oggetti utilizzati nei file multimediali, etc. si consentirebbe di ottenere una classificazione più dettagliata e meno soggettiva dei casi. L'obiettivo è avere la possibilità di collegare il più velocemente possibile immagini e video contenuti nell'ICSE database, armonizzare la categorizzazione dei file accelererebbe il processo di identificazione.[38]Il maggiore problema legato alla soggettività nell'inserimento dei dati da parte dei vari paesi membri è la differenza a livello giuridico fra CSAM (materiale di abuso sessuale su minori), il quale comprende tutto il materiale che si concentra sui genitali dei minori e rappresenta specificatamente atti di abuso sessuale ed eventuali parafilie presenti, e CSEM (materiale di sfruttamento sessuale su minori), categoria più ampia che comprende tutto il materiale considerato "pornografia infantile", comprese le immagini di minori in posa o solo in contesti sessualizzati, ma la cui detenzione in molti paesi è considerata legale.

Nel contesto di un database globale creato con lo scopo di contenere e collegare tutto il possibile materiale di abuso e sfruttamento sessuale minorile, la diversità di vedute rispetto a quali immagini, che siano CSAM o CSEM, possano essere considerate legali o no diventa essenziale. Molti dei contenuti raffiguranti minori in posa vengono considerati "zona grigia", un esempio sono i siti di "modeling" che espongono fotografie di minori modelli le cui pose possono risultare ambigue e potenzialmente sfruttabili in contesti non etici. Proprio questa differenza diventa un ostacolo, poiché sono gli stessi paesi membri, dopo aver fatto richiesta al proprio Ufficio Centrale Nazionale INTERPOL, ad inserire all'interno del database le immagini trovate e considerate materiale probatorio. Ma se determinate immagini non vengono considerate materiale pedopornografico, queste non vengono inserite, e le vittime e gli autori di reato non vengono così identificati.[39]

Conclusioni

Come illustrato, il crimine di abuso e sfruttamento sessuale online ha ormai raggiunto una diffusione globale a causa del sempre più frequente utilizzo di Internet e del Dark web, divenuto accessibile a uno svariato numero di utenti. La complessità di tali crimini si è ampliata al punto da diventare di natura forzatamente transnazionale, richiedendo interventi di cooperazione internazionale mirati e costanti da parte delle forze dell'ordine.

[38] Interpol, (2018), Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material - February 2018, Summary Report, pag.56

[39] Ibidem, pp.14-15

In prima linea contro questo crimine vi è l'organizzazione internazionale INTERPOL, che lavora, con le proprie competenze specifiche, assieme alle autorità preposte degli Stati membri aderenti alle iniziative in tale campo. Ha sviluppato e ospita strumenti tecnologici avanzati in grado di aiutare e favorire le indagini di polizia nel contrasto al crimine di abuso e sfruttamento sessuale online. Si tratta di strumenti di analisi di immagini e video e un database consultabile utile per velocizzare il lavoro degli investigatori. L'ICSE database contiene 4,9 milioni di immagini e video e ha, ad oggi, contribuito a identificare oltre 42.300 minori vittime di abuso e sfruttamento sessuale in tutto il mondo.[40]

La cooperazione internazionale per il contrasto all'abuso e allo sfruttamento sessuale di minori online è diventata uno strumento fondamentale e imprescindibile per la lotta ad un crimine di natura inevitabilmente transnazionale e richiede risposte coordinate tra le forze dell'ordine. Solo grazie alla condivisione di informazioni e risorse è possibile contrastare efficacemente il traffico di immagini e contenuti illeciti. La combinazione di risorse tecnologiche avanzate e una rete di cooperazione internazionale solida rappresenta uno dei pilastri fondamentali in un approccio globale sui cui poggia il successo dell'impegno al contrasto di un crimine così efferato.

Bibliografia

Interpol, (2018), Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material - February 2018, Technical report, disponibile online: https://www.interpol.int/content/download/9365/file/Technical%20report%20-%20Towards%20a%20Global%20Indicator%20on%20Unidentified%20Victims%20in%20Child%20Sexual%20Exploitation%20Material.%20February%202018.pdf

Quattrini F., Parafilie e devianza - psicologia e psicopatologia del comportamento sessuale atipico, Bologna, Giunti Editore, 2015

Quayle E., (2008), The COPINE Project, Irish Probation Journal, vol.5

Sitografia

Convenzione del Consiglio d'Europa sulla Protezione dei bambini contro lo sfruttamento e gli abusi sessuali, (25 Ottobre 2007), https://rm.coe.int/16809f545d

IDEMIA, (2024), https://www.idemia.com/

Interpol (15 maggio 2003), Major child pornography operation broken in Sweden, https://www.interpol.int/News-and-Events/News/2003/Major-child-pornography-operation-broken-in-Sweden

[40] Interpol, (2024), International Child Sexual Exploitation database, https://www.interpol.int/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database

Interpol General Assembly in Monaco, (4 novembre 2014), Interpol´s International Child Sexual Exploitation Database, https://www.interpol.int/content/download/5433/file/83%20GA%20-%20Ministerial%20-%20P2.1%20-%20Germany.pdf

Interpol, (14 aprile 2015), Global efforts to identify child abuse victims via INTERPOL boosted with Microsoft technology, https://www.interpol.int/en/News-and-Events/News/2015/Global-efforts-to-identify-child-abuse-victims-via-INTERPOL-boosted-with-Microsoft-technology

Interpol, (Ottobre 2023), Global Policing Goals, https://www.interpol.int/content/download/12922/file/Global%20Policing%20Goals%202023_EN.pdf

Interpol, (2024), Blocking and Categorizing Content, https://www.interpol.int/Crimes/Crimes-against-children/Blocking-and-categorizing-content

Interpol, (2024), Crimes Against Children, https://www.interpol.int/Crimes/Crimes-against-children

Interpol, (2024), Facial Racognition, https://www.interpol.int/How-we-work/Forensics/Facial-Recgnition

Interpol, (2024), International Child Sexual Exploitation Database, https://www.interpol.int/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database

Interpol, (2024), Victim Identification, https://www.interpol.int/Crimes/Crimes-against-children/Victim-identification

Interpol, (2024), Victim Identification Task Force, https://www.interpol.int/var/interpol/storage/images/7/4/6/5/155647-1-eng-GB/adb3991e86a9-038-48-Infographic_Victim-identification-Lab_03.jpg

Kaspersky, (2024), Cos'è la biometrica? Come viene utilizzata nella sicurezza?, https://www.kaspersky.it/resource-center/definitions/biometrics

Microsoft, (2024), PhotoDAN, https://www.microsoft.com/en-us/PhotoDNA

Ministero dell'Interno, (2012), Cos'è l'Interpol, https://www1.interno.gov.it/mininterno/export/sites/default/it/sezioni/sala_stampa/notizie/polizia/2012_11_09_Interpol_storia.html

Onemi Global Solution, (2024), Our Story, https://www.onemi-global.com/ourstory

Polizia di Stato, (5 maggio 2024), INTERNET, IL PAESE DELLE MERAVIGLIE...?, https://www.poliziadistato.it/statics/20/brochure-5-maggio-2024.pdf

Save the Children, (2024), Il sexting e gli adolescenti: cos'è e perché è diffuso, https://www.savethechildren.it/blog-notizie/il-sexting-e-gli-adolescenti-cos-e-perche-e-diffuso

Address correspondence to bianca.francesca.ber@alice.it

Received September 15, 2024 accepted September 21, 2024

EUROPOL: contrasto alla pedopornografia online (PARTE II)

Bianca Francesca Berardi[1]

RIASSUNTO

Il contrasto alla pedopornografia online rappresenta una delle sfide più complesse per le autorità di polizia a livello globale. La crescente diffusione di materiale di abuso sessuale su minori attraverso Internet e l'anonimato garantito dalle nuove tecnologie hanno reso indispensabile una cooperazione internazionale efficace e un costante aggiornamento delle strategie in corso.

L'EUROPOL, attraverso il suo European Cybercrime Centre (EC3), svolge un ruolo centrale nel coordinare le attività investigative e sviluppare strumenti tecnologici avanzati per l'identificazione delle vittime e la repressione di tale crimine. L'uso di database specializzati, come l'Analysis Project Twins e l'Investigation Video and Audio System (IVAS), unito al supporto di taskforce internazionali come la Virtual Global Taskforce (VGT) e la Victim Identification Taskforce (VIDTF), ha permesso di migliorare significativamente le capacità di individuazione e soccorso delle vittime. Inoltre, la cooperazione tra autorità di polizia, enti governativi e organizzazioni internazionali ha favorito un maggiore coordinamento nel monitoraggio delle reti illecite e nella prevenzione degli abusi.

Tuttavia, la continua evoluzione delle minacce, come la produzione di materiale generato dall'Intelligenza Artificiale, la diffusione di reti peer-to-peer e l'uso crescente del Dark web, richiede un costante aggiornamento delle strategie e delle tecnologie investigative.

Questo studio analizza le iniziative in corso e le sfide emergenti evidenziate dal EUROPOL nel contrasto alla pedopornografia online, evidenziando l'importanza della cooperazione transnazionale e dell'innovazione tecnologica nella lotta a questo fenomeno.

Parole chiave: Contrasto alla pedopornografia online, Europol, EC3, Database e software, Taskforce, Condivisione di informazioni.

ABSTRACT

The fight against online child sexual abuse material (CSAM) represents one of the most complex challenges for law enforcement authorities worldwide. The increasing dissemination of such material through the Internet and the anonymity provided by new technologies have made effective international cooperation indispensable, alongside a continuous update of ongoing strategies.

EUROPOL, through European Cybercrime Centre (EC3), plays a central role in coordinating investigative activities and developing advanced technological tools for victim identification and crime suppression. The use of specialized databases, such as the Analysis Project Twins and the Investigation Video and Audio System (IVAS), combined with the support of international task

[1] Dottoressa magistrale in Investigazione, Criminalità e Sicurezza Internazionale - Università degli Studi Internazionali di Roma (UNINT)

forces like the Virtual Global Taskforce (VGT) and the Victim Identification Taskforce (VIDTF), has significantly enhanced the ability to locate and rescue victims. Furthermore, cooperation among law enforcement authorities, government agencies, and international organizations has facilitated greater coordination in monitoring illicit networks and preventing abuse.

However, the continuous evolution of threats, such as the production of AI-generated CSAM, the proliferation of peer-to-peer networks, and the increasing use of the Dark Web, requires constant updates in investigative strategies and technologies.

This study analyses ongoing initiatives and emerging challenges highlighted by EUROPOL in combating online CSAM, underscoring the importance of transnational cooperation and technological innovation in the fight against this phenomenon.

Keywords: Countering online child pornography, Europol, EC3, Databases and software, Taskforce, Information sharing

RESUMEN

La lucha contra el material de abuso sexual infantil en línea (CSAM) representa uno de los desafíos más complejos para las autoridades policiales globalmente. La creciente difusión de dicho material a través de Internet y el anonimato garantizado por las nuevas tecnologías han hecho indispensable una cooperación internacional efectiva, además de una actualización constante de las estrategias en curso.

EUROPOL, a través de el European Cybercrime Centre (EC3), desempeña un papel central en la coordinación de actividades investigativas y el desarrollo de herramientas tecnológicas avanzadas para la identificación de víctimas y la represión de este delito. El uso de bases de datos especializadas, como el Analysis Project Twins y el Investigation Video and Audio System (IVAS), junto con el apoyo de taskforce internacionales como la Virtual Global Taskforce (VGT) y la Victim Identification Taskforce (VIDTF), ha mejorado significativamente la capacidad de localizar y rescatar a las víctimas. Además, la cooperación entre autoridades policiales, organismos gubernamentales y organizaciones internacionales ha favorecido una mejor coordinación en el monitoreo de redes ilícitas y en la prevención de abusos.

Sin embargo, la constante evolución de las amenazas, como la producción de CSAM generado por Inteligencia Artificial, la proliferación de redes peer-to-peer y el creciente uso de la Dark Web, exige una actualización continua de las estrategias y tecnologías investigativas.

Este estudio analiza las iniciativas en curso y los desafíos emergentes destacados por EUROPOL en el contraste contra la pedopornografía en línea, resaltando la importancia de la cooperación transnacional y la innovación tecnológica en la lucha contra este fenómeno.

Palabras clave: Lucha contra la pornografía infantil en línea, Europol, EC3, Bases de datos y software, Grupo de trabajo, Intercambio de información

1. Introduzione

"La portata globale e l'anonimato di Internet hanno notevolmente facilitato la distribuzione e l'accesso a materiale di abusi sessuali su minori. Gli autori di reati possono ora produrre, scambiare e persino dirigere video in diretta di bambini e neonati che subiscono abusi. Possono anche entrare in contatto diretto con i bambini tramite social network e funzioni di chat in giochi o app."[2]

Il ruolo cruciale della cooperazione, sia a livello internazionale che nazionale, nella prevenzione e nel contrasto alla pedopornografia online è diventato non solo fondamentale, ma è l'unica risposta possibile per un crimine diventato inevitabilmente di natura globale. L'esatta portata del problema non è chiara, le forze dell'ordine di tutto il mondo concordano che sia sottostimato e onnipresente anche se ben nascosto: trovare evidenze empiriche indiscutibili è molto difficile.

L'European Police Office (EUROPOL), organo soprannazionale istituito in ambito intergovernativo allo scopo di rendere più efficace la cooperazione delle autorità nazionali di polizia nella lotta contro le forme più gravi di criminalità, considera il crimine di abuso e sfruttamento sessuale di minori online un crimine informatico ed è pertanto di competenza del European Cybercrime Centre (EC3)[3], a cui verrà riservata particolare attenzione. Il lavoro dell'EC3 è accostato al rilevante contributo della Victim Identification Taskforce (VIDTF) e della Virtual Global Taskforce (VGT), gruppi di esperti creati con l'obiettivo di identificare le vittime di abusi e sfruttamenti sessuali online, di cui verranno spiegati ruolo e apporto.

[2] Interpol, (2024), https://www.interpol.int/Crimes/Crimes-against-children

[3] Europol, (2024), Child Sexual Exploitation, https://www.europol.europa.eu/crime-areas/child-sexual-exploitation

2. European Cybercrime Centre

L'European Cybercrime Centre (EC3), centro europeo per la lotta alla criminalità informatica, istituito nel 2010 dalla Commissione Europea, offre supporto agli Stati membri fungendo da polo centrale per le informazioni, agevola ricerca e sviluppo per le operazioni e le indagini delle forze di polizia ed è specializzato per indagini e operazione nel fornire supporto tecnico e forense.

Ogni anno l'EC3 pubblica l'Internet Organized Crime Threat Assessment (IOCTA), valutazione delle minacce su Internet poste dalla criminalità organizzata e rapporto strategico volto a descrivere gli sviluppi emergenti riguardo la criminalità informatica, così da individuare questi processi e riuscire a bloccarli sul nascere. Uno dei suoi obiettivi è partecipare attivamente nella lotta alla distribuzione di materiale di abuso e sfruttamento sessuale di minori, adescamento, sextortion[4] e materiale autoprodotto, dedicandosi alla prevenzione, intercettazione e impedimento della condivisione di questi materiali tramite reti peer-to-peer e la chiusura di siti e reti pedopornografiche.

Le principali minacce in materia di sfruttamento sessuali di minori evidenziate dall'EC3:

1. Reti peer-to-peer (P2P) e accesso anonimizzato grazie alle Darknet – La tecnologia P2P permette a due utenti il trasferimento di materiale (immagini, video, valuta virtuale) senza la necessità che vi sia un ente centrale terzo che governi la transazione. Le Darknet sono reti private virtuali che consentono di oscurare gli indirizzi IP, di conseguenza diventa difficile individuare i fornitori dei servizi e l'identità dell'emittente, impediscono di tracciare il traffico e l'identità di coloro che partecipano ad una comunicazione digitale, la più famosa è TOR (The Onion Router), utilizzata per accedere al dark web, rende difficile il tracciamento delle navigazioni grazie al suo circuito virtuale crittografato a strati. Queste tecnologie, grazie all'alto livello di anonimato garantito, creano le piattaforme adatte all'accesso, scambio e distribuzione di materiale di abuso e sfruttamento su minori e in cui i criminali si sentono liberi di portare avanti il loro comportamento abusivo.[5]

[4] Trattasi di truffa perpetrata ai danni di utenti internet, i truffatori una volta che hanno costruito una buona relazione e hanno acquisito informazioni, invitano le vittime a coinvolgersi in attività sessuali online che vengono a loro insaputa videoregistrate. Successivamente i truffatori minacciano le vittime, nell'ipotesi che non versino una certa quantità di denaro o l'invio di ulteriore materiale, di diffondere i video compromettenti a tutti i loro contatti online. Ministero della Giustizia, (7 giugno 2017), Sextortion Scams, https://www.giustizia.it/giustizia/it/mg_2_5_12_1.page?contentId=GLM1144677#

[5] Europol, (2024), Child Sexual Exploitation, https://www.europol.europa.eu/crime-areas/child-sexual-exploitation

2. Abuso sessuale di minori in live streaming – Immagini e video nuovi e non visti prima, a livello di distribuzione commerciale, sono molto preziosi e vengono quindi pagati molto di più rispetto al materiale già in circolazione. Anche per questo è diventata una pratica sempre più diffusa, permette a chi produce e distribuisce materiale di abuso e sfruttamento sessuale di minori di guadagnare somme di denaro estremamente superiori rispetto alla distribuzione di materiale già visto. L'abuso in live streaming dei minori diventa un modo più efficace per generare materiale mai visto e soddisfare nello specifico le perversioni dei paganti. Ciò che preoccupa maggiormente è la crescita degli abusi in live streaming di minori che vivono in quei paesi dove non sono protetti dalla legislazione e a causa di questa differenza legislativa fra Stati è in aumento anche il traffico di minori a fini di sfruttamento sessuale.[6]
3. Immagini autoprodotte ed estorsione sessuale – Il possesso di uno smartphone da parte di bambini, anche di piccola età, è ormai una prassi comunemente accettata, ma l'aumento di questo fenomeno ha portato alla produzione di un grande quantitativo di materiale sessuale auto-generato di minori, spesso adolescenti. Tale materiale è frutto principalmente di due pratiche: viene condiviso fra due coetanei minori con intenti innocenti (un esempio è il "sexting"[7] fra adolescenti, consiste nello scambio di messaggi, immagini e video sessualmente espliciti), ma un terzo soggetto viene in possesso del materiale e, senza il loro consenso, procede alla vittimizzazione dei minori; la seconda pratica riguarda l'adescamento a fini di estorsione sessuale, la vittima minore viene avvicinata online (piattaforme di gioco online e social media) e, dopo che gli adescatori ottengono la sua fiducia, la inducono ad inviare materiale sessualmente esplicito, che diventerà poi leva di estorsione per ottenere ulteriori immagini e video.[8]

[6] Polizia di Stato, (5 maggio 2024), INTERNET, IL PAESE DELLE MERAVIGLIE...? https://www.poliziadistato.it/statics/20/brochure-5-maggio-2024.pdf , pag. 10

[7] Con sexting si intende generalmente lo scambio messaggi, audio, immagini o video - specialmente attraverso smartphone o chat di social network - a sfondo sessuale o sessualmente espliciti, comprese immagini di nudi o seminudi. Questo fenomeno si è molto diffuso negli ultimi anni, anche tra i minori." Save the Children, (2024), Il sexting e gli adolescenti: cos'è e perché è diffuso, https://www.savethechildren.it/blog-notizie/il-sexting-e-gli-adolescenti-cos-e-perche-e-diffuso

[8] ECPAT, (2024), Summary paper on online child sexual exploitation, https://ecpat.org/wp-content/uploads/2021/05/ECPAT-Summary-paper-on-Online-Child-Sexual-Exploitation-2020.pdf pp. 7-8

4. CSAM[9] prodotti dall'Intelligenza Artificiale – Il problema principale del materiale di abuso e sfruttamento sessuale di minori prodotto dall'Intelligenza Artificiale è lo sviluppo repentino per cui il materiale appare autentico e le vittime sembrano reali, diventa quindi difficile distinguere immagini e video generati artificialmente da materiali raffiguranti bambini realmente abusati. Questi nuovi tipi di file multimediali pongono una grande sfida per le agenzie delle forze dell'ordine nell'identificazione di vittime e autori. I motivi sono diversi, molte immagini potrebbero raffigurare minori non coinvolti realmente in attività sessuali, ma comunque vittimizzati in quanto la loro immagine viene distorta, utilizzata e pubblicata, inoltre il quantitativo di immagini interamente generate dall'AI tiene occupati gli agenti incaricati di analizzare le immagini creando così rallentamenti nell'identificazione di vere vittime che subiscono abusi.[10]

Lo IOCTA 2024 mette in luce come le nuove tecnologie stiano diventando una sfida per le forze dell'ordine che devono aggiornarsi e trovare nuovi strumenti investigativi, sia in termini di risorse umane che di competenze tecniche. I minori che subiscono abuso e sfruttamento sessuale online non vengono vittimizzati solo per interesse sessuale, ma anche per un interesse economico: sia a fini di estorsione sia, principalmente, per un vero e proprio mercato di file multimediali pedopornografici, che attraverso il black market si sta espandendo sempre di più e con l'utilizzo delle nuove tecnologie sopra descritte sta diventando più difficile tenere d'occhio i flussi di denaro e di scambio dati.[11]

Vi è un sistema "Notice and Takedown" (avviso e rimozione) per cui i dominii riportati alle forze dell'ordine vengono rimossi dall'accesso pubblico. Le segnalazioni arrivano alle hotline[12], le quali hanno il compito di valutare la legalità del contenuto segnalato. Nel caso si tratti di materiale illecito, la segnalazione viene passata alle agenzie di forze dell'ordine interessate e all'Internet Service Provider (ISP, fornitore di servizi Internet). Sarà poi il Content

[9] "CSAM (Child Sexual Abuse Material), materiale di abuso sessuale su minori", Europol, (22 luglio 2024), Fragmented and multiplied cybercriminal landscape, warns new Europol report, https://www.europol.europa.eu/media-press/newsroom/news/fragmented-and-multiplied-cybercriminal-landscape-warns-new-europol-report

[10] Europol, (2024), Internet Organised Crime Threat Assessment (IOCTA) 2024, Publications Office of the European Union, Luxembourg, https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf , pp.25-27

[11] Europol, (2024), Child Sexual Exploitation, https://www.europol.europa.eu/crime-areas/child-sexual-exploitation

[12] "Le hotline forniscono un meccanismo per ricevere segnalazioni dal pubblico di contenuti illegali su Internet, di solito tramite l'interfaccia web o via e-mail, e disporre di procedure trasparenti ed efficaci per il trattamento dei reclami." INHOPE – Association of Internet Hotline Providers, (2018), Code of Practice, https://inhope.org/media/site/1fffcc1905-1614610382/inhope_codeofpractice.pdf , p.3

Service Provider a procedere con la rimozione dei contenuti, la chiusura del sito o degli account di scambio valuta. L'EC3 continua costantemente a monitorare i black market presenti per determinare l'aumento di materiale di abuso e sfruttamento sessuale di minori messo in commercio, inoltre, tenta costantemente di bloccare ogni forma di pagamento attuata per evitare una completa trasformazione del mercato CSAM a un sistema di pagamento digitale interamente nuovo e non del tutto regolamentato.[13]

3. Database dell'EUROPOL

L'European Cybercrime Centre gestisce una serie di database creati per uno scambio di informazioni e dati più fluido fra paesi membri, paesi terzi, associazioni membre ed Europol. Ve ne sono per ogni tipo di indagini su crimini per cui EUROPOL aiuta favorendo cooperazione internazionale. Anche per l'abuso e lo sfruttamento sessuale di minori online i database sono diversi.

3.1.Analysis Project Twins (AP Twins)

L'AP Twins sostiene la prevenzione e il contrasto di tutte le forme di criminalità legate allo sfruttamento sessuale e all'abuso dei minori. Si tratta di un sistema di elaborazione di informazioni, raccoglie e classifica file multimediali CSAM e presenta un programma in grado di collegare quelle immagini che sembrano avere dei tratti in comune in modo da facilitare il lavoro degli nvestigatori ("cross-matching"). Il database archivia tutti i tipi di informazione che sono utili ai fini delle indagini e le raccoglie in un pacchetto in modo da evitare la dispersione dei dati, può raccogliere immagini e video insieme a testimonianze, intercettazioni, e tutto ciò che il paese che carica le informazioni ritiene utile. In questo modo determinati crimini possono essere individuati singolarmente e poi fermati.

Inoltre, Il database è integrato con un programma in grado di individuare tendenze e modelli criminali tra i diversi dati caricati, facilitando così la combinazione di informazioni e la formazione di indagini specifiche e mirate.

I fascicoli vengono classificati in base ad alto, medio e basso livello di intervento. I dati vengono conservati per 18 mesi, al loro scadere, se i dati sono ancora utili, vengono spostati ad un livello di fascicolo più basso o trasferiti in altra sede per scopi di analisi specifiche riferite

[13] European Cybercrime Centre, (2015), The European Financial Coalition against Commercial Sexual Exploitation of Children Online - A Strategic Assesment, https://www.europol.europa.eu/cms/sites/default/files/documents/efc_strategic_assessment_2014.pdf , pp.8-9

ad eventi o interventi. Le informazioni contenute nell'AP Twins possono essere consultate tramite richiesta dalle autorità certificate, se la richiesta di dati è giustificata si riceveranno i risultati e le analisi dagli esperti che si occupano della gestione del database.[14]

3.2.Investigation Video and Audio System (IVAS)

Creato e gestito da EUROPOL, si tratta di un database di materiale riguardante abuso e sfruttamento sessuale di minori online. Tutto il materiale raccolto è sequestrato dalle autorità di polizia dei paesi membri dell'UE o dei paesi terzi con cui EUROPOL ha un accordo.

Funziona come l'International Child Sexual Exploitation database dell'INTERPOL. Le immagini e i video vengono classificati secondo la scala COPINE[15] dalle autorità di polizia che li inseriscono nel sistema, in seguito vengono riportate tutte le informazioni visibilmente disponibili riguardo vittima, trasgressore se presente e attività in svolgimento.

È integrato con la tecnologia di hashing (impronte digitali) in modo da consentire segnalazione automatica di nuovo materiale al suo interno al team di identificazione delle vittime ed evitare la ri-vittimizzazione dei minori, evitando agli investigatori che caricano nuovo materiale di guardarlo, ma consentendogli di caricare i file e collegarli solo tramite hash.[16]

3.3. Project VIC

Progetto del National Center for Missing and Exploited Children, partito nel 2015 e ospitato dall'European Cybercrime Centre. È un progetto che propone un approccio "Victim Centric" nelle indagini contro lo sfruttamento e l'abuso sessuale su minori online, il suo obiettivo è mirare a ridurre il carico di lavoro degli investigatori nell'identificazione delle vittime di questo crimine tramite lo sviluppo di nuove tecnologie[17]:

- PhotoDNA – Tecnologia sviluppata da Microsoft e integrata in molti database di contrasto allo sfruttamento e abuso sessuale su minori (come l'ICSE database di INTERPOL e l'IVAS database di EUROPOL). Evita la duplicazione degli sforzi degli investigatori garantendo che le immagini modificate siano riconducibili alla

[14] Europol, (31 maggio 2012), New AWF Concept - Guide for MS and Third Parties, https://www.statewatch.org/media/documents/news/2013/jan/europol-awf-new-concept.pdf

[15] Scala suddivisa in 10 livelli, creata per descrivere la gravità di vittimizzazione mostrata nei materiali di abuso e sfruttamento sessuale. Quayle E., (2008), The COPINE Project, Irish Probation Journal, vol.5, pp.66 -69

[16] ECPAT International, (2018), Trends in online child sexual abuse material, Bangkok, https://ecpat.org/wp-content/uploads/2021/05/ECPAT-International-Report-Trends-in-Online-Child-Sexual-Abuse-Material-2018.pdf

[17] Project Vic International, (2024), https://www.projectvic.org/

stessa serie di materiali originali assegnando un valore numerico univoco alle stesse.[18]

- VIC Safer - Tecnologia di Machine learning[19] in grado di identificare determinate caratteristiche presenti in uno specifico frame di file multimediali. È in grado di riconoscere età, sesso, parti del corpo e azioni, rileva quindi la presenza di materiale pedopornografico. È progettato per analizzare grandi volumi di immagini e video che ancora non sono stati analizzati dalle forze dell'ordine e che non sono ancora stati registrati in un database hash. In seguito, procede con una classificazione basata sul contenuto dei file: "sicuro", "sicuro ma contenente minori", "pornografia per adulti", "pornografia senza volto", "abuso su minori". Inoltre, genera report Excel che forniscono i dati etichettati necessari per un esame rapido dei materiali analizzati dal sistema.[20]
- VIC Point – Modello di elaborazione del linguaggio naturale, classificatore di percorsi di file (metadati), è programmato per accertare la presenza di materiale di abuso e sfruttamento sessuale di minori all'interno del file system di un computer in base alle convenzioni di denominazione ed etichettatura. L'estrazione dei dati utilizza una tecnica forense nota come "file carving", ossia, recupera i file scansionando i byte di un sistema di archiviazione ri-assemblandoli. Viene utilizzato per recuperare file e frammenti di file quando le voci della directory sono danneggiate o mancanti. Soprattutto nei casi CSAM, gli agenti delle forze dell'ordine spesso riescono a recuperare più immagini dal sistema di archiviazione del sospettato utilizzando questo tipo di tecninca.[21]
- Illuminate – Programma sviluppato per aiutare gli investigatori ad indentificare determinati oggetti all'interno dei file di cui sono in possesso, ospita una vasta raccolta di immagini. Quando un nuovo materiale CSAM viene caricata al suo interno, l'applicazione Illuminate è in grado di raggrupparla con frame simili contenuti all'interno del suo database o raccolti sul web tramite web scraping (estrazione).

Project Vic si pone in prima linea nello sviluppo di strumenti forensi e di visione artificiale consentendo alle organizzazioni di combattere la distribuzione di materiale pedopornografico a livello globale. Questi sistemi automatizzati basati sull'apprendimento automatico possono aiutare le forze dell'ordine o le organizzazioni di cooperazione di polizia a identificare rapidamente vittima e aggressori e intraprendere le azioni appropriate.

4. Taskforce dell'EUROPOL

Identificare le vittime di abuso e sfruttamento sessuale di minori è una priorità delle forze di polizia di tutto il mondo, ma i loro sforzi sono costantemente ostacolati dall'ingente quantità di materiale CSAM sempre più crescente e conseguentemente vi è un aumento di bambini sfruttati

[18] Ibidem

[19] Il Machine learning è un sistema di apprendimento automatico, è in grado di apprendere da dati ed esperienza, viene addestrato a svolgere un compito piuttosto che essere esplicitamente programmato per svolgerlo. L'apprendimento può essere supervisionato, semi-supervisionato o per rinforzo. SAP Italia, (2024), Che cos'è il machine learning?, https://www.sap.com/italy/products/artificial-intelligence/what-is-machine-learning.html

[20] Project Vic International, (2024), https://www.projectvic.org/

[21] Ibidem

sessualmente. I minori abusati vengono ri-vittimizzati nel momento in cui i loro abusi vengono registrati e le loro immagini o video vengono riprodotti. Questo aumento è dovuto al più frequente utilizzo di nuove tecnologie che permettono di mascherare la propria identità e provenienza nella frequentazione o creazione di siti che forniscono tale materiale. Nel mercato illegale la domanda di nuovo materiale è in aumento e la sua accessibilità è alla portata di tutti, si è quindi riconosciuta un'esigenza ed emergenza internazionale che ha portato alla collaborazione volta all'analisi di immagini e video con l'obiettivo di identificare più vittime possibili e fermare i trasgressori.

Con lo scopo di risolvere l'emergenza e sfruttare al meglio la cooperazione internazionale con metodi innovativi per identificare il maggior numero di vittime possibili, l'EUROPOL nel 2011 prende parte alla Virtual Global Taskforce (VGT) e nel 2014 dà il via alla Victim Identification Taskforce (VIDTF), che supportano il lavoro dell'EC3.

4.1.Virtual Global Taskforce – VGT

Alleanza strategica tra le forze dell'ordine, creata nel 2003 dagli Stati Uniti per combattere l'aumento di l'abuso e lo sfruttamento sessuale dei bambini online. Attualmente guidata dal Regno Unito e presieduta dalla National Crime Agency (NCA).[22]

Le forze di polizia aderenti alla VGT si riuniscono per condividere informazioni, strategie investigative e per stabilire un programma di attività ed operazioni coordinate. Tale rapporto, Environmental Scan, esamina la situazione complessiva della minaccia dello sfruttamento e abuso sessuale di minori online per fornire le indicazioni strategiche adatte per proseguire nella lotta a questo crimine.[23]

Osserva a livello globale le emergenze più significative, dall'utilizzo delle tecnologie alle sue più svariate applicazioni, come la tecnologia Peer-to-Peer, i social media, lo streaming live degli abusi commercializzato. L'obiettivo è quello di sviluppare e gestire nuove tecnologie innovative che rafforzino il lavoro di indagine in questo particolare settore criminale. Nel 2024 rilascia la prima dichiarazione riguardo a dispositivi in grado di riuscire a sviare le indagini circa la provenienza di determinati account che usufruiscono dal web di siti illegali. Denuncia:

[22] Virtual Global Taskforce, (2024), Tackling the global threat from child sexual abuse, https://www.nationalcrimeagency.gov.uk/virtual-global-taskforce/

[23]Europol, (8 novembre 2019), 2019 Virtual Global Taskforce Releases Environmental Scan, https://www.europol.europa.eu/media-press/newsroom/news/2019-virtual-global-taskforce-releases-environmental-scan

- La crittografia end-to-end (E2EE), ormai tecnologia preinstallata di default su molte applicazioni messaggistiche e alla portata di tutti;
- Materiale CSAM e CSEM prodotto dall'intelligenza artificiale che intensifica e prolunga il tempo e le risorse delle forze dell'ordine per identificare e salvaguardare veri bambini in pericolo; l'AI può essere utilizzata per migliorare o creare nuovi metodi di adescamento e generare grandi volumi di materiale illegale in pochissimo tempo.

Tra le altre mansioni che la VGT si pone, vi è anche quella della prevenzione. Si pone l'obiettivo di aiutare le forze dell'ordine, le organizzazioni nazionali e internazionali nelle campagne di prevenzione all'abuso e sfruttamento sessuale di minori online, partecipando e finanziando campagne di sensibilizzazione sia online sui social media, che di persona nelle scuole per studenti e genitori, istituti di formazione e altri luoghi di istruzione.[24]

Essenziali per la VGT sono le hotline, poiché attraverso le segnalazioni della popolazione, il numero di indagini aperte è aumentato, e vi sono veri e propri risultati di riconoscimento vittima o del trasgressore dovute a segnalazioni fatte tramite siti di hotline. Proprio per questo sostiene le iniziative di invenzione di database di segnalazioni, come l'ICCAM database dell'associazione di segnalazione online INHOPE: rete internazionale che unisce le hotline nazionali impegnate nella lotta a questo crimine. Creato nel 2015 con l'aiuto dell'European Cybercrime Centre, database di URL che vengono segnalati alle hotline: Quando una persona si imbatte in siti, situazioni o materiale di abuso o sfruttamento sessuale su minori su internet, è possibile fare una segnalazione in forma anonima alle hotline esistenti che provvederanno ad analizzare la segnalazione ed eventualmente, se utile, a riportarla alle forze dell'ordine. Una volta scansionati gli URL, si scaricano le immagini e i video, poi classificati in base a criteri predeterminati simili alla categorizzazione dell'ICSE database. Come quest'ultimo, l'ICCAM System presenta un sistema di hashing integrato che crea un'impronta digitale propria per ogni frame dei file multimediali analizzati e certificati.[25]

4.2.Victim Identification Taskforce – VIDTF

Nel 2014, su richiesta degli stati membri dell'UE e delle agenzie aderenti, l'EUROPOL ha dato il via all'iniziativa della VIDTF.

"Il problema che stiamo affrontando è globale e richiede una risposta globale coordinata da parte delle forze dell'ordine, dell'industria privata e della società civile. […] Pertanto,

[24] Virtual Global Taskforce, (22 aprile 2024), Technological Tipping Point Reached in Fight Against Child Sexual Abuse, https://www.nationalcrimeagency.gov.uk/technological-tipping-point-reached-in-fight-against-child-sexual-abuse

[25] INHOPE, (2024), A deep dive into ICCAM, https://inhope.org/EN/articles/a-deep-dive-into-iccam

incoraggiamo i paesi a utilizzare gli strumenti e le reti uniche di Europol per scambiare informazioni in modo che ogni caso possa concludersi con un esito positivo. […] Operazioni come quella odierna dimostrano che la messa in comune di risorse, conoscenze e competenze tecniche è il modo più efficace per identificare e salvare questi bambini. Ecco perché è così importante che le autorità di polizia in Europa e oltre continuino a investire e partecipare a task force per l'identificazione delle vittime come questa." (RobWainwright, direttore Europol, 2016)[26]

Si tratta di un'iniziativa che regolarmente, per due settimane due volte l'anno, riunisce esperti provenienti da tutto il mondo[27]. Gli specialisti di identificazione delle vittime mirano a sviluppare tecniche investigative implementate da condividere a livello globale per creare una cooperazione unitaria e più fluida.

Le immagini e i video che gli specialisti sono chiamati ad analizzare provengono da indagini in corso o arrivate ad un punto senza sviluppi. I file multimediali vengono centralizzati in un unico archivio presso EUROPOL, dove la VIDTF è ospitata, in modo da rendere più efficiente il lavoro degli esperti, il quale obiettivo è individuare le caratteristiche comuni alle varie immagini provenienti da fonti diverse, restringere il campo di ricerca ed eventualmente localizzare le vittime o il paese in cui i minori vengono abusati, in modo tale da allertare per tempo la polizia del paese interessato. Una volta finito il lavoro di analisi durato due settimane, le immagini che riportano l'identificazione di oggetti, vittime o trasgressori vengono caricate nuovamente, con le informazioni aggiuntive, all'interno dei database internazionali con lo scopo e la speranza di chiudere indagini in corso e salvare i bambini abusati.

L'EUROPOL e l'EC3 sono stati in grado di fornire strumenti adatti all'identificazione delle vittime, gli esperti delle VIDTF raccolgono le immagini dai database EUROPOL e dall'International Child Sexual Exploitation Database dell'INTERPOL, e assieme hanno sviluppato pacchetti di intelligence (di informazioni) da distribuire ai paesi interessati a vittime e trasgressori. Dal 2014, per 1.726 casi è stato identificato un probabile paese di produzione e

[26] Europol, (19 aprile 2016), Europol Coordinates International Operation Aimed at Identifying Victims of Child Abuse, https://www.europol.europa.eu/media-press/newsroom/news/europol-coordinates-international-operation-aimed-identifying-victims-of-child-abuse

[27] Australia, Belgio, Bulgaria, Canada, Repubblica Ceca, Danimarca, Estonia, Francia, Germania, Irlanda, Italia, Lettonia, Malta, Moldavia, Paesi Bassi, Norvegia, Polonia, Portogallo, Romania, Slovacchia, Slovenia, Spagna, Svezia, Svizzera, Regno Unito, Stati Uniti più le agenzie di Europol e Interpol. Europol, (18 novembre 2021), https://www.europol.europa.eu/media-press/newsroom/news/global-europol-taskforce-identifies-18-child-victims-of-sexual-abuse

grazie alle operazioni VIDTF, sono stati tutelati oltre 695 bambini e sono stati arrestati 228 trasgressori.[28]

Nel maggio del 2017, a causa del grave aumento del materiale di abuso sessuale su minori dovuto anche al sempre più comune utilizzo del dark web, l'Europol, con l'aiuto dell'European Cybercrime Centre, su spinta della VIDTF, lancia la campagna "Stop Child Abuse – Trace an Object". Pagina web ospitata dal sito dell'EUROPOL, l'iniziativa chiede aiuto alle persone in tutto il mondo per identificare oggetti e i loro luoghi di provenienza in modo da riuscire a localizzare e possibilmente salvare i minori vittime di abuso e sfruttamento sessuale online. Data la grande mole di materiale che gli agenti si trovano a dover analizzare, si è pensato di chiedere aiuto a uno spettro più grande di persone per riuscire a velocizzare il processo di identificazione della vittima. Nella pagina web vengono caricate le immagini selezionate dalla VIDTF raffiguranti oggetti presi dallo sfondo di un file multimediale raffigurante abusi e sfruttamenti sessuali su minori, questi file multimediali sono già stati analizzati ed esaminati, si è già seguita ogni pista investigativa possibile senza però risultati concreti.[29]

Per aiutare il processo di identificazione della VIDTF, il pubblico deve collegarsi al sito Europol apposito: https://www.europol.europa.eu/stopchildabuse. Se si riconosce un determinato oggetto (può essere un logo su una maglietta, una scatola, un poster, una strada o un particolare oggetto di sfondo) si può inviare le informazioni scrivendole nell'apposito spazio:

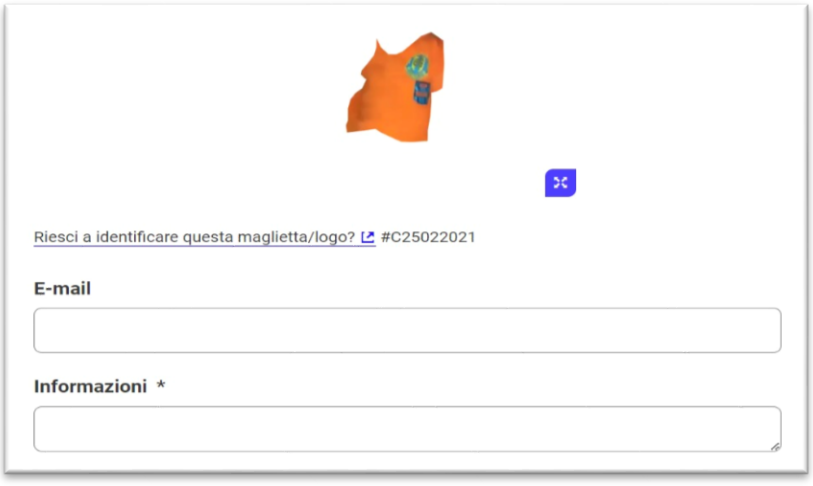

Figura 4: Trace an Object

[28] Europol, (18 novembre 2021), Global Europol taskforce identifies 18 child victims of sexual abuse, https://www.europol.europa.eu/media-press/newsroom/news/global-europol-taskforce-identifies-18-child-victims-of-sexual-abuse

[29] Europol, (2017), Trace an Object explained, https://youtu.be/YVIHBDFLPUw

Il grande successo della campagna “Trace and Object” dell’EUROPOL e l’enorme contributo fornito dall’ampia partecipazione del pubblico hanno motivato la Polizia Federale Australiana a lanciare la propria versione dell’iniziativa nel marzo 2021. La campagna è la medesima, il sito australiano è focalizzato all’identificazione di oggetti di cui si è convinti essere di provenienza della regione Asiatico-Pacifica. Se si pensa di avere informazioni utili ad aiutare l’identificazione di luoghi presenti nell’area Asiatico-Pacifica basta accedere al sito australiano https://www.accce.gov.au/what-we-do/trace-an-object.

Dal 2017 sono state inviate 28.000 segnalazioni dal pubblico, grazie alle quali gli investigatori della VIDTF sono riusciti a identificare e sottrarre dagli abusi 28 bambini e ad arrestare 6 trasgressori. Inoltre, sono riusciti a circoscrivere in Stati ben precisi 127 casi, riducendo così il campo di ricerca in cui prima si trovavano.[30]

Conclusioni

Il fenomeno della pedopornografia online continua a rappresentare una minaccia grave e in continua evoluzione, alimentata dall'uso di tecnologie sempre più sofisticate che ostacolano l'azione delle forze dell'ordine. L'EUROPOL e l’European Cybercrime Centre (EC3) rivestono un ruolo primario nella lotta contro questi crimini, promuovendo la cooperazione internazionale, lo sviluppo di strumenti investigativi avanzati e la condivisione di informazioni tra le autorità competenti.

L'implementazione di database specializzati e il coinvolgimento di taskforce dedicate hanno permesso di ottenere risultati significativi, sebbene la sfida rimanga complessa a causa della continua innovazione tecnologica da parte dei criminali. In particolare, la diffusione di materiale generato tramite Intelligenza Artificiale e la facilità di accesso alle Darknet richiedono un aggiornamento costante delle strategie di contrasto. La collaborazione tra governi, forze dell'ordine, organizzazioni non governative e aziende tecnologiche è fondamentale per sviluppare risposte efficaci e proteggere i minori dagli abusi online. Solo attraverso un impegno congiunto e l'adozione di strumenti sempre più sofisticati sarà possibile mitigare l'impatto di questo crimine e garantire una maggiore sicurezza per le vittime e per la società nel suo complesso.

[30] Europol, (2024), Stop Child Abuse – Trace an Object, https://www.europol.europa.eu/stopchildabuse

Bibliografia

Quayle E., (2008), The COPINE Project, Irish Probation Journal, vol.5

Sitografia

ECPAT, (2024), Summary paper on online child sexual exploitation, https://ecpat.org/wp-content/uploads/2021/05/ECPAT-Summary-paper-on-Online-Child-Sexual-Exploitation-2020.pdf

ECPAT International, (2018), Trends in online child sexual abuse material, Bangkok, https://ecpat.org/wp-content/uploads/2021/05/ECPAT-International-Report-Trends-in-Online-Child-Sexual-Abuse-Material-2018.pdf

Europol, (31 maggio 2012), New AWF Concept - Guide for MS and Third Parties, https://www.statewatch.org/media/documents/news/2013/jan/europol-awf-new-concept.pdf

Europol, (19 aprile 2016), Europol Coordinates International Operation Aimed at Identifying Victims of Child Abuse, https://www.europol.europa.eu/media-press/newsroom/news/europol-coordinates-international-operation-aimed-identifying-victims-of-child-abuse

Europol, (2017), Trace an Object explained, https://youtu.be/YVIHBDFLPUw

Europol, (8 novembre 2019), 2019 Virtual Global Taskforce Releases Environmental Scan, https://www.europol.europa.eu/media-press/newsroom/news/2019-virtual-global-taskforce-releases-environmental-scan

Europol, (18 novembre 2021), Global Europol taskforce identifies 18 child victims of sexual abuse, https://www.europol.europa.eu/media-press/newsroom/news/global-europol-taskforce-identifies-18-child-victims-of-sexual-abuse

Europol, (2024), Child Sexual Exploitation, https://www.europol.europa.eu/crime-areas/child-sexual-exploitation

Europol, (22 luglio 2024), Fragmented and multiplied cybercriminal landscape, warns new Europol report, https://www.europol.europa.eu/media-press/newsroom/news/fragmented-and-multiplied-cybercriminal-landscape-warns-new-europol-report

Europol, (2024), Internet Organised Crime Threat Assessment (IOCTA) 2024, Publications Office of the European Union, Luxembourg, https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf

Europol, (2024), Stop Child Abuse – Trace an Object, https://www.europol.europa.eu/stopchildabuse

INHOPE, (2024), A deep dive into ICCAM, https://inhope.org/EN/articles/a-deep-dive-into-iccam

INHOPE – Association of Internet Hotline Providers, (2018), Code of Practice, https://inhope.org/media/site/1fffcc1905-1614610382/inhope_codeofpractice.pdf

Interpol, (2024), https://www.interpol.int/Crimes/Crimes-against-children

Ministero della Giustizia, (7 giugno 2017), Sextortion Scams, https://www.giustizia.it/giustizia/it/mg_2_5_12_1.page?contentId=GLM1144677#

Polizia di Stato, (5 maggio 2024), INTERNET, IL PAESE DELLE MERAVIGLIE...? https://www.poliziadistato.it/statics/20/brochure-5-maggio-2024.pdf

Project Vic International, (2024), https://www.projectvic.org/

SAP Italia, (2024), Che cos'è il machine learning?, https://www.sap.com/italy/products/artificial-intelligence/what-is-machine-learning.html

Save the Children, (2024), Il sexting e gli adolescenti: cos'è e perché è diffuso, https://www.savethechildren.it/blog-notizie/il-sexting-e-gli-adolescenti-cos-e-perche-e-diffuso

Virtual Global Taskforce, (2024), Tackling the global threat from child sexual abuse, https://www.nationalcrimeagency.gov.uk/virtual-global-taskforce/

Virtual Global Taskforce, (22 aprile 2024), Technological Tipping Point Reached in Fight Against Child Sexual Abuse, https://www.nationalcrimeagency.gov.uk/technological-tipping-point-reached-in-fight-against-child-sexual-abuse

Address correspondence to bianca.francesca.ber@alice.it

Received September 24, 2024 accepted September 29, 2024

Operazioni congiunte di cooperazione internazionale nel contrasto alla pedopornografia online: prospettiva italiana

Bianca Francesca Berardi[1]

RIASSUNTO

Il contrasto alla pedopornografia online richiede un approccio coordinato a livello internazionale, data la natura transnazionale di questo crimine e l'uso diffuso delle reti informatiche per la condivisione di materiale illecito. Le operazioni congiunte tra forze dell'ordine, facilitate da strumenti di comunicazione sicura come "I-24/7" di INTERPOL e "SIENA" di EUROPOL, rappresentano un elemento chiave nella lotta contro il fenomeno. Questi sistemi consentono uno scambio rapido ed efficiente di informazioni sensibili tra Stati, garantendo un coordinamento efficace nelle indagini e nelle operazioni repressive.

L'articolo esamina le strategie adottate dall'Italia nel contesto della cooperazione internazionale, evidenziando il ruolo di iniziative quali gli "Action Day" e le "Action Week", che permettono interventi simultanei in più Paesi per smantellare reti criminali e identificare vittime e trasgressori. Viene inoltre analizzato il contributo delle principali organizzazioni di contrasto alla pedopornografia online, tra cui EUROPOL e INTERPOL, e il supporto fornito dai sistemi di comunicazione sicura, essenziali per il coordinamento transnazionale di questo tipo operazioni congiunte.

L'analisi sottolinea l'importanza della collaborazione tra autorità nazionali e internazionali, l'utilizzo di tecnologie avanzate per il contrasto dei reati informatici e il continuo aggiornamento delle strategie investigative. In un contesto in cui le minacce evolvono rapidamente, la cooperazione multilaterale e l'adozione di strumenti tecnologici innovativi risultano indispensabili per rafforzare la capacità di prevenzione e repressione di questo crimine.

Parole chiave: Operazioni congiunte, Comunicazione sicura, Cooperazione internazionale, "Action Day" e "Action Week"

[1] Dottoressa magistrale in Investigazione, Criminalità e Sicurezza Internazionale - Università degli Studi Internazionali di Roma (UNINT)

ABSTRACT

Combating online child sexual abuse material (CSAM) requires a coordinated international approach, given the transnational nature of this crime and the widespread use of digital networks for sharing illicit material. Joint operations among law enforcement agencies, facilitated by secure communication tools such as INTERPOL's "I-24/7" and EUROPOL's "SIENA," constitute a key element in the fight against this phenomenon. These systems enable a rapid and efficient exchange of sensitive information between states, ensuring effective coordination in investigations and enforcement actions.

This article examines the strategies adopted by Italy in the context of international cooperation, highlighting the role of initiatives such as "Action Day" and "Action Week," which allow for simultaneous interventions in multiple countries to dismantle criminal networks and identify victims and offenders. Furthermore, it analyses the contributions of major organizations engaged in the fight against online CSAM, including EUROPOL and INTERPOL, and the support provided by secure communication systems, which are essential for the transnational coordination of joint operations.

The analysis underscores the importance of collaboration between national and international authorities, the use of advanced technologies to combat cybercrimes, and the continuous updating of investigative strategies. In a context where threats evolve rapidly, multilateral cooperation and the adoption of innovative technological tools are indispensable for strengthening the capacity to prevent and combat this crime.

Keywords: Joint operations, **S**ecure communication, International cooperation, “Action Day” and “Action Week”

RESUMEN

La lucha contra el material de abuso sexual infantil en línea (CSAM) requiere un enfoque coordinado a nivel internacional, dada la naturaleza transnacional de este delito y el uso extendido de redes digitales para la distribución de material ilícito. Las operaciones conjuntas entre fuerzas del orden, facilitadas por herramientas de comunicación segura como "I-24/7" de INTERPOL y "SIENA" de EUROPOL, constituyen un elemento clave en la lucha contra este fenómeno. Estos sistemas permiten un intercambio rápido y eficiente de información sensible entre Estados, garantizando una coordinación efectiva en las investigaciones y acciones represivas.

Este artículo examina las estrategias adoptadas por Italia en el marco de la cooperación internacional, destacando el papel de iniciativas como "Action Day" y "Action Week," que

permiten intervenciones simultáneas en múltiples países para desmantelar redes criminales e identificar víctimas y delincuentes. Además, se analiza la contribución de las principales organizaciones dedicadas a la lucha contra el CSAM en línea, incluyendo EUROPOL e INTERPOL, y el apoyo proporcionado por los sistemas de comunicación segura, esenciales para la coordinación transnacional de este tipo de operaciones conjuntas.

El análisis subraya la importancia de la colaboración entre autoridades nacionales e internacionales, el uso de tecnologías avanzadas para combatir los delitos cibernéticos y la actualización continua de las estrategias investigativas. En un contexto donde las amenazas evolucionan rápidamente, la cooperación multilateral y la adopción de herramientas tecnológicas innovadoras resultan indispensables para fortalecer la capacidad de prevención y represión de este delito.

Palabras clave: Operaciones conjuntas, Comunicación segura, Cooperación internacional, "Día de acción" y "Semana de acción"

1. Introduzione

Il crimine di abuso e sfruttamento sessuale online ha ormai raggiunto una diffusione globale a causa del sempre più frequente utilizzo di Internet e del dark web, divenuto accessibile a uno svariato numero di utenti. La complessità di tali crimini si è ampliata al punto da diventare di natura forzatamente transnazionale, richiedendo interventi di cooperazione internazionale mirati e costanti. Risulta quindi di importanza fondamentale stabilire un clima di collaborazione fra Stati, a fine di riuscire a sventare e contrastare al meglio le reti e i siti criminali che si occupano di produzione, diffusione e scambio di materiale pedopornografico, di abuso e sfruttamento sessuale di minori online.

In prima linea contro questo crimine vi sono le organizzazioni INTERPOL ed EUROPOL, che hanno sviluppato i sistemi di comunicazione sicura "I-24/7" e "SIENA", tanto indispensabili quanto gli strumenti ideati per l'identificazione di vittima e trasgressore, poiché consentono la condivisione di informazioni sensibili in modo sicuro e tempestivo tra i diversi Stati aderenti a tali piattaforme. Tutti questi sistemi rafforzano la collaborazione internazionale, rendendo possibili interventi congiunti rapidi e coordinati.

"Action Day" o "Action Week" sono una particolare forma di cooperazione internazionale supportata da tali organizzazioni intente nel coordinamento della collaborazione tra Stati al fine dell'identificazione e smantellamento di reti criminali. L'articolo, sviluppato con il contributo di alcuni membri del Centro Nazionale per il Contrasto della pedopornografia On-line con sede a Roma, si propone di analizzare il funzionamento di queste operazioni congiunte.

2. “Action Day” e “Action Week”

Questo tipo di iniziative di cooperazione internazionale sono il perfetto esempio che sottolinea l’importanza di operazioni coordinate per quei tipi di crimini che sono inevitabilmente di natura transnazionale, le azioni simultanee consentono di colpire reti criminali attive in più paesi, e mirano a ridurre la possibilità di fuga, elusione o diffusione di informazioni sensibili. Inoltre, rafforzano la collaborazione fra Stati e favoriscono lo scambio di informazioni e competenze al fine di aumentare la sicurezza internazionale.

Grazie all’aiuto di alcuni membri del Centro Nazionale per il Contrasto della pedopornografia On-line con sede a Roma, che hanno fornito informazioni quanto più dettagliate potessero, è stato possibile illustrare il processo con cui hanno origine i metodi di pianificazione e coordinamento delle operazioni denominate “Action Week” e “Action Day”. Queste iniziative sono pianificate e organizzate per essere svolte simultaneamente in diverse nazioni, per una durata di tempo limitata e prestabilita, che può variare a seconda della complessità degli obiettivi o della mole di informazioni da raccogliere. Durante questo periodo di tempo limitato, i differenti paesi coinvolti mettono in atto una serie di misure e operazioni sincronizzate che possono includere dal monitoraggio agli arresti.

Le operazioni congiunte prendono avvio da segnalazioni che possono provenire da Stati esteri o attraverso il sistema di comunicazione sicura “I-24/7” di INTERPOL dall’ICSE database. Grazie a questo sistema si raccolgono rapidamente elementi preliminari che danno avvio alle attività investigative. Dalle segnalazioni ricevute iniziano tali attività di indagine, che possono per esempio includere operazioni di monitoraggio, sorveglianza e attività sotto copertura, allo scopo di ottenere ulteriori elementi e informazioni utili al caso originale. Gli elementi raccolti vengono poi analizzati e verificati grazie all’utilizzo di strumenti investigativi specifici e specializzati, propri delle forze dell’ordine del paese di competenza. Questo lavoro viene supportato da database e strumenti di analisi, forniti dalle agenzie internazionali come EUROPOL e INTERPOL, che permettono di operare un controllo incrociato delle informazioni in modo da favorire una visione più ampia e dettagliata del crimine investigato. Qualora, durante queste indagini, emergano prove del coinvolgimento di diversi Stati, questi verranno avvisati tramite il sistema di comunicazione sicura SIENA (Secure Information Exchange Network Application) di EUROPOL, attraverso il quale vengono condivise le varie informazioni raccolte in maniera rapida e sicura.

In base alla quantità e complessità delle informazioni raccolte, da file multimediali a dati tecnici, viene stabilita la durata complessiva dell’operazione, decidendo quindi se organizzare

operazioni congiunte di intervento in un unico giorno, chiamato "Action Day", o in un intervallo di tempo più prolungato, noto come "Action Week". Questa decisione consente una pianificazione adeguata di risorse e coordinamento fra i vari paesi, massimizzando l'efficacia di azioni congiunte in lotta a crimini tanto efferati come lo sfruttamento e l'abuso sessuale dei minori online. Una volta che tutti i paesi coinvolti nell'operazione, sia membri dell'Unione Europea che Stati extra-UE, dichiarano di aver ottenuto tutte le informazioni e i dati necessari all'indagine e di essere pronti ad agire, viene concordata una data indicativa per l'inizio delle azioni operative. La scelta della data è sempre concordata congiuntamente fra i vari paesi membri, che valutano un tempo opportuno tenendo conto delle esigenze logistiche e operative che i diversi Stati devono affrontare per completare gli ultimi preparativi e verifiche.

Al termine delle operazioni congiunte, tutti i materiali acquisiti vengono condivisi non solo sugli strumenti di analisi di ciascun paese partecipante, ma anche sui database delle agenzie internazionali di cooperazione di polizia, come Europol e Interpol. Questi dati vengono poi esaminati dalle task force specializzate nell'identificazione delle vittime e arresto dei trasgressori. Le informazioni ottenute da questo tipo di operazioni diventano un importante strumento di condivisione che permette alle diverse unità specializzate di approfondire le indagini e adottare misure di contrasto adeguate.

Si prenda come esempio L'"Operazione Icaro", supportata e coordinata dall'European Cybercrime Centre (EC3) di EUROPOL nel 2011, in cooperazione con 22 paesi europei: Austria, Belgio, Bulgaria, Cipro, Repubblica Ceca, Danimarca, Estonia, Finlandia, Francia, Germania, Irlanda, Italia, Lussemburgo, Malta, Paesi Bassi, Polonia, Slovacchia, Spagna, Svezia, Croazia, Norvegia, Svizzera. Si tratta di un'operazione volta a smantellare le reti di condivisione di file di abuso e sfruttamento sessuale di minori online, prendendo di mira coloro che condividevano le forme più estreme di tale materiale, che ritraeva neonati e bambini di piccola età. Vennero identificati 269 sospettati e arrestati 112 individui, in 22 paesi differenti.[2] Si trattò di una delle prime "Action Week" organizzate dal progetto COSPOL – Internet Related Child Abuse Material (CIRCAMP), iniziativa finalizzata alla prevenzione della ri-vittimizzazione di bambini vittime di abusi impendendo l'accesso a tali materiali.[3]

[2] Europol, (16 dicembre 2011), Joint action in 22 European countries against online child sexual abuse material in the internet, https://www.europol.europa.eu/mediapress/newsroom/news/joint-action-in-22-european-countries-against-online-child-sexual-abusematerial-in-internet

[3] Dipartimento di Giustizia degli Stati Uniti d'America, (agosto 2009), Moving Public-Private Partnerships From Rhetoric to Reality: CIRCAMP / CSAADF Transferability Assessment, https://www.ojp.gov/ncjrs/virtual-library/abstracts/moving-public-private-partnerships-rhetoric-reality-circamp-csaadf

"Questi bambini sono vittime di molteplici crimini. Innanzitutto, quando avviene l'abuso vero e proprio. Poi, quando viene filmato. In seguito, ogni volta che le immagini vengono pubblicate, diffuse o visualizzate. L'azione congiunta condotta sotto il coordinamento di Europol dimostra il nostro impegno a sostenere la lotta contro questo crimine spaventoso. Sottolinea l'importanza della cooperazione tra le autorità di polizia a livello europeo e internazionale per contrastare le attività criminali che non conoscono confini. Continueremo a utilizzare tutti gli strumenti a nostra disposizione, per sostenere gli sforzi per combattere questi crimini orrendi e per aiutare a proteggere i nostri bambini" – Cecilia Malmström, Commissaria UE per gli Affari Interni

3. Sistemi di comunicazione sicura in favore della cooperazione internazionale

La tempestività delle comunicazioni e un fluido coordinamento multilaterale sono fondamentali per l'efficacia nella lotta all'abuso e allo sfruttamento sessuale dei minori online, crimine per sua natura divenuto inevitabilmente transnazionale. Il lavoro delle organizzazioni internazionali di polizia è favorire una cooperazione continua ed efficace, proprio per questo hanno sviluppato piattaforme all'avanguardia che consentono comunicazioni rapide e sicure per lo scambio di informazioni operative e strategiche.

3.1."I-24/7" di INTERPOL

Lanciato nel 2002, è l'unico sistema di comunicazione sicura per la polizia a livello globale. Si presentava come tipologia di rete informatica interamente nuova allo scopo primario di assistere nella prevenzione, accertamento e investigazione dei reati, in conformità con il mandato dell'INTERPOL.

Ad oggi, permette di collegare tutti gli uffici centrali nazionali e gli ufficiali in prima linea, favorendo l'accesso a tutti i database INTERPOL e lo scambio istantaneo di informazioni, inoltre, come suggerisce il nome, è attivo 7 giorni su 7, 24 ore su 24.

Dal 2007 sono connessi all'" I-24/7" ONU, EUROPOL, Unione Europea e Unione Africana oltre che tutti i paesi aderenti ad INTERPOL (196 Stati).[4]

[4] Valeri, Mauro (gennaio 2024), INTERPOL - Un secolo di attività, inserto di Polizia Moderna, https://poliziamoderna.poliziadistato.it/statics/31/interpol.pd, pp.78-79

3.2.“SIENA” di EUROPOL

EUROPOL comunica con le forze dell’ordine di Stati membri e paesi terzi e con le organizzazioni internazionali tramite il Secure Information Exchange Network Application (SIENA) System, piattaforma all’avanguardia che consente comunicazioni rapide e sicure per informazioni operative e strategiche. È diventato il canale predefinito per lo scambio di informazioni e dati estremamente sensibili, utilizzato durante operazioni e indagini che necessitano di risposta immediata, è difatti progettato per avvicinare EUROPOL alla prima linea delle forze dell’ordine dei paesi coinvolti. È prevista una sua ulteriore implementazione che adotta nuovi metodi e tecnologie nell’architettura della gestione delle informazioni, traduzione automatica, estrazione di entità, funzionalità per dispositivi mobili e ulteriori funzionalità intelligenti.[5]

Per le informazioni provenienti da qualsiasi paese aderente o in accordo con EUROPOL, il sistema SIENA garantisce che i partner utilizzino le informazioni solo se “il destinatario si impegna a utilizzare i dati solo per lo scopo per cui sono stati trasmessi"[6]. Per stabilire la necessità di utilizzo delle informazioni, la loro affidabilità e accuratezza il sistema utilizza un meccanismo di “handling and evaluation codes”. Gli handling codes rettificano come l’informazione deve essere gestita attraverso proprio dei codici specifici, gli evaluation codes servono a stabilire l’affidabilità e l’accuratezza delle informazioni:

1. Gestione delle informazioni
    - H0 = le informazioni possono essere utilizzate esclusivamente al fine di prevenzione e contrasto in reati competenti ad EUROPOL, in ambito di cooperazione di polizia;
    - H1 = le notizie non possono essere divulgate in sede di procedimento penale o giudiziario senza previo consenso dell’ente originario dell’informazione;
    - H2 = le informazioni non possono essere divulgate senza previo consenso dell’ente originario;
    - H3 = sono indicate restrizioni e osservazioni che accompagnano informazioni specifiche, diverse da quelle predefinite nei codici precedenti.
2. Affidabilità della fonte
    - A = fonte assolutamente affidabile, non ci sono dubbi circa l’autenticità e affidabilità della fonte;
    - B = informazioni fornite da una fonte che, nella maggior parte dei casi, si è dimostrata affidabile;
    - C = informazioni fornite da una fonte che, nella maggior parte dei casi, si è rivelata inaffidabile;

[5]Europol, (10 giugno 2022), Secure Information Exchange Network Application (SIENA), https://www.europol.europa.eu/operations-services-and-innovation/servicessupport/information-exchange/secure-information-exchange-network-application-siena

[6] Europol, (2012), Data Protection at Europol, https://www.europol.europa.eu/sites/default/files/documents/europol_dpo_booklet_0.pdf, pp.19-21

- X = non è possibile valutare l'affidabilità della fonte.

3. Accuratezza delle informazioni
    - 1 = accuratezza delle informazioni non dubbia;
    - 2 = informazione personalmente conosciuta dalla fonte, ma non conosciuta personalmente dall'agente a cui viene trasmessa;
    - 3 = informazioni non conosciute personalmente dalla fonte, ma avvalorate da informazioni precedentemente registrate;
    - 4 = informazioni non note personalmente ne avvalorate da altre notizie.

Per ogni notizia, informazione, dato sensibile affidato ad EUROPOL, il paese o l'ente originatore del documento ha il compito di assegnare gli handiling codes giusti rispetto a quello che ritiene il metodo corretto di gestione di informazioni.[7]

Questa piattaforma sicura di comunicazione non solo serve per mettere in contatto e favorire una più fluida collaborazione fra Stati diversi, ma con la sua possibilità di scambio sicuro di informazioni, il controllo incrociato dei dati e la loro analisi operativa riesce a garantire un perfetto supporto per le azioni coordinate in diversi Stati. In queste operazioni lo scambio di informazioni in tempo reale e in modo rapido è essenziale, EUROPOL contribuisce non solo a favorire la cooperazione, ma aiuta fisicamente nella collaborazione fornendo supporto in loco.

3.3. Richieste di informazioni da parte dell'Italia

In Italia, per richieste di informazioni vincolate dalle forze dell'ordine di uno Stato, vengono istituiti trattati e decisioni riconducibili alle autorità giudiziarie. Questi ordini servono per avviare perquisizioni, intercettazioni telefoniche, sorveglianza, interrogatori, citazioni in giudizio, ecc. che siano ammissibili in fase giudiziaria. Anche questi servono a favorire e contribuire ad una più completa cooperazione internazionale per il contrasto a crimini gravi. Si fa riferimento all'European Investigation Order (EIO) e ai Mutual Legal Assistance Treaties (MLAT).

L'European Investigation Order (EIO) è stato istituito dalla Direttiva 2014/41/UE del Parlamento Europeo e del Consiglio del 3 aprile 2014. La direttiva crea un quadro unico e completo per l'acquisizione di prove e informazioni all'interno dell'Unione Europea (non si applica in Danimarca e Irlanda). Si tratta di una decisione giudiziaria emessa o convalidata dall'Autorità Giudiziaria preposta di un paese dell'UE, al fine di disporre misure investigative

[7] Ibidem

per raccogliere o utilizzare prove in questioni penali svolte in un paese diverso sempre all'interno dell'UE.[8] La richiesta deve contenere informazioni specifiche[9]:

- Dati specifici riguardanti l'autorità di emissione delle informazioni richieste e sull'autorità di convalida;
- L'oggetto e le motivazioni per cui si richiede un'EIO;
- Le informazioni necessarie e disponibili sulle persone interessate;
- La descrizione del reato oggetto di indagine o del procedimento e le disposizioni penali applicabili dallo Stato di emissione;
- La descrizione delle indagini e delle prove richiesta da acquisire;
- Indicazione circa le lingue che possono essere utilizzate per compilare l'EIO, sia dallo Stato richiedente che da quello di esecuzione.

I Mutual Legal Assistance Treaties (MLAT), in Italia, viengono utilizzati per richiedere informazioni specifiche a quei paesi che non fanno parte della comunità Europea, in particolare agli Stati Uniti. Consentono alle autorità di contrasto e ai Pubblici Ministeri di ottenere prove, informazioni e testimonianze in una forma ammissibile davanti ai tribunali dello Stato richiedente, a condizione che siano soddisfatti i requisiti del trattato. In generale, lo stato a cui è stata sottoposta la richiesta ha l'obbligo di assistenza in determinati casi: localizzazione di persone, notificazione di documenti, produzione e registrazione di documenti, esecuzione di richieste di perquisizione e sequestro, raccolta testimonianze, trasferimento di persone a fini testimoniali e immobilizzazione e confisca di beni.[10] Viene poi istituita un'Autorità Centrale all'interno di ciascun paese, che ha il compito di effettuare, ricevere ed eseguire le richieste del proprio e degli altri Stati. In Italia, l'autorità centrale predefinita è il Ministero della Giustizia. Una richiesta di assistenza MLAT deve contenere informazioni specifiche[11]:

- Il nome dell'autorità che conduce l'indagine penale o il processo per il quale si fa richiesta;
- L'oggetto e la natura dell'indagine o del procedimento;
- La descrizione delle prove o informazioni richieste e delle manovre che si compiranno con tali informazioni;
- Lo scopo per il quale si ricercano le informazioni;
- L'identità e l'ubicazione della persona da notificare, il rapporto di tale persona con il procedimento e il modo in cui deve essere effettuata la notifica;
- L'identità e l'ubicazione della persona alla quale si richiedono le prove;

[8] Official Journal of the European Union, (1 maggio 2014), DIRECTIVE 2014/41/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 3 April 2014 regarding the European Investigation Order in criminal matters, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0041, Capitolo 1, Articoli 1,2 e 3

[9] Ibidem, Capitolo1, Articolo 5

[10] Dipartimento di Stato degli Stati Uniti d'America, (9 Novembre 1982), Mutual Legal Assistance Treaty Between the UNITED STATES OF AMERICA and ITALY, https://www.state.gov/wp-content/uploads/2019/02/85-1113-Italy-Mutual-Legal-Assist-Treaty.pdf, Roma, pag. 4

[11] Ibidem, pp.5-6

- Una descrizione del modo in cui qualsiasi testimonianza deve essere raccolta e registrata;
- Una descrizione dell'eventuale procedura particolare da seguire nell'esecuzione della richiesta;
- La richiesta e la documentazione di accompagnamento devono essere redatte sia in inglese che in italiano.

Conclusioni

Iniziative come gli "Action Day" o "Action Week" dimostrano che la collaborazione tra Paesi e agenzie internazionali di cooperazione di polizia non sia solo vantaggiosa, ma essenziale per affrontare minacce che si estendono oltre i confini nazionali. Attraverso le operazioni congiunte si moltiplica l'efficacia degli interventi, lo si deve al potenziamento delle capacità operative collettive, alla condivisione delle informazioni e al coordinamento delle attività investigative. Tali collaborazioni rendono possibili pianificazioni di strategie su vasta scala, offrendo un valido strumento di contrasto alle reti criminali internazionali e la protezione della sicurezza globale.

Attraverso piattaforme di comunicazione sicure e codificate, il sistema SIENA di EUROPOL e l'" I-24/7" di INTERPOL, gli Stati membri possono comunicare e coordinarsi sia in investigazioni in cui ogni paese agisce nella propria giurisdizione in modo autonomo, sia su operazioni simultanee che mirano alla disgregazione delle reti criminali coinvolte in attività pedopornografiche in brevissimo tempo.

Il carattere globale del crimine di abuso e sfruttamento sessuale dei minori online richiede risposte coordinate tra le forze dell'ordine e le istituzioni governative e non governative. L'azione collettiva rappresenta la chiave per affrontare la minaccia globale che questo crimine rappresenta.

Sitografia

Dipartimento di Giustizia degli Stati Uniti d'America, (agosto 2009), Moving Public-Private Partnerships From Rhetoric to Reality: CIRCAMP / CSAADF Transferability Assessment, https://www.ojp.gov/ncjrs/virtual-library/abstracts/moving-public-private-partnerships-rhetoric-reality-circamp-csaadf

Dipartimento di Stato degli Stati Uniti d'America, (9 Novembre 1982), Mutual Legal Assistance Treaty Between the UNITED STATES OF AMERICA and ITALY, Roma, https://www.state.gov/wp-content/uploads/2019/02/85-1113-Italy-Mutual-Legal-Assist-Treaty.pdf

Europol, (16 dicembre 2011), Joint action in 22 European countries against online child sexual abuse material in the internet, https://www.europol.europa.eu/mediapress/newsroom/news/joint-action-in-22-european-countries-against-online-child-sexual-abusematerial-in-internet

Europol, (2012), Data Protection at Europol, https://www.europol.europa.eu/sites/default/files/documents/europol_dpo_booklet_0.pdf

Europol, (10 giugno 2022), Secure Information Exchange Network Application (SIENA), https://www.europol.europa.eu/operations-services-and-innovation/servicessupport/information-exchange/secure-information-exchange-network-application-siena

Official Journal of the European Union, (1 maggio 2014), DIRECTIVE 2014/41/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 3 April 2014 regarding the European Investigation Order in criminal matters, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0041

Valeri, Mauro (gennaio 2024), INTERPOL - Un secolo di attività, inserto di Polizia Moderna, https://poliziamoderna.poliziadistato.it/statics/31/interpol.pd

Address correspondence to bianca.francesca.ber@alice.it

Received October 15, 2024 accepted October 25, 2024

Analisi delle attività di prevenzione alla pedopornografia online: Il Caso italiano

Bianca Francesca Berardi[1]

RIASSUNTO

L'espansione degli ambienti virtuali e la rapidità con cui si moltiplicano le tecnologie digitali favoriscono l'incremento dei casi di abuso e sfruttamento sessuale di minori, evidenziando la necessità di politiche di contrasto e percorsi educativi mirati. In Italia, la Polizia Postale, in collaborazione con enti governativi e organizzazioni internazionali, promuove campagne di informazione volte a educare cittadini di tutte le fasce d'età sui rischi connessi all'uso delle tecnologie digitali. L'obiettivo primario è contrastare fenomeni come sextortion e diffusione non consensuale di materiale sensibile, i quali possono culminare nella produzione e condivisione di contenuti pedopornografici.

Il presente studio analizza l'efficacia delle iniziative di prevenzione attraverso un'indagine empirica condotta su un campione di 175 individui, suddivisi per età, genere e livello di istruzione. I risultati evidenziano una conoscenza disomogenea del fenomeno: mentre la fascia di età 18-35 anni mostra maggiore consapevolezza, i minori e gli adulti over 50 dimostrano significative lacune informative. Inoltre, emerge una scarsa partecipazione a programmi di sensibilizzazione, con il 90% degli intervistati che dichiara di non aver mai ricevuto informazioni sui rischi dell'adescamento online su social network, chat di videogiochi online e app di messaggistica crittografate.

La ricerca sottolinea la necessità di strategie di comunicazione più mirate, adattate ai diversi target di età e ai canali digitali da essi frequentati. L'integrazione di strumenti interattivi e il coinvolgimento di istituzioni scolastiche risultano essenziali per un'efficace diffusione della consapevolezza e per la protezione dei minori da minacce digitali sempre più sofisticate.

Parole chiave: Prevenzione, Campagne di sensibilizzazione, Forme di adescamento, Social Network, Videogiochi online

[1] Dottoressa magistrale in Investigazione, Criminalità e Sicurezza Internazionale - Università degli Studi Internazionali di Roma (UNINT)

ABSTRACT

The expansion of virtual environments and the rapid proliferation of digital technologies contribute to the increase, in cases of child sexual abuse and exploitation, highlighting the need for counteracting policies and targeted educational programs. In Italy, the Italian police department Polizia Postale, in collaboration with government agencies and international organizations, promotes information campaigns aimed at educating citizens of all age groups about the risks associated with the use of digital technologies. The primary objective is to combat phenomena such as sextortion and the non-consensual dissemination of sensitive material, which can ultimately lead to the production and sharing of child sexual abuse and exploitation content.

This study analyses the effectiveness of prevention initiatives through an empirical investigation conducted on a sample of 175 individuals, categorized by age, gender, and level of education. The results reveal a heterogeneous understanding of the phenomenon: while the 18–35 age group demonstrates greater awareness, minors and adults over 50 exhibit significant informational gaps. Additionally, there is limited participation in awareness programs, with 90% of respondents stating that they have never received information about the risks of online grooming on social networks, online video game chats, and encrypted messaging apps.

The research underscores the need for more targeted communication strategies, tailored to different age groups and the digital channels they frequent. The integration of interactive tools and the involvement of educational institutions are essential for effectively disseminating awareness and protecting minors from increasingly sophisticated digital threats.

Keywords: Prevention, Awareness campaigns, Forms of solicitation, Social Networks, Online video games

RESUMEN

La expansión de los entornos virtuales y la rápida proliferación de las tecnologías digitales contribuyen al aumento de los casos de abuso y explotación sexual infantil, evidenciando la necesidad de políticas de lucha contra este fenómeno y de programas educativos específicos. En Italia, la Policía Postal, en colaboración con entidades gubernamentales y organizaciones internacionales, promueve campañas informativas dirigidas a educar a ciudadanos de todas las franjas de edad sobre los riesgos asociados

al uso de las tecnologías digitales. El objetivo principal es combatir fenómenos como la sextorsión y la difusión no consentida de material sensible, los cuales pueden culminar en la producción y el intercambio de contenido de abuso sexual infantil.

El presente estudio analiza la eficacia de las iniciativas de prevención a través de una investigación empírica realizada sobre una muestra de 175 individuos, clasificados según edad, género y nivel de educación. Los resultados evidencian un conocimiento heterogéneo del fenómeno: mientras el grupo de edad de 18 a 35 años muestra una mayor concienciación, los menores y los adultos mayores de 50 presentan importantes lagunas informativas. Además, se observa una escasa participación en programas de sensibilización, con un 90% de los encuestados que afirman no haber recibido nunca información sobre los riesgos de la captación de menores en redes sociales, chats de videojuegos en línea y aplicaciones de mensajería cifrada.

La investigación subraya la necesidad de estrategias de comunicación más específicas, adaptadas a los distintos grupos etarios y a los canales digitales que frecuentan. La integración de herramientas interactivas y la implicación de las instituciones educativas resultan esenciales para una difusión eficaz de la concienciación y para la protección de los menores frente a amenazas digitales cada vez más sofisticadas.

Palabras clave: Prevención, Campañas de sensibilización, Formas de solicitación, Redes sociales, videojuegos en línea

1. Introduzione

Per lotta ai crimini di sfruttamento e abuso sessuale di minori online e offline un compito molto rilevante delle forze dell'ordine e delle organizzazioni internazionali di cooperazione di polizia consiste nella prevenzione[2]. In Italia la multidisciplinarietà dell'approccio della Polizia Postale ha elaborato la promozione di campagne di informazione sull'argomento, dirette ai cittadini di ogni età, genere o estrazione sociale. Queste iniziative vengono portate avanti non solo dagli agenti delle forze dell'ordine, ma anche da enti privati che elaborano percorsi autonomi volti a favorire la sensibilizzazione progressiva sul tema di rischio reale e imminente online.

[2] "La prevenzione consiste nell'attività dirette a evitare o ridurre la possibilità che si verifichino danni ulteriori sulla base di conoscenze acquisite dalle precedenti attività di previsione, le quali sono dirette all'identificazione e allo studio degli scenari di rischio possibili. Prevenzione e attività di prevenzione fanno parte del ciclo di analisi del rischio di intelligence." Mantici A., Corso di Buone Pratiche di contrasto alla Criminalità, Università degli Studi Internazionali di Roma, 2023/2024

Nella realtà di tutti i giorni, a meno che non si partecipi fortuitamente alle campagne di sensibilizzazione o non si sia già informati dell'argomento tanto da seguire le pagine della Polizia di Stato e le organizzazioni interessate sui social, non è chiara la risonanza che l'argomento presenta nella popolazione di ogni età e genere.

Il presente articolo propone un'indagine delle conoscenze della popolazione italiana riguardo al crimine di abuso e sfruttamento sessuale online, i rischi che questo crimine porta ogni giorno e le azioni di prevenzione che ogni cittadino, minore o adulto, può attuare per proteggersi attraverso l'analisi di un questionario elaborato sulla base di informazioni reperite nelle brochure e nei documenti pubblici presenti nel sito della Polizia Postale italiana, sui documenti ufficiali pubblici di hotlines conosciute come Save the Children e Telefono Azzurro, e sulla base della documentazione ufficiale pubblica presente nelle pagine web di INTERPOL ed EUROPOL.

2. La prevenzione di abuso e sfruttamento sessuale di minori online in Italia

L'obiettivo principale delle campagne di informazione è la sensibilizzazione di minori e adulti in modo da prevenire rischi di pericoli dal web. Vi sono state due campagne significative con l'obiettivo di parlare dell'uso consapevole e responsabile di internet e delle nuove tecnologie, volto ai più giovani ma non solo. Si citano la "Safer Internet Day", istituita nel 2014 dalla Commissione Europea e il "Safer Internet Centre – Generazioni Connesse", istituito dalla Commissione Europea in accordo con il Ministero dell'Istruzione. Quando si affronta il tema dei crimini di abuso e sfruttamento sessuale di minori, sia online che offline, questo crimine viene comunemente associato alla tratta di minori e a gravi abusi fisici. Tuttavia, tale crimine comprende anche la vittimizzazione dei minori attraverso la diffusione di immagini che li ritraggono in atteggiamenti o situazioni inappropriate. Queste immagini possono derivare non solo da atti di abuso diretto, ma anche da fenomeni di sextortion o adescamento, compiuti online tramite piattaforme social, videogiochi o applicazioni di messaggistica crittografate.

"Una vita da social" è la più grande campagna educativa itinerante realizzata dalla Polizia Postale in accordo con il MIUR. L'obiettivo era la sensibilizzazione e la prevenzione dal rischio di abuso e sfruttamento online, differenziando i vari social network e spiegando l'utilizzo delle nuove tecnologie di messaggistica crittografata. La campagna ha raggiunto oltre 3 milioni di studenti, 230.000 genitori e 450 città. È stata pubblicizzata su Twitter, Facebook e sui siti ufficiali della Polizia Postale e del Ministero dell'Istruzione.

"Sfide e opportunità del Gaming per la diffusione delle competenze digitali", l'obiettivo di questa campagna è la costruzione di una cultura dei videogiochi sana, rendendo l'ambiente sicuro anche per i minori. Ha promosso la pubblicazione di consigli e suggerimenti per bambini e adulti da sfruttare nel mondo dei giochi online per ridurre al minimo i rischi.[3]

Oltre alle iniziative promosse dalla Polizia di Stato italiana, vi sono numerose organizzazioni che organizzano campagne di sensibilizzazione, come l'INTERPOL, INHOPE, ECPAT, Save the Children o il Telefono Azzurro. Molte di queste organizzazioni fungono anche da centri di hotline: forniscono un meccanismo di ricezione di segnalazione dal pubblico di contenuti illegali su internet, tramite interfaccia web a campo libero o via e-mail. La peculiarità delle hotline è che garantiscono l'anonimato per chiunque voglia segnalare qualsiasi attività sospetta, dall'immagine trovata online, al nome utente di un soggetto sospetto.[4] Le associazioni che fungono da hotlines avranno poi il compito di valutare la legalità del contenuto segnalato e, se ritenuto il caso, la segnalazione verrà passata alle agenzie delle forze dell'ordine dell'organizzazione o del paese competente.

"Know2Protect" è una campagna di sensibilizzazione particolare, lanciata dal Dipartimento della Sicurezza Nazionale degli Stati Uniti e arrivata in Italia grazie ai social. L'obiettivo è educare e responsabilizzare bambini, adolescenti, genitori, adulti e decisori politici per: prevenire e combattere lo sfruttamento e l'abuso sessuale dei minori online, spiegare come denunciare episodi di adescamento e vittimizzazione online e offrire risorse alle vittime, ai sopravvissuti e ai loro sostenitori. È particolare in quanto non solo vuole informare la popolazione dell'efferato crimine, ma si pone anche come sostegno in favore della lotta alla pedopornografia online attraverso la creazione di una piattaforma di segnalazione e di sostegno. Coinvolge moltissime aziende che lavorano con giovani e genitori, come la National Football League, e le sue collaborazioni puntano a coinvolgere gli adolescenti attraverso le piattaforme che più utilizzano. Utilizza Facebook e X, ma sopratutto Snapchat[5], social network molto popolare in America, che

[3]Polizia Postale, (5 maggio 2023), DENTRO I NUMERI - LA LOTTA ALLA PEDOFILIA ONLINE, https://www.interno.gov.it/sites/default/files/2023-05/dati_polizia_postale.pdf

[4] INHOPE – Association of Internet Hotline Providers, (2018), Code of Practice, https://inhope.org/media/site/1fffcc1905-1614610382/inhope_codeofpractice.pdf, p.3

[5] Snapchat è un'applicazione per dispositivi mobili e servizio di messaggistica istantanea multimediale americana. Una delle caratteristiche principali dell'applicazione è che le immagini e i messaggi sono solitamente disponibili solo per un breve periodo di tempo, deciso dall'utente che li invia, prima di diventare inaccessibili ai destinatari. Presenta anche la

per la campagna ha creato un filtro[6] interattivo per il quale vengono proposte una serie di informazioni relative al crimine di abuso e sfruttamento sessuale di minori, volto a informare ed educare attraverso un metodo interattivo e una piattaforma ampliamente utilizzata dal target di vittime colpito.

Vi sono ulteriori iniziative e campagne avviate dalle organizzazioni e forze dell'ordine di tutto il mondo che spingono ad una completa collaborazione e cooperazione da parte della popolazione. Un esempio particolare è la campagna "Stop Child Abuse – Trace an Object" avviata dalla VIDTF di EUROPOL e ripresa dalla Polizia Federale Australiana, sono due siti distinti che mirano a chiedere l'aiuto del pubblico nell'identificazione del luogo di provenienza di determinati oggetti di sfondo o il riconoscimento di stanze di hotel o settings di sfondo. La campagna ha avuto molto successo, con innumerevoli segnalazioni che hanno portato all'apertura di casi concreti su cui investigare.[7]

Come precedentemente detto, purtroppo, imbattersi in tali campagne non è comune, sebbene il lavoro di sensibilizzazione sia pensato per arrivare al massimo pubblico possibile.

3. Analisi sulla conoscenza del fenomeno di abuso e sfruttamento sessuale di minori online in Italia

L'indagine è basata su un questionario appositamente creato per lo studio con lo scopo di valutare il livello di conoscenza e consapevolezza del fenomeno tra un campione eterogeneo di persone. L'analisi permette di ottenere dati significativi sulla percezione del problema e sull'efficacia delle campagne di sensibilizzazione, evidenziando eventuali lacune o aree di miglioramento. Lo studio di queste indagini consente di comprendere in maniera più approfondita le dinamiche operative, l'efficacia della cooperazione internazionale, nonché le difficoltà incontrate nel contrasto a un crimine così complesso e radicato.

possibilità di pubblicazione di "Storie", immagini o video disponibili agli utenti per un periodo di 24 ore che insieme alla funzione "Scopri", funzionalità che permette agli utenti privati di guardare le "Storie" degli utenti pubblici, consente ai marchi di mostrare contenuti in formato breve supportati da pubblicità. Consente inoltre agli utenti di archiviare le foto in un'area protetta da password. https://snap.com/it-IT

[6] Snapchat introduce anche la possibilità agli utenti di interagire attraverso i "filtri": adesivi virtuali e oggetti di realtà aumentata che si presentano sullo schermo a ridosso dell'immagine puntata dalla fotocamera. Proprio per questa possibilità, Snapchat è popolare tra le generazioni più giovani, in particolare quelle di età inferiore ai 16 anni, il che porta a molte preoccupazioni sulla privacy per i genitori. https://snap.com/it-IT

[7] Europol, (2024), Stop Child Abuse - Trace an Object, https://www.europol.europa.eu/stopchildabuse

Ogni questionario a cui si fa riferimento è stato compilato da un singolo individuo, il totale delle persone che compongono il campionario investigato (175individui) sono state selezionate tramite un "campionamento di convenienza"[8].

I questionari sono stati visionati uno per volta, e i dati ottenuti sono stati inseriti manualmente in un file Excel, i grafici sono stati costruiti su base percentuale utilizzando come denominatore 175, ossia il numero totale dei questionari ottenuti.

Il questionario è suddiviso in quattro sezioni distinte al fine di raccogliere dati su aspetti specifici del tema oggetto di studio e comprendere al meglio la conoscenza dei soggetti sui pericoli presenti online per i minori. Queste informazioni servono a fornire un profilo generale per il campionario di persone coinvolte nell'indagine, inoltre, consentono di avere un'interpretazione dei dati qualitativi correlati alla situazione sociodemografica dei partecipanti.

3.1. Prima Sezione: generalità

La prima sezione riguarda le generalità delle persone a cui il questionario è stato sottoposto. In questa fase, vengono chiesti dati relativi all'età, livello di istruzione e regione di provenienza. Il campionario di persone prevede 175 individui, per il 72% di sesso femminile e 28% di sesso maschile, di età compresa tra la pubertà (13 anni) all'età più adulta (oltre i 50 anni). La fascia d'età maggiormente presente è quella compresa tra i 18 e i 25 anni, rappresentano il 33% sul totale di persone che hanno risposto al questionario.

Per quanto riguarda il livello di istruzione, il 36% dei partecipanti ha un diploma di scuola secondaria di secondo grado, il 27% ha conseguito la laurea triennale, il 23% la laurea magistrale e il 10% il diploma di scuola secondaria di primo grado. Rilevare il livello di istruzione è particolarmente importante in questo contesto, permette di valutare la diffusione delle campagne di sensibilizzazione in correlazione con i diversi livelli educativi per valutarne l'efficacia.

Infine, la provenienza geografica del campionario di persone è diversificata: la percentuale più alta è rappresentata dalla Lombardia (30%), seguono a livello di

[8] Il campionamento di convenienza è una tecnica di campionamento non probabilistico, in cui gli elementi sono selezionati in base alla comodità del ricercatore, in questo caso specifico il questionario è stato creato tramite Google Moduli, ed è stato poi inoltrato a individui che hanno provveduto a condividere il link legato al questionario con i propri conoscenti.

percentuale la Campania e il Lazio (16%), il Piemonte, la Liguria e la Puglia (10%). Una piccola percentuale di persone proviene da Umbria, Calabria, Toscana, Marche, Sicilia, Veneto, Emilia-Romagna, Friuli-Venezia Giulia ed Abruzzo. La totalità dei partecipanti minori di 18 anni è proveniente dalla regione Lazio.

Per l'analisi dei dati nelle sezioni successive, gli intervalli di età sono stati ristretti, per maggiore praticità, alle seguenti fasce: <15 – 18, 18 – 35 e 35 – >50.

3.2. Seconda Sezione: informazioni generali sull'argomento

La seconda sezione del questionario interroga il livello di conoscenza dei partecipanti riguardo a tematiche legate all'abuso e allo sfruttamento sessuale online. In particolare, si fa diretto riferimento alla conoscenza del termine "pedopornografia" e dei fenomeni online pericolosi per i minori: "sextortion", "sexting" e "revenge porn". In questa sezione vengono proposte 12 domande per capire e valutare la comprensione di tali problematiche e la consapevolezza dei rischi che queste condotte portano, soprattutto per i minori. Tali domande sono finalizzate a raccogliere dati sulle conoscenze generali dell'argomento, in modo da stabilire delle basi utili ad approfondire l'efficacia delle campagne di sensibilizzazione in merito.

La prima domanda indaga se si fosse già sentito parlare di "pedopornografia" online prima del questionario sottoposto. Il 92% delle persone intervistate ha risposto in modo affermativo. È però di particolare rilevanza il restante 8% di risposte negative, questa percentuale di persone è composta esclusivamente da minori di 18 anni e maggiori di 50 anni. In particolare, il 41% dei minori di 18 anni non aveva mai sentito parlare prima di "pedopornografia online".

Le domande seguenti indagano la conoscenza dei fenomeni di "sextortion", "sexting" e "revenge porn". In questo caso è interessante notare le differenze di conoscenza fra le diverse fasce d'età. Il 30% del campionario di intervistati adulto (35 – >50) non era a conoscenza dei fenomeni di sextortion e sexting in un contesto minorile, il revenge porn è invece un fenomeno più conosciuto fra gli adulti. Il 52% del campionario di intervistati minorenni (<15 – 18) ha dichiarato di non conosce questi fenomeni. Al contrario, il campionario di intervistati di età media (18 – 35), sembra conoscere molto bene questi tipi di fenomeni e problematiche, con una percentuale di risposte affermative del 92%.

Dopo aver posto domande sui termini generici, l'indagine è proseguita entrando più nello specifico della materia oggetto di indagine, verificando che il campionario di persone fosse consapevole che le immagini e i video di minori derivanti da atti di sextortion, sexting o revenge porn possano essere diffusi su siti pedopornografici.

Come per le domande generiche, vi sono differenze sostanziali fra i diversi gruppi di età. Il 30% del campionario di persone di età maggiore dei 35 anni non era consapevole di tale rischio, tranne che per le immagini di derivazione dall'atto criminoso del revenge porn, in quanto fenomeno più conosciuto come precedentemente stabilito, in questo caso si tratta dei medesimi questionari. Il 63% dei minori di 18 anni ha risposto a queste domande in modo negativo, rispetto alle domande generiche sulla conoscenza dei fenomeni si evidenzia un aumento della percentuale delle risposte negative del 50%, ciò implica che conoscono i fenomeni pericolosi per loro, ma non le conseguenze che questi fenomeni possono comportare. Analogamente alle domande generali su questi tre fenomeni, la percentuale di risposte affermative per il campionario di persone di età compresa fra i 18 e i 35 anni è pari al 87%, anche in questo caso si evidenzia un aumento delle risposte negative, sottolineando come la correlazione fra questi fenomeni non sia di conoscenza comune. Ciò sottolinea la necessità di potenziare le campagne di sensibilizzazione non solo per informare sui comportamenti rischiosi, ma anche per educare maggiormente la popolazione sui pericoli concreti che essi comportano, soprattutto i minori quali vittime primarie, e i loro genitori, in modo che possano aiutare a pervenire eventuali adescamenti.

L'indagine è proseguita approfondendo la questione relativa ai canali attraverso i quali tali persone hanno ottenuto informazioni riguardo le domande precedentemente poste, la risposta prevista per questa domanda è aperta, vi era la possibilità di scrivere ogni genere di contesto in cui si è venuti a conoscenza dell'argomento. Le risposte sono state omogenee con evidenti differenze tra le varie fasce d'età. Un dato importante, emerso da questa particolare domanda, indica una mancata trattazione dell'argomento di pedopornografia e dei rischi portati dalle condotte di sextortion, sexting e revenge porn in contesto scolastico. Le scuole, in quanto istituzioni per la formazione e lo sviluppo dei giovani, dovrebbero contribuire a informare gli studenti dei pericoli che corrono, in particolare, per questi crimini per cui i giovani rappresentano le principali vittime, e svolgere quindi un ruolo centrale nella prevenzione di questo crimine sempre più diffuso anche a causa dello sviluppo tecnologico. Tale mancanza compromette la possibilità di fornire ai giovani strumenti per potersi proteggere nel migliore dei modi. Rafforzare

l’educazione su questi argomenti delicati è essenziale per una corretta e completa prevenzione nel coinvolgimento di minori in situazioni rischiose.

Lo sviluppo tecnologico ha influenzato non solo il modo di compiere il reato, ma anche la metodologia con cui vengono condotte le indagini. Nell’ultima parte della seconda sezione dedicata alle informazioni generali, le domande proposte intendono valutare le conoscenze riguardo le innovazioni tecnologiche in questo campo: l’utilizzo dell’Intelligenza Artificiale per la creazione di materiale di abuso e sfruttamento sessuale di minori e la creazione di hotline anonime per la denuncia di materiali CSAM, siti pedopornografici e abusi reali.

La consapevolezza dell’utilizzo dell’Intelligenza Artificiale per la creazione di immagini CSAM è poco nota fra i più adulti e i minorenni: i minori hanno risposto negativamente per una percentuale del 77%, il gruppo più anziano presenta risposte negative per il 48%, mentre per il range di età a metà fra i due, il fenomeno sembra conosciuto, con una percentuale di risposte affermative pari all’84%. Le risposte affermative diminuiscono alla seconda domanda sull’argomento, che indaga il livello di conoscenza riguardo al fatto che le immagini di minori, pubblicate online dai minori stessi o da terzi, è utilizzato sia per alimentare i contenuti dei siti pedopornografici, sia per creare nuovo materiale CSAM tramite l’uso dell’Intelligenza Artificiale: per i minorenni si tratta di risposte negative pari al 88%, il gruppo più adulto con una percentuale del 64% e il gruppo mediano una percentuale pari al 37%.

L’abbassamento di percentuale di consapevolezza, che colpisce tutti i gruppi di età presi in considerazione, evidenzia una conoscenza limitata e poco diffusa delle nuove tecnologie applicate a certi tipi di crimine. Sebbene sia una questione molto delicata, la carenza di informazioni appare grave. È essenziale che minori e genitori, ma non solo, siano informati sugli sviluppi e i rischi emergenti legati a questo tipo di crimine in modo da poter adottare tutte le misure preventive ritenute adeguate. La consapevolezza dei pericoli legati all’utilizzo di nuove tecnologie è necessaria per consentire la tutela dei più giovani, e una campagna di sensibilizzazione mirata a tale target di persone è diventata di importanza essenziale per raggiungere un adeguato livello di formazione sull’argomento.

A conclusione di questa sezione, è stata approfondita la conoscenza riguardo alla natura e alla dimensione transnazionale del fenomeno trattato. Viene chiesto agli intervistati se fossero consapevoli del fatto che i siti pedopornografici, sebbene possano essere

amministrati in un unico paese, operano attraverso una rete internazionale attiva che collega numerosi paesi, per questo la cooperazione internazionale transfrontaliera è fondamentale. Questo crimine genera ri-vittimizzazione dei minori, le cui immagini sensibili vengono diffuse a livello globale su siti pedopornografici, complicando notevolmente la possibilità di fermare questo fenomeno.

Dall'indagine, la conoscenza di questo fatto riscontra una consapevolezza dell'88% negli intervistati adulti (35- maggiori di 50 anni) e di fascia d'età media (18 – 35). Il 12% dei restanti è composto quasi totalmente da minori di 18 anni, ciò rappresenta il dato fondamentale in questa particolare domanda: dei minorenni, solo il 60% è consapevole della natura inevitabilmente transnazionale del crimine e delle ripercussioni globali che ne derivano per le vittime. Sebbene questa percentuale sia comunque elevata, è preoccupante in considerazione della gravità dei crimini e dei rischi associati, evidenziando la necessità di una più profonda educazione riguardo questa materia. Diventa perciò di importanza determinante, non solo informare e sensibilizzare la popolazione circa i pericoli che incorrono nell'utilizzo dei social e dei rischi conseguenti a livello globale, ma anche riguardo gli sforzi significativi della Polizia nella collaborazione con forze dell'ordine di altri paesi e con le organizzazioni internazionali, di polizia e indipendenti, che si occupano di questi crimini. Tali cooperazioni facilitano le indagini e le operazioni per la salvaguardia dei minori con grande successo e offrono strumenti dediti alla cooperazione e reciprocità tra le diverse giurisdizioni. Il 90% degli intervistati dichiara di non conoscere iniziative promosse dalle forze dell'ordine o dalle varie organizzazioni. Il dato significativo emerso da questa particolare domanda risulta nel 10% degli intervistati che ha risposto in maniera positiva: i questionari di tali soggetti sono stati esaminati singolarmente, è emerso che questi individui hanno frequentato corsi di studio universitari nei quali l'argomento viene trattato oppure lavorano in questo settore. Si evidenzia quindi un ampio margine di miglioramento nella diffusione di informazione al pubblico, al fine di ottenere una collaborazione internazionale realmente inclusiva, che coinvolga non solo le forze di polizia e le organizzazioni indipendenti, ma anche i cittadini mossi da senso civico e spirito di collaborazione e solidarietà.

3.3. Terza Sezione: informazioni sull'utilizzo di social media e videogiochi online

La terza sezione si concentra sull'utilizzo dei social network e dei videogiochi online, strumenti ormai ampiamente diffusi tra i giovani e tra i principali veicoli di sfruttamento

sessuale. Le domande indagano quali di queste piattaforme il singolo individuo utilizza e verificano la consapevolezza dei partecipanti in merito ai rischi legati all'abuso e allo sfruttamento sessuale di minori perpetrati attraverso questi mezzi, comprese le applicazioni messaggistiche crittografate che rendono più difficile il tracciamento dei crimini. Questa sezione consente di valutare il grado di esposizione ai pericoli online dei minori, la capacità dei partecipanti di riconoscerli e valutare i social più utilizzati in base alle età al fine di una più mirata campagna di sensibilizzazione sui social, che punti a toccare adulti e giovanissimi.

Ad eccezione di Instagram, che risulta essere il più utilizzato dalla maggioranza, che vede quasi il 100% di utilizzo da parte di tutte le fasce di età, nell'utilizzo degli altri social si crea come un gap generazionale: i social network più datati tendono ad essere impiegati maggiormente dalla popolazione adulta, che rimane legata ai primi social e ad un metodo più tradizionale di condivisione, mentre i social network più recenti vengono utilizzati dai più giovani che approcciano nuovi metodi più rapidi e interattivi, che prediligono la condivisione di contenuti multimediali. Si prenda ad esempio Facebook, social network ancora ampliamente utilizzato, il campionario di persone investigate vede il 100% di utilizzo per la fascia d'età compresa fra i 35 e i maggiori di 50 anni, mentre è pari 0% nelle risposte dei più giovani e 27% per la fascia di età compresa tra i 15 e i 18 anni, che invece utilizzano Instagram e TikTok.

La domanda relativa all'utilizzo dei social network del campionario di persone intervistate è stata posta in modo da poter raccogliere dati concreti a supporto di una pianificazione eventuale di una campagna di sensibilizzazione mirata a contesti in cui vi sia scarsa consapevolezza di tali crimini, come dimostrato dai dati raccolti da alcune domande della seconda sezione. Tale analisi evidenzia quali siano le preferenze delle varie fasce d'età in materia di social network e ha l'obiettivo di offrire una base su cui poter progettare azioni di prevenzioni più efficaci. Se si intendesse promuovere una campagna rivolta ai più giovani, sarebbe più efficiente mirare a social network che utilizzano e adottare i format e il linguaggio con cui familiarizzano. Lo stesso vale per le varie fasce di età intervistate, in quanto dall'analisi è emerso che ogni range di età mostra un particolare interesse verso un social network che altre fasce di età non utilizzano. La strategia comunicativa deve essere flessibile e adattabile al target di persone a cui ci si rivolge, dagli adulti ai più giovani e deve tenere conto delle diverse specificità che ogni target potrebbe presentare, in modo da poter veicolare il messaggio più efficacemente possibile.

La seconda e ultima parte della terza sezione del questionario si concentra sull'indagine riguardo l'utilizzo dei giochi online, in modo da valutare quali fasce d'età ne facciano uso più frequentemente. In generale, del campionario di persone investigate solo il 26% utilizza videogiochi in modalità online. Di questa percentuale, fanno parte il 56% della fascia d'età <15–18 anni, il 35% del range di età media (18-35) e il 17% della fascia adulta (35–>50). Denotabile come proprio la fascia vulnerabile per questo tipo di crimine risulta, dall'indagine, quella che utilizza di più i giochi in modalità online.

Un dato rilevante ottenuto dall'analisi incrociata rispetto agli intervistati che utilizzano i giochi online e quelli che conoscono i rischi di adescamento tramite essi risulta interessante. Del campionario di intervistati appartenenti alla fascia di età media (18-35 anni) e la fascia più adulta (35-50< anni), il 40% è conscio dei rischi legati ai giochi online, rispetto agli intervistati minorenni, di cui solo il 19% è conscio dei rischi legati ai giochi online, la percentuale è molto più alta. Sono comunque tutte percentuali basse e rappresentano una lacuna informativa sostanziale, in quanto i minori sono proprio coloro che utilizzano maggiormente la modalità online e rappresentano le vittime del fenomeno criminoso indagato. Per quanto riguarda il resto degli intervistati, sebbene il 40% per entrambe le fasce sia conscio dei rischi, rimane un restante 60% che è ignaro delle possibili conseguenze legate all'utilizzo dei giochi online. È un dato molto rilevante considerando che si tratta della fascia d'età composta da partecipanti che potrebbero essere genitori responsabili di minori. È essenziale per questa fascia d'età essere informati sui rischi legati ai giochi online in modo da proteggere al meglio i propri figli da situazioni di adescamento e abuso.

Dato il frequente utilizzo da parte dei minori di piattaforme di gioco online e allo stesso tempo la loro scarsa consapevolezza dei rischi che questi ambienti portano, diventa essenziale e urgente promuovere maggiori campagne di sensibilizzazione proprio su tale argomento, non solo fra i minori, ma anche fra i genitori e gli adulti in generale, per aumentare la prevenzione e contrastare in modo efficace i rischi.

3.4.Quarta Sezione: informazioni sulle campagne di sensibilizzazione

Nella quarta sezione si affronta il tema delle campagne di sensibilizzazione sull'abuso e lo sfruttamento sessuale online e sui pericoli che i minori incorrono navigando in web o nell'utilizzo dei social media e dei videogiochi online. Ai partecipanti al questionario sono state poste domande riguardanti il proprio eventuale coinvolgimento in campagne di sensibilizzazione o di prevenzione sull'abuso e sfruttamento sessuale di minori o

sull'uso sicuro di internet in modo diretto, sui social o tramite altri mezzi di comunicazione.

La prima domanda mirava a verificare il coinvolgimento in iniziative di sensibilizzazione e prevenzione da parte di forze dell'ordine, associazioni o istituzioni educative o di qualsiasi genere e, nel caso di risposta affermativa, di indicarne il contesto del coinvolgimento. I risultati evidenziano 145 risposte negative su 175 partecipanti. Solo 30 partecipanti hanno risposto in modo affermativo: 5 tra loro fanno parte della fascia d'età più adulta e hanno indicato di essere stati coinvolti per la prima volta in iniziative simili in ambito lavorativo; gli individui nella fascia d'età dai 25 ai 35 anni hanno indicato per la maggioranza il contesto universitario.

Dalle risposte ottenute da questo questionario si evince che vi è una particolare presenza di iniziative di sensibilizzazione, in ambito scolastico e istituzionale, nelle regioni Lombardia e Lazio, mettendo in luce una evidente disparità territoriale nella diffusione di campagne preventive rispetto alle altre regioni coinvolte nel questionario citate nella seconda sezione. Tali dati potrebbero indicare una maggiore presenza di campagne di prevenzione e sensibilizzazione o una migliore strategia comunicativa ed educativa, ma potrebbe anche dipendere dalla percentuale di intervistati appartenenti alle due regioni sopra citate. Rimane, in ogni caso, fondamentale garantire una distribuzione equa di tali iniziative su tutto il territorio, per evitare che alcune aree della nazione rimangano meno protette e informate sui rischi anche emergenti derivati dall'utilizzo di internet. Più in generale, la grande lacuna informativa è rappresentata dalla limitata partecipazione a tali campagne dei soggetti minorenni, che costituiscono la fascia vulnerabile per questo tipo di crimine. Soprattutto in contesti scolastici o contesti sociali frequentati da minori, vi è la necessità di incrementare iniziative e campagne di prevenzione e sensibilizzazione, poiché si rischia di lasciare esposti coloro che più necessitano di informazioni e strumenti conoscitivi e pratici riguardo ai rischi legati all'uso di internet in modo da potersi proteggere autonomamente.

Successivamente, le domande sono volte a indagare se i partecipanti al questionario abbiano mai incontrato, sui social utilizzati, campagne di sensibilizzazione relative all'abuso e allo sfruttamento sessuale di minori online, alla possibilità di adescamento ed altri comportamenti rischiosi perpetrati sui social e in generale all'uso sicuro di internet. In caso di risposta affermativa, è stato chiesto se queste campagne fossero state percepite interessanti e coinvolgenti, tali da spingere l'utente a fermarsi a leggere. Il 37,7% ha dichiarato di essersi imbattuto sui social in tali campagne, questa percentuale è composta

da 66 individui appartenenti a fasce d'età comprese tra i 18 e i 50 anni, ma fra questi, solo 20 individui hanno risposto di aver provato interesse per le campagne ed essersi fermati a leggere. Le campagne potrebbero quindi essere sviluppate con strategie più mirate alle fasce d'età più vulnerabili, e potrebbero utilizzare linguaggi e format specifici popolari fra tali target per essere più coinvolgenti. L'obiettivo, in un'epoca in cui i contenuti video diventano sempre più di breve durata, e l'attenzione diviene sempre più limitata, deve essere quello di rendere le informazioni importanti accessibili ma soprattutto coinvolgenti, soprattutto se le vittime fanno parte delle fasce di età vulnerabili e poco consce dei pericoli che li circondano.

In seguito, è stato chiesto ai partecipanti se si fossero mai imbattuti in campagne di sensibilizzazione sui rischi legati all'utilizzo della modalità online dei videogiochi, attraverso qualsiasi forma e mezzo di comunicazione. La risposta è stata in gran parte negativa: il 90% dei partecipanti ha risposto di non aver mai partecipato o visto iniziative di tal genere. È un dato particolarmente rilevante se messo in relazione con i risultati ricevuti dalle domande della terza sezione, nelle quali è evidente come il fenomeno di adescamento di minori tramite videogiochi online sia il meno conosciuto, con una percentuale del 50% sul totale delle risposte. Tale fenomeno risulta, da questa particolare indagine, essere il meno pubblicizzato dalle campagne di sensibilizzazione sull'uso di internet sicuro. Meriterebbe, invece, attenzione particolare per poter prevenire situazioni di rischio che possono coinvolgere proprio quelle fasce più giovani e vulnerabili. Le modalità di gioco online prevedono la possibilità di interagire in modo costante e in tempo reale fra utenti attraverso chat messaggistiche o vocali, creando un ambiente ideale per fenomeni pericolosi come quelli indagati. Le campagne preventive dovrebbero tenere conto della grande popolarità, soprattutto fra i più giovani, di questo genere di modalità di gioco ed essere maggiormente mirate ad informare la popolazione, minori e genitori, circa le dinamiche pericolose che possono svilupparsi e i comportamenti che si potrebbe adottare per proteggersi.

L'ultima domanda del questionario è stata posta con l'obiettivo di valutare l'efficacia delle campagne di sensibilizzazione riguardanti l'abuso e lo sfruttamento sessuale di minori online, nonché l'uso sicuro di internet e dei social media. In particolare, si è chiesto ai partecipanti se, in seguito alla loro partecipazione o esposizione a una campagna di sensibilizzazione, il loro atteggiamento e il loro comportamento nei confronti dei social e di internet in generale fossero cambiati. Si trattava di una domanda a risposta libera e non obbligatoria, volta a raccogliere testimonianze dirette sull'impatto

reale di tali iniziative. I risultati mostrano solo il 9% dei partecipanti con una percezione e approccio a internet modificati a seguito di coinvolgimenti in campagne di sensibilizzazione. L'8% ha invece risposto in modo negativo, dichiarando che tali campagne non hanno avuto sufficiente impatto da modificare il modo di porsi a internet e ai social. Anche se, ancora una volta, il dato più significativo riguarda l'83% dei partecipanti che ha dichiarato di non essere mai stato coinvolto in nessun genere di campagna di sensibilizzazione.

Molti genitori hanno dichiarato di aver acquisito una maggiore consapevolezza dei rischi legati all'utilizzo di social, videogiochi online e internet in generale per poter adottare strategie di controllo e dialoghi più adatti a proteggere i propri figli da eventuali rischi. Mentre, purtroppo, molti giovanissimi, hanno risposto che le campagne di sensibilizzazione che hanno riscontrato online o a cui hanno partecipato di persona non sono state abbastanza coinvolgenti o interessanti da scaturire dubbi e modificare il proprio comportamento verso i social e internet.

Nel mondo di oggi, i rischi online sono in continua crescita e diventa sempre più importante garantire l'accesso alle informazioni per una corretta prevenzione da tali problematiche. L'alta percentuale di coloro che non sono ancora mai stati coinvolti nelle campagne di sensibilizzazione rappresenta un punto critico da cui partire per lo sviluppo di nuove campagne più mirate al target di età che diventa vittima di tali crimini. Aumentare la presenza e la visibilità di queste iniziative sui social media e in contesto scolastico contribuirebbe alla sensibilizzazione di un maggiore numero di persone che potrebbero cadere vittima dei crimini indagati.

4. Conclusioni

Le forze dell'ordine e le organizzazioni internazionali di cooperazione di polizia svolgono un ruolo fondamentale nella prevenzione del crimine di abuso e sfruttamento sessuale di minori, online e offline. In Italia, la Polizia di Stato promuove campagne di sensibilizzazione dirette a ogni genere di cittadino, coinvolgendo anche enti privati che operano autonomamente per diffondere informazioni e aiutare nelle campagne di prevenzione riguardo i rischi legati all'utilizzo di internet.

Come emerge dal questionario presentato, sottoposto a un campionario diversificato di persone, la partecipazione del pubblico alle campagne di sensibilizzazione è fondamentale, ma spesso limitata. A meno che non vi sia un coinvolgimento diretto, molte persone non sono consapevoli delle iniziative attive in corso.

Dalle risposte ottenute dai questionari si evince che più del 50% dei minori di 18 anni, fascia vulnerabile per questi tipi di crimini, non ha dimostrato una grande conoscenza dell'argomento: né i rischi legati all'utilizzo poco sicuro di internet né dei pericoli a lungo termine che questi rischi possono portale. Si tratta di condotte quali adescamento, sextortion, revenge porn e possibili pubblicazioni non consensuali di immagini e video derivanti da sexting. Inoltre, queste condotte già di per sé pericolose, possono portare a una ri-vittimizzazione dei minori a causa della possibile pubblicazione di loro immagini e video in siti pedopornografici e divenire così materiale di abuso e sfruttamento sessuale. In più, non vi è conoscenza della possibilità di incorrere in situazioni di adescamento tramite giochi online, specialmente tra il pubblico adulto, lacuna informativa che necessita di campagne di informazione mirate, come la campagna "Sfide e opportunità del Gaming per la diffusione delle competenze digitali", che mira alla costruzione di una cultura dei videogiochi sana, promuovendo la pubblicazione di consigli e suggerimenti per bambini e adulti da sfruttare nel mondo dei giochi online per ridurre al minimo i rischi.

È emersa quindi la necessità di adottare strategie più mirate nella progettazione di campagne di sensibilizzazione in merito all'abuso e allo sfruttamento sessuale di minori online connesso all'utilizzo di internet, dei social network e dei videogiochi online, sia nelle campagne dirette, in strutture in cui la formazione del giovane è di primaria importanza, sia nelle campagne online. È essenziale adattare ogni iniziativa ai diversi target, tenendo conto delle specifiche preferenze di mezzi di comunicazione e informazione e dei rischi che ciascuna fascia d'età corre. Anche l'attrattività di tali campagne deve essere mirata, attraverso un utilizzo di formate linguaggi adatti al target interessato, con l'obiettivo di informare e proteggere le fasce più vulnerabili.

Il coinvolgimento delle scuole e delle istituzioni dovrebbe essere particolarmente rilevante per affrontare la scarsa consapevolezza tra i minori sui pericoli specifici di fenomeni come "sextortion" o "revenge porn", per promuovere l'uso sicuro dei social e delle piattaforme di gioco online, aree in cui avviene parte delle attività criminali, e per incoraggiare la collaborazione dei cittadini sia nelle attività di segnalazione e identificazione di comportamenti, siti o immagini sospette, sia in attività di sensibilizzazione.

Sitografia

Europol, (2024), Stop Child Abuse - Trace an Object, https://www.europol.europa.eu/stopchildabuse

INHOPE – Association of Internet Hotline Providers, (2018), Code of Practice, https://inhope.org/media/site/1fffcc1905-1614610382/inhope_codeofpractice.pdf

Polizia Postale, (5 maggio 2023), DENTRO I NUMERI - LA LOTTA ALLA PEDOFILIA ONLINE, https://www.interno.gov.it/sites/default/files/2023-05/dati_polizia_postale.pdf

Snapchat, (2024), Official Site, https://snap.com/it-IT

Address correspondence to bianca.francesca.ber@alice.it

Received October 29, 2024 accepted Nomember 15, 2024